

DANH MỤC CÁC TỪ VIẾT TẮT

STT	KÝ HIỆU	NGUYÊN NGHĨA
1	ASOSAI	Tổ chức các Cơ quan Kiểm toán tối cao châu Á
2	ATTT	An toàn thông tin
3	BCTC	Báo cáo tài chính
4	CAATs	Viết tắt tiếng Anh: Computer Assisted Audit Techniques - Các kỹ thuật kiểm toán với sự hỗ trợ của máy tính.
5	CNTT	Công nghệ thông tin
6	CSDL	Cơ sở dữ liệu
7	DVBN	Dịch vụ bên ngoài
8	ĐMKT	Đầu mối kiểm toán
9	HĐLT	Hoạt động liên tục
10	HQĐT	Hệ thống Hải quan điện tử của Tổng cục Hải quan
11	INTOSAI	Tổ chức Quốc tế các cơ quan Kiểm toán tối cao
12	ISSAI	Hệ thống các Chuẩn mực kiểm toán của các Cơ quan Kiểm toán Tối cao
13	KBNN	Kho bạc nhà nước
14	KPTH	Khắc phục thảm họa
15	KTTC	Kiểm toán tối cao
16	KTNN	Kiểm toán nhà nước
17	KTV	Kiểm toán viên
18	NSNN	Ngân sách nhà nước

19	SAI	Viết tắt tiếng Anh: Supreme Audit Institutions - Cơ quan Kiểm toán tối cao
20	SDLC	Viết tắt tiếng Anh: System Development Life Cycle – Vòng đời phát triển phần mềm
21	SLA	Viết tắt tiếng Anh: Service Level Agreement - Thỏa thuận cung cấp dịch vụ
22	TABMIS	Hệ thống thông tin Quản lý Ngân sách và Kho bạc của Kho bạc Nhà nước
23	TCHQ	Tổng cục Hải quan
24	TCT	Tổng cục Thuế
25	TMS	Hệ thống quản lý thuế tập trung của Tổng cục Thuế

LỜI NÓI ĐẦU

Ngày nay, công nghệ thông tin (CNTT) đóng vai trò quan trọng trong mọi mặt của đời sống kinh tế - xã hội. Đảng và Chính phủ Việt Nam đã chọn CNTT là một trong những nhiệm vụ trọng tâm cần đẩy mạnh phát triển, và không ngừng tăng cường đầu tư cho CNTT nhằm tận dụng tối đa các ưu thế và thành quả của cách mạng công nghệ 4.0, hướng đến Chính phủ điện tử với các hệ thống cơ sở dữ liệu quốc gia. Hệ thống thông tin quản lý, hạ tầng CNTT... được triển khai trên diện rộng tại hầu hết các cơ quan nhà nước, các bộ ban ngành và các tổ chức đã làm thay đổi phương pháp kiểm toán cùng cách thức làm việc của Kiểm toán nhà nước. Chính vì vậy, kiểm toán CNTT đã trở thành một nhu cầu cấp thiết đối với Kiểm toán nhà nước và sẽ không ngừng phát triển trong tương lai.

Với tầm nhìn chiến lược phát triển lâu dài, Kiểm toán nhà nước đã xác định kiểm toán CNTT là một trong những định hướng phát triển cần đẩy mạnh. Điều này được cụ thể hóa trong Kế hoạch tổng thể phát triển CNTT đến năm 2020 và những năm tiếp theo. Kiểm toán nhà nước đã cử các Đoàn đi học tập kinh nghiệm triển khai kiểm toán CNTT ở các cơ quan Kiểm toán tối cao (SAI) như: Ấn Độ, Hàn Quốc, Malaysia nhằm chuẩn bị cho việc triển khai và phát triển kiểm toán CNTT tại Kiểm toán nhà nước.

Tháng 10 năm 2015, Kiểm toán nhà nước đã thành lập Phòng kiểm toán CNTT trực thuộc Trung tâm Tin học. Kiểm toán nhà nước đã bước đầu tổ chức triển khai ứng dụng một số nội dung kiểm toán CNTT trong hoạt động kiểm toán ở 05 Đoàn kiểm toán ngân hàng và ngân sách địa phương trong hai năm 2015 và 2016. Đặc biệt, tháng 11 năm 2016 kiểm toán CNTT lần đầu tiên được triển khai thành một cuộc kiểm toán độc lập tại Ngân hàng Ngoại thương Việt Nam. Các kết quả của việc áp dụng kiểm toán CNTT mang lại đã được Kiểm toán nhà nước đánh giá cao. Các thành quả chính là: Việc tiếp cận được dữ liệu gốc của đơn vị; Phát hiện những sai sót mang tính hệ thống; Hỗ trợ Đoàn thực hiện các nội dung khó đòi hỏi kỹ thuật phân tích và đối chiếu dữ liệu lớn. Đặc biệt, qua các kinh nghiệm và kết quả thực tiễn đã giúp Kiểm toán nhà nước hình thành những phương pháp tiếp cận và kiểm toán mới cho những hệ thống nghiệp vụ được vận hành bởi các hệ thống CNTT.

Tài liệu hướng dẫn kiểm toán CNTT (gọi tắt là Hướng dẫn) ra đời nhằm mục đích đẩy mạnh hơn nữa việc triển khai các nội dung kiểm toán CNTT tại Kiểm toán nhà

nước. Hướng dẫn tập trung vào 03 hoạt động chính trong việc triển khai kiểm toán CNTT tại Kiểm toán nhà nước bao gồm: kiểm toán hệ thống CNTT, kiểm toán dự án CNTT và kiểm toán trong môi trường CNTT. Hướng dẫn sẽ hướng dẫn chi tiết từng nội dung kiểm toán, mô tả cách thức áp dụng kiểm toán CNTT cho từng loại hình kiểm toán. Hướng dẫn cũng đề cập đến mối tương quan giữa 3 hoạt động trên.

Phương pháp xây dựng Hướng dẫn dựa trên các chuẩn mực kiểm toán của Kiểm toán nhà nước, các tài liệu về kiểm toán CNTT của các cơ quan kiểm toán tối cao trên thế giới như: Chuẩn mực ISSAI 5300 hướng dẫn kiểm toán CNTT của Tổ chức các cơ quan kiểm toán tối cao (INTOSAI) ban hành năm 2016; Sổ tay hướng dẫn kiểm toán CNTT của INTOSAI ban hành năm 2014; Hướng dẫn kiểm toán CNTT của Tổ chức các cơ quan kiểm toán tối cao Châu Á (ASOSAI) năm 2003; Sổ tay hướng dẫn kiểm toán CNTT của Kiểm toán nhà nước Mỹ; Sổ tay hướng dẫn Kiểm toán CNTT của ISACA- Hiệp hội quốc tế Kiểm toán và kiểm soát hệ thống CNTT. Ngoài ra, trong quá trình xây dựng tài liệu cũng nhận được sự tham gia và đóng góp ý kiến từ các chuyên gia của Công ty kiểm toán KPMG trong khuôn khổ hợp tác giữa Kiểm toán nhà nước và dự án GIG do tổ chức USAID tài trợ. Bên cạnh đó, việc xây dựng tài liệu được đúc rút kinh nghiệm từ các cuộc kiểm toán có sự thử nghiệm ứng dụng kiểm toán CNTT đã được triển khai trước đây của Kiểm toán nhà nước. Các nội dung hướng dẫn được xây dựng tuân thủ theo đúng các chuẩn mực, quy định và quy trình của Kiểm toán nhà nước liên quan đến các hoạt động kiểm toán.

Bố cục của hướng dẫn gồm 3 phần: Phần I- Hướng dẫn chung giới thiệu các nguyên tắc của kiểm toán CNTT; Phần II – Hướng dẫn chi tiết kiểm toán CNTT theo từng loại hình hoạt động, chuyên đề, vấn đề kiểm toán CNTT dưới dạng các chương trình kiểm toán mẫu, các bảng hỏi chi tiết; Phần III bao gồm các Phụ lục là các biểu mẫu, danh sách chi tiết hỗ trợ hoạt động kiểm toán.

Hướng dẫn này được hoàn thiện nhờ sự quan tâm sát sao của lãnh đạo Kiểm toán nhà nước, hỗ trợ của các đồng nghiệp trong Kiểm toán nhà nước và sự giúp đỡ của các chuyên gia đến từ dự án GIG dưới sự tài trợ của tổ chức USAID. Nhóm biên soạn chân thành cảm ơn lãnh đạo cùng các đồng nghiệp tại Kiểm toán nhà nước và dự án GIG.

Đây là phiên bản đầu tiên của Cẩm nang hướng dẫn kiểm toán CNTT của Kiểm toán nhà nước và sẽ được cập nhật bổ sung kịp thời. Vì vậy, nhóm biên soạn rất mong nhận được sự góp ý của đồng nghiệp. Mọi thắc mắc liên quan đến việc triển khai thực

tế kiểm toán CNTT xin gửi về: Phòng Kiểm toán CNTT, KTNN chuyên ngành VII –
Kiểm toán nhà nước.

Phần I - HƯỚNG DẪN CHUNG

A. KHUNG KIỂM TOÁN CÔNG NGHỆ THÔNG TIN

1. Quy định chung

a. Cơ sở xây dựng

- 1.1. Hướng dẫn này được xây dựng và phát triển dựa trên cơ sở CMKTNN 100 - Các nguyên tắc cơ bản trong hoạt động kiểm toán của Kiểm toán nhà nước; CMKTNN 200 - Các nguyên tắc cơ bản của kiểm toán tài chính; CMKTNN 300 - Các nguyên tắc cơ bản của kiểm toán hoạt động; CMKTNN 400 - Các nguyên tắc cơ bản của kiểm toán tuân thủ; Các chuẩn mực khác của Kiểm toán nhà nước được viện dẫn để làm rõ các nội dung liên quan đến kiểm toán CNTT; Các hướng dẫn kiểm toán CNTT của các Tổ chức kiểm toán quốc tế gồm: ISSAI 5300 – Hướng dẫn kiểm toán CNTT của Tổ chức các cơ quan kiểm toán tối cao (INTOSAI) ban hành năm 2016; Sổ tay hướng dẫn kiểm toán CNTT của INTOSAI ban hành năm 2014; Hướng dẫn kiểm toán CNTT của Tổ chức các cơ quan kiểm toán tối cao Châu Á (ASOSAI) năm 2003; Sổ tay hướng dẫn kiểm toán CNTT của Hiệp hội Quốc tế kiểm toán và kiểm soát hệ thống CNTT – ISACA.

b. Mục đích và phạm vi áp dụng

- 1.2. Hướng dẫn này là cơ sở giúp Kiểm toán viên nhà nước thực hiện kiểm toán CNTT dưới hình thức là cuộc kiểm toán độc lập hoặc cuộc kiểm toán được thực hiện kết hợp với kiểm toán tài chính hoặc kiểm toán hoạt động hoặc kiểm toán tuân thủ hoặc kết hợp cả 03 loại hình kiểm toán.
- 1.3. Các nội dung trong Hướng dẫn làm cơ sở cho việc xây dựng các chương trình kiểm toán mẫu và chương trình kiểm toán cho từng cuộc kiểm toán cụ thể liên quan đến kiểm toán CNTT trình bày ở phần Phụ lục của Hướng dẫn này.
- 1.4. Trường hợp cuộc kiểm toán CNTT kết hợp với kiểm toán tài chính, kiểm toán hoạt động hoặc kiểm toán tuân thủ, Kiểm toán viên nhà nước phải tuân thủ các chuẩn mực và hướng dẫn của kiểm toán tài chính, kiểm toán hoạt động hoặc kiểm toán tuân thủ. Trường hợp có sự khác biệt giữa các chuẩn mực và hướng

dẫn của các loại hình kiểm toán, Kiểm toán viên nhà nước phải ưu tiên áp dụng nhóm chuẩn mực cùng hướng dẫn phù hợp với loại hình kiểm toán được áp dụng và nội dung trọng tâm của cuộc kiểm toán.

- 1.5. Kiểm toán viên nhà nước phải tuân thủ các quy định và hướng dẫn của Hướng dẫn này trong quá trình thực hiện kiểm toán CNTT. Đơn vị được kiểm toán, các bên có liên quan và các bên sử dụng kết quả kiểm toán CNTT phải có những hiểu biết cần thiết về các quy định và hướng dẫn của Hướng dẫn này để phối hợp công việc với Kiểm toán viên nhà nước và giải quyết các mối quan hệ trong quá trình kiểm toán.

c. Nguyên tắc sử dụng thuật ngữ

- 1.6. Các thuật ngữ sử dụng trong Hướng dẫn này được định nghĩa như trong các chuẩn mực kiểm toán do Kiểm toán nhà nước ban hành. Danh sách thuật ngữ kỹ thuật nằm trong phần Phụ lục B của Hướng dẫn.

2. Giới thiệu kiểm toán Công nghệ thông tin

a. Thách thức và bối cảnh ra đời kiểm toán CNTT

- 2.1. Thảm quyền và mục tiêu kiểm toán công của Kiểm toán nhà nước được quy định trong CMKTNN.100 - Các nguyên tắc cơ bản trong hoạt động kiểm toán của Kiểm toán nhà nước như sau:

- (i) Kiểm toán nhà nước thực hiện kiểm toán liên quan đến việc quản lý và sử dụng tài sản công, tài chính công (CMKTNN.100.7-8).
- (ii) Kiểm toán nhà nước giúp tăng cường tính hiệu quả, trách nhiệm giải trình, hiệu quả và tính minh bạch của dịch vụ hành chính công nói chung và các hệ thống CNTT liên quan (CMKTNN.100.9-13).

- 2.2. Điều này đang đặt ra cho Kiểm toán nhà nước các thách thức liên quan đến lĩnh vực CNTT như sau:

- (i) CNTT đã và đang là một trong những động lực quan trọng, thúc đẩy sự phát triển kinh tế – xã hội. Đầu tư của Chính phủ vào CNTT ngày càng gia tăng trên mọi lĩnh vực của đời sống xã hội. Thách thức đặt ra là: Việc đầu tư các dự án CNTT từ việc quản lý và sử dụng tài sản công và tài chính công có thực sự hiệu quả, kinh tế và đáp ứng được các nhu cầu thực tế?

- (ii) Việc ứng dụng và phát triển CNTT trong hoạt động của các đơn vị (tổ chức và doanh nghiệp) ngày càng trở nên quan trọng, số lượng dữ liệu cần lưu trữ và thông tin được xử lý ngày càng tăng – làm ảnh hưởng đến môi trường kiểm soát. Mặt khác, CNTT cũng là một thành phần quan trọng trong chiến lược xây dựng và phát triển của đơn vị. Vì vậy, quản lý rủi ro CNTT ngày càng được chú trọng – thậm chí trở thành một phần tất yếu của quản trị, đóng vai trò quyết định cho sự thành công của hầu hết các đơn vị. Thách thức đặt ra là: Các hệ thống CNTT của các đơn vị được kiểm toán có được kiểm soát chặt chẽ nhằm đảm bảo tính tuân thủ pháp luật, hiệu quả, hiệu lực và kinh tế?
- (iii) Do CNTT ngày càng phát triển, các đơn vị trở nên phụ thuộc vào các hệ thống CNTT để thực hiện các hoạt động quản lý, kinh doanh và cung cấp dịch vụ cũng như công tác xử lý, duy trì và báo cáo những thông tin cần thiết. Điều này ảnh hưởng đến môi trường làm việc của Kiểm toán viên nhà nước khi tiếp cận với dữ liệu, thông tin tài chính được xử lý bởi các hệ thống CNTT của đơn vị. Thách thức đặt ra là: Các thông tin tài chính và nghiệp vụ được hệ thống CNTT đơn vị được kiểm toán xử lý có đầy đủ và chính xác khi bàn giao cho Kiểm toán viên nhà nước?
- (iv) Với thẩm quyền, chức năng và nhiệm vụ của mình, Kiểm toán nhà nước có quyền tiếp cận và kiểm tra rất nhiều nguồn dữ liệu khác nhau. Thách thức đặt ra là: Làm sao xây dựng và khai thác hiệu quả nguồn thông tin từ các CSDL kiểm toán chuyên ngành được kế thừa từ các CSDL quốc gia phục vụ công tác kiểm toán?

2.3. Ở Việt Nam, khái niệm về kiểm toán CNTT còn khá mới mẻ, nhưng đối với nhiều nước phát triển trên thế giới thì đây là loại hình kiểm toán đã được thực hiện thường xuyên bởi các cơ quan kiểm toán tối cao, các công ty kiểm toán độc lập danh tiếng hoặc trong nội bộ các tổ chức kinh tế - tài chính lớn. Để bắt kịp với xu thế của thế giới và nhu cầu thực tế, Kiểm toán nhà nước đã tổ chức thực hiện các hoạt động sau:

- (i) Xây dựng "Chiến lược phát triển Kiểm toán nhà nước đến năm 2020" và được Ủy ban Thường vụ Quốc hội ban hành thông qua Nghị quyết số

927/2010/UBTVQH12 ngày 19/4/2010 với mục tiêu phát triển Kiểm toán nhà nước đến năm 2020 là:

- Nâng cao năng lực hoạt động, hiệu lực pháp lý, chất lượng và hiệu quả hoạt động của Kiểm toán nhà nước như một công cụ hữu hiệu của Nhà nước trong kiểm tra, giám sát quản lý và sử dụng ngân sách, tiền và tài sản nhà nước;
- Xây dựng Kiểm toán nhà nước có trình độ chuyên nghiệp cao, từng bước hiện đại, trở thành cơ quan kiểm tra tài chính công có trách nhiệm và uy tín, đáp ứng yêu cầu của sự nghiệp công nghiệp hoá, hiện đại hoá đất nước, phù hợp với các thông lệ và chuẩn mực quốc tế.

- (ii) Xây dựng "Kế hoạch hành động thực hiện Chiến lược phát triển Kiểm toán nhà nước đến năm 2020" và được Tổng Kiểm toán nhà nước ban hành thông qua Quyết định 1876/QĐ-KTNN ngày 06/12/2010 để xác định rõ những mục tiêu, hoạt động, các ưu tiên và các nguồn lực cần thiết để hiện thực hóa chiến lược.
- (iii) Nhằm lựa chọn và thực hiện một số hoạt động quan trọng, mang tính ưu tiên cao trong chiến lược và kế hoạch hành động nêu trên, Kiểm toán nhà nước đã xây dựng "Kế hoạch chiến lược phát triển Kiểm toán nhà nước giai đoạn 2013 – 2017" và được Tổng Kiểm toán nhà nước ban hành thông qua Quyết định 1145/QĐ-KTNN ngày 09/10/2013. Một trong tám (8) mục đích chiến lược giai đoạn 2013-2017 gồm có “Tăng cường ứng dụng công nghệ thông tin trong hoạt động của Kiểm toán nhà nước”.
- (iv) Năm 2015, Tổng Kiểm toán nhà nước ra Quyết định số 1468/QĐ-KTNN ngày 22/10/2015, thành lập Phòng Kiểm toán CNTT trực thuộc Trung tâm Tin học, sau đó chuyển sang KTNN Chuyên ngành VII. Chức năng của Phòng là tham mưu giúp Kiểm toán trưởng KTNN Chuyên ngành VII nghiên cứu, đề xuất Tổng Kiểm toán nhà nước xây dựng các văn bản hướng dẫn kiểm toán công nghệ thông tin; triển khai áp dụng kiểm toán công nghệ thông tin trong hoạt động kiểm toán của Kiểm toán nhà nước.

b. Định nghĩa kiểm toán CNTT

2.4. Theo chuẩn mực ISSAI 5300 của Tổ chức Quốc tế các cơ quan Kiểm toán tối cao (INTOSAI) ban hành vào tháng 6 năm 2016, kiểm toán CNTT được định nghĩa như sau:

“Kiểm toán CNTT là hoạt động kiểm tra và đánh giá các hệ thống CNTT và các kiểm soát liên quan nhằm đạt được sự đảm bảo, hoặc nhận diện các vi phạm nguyên tắc về: tính pháp lý, tính hữu hiệu, tính kinh tế và tính hiệu quả của hệ thống CNTT và các kiểm soát liên quan”.

2.5. Như vậy, đối tượng của kiểm toán CNTT bao gồm:

- (i) Hệ thống CNTT và dữ liệu của hệ thống CNTT;
- (ii) Các kiểm soát liên quan đến hệ thống CNTT đó.

Tham khảo ví dụ thực tế tại Phụ lục A. Ví dụ 1.01 – Một số đối tượng kiểm toán của cuộc kiểm toán hệ thống TABMIS.

2.6. Theo INTOSAI, kiểm toán CNTT là một khái niệm rộng, bao hàm các loại hình kiểm toán báo cáo tài chính, kiểm toán tuân thủ, kiểm toán hoạt động.

Khi kết hợp với loại hình kiểm toán tài chính

2.7. Mục tiêu của loại hình kiểm toán tài chính là đưa ra ý kiến đánh giá về tính trung thực, đúng đắn về thông tin tài chính và báo cáo tài chính của đơn vị được kiểm toán. Một cuộc kiểm toán tài chính cần thực hiện các nội dung kiểm toán CNTT nếu như hệ thống kế toán/tài chính hoặc các nghiệp vụ chính của đơn vị được kiểm toán phần lớn được thực hiện bằng hệ thống CNTT. Trong trường hợp này, kiểm toán viên cần đưa ra ý kiến về mức độ tin cậy đối với hệ thống CNTT.

Tham khảo ví dụ thực tế tại Phụ lục III.A. Ví dụ 1.02 – Kiểm toán CNTT thực hiện trong Đoàn kiểm toán báo cáo quyết toán ngân sách của một tỉnh.

Khi kết hợp với loại hình kiểm toán tuân thủ

2.8. Mục tiêu của loại hình kiểm toán tuân thủ là đưa ra ý kiến về việc tuân thủ pháp luật, quy chế, quy định mà đơn vị được kiểm toán phải thực hiện. Trong trường hợp này, mục tiêu của kiểm toán CNTT là đánh giá hệ thống kiểm soát nội bộ liên quan đến hệ thống CNTT có tuân thủ các quy định pháp luật, nội quy, và quy định mà đơn vị phải tuân theo.

Tham khảo ví dụ thực tế tại Phụ lục III.A.Ví dụ 1.03 - Kiểm toán CNTT khi kết hợp với kiểm toán tuân thủ việc xác định lượng xe đi qua trạm thu phí đường cao tốc thuộc dự án BOT.

Khi kết hợp với loại hình kiểm toán hoạt động

- 2.9. Mục tiêu của loại hình kiểm toán hoạt động là đánh giá tính hiệu lực, tính hiệu quả và tính kinh tế của các hoạt động dưới sự kiểm soát của nhà quản lý của đơn vị được kiểm toán. Trong trường hợp này, cuộc kiểm toán cần một cuộc kiểm toán trong môi trường CNTT nếu CNTT được sử dụng phần lớn trong hoạt động của đơn vị và kiểm toán viên nhà nước cũng cần áp dụng những kỹ thuật kiểm toán nhằm xác định tính hiệu lực, hiệu quả và kinh tế của các hoạt động nghiệp vụ được tin học hóa.

Tham khảo ví dụ thực tế tại Phụ lục III.A.Ví dụ 1.04 - Kiểm toán CNTT khi kết hợp với kiểm toán hoạt động dự án đầu tư Chính phủ điện tử của một Tỉnh.

Xây dựng, cập nhật các CSDL chuyên ngành

- 2.10. Khi tiến hành kiểm toán định kỳ các hệ thống CNTT và các CSDL quốc gia, mục tiêu khác đặt ra là bổ sung các dữ liệu thu thập được để xây dựng thành CSDL chuyên ngành của Kiểm toán nhà nước.

Tham khảo ví dụ thực tế tại Phụ lục A.Ví dụ 1.05 - Kiểm toán CNTT hỗ trợ xây dựng CSDL chuyên ngành về các hóa đơn bất hợp pháp khi kiểm toán hệ thống CNTT của cơ quan Thuế.

c. Các nhiệm vụ quan trọng của kiểm toán CNTT

- 2.11. Với định nghĩa kiểm toán CNTT và những thách thức cần giải quyết đã nêu, kiểm toán CNTT tại Kiểm toán nhà nước có các nhiệm vụ quan trọng như sau:
- (i) Kiểm toán các dự án và hệ thống CNTT quan trọng đang được xã hội quan tâm, hoặc các dự án có độ rủi ro cao và trọng yếu, nhằm đảm bảo việc đầu tư phát triển lĩnh vực CNTT của nhà nước nói chung cũng như đầu tư vào các hệ thống CNTT cụ thể của các đơn vị được hoạt động chính xác, hiệu quả và tuân thủ theo các quy định pháp luật.
 - (ii) Thông qua việc kiểm toán, thu thập các thông tin về: (1) Hệ thống thông tin Tài chính Quốc gia, (2) Đầu mối kiểm toán, và (3) Phần mềm và dữ liệu

quan trọng nhằm tạo nền tảng cho việc xây dựng các CSDL chuyên ngành của Kiểm toán nhà nước.

- (iii) Tiếp cận, khai thác và phân tích dữ liệu của CSDL Tài chính Quốc gia, phục vụ cho việc xây dựng và cung cấp dữ liệu cho CSDL chuyên ngành của Kiểm toán nhà nước.
- (iv) Hỗ trợ các loại hình kiểm toán khác: (1) Đánh giá hệ thống CNTT liên quan đến lập và trình bày báo cáo kiểm toán trong việc hỗ trợ lập BCTC đảm bảo tính chính xác, đầy đủ, phù hợp với các chuẩn mực kiểm toán và chế độ tài chính hiện hành của nhà nước, tính an toàn, bảo mật thông tin hoạt động nghiệp vụ của đơn vị được kiểm toán, và (2) Đánh giá việc chấp hành pháp luật và các quy định về xây dựng, quản lý, vận hành, kiểm soát hệ thống CNTT liên quan đến lập BCTC của đơn vị được kiểm toán.

d. Phương thức vận dụng thực hiện kiểm toán CNTT tại Kiểm toán nhà nước

2.12. Kiểm toán CNTT có thể được tổ chức một cách độc lập hoặc lồng ghép với các loại hình kiểm toán khác. Khi thực hiện kiểm toán CNTT, cần xác định loại hình kiểm toán của cuộc kiểm toán dự kiến, từ đó xác định vai trò của kiểm toán CNTT trong cuộc kiểm toán và xây dựng chương trình kiểm toán phù hợp với mục tiêu chung của cuộc kiểm toán. Nhìn chung, kiểm toán CNTT của Kiểm toán nhà nước gồm 3 hoạt động chính sau:

- Triển khai một số hoạt động kiểm toán CNTT trong các cuộc kiểm toán – hay còn gọi là kiểm toán trong môi trường CNTT;
- Tổ chức cuộc kiểm toán hệ thống CNTT độc lập;
- Tổ chức cuộc kiểm toán dự án CNTT độc lập.

Kiểm toán trong môi trường CNTT

2.13. Là việc áp dụng một số nội dung, phương pháp kiểm toán CNTT trong cuộc kiểm toán nhằm nâng cao chất lượng, hiệu quả kiểm toán. Hoạt động này thường xảy ra khi đơn vị được kiểm toán sử dụng các hệ thống CNTT trong việc xử lý các thông tin tài chính và nghiệp vụ liên quan. Các chuẩn mực, hướng dẫn kiểm toán của Kiểm toán nhà nước cũng yêu cầu phải thực hiện các nội dung kiểm toán CNTT để đảm bảo chất lượng kiểm toán và giảm thiểu rủi ro kiểm toán. Các nội dung kiểm toán CNTT có thể là: kiểm toán hệ thống CNTT nghiệp vụ

trọng yếu hoặc xử lý thông tin tài chính; trích xuất và phân tích dữ liệu nghiệp vụ gốc từ hệ thống CNTT của đơn vị nhằm hỗ trợ các công tác kiểm toán khác; khai thác các CSDL kiểm toán chuyên ngành. Ngoài mục tiêu kiểm toán chung, việc triển khai một số nội dung kiểm toán CNTT sẽ nâng cao năng lực áp dụng các kỹ thuật kiểm toán CNTT của Kiểm toán nhà nước, phát huy tối đa hiệu quả các CSDL kiểm toán chuyên ngành.

Cuộc kiểm toán hệ thống CNTT

- 2.14. Là việc tổ chức cuộc kiểm toán kiểm tra đánh giá (một hay nhiều) hệ thống CNTT cùng hệ thống kiểm soát liên quan theo các mục tiêu kiểm toán nhất định. Ngoài mục tiêu kiểm toán thông thường, việc kiểm toán hệ thống CNTT còn nâng cao sự hiểu biết của Kiểm toán nhà nước về các hệ thống CNTT trên và hệ thống kiểm soát liên quan. Các kết quả đạt được sẽ phục vụ cho các cuộc kiểm toán tiếp theo cũng như xây dựng các CSDL chuyên ngành.

Cuộc kiểm toán dự án CNTT

- 2.15. Là việc tổ chức cuộc kiểm toán kiểm tra đánh giá (một hay nhiều) dự án CNTT hoặc kiểm toán báo cáo quyết toán của dự án hoặc thực hiện cả hai nội dung trên. Mục tiêu chính của một cuộc kiểm toán dự án CNTT là kiểm tra và đánh giá trạng thái hiện tại của việc hiện thực hóa dự án, tìm hiểu mức độ tuân thủ đối với các tiêu chuẩn của một dự án thành công và xác định các cơ hội nhằm cải thiện việc hiện thực hóa cũng như quản trị dự án hoặc xác nhận số liệu quyết toán của dự án CNTT. Công tác kiểm toán có thể thực hiện sau khi hoàn thành dự án hoặc sau một giai đoạn hiện thực hóa dự án hoặc trong khi đang hiện thực hóa dự án hoặc ngay trong giai đoạn lập dự toán để đánh giá tính khả thi.

3. Kiểm toán hệ thống CNTT

a. Khái niệm hệ thống CNTT và các tiêu chí đánh giá chung

- 3.1. Hệ thống CNTT là hệ thống bao gồm các tài sản CNTT như phần cứng, phần mềm, hệ thống mạng, dữ liệu và quy trình vận hành được xây dựng và sử dụng để thu thập, chia sẻ các dữ liệu, thông tin nhằm phục vụ các mục tiêu của tổ chức.
- 3.2. Các tổ chức sử dụng các hệ thống CNTT với nhiều mục đích khác nhau. Trong công tác quản trị nội bộ, hệ thống CNTT giúp đạt được sự thông hiểu nội bộ,

thống nhất hành động, duy trì sức mạnh của tổ chức, đạt được lợi thế cạnh tranh. Trong công tác quản lý đối tác bên ngoài, hệ thống CNTT giúp tổng hợp làm giàu thông tin về khách hàng hoặc cải tiến dịch vụ, nâng cao sức cạnh tranh và tạo đà cho phát triển của tổ chức.

- 3.3. Một hệ thống CNTT sẽ được xem là hiệu quả nếu đưa tổ chức đạt được các mục tiêu đặt ra và sẽ được xem là hữu hiệu nếu giúp sử dụng tối thiểu các nguồn lực để đạt được các mục tiêu trên. Do đó, Kiểm toán viên nhà nước cần phải hiểu rõ các đặc điểm của người dùng hệ thống CNTT và môi trường CNTT cũng như cách thức đưa ra quyết định của đơn vị liên quan đến hệ thống CNTT đó nhằm đánh giá tính hiệu quả, hiệu lực và kinh tế của hệ thống CNTT.
- 3.4. Khi kiểm toán hệ thống CNTT của đơn vị, Kiểm toán viên nhà nước có thể đánh giá trên năm tiêu chí cơ bản sau: tính bảo mật, tính trung thực, tính khả dụng, tính tin cậy và việc tuân thủ theo văn bản pháp luật và quy định.

Tính bảo mật

- 3.5. Là việc bảo vệ thông tin nhạy cảm không bị công bố trái phép. Mức độ nhạy cảm của dữ liệu quyết định mức độ quan tâm và mức độ nghiêm ngặt của các kiểm soát trong việc tiếp cận các dữ liệu đó. Ban lãnh đạo cũng cần đảm bảo khả năng của đơn vị trong việc duy trì tính bảo mật của thông tin, bất kỳ sự vi phạm nào cũng có thể ảnh hưởng nghiêm trọng đến với danh tiếng của đơn vị, đặc biệt khi thông tin liên quan đến các dữ liệu nhạy cảm.

Tính trung thực

- 3.6. Là độ chính xác và toàn vẹn của thông tin cũng như tính hợp lệ của nó theo các giá trị và như kỳ vọng của hoạt động kinh doanh. Đây là một mục tiêu kiểm toán quan trọng vì nó cung cấp sự đảm bảo cho cả ban điều hành lẫn các đối tượng sử dụng báo cáo bên ngoài rằng hệ thống thông tin của tổ chức đáng tin cậy và có thể dựa vào nó để ra các quyết định.

Tính khả dụng

- 3.7. Là việc thông tin sẵn sàng để sử dụng khi được yêu cầu bởi quy trình hoạt động trong hiện tại hoặc trong tương lai. Điều này bao gồm cả việc tổ chức đảm bảo các kế hoạch hoạt động liên tục hoặc kế hoạch phục hồi sau thảm họa có thể

được thực thi một cách kịp thời nhằm đảm bảo thông tin khả dụng khi người dùng yêu cầu.

Tính tin cậy

- 3.8. Phản ánh mức độ nhất quán của hệ thống hay khả năng của hệ thống thực hiện các nghiệp vụ trong các điều kiện cho trước. Đây là yếu tố quan trọng của kiểm toán CNTT để đảm bảo hệ thống vận hành nhất quán và hoạt động như kỳ vọng.

Tuân thủ theo văn bản pháp luật và quy định

- 3.9. Là yêu cầu buộc hệ thống CNTT cùng các chốt kiểm soát liên quan phải tuân theo các quy định của pháp luật và các quy định liên quan.

Các ví dụ thực tế tham khảo tại Phụ lục III.A.Ví dụ 1.06 – Tính bảo mật, trung thực, tin cậy, khả dụng và tuân thủ theo văn bản pháp luật và các quy định của các hệ thống CNTT.

b. Các nhóm hệ thống CNTT quan trọng đối với hoạt động kiểm toán CNTT của KTNN

- 3.10. Đối tượng của các cuộc kiểm toán hệ thống CNTT của Kiểm toán nhà nước là các hệ thống CNTT thuộc về các đơn vị thuộc phạm vi kiểm toán của Kiểm toán nhà nước được quy định trong Luật Kiểm toán nhà nước.
- 3.11. Căn cứ vào chiến lược, kế hoạch kiểm toán, đối tượng kiểm toán các hệ thống CNTT được phân loại và xác định mức độ trọng yếu trước khi thực hiện kiểm toán chi tiết. Các loại hệ thống CNTT có mức quan trọng chính bao gồm: các hệ thống CNTT quản lý Ngân sách nhà nước, các hệ thống thông tin và CSDL Quốc gia, các hệ thống CNTT của đầu mối kiểm toán quan trọng, các hệ thống CNTT được xã hội quan tâm.

Các hệ thống CNTT quản lý ngân sách nhà nước

- 3.12. Các hệ thống CNTT quản lý ngân sách được triển khai tại các cơ quan tài chính, KBNN, cơ quan hải quan, cơ quan thuế trên phạm vi toàn quốc. Báo cáo quyết toán, lập dự toán, điều hành và hạch toán các khoản thu chi ngân sách liên quan chặt chẽ đến các hệ thống CNTT trên. Tính chính xác, đầy đủ và tuân thủ của các báo cáo quyết toán Ngân sách các cấp cũng như việc chấp hành trong điều hành Ngân sách phụ thuộc vào việc vận hành các hệ thống CNTT trên cùng hệ thống kiểm soát CNTT liên quan.

- 3.13. Vai trò các hệ thống CNTT trên đối với việc điều hành và quản lý ngân sách rất quan trọng do đóng vai trò then chốt trong việc lập, xử lý, báo cáo và lưu trữ thông tin ngân sách nhà nước. Kiểm toán nhà nước nên tổ chức kiểm toán định kỳ các hệ thống trên để kiểm tra đánh giá và xác nhận tính tuân thủ trong việc vận hành CNTT có đúng theo quy định Nhà nước về việc lập, xử lý, báo cáo thông tin ngân sách hay không, cũng như thu thập các thông tin trọng yếu từ các hệ thống CNTT trên để xây dựng và làm giàu CSDL chuyên ngành của Kiểm toán nhà nước phục vụ công tác tra cứu, phân tích thông tin cho các cuộc kiểm toán Ngân sách.

Các hệ thống thông tin và cơ sở dữ liệu quốc gia

- 3.14. Với chiến lược xây dựng một chính phủ điện tử với cốt lõi là các CSDL quốc gia, các Bộ, Ngành dưới sự chỉ đạo của Chính phủ, đã và đang xây dựng các hệ thống thông tin quốc gia (HTTTQG) kết nối vào CSDL quốc gia.
- 3.15. Các hệ thống thông tin và cơ sở dữ liệu quốc gia đều liên quan đến việc quản lý các tài sản, tài nguyên công của nhà nước trên quy mô toàn quốc nên đều là các đối tượng quan trọng cần xem xét trong các hoạt động kiểm toán của Kiểm toán nhà nước. Khi tiếp cận, phân tích dữ liệu của các CSDL chuyên ngành quốc gia rất cần kiến thức về kiểm toán CNTT liên quan đến cách tổ chức và vận hành của các hệ thống CNTT trên. Việc kiểm toán các hệ thống trên đóng vai trò quan trọng trong kiểm toán chuyên đề về nghiệp vụ liên quan và đặc biệt phát huy tác dụng khi tổ chức đối chiếu chéo các hệ thống CSDL quốc gia với nhau.

Các hệ thống CNTT của đầu mối kiểm toán quan trọng

- 3.16. Các đầu mối kiểm toán quan trọng của Kiểm toán nhà nước đã, đang và sẽ áp dụng các hệ thống CNTT phục vụ công tác điều hành của mình. Tiêu biểu như: các ngân hàng, công ty bảo hiểm có vốn sở hữu nhà nước đều có hệ thống CNTT phục vụ việc điều hành các nghiệp vụ chính.
- 3.17. Hệ thống Chính phủ điện tử của các Bộ, Ban, Ngành và Địa phương cũng đang được quan tâm và phát triển một cách bài bản và hệ thống.
- 3.18. Các hệ thống CNTT trên đều không thể thiếu trong việc vận hành của đơn vị. Đặc biệt là các hệ thống CNTT liên quan đến việc xử lý thông tin tài chính. Vì vậy, việc tổ chức định kỳ các cuộc kiểm toán các hệ thống CNTT trọng yếu (đặc

biệt là liên quan đến việc xử lý thông tin tài chính) của các đầu mối kiểm toán quan trọng là một nhu cầu thực tế để nâng cao chất lượng kiểm toán của Kiểm toán nhà nước.

Các hệ thống CNTT được xã hội quan tâm

- 3.19. Ngày nay, rất nhiều hoạt động đời sống xã hội chịu sự chi phối của các hệ thống CNTT thuộc đối tượng kiểm toán của Kiểm toán nhà nước.
- 3.20. Tùy theo mức độ trọng yếu, rủi ro, sự quan tâm của xã hội, yêu cầu của Quốc hội, Chính phủ và kế hoạch chiến lược cũng như năng lực đội ngũ nhân sự của Kiểm toán nhà nước để tiến hành lựa chọn đối tượng hệ thống CNTT để kiểm toán cho thích hợp.

Các ví dụ thực tế tham khảo tại Phụ lục III.A. Ví dụ 1.07 – Các nhóm hệ thống CNTT quan trọng đối với hoạt động kiểm toán CNTT của KTNN.

c. Các cuộc kiểm toán hệ thống CNTT trong thực tế

- 3.21. Căn cứ vào tính chất và đặc thù của các cuộc kiểm toán hệ thống CNTT, các cuộc kiểm toán sau đây có thể được xem xét để tiến hành triển khai trong thực tế:

Kiểm toán các Hệ thống thông tin quản lý Ngân sách nhà nước

- 3.22. Mục tiêu kiểm toán: Xác nhận, đánh giá tính đầy đủ và hiệu quả của các hệ thống CNTT quản lý và điều hành Ngân sách nhà nước cùng hệ thống kiểm soát liên quan vận hành bởi các cơ quan tài chính, KBNN, Thuế và Hải quan.
- 3.23. Mục tiêu chuyên môn khác:
 - (i) Cập nhật kiến thức của Kiểm toán nhà nước về hệ thống kiểm soát, cách thức lưu trữ các dữ liệu thông tin liên quan đến Ngân sách.
 - (ii) Cung cấp và cập nhật CSDL kiểm toán chuyên ngành phục vụ cho các Đoàn kiểm toán Ngân sách cần các dữ liệu liên quan.

Kiểm toán chuyên đề các hệ thống thông tin và CSDL quốc gia và các hệ thống CNTT được xã hội quan tâm

- 3.24. Các cuộc kiểm toán chuyên đề nên hướng đến việc đối chiếu chéo các hệ thống CSDL quốc gia hoặc các hệ thống CNTT liên quan đến các hoạt động được xã hội quan tâm.

- 3.25. Mục tiêu kiểm toán: Đánh giá tính trung thực, đầy đủ và tuân thủ của việc xử lý thông tin nghiệp vụ được chọn kiểm toán của các hệ thống CNTT liên quan.
- 3.26. Mục tiêu chuyên môn khác:
- (i) Nâng cao sự hiểu biết của Kiểm toán nhà nước về các hệ thống CNTT cùng hệ thống kiểm soát liên quan được chọn kiểm toán nhằm phục vụ các công tác chuyên môn khác.
 - (ii) Làm giàu các CSDL chuyên ngành của Kiểm toán nhà nước.

Kiểm toán các hệ thống CNTT liên quan đến việc xử lý thông tin tài chính của các ĐMKT quan trọng

- 3.27. Các cuộc kiểm toán các hệ thống CNTT liên quan đến việc lập BCTC nên triển khai với các đầu mối kiểm toán quan trọng đã ứng dụng CNTT mạnh mẽ trong mọi hoạt động của mình như Ngân hàng, Các công ty bảo hiểm, xăng dầu cũng như các công ty thương mại có hệ thống đại lý bán lẻ rộng khắp. Cách thức triển khai cũng giống như cách thức các công ty kiểm toán độc lập uy tín nhất ở Việt Nam đang triển khai đối với các đơn vị này, đó là phải triển khai kiểm toán CNTT trước khi triển khai kiểm toán BCTC.
- 3.28. Mục tiêu kiểm toán: Đánh giá tính trung thực, đầy đủ và tuân thủ trong việc vận hành hệ thống CNTT liên quan đến việc lập BCTC.
- 3.29. Mục tiêu chuyên môn khác: Cập nhật kiến thức của Kiểm toán nhà nước về hệ thống kiểm soát, cách thức lưu trữ các dữ liệu thông tin liên quan đến việc lập BCTC của đơn vị phục vụ cho các cuộc kiểm toán BCTC và chuyên đề tiếp theo của đơn vị.

Các ví dụ thực tế tham khảo tại Phụ lục III.A. Ví dụ 1.08 – Mục tiêu các cuộc kiểm toán hệ thống CNTT tại KTNN.

4. Kiểm toán dự án CNTT

a. Khái niệm dự án CNTT, mục tiêu và các chỉ tiêu dự án

Khái niệm dự án CNTT

- 4.1. Theo định nghĩa tại Nghị định số 102/2009/NĐ-CP, dự án đầu tư CNTT là tập hợp những đề xuất có liên quan đến việc bỏ vốn để thiết lập mới, mở rộng hoặc nâng cấp cho hệ thống hạ tầng kỹ thuật, phần mềm và cơ sở dữ liệu nhằm đạt

được sự cải thiện về tốc độ, hiệu quả vận hành, nâng cao chất lượng dịch vụ trong ít nhất một chu kỳ phát triển của công nghệ thông tin.

- 4.2. Một dự án sẽ có các tính chất cơ bản sau: luôn bị ràng buộc về thời gian, có các mục tiêu và sản phẩm bàn giao cụ thể, ngày bắt đầu và ngày kết thúc và hầu hết có giai đoạn thực hiện rõ ràng.

Mục tiêu, chỉ tiêu dự án CNTT – thuộc tính căn bản nhất cho việc đánh giá

- 4.3. Mục tiêu của dự án là những tuyên bố hành động cụ nhằm đạt được các mục đích đã lập. Tất cả các mục đích của dự án sẽ có một hoặc nhiều mục tiêu với các hành động cần thiết để đạt được mục tiêu đó. Cần bắt đầu mục tiêu của dự án bằng một động từ mang tính hành động. Cú pháp này đảm bảo rằng mục tiêu là đo lường được và có thể được sử dụng để xác minh rằng kết quả của dự án có thể được theo dõi trực tiếp với hành động của mục tiêu.

Ví dụ thực tế tham khảo tại Phụ lục III.A. Ví dụ 1.09 – Các mục tiêu thực tế của dự án CNTT lĩnh vực Chính phủ điện tử.

- 4.4. Một dự án cần có những chỉ tiêu dự án phản ánh qua các mục tiêu dự án. Các chỉ tiêu phải có các tính chất sau: được xác định rõ ràng mang tính cụ thể; có thể đo lường; có thể đạt được; có tính thực tế; và kịp thời.

b. Phân loại dự án CNTT

- 4.5. Dự án CNTT có thể được phân loại dựa theo các tiêu chí về nguồn vốn gắn với cơ chế quản lý; quy mô tài chính; mức độ ảnh hưởng và phổ biến.

Phân loại theo nguồn vốn

- 4.6. Xét theo tiêu chí về nguồn vốn gắn liền với cơ chế quản lý, dự án được phân loại như sau:
- Ngân sách nhà nước;
 - Hỗ trợ phát triển chính thức (vốn ODA);
 - Viện trợ phi chính phủ;
 - Nguồn một phần từ tài sản/ tài chính công (trong đó bao gồm nguồn vốn đầu tư của các doanh nghiệp có vốn sở hữu Nhà nước);
 - Các dự án nghiên cứu liên quan đến CNTT.

Phân loại theo quy mô đầu tư tài chính

- 4.7. Xét theo tiêu chí tính chất của dự án và quy mô đầu tư, dự án ứng dụng CNTT sử dụng nguồn vốn ngân sách nhà nước theo Nghị định 102/2009/NĐ-CP được phân loại thành các nhóm như sau:
- Dự án quan trọng quốc gia (≥ 10.000 tỷ VND và/hoặc các tiêu chí khác theo luật);
 - Dự án nhóm A (≥ 800 tỷ VND);
 - Dự án nhóm B (từ 45 \rightarrow 800 tỷ VND);
 - Dự án nhóm C (< 45 tỷ VND);
 - Phân loại theo mức độ ảnh hưởng và phổ biến.
- 4.8. Xét theo tiêu chí mức độ ảnh hưởng và phổ biến, dự án được phân loại như sau:
- Các chương trình quốc gia về CNTT;
 - Các dự án CNTT triển khai các hệ thống thông tin quốc gia;
 - Các dự án đầu tư xây dựng Chính quyền điện tử ở các cơ quan ngang Bộ/Tỉnh;
 - Các dự án đầu tư CNTT thuộc các doanh nghiệp/đơn vị sự nghiệp nhà nước;
 - Các đề án nghiên cứu liên quan đến CNTT.

c. Cơ chế kiểm soát đầu tư dự án CNTT liên quan đến tài sản công, tài chính công

- 4.9. Hiện tại, đầu tư dự án CNTT đang được quy định bởi nhiều văn bản pháp luật khác nhau, kiểm toán viên nhà nước cần nhận thức đầy đủ về tính hiệu lực của các văn bản này cũng như cập nhật những văn bản mới được ban hành, một số văn bản liên quan có thể kể đến bao gồm:
- Luật Công nghệ thông tin;
 - Luật Đầu tư Công;
 - Luật Đấu thầu;
 - Nghị định 102/2009/NĐ-CP;
 - Và các văn bản liên quan khác.
- 4.10. Danh sách các văn bản ở mức độ đầy đủ hơn có thể tìm thấy ở Phụ lục III.E của Hướng dẫn.

d. Các cuộc Kiểm toán dự án CNTT trong thực tế

4.11. Trên cơ sở phân loại dự án CNTT, các cuộc kiểm toán dự án CNTT trong thực tế gồm có:

- (i) Kiểm toán các chương trình quốc gia về CNTT;
- (ii) Kiểm toán các dự án CNTT triển khai các hệ thống thông tin quốc gia;
- (iii) Kiểm toán việc đầu tư xây dựng Chính quyền điện tử ở các cơ quan Ngang Bộ/ Tỉnh;
- (iv) Kiểm toán các dự án đầu tư CNTT thuộc các doanh nghiệp/ đơn vị sự nghiệp nhà nước;
- (v) Kiểm toán các đề án nghiên cứu liên quan đến CNTT.

Ví dụ thực tế tham khảo tại Phụ lục.A.Ví dụ 1.10 – Các ví dụ khác nhau về kiểm toán dự án CNTT.

4.12. Mục tiêu cuộc kiểm toán dự án CNTT tương tự như mục tiêu một cuộc kiểm toán dự án đầu tư thông thường. Các mục tiêu kiểm toán có thể là:

- Xác nhận tính đúng đắn, trung thực của các tài liệu, số liệu kế toán (nguồn vốn đầu tư, chi phí đầu tư) và Báo cáo quyết toán vốn đầu tư dự án hoàn thành, báo cáo tài chính hàng năm của dự án.
- Đánh giá việc tuân thủ pháp luật, chế độ quản lý đầu tư xây dựng, chế độ quản lý tài chính kế toán của Nhà nước.
- Phát hiện những tồn tại bất cập của cơ chế chính sách của Nhà nước có liên quan để kiến nghị các cơ quan nhà nước có thẩm quyền điều chỉnh, bổ sung (nếu có).
- Đánh giá tính kinh tế, hiệu lực, hiệu quả của dự án.
- Cung cấp thông tin, số liệu tin cậy cho Quốc hội và các cơ quan quản lý nhà nước thực hiện chức năng giám sát trong quá trình đầu tư các dự án.
- Phát hiện kịp thời các hành vi tham nhũng, lãng phí và sai phạm trong quá trình thực hiện dự án (nếu có); xác định trách nhiệm tập thể, cá nhân và kiến nghị xử lý đối với các sai phạm theo quy định của pháp luật; kiến nghị với cơ quan có thẩm quyền sửa đổi, bổ sung, hoàn thiện chính sách chế độ, quản lý kinh tế - kỹ thuật và quản lý tài chính kế toán.

5. Kiểm toán trong môi trường CNTT

a. Các khái niệm cơ bản về kiểm toán trong môi trường CNTT

- 5.1. Môi trường CNTT/hay môi trường tin học là môi trường mà trong đó đơn vị được kiểm toán thực hiện công việc hoặc xử lý thông tin trên máy vi tính với các mức độ áp dụng khác nhau, chủng loại máy hoặc phần mềm có quy mô và mức độ phức tạp khác nhau, cho dù hệ thống máy tính do đơn vị được kiểm toán hoặc bên thứ ba vận hành.
- 5.2. Môi trường kiểm soát CNTT tổng quan được định nghĩa như một “môi trường hoạt động” chứa những bộ chính sách, thủ tục kiểm soát CNTT tổng quan thông thường nhằm hỗ trợ sự vận hành của các kiểm soát ứng dụng tự động liên quan.
- 5.3. Kiểm toán trong môi trường CNTT được hiểu là việc thực hiện kiểm toán trong môi trường CNTT của đơn vị được kiểm toán. Các công việc chính của kiểm toán trong môi trường CNTT bao gồm:
- Thử nghiệm hệ thống kiểm soát chung CNTT liên quan đến cuộc kiểm toán;
 - Thử nghiệm hệ thống kiểm soát ứng dụng nghiệp vụ liên quan đến cuộc kiểm toán;
 - Thực hiện các kỹ thuật kiểm toán với sự hỗ trợ của máy tính (CAATs).
- Ví dụ thực tế tham khảo tại Phụ lục.A.Ví dụ 1.11 – Một số nội dung kiểm toán trong môi trường CNTT trong Đoàn Kiểm toán Ngân sách địa phương.*

b. Kiểm toán trong môi trường công nghệ thông tin và hệ thống chuẩn mực KTNN

- 5.4. Yêu cầu về việc thực hiện kiểm toán trong môi trường CNTT tuân theo hệ thống chuẩn mực của KTNN từ việc đảm bảo chất lượng (CMKTNN 40), các giai đoạn thực hiện cuộc kiểm toán tài chính (các chuẩn mực từ 1200 đến 1805, hướng dẫn chi tiết kiểm toán tài chính).
- 5.5. Việc thực hiện kiểm toán CNTT trong kiểm toán tài chính thể hiện qua các chuẩn mực 1200 – 1805 như sau:
- Về yêu cầu nhân lực có trình độ về CNTT của đoàn kiểm toán được quy định tại đoạn CMKTNN 1220.23 - Kiểm soát chất lượng đối với cuộc kiểm toán tài chính.
 - Về việc từ chối cho kiểm toán viên tiếp cận nhân viên cùng hệ thống CNTT đơn vị phải được xem là dấu hiệu của hành vi gian lận đề cập Phụ lục 3 –

CMKTNN 1240 - Trách nhiệm của Kiểm toán viên nhà nước liên quan đến gian lận trong cuộc kiểm toán tài chính.

- (iii) Về việc phải đánh giá tính tuân thủ pháp luật, các hạn chế của hệ thống CNTT của đơn vị, cũng như phải nghi ngờ và tìm hiểu khi đơn vị không cung cấp dữ liệu từ hệ thống CNTT tại các đoạn 10, 19 trong CMKTNN 1250 - Đánh giá tính tuân thủ pháp luật và các quy định trong kiểm toán tài chính.
- (iv) Về yêu cầu tổ chức khảo sát, thu thập thông tin về hệ thống CNTT của đầu mối kiểm toán được quy định trong đoạn CMKTNN 1300.15 - Lập kế hoạch kiểm toán của cuộc kiểm toán tài chính.
- (v) Về yêu cầu thực hiện đánh giá rủi ro thông qua việc tìm hiểu CNTT và bản chất của kiểm soát được quy định trong các đoạn 17, 23, 33, 36, 40 và Phụ lục 01, 02 thuộc CMKTNN 1315 - Xác định và đánh giá rủi ro có sai sót trọng yếu thông qua hiểu biết về đơn vị được kiểm toán và môi trường hoạt động của đơn vị trong kiểm toán tài chính. Đây có thể xem là các nội dung căn bản cần thực hiện các nội dung kiểm toán CNTT trong cuộc kiểm toán tài chính phục vụ cho việc đánh giá hệ thống kiểm soát liên quan đến CNTT.
- (vi) Về việc xử lý các rủi ro kiểm toán liên quan đến hệ thống CNTT tại đơn vị cũng được đề cập tại Đoạn 15, 20, 32, 34 và 36 của CMKTNN 1330 - Biện pháp xử lý rủi ro kiểm toán trong kiểm toán tài chính. Trong đó nêu rõ cách thức tiến hành thủ tục, đánh giá rủi ro kiểm toán liên quan đến CNTT và các biện pháp xử lý rủi ro tương ứng. Chuẩn mực cũng đã đề cập cụ thể đến các nội dung kiểm toán kiểm soát chung CNTT như việc quản lý thay đổi hệ thống CNTT, quản lý các phiên bản phần mềm, cũng như các nội dung kiểm toán CNTT quan trọng khác trong quá trình kiểm toán.
- (vii) Về việc đơn vị sử dụng dịch vụ CNTT bên ngoài liên quan đến việc lập BCTC cũng được hướng dẫn tại đoạn CMKTNN 1402.13.i - Các yếu tố cần xem xét khi kiểm toán đơn vị có sử dụng dịch vụ bên ngoài trong kiểm toán tài chính.

- (viii) Về việc chọn mẫu thích hợp trong điều kiện hệ thống nghiệp vụ được xử lý bằng hệ thống CNTT được hướng dẫn tại CMKTNN 1500.50 - Bảng chứng kiểm toán trong kiểm toán tài chính.
- (ix) Về việc đơn vị có thể sử dụng hệ thống CNTT riêng để lưu các giao dịch đặc biệt với các đối tác quan trọng được hướng dẫn tại đoạn CMKTNN 1550.6- Các bên liên quan trong kiểm toán tài chính.
- (x) Về yêu cầu về việc thu thập thông tin và tìm hiểu về hệ thống CNTT cùng hoạt động kiểm soát khi kiểm toán báo cáo tài chính hợp nhất cho tập đoàn được quy định trong Phụ lục 01 của CMKTNN 1600 - Lưu ý khi kiểm toán báo cáo tài chính tập đoàn. Chuẩn mực này có nhiều nét tương đồng với cuộc kiểm toán báo cáo quyết toán Ngân sách vốn được tổng hợp từ các đơn vị dự toán trực thuộc.

B. CÁC YẾU TỐ CƠ BẢN CỦA KIỂM TOÁN CÔNG NGHỆ THÔNG TIN

6. Kiểm soát CNTT và các tiêu chí kiểm toán CNTT

a. Khái niệm về kiểm soát CNTT

- 6.1. Một hệ thống CNTT muốn đạt được hiệu quả và hữu hiệu cần có hệ thống kiểm soát giúp thực hiện năm tiêu chí đánh giá (bảo mật, khả dụng, tin cậy, toàn vẹn, tuân thủ). Tổ chức phải xây dựng hệ thống kiểm soát CNTT cho các mục đích trên. Vì vậy, các kiểm soát CNTT là đối tượng chính của kiểm toán CNTT.
- 6.2. Tùy theo bản chất, các kiểm soát CNTT có thể được chia thành 3 loại:
 - (i) Kiểm soát thủ công: Được thực hiện bên ngoài hệ thống bởi con người.
 - (ii) Kiểm soát tự động: Được thực hiện bởi các hệ thống /ứng dụng CNTT.
 - (iii) Kiểm soát thủ công có yếu tố tự động: Được thực hiện thủ công dưới sự trợ giúp của các ứng dụng CNTT.

Ví dụ thực tế tham khảo tại Phụ lục.A.Ví dụ 2.01 – Các chốt kiểm soát thủ công, tự động và thủ công có yếu tố tự động.
- 6.3. Tùy theo nội dung, kiểm soát CNTT được chia làm 2 loại: kiểm soát chung CNTT và kiểm soát ứng dụng CNTT.

b. Kiểm soát chung CNTT

- 6.4. Kiểm soát chung CNTT là nền tảng của toàn bộ hệ thống kiểm soát CNTT. Kiểm soát chung CNTT tạo ra môi trường kiểm soát chung cho việc phát triển, vận hành, quản lý và bảo hành các hệ thống CNTT. Kiểm soát chung CNTT thiết lập một khung kiểm soát cho toàn bộ các kiểm soát các hoạt động CNTT và đảm bảo rằng các mục tiêu kiểm soát đạt được các yêu cầu đặt ra.
- 6.5. Kiểm soát chung CNTT được hiện thực thông qua các công cụ khác nhau như chính sách, hướng dẫn và các thủ tục tích hợp với hệ thống quản lý chung bao gồm cả việc quản lý hệ thống CNTT.

Ví dụ thực tế tham khảo tại Phụ lục.A.Ví dụ 2.02 – Các kiểm soát chung CNTT.

c. Kiểm soát ứng dụng CNTT

- 6.6. Kiểm soát ứng dụng CNTT gắn liền với các phần mềm ứng dụng của máy tính. Các phần mềm ứng dụng tích hợp các kiểm soát vào trong để đảm bảo việc xác thực, tính đầy đủ, tính chính xác và tính hiệu lực của các giao dịch, các phương thức nhập liệu và bảo trì là phù hợp.

Ví dụ thực tế tham khảo tại Phụ lục.A.Ví dụ 2.03 – Các ví dụ tổng quát và chi tiết về kiểm soát ứng dụng CNTT.

d. Mối liên hệ giữa các hệ thống kiểm soát CNTT

- 6.7. Kiểm soát chung CNTT thường không dành cho việc xử lý giao dịch cụ thể hoặc các nhóm tài khoản nào đó, hoặc chỉ phục vụ đơn lẻ một phần mềm. Mục tiêu của kiểm soát chung CNTT là tạo ra nền tảng chính sách, môi trường hoạt động và kiểm soát chung nhằm đảm bảo cho sự phát triển và hiện thực các phần mềm ứng dụng, cũng như các dữ liệu, phần mềm đang được vận hành.
- 6.8. Việc thiết kế và thực hiện các chốt kiểm soát chung CNTT sẽ có ảnh hưởng lớn đến sự hiệu quả của các kiểm soát ứng dụng CNTT. Kiểm soát chung CNTT thiết lập cơ chế bảo vệ lên các nguồn tài nguyên mà phần mềm ứng dụng khỏi các truy cập trái phép.

Ví dụ: Phải tách biệt môi trường phát triển phần mềm và vận hành phần mềm để đảm bảo không có hiện tượng tự ý chỉnh sửa ứng dụng hoặc chỉnh sửa các dữ liệu của phần mềm.

- 6.9. Một số chốt kiểm soát chung CNTT tham gia vào việc bảo vệ phần mềm như:
- Quy trình kiểm soát việc truy cập thông qua máy tính cá nhân, hệ thống mạng, ứng dụng, dữ liệu.
 - Quản lý chu trình phát triển phần mềm.
 - Quản lý việc thay đổi mã nguồn chương trình ứng dụng.
 - Quản lý việc ra vào của nhân viên tại trung tâm dữ liệu.
 - Kiểm soát việc lưu giữ dữ liệu định kỳ và khôi phục khi cần thiết.
 - Quản lý việc vận hành sử dụng máy tính.
- 6.10. Việc thiết kế và vận hành hiệu quả của các chốt kiểm soát chung CNTT là nền tảng cho kiểm soát ứng dụng CNTT như các giao dịch nghiệp vụ, đảm bảo dữ liệu đầu vào, việc xử lý cũng như dữ liệu đầu ra là chính xác từ đó có thể quản lý được các rủi ro liên quan.

e. Các khung kiểm soát CNTT phổ biến trong cộng đồng kiểm toán

- 6.11. Nhằm mục tiêu tìm ra cách thực hành tốt nhất để quản lý CNTT, một số tổ chức đã xây dựng khung kiểm soát về quản lý CNTT, định nghĩa các kiểm soát, giải thích mục đích, phương thức xây dựng, kiểm tra những kiểm soát CNTT đó. Các khung kiểm toán CNTT được cộng đồng kiểm toán CNTT thừa nhận và đánh giá cao bao gồm: CoBiT, ITIL và ISO. INTOSAI sử dụng CoBiT và ITIL làm nguồn tài liệu tham khảo trong sổ tay KTCNTT ban hành chính thức năm 2014.

CoBIT

- 6.12. Phát hành bởi ISACA - Hiệp hội Kiểm toán và Kiểm soát hệ thống công nghệ thông tin. CoBiT mang lại giá trị bằng việc:
- Tạo sự kết nối giữa CNTT với các nhu cầu của doanh nghiệp;
 - Tổ chức các hoạt động CNTT thành các quy trình được chấp nhận rộng rãi;
 - Xác định các nguồn lực CNTT chính cần được tận dụng;
 - Định nghĩa các mục tiêu kiểm soát cho việc quản lý cần được cân nhắc.

ITIL

- 6.13. Phát hành bởi AXELOS - Liên doanh bởi Chính phủ Vương quốc Anh và Capita - một công ty quốc tế chuyên cung cấp các dịch vụ chuyên môn. ITIL tập hợp

các hướng dẫn thực hành chi tiết về quản trị dịch vụ CNTT, nhằm định hướng các dịch vụ CNTT theo nhu cầu của doanh nghiệp.

ISO 27001/38500

6.14. Phát hành bởi ISO (Tổ chức Tiêu chuẩn hóa Quốc tế) và IDC (Ủy ban Kỹ thuật Điện Quốc tế). ISO đưa ra những tiêu chuẩn và mục tiêu:

- Quản trị CNTT;
- Các kỹ thuật an ninh;
- Hệ thống quản lý an ninh thông tin;
- Và nhiều mục tiêu khác.

f. Tiêu chí kiểm toán CNTT

6.15. Các tiêu chí kiểm toán phải được xác định để làm cơ sở cho việc đánh giá các bằng chứng kiểm toán và đưa ra các phát hiện và kết luận kiểm toán. Tiêu chí kiểm toán CNTT có thể căn cứ trên:

- (i) Các quy định, hướng dẫn và tiêu chuẩn của cơ quan nhà nước hoặc các đơn vị chủ quản liên quan tới hệ thống CNTT được quản lý.
- (ii) Các quy định, hướng dẫn và tiêu chuẩn về CNTT mà đơn vị cam kết thực hiện.
- (iii) Các tiêu chí kiểm toán CNTT được Kiểm toán nhà nước ban hành trong Hướng dẫn này.
- (iv) Các tiêu chuẩn và thông lệ quốc tế trong việc quản trị hệ thống CNTT của ngành nghề, hoặc Quốc tế được cộng đồng công nhận rộng rãi. Khi áp dụng các tiêu chí trên cần tham khảo và thống nhất với đầu mối kiểm toán (nếu cần).

Ví dụ thực tế tham khảo tại Phụ lục.A.Ví dụ 2.04 – Các ví dụ tiêu chí kiểm toán.

7. Phương pháp tiếp cận dựa trên rủi ro và trọng yếu

a. Rủi ro kiểm toán CNTT

Định nghĩa và phân loại rủi ro kiểm toán CNTT

7.1. Với cách tiếp cận dựa trên rủi ro, bên cạnh rủi ro tiềm tàng, rủi ro kiểm soát hoặc rủi ro phát hiện, kiểm toán viên nhà nước phải dựa trên tìm hiểu về kiểm soát nội bộ, kiểm soát vận hành, các kiến thức về công ty hoặc ngành nghề được kiểm toán để đánh giá rủi ro kiểm toán.

- 7.2. Trên cơ sở thông tin thu thập được và kết quả phân tích, đánh giá thông tin, kiểm toán viên thực hiện xác định và đánh giá rủi ro liên quan đến CNTT để phục vụ việc xây dựng kế hoạch kiểm toán tổng quát.
- 7.3. Rủi ro kiểm toán có thể được định nghĩa là một rủi ro mà thông tin có thể chứa đựng những sai sót trọng yếu dẫn đến việc không phát hiện được trong suốt quá trình kiểm toán. Chính vì vậy kiểm toán viên CNTT cần cân nhắc thêm các yếu tố khác liên quan đến doanh nghiệp/ tổ chức như dữ liệu khách hàng, tính bảo mật, tính sẵn sàng của các dịch vụ được cung cấp.
- 7.4. Rủi ro kiểm toán phụ thuộc vào rủi ro có sai sót trọng yếu và rủi ro phát hiện. Rủi ro kiểm toán là kết quả của rủi ro có sai sót trọng yếu và rủi ro phát hiện.
- (i) Rủi ro có sai sót trọng yếu: là khả năng đối tượng kiểm toán có thể có sai sót trọng yếu do gian lận hoặc nhầm lẫn. Rủi ro có sai sót trọng yếu bao gồm rủi ro tiềm tàng và rủi ro kiểm soát.
- Rủi ro tiềm tàng: là mức độ rủi ro của hệ thống CNTT khi chưa xét đến các kiểm soát mà cấp quản lý đã thực hiện. Rủi ro tiềm tàng tồn tại một cách độc lập và tồn tại do bản chất của hệ thống CNTT.
 - Rủi ro kiểm soát: Rủi ro mà các lỗi trọng yếu không được ngăn chặn hay phát hiện kịp thời bởi hệ thống các kiểm soát nội bộ.
- (ii) Rủi ro phát hiện: Rủi ro về lỗi hay sai sót trọng yếu không được phát hiện bởi kiểm toán viên CNTT.
- 7.5. Khái niệm rủi ro kiểm toán đôi khi cũng được sử dụng để mô tả mức độ rủi ro mà một kiểm toán viên nhà nước CNTT sẵn sàng chấp nhận khi trong một cuộc kiểm toán. Kiểm toán viên do đó có thể thiết lập mức độ mục tiêu và dựa trên đó để điều chỉnh khối lượng công việc kiểm toán để giảm thiểu rủi ro kiểm toán đến mức tối đa.

Ví dụ thực tế tham khảo tại Phụ lục.A.Ví dụ 2.05 – Các ví dụ rủi ro kiểm toán CNTT.

Đánh giá, xác định rủi ro CNTT

- 7.6. Kiểm toán viên CNTT cần có một hiểu biết tốt về rủi ro kiểm toán khi lên kế hoạch kiểm toán. Một mẫu kiểm toán có thể không phát hiện hết các sai sót tiềm tàng trong toàn bộ mẫu. Tuy nhiên, bằng cách sử dụng các quy trình lấy mẫu

thống kê phù hợp hoặc một quy trình kiểm soát tốt, xác suất phát hiện rủi ro có thể giảm tới một mức độ chấp nhận được.

7.7. Việc đánh giá và xác định rủi ro liên quan đến CNTT dựa trên:

- (i) Mức độ gây nguy hại đến nghiệp vụ, hoạt động chính của đơn vị do việc thiếu hoặc không thực hiện đầy đủ đảm bảo tính bảo mật, toàn vẹn, sẵn sàng, tin cậy và tuân thủ quy định pháp luật của thông tin và các tài sản khác.
- (ii) Mức độ xảy ra thực tế các lỗi phát sinh từ các lỗ hổng của hệ thống, các chốt kiểm soát CNTT không thiết lập đầy đủ và các nguy cơ tác động từ bên ngoài. Chú ý đến từ yếu tố dồn tích khi hệ thống triển khai trên diện rộng và hoạt động theo thời gian dài thì các lỗi phát sinh có thể bị tích tụ lâu dài và đủ lớn để gây hậu quả nghiêm trọng.
- (iii) Phải cân nhắc giữa chi phí và rủi ro, cơ chế và công tác quản trị rủi ro của đơn vị được kiểm toán.

7.8. Việc đánh giá và xác định rủi ro liên quan đến CNTT được thực hiện qua các bước sau:

- (i) Thống kê và phân loại hệ thống CNTT của đơn vị được kiểm toán;
- (ii) Xác định mức ảnh hưởng của từng hệ thống tác động các nghiệp vụ hoặc tài sản quan trọng (như tiền, khách hàng, các quyết định ...) và cách thức ảnh hưởng trong thực tế;
- (iii) Đánh giá những rủi ro ảnh hưởng đến các hệ thống CNTT và mức độ ảnh hưởng lên nghiệp vụ.

b. Trọng yếu kiểm toán CNTT

7.9. Dựa trên kết quả phân tích, đánh giá thông tin, kết quả đánh giá rủi ro, kiểm toán viên CNTT xác định trọng yếu kiểm toán làm cơ sở xây dựng kế hoạch cuộc kiểm toán.

7.10. Khái niệm về tính trọng yếu cần có phán xét mang tính nghề nghiệp từ kiểm toán viên CNTT. Kiểm toán viên CNTT có thể phát hiện một lỗi nhỏ và trở thành trọng yếu ở cấp hoạt động nhưng không quan trọng đối với cấp quản lý. Những cân nhắc về tính trọng yếu, hiểu biết về rủi ro kiểm toán là những khái niệm cốt

lỗi cho việc lên kế hoạch phạm vi kiểm toán và những thử nghiệm chi tiết cần được kiểm toán.

- 7.11. Về mặt định lượng: Một sai sót có thể được coi là trọng yếu khi giá trị của sai sót đó, xét một cách riêng biệt hoặc cộng gộp với các sai sót khác, lớn hơn một mức độ nào đó.
- 7.12. Về mặt định tính: Trọng yếu được xem xét trong mối quan hệ tổng hòa với các nhân tố khác có thể ảnh hưởng tới quyết định của người sử dụng thông tin, bao gồm: tính tuân thủ pháp luật, các vi phạm trong hệ thống kiểm soát nội bộ, các giao dịch không theo các nguyên tắc thông thường, sự can thiệp và vi phạm của lãnh đạo đơn vị, khả năng hoạt động liên tục của đơn vị.
- 7.13. Việc xác định mức trọng yếu là một xét đoán chuyên môn của Kiểm toán viên nhà nước. Tùy thuộc vào kinh nghiệm và phán đoán của Kiểm toán viên nhà nước đối với rủi ro mà mức trọng yếu được xác định theo các mức cao hoặc thấp khác nhau. Mức trọng yếu thường được xét theo các khoản mục nhạy cảm đối với người sử dụng báo cáo tài chính, thường là doanh thu, lợi nhuận hoặc tổng tài sản.
- 7.14. Khi xem xét mức độ trọng yếu CNTT liên quan đến hệ thống CNTT phải xem xét đến vị trí, chức danh tác nghiệp và mức độ ảnh hưởng của người dùng gây nên các rủi ro. Khi người dùng nắm vị trí càng quan trọng thì các sai sót không tuân thủ khi sử dụng hệ thống CNTT sẽ trở nên trọng yếu.

c. Phương pháp tiếp cận kết hợp rủi ro và trọng yếu trong kiểm toán CNTT

- 7.15. Trong kiểm toán CNTT, đánh giá rủi ro có mối liên hệ chặt chẽ tới trọng yếu kiểm toán. Trọng yếu của việc không tuân thủ được đánh giá dựa trên khả năng tác động đến các quyết định của người sử dụng. Khi rủi ro tiềm tàng lớn, việc không tuân thủ dù nhỏ cũng có thể dẫn đến rủi ro trọng yếu do khả năng tích hợp của các tác động của việc không tuân thủ này. Tương tự, khi rủi ro kiểm soát cao (không kiểm soát hoặc không có khả năng kiểm soát các rủi ro đã được xác định) thì việc không tuân thủ dù nhỏ cũng có thể dẫn đến trọng yếu do khả năng tích hợp các tác động của việc không tuân thủ trên.

Ví dụ: Khi công thức tính lãi ngân hàng làm tròn lãi khách hàng thấp hơn quy định và thực hiện hoàn toàn tự động không kiểm soát thì sự không tuân

thủ dù rất nhỏ nhưng lại là trọng yếu do yếu tố dồn tích của các sai số trên từng tài khoản khách hàng kéo dài theo thời gian.

- 7.16. Các Kiểm toán viên nhà nước không phải lúc nào cũng có thể kiểm toán tất cả các vấn đề/ giao dịch/ hệ thống hoặc do sự hạn chế về nguồn lực, thời gian cũng như việc cân đối giữa chi phí và lợi ích của việc thực hiện kiểm toán. Trong trường hợp này, các Kiểm toán viên nhà nước có thể phải xác định các trọng yếu kiểm toán và thực hiện kiểm toán mẫu để kiểm toán chi tiết và đưa ra các kết luận kiểm toán.
- 7.17. Kiểm toán viên nhà nước có thể sử dụng các công cụ CNTT để đưa ra các loại mẫu khác nhau nhằm đáp ứng các tiêu chí chọn mẫu khác nhau theo mức độ rủi ro và trọng yếu đã đánh giá. Mức độ của rủi ro tiềm tàng và rủi ro kiểm soát sẽ tác động đến quy mô của mẫu. Rủi ro tiềm tàng và rủi ro kiểm soát càng cao thì yêu cầu về quy mô của mẫu càng lớn.

8. Năng lực và kỹ năng cần thiết

a. Yêu cầu căn bản

- 8.1. Đoạn CMKTTN 40.33 quy định kiểm toán viên phải có đủ năng lực chuyên môn và khả năng (thời gian và các nguồn lực) để thực hiện cuộc kiểm toán. Cụ thể:
- (i) Sự hiểu biết về ngành nghề, lĩnh vực hoạt động hoặc các vấn đề có liên quan đối với đơn vị được kiểm toán của Kiểm toán viên nhà nước;
 - (ii) Sự am hiểu về các quy định pháp lý, các yêu cầu báo cáo có liên quan đối với đơn vị được kiểm toán hoặc có khả năng đạt được các kiến thức và kỹ năng cần thiết đó một cách hiệu quả của Kiểm toán viên nhà nước.
- 8.2. Vì vậy, Kiểm toán viên nhà nước thực hiện kiểm toán CNTT bên cạnh năng lực chuyên môn cần phải có các năng lực và kỹ năng đặc thù về CNTT và kiểm toán CNTT.

b. Đặc thù về năng lực và kỹ năng cần thiết dành cho kiểm toán CNTT

- 8.3. Kiểm toán viên thực hiện kiểm toán CNTT cần phải có năng lực và kỹ năng như sau: Trình độ và năng lực chuyên môn về CNTT; Trình độ và năng lực chuyên môn về kiểm toán; Trình độ và năng lực chuyên môn về kiểm toán CNTT; Kiến

thức và giải pháp CNTT dành cho kiểm toán CNTT cho từng lĩnh vực kiểm toán;
Kiến thức và kỹ năng mềm.

Trình độ và năng lực về kiến thức CNTT

- 8.4. Để thực hiện kiểm toán CNTT, Kiểm toán viên nhà nước cần có:
- Trình độ và năng lực về quản trị rủi ro và tuân thủ trong lĩnh vực CNTT;
 - Trình độ và năng lực về máy tính và các ứng dụng CNTT phổ thông;
 - Trình độ và năng lực về cơ sở dữ liệu và mạng máy tính;
 - Trình độ và năng lực về các phương pháp phát triển, kiểm thử phần mềm.

Trình độ và năng lực về kiến thức kiểm toán

- 8.5. Để thực hiện kiểm toán tại Kiểm toán nhà nước, Kiểm toán viên nhà nước cần có trình độ và năng lực các kiến thức nền tảng sau:
- Lý thuyết kinh tế, tài chính, kế toán, thuế và phương pháp luận của kiểm toán;
 - Các loại báo cáo tài chính;
 - Các chuẩn mực, quy định, hướng dẫn của Kiểm toán nhà nước.

Trình độ, năng lực về kiểm toán CNTT

- 8.6. Là những kiến thức và kỹ năng cần thiết phục vụ cho việc triển khai kiểm toán CNTT, trong đó tập trung vào các yếu tố đặc thù đòi hỏi phải có trình độ và năng lực căn bản về kiến thức CNTT và kiến thức kiểm toán. Cụ thể:
- Hướng dẫn, quy trình và thủ tục kiểm toán CNTT;
 - Các loại kiểm soát CNTT và khả năng nhận diện các kiểm soát CNTT;
 - Các chuẩn mực, quy định, hướng dẫn về Kiểm toán CNTT của KTNN và Quốc tế.

Trình độ, năng lực về kiến thức CNTT cho các lĩnh vực kiểm toán của KTNN:

- 8.7. Hoạt động của Kiểm toán nhà nước chia làm 4 lĩnh vực kiểm toán: Ngân sách, Doanh nghiệp; Ngân hàng và các tổ chức tài chính; Đầu tư. Khi tiếp cận các hệ thống CNTT, kiểm toán viên CNTT cần có kiến thức chuyên môn về lĩnh vực kiểm toán và am hiểu về các giải pháp CNTT cho lĩnh vực đó. Cụ thể các năng lực và kỹ năng chính liên quan đến lĩnh vực kiểm toán bao gồm:
- Các loại hình và lĩnh vực hoạt động của đơn vị/tổ chức của lĩnh vực kiểm toán;

- Vai trò và trách nhiệm của các chức vụ trong đơn vị/tổ chức của lĩnh vực kiểm toán;
- Các chính sách kinh tế, pháp luật, quy định cho từng loại đơn vị/tổ chức của lĩnh vực kiểm toán;
- Kiến thức/kinh nghiệm về phát triển và triển khai giải pháp CNTT của lĩnh vực kiểm toán;
- Các xu hướng triển khai giải pháp CNTT cho lĩnh vực kiểm toán tại Việt Nam và trên thế giới.

Kiến thức và kỹ năng mềm

8.8. Là các kiến thức và kỹ năng mềm gắn chặt với công việc kiểm toán CNTT. Các nội dung chi tiết chính như sau:

- Đánh giá chuyên môn và hoài nghi nghề nghiệp;
- Xử lý số liệu và tính toán thông thường;
- Phân tích quy trình và báo cáo rõ ràng, mạch lạc và dễ hiểu;
- Lãnh đạo và làm việc nhóm;
- Giải quyết mâu thuẫn, quản lý thời gian.

9. Hồ sơ biểu mẫu

9.1. Về cơ bản hồ sơ biểu mẫu của cuộc kiểm toán CNTT tuân theo các chuẩn mực, quy định và hướng dẫn của Kiểm toán nhà nước.

9.2. Kiểm toán viên nhà nước cần lập và lưu trữ hồ sơ kiểm toán một cách đầy đủ, hoàn chỉnh và chi tiết đã thu thập hoặc tạo ra trong quá trình kiểm toán CNTT nhằm:

- Xác nhận và chứng minh cho các ý kiến trong báo cáo kiểm toán CNTT;
- Tăng cường tính hiệu quả và hiệu lực báo cáo kiểm toán CNTT;
- Cung cấp thông tin về quá trình lập báo cáo kiểm toán CNTT hoặc để giải đáp các câu hỏi phát sinh từ đơn vị được kiểm toán hay từ bên thứ ba;
- Tạo điều kiện thuận lợi cho công tác lập kế hoạch và giám sát cuộc kiểm toán CNTT;
- Giúp phát triển sự chuyên nghiệp của Kiểm toán viên nhà nước;
- Giúp bảo đảm hoàn thành tốt cuộc kiểm toán CNTT;

(vii) Cung cấp bằng chứng về công tác kiểm toán CNTT đã thực hiện, phục vụ tra cứu, tham khảo sau này.

9.3. Hồ sơ kiểm toán CNTT phải đầy đủ để cho phép một Kiểm toán viên nhà nước có kinh nghiệm về kiểm toán CNTT, không liên quan từ trước đến cuộc kiểm toán có thể hiểu về:

- (i) Nội dung, thời gian và giới hạn các công việc của cuộc kiểm toán CNTT đã thực hiện;
- (ii) Các bằng chứng đã thu thập để hình thành phát hiện và kết luận kiểm toán CNTT;
- (iii) Các vấn đề quan trọng phát sinh trong cuộc kiểm toán CNTT như thay đổi phạm vi kiểm toán, các quyết định liên quan đến rủi ro mới phát hiện khi thực hiện kiểm toán, giải pháp cho những vấn đề chưa đạt được sự đồng thuận giữa đoàn kiểm toán và đơn vị được kiểm toán.

9.4. Hồ sơ kiểm toán phải bao gồm các tài liệu của cả bốn giai đoạn kiểm toán: Lập kế hoạch kiểm toán, thực hiện kiểm toán, lập báo cáo kiểm toán và kiểm tra thực hiện kiến nghị kiểm toán. Nội dung và phạm vi của tài liệu, hồ sơ kiểm toán phụ thuộc nhiều vào xét đoán chuyên môn và đặc thù của mỗi giai đoạn kiểm toán, như:

- (i) Giai đoạn lập kế hoạch kiểm toán: Cần thể hiện được các nội dung liên quan đến kế hoạch kiểm toán và phương pháp luận của cuộc kiểm toán; các tài liệu liên quan đến quá trình xây dựng và việc trao đổi, thống nhất về mục tiêu, tiêu chí với đơn vị được kiểm toán;
- (ii) Giai đoạn thực hiện kiểm toán: Cần thể hiện được phương pháp, kết quả thu thập và phân tích bằng chứng kiểm toán làm cơ sở để đưa ra các xét đoán và kết luận quan trọng của báo cáo kiểm toán CNTT;
- (iii) Giai đoạn lập báo cáo kiểm toán: Cần thể hiện được quá trình thảo luận, trao đổi để hình thành kết luận kiểm toán, các ý kiến phản hồi của đơn vị được kiểm toán, cách thức xử lý các quan điểm trái chiều;
- (iv) Giai đoạn kiểm tra thực hiện kiến nghị kiểm toán: Cần thể hiện được bằng chứng về các kết quả đã thực hiện kiến nghị của đơn vị; ý kiến giải trình của đơn vị về những nội dung chưa thực hiện; các văn bản ý kiến, khiếu

nại về kết quả kiểm toán của đơn vị kiểm toán hoặc các tổ chức cá nhân có liên quan và văn bản trả lời của Kiểm toán nhà nước.

- 9.5. Hồ sơ kiểm toán cần thể hiện sự tham chiếu giữa báo cáo kiểm toán với giấy tờ làm việc, đồng thời Kiểm toán viên nhà nước cần áp dụng các thủ tục phù hợp để duy trì tính bảo mật và lưu trữ an toàn hồ sơ làm việc theo quy định của luật pháp và chuyên môn nghề nghiệp.
- 9.6. Sau khi kết thúc cuộc kiểm toán, Kiểm toán viên nhà nước phải kiểm tra, phân loại, sắp xếp, mã hóa, lưu trữ các tài liệu kiểm toán thành bộ hồ sơ kiểm toán của từng cuộc kiểm toán theo quy định của Kiểm toán nhà nước, đáp ứng yêu cầu kịp thời, thích hợp và đầy đủ.

C. CÁC NGUYÊN TẮC TRIỂN KHAI KIỂM TOÁN CÔNG NGHỆ THÔNG TIN THEO TỪNG GIAI ĐOẠN CỦA CUỘC KIỂM TOÁN

10. Tổng quan về các bước triển khai kiểm toán CNTT

10.1. Các bước thực hiện cuộc kiểm toán CNTT được thực hiện như sau:

- (i) Bước 1: Lập kế hoạch chiến lược về kiểm toán CNTT tại Kiểm toán nhà nước. Kế hoạch chiến lược sẽ định hướng phát triển kiểm toán CNTT từ 3 đến 5 năm tiếp theo.
- (ii) Bước 2: Lập kế hoạch năm về kiểm toán CNTT thực hiện theo quyết định số 03/2017/QĐ-KTNN.
- (iii) Bước 3: Trên cơ sở kế hoạch năm sẽ tiến hành các cuộc kiểm toán thực hiện theo đúng quy trình kiểm toán của Kiểm toán nhà nước bao gồm bốn (4) giai đoạn chính sau:
 - Giai đoạn chuẩn bị kiểm toán;
 - Giai đoạn thực hiện kiểm toán;
 - Giai đoạn lập và phát hành báo cáo kiểm toán;
 - Giai đoạn theo dõi kiểm tra thực hiện kiến nghị kiểm toán.

10.2. Để lập các kế hoạch chiến lược và năm của kiểm toán CNTT của Kiểm toán nhà nước cần triển khai cuộc khảo sát nhằm thu thập và cập nhật tình hình phát triển, ứng dụng CNTT và các vấn đề liên quan trên phạm vi toàn quốc. Cuộc khảo sát thông tin sẽ tiến hành tại các cơ quan sau:

- (i) Bộ Thông tin và Truyền thông là đầu mối quản lý chuyên môn CNTT toàn quốc. Các thông tin thu thập sẽ là các báo cáo về tình hình triển khai ứng dụng CNTT tại các Bộ, Ban Ngành và các Tỉnh cũng như các hệ thống thông tin và CSDL quốc gia.
 - (ii) Bộ Kế hoạch và Đầu tư là đầu mối quản lý các dự án CNTT. Các thông tin thu thập sẽ là:
 - CSDL Quốc gia về việc đầu tư và mua sắm công sử dụng tài sản công và tài chính công liên quan đến CNTT, các dự án CNTT được ghi vốn trung hạn và dài hạn. CSDL trên có thể được mở rộng ra các lĩnh vực khác ngoài CNTT nhằm phục vụ cho công tác kiểm toán chung của Kiểm toán nhà nước.
 - CSDL Quốc gia về việc cấp giấy phép kinh doanh, giấy phép đầu tư trên toàn quốc phục vụ cho công tác kiểm toán chung của Kiểm toán nhà nước.
 - (iii) Kho bạc Nhà nước với phần mềm TABMIS là đầu mối dự toán, tạm ứng, thanh toán, quyết toán của các khoản chi từ NSNN liên quan đến CNTT cũng như các lĩnh vực khác.
 - (iv) Các đầu mối kiểm toán có các hệ thống CNTT quan trọng đang được xã hội, Quốc hội và Kiểm toán nhà nước quan tâm và có định hướng kiểm toán trong kế hoạch kiểm toán năm hoặc chiến lược của Kiểm toán nhà nước. Các đầu mối kiểm toán nên ưu tiên chọn các đơn vị quản các hệ thống CSDL quốc gia như: Tổng cục Thuế, Hải quan gắn với các CSDL thu ngân sách; Ngân hàng nhà nước gắn với CSDL tín dụng; Bộ Tài nguyên và Môi trường gắn với CSDL đất đai ...
- 10.3. Căn cứ vào thông tin thu thập được, Kiểm toán nhà nước sẽ tiến hành xây dựng hoặc cập nhật các CSDL chuyên ngành liên quan đến kiểm toán CNTT hoặc phục vụ công tác kiểm toán chung.
- 10.4. Việc lựa chọn các chủ đề kiểm toán cho kế hoạch chiến lược và kế hoạch năm của kiểm toán CNTT dựa trên phân tích, chấm điểm theo các tiêu chí cụ thể dựa trên các CSDL chuyên ngành, thông tin thu thập bên ngoài và xét đoán chuyên môn. Các tiêu chí chọn lựa chủ đề kiểm toán là:

- (i) Tác động của cuộc kiểm toán mang lại: giá trị gia tăng, các lợi ích và những tác động của cuộc kiểm toán.
 - (ii) Mức độ trọng yếu về tài chính: Việc xem xét dựa trên các thông tin tài chính của các hệ thống/dự án CNTT khai thác từ các CSDL chuyên ngành của Kiểm toán nhà nước. Các tiêu chí tài chính cụ thể cần xem xét là: Giá trị tài chính của hệ thống/dự án CNTT; Giá trị và mức độ quan trọng của các thông tin tài chính mà hệ thống/ dự án CNTT đang/ sẽ xử lý.
 - (iii) Rủi ro trong công tác quản trị CNTT.
 - (iv) Môi trường hoạt động của hệ thống/dự án CNTT.
 - (v) Tầm quan trọng của hệ thống/dự án CNTT đối với đơn vị.
 - (vi) Mức độ ảnh hưởng của hệ thống/dự án CNTT đối với bên ngoài.
 - (vii) Tình hình kiểm toán, kiểm soát, thanh tra trước đây.
 - (viii) Khả năng thực hiện của Kiểm toán nhà nước.
- 10.5. Việc triển khai bốn giai đoạn của cuộc kiểm toán tại Bước 3 được hướng dẫn tại các Mục 11, 12, 13 và 14 tiếp theo của Phần I, Hướng dẫn.

11. Giai đoạn chuẩn bị kiểm toán

- 11.1. Giai đoạn Chuẩn bị kiểm toán về cơ bản thực hiện đúng theo trình tự các bước quy định tại Quy trình Kiểm toán của KTNN: Khảo sát, thu thập thông tin; Đánh giá hệ thống kiểm soát nội bộ và thông tin đã thu thập; Xác định và đánh giá rủi ro kiểm toán; Xác định trọng yếu kiểm toán; Lập kế hoạch kiểm toán; Xét duyệt kế hoạch kiểm toán; Lập và phê duyệt kế hoạch kiểm toán chi tiết; Quyết định kiểm toán; Phổ biến quyết định, kế hoạch kiểm toán và cập nhật kiến thức cho thành viên Đoàn kiểm toán; Chuẩn bị các điều kiện cần thiết cho Đoàn kiểm toán.
- 11.2. Bên cạnh việc tuân theo chuẩn mực, quy trình và hướng dẫn chung của KTNN, khi chuẩn bị kiểm toán cần lưu ý đến các đặc thù của các bước thực hiện chuẩn bị kiểm toán CNTT.

a. Đặc thù trong việc khảo sát, thu thập thông tin

Xây dựng đề cương khảo sát

- 11.3. Nội dung của đề cương khảo sát phải bám sát các nội dung kiểm toán CNTT và phải đảm bảo đề cập đầy đủ các thông tin cho công tác đánh giá sơ bộ và công

tác quản trị CNTT ngay trong giai đoạn khảo sát. Mẫu của đề cương khảo sát của cuộc kiểm toán CNTT độc lập tham khảo ở Phụ lục.C-Hồ sơ biểu mẫu.

Khảo sát, thu thập thông tin về hệ thống kiểm soát nội bộ liên quan đến hệ thống CNTT

Thông tin cần thu thập

11.4. Bao gồm các thông tin liên quan đến các kiểm soát CNTT. Cụ thể là:

(i) Hệ thống kiểm soát chung CNTT:

- Tùy theo mục đích, phạm vi và loại hình kiểm toán sẽ tiến hành thu thập các tài liệu liên quan đến một số hoặc toàn bộ các chuyên đề thuộc về kiểm soát chung CNTT.
- Danh mục tài liệu thu thập có thể tham khảo tại các chương trình kiểm toán mẫu tại phần Phụ lục theo từng chuyên đề, vấn đề kiểm toán kiểm soát chung CNTT.

(ii) Hệ thống kiểm soát phần mềm ứng dụng:

- Tùy theo mục đích, phạm vi và loại hình kiểm toán sẽ tiến hành thu thập các tài liệu liên quan đến việc kiểm soát một số phần mềm nghiệp vụ trọng yếu. Đối với từng phần mềm nghiệp vụ được chọn khảo sát, tài liệu cần thu thập có thể xem chi tiết tại chương trình kiểm toán mẫu các chuyên đề, vấn đề kiểm toán kiểm soát ứng dụng CNTT.

(iii) Báo cáo và các tài liệu của các cuộc kiểm toán, thanh tra trước đây:

- Báo cáo kiểm toán, báo cáo rà soát hoặc các kiểm tra chuyên đề do nội bộ hoặc bên thứ 3 thực hiện có liên quan đến nội dung kiểm toán CNTT.
- Báo cáo định kỳ hoặc báo cáo đột xuất liên quan đến hệ thống CNTT gửi các cơ quan nhà nước hoặc đơn vị chủ quản.
- Báo cáo định kỳ hoặc đột xuất liên quan đến hệ thống CNTT phục vụ công tác quản lý nội bộ.

Phương pháp thu thập thông tin

11.5. Các phương pháp thu thập thông tin tiến hành theo hướng dẫn của chung về phương pháp kỹ thuật lập kế hoạch kiểm toán CNTT ở Mục 15 – Phương pháp và kỹ thuật lập kế hoạch Phần I của Hướng dẫn.

b. Đặc thù trong việc đánh giá hệ thống kiểm soát nội bộ và phân tích thông tin đã thu thập

11.6. Đánh giá độ tin cậy của hệ thống kiểm soát chung CNTT và kiểm soát phần mềm ứng dụng hoạt động trên nền tảng quản trị CNTT phù hợp. Các nội dung đánh giá bao gồm:

- (i) Đánh giá hệ thống quản trị CNTT có được thiết lập và hoạt động.
- (ii) Đánh giá các mục tiêu của hệ thống CNTT có đáp ứng được các mục tiêu nghiệp vụ.
- (iii) Đánh giá toàn bộ hoặc chỉ một số mặt cụ thể của việc kiểm soát chung CNTT tùy theo mục tiêu của cuộc kiểm toán. Các mặt cần đánh giá bao gồm:
 - Hiệu quả của việc quản lý các dự án CNTT;
 - Việc mua sắm và phát triển các tài sản và giải pháp CNTT;
 - Việc vận hành hệ thống CNTT;
 - Việc đảm bảo an toàn bảo mật;
 - Việc đảm bảo vận hành thông suốt và đối phó với các thảm họa;
 - Việc đảm bảo quản lý sự thay đổi phù hợp;
 - Việc đảm bảo việc cung cấp dịch vụ CNTT và tiếp nhận phản hồi từ phía người dùng;
 - Việc đảm bảo sự tuân thủ các quy định nhà nước và nội bộ thông qua hệ thống giám sát, kiểm soát nội bộ;

11.7. Đánh giá kiểm soát ứng dụng trên các phần mềm nghiệp vụ được chọn kiểm toán thông qua việc nắm vững mối liên quan giữa nghiệp vụ và phần mềm và việc tin học hóa các chốt kiểm soát nghiệp vụ trong phần mềm.

c. Đặc thù trong việc xác định và đánh giá rủi ro kiểm toán

11.8. Trên cơ sở thông tin thu thập được và kết quả phân tích, đánh giá thông tin, Kiểm toán viên nhà nước thực hiện xác định và đánh giá rủi ro liên quan đến CNTT để phục vụ việc xây dựng KHKT tổng quát. Định nghĩa, phân loại, và cách xác định các loại rủi ro được hướng dẫn chung tại Mục 7.a – Rủi ro kiểm toán CNTT của Hướng dẫn.

11.9. Gắn với quy trình kiểm toán, việc xác định các rủi ro CNTT có các đặc thù sau:

- (i) Rủi ro CNTT phải gắn chặt với mục tiêu kiểm toán và kết quả khảo sát hệ thống kiểm soát rủi ro liên quan đến CNTT.
- (ii) Rủi ro kiểm soát CNTT thường xảy ra do một chuỗi yếu kém của hệ thống kiểm soát CNTT đi từ công tác kiểm soát quản trị, kiểm soát chung CNTT, kiểm soát ứng dụng và thường luôn được lưu vết trong dữ liệu của hệ thống CNTT. Vì vậy, việc xác định rủi ro kiểm soát CNTT nên được xem xét toàn diện xuyên suốt các góc nhìn khác nhau. Việc áp dụng các thủ tục phân tích số liệu để tìm các dấu vết xảy ra của rủi ro nên thực hiện ngay từ khâu khảo sát.
- (iii) Rủi ro tiềm tàng CNTT thường xảy ra do các trường hợp khá điển hình: lạc hậu về công nghệ; hệ thống CNTT bị phân tán; số người sử dụng lớn; hoặc công thức tính toán thay đổi liên tục; hệ thống máy tính xử lý thông tin chậm. Các lỗi này thường khiến người dùng bỏ qua các thao tác kiểm soát do hệ thống CNTT mang lại sự bất tiện, hoặc đơn vị chủ động bỏ đi các chốt kiểm soát làm chậm hệ thống. Điều này làm suy yếu chung cho toàn bộ hệ thống kiểm soát chung. Vì vậy, rủi ro tiềm tàng luôn phải được xem xét, đánh giá đối với các hệ thống CNTT lớn, nhiều người dùng. Rủi ro tiềm tàng CNTT cao sẽ ảnh hưởng lên toàn bộ hệ thống kiểm soát CNTT khác.

d. Đặc thù trong việc xác định trọng yếu kiểm toán

- 11.10. Việc xác định trọng yếu của kiểm toán CNTT và kết hợp với kết quả đánh giá rủi ro kiểm toán CNTT phục vụ cho việc lập kế hoạch kiểm toán tổng quát được hướng dẫn chung tại Mục 7.b và 7.c của phần Hướng dẫn chung.
- 11.11. Các bước tiến hành cụ thể liên quan đến nội dung kiểm toán CNTT sẽ được tiến hành theo 3 bước:
 - (i) Phân tầng nội dung kiểm toán thành hình cây nội dung kiểm toán với 3 mức: Chuyên đề, Vấn đề và Kiểm soát. Nội dung kiểm toán được chia thành nhiều chuyên đề; Mỗi chuyên đề tiếp tục chia thành các vấn đề; Mỗi vấn đề lại được chia nhỏ thành các kiểm soát. Cách thức tổ chức, phân chia theo mô hình cây Chuyên đề → Vấn đề → Kiểm soát mẫu có thể tham khảo tại phần Hướng dẫn chi tiết.

- (ii) Việc xác định trọng yếu kiểm toán trên các nội dung kiểm toán CNTT sẽ được tiến hành cho từng chuyên đề, vấn đề và các kiểm soát gắn với cây nội dung kiểm toán trên các tiêu chí khác nhau. Các tiêu chí đánh giá trọng yếu phải dựa trên mục tiêu, trọng tâm của cuộc kiểm toán và đánh giá mức độ rủi ro kiểm toán cũng như ngưỡng chấp nhận rủi ro kiểm toán.
- (iii) Trọng yếu của kiểm toán CNTT sẽ bao gồm các danh sách các chuyên đề, vấn đề và kiểm soát sẽ được chọn kiểm toán kèm theo mức độ kiểm toán cho các nội dung kiểm toán trên.

e. Đặc thù trong việc lập kế hoạch kiểm toán tổng quát

Mục tiêu kiểm toán

11.12. Mục tiêu cuộc kiểm toán hệ thống CNTT trong thực tế có thể là:

- (i) Toàn thể hệ thống CNTT của đơn vị:
 - Xác nhận, đánh giá tính đầy đủ và hiệu quả của hệ thống CNTT cùng hệ thống kiểm soát liên quan của đơn vị được kiểm toán.
- (ii) Hoặc chỉ hướng hệ thống CNTT cụ thể:
 - Kiểm tra, đánh giá và xác nhận việc tuân thủ pháp luật, tuân thủ các quy định nội bộ của (một phần hay toàn bộ) hệ thống CNTT.
- (iii) Hoặc hướng đến một chủ đề kiểm toán thuộc kiểm soát CNTT:
 - Đánh giá tính kinh tế, hiệu lực và hiệu quả trong mua sắm, quản lý và sử dụng tài sản CNTT của đơn vị được kiểm toán.
 - Kiểm tra, đánh giá mức độ an toàn bảo mật của hệ thống CNTT của đơn vị.

Ví dụ: Kiểm toán việc bảo mật danh sách khách hàng của các công ty hàng không.

11.13. Mục tiêu kiểm toán của cuộc kiểm toán dự án CNTT có thể là:

- (i) Kiểm tra xác nhận tính chính xác, đúng đắn của báo cáo quyết toán dự án CNTT
- (ii) Kiểm tra tính tuân thủ theo quy định của nhà nước trong việc thực hiện dự án đầu tư CNTT
- (iii) Kiểm tra đánh giá tính hiệu lực, hiệu quả và kinh tế của dự án đầu tư CNTT

- 11.14. Trong cuộc kiểm toán trong môi trường CNTT, các hoạt động kiểm toán CNTT chỉ mang tính hỗ trợ nên trong bản kế hoạch thường chỉ thể hiện các mục tiêu chính của cuộc kiểm toán.
- 11.15. Thực hiện các mục tiêu chung của KTNN: Thông qua hoạt động kiểm toán chỉ ra các sai phạm và kiến nghị với đơn vị được kiểm toán về biện pháp khắc phục, chấn chỉnh công tác quản lý nội bộ; kiến nghị với cấp có thẩm quyền xử lý các vi phạm về chính sách, chế độ và pháp luật của Nhà nước; đề xuất với Chính phủ và cơ quan liên quan những kiến nghị sửa đổi, cải tiến cơ chế quản lý nhằm bảo đảm các nguồn lực tài chính, tài sản công được sử dụng tiết kiệm và có hiệu quả.

Nội dung kiểm toán

- 11.16. Đối với cuộc kiểm toán hệ thống và dự án CNTT độc lập, nội dung kiểm toán là một số chủ đề phù hợp với mục tiêu cuộc kiểm toán và gắn với hệ thống kiểm soát CNTT.
- (i) Gắn với việc kiểm soát quản trị CNTT:
- Đánh giá việc thiết lập cùng tính tuân thủ, đầy đủ và hiệu quả trong công tác quản trị CNTT của đơn vị được kiểm toán.
- (ii) Gắn với việc kiểm soát chung CNTT:
- Đánh giá việc thiết lập cùng tính tuân thủ, đầy đủ và hiệu quả toàn bộ hoặc một phần các nội dung thuộc công tác kiểm soát chung CNTT, như:
 - Việc phát triển và tiếp nhận các sản phẩm CNTT.
 - Việc vận hành hệ thống CNTT.
 - Việc thuê khoán dịch vụ bên ngoài.
 - Việc đảm bảo hoạt động liên tục và ứng phó thảm họa.
 - Kiểm toán an toàn thông tin.
- (iii) Gắn với việc kiểm soát sự tuân thủ và quyết toán chính xác của dự án CNTT:
- (iv) Gắn với việc kiểm soát phần mềm ứng dụng: Kiểm tra và đánh giá việc thiết lập cùng tính tuân thủ đầy đủ và hiệu quả của trong công tác kiểm soát (một số hoặc toàn bộ) phân hệ của các phần mềm nghiệp vụ được

kiểm toán. (Hướng dẫn chi tiết tại các chương trình mẫu các chuyên đề liên quan đến kiểm soát ứng dụng tại phần Phụ lục A4 của Hướng dẫn).

Tiêu chí kiểm toán

- 11.17. Việc chọn tiêu chí cuộc kiểm toán CNTT được hướng dẫn chung tại Tiểu mục 6.f – Tiêu chí kiểm toán CNTT, Phần I của Hướng dẫn. Ngoài ra, có thể tham khảo theo các tiêu chí trình bày tại các chương trình kiểm toán mẫu tại các chương E, F và G thuộc phần II – Hướng dẫn chi tiết của Hướng dẫn.

Phương pháp và thủ tục kiểm toán

- 11.18. Phương pháp và kỹ thuật thực hiện kiểm toán được hướng dẫn chung tại Mục 16 – Phương pháp và kỹ thuật thực hiện kiểm toán Phần I của Hướng dẫn. Phương pháp và thủ tục kiểm toán cho từng chuyên đề, vấn đề kiểm toán và các chốt kiểm soát tham khảo ở các chương trình kiểm toán mẫu thuộc Phần II – Hướng dẫn chi tiết của Hướng dẫn.

f. Đặc thù trong việc Lập và phê duyệt kế hoạch chi tiết

- 11.19. Căn cứ trên kế hoạch tổng quát, trên cơ sở nghiên cứu, đánh giá thông tin, Tổ trưởng xây dựng kế hoạch kiểm toán chi tiết cho đơn vị kiểm toán được lựa chọn bắt đầu bằng việc đưa ra các mục tiêu kiểm toán. Việc lập kế hoạch chi tiết phải thực hiện và phê duyệt trước khi Tổng Kiểm toán nhà nước (hoặc người ủy quyền) phê duyệt quyết định kiểm toán.
- 11.20. Kế hoạch kiểm toán chi tiết phải cụ thể, chi tiết được các mục tiêu kiểm toán, nội dung kiểm toán của kế hoạch kiểm toán tổng quát; xác định rõ phương pháp kiểm toán, phạm vi kiểm toán, giới hạn kiểm toán, địa điểm kiểm toán, thời gian kiểm toán và trên cơ sở kết quả thông tin khảo sát, đánh giá cụ thể về tình hình hoạt động tại đơn vị được kiểm toán. Kế hoạch kiểm toán sẽ hỗ trợ kiểm toán viên chuẩn bị chương trình kiểm toán CNTT.
- 11.21. Chương trình kiểm toán phải bao gồm các yếu tố sau đây: Mục tiêu kiểm toán; nội dung kiểm toán; tiêu chí kiểm toán; thủ tục kiểm toán (công việc và thứ tự các bước Kiểm toán viên nhà nước phải thực hiện tương ứng với các phương pháp kiểm toán). Chương trình kiểm toán bám sát theo mô hình cây nội dung kiểm toán chuyên đề, vấn đề và kiểm soát. Chương trình kiểm toán mẫu theo

chuyên đề, vấn đề kiểm toán cùng chốt kiểm soát tham khảo tại Phần II – Hướng dẫn chi tiết.

- 11.22. Để phát triển chương trình kiểm toán, Kiểm toán viên nhà nước phải có sự hiểu biết rõ ràng về đơn vị được kiểm toán cùng hệ thống CNTT, từ đó xây dựng ma trận kiểm toán với mục tiêu kiểm toán cụ thể cho từng lĩnh vực (quản trị, an ninh thông tin ...) sẽ được kiểm toán.

g. Đặc thù trong việc chuẩn bị nguồn nhân lực kiểm toán

- 11.23. Kiểm toán viên CNTT cần phải có trình độ kỹ thuật, có kỹ năng và kiến thức cần thiết để thực hiện công tác kiểm toán. Kỹ năng và kiến thức là hai yếu tố quan trọng khi lập kế hoạch kiểm toán và phân công nhân viên cho công việc kiểm toán cụ thể.
- 11.24. Trong một số trường hợp, kiểm toán viên có thể tham khảo ý kiến của các chuyên gia về kiểm soát hệ thống thông tin trong nội bộ kiểm toán hoặc sử dụng thuê chuyên gia bên ngoài.
- 11.25. Bên cạnh đó, kiểm toán viên CNTT cần duy trì và nâng cao kỹ năng và chuyên môn thông qua các khóa đào tạo chuyên sâu thường xuyên.

h. Đặc thù trong việc chuẩn bị các điều kiện cần thiết cho Đoàn kiểm toán

- 11.26. Đối với các nội dung kiểm toán CNTT, cần phải đáp ứng các điều kiện sau:
- (i) Có thành viên có kiến thức và kỹ năng liên quan đến CNTT.
 - (ii) Hiểu được hệ thống quy định và môi trường pháp lý mà hệ thống CNTT của đơn vị phải tuân thủ.
 - (iii) Hiểu được các quy trình, chuẩn mực và hướng dẫn kiểm toán CNTT đang áp dụng tại KTNN.
 - (iv) Nắm bắt cách thức thu thập bằng chứng từ hệ thống CNTT của đơn vị.
 - (v) Sử dụng thành thạo các công cụ CNTT hỗ trợ kiểm toán trong việc thu thập, phân tích dữ liệu, thử nghiệm, và các nghiệp vụ kiểm toán khác.
 - (vi) Bảo đảm đầy đủ máy móc thiết bị số để phát hiện và lưu trữ bằng chứng kiểm toán.
 - (vii) Có sẵn các phần mềm, công cụ chuyên dụng để phân tích dữ liệu và thu thập bằng chứng.

12. Giai đoạn thực hiện kiểm toán

- 12.1. Giai đoạn thực hiện kiểm toán về cơ bản thực hiện đúng theo trình tự của các bước quy định tại Quy trình kiểm toán của Kiểm toán nhà nước bao gồm các bước sau: Công bố Quyết định kiểm toán tại đơn vị kiểm toán; Tiến hành kiểm toán; Lập và thông qua biên bản kiểm toán của Tổ kiểm toán; Dự thảo thông báo kết quả kiểm toán tại đơn vị kiểm toán chi tiết.
- 12.2. Bên cạnh việc tuân theo chuẩn mực, quy trình và hướng dẫn chung của KTNN, khi thực hiện kiểm toán cần lưu ý đến các đặc thù về bằng chứng kiểm toán CNTT và phương pháp kỹ thuật kiểm toán CNTT.

a. Đặc thù bằng chứng kiểm toán CNTT

- 12.3. Kiểm toán viên CNTT cần thu thập các thông tin và bằng chứng kiểm toán, tiến hành đánh giá về kiểm soát CNTT trong hệ thống đang được kiểm toán để hiểu được sự đảm bảo rằng các kiểm soát CNTT hiện tại là đáng tin cậy về mặt thiết kế, triển khai và hiệu quả. Ngoài ra, đối với các trường hợp các rủi ro có thể xảy ra trong thực tế do thiếu hệ thống kiểm soát CNTT hoặc hệ thống kiểm soát không hoạt động hiệu quả, Kiểm toán viên nhà nước cần phải thu thập các bằng chứng trên hồ sơ thực tế nhằm tạo cơ sở đánh giá mức độ ảnh hưởng của rủi ro trên thực tế.
- 12.4. Đoạn 40 của CMKTNN 100 – Các nguyên tắc cơ bản trong hoạt động kiểm toán của Kiểm toán nhà nước quy định về việc đầy đủ bằng chứng kiểm toán thích hợp, bằng chứng kiểm toán cần bao gồm cả tính liên quan, tính hợp lệ và độ tin cậy trong đó tính liên quan đề cập đến mức độ mà các bằng chứng kiểm toán liên kết chặt chẽ và quan trọng với mục tiêu kiểm toán, nội dung kiểm toán, tiêu chí kiểm toán được giải quyết.
- 12.5. Các bằng chứng kiểm toán CNTT thể hiện trong hồ sơ kiểm toán phải nêu rõ thuộc chốt kiểm soát gắn với chuyên đề, vấn đề đã được lên kế hoạch kiểm toán và nêu rõ các ảnh hưởng đến hoạt động của đơn vị được kiểm toán.
- 12.6. Trong quá trình thực hiện kiểm toán: Nếu có dấu hiệu làm cho Kiểm toán viên nhà nước tin rằng một tài liệu có thể không xác thực hoặc đã bị sửa đổi mà không được thông báo hoặc những nội dung, số liệu phát hiện có dấu hiệu gian lận thì Kiểm toán viên nhà nước phải tiến hành kiểm tra thêm các thủ tục như:

Xác nhận trực tiếp với bên thứ ba; Sử dụng chuyên gia và các phương pháp hợp pháp khác để đánh giá tính xác thực của tài liệu đó; Kiểm tra, xác minh tài liệu đó từ các nguồn thông tin khác. Nếu các giải trình của đơn vị được kiểm toán là không nhất quán thì Kiểm toán viên nhà nước phải tiến hành kiểm tra về các điểm không nhất quán đó nhằm thu thập đầy đủ bằng chứng thích hợp để khẳng định hoặc loại bỏ nghi ngờ của Kiểm toán viên nhà nước. Việc xác minh, điều tra,... phải lập biên bản và các bằng chứng thu thập được kèm theo. Trong trường hợp phát hiện dấu hiệu sai phạm lớn, các sai phạm có dấu hiệu hình sự, Kiểm toán viên nhà nước, Tổ trưởng phải báo cáo kịp thời cho Trưởng đoàn, Kiểm toán trưởng; Trưởng đoàn, Kiểm toán trưởng phải báo cáo kịp thời với Tổng KTNN để chỉ đạo làm rõ, xử lý.

b. Đặc thù phương pháp kỹ thuật kiểm toán CNTT

- 12.7. Khi tiến hành kiểm toán CNTT, thông thường phải kiểm tra các kiểm soát chung CNTT nhằm đánh giá môi trường CNTT tổng thể của tổ chức, bao gồm các chính sách, thủ tục và thực tiễn vận hành CNTT, cụ thể như sau:
- (i) Đánh giá cơ chế quản trị CNTT có phù hợp với việc thiết lập và thực thi;
 - (ii) Đánh giá các mục tiêu CNTT có phù hợp với mục tiêu kinh doanh;
 - (iii) Đánh giá sự phù hợp đối với quy trình thủ tục được áp dụng cho việc mua sắm giải pháp, hệ thống CNTT (bao gồm, ứng dụng CNTT, phần cứng, phần mềm, nguồn nhân lực, mạng, giải pháp dịch vụ ...);
 - (iv) Các kiểm soát cấp tổ chức được gắn trong các hoạt động CNTT hàng ngày, các quy trình bảo mật thông tin của tổ chức, các quy trình sao lưu dữ liệu và vận hành liên tục, quản lý thay đổi và quản lý dịch vụ, sự cố.
- 12.8. Các chốt kiểm soát CNTT chung khác cùng kiểm soát phần mềm ứng dụng sẽ được chọn lựa phù hợp với mục tiêu kiểm toán, đánh giá rủi ro sơ bộ, kế hoạch kiểm toán, nhân sự Đoàn kiểm toán.
- 12.9. Một số thủ tục kiểm toán CNTT yêu cầu việc áp dụng các công cụ kỹ thuật điều tra, khai thác và phân tích dữ liệu. Khi đó Kiểm toán viên nhà nước sử dụng các kỹ thuật kiểm toán với sự hỗ trợ của phần mềm máy tính như Microsoft Excel, Microsoft Access, IDEA, hoặc ACL để thực hiện. Tham khảo chi tiết thêm ở

mục 17 Phần 3 và Phụ lục C – Hướng dẫn chi tiết kiểm toán trong môi trường CNTT.

13. Giai đoạn lập, phát hành báo cáo kiểm toán

- 13.1. Việc lập và phát hành báo cáo kiểm toán CNTT về cơ bản theo đúng Quy trình kiểm toán của Kiểm toán nhà nước bao gồm các bước:
- (i) Lập dự thảo báo cáo kiểm toán;
 - (ii) Kiểm toán trưởng xét duyệt dự thảo báo cáo kiểm toán;
 - (iii) Tổng Kiểm toán nhà nước xét duyệt dự thảo báo cáo kiểm toán;
 - (iv) Hoàn thiện dự thảo báo cáo kiểm toán, lấy ý kiến của đơn vị được kiểm toán;
 - (v) Thông báo kết quả kiểm toán;
 - (vi) Phát hành báo cáo kiểm toán.
- 13.2. Khi lập báo cáo kiểm toán CNTT cần lưu ý đến các đặc thù liên quan đến đặc thù hồ sơ, tài liệu kiểm toán CNTT, báo cáo kiểm toán CNTT và kiến nghị kiểm toán CNTT.

a. Đặc thù hồ sơ, tài liệu kiểm toán CNTT

- 13.3. Hồ sơ tài liệu kiểm toán CNTT bao gồm:
- (i) Bảng chứng thu thập được làm cơ sở kết luận.
 - (ii) Tất cả các giấy tờ làm việc liên quan đến tổ chức và hệ thống CNTT.
 - (iii) Các điểm thảo luận trong các cuộc phỏng vấn nêu rõ chủ đề thảo luận, tên và chức danh người phỏng vấn, thời gian và địa điểm thực hiện.
 - (iv) Quan sát của Kiểm toán viên bao gồm: Địa điểm và thời gian, lý do quan sát và những người có liên quan.
 - (v) Các báo cáo và dữ liệu thu được từ hệ thống CNTT thực hiện trực tiếp bởi kiểm toán viên hoặc cung cấp bởi nhân viên của đơn vị được kiểm toán. Kiểm toán viên CNTT cần thể hiện và lưu giữ thông tin về nguồn báo cáo, ngày, giờ và các điều kiện chạy báo cáo.
 - (vi) Tại các điểm khác nhau trong tài liệu, kiểm toán viên có thể thêm ý kiến và giải thích của mình về những lo ngại, nghi ngờ và nhu cầu bổ sung thông tin.

- 13.4. Hồ sơ Tài liệu kiểm toán phải được bảo mật và phải được lưu trữ theo quy định của Kiểm toán CNTT.

b. Đặc thù khi lập dự thảo báo cáo kiểm toán CNTT

- 13.5. Trong báo cáo kiểm toán phải đặc biệt cẩn trọng với tính nhạy cảm của các thông tin trình bày như: mật khẩu, tên truy cập, thông tin cá nhân người dùng. Ngoài ra, nên hạn chế sử dụng các khái niệm, từ ngữ kỹ thuật chuyên sâu gây khó khăn không cần thiết cho người đọc.
- 13.6. Báo cáo kiểm toán là tài liệu ghi lại công việc kiểm toán được thực hiện và các bằng chứng kiểm toán hỗ trợ phát hiện và kết luận kiểm toán. Các tài liệu, bằng chứng cần đảm bảo tính tin cậy, đầy đủ và chính xác.
- 13.7. Báo cáo phải trình bày dễ hiểu để các cấp quản lý giám sát, các đối tượng liên quan và công chúng hiểu đúng và đầy đủ nội dung báo cáo.
- 13.8. Báo cáo kiểm toán CNTT cần xem xét các tác động tiêu cực tiềm ẩn khi được công bố/phát hành rộng rãi. Nếu kiểm toán viên CNTT phát hiện một số vấn đề bảo mật trong các hệ thống CNTT, báo cáo kiểm toán có thể xem xét xem nên nêu các tồn tại sau khi hệ thống CNTT đã được sửa chữa, hoặc không nêu các tồn tại trong chi tiết nếu chưa được sửa chữa để tránh những ảnh hưởng bất lợi của báo cáo đến đơn vị được kiểm toán.
- 13.9. Nếu kiểm toán CNTT là một bộ phận của đoàn kiểm toán tuân thủ, kiểm toán hoạt động, kiểm toán tài chính, Tổ kiểm toán CNTT phải lập Biên bản kiểm toán làm căn cứ lập báo cáo kiểm toán của đoàn kiểm toán.

c. Đặc thù kiến nghị kiểm toán CNTT

- 13.10. Các kết luận chung kiểm toán sẽ được tổng hợp từ dưới lên theo cây nội dung kiểm toán CNTT. Các phát hiện tại từng kiểm soát là cơ sở của kết luận vấn đề kiểm toán. Các kết luận tại từng vấn đề là cơ sở của kết luận cho chuyên đề.
- 13.11. Khi xây dựng kiến nghị kiểm toán từ kết luận kiểm toán, các yếu tố sau cần được quan tâm, cân nhắc:
- (i) Tiêu chí kiểm toán: Trình bày các tiêu chuẩn hợp lý về các khía cạnh của tính kinh tế, tính hiệu quả và tính hiệu lực;
 - (ii) Thực trạng: Đánh giá thông qua các phát hiện kiểm toán thu thập được trong quá trình thực hiện kiểm toán;

- (iii) Sự khác biệt giữa tiêu chí kiểm toán và thực trạng: Đây là nhận định và đánh giá của Kiểm toán viên nhà nước trên cơ sở so sánh giữa các phát hiện kiểm toán thu thập được và các tiêu chuẩn đặt ra;
 - (iv) Nguyên nhân cốt lõi: Tập trung vào phân tích nguyên nhân hơn là hiện tượng của vấn đề, xác định rõ nguyên nhân cốt lõi gây ra thực trạng;
 - (v) Tác động: Phân tích các tác động, ảnh hưởng đến các chương trình, các hoạt động, các đơn vị hoặc các nguồn công quỹ và các thể chế do sự khác biệt giữa thực trạng và tiêu chí kiểm toán;
 - (vi) Giải pháp: Liệt kê giải pháp giải quyết các nguyên nhân cốt lõi đã được phân tích;
 - (vii) Lựa chọn giải pháp: Đánh giá tính khả thi, chi phí, lợi ích và rủi ro của các giải pháp nhằm đưa ra kiến nghị kiểm toán phù hợp.
- 13.12. Kiến nghị đưa ra các nội dung phải phù hợp với bối cảnh hoạt động của đơn vị được kiểm toán. Vì vậy, cần lưu ý:
- (i) Các kiến nghị cần tập trung vào các nguyên nhân cốt lõi liên quan đến hệ thống kiểm soát CNTT và cách thức quản lý, giám sát của đơn vị.
 - (ii) Một số phát hiện liên quan đến các lỗ hổng kỹ thuật phải cân nhắc thời điểm công bố báo cáo cho đến khi đơn vị hoàn thành việc khắc phục những lỗ hổng trên để tránh các rủi ro phát sinh cho đơn vị.
 - (iii) Một số kiến nghị các giải pháp kỹ thuật phải cân nhắc đến khả năng tài chính, khả năng quản lý và kế hoạch phát triển trong tương lai của đơn vị. Ngoài ra, phải xem xét, cân trọng trong bối cảnh CNTT đang phát triển nhanh chóng.

14. Giai đoạn theo dõi, kiểm tra thực hiện kết luận kiến nghị kiểm toán

- 14.1. Công tác theo dõi kiểm tra thực hiện kiến nghị kiểm toán về cơ bản theo đúng các chuẩn mực, quy trình và hướng dẫn của Kiểm toán nhà nước liên quan đến việc theo dõi, kiểm tra thực hiện kết luận kiến nghị kiểm toán gồm các bước sau: Theo dõi, đôn đốc việc thực hiện kết luận, kiến nghị kiểm toán; Lập, thẩm định, phê duyệt kế hoạch kiểm tra, quyết định kiểm tra, chuẩn bị triển khai kiểm tra tại đơn vị được kiểm tra; Tổ chức thực hiện kiểm tra việc thực hiện kết luận,

kiến nghị kiểm toán tại đơn vị được kiểm tra; Lập biên bản, báo cáo kiểm tra; thẩm định, phát hành báo cáo kiểm tra; Lưu trữ hồ sơ kiểm tra.

- 14.2. Cần lưu ý khi theo dõi, kiểm tra thực hiện kiến nghị của cuộc kiểm toán hệ thống CNTT như sau: Nếu phát hiện đơn vị chưa thực hiện các biện pháp khắc phục kịp thời, thì phải tiến hành lại các thủ tục kiểm toán trên các nội dung kiến nghị đó. Nếu tình trạng nghiêm trọng có thể cân nhắc mở rộng việc kiểm tra để có báo cáo kiểm tra đúng với thực trạng rủi ro của hệ thống CNTT của đơn vị.

D. PHƯƠNG PHÁP, KỸ THUẬT VÀ CÔNG CỤ KIỂM TOÁN CÔNG NGHỆ THÔNG TIN

15. Phương pháp và kỹ thuật lập kế hoạch

- 15.1. Lập kế hoạch Kiểm toán CNTT dựa trên rủi ro có thể được thực hiện ở ba cấp độ: kế hoạch chiến lược, kế hoạch hàng năm và kế hoạch cuộc Kiểm toán.
- 15.2. Kế hoạch chiến lược kiểm toán CNTT được lập cho một giai đoạn 3-5 năm, nhằm thiết lập các mục đích và mục tiêu dự kiến đạt được thông qua việc thực hiện các chủ đề kiểm toán CNTT. Kế hoạch chiến lược kiểm toán CNTT do Tổng Kiểm toán nhà nước phê duyệt và được rà soát, xem xét lại hàng năm nhằm đảm bảo tính phù hợp của kế hoạch với các điều kiện đã thay đổi trong giai đoạn đó.
- 15.3. Kế hoạch chiến lược kiểm toán CNTT thường bao gồm các nội dung cơ bản sau:
- Mục đích và mục tiêu dự kiến;
 - Danh mục các chủ đề kiểm toán tiềm năng;
 - Thuyết minh về cơ sở lựa chọn và thứ tự ưu tiên các chủ đề kiểm toán;
 - Kế hoạch dự kiến về thời gian và nguồn lực kiểm toán.
- 15.4. Căn cứ vào các chủ đề kiểm toán tiềm năng được lựa chọn, Kiểm toán nhà nước xây dựng kế hoạch kiểm toán CNTT hàng năm cho phù hợp với thông tin thực tế về chủ đề kiểm toán và nguồn lực hiện có của Kiểm toán nhà nước.
- 15.5. Các kế hoạch không những được lập dựa trên cơ sở thông tin của đơn vị thực hiện kiểm toán đang có mà còn dựa trên thông tin về việc đánh giá rủi ro cùng trọng yếu. Các kỹ thuật này cũng được hướng dẫn trong bộ CMKTTN ban hành

kèm Quyết định 02/2016/QĐ-KTNN ngày 15/07/2016. Chuẩn mực kiểm toán ISSAI 5300 quy định việc lập kế hoạch kiểm toán dựa trên việc đánh giá rủi ro và trọng yếu. Vì vậy, việc lập kế hoạch kiểm toán sẽ ưu tiên và lựa chọn các cuộc kiểm toán sẽ được tiến hành dựa trên phương pháp đánh giá rủi ro và trọng yếu.

- 15.6. Kế hoạch chiến lược kiểm toán CNTT được xây dựng phù hợp với kế hoạch chiến lược tổng thể của Kiểm toán nhà nước.
- 15.7. Việc lên kế hoạch kiểm toán dựa trên rủi ro bao gồm việc giải quyết các yếu tố rủi ro sẽ ảnh hưởng đến cuộc kiểm toán và tính chính xác của các kết luận kiểm toán được rút ra sau mỗi đợt kiểm toán. Đánh giá rủi ro ở cấp độ lập kế hoạch chiến lược kiểm toán CNTT sẽ giải quyết vấn đề liên quan đến kiểm toán CNTT đối với mục tiêu chiến lược tổng thể của KTNN, nhằm đảm bảo sự quản trị tốt, tính minh bạch và trách nhiệm giải trình của chính phủ.
- 15.8. Kiểm toán nhà nước lập kế hoạch kiểm toán CNTT hàng năm phù hợp với kế hoạch chiến lược của kiểm toán CNTT. Giai đoạn này bao gồm việc lựa chọn hệ thống CNTT hoặc những thực thể cần được kiểm toán dựa trên cách tiếp cận rủi ro để ưu tiên lựa chọn danh sách cuộc kiểm toán phù hợp
- 15.9. Đối với từng cuộc kiểm toán cụ thể, KTNN sẽ tiến hành lập kế hoạch kiểm toán CNTT cấp độ Đoàn kiểm toán bao gồm vấn đề liên quan đến các lĩnh vực rủi ro quan trọng được xác định trong kế hoạch kiểm toán CNTT hàng năm và chương trình kiểm toán chi tiết cho cuộc kiểm toán trên.
- 15.10. Mục tiêu của kiểm toán CNTT phải phù hợp với các lĩnh vực rủi ro được xác định trong kế hoạch kiểm toán CNTT của cuộc kiểm toán và phụ thuộc vào loại hình tiếp cận kiểm toán – kiểm toán tài chính, kiểm toán tuân thủ hay kiểm toán hoạt động.
- 15.11. Kiểm toán viên nhà nước sẽ xác định phạm vi kiểm toán trong giai đoạn lập kế hoạch để đảm bảo đạt được các mục tiêu kiểm toán. Sau khi quyết định các mục tiêu của kiểm toán CNTT, kiểm toán viên CNTT quyết định về phạm vi kiểm toán bao gồm:

- (i) Phạm vi kiểm soát nằm trong phạm vi cho phép của hệ thống CNTT và các chức năng của hệ thống đó. Trên cơ sở đó, xác định các dữ liệu, tài liệu liên quan đến phạm vi kiểm soát đã chọn;
 - (ii) Các quy trình CNTT cần được kiểm toán, vị trí của các hệ thống CNTT, khoảng thời gian cần được thực hiện;
 - (iii) Loại hình kiểm toán (kiểm toán tài chính/kiểm toán tuân thủ/kiểm toán hoạt động).
- 15.12. Phạm vi kiểm toán phụ thuộc vào mức độ rủi ro của hệ thống CNTT được kiểm toán cũng như các nguồn lực sẵn có. Nếu rủi ro cao hơn, phạm vi có thể phải thu hẹp nhưng mở rộng phạm vi kiểm soát trong phạm vi của kiểm toán CNTT.

16. Phương pháp và kỹ thuật thực hiện kiểm toán

16.1. Một số kỹ thuật kiểm toán được sử dụng khi thực hiện kiểm toán CNTT:

- (i) Thực hiện lại: Kiểm toán viên nhà nước thực hiện lại hoạt động của một kiểm soát để đảm bảo rằng nó đã được thực hiện đúng như mô tả trong thiết kế.
- (ii) Quan sát: Kiểm toán viên nhà nước quan sát chủ kiểm soát thực hiện kiểm soát trong thực tế với các tình huống khác nhau.
- (iii) Phỏng vấn: Phỏng vấn là việc tìm kiếm thông tin từ những người có hiểu biết trong nội bộ đơn vị được kiểm toán hoặc từ bên ngoài đơn vị được kiểm toán. Phỏng vấn được sử dụng rộng rãi trong suốt quá trình kiểm toán cùng với các thủ tục kiểm toán khác. Phỏng vấn có nhiều hình thức, phỏng vấn bằng văn bản hoặc phỏng vấn bằng lời.
- (iv) Đánh giá: Kiểm toán viên nhà nước kết hợp các kỹ thuật điều tra, kiểm tra và tái thực hiện để kiểm tra kiến thức của một cá nhân về một chủ đề hoặc khả năng thực hiện kiểm soát một cách hiệu quả.
- (v) Kiểm tra chi tiết: Kiểm toán viên nhà nước xem hồ sơ hoặc tài liệu hỗ trợ hoạt động kiểm soát.
- (vi) Truy vấn hệ thống: Kiểm toán viên nhà nước kiểm tra truy vấn thông tin kiểm toán thông qua việc truy cập trực tiếp hệ thống CNTT của đơn vị.
- (vii) Thủ tục phân tích: Là việc so sánh các dữ liệu hoặc phân tích các biến động hay các mối quan hệ được xác định là không nhất quán với các tài

liệu, thông tin liên quan khác hoặc có sự chênh lệch lớn so với các giá trị dự kiến.

(viii) Tính toán lại: Là việc Kiểm toán viên nhà nước kiểm tra độ chính xác về mặt toán học của các số liệu. Tính toán lại có thể được thực hiện thủ công hoặc tự động.

(ix) Xác nhận từ bên ngoài: Là bằng chứng kiểm toán mà Kiểm toán viên nhà nước thu thập được dưới hình thức phúc đáp trực tiếp của bên thứ ba (bên xác nhận) ở dạng văn bản.

16.2. Hoạt động kiểm toán CNTT bao gồm 2 hoạt động chính sau: tiến hành kiểm toán các kiểm soát liên quan đến CNTT và đánh giá mức độ ảnh hưởng thực tế của các rủi ro gây ra do việc thiếu kiểm soát hoặc chót kiểm soát hoạt động không hiệu quả.

a. Hướng dẫn cách kiểm toán các kiểm soát

16.3. Khi đánh giá các kiểm soát CNTT, Kiểm toán viên nhà nước cần thực hiện các công việc:

(i) Đánh giá thiết kế và triển khai các kiểm soát: Là việc xem xét liệu kiểm soát, riêng lẻ hoặc kết hợp với các kiểm soát khác, có khả năng ngăn ngừa một cách hiệu quả, hoặc phát hiện và điều chỉnh sai sót trọng yếu. Thủ tục đánh giá thiết kế và triển khai sẽ kiểm tra kiểm soát tồn tại và đơn vị có thực sự đang sử dụng kiểm soát đó hay không.

(ii) Thử nghiệm hiệu quả hoạt động đối với từng kiểm soát: Là việc thu thập các bằng chứng kiểm toán nhằm chứng minh kiểm soát hoạt động một cách hiệu quả như thiết kế đưa ra xuyên suốt kỳ kiểm toán. Chính vì vậy kiểm toán viên có thể thực hiện thử nghiệm hiệu quả hoạt động tại nhiều mốc thời gian trong kỳ kiểm toán.

16.4. Kiểm toán viên chỉ thực hiện thử nghiệm hiệu quả hoạt động đối với những kiểm soát chúng ta xác định là có thiết kế hiệu quả và được triển khai. Kiểm toán viên không thực hiện thử nghiệm hiệu quả hoạt động đối với những kiểm soát có thiết kế hay triển khai không hiệu quả.

16.5. Thử nghiệm hiệu quả hoạt động của kiểm soát khác với việc thu thập các bằng chứng kiểm toán chứng minh việc kiểm soát được triển khai như sau:

- (i) Khi thu thập các bằng chứng kiểm toán của việc triển khai kiểm soát, Kiểm toán viên nhà nước xác định các kiểm soát liên quan có tồn tại và doanh nghiệp sử dụng chúng. Trong khi đó khi thực hiện việc thử nghiệm hiệu quả hoạt động, kiểm toán viên thu thập bằng chứng kiểm toán cho việc kiểm soát được hoạt động một cách hiệu quả.
 - (ii) Công tác này bao gồm việc thu thập các bằng chứng kiểm toán rằng kiểm soát được thực hiện như thế nào trong suốt kỳ kiểm toán, tính nhất quán trong việc những gì đang được sử dụng, bởi ai và bằng cách nào.
- 16.6. Thủ tục phỏng vấn riêng lẻ là không đủ để đánh giá thiết kế của một kiểm soát và để xác định xem nó đã được thực hiện hay không. Bên cạnh đó, kiểm toán viên nên thực hiện thêm các thủ tục kiểm toán khác kết hợp với thủ tục phỏng vấn để kiểm tra hiệu quả hoạt động của kiểm soát như sau:
- (i) Nếu nhiều kiểm soát khác nhau được sử dụng tại các thời điểm khác nhau trong kỳ kiểm toán, Kiểm toán viên nhà nước cần xem xét từng kiểm soát một cách độc lập và kiểm tra nó một cách riêng biệt. Việc phân tách kiểm soát cho từng giai đoạn trong kỳ kiểm toán yêu cầu phải xem xét riêng biệt về bản chất, phạm vi và thời gian của các thủ tục kiểm toán.
 - (ii) Nếu Kiểm toán viên nhà nước thực hiện kiểm toán các kiểm soát trước cuối kỳ thì cần phải bổ sung thêm các bằng chứng kiểm toán cho giai đoạn kiểm toán còn lại của kỳ kiểm toán tính từ thời điểm kiểm toán tới cuối kỳ.
 - (iii) Kiểm toán viên nhà nước cần thiết kế các thủ tục kiểm toán đủ để đảm bảo tương đối các kiểm soát được hoạt động một cách hiệu quả trong suốt kỳ kiểm toán.

Đánh giá thiết kế và triển khai các kiểm soát

- 16.7. Các thủ tục kiểm toán được Kiểm toán viên nhà nước sử dụng để thu thập các bằng chứng kiểm toán cho việc thiết kế kiểm soát bao gồm:
- (i) Kiểm tra tài liệu và hồ sơ.
 - (ii) Quan sát các kiểm soát đang được thực hiện.
 - (iii) Phỏng vấn các cán bộ chịu trách nhiệm chuyên trách.

- (iv) Tiến hành "thực nghiệm" để kiểm toán viên nhà nước theo dõi một giao dịch/sự kiện thông qua từng bước của quy trình liên quan.
 - (v) Vận dụng các kinh nghiệm liên quan đã có đối với doanh nghiệp.
- 16.8. Khi đánh giá thiết kế, Kiểm toán viên nhà nước cần phải xem xét tới các yếu tố:
- (i) Mục tiêu của kiểm soát.
 - (ii) Những rủi ro giúp giảm thiểu.
 - (iii) Kiểm soát được thực hiện như thế nào.
 - (iv) Tần suất của kiểm soát được áp dụng
 - (v) Kiểm soát có được cấp quản lý tài liệu hóa lại không.
 - (vi) Các kiến thức, kinh nghiệm và chuyên môn của người thực hiện kiểm soát (nếu là kiểm soát thủ công).
 - (vii) Khả năng / kinh nghiệm của người thực hiện kiểm soát (nếu là kiểm soát thủ công).
 - (viii) Bản chất và mức độ sai sót bao gồm cả cố ý và không cố ý mà kiểm soát có thể ngăn ngừa hoặc phát hiện và sửa sai nếu có thể.

Thử nghiệm hiệu quả hoạt động

- 16.9. Mục tiêu của thử nghiệm hiệu quả hoạt động là đánh giá các kiểm soát được áp dụng như thế nào, có nhất quán và thống nhất trong suốt kỳ kiểm toán hay không và ai là người áp dụng.
- 16.10. Khi đánh giá các Kiểm toán viên nhà nước cần xem xét các yếu tố sau:
- (i) Kỹ thuật được sử dụng để thu thập các bằng chứng kiểm toán
 - (ii) Bản chất của cuộc thử nghiệm
 - (iii) Phạm vi của cuộc thử nghiệm
 - (iv) Thời gian của cuộc thử nghiệm.
- 16.11. Thử nghiệm hiệu quả hoạt động tùy thuộc vào tần suất của kiểm soát để từ đó xác định số lượng tổng mẫu trong kỳ kiểm toán và thực hiện chọn mẫu bất kỳ để thực hiện hoạt động thử nghiệm.

b. Đánh giá mức độ ảnh hưởng thực tế của rủi ro

- 16.12 Khi đã phát hiện các rủi ro do việc thiếu kiểm soát CNTT hoặc kiểm soát CNTT hoạt động không hiệu quả, Kiểm toán viên nhà nước cần tiếp tục tiến hành đánh giá mức độ ảnh hưởng của rủi ro đã xảy ra trong thực tế thông qua chỉ rõ các

bằng chứng thực tế cụ thể. Kiểm toán viên nhà nước cần tiến hành thủ tục kiểm tra chi tiết thông qua đối chiếu giữa số liệu trên hệ thống CNTT và hồ sơ gốc nhằm đánh giá đúng mức độ ảnh hưởng thực tế của rủi ro liên quan đến hệ thống CNTT.

17. Công cụ CNTT hỗ trợ kiểm toán – CAATs

a. Tổng quan CAATs

Khái niệm CAATs

- 17.1. Kỹ thuật kiểm toán với sự trợ giúp của máy tính (Computer Assisted Audit Techniques - CAATs) là các thủ tục kiểm toán được thực hiện bằng công nghệ máy tính, thường là trên khối lượng lớn dữ liệu, cung cấp khả năng phân tích triệt để các tập dữ liệu, để mô tả, trích xuất và tổng hợp các hạng mục dựa trên các đặc tính cụ thể và áp dụng các luồng xử lý được lập trình sẵn.
- 17.2. Có nhiều yếu tố ảnh hưởng tới việc sử dụng CAATs, bao gồm cả việc thực hiện thủ tục kiểm toán bằng phương pháp thủ công sẽ không khả thi hoặc không thể thực hiện được do khối lượng giao dịch lớn và/hoặc tính phức tạp của việc tính toán.
- 17.3. Sau đây là một số ví dụ phổ biến về việc sử dụng CAATs như một phần của thủ tục kiểm toán. CAATs để hỗ trợ Kiểm toán viên nhà nước trong việc:
 - (i) Kiểm tra toàn bộ dữ liệu, bao gồm việc thực hiện lại các tính toán và kiểm tra sự nhất quán của dữ liệu theo các chuẩn mực kế toán.
 - (ii) Xác định các đối tượng không theo quy luật trong một tập đáp ứng các tiêu chuẩn đã được xác định trước (ví dụ như xác định các giao dịch bất thường)
 - (iii) Thực hiện các quy trình đánh giá rủi ro
 - (iv) Thực hiện các thủ tục phân tích
 - (v) Kiểm tra hiệu quả hoạt động của các kiểm soát
 - (vi) Kiểm tra tính chính xác của các báo cáo do hệ thống tạo ra

Lợi ích của CAATs

- 17.4. CAATs cung cấp sự đảm bảo ở mức cao hơn so với các kỹ thuật kiểm toán khác, đặc biệt các phương pháp thử nghiệm thủ công do những lý do sau đây:
 - (i) Các vấn đề kế toán cốt lõi được phân tích sâu.

- (ii) Thử nghiệm và phân tích 100% khối lượng dữ liệu lớn trong thời gian ngắn.
- (iii) Các thử nghiệm có thể được lập lại ở các dữ liệu khác nhau.
- (iv) Có thể dễ dàng thay đổi các thử nghiệm bằng cách thay đổi các tham số.
- (v) Các báo cáo, kết quả thử nghiệm có thể tự động được sinh ra bởi các ứng dụng hoặc phần mềm CAATs.
- (vi) Các nguồn lực kiểm toán được sử dụng có hiệu quả.

Vai trò của CAATs.

- 17.5. Phần lớn các đơn vị được kiểm toán đã tin học hóa các hoạt động cốt lõi, nên kỹ thuật CAATs ngày càng được sử dụng rộng rãi bởi các kiểm toán viên nhà nước khi thực hiện các thử nghiệm trọng yếu trong kiểm toán báo cáo tài chính và kiểm toán tuân thủ. Khi sử dụng kỹ thuật CAATs, mục đích của cuộc kiểm toán không thay đổi, nhưng phương pháp kiểm toán và thu thập bằng chứng thay đổi.
- 17.6. CAATs giúp tăng hiệu quả của việc lập kế hoạch kiểm toán. Kiểm toán viên nhà nước có thể sử dụng CAATs để thực hiện các thủ tục tổng hợp và phân tích dữ liệu ban đầu. Từ đó, kiểm toán viên nhà nước có thể xác định trọng tâm kiểm toán, các số liệu bất thường, các trường hợp ngoại lệ và lập kế hoạch kiểm tra chi tiết sau này.
- 17.7. CAATs giúp tăng tính hiệu lực của việc thực hiện kiểm toán. Kiểm toán viên nhà nước có thể sử dụng CAATs để phân tích sâu dữ liệu bằng cách áp dụng các tham số, các tiêu chuẩn phân tích khác nhau. Việc chọn mẫu kiểm toán được thực hiện dễ dàng bằng cách áp dụng các phương pháp chọn mẫu theo thống kê được cài đặt sẵn trong ứng dụng hoặc phần mềm. CAATs giúp kiểm toán viên nhà nước kiểm tra chất lượng dữ liệu bằng cách kiểm tra các khoảng trống, sự trùng lặp, thiếu sót của các bản ghi dữ liệu. CAATs giúp tiết kiệm thời gian, chi phí và nguồn nhân lực khi thực hiện kiểm toán.

b. Phân loại theo kỹ thuật ứng dụng CAATs

- 17.8. Có hai loại CAATs: CAATs được sử dụng để xem xét và đánh giá các chương trình/phần mềm CNTT; và CAATs được sử dụng để phân tích và kiểm tra dữ liệu.

- 17.9. Thông thường, CAATs phân tích chương trình/phần mềm CNTT yêu cầu trình độ hiểu biết chuyên môn về CNTT của kiểm toán viên nhà nước cao hơn CAATs phân tích dữ liệu. Kiểm toán viên nhà nước cần phải trang bị các hiểu biết, kỹ năng, kỹ thuật liên quan đến cấu trúc và môi trường đặc trưng của hệ thống CNTT được kiểm toán. Nếu nguồn nhân lực không đáp ứng được yêu cầu chuyên môn thì không được tiến hành CAATs phân tích chương trình/phần mềm.
- 17.10. Việc phân tích dữ liệu thông thường bỏ qua các chương trình sinh ra các dữ liệu, mà tập trung nhiều hơn vào việc đánh giá dữ liệu được xử lý bởi hệ thống. Trong khi đó, dữ liệu có thể được đánh giá khá hiệu quả bằng cách phân tích chương trình sinh ra dữ liệu đó. Phương pháp này chủ yếu được sử dụng để xác định các đoạn mã thừa hoặc đoạn mã được sử dụng với mục đích xấu. Việc kiểm tra được thực hiện bằng cách chạy chương trình CAATs độc lập để kiểm tra xem có những sự thay đổi không được phép nào trong chương trình hay không.
- 17.11. CAATs được sử dụng để xem xét và đánh giá các chương trình/phần mềm CNTT thường được sử dụng trong kiểm toán tuân thủ trong khi CAATs phân tích dữ liệu được sử dụng trong kiểm toán hoạt động và kiểm toán điều tra.

c. Phân loại phần mềm CAATs

- 17.12. Các loại phần mềm CAATs được phân chia thành các loại như phần mềm kiểm toán chung GAS (General Purpose Audit Software), phần mềm tiện ích, kiểm tra dữ liệu và hệ thống chuyên gia. Một số loại phần mềm CAATs phổ biến: Phần mềm kiểm toán chung (GAS); SQL và các công cụ dựa trên SQL; Microsoft Access; và các công cụ khác như Microsoft Excel.

Phần mềm kiểm toán chung (GAS)

- 17.13. GAS là một phần mềm chuẩn có khả năng đọc trực tiếp và truy cập dữ liệu từ các nền tảng cơ sở dữ liệu khác nhau, hệ thống file dữ liệu phẳng và định dạng ASCII. GAS cung cấp cho Kiểm toán viên nhà nước một phương thức độc lập để truy cập vào dữ liệu để thực hiện việc phân tích. Các chức năng của GAS bao gồm:
- (i) Truy cập file – cho phép đọc các định dạng bản ghi và cấu trúc file khác nhau

- (ii) Tổ chức lại tập tin – Cho phép lập chỉ mục (index), sắp xếp, nối và liên kết (link) tới các file khác
 - (iii) Chọn lọc dữ liệu – cho phép lọc trên toàn tập dữ liệu theo các điều kiện và tiêu chí lựa chọn
 - (iv) Chức năng thống kê – cho phép chọn mẫu, phân tầng và phân tích tần suất dữ liệu
 - (v) Chức năng số học- Cho phép thực hiện các phép toán số học trên tập dữ liệu
- 17.14. Một số phần mềm GAS điển hình như IDEA (Interactive Data Extraction & Analysis) và ACL (Audit Command Language). Cả hai phần mềm này sử dụng trên nền MS Windows có khả năng nhập và xuất dữ liệu ở nhiều định dạng khác nhau. Kiểm toán viên nhà nước cần hiểu rõ khả năng và hạn chế của GAS để sử dụng chúng một cách hiệu quả.

Các công cụ dựa trên ngôn ngữ SQL

- 17.15. Ngôn ngữ truy vấn có cấu trúc (SQL – Structured Query Language) được sử dụng để định nghĩa và thao tác dữ liệu trong các hệ thống quản lý dữ liệu quan hệ. Ngôn ngữ SQL cho phép Kiểm toán viên nhà nước thực hiện các câu lệnh truy vấn trong CSDL và các nền tảng không phổ biến.
- 17.16. Các công cụ dựa trên ngôn ngữ SQL cung cấp giao diện thân thiện cho phép lựa chọn các dữ liệu theo yêu cầu và đưa ra các tiêu chí cụ thể để chiết xuất dữ liệu. Công cụ này cho phép Kiểm toán viên nhà nước thực hiện các câu truy vấn trực tiếp trên CSDL của đơn vị kiểm toán (trong trường hợp Kiểm toán viên nhà nước gặp khó khăn khi tải dữ liệu về máy tính của Kiểm toán viên nhà nước). Nếu có thể tải dữ liệu về máy tính cá nhân, Kiểm toán viên nhà nước có thể thực hiện phân tích dữ liệu bằng cách sử dụng SQL.
- 17.17. Tuy nhiên các công cụ CAATs dựa trên ngôn ngữ SQL không hiệu quả khi sử dụng trên các hệ thống cũ do nền tảng cơ sở dữ liệu của các hệ thống này khác với cấu trúc dữ liệu SQL và đòi hỏi Kiểm toán viên nhà nước phải có kỹ năng lập trình nhất định để trích xuất và khai thác dữ liệu cần thiết.
- 17.18. Trên thực tế, kể cả trong trường hợp đơn vị được kiểm toán cung cấp quyền cho Kiểm toán viên nhà nước truy cập vào hệ thống và/hoặc CSDL, Kiểm toán viên

nhà nước cũng không được khuyến nghị thực hiện truy vấn dữ liệu trực tiếp trên CSDL được kiểm toán vì các lý do sau:

- Hiệu năng của hệ thống có thể bị ảnh hưởng trong trường hợp thực hiện câu lệnh truy vấn phức tạp.
- Khi thực hiện truy vấn, Kiểm toán viên nhà nước có thể vô tình xóa hoặc thay đổi dữ liệu kiểm toán;
- Kiểm toán viên nhà nước có thể không có khả năng bảo vệ các tài liệu/dữ liệu kiểm toán và bằng chứng kiểm toán có thể bị thay đổi nếu việc phân tích dữ liệu được thực hiện trực tiếp trên hệ thống của đơn vị kiểm toán.

TOAD (Tool for Application Developers) – Công cụ dùng cho phát triển ứng dụng

- 17.19. Công cụ này dùng để xem các quan hệ, các ràng buộc, hạn chế trong các hệ quản trị CSDL như Oracle hoặc Microsoft SQL. Công cụ này đòi hỏi người dùng phải có kiến thức về CSDL căn bản.

Microsoft Access

- 17.20. Microsoft Access cho phép Kiểm toán viên nhà nước dễ dàng thực hiện câu lệnh truy vấn và nhập xuất dữ liệu từ rất nhiều định dạng khác nhau. Hạn chế của phần mềm là mỗi CSDL trên Access không được vượt quá 2GB dung lượng và hiệu năng bị ảnh hưởng trong trường hợp thực hiện truy vấn trên các file dữ liệu lớn.

Các công cụ khác

- 17.21. Các công cụ tương tự như Microsoft Excel có thể được sử dụng để thực hiện một số tác vụ đơn giản như trích xuất dữ liệu đáp ứng một vài tiêu chí, sắp xếp và tính toán. Tuy nhiên, số lượng bản ghi trong một file rất hạn chế. Các công cụ khác để khai phá dữ liệu như WizRule, có thể xử lý dữ liệu lớn và xử lý trên hàng trăm giả thiết và luật khác nhau. Nó có thể truy cập các CSDL như Oracle, SQL, Microsoft Access và có thể hoạt động như công cụ phân tích dữ liệu trực tuyến (OLAP).

d. Ứng dụng CAATs

- 17.22. Một số yếu tố cần xem xét khi quyết định việc sử dụng CAATs như sau:

- (i) Việc sử dụng CAATs có mang lại giá trị tăng thêm cho cuộc kiểm toán không?
 - (ii) Các thử nghiệm có được lặp lại ở các cuộc kiểm toán tương tự trong tương lai tại cùng đơn vị kiểm toán hay tại các đơn vị kiểm toán khác có bản chất kinh doanh tương tự không?
 - (iii) Lĩnh vực kiểm toán có độ rủi ro cao không?
 - (iv) Đơn vị được kiểm toán có sử dụng hệ thống CNTT hỗ trợ hoạt động kinh doanh chính không?
 - (v) Các giao dịch có được xử lý online, theo thời gian thực không?
 - (vi) Việc sử dụng các kỹ thuật kiểm toán khác có hiệu quả không?
- 17.23. Thông thường, CAATs được sử dụng để phân tích chương trình/ứng dụng đóng vai trò quan trọng trong hoạt động của đơn vị được kiểm toán, mà ở đó việc phân tích dữ liệu không thể đưa ra đảm bảo về tính chính xác và hiệu lực của các kiểm soát.
- 17.24. CAATs được ứng dụng khi Kiểm toán viên nhà nước cần lặp lại các thử nghiệm trong các cuộc kiểm toán tương lai. Các ứng dụng hoặc phần mềm CAATs sẽ hữu ích khi kiểm toán các hệ thống xử lý dữ liệu trực tuyến trên thời gian thực và những hệ thống có rủi ro cao khác.

Nguyên tắc sử dụng CAATs

- 17.25. Khi đã quyết định sử dụng CAATs để thực hiện kiểm toán, Kiểm toán viên nhà nước cần phải xây dựng kế hoạch sử dụng CAATs. Điều quan trọng là phải lấy được đúng dữ liệu và xử lý dữ liệu đúng. Do vậy, Kiểm toán viên nhà nước cần có hiểu biết về các vấn đề sau:
- (i) Đơn vị được kiểm toán và các hoạt động liên quan đến CNTT.
 - (ii) Tổng quan về hệ thống CNTT của đơn vị
 - (iii) Hệ thống CNTT cần kiểm toán: Cấu trúc của CSDL, chi tiết định dạng các bảng, file dữ liệu, quan hệ giữa các bảng, file dữ liệu, các khóa chính, người sử dụng hệ thống, dữ liệu đầu vào, đầu ra và các báo cáo sinh ra từ hệ thống.

- 17.26. Kiểm toán viên nhà nước ghi chép lại hiểu biết về hệ thống và trao đổi với đơn vị kiểm toán nhằm xác nhận hiểu biết của mình. Xác định các thử nghiệm sẽ được thực hiện và xác định các file, các bảng dữ liệu sẽ được phân tích.

Mục tiêu sử dụng CAATs

- 17.27. Kiểm toán viên nhà nước có thể sử dụng các chức năng sẵn có của phần mềm CAATs hoặc tự thực hiện phân tích dữ liệu để đạt được các mục tiêu sau:

- (i) Phát hiện các ngoại lệ: Kiểm toán viên nhà nước có thể truy xuất dữ liệu đáp ứng hoặc vi phạm một số các tiêu chí đề ra hoặc các trường hợp ngoại lệ từ dữ liệu đơn vị cung cấp để kiểm toán chi tiết sau này.
- (ii) Tổng hợp số liệu: Tổng hợp số liệu được Kiểm toán viên nhà nước thực hiện để kiểm tra tính đầy đủ của dữ liệu và số liệu đơn vị cung cấp cũng như điều chỉnh số liệu kế toán.
- (iii) So sánh các tệp tin: So sánh các tệp tin dữ liệu tại các thời điểm khác nhau để xác định các thay đổi giữa các thời điểm.
- (iv) Phân tầng dữ liệu: Kiểm toán viên nhà nước phân chia dữ liệu theo mảng số liệu, hoặc nhóm theo một số tiêu chuẩn để chọn mẫu.
- (v) Chọn mẫu: Kiểm toán viên nhà nước có thể chọn mẫu đại diện một cách khoa học bằng cách sử dụng các phương pháp chọn mẫu cài đặt sẵn trong phần mềm.
- (vi) Kiểm tra sự trùng lặp: xác định và phân tích trùng lặp trong file dữ liệu đơn vị cung cấp.

Ví dụ: Các hóa đơn trùng hoặc giao dịch trùng có thể dễ dàng phát hiện khi sử dụng phần mềm phân tích. Điều này không chỉ giúp đánh giá kiểm soát đầu vào của hệ thống mà còn trong việc xác định các giao dịch khả nghi.

- (vii) Xác định các khoảng trống: Chức năng này nếu có sẵn trong các phần mềm hỗ trợ kiểm toán sẽ cho phép Kiểm toán viên nhà nước xác định các khoảng trống trong dữ liệu như số hóa đơn, ngày tháng và số thứ tự mua hàng. Điều này có thể chỉ ra sự thiếu sót kiểm soát trong hệ thống cũng như các sai sót hay sai phạm.

Ví dụ: Sử dụng phần mềm hỗ trợ kiểm toán có thể dễ dàng tính toán thời gian cần thiết từ khi lập lệnh mua hàng tới khi nhận hàng và thanh toán. Tương

tự như vậy, Kiểm toán viên nhà nước có thể phân tích tuổi nợ dễ dàng bằng các phần mềm hỗ trợ này.

- (viii) Phân tích thời gian: Kiểm toán viên nhà nước có thể nhóm các giao dịch theo thời gian để kiểm tra tính hợp lệ của các thủ tục.
- (ix) Hỗ trợ thực hiện thủ tục phân tích khi kiểm toán: CAATs có thể được sử dụng bởi Kiểm toán viên nhà nước để thực hiện thủ tục phân tích cơ bản như phân tích xu hướng, tính toán các tỷ lệ, phân tích thành phần, kỹ thuật mô hình hóa, tính toán chuẩn giúp dễ dàng so sánh mối quan hệ bên trong của tập các dữ liệu và tập trung vào các vùng dữ liệu cần kiểm toán lưu ý.
- (xi) Tính toán lại: Tính toán lại có thể được thực hiện để xác định tính chính xác của công thức. Cũng như vậy, dữ liệu đầu vào có thể được xử lý lại để đánh giá các kiểm soát và so sánh kết quả của việc tính toán với dữ liệu đơn vị cung cấp từ hệ thống.
- (x) Khai thác dữ liệu: Kỹ thuật này cho phép khai thác những thông tin quan trọng từ một số lượng lớn dữ liệu, được sử dụng trong các hệ thống hỗ trợ ra quyết định. Kiểm toán viên nhà nước có thể khai thác sâu dữ liệu để tìm kiếm các xu hướng cũng như các hình thái trong một khoảng thời gian giúp xác định các giao dịch bất thường để kiểm tra chuyên sâu.
- (xii) Tạo thêm trường dữ liệu: CAATs có thể được sử dụng để tạo thêm các trường trong dữ liệu kiểm toán để trích xuất các bản ghi đáp ứng các tiêu chuẩn nhất định hoặc tạo ra các trường tính toán từ các dữ liệu của đơn vị được kiểm toán.

Ứng dụng CAATs trong kiểm toán tài chính

- 17.28. Trong kiểm toán báo cáo tài chính CAATs được sử dụng để đảm bảo tính chính xác của các tài khoản bằng cách kiểm tra các giao dịch/bản ghi cấu thành. Khác với thủ tục kiểm toán thủ công, việc sử dụng CAATs sẽ cho phép kiểm toán viên thử nghiệm trên toàn bộ tập giao dịch/bản ghi và chọn mẫu dựa trên các phương pháp thống kê / phán đoán để kiểm tra chi tiết từng mẫu bằng các thủ tục thủ công.
- 17.29. Kiểm toán viên cũng có thể chọn mẫu giao dịch theo bất kỳ phương pháp dưới đây:

- (i) Phương pháp ngẫu nhiên (lấy mẫu ngẫu nhiên), khi mà mọi bản ghi / giao dịch đều có cơ hội bình đẳng để được lựa chọn;
 - (ii) Chọn tất cả các giao dịch thứ n (lấy mẫu theo khoảng), từ một vị trí bắt đầu ngẫu nhiên;
 - (iii) Phân chia toàn bộ giao dịch/tổng mẫu vào các tầng hoặc dải khác nhau, dựa trên giá trị và lựa chọn một số lượng giao dịch cụ thể từ mỗi tầng để kiểm tra chi tiết (lấy mẫu ngẫu nhiên);
 - (iv) Chọn các mẫu có giá trị cao (lấy mẫu theo đơn vị tiền tệ);
- 17.30. Các kỹ thuật chọn giao dịch có thể được chọn tự động, hoặc dựa trên giá trị lớn, hoặc các đặc điểm nghiệp vụ rủi ro cao hoặc chọn mẫu đại diện với sự trợ giúp của CAATs. Tham khảo thêm chi tiết ứng dụng CAATs trong kiểm toán BCTC ở phụ lục G.

Ứng dụng CAATs trong kiểm toán hoạt động

- 17.31. Trong kiểm toán hoạt động, CAATs có thể được ứng dụng trong để đánh giá hiệu quả các quy trình hoạt động trong đơn vị doanh nghiệp.

Ví dụ: Dưới đây nêu một số ví dụ thử nghiệm có thể thực hiện bằng CAATs đối với Hệ thống Quản lý nguyên vật liệu và Hàng tồn kho:

- *Kiểm tra thời gian để xử lý đơn đặt hàng*
- *Kiểm tra xem mẫu đơn mua hàng điện tử được điền và hoàn thiện đầy đủ không*
- *Kiểm tra xem đơn hàng có được đặt đúng hạn không?*
- *Kiểm tra tính toán chu kỳ mua hàng*
- *Phân chia lệnh mua hàng theo loại đơn hàng (ví dụ như khẩn cấp, gấp, và bình thường)*
- *Phân chia lệnh mua hàng phân chia theo hình thức thanh toán (ví dụ: tiền mặt, tín dụng, tạm ứng, thư tín dụng, và ngoại tệ)*
- *Xác định thời gian trễ giữa yêu cầu mua hàng và đơn đặt hàng*
- *Kiểm tra phê duyệt với các đơn hàng mua nằm ở ngưỡng phê duyệt*
- *Kiểm tra ngân sách khi thực hiện mua hàng*
- *Kiểm tra thông tin nhà cung cấp có được cập nhật*

- Kiểm tra trường hợp mã nhà cung cấp khác nhau nhưng địa chỉ giống nhau
- Kiểm tra các trường hợp có địa chỉ khác nhau nhưng mã nhà cung cấp giống nhau
- Xác minh xem có đặt nhiều đơn hàng cùng đặt cho một mặt hàng
- Kiểm tra trường hợp ngày đặt hàng trước ngày báo giá
- Kiểm tra các trường hợp báo giá của nhà thầu thắng thầu nhưng gửi sau ngày cuối cùng để nhận báo giá
- Xác minh số tiền đã thanh toán phù hợp với đơn đặt hàng đã được phê duyệt
- Kiểm tra hình thức thanh toán; Kiểm tra tất cả các trường hợp thanh toán bằng tiền mặt
- Kiểm tra những khoản tạm ứng đã trả được điều chỉnh theo giá cuối cùng
- Xác định các hạng mục không được thanh toán
- Kiểm tra sự trùng lặp của các lệnh mua hoặc thanh toán

17.32. Tùy thuộc vào dữ liệu, quy trình của các đầu mối kiểm toán, Kiểm toán viên nhà nước có thể đề ra các giả định khác nhau và tiến hành thực hiện kiểm toán bằng công cụ CAATs.

Ứng dụng CAATs trong kiểm toán tuân thủ

17.33. Ngày nay hệ thống CNTT thể hiện vai trò quan trọng trong hoạt động sản xuất kinh doanh của các doanh nghiệp/tổ chức và CAATs được các Kiểm toán viên nhà nước sử dụng một cách hiệu quả để điều tra các trường hợp gian lận.

Ví dụ: Dưới đây nêu một số ví dụ thử nghiệm có thể thực hiện bằng CAATs trong kiểm toán điều tra:

- Xác định người dùng có quyền truy cập vào hệ thống, xác định danh sách người dùng trái phép và các giao dịch do họ khởi tạo
- Xác định các giao dịch thu /chuyển tiền trái phép
- Phát hiện các thay đổi trái phép đối với các bảng / tệp / dữ liệu do các nhân viên trong Phòng CNTT / Tài chính / Quản trị cơ sở dữ liệu và hệ thống

- *Xác định các giao dịch được thực hiện ngoài giờ làm việc*
- *Kiểm tra các yêu cầu chi trả bảo hiểm sức khỏe cho nhân viên với giá trị lớn*
- *Xác định các khoản vay vượt quá giá trị thế chấp*
- *Kiểm tra các trường hợp có giao dịch trong các tài khoản không hoạt động*
- *Kiểm tra hóa đơn có ngày trước ngày đặt mua hàng*
- *Các khoản thanh toán cá nhân lớn*
- *Kiểm tra các khoản thanh toán cho các nhà cung cấp không có trong cơ sở dữ liệu nhà cung cấp*
- *Kiểm tra tất cả các tài khoản dư âm*
- *Kiểm tra những khoản tiền bất thường trong các khoản phải thu*

e. Lưu ý trong xử lý và chuẩn hóa dữ liệu

17.34. Dữ liệu có thể được lưu trữ trong máy tính dưới các dạng sau: Hệ thống tệp dữ liệu phẳng (Flat File System); Hệ thống quản lý dữ liệu quan hệ (RDBMS); và các định dạng khác.

Hệ thống tệp dữ liệu phẳng

- 17.35. Dữ liệu được lưu trữ dưới dạng tệp văn bản đơn giản như ASCII hay RBCDIC. Những dữ liệu này có thể xem được bằng cách sử dụng các trình duyệt văn bản (ví dụ như Notepad của Microsoft).
- 17.36. Thông thường, trong một hệ thống tệp dữ liệu phẳng có rất nhiều file dữ liệu. Mỗi tệp chứa rất nhiều các yếu tố dữ liệu mà không có mối quan hệ tiềm tàng nào và để tạo ra các mối quan hệ đó thì cần phải tiến hành lập trình. Điều này dẫn đến việc dư thừa dữ liệu cũng như ảnh hưởng tới tính nhất quán của dữ liệu và gây lãng phí không gian bộ nhớ.
- 17.37. Tệp dữ liệu phẳng có thể được chia thành ba (3) loại: Dữ liệu có độ dài cố định; Dữ liệu có độ dài thay đổi; và Dữ liệu có dấu hiệu phân cách (Delimited Data). Một số phần mềm kiểm toán CAATs cung cấp chức năng tải và chuyển đổi từ hệ thống tệp dữ liệu phẳng thành định dạng mà Kiểm toán viên nhà nước có thể sử dụng để phân tích. Tuy nhiên quá trình này thường khá phức tạp và tốn thời gian.

Hệ thống quản lý dữ liệu quan hệ (RDBMS)

- 17.38. Ngày nay hầu hết các hệ thống CNTT đều sử dụng mô hình CSDL quan hệ để lưu trữ dữ liệu. Khi đó các dữ liệu được lưu trữ trong các bảng dữ liệu có quan hệ với nhau và giảm lượng dữ liệu dư thừa cũng như không gian bộ nhớ đáng kể. RDBMS sử dụng khóa chính (Primary Key) và khóa ngoại (Foreign Key) để xác định một cách duy nhất các bản ghi và giá trị trong một bảng cùng với một bảng quan hệ. Trong các hệ quản trị CSDL loại này, các truy vấn được xây dựng bằng ngôn ngữ SQL, cũng được sử dụng để thao tác và định nghĩa dữ liệu.
- 17.39. Hiện nay có rất nhiều các hệ quản trị cơ sở dữ liệu quan hệ do các hãng nổi tiếng cung cấp như Oracle, IBM, Microsoft, Sybase trong đó thông dụng nhất có thể kể đến Oracle. Để có thể tải dữ liệu từ một hệ quản trị cơ sở dữ liệu, Kiểm toán viên nhà nước cần phải có kiến thức về cơ sở dữ liệu quan hệ.

Các định dạng khác

- 17.40. Microsoft Access là một dạng lưu trữ dữ liệu có cấu trúc, nó có thể coi là một CSDL quan hệ nhưng không hỗ trợ mô hình client-server cũng như các tính năng bảo mật của một hệ quản trị CSDL quan hệ.

f. Các yêu cầu trước khi tải dữ liệu

- 17.42. Để có thể tải dữ liệu từ hệ thống của đơn vị được kiểm toán thì Kiểm toán viên nhà nước cần phải có sự cho phép chính thức. Căn cứ vào đó, bộ phận CNTT của đơn vị sẽ tạo một tài khoản (user account) trên hệ thống với quyền “Đọc” (read-only) để Kiểm toán viên nhà nước thực hiện xuất dữ liệu.
- 17.43. Việc tải dữ liệu có thể thực hiện qua các cách sau:
- (i) Sử dụng các thiết bị lưu trữ như CD-ROM, USB hoặc ổ cứng ngoài.
 - (ii) Truy cập vào mạng nội bộ của đơn vị (cần được cấp quyền bởi bộ phận CNTT đơn vị) và thiết lập đường kết nối ODBC.
- 17.44. Kiểm toán viên nhà nước cần thu thập các thông tin/chi tiết sau từ đơn vị để có thể tải được dữ liệu một cách chính xác và đầy đủ:
- (i) Chi tiết tệp, bảng dữ liệu dùng chung và bảng dữ liệu các giao dịch
 - (ii) Mối quan hệ giữa các tệp và bảng
 - (iii) Cấu trúc bản ghi (tên, mô tả, độ dài và loại)
 - (iv) Số lượng bản ghi trên mỗi tệp và bảng

- (v) Kích thước của tệp và bảng
- (vi) Định dạng dữ liệu (với trường hợp là dữ liệu phẳng)
- (vii) Phương thức chuyển dữ liệu
- (viii) Các tệp liên quan và các mối quan hệ logic nếu có giữa các trường dữ liệu.
- (ix) Kiểm soát số tổng của tệp dữ liệu chi tiết

Phần II - HƯỚNG DẪN KIỂM TOÁN CHI TIẾT

A. HƯỚNG DẪN CHI TIẾT KIỂM TOÁN HỆ THỐNG CÔNG NGHỆ THÔNG TIN

1. Tóm tắt và cách sử dụng các hướng dẫn chi tiết

a. Bố cục hướng dẫn

Hướng dẫn chi tiết kiểm toán hệ thống CNTT gồm 8 chuyên đề:

- Chuyên đề 2: Hướng dẫn cách sử dụng bảng câu hỏi mẫu phục vụ việc đánh giá rủi ro sơ bộ hệ thống CNTT;
- Từ Chuyên đề 3 (A1) đến Chuyên đề 8 (A6): Trình bày các chương trình kiểm toán mẫu của 6 chuyên đề liên quan đến các kiểm soát chung CNTT;
- Chuyên đề 9 (A7): Trình bày các chương trình kiểm toán mẫu của chuyên đề liên quan đến các kiểm soát ứng dụng CNTT.

b. Cách áp dụng trong thực tế

Các cuộc kiểm toán CNTT độc lập hoặc kiểm toán trong môi trường CNTT nên thực hiện nội dung kiểm toán Chuyên đề A1 - Quản trị CNTT ngay trong giai đoạn khảo sát. Để thực hiện việc kiểm toán công tác quản trị CNTT cần tham khảo:

- Bảng câu hỏi mẫu gửi cho đơn vị trình bày ở chuyên đề 2;

Các cuộc kiểm toán hệ thống CNTT tùy theo mục đích của cuộc kiểm toán, kết quả đánh giá rủi ro và xác định trọng yếu mà áp dụng toàn bộ hoặc một số chương trình kiểm toán mẫu theo từng vấn đề kiểm toán trình bày ở các chuyên đề từ A1 đến A7.

Các cuộc kiểm toán trong môi trường CNTT nên tập trung vào kiểm soát CNTT liên quan đến các phần mềm nghiệp vụ trọng yếu hoặc hệ thống thông tin liên quan đến báo cáo tài chính của đơn vị được kiểm toán. Các nội dung kiểm toán chi tiết là:

- Các chương trình kiểm toán mẫu ở phần Chuyên đề A7 - Kiểm soát ứng dụng CNTT.
- Một số chương trình kiểm toán mẫu ở các chuyên đề kiểm soát chung (từ A1 đến A7) như kiểm soát truy cập, kiểm soát lưu vết, kiểm soát dữ liệu sao lưu, kiểm soát sự thay đổi nghiệp vụ bằng phần mềm ...
- Các kỹ thuật thử nghiệm sử dụng CAATs trình bày ở Hướng dẫn C.

2. Bảng câu hỏi mẫu đánh giá rủi ro sơ bộ hệ thống CNTT

Việc cung cấp bảng câu hỏi đánh giá sơ bộ hệ thống CNTT của đơn vị thực hiện ngay trong khâu khảo sát hoặc lập kế hoạch kiểm toán năm. Đây là thủ tục kiểm toán đánh giá sơ bộ các rủi ro trên từng lĩnh vực của các hệ thống CNTT dự kiến sẽ tiến hành kiểm toán.

a. Nguyên tắc xây dựng, chấm điểm

Hệ số điểm

Là trọng số quan trọng của từng câu hỏi (Câu hỏi càng quan trọng thì trọng số càng cao). Tùy thuộc vào mục tiêu và chủ đề trọng điểm của cuộc kiểm toán mà quyết định hệ số điểm của từng câu hỏi trong bảng theo mức độ liên quan. Việc phân bổ hệ số điểm cho các câu hỏi có thể tham khảo các đơn vị liên quan trong trường hợp cần thiết. Nếu hệ số điểm không được xác định, KTNN có thể xác định hệ số điểm bằng nhau (bảng 1) cho tất cả câu hỏi.

Thang điểm

Thang điểm từ 1-5 (điểm 1 thể hiện rủi ro thấp nhất và điểm 5 thể hiện rủi ro cao nhất). Tại bảng câu hỏi mẫu tại tiểu mục 4.1.2, số liệu trong ngoặc đơn () là điểm số các câu trả lời của mỗi câu hỏi. Lưu ý rằng điểm số trong bảng chỉ là gợi ý, tùy thuộc vào từng cuộc kiểm toán, KTNN có thể cho điểm các câu trả lời khác với số điểm trong bảng. Cột “Điểm số” thể hiện số điểm cuối cùng của câu trả lời, được tính bằng hệ số điểm nhân (x) với điểm số của từng câu trả lời (số điểm trong ngoặc đơn).

b. Xây dựng, gửi bảng câu hỏi và kết quả cho đơn vị

Các câu hỏi mẫu trong bảng có thể chưa phản ánh toàn diện hết mọi khía cạnh của các cuộc kiểm toán. KTNN có thể sử dụng hệ thống câu hỏi trong bảng câu hỏi hoặc phát triển các câu hỏi khác tùy theo yêu cầu của từng cuộc kiểm toán.

Các thông tin trong bảng câu hỏi phải được thu thập cho tất cả các đơn vị nằm trong đối tượng được chọn cho kế hoạch kiểm toán năm hoặc cuộc kiểm toán.

Ví dụ: Khi kế hoạch năm dự kiến có cuộc kiểm toán các hệ thống dịch vụ công cấp độ 4 của các Bộ Ngành thì câu hỏi sẽ được gửi cho tất cả Bộ Ngành để phục vụ cho việc đánh giá sơ bộ và chọn mẫu; Khi cuộc kiểm toán lại chỉ hướng đến các phần mềm tính tiền lương một số đơn vị trên địa bàn Tỉnh X, thì bảng câu hỏi sẽ gửi đến tất cả các đơn vị trên địa bàn tỉnh X. Thông tin nên được thu thập càng nhiều càng tốt để chấm điểm và thực hiện các so sánh có liên quan.

Việc cho điểm và xếp hạng có thể được giữ bí mật hay chia sẻ với các bên liên quan tùy theo chính sách của Kiểm toán nhà nước.

c. Bảng câu hỏi mẫu

STT	Tiêu chí	Hệ số điểm	Điểm số
I. Quản trị công nghệ thông tin			
1	Tình trạng chung về công tác tin học hóa trong đơn vị. Đơn vị đã được tin học hóa:		
	<i>Tất cả các quy trình kinh doanh (5)</i>		
	<i>Hầu hết các quy trình kinh doanh (4)</i>		
	<i>Chỉ có một vài quy trình (3)</i>		
	<i>Không có quy trình nào (1)</i>		
2	Đơn vị có một hệ thống CNTT và các chính sách liên quan		
	<i>Có (1)</i>		
	<i>Một phần (3)</i>		
	<i>Không (5)</i>		
3	Đơn vị:		
	<i>Có bộ phận CNTT riêng biệt để thực hiện tất cả các nhiệm vụ CNTT(2)</i>		
	<i>Thuê ngoài để thực hiện một số chức năng CNTT (5)</i>		
	<i>Đã thuê ngoài các thiết bị, phương tiện CNTT (5)</i>		

STT	Tiêu chí	Hệ số điểm	Điểm số
4	Đơn vị có một:		
	<i>Giám đốc thông tin có trách nhiệm về các hoạt động liên quan đến CNTT (1)</i>		
	<i>Đơn vị đã có nhân viên cấp cao đầy đủ trách nhiệm về các hoạt động liên quan đến CNTT (3)</i>		
	<i>Đơn vị đã có nhân viên cấp dưới chịu trách nhiệm về các hoạt động liên quan đến CNTT (3)</i>		
	<i>Đơn vị chưa có nhân viên được giao nhiệm vụ giám sát các hoạt động CNTT (5)</i>		
II. Phát triển, mua sắm và thuê ngoài sản phẩm CNTT			
5	Hệ thống CNTT đã được phát triển		
	<i>Bởi chính nội bộ của đơn vị với đầy đủ khả năng chuyên môn và kỹ thuật (1)</i>		
	<i>Bởi nội bộ của đơn vị nhưng khả năng chuyên môn và kỹ thuật chưa đầy đủ (5)</i>		
	<i>Bằng một nhà thầu hoặc tổ chức chính phủ khác (1)</i>		
	<i>Pha trộn cả hệ thống nội bộ và thuê ngoài (5)</i>		
6	Việc mua sắm đã được thực hiện		
	<i>Đơn vị đã tự thực hiện việc mua sắm hệ thống CNTT bằng chính khả năng đầy đủ của mình (3)</i>		
	<i>Đơn vị đã thực hiện việc mua sắm hệ thống CNTT bằng việc sử dụng khả năng của hệ thống nội bộ và cả việc sử dụng dịch vụ tư vấn (5)</i>		
	<i>Bằng việc sử dụng dịch vụ tư vấn (4)</i>		
7	Hệ thống tài liệu liên quan đến hệ thống CNTT		
	<i>Sẵn có (1)</i>		
	<i>Sẵn có một phần (3)</i>		
	<i>Không sẵn có (5)</i>		

STT	Tiêu chí	Hệ số điểm	Điểm số
8	Việc cập nhật thông tin và bảo hành		
	<i>Được thực hiện nhiều hơn 5 lần trong một năm (5)</i>		
	<i>Được thực hiện ít hơn 5 lần và nhiều hơn 2 lần trong một năm (3)</i>		
	<i>Được thực hiện ít hơn 2 lần trong một năm (2)</i>		
	<i>Thậm chí không được thực hiện 1 lần trong một năm (1)</i>		
III. Hoạt động hệ thống CNTT và bảo đảm vận hành hệ thống CNTT			
9	Số các điểm truy cập/địa điểm giao dịch/người sử dụng		
	<i>Nhiều hơn Y (5)</i>		
	<i>Nhiều hơn X, ít hơn Y (3)</i>		
	<i>Ít hơn X (1)</i>		
	<i>(Số X và Y được quyết định bởi KTNN, KTNN cũng có thể đặt ra nhiều mức X, Y, Z,... nếu cần thiết)</i>		
10	Mạng sử dụng của hệ thống CNTT		
	<i>Không có mạng (1)</i>		
	<i>Mạng nội bộ (LAN) (3)</i>		
	<i>Mạng diện rộng (WAN) (4)</i>		
	<i>Mạng internet (5)</i>		
11	Số lượng các vị trí (đơn vị con) triển khai hệ thống CNTT		
	<i>Chỉ có một vị trí (1)</i>		
	<i>Nhiều hơn 1 và ít hơn X vị trí (3)</i>		
	<i>Nhiều hơn X vị trí (5)</i>		
	<i>(Số X và Y được quyết định bởi KTNN, KTNN cũng có thể đặt ra nhiều mức X, Y, Z,... nếu cần thiết)</i>		
12	Hệ thống có được kết nối trực tiếp với các bên thứ 3		
	<i>Có (5)</i>		
	<i>Không (1)</i>		
13	Số các người sử dụng cuối cùng của hệ thống CNTT		

STT	Tiêu chí	Hệ số điểm	Điểm số
	<i>Ít hơn X (1)</i>		
	<i>Nhiều hơn X, ít hơn Y (3)</i>		
	<i>Nhiều hơn Y (5)</i>		
	(Số X và Y được quyết định bởi KTNN, KTNN cũng có thể đặt ra nhiều mức X, Y, Z,... nếu cần thiết)		
14	Đơn vị đang duy trì các dữ liệu và ứng dụng:		
	<i>Bằng năng lực nội bộ (1)</i>		
	<i>Một phần dựa vào năng lực nội bộ và một phần dựa vào phương tiện bên ngoài (3)</i>		
	<i>Máy chủ ở thiết bị thuê ngoài (5)</i>		
15	Hệ thống CNTT đã được hoạt động		
	<i>Nhiều hơn 10 năm (1)</i>		
	<i>Từ 5 đến 10 năm</i>		
	<i>Từ 2 đến 5 năm</i>		
	<i>Ít hơn 2 năm (5)</i>		
16	Khối lượng dữ liệu trong hệ thống CNTT (bao gồm cả dữ liệu lưu vết nghiệp vụ) xấp xỉ:		
	<i>Nhiều hơn 10 GB (5)</i>		
	<i>Từ 2 GB đến 10 GB</i>		
	<i>Ít hơn 2 GB (1)</i>		
IV. Về tài chính			
17	Vốn đã đầu tư vào hệ thống CNTT		
	<i>Lớn hơn Y (5)</i>		
	<i>Nhiều hơn X, ít hơn Y (3)</i>		
	<i>Dưới mức X (1)</i>		
	(Số X và Y được quyết định bởi KTNN, KTNN cũng có thể đặt ra nhiều mức X, Y, Z,... nếu cần thiết)		
18	Phương thức huy động vốn		

STT	Tiêu chí	Hệ số điểm	Điểm số
	<i>Từ nguồn lực nội bộ (3)</i>		
	<i>Vay từ bên ngoài (4)</i>		
	<i>Vay từ các tổ chức quốc tế (5)</i>		
19	Chi phí định kỳ của hệ thống CNTT		
	<i>Trên mức Y (5)</i>		
	<i>Nhiều hơn X, ít hơn Y (và những mức như vậy, nếu cần) (3)</i>		
	<i>Dưới mức X (1)</i>		
	(Số X và Y được quyết định bởi KTNN, KTNN cũng có thể đặt ra nhiều mức X, Y, Z,... nếu cần thiết)		
V. Việc thực hiện các chức năng/tính hữu dụng của hệ thống			
20	Hệ thống đã được sử dụng cho		
	<i>Chỉ các quy trình nội bộ (3)</i>		
	<i>Chỉ các quy trình bên ngoài (4)</i>		
	<i>Dùng cả cho các quy trình nội bộ và bên ngoài (5)</i>		
21	Hệ thống có cung cấp dịch vụ cho công dân?		
	<i>Có (5)</i>		
	<i>Không (3)</i>		
VI. Kiểm soát, kiểm toán nội bộ và dịch vụ bảo đảm chất lượng			
22	Có một chứng nhận của bên thứ 3 đối với hệ thống		
	<i>Có (1)</i>		
	<i>Không (5)</i>		
23	Hệ thống CNTT đã được kiểm toán bởi cuộc kiểm toán CNTT của KTNN		
	<i>03 năm trước (2)</i>		
	<i>05 năm trước (4)</i>		
	<i>Chưa bao giờ (5)</i>		
24	Đã có cuộc kiểm toán khác (tài chính/tuân thủ/hoạt động) đã thực hiện các quan sát có liên quan đến hệ thống CNTT		

STT	Tiêu chí	Hệ số điểm	Điểm số
	<i>Đã có một số quan sát kiểm toán đã được thực hiện (5)</i>		
	<i>Chỉ rất ít quan sát kiểm toán được thực hiện trước đây (3)</i>		
	<i>Chưa có quan sát kiểm toán nào được thực hiện (1)</i>		
	TỔNG SỐ ĐIỂM		

d. Đánh giá rủi ro sơ bộ hệ thống CNTT

Phân loại rủi ro	Phạm vi của tổng số điểm
A	L1-L2
B	>L2 và <L3
C	>L3 và <L4
D	> L4

Ghi chú: L1, L2, L3, L4 là phạm vi điểm trong phân loại rủi ro và được quyết định bởi KTNN.

Sau khi hoàn thành Bảng câu hỏi đánh giá rủi ro nêu trên, Kiểm toán viên Nhà nước có thể sử dụng bảng dưới đây để tổng kết đánh giá về hệ thống CNTT và Bảng phân loại rủi ro nêu trên để phân loại rủi ro của hệ thống CNTT các đơn vị.

Tên của hệ thống	Tổng điểm	Phân loại rủi ro	Xếp hạng thứ tự ưu tiên
...			
...			

3. Chuyên đề A1 - Quản trị Công nghệ thông tin

a. Giới thiệu việc quản trị CNTT

Khái niệm

Quản trị CNTT là nền tảng hướng dẫn mọi hoạt động CNTT của đơn vị nhằm đảm bảo cho sự đáp ứng các nhu cầu hoạt động trong hiện tại cũng như cho kế hoạch phát triển lâu dài của đơn vị. Quản trị CNTT là bộ phận không thể thiếu trong công tác quản trị chung, liên quan đến sự lãnh đạo đơn vị, cấu trúc tổ chức cũng như các quy trình và các hoạt động khác (báo cáo và phản hồi, củng cố và quản lý nguồn lực , ...)

nhằm đảm bảo hệ thống CNTT duy trì được các mục tiêu và chiến lược của tổ chức đồng thời cân đối giữa rủi ro và quản lý nguồn lực hiệu quả.

Vai trò và vị trí của quản trị CNTT

Quản trị CNTT đóng vai trò quan trọng trong việc định nghĩa môi trường kiểm soát, đặt nền tảng cho việc triển khai thực hành kiểm soát nội bộ chặt chẽ, chính xác, hiệu quả đồng thời giúp ban quản lý có cái nhìn toàn diện thông qua việc báo cáo các cấp chức năng.

Quản trị CNTT là một phần không thể thiếu trong quản trị doanh nghiệp/tổ chức. Quản trị CNTT cần được xem xét như là phương thức CNTT tạo ra các giá trị phù hợp với chiến lược quản trị tổng quát của tổ chức. Do đó, các bộ phận, ban ngành của đơn vị cần phối hợp và tham gia trong quá trình đưa ra các quyết định liên quan tới quản trị CNTT. Điều này đảm bảo việc tạo ra những cam kết trách nhiệm chung của cả đơn vị đối với các hệ thống CNTT trọng yếu và đảm bảo các quyết định liên quan tới CNTT xuất phát từ nhu cầu thực tế của đơn vị chứ không phải ngược lại.

Quản trị CNTT đảm bảo những quyết định đầu tư cho CNTT sẽ đem đến những lợi ích trong hoạt động, giảm thiểu các rủi ro gắn với CNTT. Trong công tác quản trị CNTT, đơn vị cần xây dựng cấu trúc tổ chức với các thứ bậc được định nghĩa rõ ràng nhằm phân định rõ trách nhiệm đối với thông tin, quy trình, ứng dụng và cơ sở hạ tầng CNTT đang được sử dụng.

Quản trị CNTT phải tham gia vào việc phát hiện và cập nhật các nhu cầu hoạt động, cung cấp các giải pháp CNTT cho người dùng. Trong quá trình phát triển và mua sắm giải pháp, quản trị CNTT đảm bảo giải pháp được chọn phù hợp với hoạt động, và các nguồn lực (phần cứng, công cụ, mạng lưới, khả năng đáp ứng v.v...) và các đào tạo cần thiết để triển khai giải pháp.

Hoạt động giám sát liên quan đến công tác quản trị CNTT cần được thực hiện bởi các bộ phận kiểm soát nội bộ (hoặc bộ phận đảm bảo chất lượng) thông qua việc báo cáo định kỳ kết quả giám sát lên các cấp quản lý.

Hiện nay, có nhiều bộ khung và chuẩn mực khác nhau về quản trị CNTT để đơn vị có thể chọn lựa triển khai.

b. Rủi ro thường gặp

Kiểm toán viên nhà nước cần am hiểu và đánh giá được các thành phần khác nhau trong cấu trúc quản trị CNTT để có thể xác minh các quyết định, phương hướng, nguồn lực, quản lý và giám sát về CNTT đóng góp cho chiến lược phát triển và mục tiêu của đơn vị.

Để đánh giá chính xác, Kiểm toán viên nhà nước cần tìm hiểu kỹ các thành phần trọng yếu của công tác quản trị và quản lý CNTT. Kiểm toán viên nhà nước cần nhận thức được những rủi ro sẽ phát sinh do thành phần nào đó của công tác quản trị đang bị thiếu sót hoặc thực hiện chưa chính xác...

Mỗi đơn vị đều phải đối mặt với những thách thức riêng do khác nhau về mặt môi trường, chính trị, địa lý, kinh tế và xã hội. Một số rủi ro phổ biến và hậu quả của việc thiếu Quản trị CNTT như sau:

Hệ thống CNTT không hữu hiệu, kém hiệu quả hoặc không thân thiện với người dùng

Các hệ thống CNTT quản lý phục vụ xã hội, doanh nghiệp hoặc tăng cường khả năng vận hành của các cơ quan chính phủ thường rất đa dạng và khá phức tạp. Do đó, các hệ thống trên phải được thiết kế đúng, tinh chỉnh phù hợp với nhu cầu thực tế, phối hợp nhiều bộ phận và được vận hành hữu hiệu.

Quản trị CNTT kém ở các tổ chức chính phủ và doanh nghiệp là trở ngại đầu tiên để có hệ thống CNTT đạt chất lượng tốt.

Hệ thống CNTT thiếu định hướng, không bám sát yêu cầu nghiệp vụ

Việc đầu tư lớn CNTT không phù hợp với mục tiêu và nguồn lực của tổ chức có thể không mang lại hoặc mang lại rất ít giá trị hoạt động. Ngay cả khi triển khai hệ thống CNTT tốt nhưng thiếu định hướng rõ ràng cũng sẽ không đóng góp hiệu quả và hữu hiệu giúp đạt được các mục tiêu chung của tổ chức.

Nhằm đảm bảo mối tương quan giữa việc đầu tư CNTT với nguồn lực và mục tiêu của đơn vị, cần có sự phối hợp chặt chẽ giữa các bên liên quan và nhóm người dùng am hiểu về hoạt động của đơn vị trước khi đưa ra các quyết định đầu tư CNTT.

Kìm hãm sự phát triển của đơn vị

Công tác lập kế hoạch CNTT không được thực hiện hoặc thực hiện không đầy đủ sẽ dẫn đến sự phát triển kinh doanh bị kìm hãm do thiếu nguồn lực CNTT hoặc sử dụng không hiệu quả các nguồn lực hiện có. Để giảm thiểu rủi ro trên, đơn vị phải cập nhật

chiến lược CNTT định kỳ, nhằm xác định các nguồn lực và kế hoạch hợp lý cho nhu cầu phát triển trong tương lai.

Quản lý nguồn lực CNTT không hiệu quả

Để đạt được kết quả tối ưu với chi phí thấp nhất, đơn vị cần quản lý các nguồn lực CNTT một cách hiệu quả và hữu hiệu. Đơn vị phải đảm bảo đầy đủ các nguồn lực về kỹ thuật, phần cứng, phần mềm và quan trọng nhất là việc có đầy đủ nhân sự để cung cấp các dịch vụ CNTT. Đây là nhân tố then chốt để đạt được hiệu quả trong việc đầu tư CNTT. Hoạch định và giám sát việc sử dụng các nguồn lực CNTT (Ví dụ: các nguồn lực trong một thỏa thuận dịch vụ) sẽ giúp đơn vị dễ dàng nhận ra việc đáp ứng về nguồn lực là phù hợp hay chưa, có đáp ứng được cho nhu cầu nghiệp vụ hay không.

Ra quyết định không phù hợp

Hệ thống báo cáo nghèo nàn có thể dẫn tới các quyết định không phù hợp, thiếu chính xác. Điều này ảnh hưởng tới khả năng cung cấp dịch vụ cũng như ngăn cản việc đáp ứng các nhiệm vụ của đơn vị. Ban lãnh đạo và các ban khác của đơn vị (ban quản lý, ban kiểm soát v.v...) tham gia vào công tác quản trị CNTT sẽ hỗ trợ việc ra quyết định hiệu quả hơn.

Các dự án CNTT thất bại

Nhiều đơn vị không thành công trong việc đánh giá tầm quan trọng của quản trị CNTT. Việc đảm nhận triển khai các dự án CNTT mà không có sự hiểu biết đầy đủ về yêu cầu của đơn vị đối với dự án cũng như mối liên hệ giữa dự án và mục tiêu của đơn vị sẽ dẫn tới việc các dự án CNTT dễ dàng bị thất bại.

Đó cũng là nguyên nhân thất bại phổ biến khi mua mới hoặc phát triển các phần mềm ứng dụng không đáp ứng được các tiêu chuẩn tối thiểu về an ninh và kiến trúc. Các dự án này sẽ làm phát sinh thêm chi phí để duy trì cũng như quản lý các hệ thống và phần mềm ứng dụng không được phát triển theo tiêu chuẩn chất lượng. Để khắc phục rủi ro trên, đơn vị cần thiết lập “Chu trình phát triển phần mềm” (SDLC) và nghiêm túc thực hiện quy trình trên trong việc triển khai các dự án CNTT nhằm đảm bảo chất lượng sản phẩm đầu ra.

Phụ thuộc vào bên thứ 3

Việc không có quy trình kiểm soát việc mua sắm và thuê khoán có thể khiến đơn vị đối mặt với tình huống phụ thuộc hoàn toàn vào một nhà cung cấp. Đây là rủi ro cao

vì tổ chức sẽ gặp rất nhiều khó khăn nếu nhà cung cấp rời khỏi thị trường hoặc không cung cấp các dịch vụ được ký hợp đồng. Ngoài ra, còn có thể phát sinh những vấn đề khác như: tranh chấp về sở hữu trí tuệ, hệ thống và CSDL.

Vì vậy, cần xây dựng một chính sách thuê khoán hay mua sắm rõ ràng nhằm xác định những gì có thể hoặc không thể thuê ngoài.

Thiếu tính minh bạch và trách nhiệm giải trình

Minh bạch cùng trách nhiệm giải trình là hai yếu tố quan trọng trong công tác quản trị. Minh bạch là công cụ hiệu quả, đặc biệt khi áp dụng nhất quán sẽ giúp đơn vị chống lại hiện tượng tham nhũng, tăng cường công tác quản trị và nâng cao trách nhiệm giải trình. Vì vậy, trong trường hợp cơ cấu tổ chức, chiến lược, thủ tục CNTT cũng như việc kiểm soát giám sát không được tổ chức một cách hợp lý sẽ dẫn đến sự thiếu minh bạch và trách nhiệm giải trình.

Không tuân thủ các nội quy, quy định và văn bản pháp luật

Các bên liên quan thường yêu cầu đơn vị đảm bảo việc tuân thủ luật pháp và các quy định chung phù hợp với thực tiễn quản trị doanh nghiệp trong môi trường hoạt động kinh doanh. Ngoài ra, CNTT đã tạo ra các quy trình kinh doanh liên tục giữa các doanh nghiệp. Do vậy, nhu cầu về việc đảm bảo trong các hợp đồng cần được những nội dung liên quan đến CNTT như tính riêng tư, bảo mật, sở hữu trí tuệ và ATTT cần phải được nghiêm chỉnh chấp hành. Các chính sách khác nhau về an toàn bảo mật thông tin, thuê khoán bên ngoài, nhân sự, phải phù hợp với hệ thống luật pháp và các quy định nội bộ, ban, ngành.

Đối mặt với các rủi ro về ATTT

Rất nhiều rủi ro về ATTT có thể gia tăng do thiếu những bộ phận chuyên trách, quy trình và chính sách, ví dụ như: chiếm đoạt tài sản, tiết lộ trái phép thông tin, truy cập trái phép, hệ thống bị tấn công (vật lý và logic), gián đoạn và không có thông tin, sử dụng thông tin sai mục đích, không tuân thủ pháp luật và các quy định về dữ liệu cá nhân, không phục hồi được dữ liệu sau các thảm họa. Chính sách về ATTT phải định nghĩa các tài sản CNTT (dữ liệu, dụng cụ, quy trình) cần được bảo vệ cùng các thủ tục, công cụ cũng như các biện pháp bảo vệ các tài sản trên.

Quản trị CNTT tiếp tục là vấn đề được quan tâm nhất trong các cơ quan công quyền vì đó là gốc rễ của nhiều vấn đề, Vì vậy nên đảm bảo nội dung kiểm toán công tác quản trị CNTT cần được thực hiện trong các cuộc kiểm toán CNTT.

c. Các vấn đề kiểm toán thành phần

Công tác quản trị CNTT của đơn vị được đánh giá thông qua việc kiểm toán các vấn đề kiểm toán sau:

- Vấn đề kiểm toán A1.01 - Xác định, định hướng và giám sát nhu cầu liên quan đến CNTT nhằm kiểm tra các yêu cầu liên quan đến CNTT có bám sát, xuất phát từ các yêu cầu nghiệp vụ của đơn vị.
- Vấn đề kiểm toán A1.02 - Lập, triển khai kế hoạch chiến lược CNTT nhằm đánh giá kiểm tra công tác triển khai ứng dụng CNTT một cách có được thực hiện một cách hệ thống, có theo chiến lược, và bám sát các định hướng phục vụ các hoạt động nghiệp vụ, cũng như có phương án đối phó với các rủi ro.
- Vấn đề kiểm toán A10300 - Cơ cấu tổ chức, chính sách và thủ tục liên quan đến CNTT nhằm đánh giá sự phù hợp của các yếu tố trên trong việc giữ vai trò nền tảng triển khai cho mọi hoạt động CNTT của đơn vị.
- Vấn đề kiểm toán A10400 - Xây dựng và phát triển đội ngũ nhân sự CNTT nhằm đánh giá việc đội ngũ nhân sự CNTT có thực sự vận hành được hệ thống CNTT và có nguồn lực cần thiết cho việc đào tạo nhân sự CNTT.
- Vấn đề kiểm toán A10500 -Đảm bảo sự tuân thủ chính sách và thủ tục CNTT nhằm kiểm tra hệ thống chính sách cùng thủ tục CNTT được thực hiện nghiêm túc trong thực tế thông qua một cơ chế đảm bảo hữu hiệu.

d. Chương trình kiểm toán mẫu

Vấn đề A1.01 - Xác định, định hướng và giám sát nhu cầu CNTT

Mục tiêu kiểm toán:

Đánh giá xem lãnh đạo của đơn vị có chỉ đạo, đánh giá và quản lý việc ứng dụng CNTT một cách hiệu quả để hoàn thành mục tiêu của đơn vị hay không

Kiểm soát A1.01.01 - Cách thức xác định và phê duyệt nhu cầu CNTT phù hợp

Tiêu chí kiểm toán

Đảm bảo đơn vị có kế hoạch trong việc xác định các nhu cầu CNTT và ban lãnh đạo có đầy đủ thông tin để ra quyết định phê duyệt các dự án CNTT.

Tài liệu yêu cầu

- Quy trình quản lý các dự án CNTT
- Điều lệ và nguyên tắc phê chuẩn: các ngưỡng chấp nhận và từ chối các yêu cầu liên quan đến CNTT.
- Danh sách các dự án CNTT được phê duyệt và từ chối.

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo CNTT của đơn vị về quy trình quản lý các nhu cầu CNTT, xác minh xem đơn vị có chính sách cụ thể nào liên quan tới quản lý các dự án CNTT hay không.
- Rà soát quy trình quản lý các dự án CNTT, đánh giá mức độ phù hợp về điều lệ và nguyên tắc phê chuẩn: các ngưỡng chấp nhận và từ chối các dự án liên quan đến hoạt động CNTT.
- Quy trình thu thập nhu cầu CNTT được lập thành văn bản, được phê duyệt bởi lãnh đạo.
- Phòng văn người quản lý và những người có trách nhiệm khác đối với việc phê duyệt các dự án CNTT để đảm bảo họ đã xem xét năng lực, kỹ năng, nguồn lực của đơn vị cũng như khả năng những người sử dụng có thể phát huy vai trò của họ thông qua việc sử dụng các công cụ, phương pháp và các thủ tục mới ứng dụng CNTT.
- Thu thập bằng chứng dự án CNTT được phê duyệt.

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách các dự án được thông qua và từ chối, Kiểm toán viên nhà nước tiến hành lấy mẫu và xác minh các vấn đề sau:

- Đảm bảo dự án mới của đơn vị được xác định và đánh giá theo quy trình quản lý các dự án CNTT của đơn vị.
- Đảm bảo việc phê duyệt hoặc từ chối các dự án CNTT là theo các điều lệ và nguyên tắc phê chuẩn của đơn vị, thông qua các ngưỡng chấp nhận và từ chối các yêu cầu liên quan đến hoạt động CNTT.

Kiểm soát A1.01.02 - Chỉ đạo, định hướng và giám sát hiệu quả các mục tiêu CNTT

Tiêu chí kiểm toán

Đảm bảo đơn vị có thiết lập các chỉ số để đánh giá mức độ hiệu quả của các mục tiêu CNTT; ban chỉ đạo hoặc các cấp tương đương tiến hành họp và rà soát định kỳ và

ra những quyết định chỉ đạo phù hợp hoặc đơn vị có một hệ thống báo cáo định kỳ lên các cấp lãnh đạo về hiện trạng của các chỉ số đo lường mức độ hiệu quả các mục tiêu CNTT đã đề ra.

Tài liệu yêu cầu

- Các chỉ số đánh giá mức độ hiệu quả của đơn vị và các mục tiêu CNTT
- Báo cáo định kỳ về tình trạng của dự án
- Biên bản họp rà soát định kỳ
- Danh sách các hoạt động cần thực hiện và tình trạng các hoạt động đó

Đánh giá thiết kế và triển khai

▪ Phòng văn lãnh đạo CNTT của đơn vị về cách thức quản lý và các chỉ số đo lường mức độ hiệu quả của các mục tiêu CNTT mà đơn vị đang sử dụng. Thu thập các văn bản, chính sách quy định các chỉ số đo lường mức độ hiệu quả tối thiểu cần phải có cho một lĩnh vực. Ví dụ, báo cáo về tình trạng dự án cần có các chỉ số liên quan đến chi phí, tiến độ, khả năng đáp ứng việc bàn giao dự án đúng hạn.

▪ Phòng văn lãnh đạo CNTT của đơn vị về cách thức báo cáo mức độ hiệu quả các mục tiêu CNTT lên các cấp lãnh đạo, cách thức ban lãnh đạo đưa ra những ý kiến chỉ đạo cho các mục tiêu CNTT

▪ Thu thập các quy trình, cách thức báo cáo được lập thành văn bản và được lãnh đạo phê duyệt.

- Thu thập mẫu báo cáo.

Thử nghiệm hiệu quả hoạt động

Dựa trên biên bản họp hoặc báo cáo định kỳ, Kiểm toán viên nhà nước lấy mẫu và xác minh các vấn đề sau:

▪ Rà soát báo cáo đo lường mức độ hiệu quả để bảo đảm nó bao gồm tất cả các chỉ số theo quy định của đơn vị.

▪ Rà soát các quyết định chỉ đạo của ban lãnh đạo để bảo đảm nó rành mạch, có bằng chứng rõ ràng và không gây hiểu nhầm.

▪ Rà soát danh sách các chỉ đạo, các hoạt động cần thực hiện sau các buổi họp để đảm bảo chúng được phân công, hoàn thành và có những bài học kinh nghiệm

Kiểm soát A1.01.03 - Phương thức quản lý các dự án đầu tư CNTT thích hợp và hiệu quả

Tiêu chí kiểm toán

Các dự án đầu tư CNTT của đơn vị được quản lý một cách thích hợp và hiệu quả

Tài liệu yêu cầu

- Quy trình và kế hoạch quản lý các dự án đầu tư CNTT
- Danh sách các dự án đầu tư CNTT
- Bản mẫu phân tích chi phí – lợi nhuận
- Danh sách các dự án CNTT được phê duyệt, từ chối hoặc trì hoãn
- Báo cáo tình trạng dự án của các dự án được phê duyệt
- Bản mẫu báo cáo đánh giá dự án sau triển khai

Đánh giá thiết kế và triển khai

▪ Phòng vận lãnh đạo CNTT của đơn vị về phương thức đơn vị quản lý các dự án đầu tư CNTT. Thu thập các chính sách liên quan về quy trình quản lý các dự án đầu tư CNTT

▪ Rà soát danh sách các dự án đầu tư CNTT để xác minh xem chúng đã được ưu tiên theo các tiêu chí được phê duyệt hay chưa

▪ Phòng vận lãnh đạo CNTT của đơn vị để xác minh xem tổ chức ra quyết định cho việc xây dựng hoặc mua mới như thế nào (ví dụ như dựa trên khả năng của đơn vị, các kỹ năng hiện có, chi phí, rủi ro...)

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách các dự án CNTT, Kiểm toán viên nhà nước chọn mẫu và xác minh các vấn đề sau:

- Rà soát bản phân tích chi phí
- Lợi nhuận để bảo đảm chúng đã được hoàn thành, phản ánh đúng tình trạng của dự án, không khuếch trương lợi nhuận cũng như không đánh giá thấp chi phí hoặc tiến độ dự án
- Đối với dự án đang gặp khó khăn, xác định xem liệu phương pháp luận triển khai dự án có phù hợp với loại hình dự án đó không, và liệu rằng đội ngũ quản lý chất lượng có tham gia vào quá trình quản lý dự án hay không

- Phỏng vấn các cấp quản lý để xem có dự án nào bị dừng triển khai do không đáp ứng được nhu cầu về lợi ích và mức độ hiệu quả.

Vấn đề A1.02 - Lập, triển khai kế hoạch chiến lược CNTT

Mục tiêu kiểm toán

Đánh giá xem đơn vị có chiến lược CNTT hay không. Chiến lược CNTT có bao gồm các kế hoạch CNTT và các quá trình cho việc xây dựng, phê duyệt, thực hiện và duy trì chiến lược sao cho phù hợp với các chiến lược và mục tiêu của tổ chức. Các rủi ro và nguồn lực trong khi thực hiện các mục tiêu CNTT được quản lý hiệu quả.

Kiểm soát A1.02.01 - Đơn vị có kế hoạch chiến lược CNTT ở cấp độ toàn đơn vị

Tiêu chí kiểm toán

- Đơn vị có một kế hoạch chiến lược CNTT ở cấp độ toàn đơn vị. Kế hoạch chiến lược CNTT giúp chuyển hóa các mục tiêu nghiệp vụ thành các mục tiêu và yêu cầu CNTT.

- Kế hoạch CNTT được xem xét, cập nhật định kỳ.

Tài liệu yêu cầu

- Kế hoạch chiến lược CNTT hoặc tương đương.
- Các biên bản họp giữa ban lãnh đạo đơn vị và bộ phận CNTT.

Đánh giá thiết kế và triển khai

- Phỏng vấn lãnh đạo CNTT của đơn vị và xác minh xem đơn vị đã có chiến lược CNTT chưa và chiến lược CNTT của đơn vị đã được thực hiện như thế nào? Rà soát chiến lược CNTT của đơn vị và xác minh xem chiến lược CNTT được ban hành bởi ai vào thời điểm nào.

- Phỏng vấn lãnh đạo cao nhất doanh nghiệp để xác định liệu những yêu cầu của họ đã được đáp ứng bởi hệ thống CNTT của tổ chức hay chưa? Chiến lược CNTT có phù hợp với chiến lược và mục tiêu của tổ chức

- Phỏng vấn lãnh đạo CNTT của đơn vị và xác minh tần suất đơn vị tiến hành rà soát, cập nhật chiến lược CNTT.

- Xem xét các biên bản cuộc họp định kỳ của Ban chỉ đạo CNTT và Ban lãnh đạo của đơn vị để đảm bảo có sự tham gia của chủ doanh nghiệp và các quyết định chiến lược CNTT được Ban hành bởi những lãnh đạo cấp cao của đơn vị.

- Rà soát chiến lược CNTT hoặc Phòng vấn các cấp quản lý để xác định các yêu cầu về nguồn lực, cách thức chúng được xác định và được phê chuẩn, cũng như ai là người phê chuẩn việc đầu tư các công cụ hay các nguồn lực khác (VD: nhân viên, nhà thầu, kỹ năng thông qua đào tạo ...).

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát A1.02.02 - Đơn vị có kế hoạch và chính sách QLRR

Tiêu chí kiểm toán

Đơn vị có đầy đủ các kế hoạch và chính sách QLRR cũng như có sự chuẩn bị đầy đủ về mặt nguồn lực cho việc xác định và QLRR.

Tài liệu yêu cầu

- Kế hoạch quản lý rủi ro
- Danh sách các rủi ro và chiến lược giảm thiểu rủi ro
- Biên bản các cuộc họp đánh giá rủi ro định kỳ hoặc các văn bản tương đương

Đánh giá thiết kế và triển khai

- Phòng vấn lãnh đạo CNTT của đơn vị và xác minh xem đơn vị có kế hoạch/chính sách QLRR? Rà soát kế hoạch/chính sách của đơn vị để đảm bảo trách nhiệm QLRR được phân công rõ ràng, minh bạch. Đơn vị có sự chuẩn bị đầy đủ về mặt nguồn lực cho việc xác định và đánh giá rủi ro hay không?

- Rà soát kế hoạch/chính sách QLRR của đơn vị và xác minh xem rủi ro CNTT có phải là một phần trong khuôn khổ về quản trị rủi ro và tuân thủ (GRC) hay không

- Rà soát các biên bản cuộc họp để đảm bảo rằng các rủi ro mới đã được phân tích và bổ sung phù hợp.

- Phòng vấn quản lý hoặc xem xét các biên bản cuộc họp để xác định xem lãnh đạo đơn vị có ý thức rõ cả về rủi ro CNTT, các rủi ro khác và theo dõi tình trạng một cách định kỳ hay không.

- Phòng vấn những cá nhân có trách nhiệm QLRR để xác định xem các rủi ro đã được giảm thiểu có được ước tính chi phí thích hợp không và nguồn lực đã được phân bổ cho xử lý rủi ro hay chưa?

Thử nghiệm hiệu quả hoạt động

Vấn đề A1.03 - Cơ cấu tổ chức, chính sách và thủ tục liên quan đến CNTT

Mục tiêu kiểm toán

Đảm bảo đơn vị có cơ cấu tổ chức, chính sách và các thủ tục CNTT phù hợp giúp đơn vị đạt được mục tiêu kinh doanh.

Kiểm soát A1.03.01 - Cơ cấu tổ chức, các chính sách và thủ tục CNTT phù hợp, cho phép đơn vị hoàn thành các nhiệm vụ đáp ứng mục tiêu hoạt động

Tiêu chí kiểm toán

Bộ phận CNTT của đơn vị được tổ chức một cách phù hợp, vai trò và trách nhiệm của bộ phận CNTT được xác định rõ ràng bao gồm trong đó là vai trò của giám đốc CNTT (CIO) hoặc các vị trí tương đương. Các chính sách và thủ tục CNTT của đơn vị là phù hợp, được tài liệu hóa, phê duyệt đầy đủ, đóng vai trò quan trọng trong công tác hướng dẫn các hoạt động của đơn vị nói chung và các hoạt động CNTT nói riêng đáp ứng nhiệm vụ của mình.

Tài liệu yêu cầu

- Cơ cấu tổ chức tổng thể đơn vị
- Cơ cấu tổ chức bộ phận CNTT

Đánh giá thiết kế và triển khai

- Rà soát sơ đồ cơ cấu tổ chức tổng thể của đơn vị xác minh xem bộ phận CNTT của đơn vị đã được bố trí ở vị trí chiến lược hay chưa.
- Rà soát sơ đồ về cơ cấu tổ chức bộ phận CNTT của đơn vị và xác minh xem bộ phận CNTT đã được phân chia thành các phòng ban nhỏ để hỗ trợ các hoạt động của đơn vị hay chưa (ví dụ bộ phận CNTT cần có các ban liên quan tới hỗ trợ dịch vụ CNTT, quản lý CSDL, bảo trì hay tham gia vận hành hệ thống CNTT của nhà thầu)
- Phòng văn lãnh đạo CNTT của đơn vị và xác minh các chính sách liên quan trực tiếp đến bộ phận CNTT của tổ chức (ví dụ như các chính sách về lưu trữ tài liệu, phát triển phần mềm...), các phương thức mà qua đó chính sách, thủ tục CNTT được truyền thông tới người dùng cũng như các bên liên quan. Thu thập các bằng chứng liên quan tới việc truyền thông các chính sách CNTT tới người dùng (ví dụ như thư điện tử, các tài liệu đào tạo cho nhân viên mới hoặc đào tạo định kỳ hàng năm)

- Thu thập các yêu cầu thay đổi chính sách CNTT, rà soát lịch sử thay đổi của các chính sách CNTT để xác định rằng các chính sách có được cập nhật định kỳ hoặc khi cần thiết.

- Phỏng vấn một số nhân viên trong công ty để hiểu được sự nhận thức của họ đối với các chính sách và thủ tục CNTT đã được ban hành, đảm bảo các chính sách và thủ tục CNTT được ban hành và truyền thông tới các nhân viên trong đơn vị.

- Phỏng vấn các nhân viên giám sát chất lượng, rà soát các báo cáo giám sát chất lượng để đảm bảo các chính sách hoặc thủ tục đã và đang được tuân thủ hợp lý. Lấy thêm bằng chứng về các thủ tục của đơn vị đối với các trường hợp không tuân thủ.

Thử nghiệm hiệu quả hoạt động

Vấn đề A1.04 - Xây dựng và phát triển đội ngũ nhân sự CNTT

Mục tiêu kiểm toán:

Đội ngũ nhân sự CNTT của đơn vị bao gồm các cá nhân có đủ năng lực, được đào tạo bài bản và được tiếp cận đến các nguồn tài liệu một cách phù hợp để đáp ứng các mục tiêu hoạt động của đơn vị.

Kiểm soát A1.04.01 - Kế hoạch quản lý nhân sự CNTT phù hợp, đáp ứng cho nhu cầu hoạt động của đơn vị trong hiện tại và tương lai

Tiêu chí kiểm toán

Đội ngũ nhân sự CNTT của đơn vị bao gồm các cá nhân có đủ năng lực, được đào tạo bài bản và được tiếp cận đến các nguồn tài liệu một cách phù hợp để đáp ứng các mục tiêu hoạt động của đơn vị. Kế hoạch thuê và đào tạo nhân sự CNTT phản ánh đúng nhu cầu đã được xác định.

Tài liệu yêu cầu

Các chính sách của đơn vị liên quan đến:

- Kế hoạch nguồn lực và đào tạo nhân sự
- Kế hoạch chiến lược CNTT
- Kế hoạch thuê và đào tạo nhân sự CNTT

Đánh giá thiết kế và triển khai

- Rà soát các chính sách liên quan đến nhân sự CNTT để đảm bảo chúng được phê chuẩn và đang được thực hiện.

- Rà soát các chính sách liên quan đến nhân sự CNTT để đảm bảo các chính sách yêu cầu các bộ phận khác nhau (bộ phận CNTT, bộ phận đảm bảo chất lượng – QA, người dùng), xác định rõ nhu cầu về nhân sự và nguồn lực ở cả hiện tại và trong tương lai .

- Rà soát kế hoạch thuê và đào tạo nhân sự CNTT để đảm bảo rằng chúng phản ánh đúng nhu cầu đã được xác định.

- Thu thập các quy trình, chính sách, kế hoạch được lập thành văn bản và được lãnh đạo phê duyệt.

- Đánh giá các chính sách nguồn nhân lực để xác định xem các yêu cầu về kỹ năng đã được xác định hay chưa, và việc đào tạo có được áp dụng cho nhân viên mới và các nhân viên khác hay không. Phỏng vấn những người quản lý nguồn nhân lực hoặc quản lý hoạt động để kiểm tra xem họ đảm bảo các vị trí quan trọng được luôn được bố trí nhân sự trong các trường hợp nghỉ việc bất ngờ hoặc thiếu nhân sự kéo dài.

- Xem lại kế hoạch chiến lược CNTT để đảm bảo rằng kế hoạch đó bao hàm các yêu cầu về công tác nhân sự và bố trí nguồn lực đáp ứng nhu cầu hiện tại và tương lai.

- Rà soát cơ cấu nhân sự CNTT của đơn vị và bảo đảm cơ cấu nhân sự CNTT hiện tại bao gồm đầy đủ nhân sự cho các phòng ban khác nhau (hỗ trợ nghiệp vụ, quản lý chất lượng, quản trị CSDL....), các vị trí quan trọng luôn được bố trí nhân sự đầy đủ, kịp thời nếu có nhân sự chuyển việc

Thử nghiệm hiệu quả hoạt động

Vấn đề A1.05 - Đảm bảo sự tuân thủ chính sách và thủ tục CNTT

Mục tiêu kiểm toán:

Đảm bảo đơn vị có một cơ chế tuân thủ đầy đủ và hợp lý để đảm bảo tất cả các chính sách và thủ tục đang được vận hành theo quy định

Kiểm soát A1.05.01 - Cơ chế đảm bảo sự tuân thủ các chính sách và thủ tục

Tiêu chí kiểm toán

Đơn vị có một cơ chế đầy đủ và hiệu quả để đảm bảo tính tuân thủ của các chính sách

Tài liệu yêu cầu

- Các chính sách và thủ tục của đơn vị (bao gồm: ATTT, SDLC, đào tạo).
- Cơ cấu tổ chức đơn vị.

- Kế hoạch quản lý chất lượng.
- Các báo cáo từ nhóm chịu trách nhiệm cho việc tuân thủ.
- Biên bản họp từ ban lãnh đạo.

Đánh giá thiết kế và triển khai

- Phòng vận lãnh đạo CNTT của đơn vị để xác định ai là người chịu trách nhiệm đảm bảo việc tuân thủ của các chính sách và thủ tục CNTT.
- Phòng vận đội hoặc nhóm chịu trách nhiệm cho việc tuân thủ các chính sách và thủ tục trên để xác định cách thức họ thực hiện nhiệm vụ của mình.
- Phòng vận lãnh đạo CNTT của đơn vị về các phương án chế tài đối với các trường hợp không tuân thủ chính sách.
- Phòng vận và rà soát báo cáo từ các nhóm/đội có trách nhiệm đảm bảo tuân thủ khác nhau để xem xét những phát hiện của họ, những hành động mà họ đã thực hiện và báo cáo cho ban quản lý.
- Phòng vận nhóm/đội xây dựng các chính sách và thủ tục đánh giá rủi ro và cơ chế tuân thủ để xác định nguyên nhân cho việc cập nhật những chính sách và các thủ tục hiện hành.

Thử nghiệm hiệu quả hoạt động

Dựa trên số lượng mẫu các chính sách và thủ tục CNTT của đơn vị, Kiểm toán viên nhà nước tiến hành chọn mẫu và xác minh mức độ tuân thủ của chính sách như sau:

- Đảm bảo đơn vị có phân công việc đảm bảo tính tuân thủ của chính sách cho một nhóm/đội trong đơn vị (nhóm đảm bảo chất lượng (QA), kiểm toán nội bộ, kiểm tra tại chỗ...) Đảm bảo nhóm chịu trách nhiệm cho việc tuân thủ của chính sách/thủ tục CNTT ghi nhận lại đầy đủ các trường hợp không tuân thủ trong quá khứ, phương án chế tài và giải pháp
- Rà soát các bản báo cáo đảm bảo việc ghi nhận các trường hợp không tuân thủ là chính xác, áp dụng các phương án chế tài phù hợp theo quy định
- Rà soát các khóa đào tạo hoặc các phương pháp phổ biến khác (email, bản ghi nhớ, thông báo) để đánh giá liệu vấn đề không tuân thủ đã được giải quyết hay chưa.

4. Chuyên đề A2 - Phát triển, mua sắm và tiếp nhận các sản phẩm Công nghệ thông tin

a. Giới thiệu về phát triển, mua sắm và tiếp nhận các sản phẩm CNTT

Để hỗ trợ chiến lược phát triển của đơn vị, bộ phận CNTT đưa ra các giải pháp CNTT cho đơn vị hoặc cho người dùng ở khối nghiệp vụ. Quá trình phát triển, mua sắm hay ký kết hợp đồng một giải pháp CNTT phải được lên kế hoạch để QLRR, tối đa hóa cơ hội thành công. Ngoài ra, các yêu cầu cho giải pháp trên cần được nhận diện, phân tích, tài liệu hóa và phân loại ưu tiên... Đơn vị phải áp dụng quy trình đảm bảo chất lượng và thử nghiệm chức năng để đảm bảo chất lượng của các sản phẩm CNTT.

Thông thường, các giải pháp CNTT sẽ được phát triển hoặc mua sắm dưới hình thức dự án CNTT. Tuy nhiên, đôi khi đơn vị có thể không sử dụng hình thức dự án để quản lý việc triển khai sản phẩm CNTT, tuy nhiên các hoạt động trên vẫn phải tuân theo một số quy định chung của nhà nước cũng như của đơn vị.

Các sản phẩm CNTT được cung cấp bằng cách đơn vị tự phát triển nội bộ hoặc tiếp nhận từ đối tác bên ngoài thông qua hình thức mua sắm, hợp đồng phát triển hoặc thuê khoán. Thông thường, các đơn vị chọn cách tiếp cận tổng hợp cả ba hình thức trên.

Hiện tại, các tổ chức đang có xu hướng mua hoặc thuê sản phẩm và dịch vụ CNTT sẵn có vì thường có chi phí ít hơn so với việc tự phát triển. Điều này dẫn đến nguy cơ là các sản phẩm không đáp ứng được mục tiêu kinh doanh hoặc đáp ứng yêu cầu người sử dụng trong thực tế do các đặc thù riêng của đơn vị. Các rủi ro trên cần được quản lý để đảm bảo việc triển khai đạt được mục tiêu phát triển của đơn vị. Khi thực hiện triển khai đúng nguyên tắc, đơn vị sẽ thu được lợi ích thông qua việc tận dụng khả năng của nhà cung cấp để nhận được giải pháp chất lượng một cách nhanh chóng, với chi phí thấp và công nghệ thích hợp nhất.

Khi mua hay phát triển một sản phẩm hoặc giải pháp CNTT, đơn vị bắt buộc phải xác định chính xác nhu cầu của mình và các yêu cầu kỹ thuật. Quy trình khảo sát phải có sự tham gia của tất cả các bên liên quan đến quy trình nghiệp vụ, bao gồm khối người dùng cuối và khối nhân viên kỹ thuật sẽ tham gia việc duy trì và hỗ trợ hệ thống. Khi tiếp nhận các dịch vụ CNTT, bộ phận CNTT được giao nhiệm vụ làm việc với nhà cung cấp phải tham gia vào quy trình khảo sát yêu cầu. Các yêu cầu CNTT phải được sắp

xếp theo thứ tự ưu tiên nếu thiếu hụt ngân sách hoặc chi phí triển khai có hạn, một số yêu cầu có thể tạm hoãn và sẽ được đáp ứng trong tương lai khi có điều kiện phù hợp.

Xác định chính xác yêu cầu CNTT chỉ là bước đầu tiên trong quá trình phát triển, mua sắm và tiếp nhận. Việc triển khai còn đòi hỏi quản lý trên nhiều lĩnh vực khác như: QLRR, quản lý chương trình, công tác thử nghiệm, công tác giám sát nhà cung cấp trong quá trình triển khai và sau triển khai, đào tạo nội bộ và các sự cố triển khai v.v...

Có nhiều tiêu chuẩn để đơn vị lựa chọn nhằm tăng thành công trong việc triển khai sản phẩm hoặc dịch vụ.

b. Rủi ro thường gặp

Khi tự phát triển phần mềm nội bộ, đơn vị sẽ phải đối mặt với một số rủi ro hoặc thách thức liên quan đến kỹ năng trong lĩnh vực phần mềm, kinh nghiệm kiểm thử và quản lý dự án, ước tính hợp lý chi phí và lợi ích, giám sát và theo dõi tiến độ dự án.

c. Các vấn đề kiểm toán thành phần

Các yêu cầu phần mềm hay hệ thống CNTT phải được xuất phát từ yêu cầu của người dùng, Kiểm toán viên nhà nước cần xem xét liệu:

- Người dùng có được tư vấn trong việc xác định các yêu cầu.
- Có nhân sự thuộc bộ phận quản lý chất lượng tham gia đánh giá chất lượng của hệ thống đang được phát triển.
- Khi mua sắm sản phẩm CNTT, cấp quản lý cần được báo cáo định kỳ về tình trạng của sản phẩm cùng như dự án, để kịp thời chấn chỉnh khi cần thiết.

Mục tiêu chính của Kiểm toán viên nhà nước là việc xác định đầu mỗi kiểm toán có:

- Quản lý nhà cung cấp;
- Nhận báo cáo tiến độ định kỳ;
- Thực hiện chấn chỉnh.

Nhằm thực hiện được các việc trên, hợp đồng cần thể hiện rõ:

- Các mốc dự án quan trọng trong quá trình phát triển;
- Các báo cáo rà soát và báo cáo tình trạng dự án nhằm cung cấp các thông tin về chi phí, tiến độ, hiệu quả.

Kiểm toán viên nhà nước cũng cần đảm bảo ban quản lý hoặc một cá nhân được chỉ định chịu trách nhiệm nhận các báo cáo, rà soát và thực hiện các biện pháp chấn chỉnh khi cần thiết.

Việc phát triển, mua sắm và tiếp nhận các sản phẩm CNTT của đơn vị được đánh giá thông qua việc kiểm toán các đối tượng liên quan đến dự án CNTT, bao gồm: Xác định nhu cầu nghiệp vụ; Việc quản lý và kiểm soát dự án; Việc đảm bảo chất lượng và kiểm thử; Chọn nhà thầu; và Cấu hình hệ thống. Cụ thể như sau:

- Vấn đề A20100 - Xác định và quản lý nhu cầu nghiệp vụ nhằm đảm bảo các nhu cầu nghiệp vụ có thực sự xuất phát từ người dùng cuối cũng như cách thức đơn vị phân tích, ưu tiên và giải quyết nhu cầu nghiệp vụ trên là hợp lý và khoa học.
- Vấn đề A20200 - Quản lý và kiểm soát dự án CNTT nhằm đánh giá việc triển khai kế hoạch dự án CNTT cùng việc kiểm soát để hạn chế các rủi ro cũng như tuân thủ các quy định của luật pháp và đơn vị.
- Vấn đề A20300 - Đảm bảo chất lượng và kiểm thử dự án CNTT nhằm đảm bảo các dự án tự phát triển hoặc thuê ngoài của đơn vị đạt được các kết quả cam kết thể hiện trong các hợp đồng.
- Vấn đề A20400 - Công tác đấu thầu nhằm đảm bảo tính tuân thủ của công tác đấu thầu thông qua các nội dung chi tiết: Hồ sơ mời thầu, hồ sơ dự thầu, quyết định chọn nhà thầu, các hợp đồng, các văn bản gia hạn hợp đồng, các đề xuất đánh giá trước nhà thầu, các tài liệu thiết kế sơ bộ,...
- Vấn đề A20500 - Quản lý cấu hình nhằm đảm bảo phương thức quản lý cấu hình các hệ thống CNTT được phát triển, tiếp nhận hoặc mua sắm phù hợp, an toàn và không lãng phí.

d. Chương trình kiểm toán mẫu

Vấn đề A2.01 - Quản lý và xác định nhu cầu mua sắm và đầu tư CNTT

Mục tiêu kiểm toán

Đánh giá việc xác định, xếp thứ tự ưu tiên và quản lý các yêu cầu của đơn vị đối với các yêu cầu hệ thống CNTT.

Kiểm soát A2.01.01 - Nhận diện nhu cầu của người dùng đối với hệ thống CNTT

Tiêu chí kiểm toán

Đơn vị có kế hoạch hoặc thủ tục trong việc thu thập, xem xét và phân nhóm các yêu cầu cho những chức năng mới hoặc chức năng bổ sung trên Hệ thống.

Tài liệu yêu cầu

- Kế hoạch hoặc các thủ tục quản lý các yêu cầu
- Bản mẫu các yêu cầu của người dùng
- Bản mẫu đánh giá ban đầu yêu cầu người dùng

Đánh giá thiết kế và triển khai

▪ Phòng vấn ban lãnh đạo CNTT, thu thập và rà soát kế hoạch, thủ tục quản lý yêu cầu đã được duyệt và ban hành để bảo đảm rằng người dùng, các bên liên quan đều được tham gia trong quá trình xác định các yêu cầu cho hệ thống CNTT.

▪ Thực hiện xuyên suốt một quy trình yêu cầu được đề xuất bởi người dùng, ghi nhận, xem xét, phân loại bằng việc thu thập danh sách các yêu cầu người dùng của đơn vị về hệ thống CNTT, rà soát các mẫu yêu cầu đảm bảo các yêu cầu tương tự nhau hoặc trùng lặp nhau được nhóm lại thành một nhóm, được ghi nhận, phản hồi.

▪ Đối với các thay đổi, nâng cấp lớn, việc phát triển các mẫu thử và việc tư vấn người dùng có thể diễn ra song song, trong trường hợp này, Kiểm toán viên nhà nước rà soát quá trình trao đổi thông tin giữa bộ phận nghiệp vụ, ban CNTT và nhà thầu.

Thử nghiệm hiệu quả hoạt động

Dựa vào danh sách yêu cầu của người dùng cho hệ thống CNTT, Kiểm toán viên nhà nước tiến hành chọn mẫu yêu cầu và xác định người dùng, bên liên quan đều tham gia trong quá trình xác định yêu cầu đầy đủ.

▪ Kiểm tra và xác minh các mẫu yêu cầu được chọn có trùng lặp hay tương tự yêu cầu nào không? Nếu có, các yêu cầu đó có được nhóm chung lại với nhau hay không?

▪ Dựa vào danh sách các yêu cầu nâng cấp chức năng, xác minh xem việc tư vấn người dùng và phát triển các mẫu kiểm thử có được tiến hành song song hay không? Nếu có thì các yêu cầu này có được xem xét, đánh giá và trao đổi giữa bộ phận nghiệp vụ, ban CNTT và nhà thầu hay không?

Kiểm soát A2.01.02 - Phân tích, sắp xếp thứ tự ưu tiên và quản lý yêu cầu của người dùng.

Tiêu chí kiểm toán

Tổ chức phân tích, sắp xếp thứ tự và quản lý các yêu cầu để đảm bảo rằng nhu cầu của người dùng được đáp ứng một cách tối ưu và hiệu quả về chi phí

Tài liệu yêu cầu

- Danh sách các yêu cầu CNTT
- Bản mẫu phân tích các yêu cầu CNTT
- Bảng ma trận theo dõi các yêu cầu CNTT
- Tiêu chí ưu tiên cho các yêu cầu

Đánh giá thiết kế và triển khai

- Phòng văn ban lãnh đạo CNTT và thu thập tài liệu đã được lãnh đạo phê duyệt, mô tả quy trình phân tích yêu cầu của người dùng, các tiêu chí đánh giá mức độ ưu tiên cho các yêu cầu như: chi phí, nhu cầu nghiệp vụ, vấn đề khẩn cấp hay bắt buộc cần thêm mới...

- Thu thập mẫu biểu rà soát yêu cầu để đảm bảo yêu cầu có chứa đầy đủ các thông tin: người yêu cầu, ngày, thứ tự ưu tiên, chi phí, rủi ro...

- Thu thập các bản phân tích yêu cầu hoặc nhận xét về yêu cầu của nhân viên nghiệp vụ hoặc các bên liên quan để xác minh tất cả các quan điểm, ý kiến được thu thập và tóm tắt để đưa ra kết luận phân tích thích hợp (chấp nhận, trì hoãn, từ chối...)

- Đánh giá bảng nhu cầu người dùng để làm rõ các nhu cầu được duyệt có nằm trong dự án phát triển hoặc mua ngoài của đơn vị hay không, thời gian thực hiện có bám sát và thực hiện đúng tiến độ hay không? Thu thập và rà soát yêu cầu để xác định yêu cầu được phê duyệt, phân công thực hiện trong các dự án phát triển phần mềm hoặc dự án mua ngoài. Xác minh xem các yêu cầu đó có đang được theo dõi, quản lý hay không?

Thử nghiệm hiệu quả hoạt động

Dựa vào danh sách các yêu cầu, Kiểm toán viên nhà nước tiến hành chọn mẫu và xác minh việc ghi lại các thông tin liên quan của yêu cầu như: người yêu cầu, ngày tháng mức độ ưu tiên, chi phí, rủi ro...

- Rà soát việc phân tích đối với các yêu cầu đã chọn để xác minh việc chấp nhận, từ chối... yêu cầu là hợp lý

- Đối chiếu tiêu chí đánh giá yêu cầu với các yêu cầu đã chọn, đảm bảo việc đánh giá mức độ ưu tiên tuân theo các tiêu chí đề ra

Vấn đề A2.02 - Kiểm soát và quản lý việc mua sắm và phát triển dự án CNTT

Mục tiêu kiểm toán

Đánh giá được cách đơn vị kiểm soát và quản lý sự phát triển hoặc mua lại các dự án CNTT đã được phê duyệt.

Kiểm soát A2.02.01 - Kế hoạch phát triển hoặc mua sắm các dự án CNTT

Tiêu chí kiểm toán

Đơn vị có thực hiện lập kế hoạch quản lý dự án hoặc các thủ tục tương đương cho các dự án được phê duyệt để làm căn cứ, hướng dẫn cho việc thực thi dự án.

Tài liệu yêu cầu

- Kế hoạch quản lý dự án hoặc các tài liệu tương đương

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo CNTT và thu thập tài liệu kế hoạch quản lý dự án hoặc các văn bản tương đương. Tìm hiểu và thu thập các quy trình, quy định đã được duyệt bởi lãnh đạo có liên quan đến việc lập kế hoạch.

- Xem xét đánh giá kế hoạch quản lý các yêu cầu hoặc tương đương để đảm bảo nó bao gồm mô tả dự án, phạm vi, chi phí, tiến độ, rủi ro, cơ cấu quản lý và xác định các bên liên quan (nội bộ hoặc bên ngoài). Xem xét, đánh giá các kế hoạch để làm rõ kế hoạch đã được phê duyệt bởi lãnh đạo đơn vị và tổng hợp ý kiến của các bên liên quan;

- Xem xét tổng thể dự án để xác định vai trò của từng cá nhân đối với việc kiểm thử, phát triển và cài đặt hệ thống cơ sở hạ tầng CNTT, nhóm hỗ trợ ...

- Đối với các dự án mua ngoài, xác định xem kế hoạch hoặc các văn bản tương đương có thực hiện phân công, phân nhiệm đối với những cá nhân thực hiện giám sát hoạt động của các nhà thầu hay không; Phỏng vấn những người quản lý dự án để xác định phương pháp chu trình phát triển phần mềm (System Development Life Cycle) có được áp dụng đối trong quy trình phát triển dự án hay không?

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát A2.02.02 - Kiểm soát các dự án CNTT

Tiêu chí kiểm toán

Đơn vị kiểm soát và theo dõi các dự án CNTT đảm bảo đáp ứng các yêu cầu về chi phí, tiến độ và hiệu quả công việc.

Tài liệu yêu cầu

- Chi phí và tiến độ dự án ban đầu
- Báo cáo tình trạng dự án
- Các báo cáo liên quan tới nhà thầu, thỏa thuận dịch vụ (SLA)
- Kết quả đánh giá
- Các hoạt động cần thực hiện

Đánh giá thiết kế và triển khai

- Phòng vấn người quản lý dự án và thu thập tài liệu chi phí, tiến độ dự án các báo cáo tình hình dự án;
- So sánh chi phí và tiến độ dự án với các báo cáo về thực trạng dự án để đánh giá các điểm không phù hợp;
- Phòng vấn đội ngũ quản lý dự án và thu thập các tài liệu về kết quả đánh giá các hạng mục công việc, thu thập biên bản các cuộc họp giữa đơn vị và các nhà thầu, xem xét và đánh giá tính hiệu quả trong việc giám sát các dự án thuê ngoài; Phòng vấn quản lý dự án và thu thập các hợp đồng giữa đơn vị và nhà thầu cung cấp dịch vụ, đánh giá việc triển khai có đảm bảo tuân thủ theo các điều khoản của hợp đồng và quy định của nhà nước hay không?
- Trong trường hợp không có hợp đồng cung cấp dịch vụ. Phòng vấn nhân viên phụ trách hợp đồng tại đơn vị để xác định cách quản lý nhà thầu về thuê nhà thầu khác giám sát, theo dõi, đánh giá báo cáo định kỳ về tình hình hoạt động và báo cáo các rủi ro cho đơn vị.

Thử nghiệm hiệu quả hoạt động

Dựa vào danh sách dự án CNTT, Kiểm toán viên nhà nước lựa chọn mẫu dự án, tiến hành rà soát và xác minh tài liệu liên quan tiến độ dự án, báo cáo tình hình dự án; các bản so sánh chi phí và tiến độ dự án với các báo cáo về thực trạng dự án để đánh giá các điểm không phù hợp và xác minh các phản hồi của đơn vị về các điểm không phù hợp đó. Thu thập biên bản các cuộc họp giữa đơn vị và các nhà thầu, xác minh xem đơn vị có thực đánh giá tính hiệu quả trong việc giám sát các dự án thuê ngoài hay không?

Vấn đề A2.03 - Kiểm thử và đảm bảo chất lượng dự án CNTT

Mục tiêu kiểm toán:

Đánh giá các dự án tự phát triển hoặc thuê ngoài của đơn vị có đạt được các tiêu chí về chất lượng hay không?

Kiểm soát A2.03.01 - Xây dựng và quy định vai trò, trách nhiệm của đội ngũ kiểm soát chất lượng

Tiêu chí kiểm toán

- Đơn vị có tổ chức đội ngũ kiểm soát chất lượng;
- Đội ngũ kiểm soát chất lượng được quy định vai trò và trách nhiệm rõ ràng.

Tài liệu yêu cầu

Kế hoạch quản lý dự án hoặc các tài liệu tương đương

Đánh giá thiết kế và triển khai

- Phòng văn ban quản lý dự án thu thập tài liệu kế hoạch và chính sách liên quan đến việc đảm bảo chất lượng của dự án, xác định danh sách nhóm/cá nhân chịu trách nhiệm chính trong việc đảm bảo chất lượng, mục tiêu của dự án.

Ví dụ: Kiểm toán viên nhà nước cần xem xét, đánh giá nhóm đảm bảo chất lượng của dự án trong quá trình thực hiện có nghiên cứu các hồ sơ dự án như: yêu cầu, mục tiêu, hướng dẫn sử dụng làm căn cứ đánh giá dự án có đảm bảo đầy đủ về nội dung và trình tự thực hiện hay không?

- Phòng văn ban quản lý dự án, xác định các thủ tục đảm bảo chất lượng và phòng văn các cá nhân chịu trách nhiệm đảm bảo chất lượng, xác minh danh sách phần việc họ phải thực hiện trong quy trình đảm bảo chất lượng (chịu trách nhiệm giám sát tiến độ, chịu trách nhiệm đảm bảo chất lượng thiết kế sản phẩm...)

- Thu thập các báo cáo kết quả hoạt động của bộ phận đảm bảo chất lượng dự án để đánh giá đội dự án có theo đúng kế hoạch quản lý dự án, có đúng theo SDLC... hay không?

Thử nghiệm hiệu quả hoạt động

Dựa vào nhân sự chịu trách nhiệm chính trong việc đảm bảo chất lượng, mục tiêu của dự án, Kiểm toán viên nhà nước lựa chọn mẫu nhân sự chịu trách nhiệm để xác minh vai trò của học dự án. Xác minh đơn vị có đánh giá dự án có đảm bảo đầy đủ về nội dung đúng theo trình tự, kế hoạch quản lý dự án, quy trình phát triển phần mềm hay không?

Kiểm soát A2.03.02 - Tổ chức kế hoạch và tiến hành thử nghiệm trên hệ thống CNTT

Tiêu chí kiểm toán

Đơn vị tiến hành kiểm thử trên hệ thống CNTT, dựa vào kết quả kiểm thử chấp nhận hoặc từ chối hệ thống.

Tài liệu yêu cầu

- Kế hoạch kiểm thử
- Lịch trình kiểm thử
- Kết quả kiểm thử
- Các tiêu chí chấp thuận/từ chối sau kiểm thử

Đánh giá thiết kế và triển khai

- Phòng văn quản lý dự án về quy trình kiểm thử của đơn vị, thu thập quy trình đã được lập thành văn bản và được lãnh đạo chấp thuận.

- Thu thập kế hoạch kiểm thử, rà soát và đánh kế hoạch kiểm thử hệ thống CNTT của đơn vị.

- Phòng văn quản lý dự án về tiến độ dự án; thu thập báo cáo và tiến hành so sánh chi phí, thời gian dự án với các báo cáo tiến độ của dự án để tìm ra sự bất hợp lý (nếu có).

- Phòng văn người quản lý dự án, thu thập các báo cáo đánh giá để xem xét đánh giá các hoạt động chưa phù hợp trong dự án có được tập trung xử lý hay không? Phòng văn đội ngũ quản lý dự án và thu thập các biên bản cuộc họp với các nhà thầu nhằm đánh giá tính hiệu quả trong việc giám sát các dự án thuê ngoài; Phòng văn quản lý dự

án, thu thập các hợp đồng cung cấp dịch vụ để đánh giá tính thực thi các điều khoản trong hợp đồng.

Thử nghiệm hiệu quả hoạt động

Dựa vào danh sách các dự án CNTT, chọn dự một dự án đã có kết quả kiểm thử và bị từ chối (nếu có), tiến hành:

- Thu thập báo cáo tiến độ dự án, tiến hành so sánh chi phí, thời gian dự án với các báo cáo tiến độ của dự án để tìm ra sự bất hợp lý
- Thu thập tài liệu liên quan xác minh nguyên nhân kết quả từ chối Thu thập biên bản cuộc họp với các nhà thầu xác minh các phương pháp giải quyết của đơn vị
- Xác minh các tính tuân thủ trong của các nhà thầu cung cấp theo các điều khoản trong hợp đồng với đơn vị.

Dựa vào danh sách các dự án CNTT, chọn dự một dự án đã có kết quả kiểm thử và được chấp nhận (nếu có), tiến hành: Thu thập báo cáo tiến độ dự án, tiến hành so sánh chi phí, thời gian dự án với các báo cáo tiến độ của dự án

- Thu thập kết quả đánh giá hoạt động của nhà thầu tuân thủ đúng các yêu cầu trong hợp đồng.

Vấn đề A2.04 - Hoạt động đấu thầu

Mục tiêu kiểm toán:

Đánh giá tính tuân thủ và hiệu quả của hoạt động đấu thầu của đơn vị thông qua các nội dung chi tiết: Hồ sơ mời thầu, hồ sơ dự thầu, quyết định chọn nhà thầu, các hợp đồng, các văn bản gia hạn hợp đồng, các đề xuất đánh giá trước nhà thầu, các tài liệu thiết kế sơ bộ.

Kiểm soát A2.04.01 - Kế hoạch/thủ tục trong hoạt động đấu thầu của đơn vị

Tiêu chí kiểm toán

Các hoạt động đấu thầu trong việc lựa chọn nhà cung cấp được tiến hành theo kế hoạch đấu thầu của đơn vị.

Tài liệu yêu cầu

- Kế hoạch/thủ tục mời thầu
- Hồ sơ thầu
- Đánh giá yêu cầu người dùng
- Đánh giá hồ sơ thầu

- Các văn bản pháp luật, các quy định liên quan đến đấu thầu

Đánh giá thiết kế và triển khai

▪ Phòng văn cá nhân chịu trách nhiệm chính trong việc mời thầu, thu thập hồ sơ mời thầu, xác minh các tiêu chí đánh giá lựa chọn nhà thầu của đơn vị. Phòng văn nhân sự chính phụ trách ký hợp đồng thầu làm thế nào để đảm bảo gói thầu hoàn thiện (ví dụ xin ý kiến người dùng, các bên liên quan, rà soát bởi các chuyên gia...).

▪ Thu thập các gói thầu, kế hoạch và thủ tục triển khai thực hiện, đánh giá người dùng về yêu cầu đấu thầu, đánh giá người dùng về các gói thầu, các văn bản quy định liên quan tới việc đấu thầu, lựa chọn nhà thầu.

Ví dụ: Phòng văn người dùng, các chuyên gia... để xác định, đánh giá tính đầy đủ, hiệu quả, đúng quy định của các gói thầu. Phòng văn người dùng hoặc lãnh đạo đơn vị để làm rõ các yêu cầu kỹ thuật của đơn vị và việc đáp ứng của nhà thầu như thế nào đối với các yêu cầu của đơn vị; Phòng văn nhân sự tham gia soạn thảo và ký hợp đồng để xác định xem hoạt động đấu thầu của đơn vị có thực hiện theo đúng quy định và pháp luật không?

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách các gói thầu đã, đang hoặc dự kiến thực hiện, Kiểm toán viên nhà nước chọn mẫu nhằm:

- Đảm bảo kế hoạch và thủ tục được xác định rõ ràng để thực hiện các hoạt động đấu thầu.
- Các biên bản thảo luận, nghiên cứu thị trường, hồ sơ mời thầu v.v... được lập và xét duyệt theo đúng quy định.

Kiểm soát A2.04.02 -Tiêu chí lựa chọn nhà thầu

Tiêu chí kiểm toán

Đơn vị sử dụng các tiêu chí khách quan, được quy định rõ ràng trong các văn bản để lựa chọn nhà thầu.

Tài liệu yêu cầu

- Tiêu chí lựa chọn nhà thầu

Đánh giá thiết kế và triển khai

▪ Phòng văn cán bộ phụ trách quản lý việc đấu thầu và thu thập danh sách các tiêu chí lựa chọn nhà thầu

- Rà soát các tiêu chí lựa chọn nhà thầu của đơn vị và đảm bảo các tiêu chí đúng với mục đích của việc đấu thầu
- Phỏng vấn các bên liên quan để đánh giá lý do họ đưa ra các tiêu chí đó
- Ma trận chấm điểm nhà thầu hoặc tài liệu tương đương
- Rà soát bảng chấm điểm nhà thầu để xác định bảng điểm có phù hợp với tiêu chí lựa chọn hay không.

Thử nghiệm hiệu quả hoạt động

Dựa vào danh sách các tiêu chí lựa chọn nhà thầu, Kiểm toán viên nhà nước lựa chọn mẫu các tiêu chí, phỏng vấn các bên liên quan về lý do đưa ra tiêu chí đó, rà soát bảng điểm đấu thầu và xác minh tiêu chí đó đưa vào trong việc lựa chọn nhà thầu.

Vấn đề A2.05– Quản lý cấu hình

Mục tiêu kiểm toán:

Đánh giá phương thức quản lý cấu hình của đơn vị trong việc phát triển hoặc mua mới

Kiểm soát A2.05.01 - Chính sách đơn vị sử dụng cho quản lý cấu hình

Tiêu chí kiểm toán

Các hoạt động quản lý cấu hình được tiến hành tuân theo các quy định, chính sách của đơn vị

Tài liệu yêu cầu

- Chính sách, thủ tục quản lý cấu hình hoặc các văn bản tương đương

Đánh giá thiết kế và triển khai

- Phỏng vấn nhân sự phụ trách quản lý cấu hình, thu thập chính sách quản lý cấu hình và rà soát: Phạm vi của chính sách và các yêu cầu bắt buộc, vai trò và trách nhiệm của các cá nhân trong việc quản lý cấu hình, các yêu cầu về tài nguyên/công cụ cho quản lý cấu hình, sự liên kết giữa các thủ tục cấu hình, các nguyên tắc xử phạt đối với trường hợp không tuân thủ quản lý cấu hình.

- Trong trường hợp không có thủ tục quản lý cấu hình, phỏng vấn nhân sự phụ trách làm thế nào họ có thể đảm bảo họ chịu trách nhiệm hoàn toàn về việc cấu hình của tổ chức

- Phỏng vấn một nhân sự trực tiếp tham gia quản lý cấu hình, kiểm tra và xác minh xem họ có nắm vững phạm vi của việc quản lý cấu hình, vai trò của mình trong

việc quản lý cấu hình, xác minh cá tài nguyên/công cụ mà họ sử dụng trong việc quản lý cấu hình.

Thử nghiệm hiệu quả hoạt động

Dựa vào danh sách không tuân thủ quản lý cấu hình của đơn vị (nếu có), xác minh lại các thủ tục xử phạt có tuân theo đúng nguyên tắc đã định hay không?

Kiểm soát A2.05.02- Nhóm/cá nhân nào phụ trách việc thay đổi và cài đặt cuối cùng trên môi trường sản phẩm.

Tiêu chí kiểm toán

Chỉ có những thay đổi đã được chấp thuận và phê duyệt mới được phép đưa lên môi trường sản phẩm

Tài liệu yêu cầu

- Danh sách nhóm/cá nhân chịu trách nhiệm cho việc thay đổi trên môi trường vận hành
- Quy trình phê duyệt và đưa các thay đổi đã được kiểm thử và thông qua lên môi trường vận hành.

Đánh giá thiết kế và triển khai

- Phòng vận lãnh đạo ban CNTT để nắm được danh sách nhóm/cá nhân có quyền thay đổi trên môi trường thật. Nhóm/cá nhân này có thể là ban kiểm soát thay đổi hoặc các bộ phận tương tự thực hiện công tác rà soát và phê duyệt thay đổi. Thu thập danh sách các cá nhân trong nhóm/cá nhân có quyền thay đổi trên môi trường thật
- Phòng vận nhân sự chịu trách nhiệm chính cho việc đưa phần mềm mới lên môi trường và đảm bảo rằng phần mềm đó đã được kiểm thử, đảm bảo các tiêu chí đề ra, được tài liệu hóa phù hợp, đào tạo sử dụng cho người dùng trước khi đưa lên môi trường thật.
- Thu thập các tài liệu liên quan tới việc kiểm thử chức năng, kiểm thử người dùng cuối, các biên bản chứng minh đã đào tạo cho người dùng cuối trước khi đưa phần mềm mới lên môi trường thật.
- Phòng vận nhân sự chịu trách nhiệm chính cho việc cấp quyền thay đổi về các thủ tục ngăn chặn việc cập nhật thay đổi bất hợp pháp lên hệ thống thật như kiểm soát quyền truy cập trên môi trường thật, tách bạch giữa môi trường kiểm thử và môi trường thật.

- Thu thập tài liệu kiểm soát quyền truy cập trên môi trường thật: danh sách nhân sự được phép truy cập, quyền hạn truy cập. Thu thập địa chỉ môi trường thật, môi trường kiểm thử, đảm bảo tính tách bạch của hai môi trường đó

Thử nghiệm hiệu quả hoạt động

Dựa vào danh sách cập nhật thay đổi, phát triển phần mềm mới được phê duyệt trên môi trường thật, Kiểm toán viên nhà nước lựa chọn mẫu cập nhật thay đổi/phát triển phần mềm mới, thu thập các tài liệu và bằng chứng liên quan (như phần TOD) xác minh:

- Chỉ có các cá nhân được cấp quyền mới được phép truy cập trên môi trường thật
- Có các thủ tục kiểm thử chức năng, kiểm thử chấp nhận người dùng, hướng dẫn người dùng cuối trước khi được đưa lên môi trường thật.

5. Chuyên đề A3 - Vận hành hệ thống Công nghệ thông tin

a. Khái niệm

Vận hành hệ thống CNTT là công việc hàng ngày liên quan đến việc vận hành và hỗ trợ các hệ thống CNTT của đơn vị (ví dụ như chạy các máy chủ, bảo trì, cung cấp dung lượng lưu trữ cần thiết, hỗ trợ thường trực, v.v...). Các tác vụ này được đo lường và quản lý bằng các Chỉ số đo lường hiệu quả hoạt động (KPI).

Các KPI thường được ghi nhận và xem xét định kỳ. Cách thức đo lường và cam kết về hiệu quả hoạt động của việc vận hành hệ thống CNTT phải ghi nhận cụ thể thông qua bản cam kết chất lượng dịch vụ nội bộ (SLA) giữa bộ phận CNTT và tổ chức.

Ví dụ: Bộ phận CNTT của Ngân hàng cam kết vận hành các Hệ thống máy chủ với chỉ số “Máy hoạt động liên tục” (Uptime) đạt 99.99% tương ứng với tổng thời gian hệ thống dừng hoạt động (do sự cố, bảo trì, nâng cấp v.v...) không vượt quá 4 phút 19 giây cho mỗi chu kỳ 30 ngày.

Kiểm toán viên nhà nước có thể kiểm toán một số vấn đề sau để đánh giá mức độ hiệu quả của công tác vận hành hệ thống CNTT ở đơn vị kiểm toán như:

- Quản lý dịch vụ CNTT;
- Quản lý hiệu năng;
- Quy trình giải quyết sự cố để đảm bảo hoạt động liên tục;
- Các thông lệ hoặc thực hành để quản lý thay đổi.

Quản lý dịch vụ CNTT

Nhằm mục đích đánh giá xem bộ phận CNTT đã cung cấp dịch vụ đạt yêu cầu như cam kết hay chưa, các bộ phận sử dụng dịch vụ có hài lòng, và các hoạt động ứng phó khi có sai biệt về dịch vụ cung cấp so với cam kết.

Quản lý hiệu năng

Bao gồm quản lý các loại dịch vụ khác nhau hỗ trợ cho hoạt động kinh doanh theo cách thức đáp ứng được yêu cầu của doanh nghiệp hoặc người sử dụng ví dụ như tối ưu hóa băng thông mạng, tăng cường tính khả dụng của các nguồn lực, tối ưu hóa và tăng cường lưu trữ, v.v...

Quản lý sự cố

Là các hệ thống và thông lệ được sử dụng để xác định sự cố hoặc sai sót được ghi lại, phân tích và giải quyết kịp thời.

Quản lý sự cố và các vấn đề phát sinh nhằm đảm bảo công tác vận hành hệ thống được giảm thiểu các tác động xấu do các sự cố và các vấn đề phát sinh.

Quản lý sự thay đổi

Trong các tổ chức CNTT, quá trình quản lý thay đổi thường được sử dụng để quản lý và kiểm soát các thay đổi đến tài sản, chẳng hạn như phần mềm, phần cứng và tài liệu liên quan. Kiểm soát thay đổi là cần thiết để đảm bảo rằng tất cả các thay đổi cấu hình hệ thống được ủy quyền, kiểm tra, tài liệu hóa và kiểm soát để các hệ thống tiếp tục hỗ trợ hoạt động kinh doanh theo kế hoạch, và những thay đổi được ghi nhận lại.

b. Rủi ro thường gặp

Việc xác định rủi ro trong việc vận hành hệ thống CNTT căn cứ vào các văn bản, quy định về chức năng, nhiệm vụ, quyền hạn của bộ phận CNTT cùng các SLA giữa bộ phận CNTT với đơn vị, cơ quan chức năng cũng như người dùng cuối. Các tài liệu trên phản ánh những nội dung công việc cùng yêu cầu về chất lượng mà bộ phận CNTT cần phải bảo đảm khi vận hành hệ thống CNTT.

Trong trường hợp các tài liệu này thiếu hoặc không ban hành chính thức, sẽ xuất hiện rủi ro là các nguồn lực CNTT của đơn vị không được sử dụng một cách hiệu lực và hiệu quả. Do vậy, khi kiểm toán vận hành hệ thống CNTT, Kiểm toán viên nhà nước cần thu thập các tài liệu quy định về mục tiêu tổng thể và các thông số kỹ thuật, thông thường là ở trong các SLA.

Trong việc quản lý thay đổi, Kiểm toán viên nhà nước cần kiểm tra xem đơn vị có quy trình quản lý thay đổi không và quy trình quản lý thay đổi cần phải bảo đảm được tính toàn vẹn của hệ thống. Cần bảo đảm chỉ có các ứng dụng đã được kiểm thử và phê duyệt mới được đưa lên môi trường vận hành.

Kiểm toán viên nhà nước cũng cần đánh giá việc quản lý khả năng đáp ứng của hệ thống CNTT (tài nguyên, CPU, mạng v.v...) phù hợp với nhu cầu người dùng, quản lý sự cố và các vấn đề an toàn CNTT khác nhằm bảo đảm không làm ảnh hưởng đến hoạt động của đơn vị do các nguyên nhân trên.

c. Các vấn đề kiểm toán thành phần

Các vấn đề kiểm toán của chuyên đề bao gồm:

- Vấn đề A3.01 – Quản lý dịch vụ CNTT nhằm đánh giá và kiểm tra việc triển khai và vận hành hệ thống CNTT có theo hướng tiếp cận dịch vụ.
- Vấn đề A3.02 – Khả năng đáp ứng hệ thống CNTT nhằm đánh giá và kiểm tra bộ phận CNTT có kế hoạch để đảm bảo hiệu năng và công suất hoạt động của hệ thống đáp ứng được các yêu cầu nghiệp vụ hiện tại và tương lai của đơn vị.
- Vấn đề A3.03 – Quản lý sự cố và các vấn đề phát sinh nhằm đánh giá tính hiệu quả của các văn bản, chính sách và các thủ tục liên quan đến quản lý sự cố và các vấn đề phát sinh của đơn vị.
- Vấn đề A3.04 - Quản lý sự thay đổi nhằm đánh giá xem đơn vị đã triển khai thủ tục chuẩn hóa để kiểm soát tất cả thay đổi đối với các hệ thống và ứng dụng CNTT cốt lõi.

d. Chương trình kiểm toán mẫu

Vấn đề A3.01 - Quản lý dịch vụ CNTT

Mục tiêu kiểm toán

Đánh giá xem liệu bộ phận CNTT có đang tích cực giám sát công tác vận hành CNTT dựa trên các SLA hoặc hợp đồng hay không?

Kiểm soát A3.01.01 - SLA được thiết lập giữa bộ phận CNTT với các đơn vị phòng ban liên quan

Tiêu chí kiểm toán

SLA được thiết lập giữa bộ phận CNTT với các phòng ban liên quan và SLA tuân thủ các quy định. Ví dụ: SLA cần phân chia trách nhiệm rạch ròi giữa chủ sở hữu quy

trình kinh doanh và nhóm hỗ trợ CNTT; SLA cần bao gồm các mục tiêu quản trị doanh nghiệp, dịch vụ cung ứng và các chỉ số đảm bảo chất lượng, định nghĩa về các loại rủi ro, trách nhiệm hỗ trợ của bộ phận vận hành CNTT.

Tài liệu yêu cầu

- Văn bản quy định và/hoặc các SLA được ký kết giữa đơn vị và bộ phận CNTT liên quan đến việc cam kết bảo đảm chất lượng dịch vụ.

Đánh giá thiết kế và triển khai

- Thu thập các văn bản quy định và/hoặc SLA được ký kết giữa đơn vị và bộ phận CNTT liên quan đến việc cam kết bảo đảm chất lượng dịch vụ.

- Rà soát các SLA để kiểm tra xem các tài liệu bao gồm các nội dung, các mục tiêu và cấp độ dịch vụ được đo lường, hệ thống và dịch vụ trong/ngoài phạm vi cam kết, hỗ trợ ở cấp độ ứng dụng và xử lý sự cố, tính khả dụng của hệ thống, khung thời gian trợ giúp, thời gian đáp ứng và giải quyết phụ thuộc vào phân loại mức độ nghiêm trọng của một vấn đề, lịch trình bảo trì, ...

- Kiểm tra xem các chủ sở hữu quy trình kinh doanh đã ký vào SLA hay chưa.

- Phỏng vấn đại diện một số chủ sở hữu quy trình kinh doanh để đánh giá nhận thức của họ về các SLA cũng như mức độ hài lòng của họ đối với dịch vụ bộ phận CNTT cung cấp.

- Thu thập danh sách các SLA và kiểm tra tính hiệu lực của các SLA này. Trao đổi và đánh giá việc nhận thức của trưởng bộ phận CNTT về các SLA hết hiệu lực/hoặc vô hiệu.

Thử nghiệm hiệu quả hoạt động

Kiểm soát A3.01.02- SLA được thực hiện, theo dõi và điều chỉnh khi cần thiết

Tiêu chí kiểm toán

Đơn vị có các cơ chế để đảm bảo SLA được tuân thủ một cách nhất quán.

Tài liệu yêu cầu

- Các báo cáo ngày, tháng, quý hoặc đột xuất của bộ phận CNTT;
- Thỏa thuận dịch vụ (SLA).

Đánh giá thiết kế và triển khai

- Rà soát lại các báo cáo của bộ phận CNTT để đảm bảo tất cả các chỉ số đã đồng ý đang được theo dõi thông qua các báo cáo này hoặc các biểu đồ xu hướng thể hiện trên báo cáo...
- Rà soát lại các báo cáo và xác minh xem những chỉ số nào thường được ghi nhận và báo cáo định kỳ lên các cấp lãnh đạo
- Rà soát báo cáo để đảm bảo các báo cáo hỗ trợ người dùng được xem xét bởi các cấp lãnh đạo và các vấn đề nghiêm trọng sẽ được ghi nhận lại và sử dụng như một tiêu chí khi ra quyết định mua mới các dịch vụ hay khi định kỳ rà soát lại bản thỏa thuận dịch vụ.
- Kiểm tra xem các hoạt động cụ thể của bộ phận CNTT hay ban lãnh đạo đơn vị (trong trường hợp thuê ngoài đội ngũ hỗ trợ) khi các chỉ số hoạt động không phù hợp với những quy định trong SLA.
- Phỏng vấn nhân viên bộ phận CNTT và đánh giá khả năng giám sát hệ thống của các nhân viên hỗ trợ người dùng, các công cụ được sử dụng, việc ưu tiên các nhiệm vụ hỗ trợ.
- Thu thập các lưu đồ cơ bản của hệ thống mạng và mối liên hệ giữa các ứng dụng, các thông số về thời gian phản hồi, tần suất sao lưu, kiểm thử của dữ liệu sao lưu để xác minh sự tuân thủ đối với các yêu cầu được quy định trong SLA.

Thử nghiệm hiệu quả hoạt động

Kiểm soát A3.01.03- Công tác quản lý các dịch vụ CNTT nhận được sự hài lòng của người dùng cuối cũng như góp phần đạt được các mục tiêu hoạt động của đơn vị.

Tiêu chí kiểm toán

Các chỉ số KPI của công tác quản lý dịch vụ CNTT phù hợp với nhu cầu và mục tiêu hoạt động của đơn vị.

Tài liệu yêu cầu

- Báo cáo hỗ trợ người dùng
- Thỏa thuận dịch vụ (SLA)

Đánh giá thiết kế và triển khai

- Rà soát lại báo cáo hỗ trợ người dùng và xác minh xem liệu một khối lượng lớn các vấn đề liên quan tới các dịch vụ CNTT đã được ngăn chặn trước khi người dùng báo cáo
- Rà soát lại báo cáo hỗ trợ người dùng và xác minh xem liệu rằng thời gian giải quyết cho các vấn đề nhỏ hơn thời gian được quy định trong SLA.
- Phòng vận lãnh đạo CNTT của đơn vị và xác minh xem các chỉ số quy định trong thỏa thuận dịch vụ có được rà soát và đánh giá chất lượng định kỳ bởi các cấp lãnh đạo hay không, đảm bảo công tác quản lý dịch vụ CNTT giúp đạt được các mục tiêu kinh doanh của đơn vị
- Phòng vận một vài người dùng cuối ở đơn vị (ở các cấp khác nhau) hoặc thực hiện một cuộc khảo sát về sự hài lòng chất lượng dịch vụ CNTT để đánh giá xem công tác quản lý CNTT có nhận được sự hài lòng từ người dùng cuối hay không?

Thử nghiệm hiệu quả hoạt động

Vấn đề A3.02 - Khả năng đáp ứng hệ thống CNTT

Mục tiêu kiểm toán:

Bộ phận CNTT có kế hoạch để đảm bảo hiệu năng và công suất hoạt động của hệ thống đáp ứng được các yêu cầu nghiệp vụ hiện tại và tương lai của đơn vị.

Kiểm soát A3.02.01 – SLA giữa các bộ phận nghiệp vụ và bộ phận CNTT đảm bảo cho việc lựa chọn ra những chỉ số KPI của hệ thống CNTT

Tiêu chí kiểm toán

Đảm bảo đơn vị thực hiện theo dõi và giám sát việc xây dựng các chỉ số KPI của hệ thống CNTT.

Tài liệu yêu cầu

- Văn bản quy định về các chỉ số KPI của hệ thống CNTT
- Các SLA hoặc văn bản tương đương
- Văn bản "Hướng dẫn hoạt động" của đơn vị

Đánh giá thiết kế và triển khai

- Phòng vận lãnh đạo CNTT của đơn vị và xác minh xem đơn vị có các thỏa thuận nội bộ hay văn bản nào quy định về các chỉ số đo lường mức độ hiệu quả và công suất của hệ thống CNTT hay không?

- Rà soát bản thỏa thuận nội bộ hoặc văn bản tương đương và xác minh xem các chỉ số đo lường mức độ hiệu quả hệ thống CNTT mà đơn vị đang sử dụng là gì? Đảm bảo bao gồm các chỉ số như: hiệu năng sử dụng các tài nguyên sẵn có, thời gian đăng nhập hệ thống trung bình, % thời gian chết, thời gian phản hồi hệ thống trung bình...

- Rà soát bản thỏa thuận nội bộ hoặc văn bản tương đương, đảm bảo nó đã được xem xét, ký kết bởi các phòng ban liên quan hoặc các lãnh đạo cấp cao.

- So sánh các chỉ số đo lường mức độ hiệu quả hoạt động CNTT được thiết lập bởi bộ phận CNTT (ví dụ như tính sẵn có của hệ thống mạng, thời gian phản hồi của máy chủ) với "Hướng dẫn hoạt động" của đơn vị để xác minh xem bộ phận CNTT đã tuân thủ theo "Hướng dẫn hoạt động" hay chưa.

Thử nghiệm hiệu quả hoạt động

Dựa vào danh sách các SLA, chọn mẫu để xác minh các bên tham gia đều nhận thức đầy đủ về thỏa thuận này.

Kiểm soát A3.02.02- Đơn vị tiến hành thu thập và rà soát các chỉ số về hiệu năng hoạt động của hệ thống định kỳ, qua đó đưa ra những điều chỉnh thích hợp, phù hợp hơn với mục tiêu kinh doanh của đơn vị

Tiêu chí kiểm toán

Đảm bảo đơn vị tiến hành rà soát và đánh giá hiệu năng hoạt động của hệ thống định kỳ

Tài liệu yêu cầu

- Các báo cáo định kỳ hiệu năng hoạt động của hệ thống
- Thỏa thuận nội bộ hoặc các văn bản tương đương

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo CNTT của đơn vị hoặc bộ phận quản lý chất lượng về tần suất mà bộ phận CNTT báo cáo lên các cấp lãnh đạo về thông tin các chỉ số mà qua đó hiệu năng hoạt động của hệ thống được xác định hoặc tần suất mà đơn vị chủ động thu thập các thông tin để đánh giá hiệu năng của hệ thống CNTT.

- Xác minh xem thời gian báo cáo, thu thập hoặc đánh giá các chỉ số có được quy định trong thỏa thuận nội bộ hay văn bản tương đương nào không?

- Rà soát thỏa thuận nội bộ hoặc các văn bản tương đương và đánh giá mức độ hợp lý của thời gian báo cáo.

- Phòng vận lãnh đạo CNTT của đơn vị về các thông tin thường được sử dụng để quản lý hiệu năng và công suất của hệ thống.
- Rà soát báo cáo đánh giá hiệu năng hoạt động hệ thống CNTT của đơn vị để đảm bảo đã bao gồm việc phân tích và so sánh các chỉ số đánh giá hiệu năng của hệ thống với các chỉ số được quy định trong SLA.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước xác định chu kỳ của việc rà soát và số lần thực hiện rà soát trong năm, chọn mẫu để kiểm tra nhằm đảm bảo việc rà soát được thực hiện đầy đủ, được báo cáo và phê duyệt bởi lãnh đạo cũng như kết luận về hiệu năng hoạt động của hệ thống và các tinh chỉnh (nếu có)

Kiểm soát A3.02.03 - Đơn vị thực hiện phân tích trên các dữ liệu về hiệu năng hệ thống để nâng cao hiệu quả. Trong trường hợp cần thiết, bộ phận CNTT lên kế hoạch và mua các tài nguyên bổ sung để đáp ứng yêu cầu kinh doanh.

Tiêu chí kiểm toán

Đảm bảo đơn vị thực hiện việc phân tích trên dữ liệu hiệu năng hệ thống căn cứ trên các tham số thiết lập trong thỏa thuận /hướng dẫn vận hành. Các bước khắc phục, tăng cường hiệu quả được đơn vị nghiêm túc thực hiện dựa trên các kết quả phân tích

Tài liệu yêu cầu

- Tài liệu về quy trình thủ tục phân tích dữ liệu hiệu năng hệ thống
- Tài liệu về quy trình thủ tục khắc phục, tăng cường hiệu quả hệ thống
- Các báo cáo định kỳ của bộ phận CNTT hoặc các văn bản liên quan thể hiện việc đơn vị thực hiện đánh giá và phân tích dữ liệu
- Các biên bản họp liên quan

Đánh giá thiết kế và triển khai

- Phòng vận lãnh đạo CNTT/cán bộ chuyên trách có thẩm quyền về:
 - Quy trình thủ tục phân tích dữ liệu hiệu năng
 - Căn cứ phân tích để đưa ra kết quả phân tích
 - Thủ tục khắc phục, tăng cường hiệu quả hệ thống dựa trên kết quả phân tích
 - Có trường hợp nào xảy ra về việc không giải quyết kịp thời vấn đề hiệu năng của hệ thống CNTT tại đơn vị hay chưa?

- Rà soát các báo cáo định kỳ của bộ phận CNTT hoặc các văn bản liên quan thể hiện việc đơn vị thực hiện đánh giá và phân tích dữ liệu, so sánh với yêu cầu về dịch vụ CNTT để hiểu đúng bản chất nguyên nhân của việc không đáp ứng được nhu cầu sử dụng.

- Rà soát các biên bản họp và tìm ra các vấn đề về việc không đáp ứng kịp thời hoặc chỉ đáp ứng một phần của hệ thống CNTT, cũng như các đề xuất giải quyết các vấn đề hiệu năng hệ thống CNTT

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước chọn mẫu các phân tích và xem xét liệu kiểm soát này có hoạt động hiệu quả trong suốt giai đoạn kiểm toán. Các phân tích có hợp lý, kết quả phân tích có được ban lãnh đạo phê duyệt.

Vấn đề A3.03 - Quản lý sự cố và các vấn đề phát sinh

Mục tiêu kiểm toán:

Đánh giá tính hiệu quả của các văn bản, chính sách và các thủ tục liên quan đến quản lý sự cố và các vấn đề phát sinh của đơn vị.

Kiểm soát A3.03.01 - Đơn vị có ban hành chính sách, quy định về việc ứng phó sự cố và nhận thức của người dùng về chính sách, quy định đó.

Tiêu chí kiểm toán

Góp phần đảm bảo công tác ứng phó được thực hiện hiệu quả.

Tài liệu yêu cầu

- Các tài liệu liên quan tới chính sách, quy định của đơn vị về việc ứng phó khi có sự cố.

- Tài liệu hướng dẫn trao đổi đối với người dùng và với đối tác bên ngoài khi có sự cố xảy ra.

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo CNTT, thu thập tài liệu liên quan tới chính sách, quy định của đơn vị về việc ứng phó khi có sự cố. Xác minh xem tài liệu đó đã mô tả đầy đủ các bước cần thực hiện hay chưa (các bước có thể bao gồm, chuẩn bị, phát hiện, phân tích đánh giá, ngăn chặn và loại trừ, các hoạt động sau sự cố)? Đánh giá các bước cần thực hiện có phụ thuộc vào cấp độ ảnh hưởng hoặc mức độ thường xuyên xảy ra sự cố hay không?

- Phòng vấn lãnh đạo CNTT, tìm hiểu các thủ tục về việc phổ biến cho người dùng chính sách, quy định của đơn vị về việc ứng phó khi có sự cố. Tìm hiểu và xác minh cách thức trao đổi giữa đội ứng phó sự cố và các bên liên quan. Thu thập tài liệu hướng dẫn trao đổi với đối tác bên ngoài khi có sự cố xảy ra.

- Phòng vấn một vài nhân sự trong đội ứng phó sự cố, xác minh xem nhân sự đó có nắm được các bước cần thực hiện nếu như có sự cố xảy ra hay không?

Thử nghiệm hiệu quả hoạt động

Kiểm soát A3.03.02- Đội ứng phó sự cố có được trang bị đầy đủ kỹ năng cùng với công cụ hỗ trợ và các nguồn lực hay không? Quản lý cấp cao hơn có hỗ trợ giải quyết sự cố hay không?

Tiêu chí kiểm toán

Đơn vị ứng phó với các sự cố một cách hiệu quả, tuân theo hướng dẫn trong thỏa thuận dịch vụ.

Tài liệu yêu cầu

- Tài liệu về quy trình thủ tục quản lý sự cố leo thang
- Danh sách công cụ/phần mềm đội ứng phó sử dụng trong ứng phó sự cố
- Các tài liệu liên quan tới quy trình, thủ tục và các tiêu chí cho việc ghi lại thông tin của sự cố

Đánh giá thiết kế và triển khai

- Phòng vấn đội ứng phó sự cố, xác minh họ có tiến hành điều tra sự cố không? Phòng vấn trao đổi với các chuyên gia trong đơn vị phụ trách về an ninh mạng, hệ điều hành, bảo mật và xác minh họ tiến hành công việc của mình như thế nào trong công tác ứng phó sự cố.

- Phòng vấn đội ứng phó sự cố, rà soát các thủ tục leo thang của sự cố có được giải quyết ngay lúc đó theo đúng danh mục rủi ro được định nghĩa trong thỏa thuận dịch vụ hay không?

- Phòng vấn đội ứng phó sự cố, tìm các hoạt động mà đội đã thực hiện để ứng phó với các sự cố trong quá khứ. Xác minh về công cụ/phần mềm mà đơn vị sử dụng trong việc quản lý sự cố.

- Phòng văn lãnh đạo CNTT xác minh liệu tổ chức đã thiết lập các tiêu chuẩn và thủ tục ghi lại để đảm bảo thông tin sự cố được ghi lại đầy đủ, các phần mềm bảo mật được rà soát thường xuyên

Thử nghiệm hiệu quả hoạt động

Dựa vào danh sách các sự cố, Kiểm toán viên nhà nước tiến hành chọn mẫu và xác minh

- Các thủ tục mà đơn vị ứng phó sự cố đã thực hiện
- Các chuyên gia có cùng tham gia trong việc điều tra sự cố hay không?
- Xác định các công cụ và đội ứng phó sự cố sử dụng trong việc ứng phó sự cố
- Kiểm tra các tài liệu liên quan tới việc lại thông tin của sự cố, xác minh các thông tin được ghi lại có đúng theo tiêu chí và thủ mà đơn vị đề ra hay không?

Kiểm soát A3.03.03 - Đánh giá mức độ hiệu quả trong việc khắc phục sự cố

Tiêu chí kiểm toán

Đơn vị triển khai ứng phó sự cố một cách hiệu quả.

Tài liệu yêu cầu

- Tài liệu hướng dẫn về mức độ ưu tiên của sự cố
- Tài liệu về các thủ tục xử lý sự cố
- Tài liệu đào tạo nhận thức về bảo mật định kỳ
- Các tài liệu, báo cáo liên quan tới các hoạt động sau khi xảy ra sự cố
- Các tài liệu liên quan với các sự cố đã được xác định

Đánh giá thiết kế và triển khai

- Phòng văn đội ứng phó sự cố, thu thập các tài liệu hướng dẫn về mức độ ưu tiên của sự cố, kiểm tra mức độ ưu tiên khắc phục sự cố cho từng tài sản hoặc dịch vụ của đơn vị.

- Thu thập tài liệu về các thủ tục xử lý sự cố, xem xét các thủ tục có đảm bảo việc nắm bắt, phân tích dữ liệu một cách nhanh chóng kịp thời hay không? Thu thập tài liệu "đào tạo nhận thức về bảo mật định kỳ", xác minh đội ứng phó có thực hiện phổ biến định kỳ cho người dùng về các chính sách và thủ tục liên quan tới việc sử dụng mạng, hệ thống, và phương tiện truyền thông bên ngoài và các ứng dụng.

- Thu thập các tài liệu, báo cáo liên quan tới các hoạt động sau khi xảy ra sự cố, rà soát công tác đào tạo bồi dưỡng cho người dùng để tránh lặp lại các sự cố tương tự.

- Với các sự cố đã xác định được nguyên nhân, thu thập các tài liệu liên quan và kiểm tra các hoạt động của đơn vị như: thay đổi của thủ tục, khiển trách, đào tạo... Kiểm tra xem đội phản ứng phó sự cố có ghi lại tất cả các sự cố đã được giải quyết một cách chi tiết hay không.

Thử nghiệm hiệu quả hoạt động

Dựa vào danh sách các báo cáo các sự cố, Kiểm toán viên nhà nước chọn mẫu và tiến hành các bước sau:

- Thu thập tài liệu ghi lại thông tin của sự cố, kiểm tra xem thông tin của các sự cố có được ghi chi tiết đầy đủ hay không? xác minh các sự cố trên có được đơn vị xử lý kịp thời hay không?
- Dựa và bản hướng dẫn mức độ ưu tiên sự cố của đơn vị, so sánh đối chiếu xem việc sắp xếp mức độ ưu của các sự cố được chọn có đúng với trong bản hướng dẫn hay không? Đối với sự cố đã xác định được nguyên nhân, kiểm tra và xác minh các hành động của đơn vị tránh các sự cố này lặp lại như thay đổi thủ tục, khiển trách đào tạo người dùng.

Vấn đề A3.04 - Quản lý sự thay đổi

Mục tiêu kiểm toán

Đánh giá xem đơn vị đã triển khai thủ tục chuẩn hóa để kiểm soát tất cả thay đổi đối với các hệ thống và ứng dụng CNTT cốt lõi.

Kiểm soát A3.04.01 - Đơn vị có ban hành chính sách quản lý thay đổi đã được phê duyệt hay không?

Tiêu chí kiểm toán

Kiểm soát thay đổi một cách hiệu quả bao gồm các bước chính: Yêu cầu chứng thực chấp nhận xét mức độ ưu tiên thiết kế kiểm thử thực thi tài liệu hóa

Tài liệu yêu cầu

- Tài liệu chính sách quản lý thay đổi
- Chính sách và các thủ tục trong quản trị CNTT
- Các tài liệu liên quan tới quản lý thay đổi như thu thập nhật ký và báo cáo trong quy trình quản lý thay đổi
- Danh sách nhận sự được phép truy cập vào thư viện tài nguyên trên hệ thống thật

Đánh giá thiết kế và triển khai

- Phòng vấn lãnh đạo ban CNTT, thu thập chính sách quản lý thay đổi của đơn vị, có thể tham khảo các yêu cầu chung về chính sách và các thủ tục trong quản trị CNTT
 - Rà soát tài liệu chính sách quản lý thay đổi và xác minh các thủ tục khởi tạo, rà soát và phê duyệt thay đổi được gắn với các trách nhiệm đi kèm.
 - Phòng vấn nhân sự tham gia vào trong quá trình thay đổi quan sát các hoạt động thực tế, thu thập các tài liệu liên quan (đã được phê duyệt và tài liệu hóa) đảm bảo rằng các thủ tục quản lý thay đổi tuân theo các bước chính sau: yêu cầu thay đổi, theo dõi thay đổi trong mô trường vận hành, xem xét các thủ tục cần thiết (như rà soát quản lý thay đổi, mức độ ưu tiên thay đổi)
 - Phòng vấn nhân sự đảm bảo chất lượng, thu thập nhật ký và báo cáo trong quy trình quản lý thay đổi, xác minh các nhật ký và báo cáo đó có được rà soát một cách đầy đủ hay không?
 - Phòng vấn ban lãnh đạo CNTT, thu thập danh sách nhận sự được phép truy cập vào thư viện tài nguyên trên hệ thống thật, đảm bảo chỉ có một nhân viên được cấp mới được phép truy cập, ban CNTT chịu trách nhiệm trong việc ngăn chặn các thay đổi trái phép trên môi trường thật.
 - Thu thập tài liệu liên quan tới việc thay đổi chương trình, rà soát tài liệu đó, xem xét cách đơn vị triển khai thực tế xác minh xem người dùng cuối có tham gia vào giai đoạn kiểm thử thay đổi để bảo tính đúng đắn của thay đổi hay không? Thu thập tài liệu liên quan tới thay đổi chương trình, rà soát tài liệu đó và đảm bảo các tài liệu đó đã được thống nhất, ký xác nhận trước khi chuyển lên hệ thống thật.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát A3.04.02 – Cách thức đảm bảo phục hồi lại phiên trước của hệ thống CNTT khi cần.

Tiêu chí kiểm toán

Tài liệu hóa các thủ tục và trách nhiệm trong việc khôi phục dữ liệu bị ảnh hưởng bởi các thay đổi không mong muốn

Tài liệu yêu cầu

- Văn bản chính sách quy định thủ tục khôi phục dữ liệu

Đánh giá thiết kế và triển khai

- Phòng vấn lãnh đạo CNTT, xác minh đơn vị có thực hiện các thủ tục khôi phục dữ liệu hay không? Thu thập văn bản chính sách quy định thủ tục khôi phục dữ liệu, kiểm tra văn bản có được phê duyệt hay không?
- Phòng vấn người dùng nghiệp vụ để tìm ra nếu những tác động ngoài ý định của các thay đổi chức năng/cải tiến đã được ưu tiên, phù hợp với lợi ích kinh doanh.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát A3.04.03- Đơn vị ban hành chính sách quy định về việc thay đổi khẩn cấp

Tiêu chí kiểm toán

Đơn vị ban hành chính sách quy định về việc thay đổi khẩn cấp phù hợp

Tài liệu yêu cầu

- Tài liệu liên quan tới quy trình quản lý thay đổi
- Các tài liệu kiểm thử thay đổi khẩn cấp trước khi chuyển lên môi trường vận hành.

Đánh giá thiết kế và triển khai

- Phòng vấn ban lãnh đạo CNTT, thu thập các tài liệu liên quan tới quy trình thay đổi, xác minh xem tài liệu đó có bao gồm chuyên mục kiểm soát cho các thay đổi khẩn cấp trên hệ thống hay không? Phòng vấn ban lãnh đạo CNTT, lấy một ví dụ về thay đổi khẩn cấp, so sánh việc thực hiện của đơn vị với các thủ tục chuyên mục thay đổi khẩn cấp hay không? Thu thập các tài liệu kiểm thử thay đổi khẩn cấp trước khi chuyển lên môi trường thật.
- Phòng vấn ban lãnh đạo CNTT, thu thập các tài liệu liên quan về việc các thay đổi khẩn cấp, kiểm tra các thay đổi khẩn cấp đó có được phê duyệt bởi các cấp lãnh đạo hay không trước khi chuyển lên môi trường thật hay không?

Thử nghiệm hiệu quả hoạt động

Dựa vào danh sách các thay đổi khẩn cấp, Kiểm toán viên nhà nước tiến hành lựa chọn mẫu và tiến hành các bước sau:

- Thu thập các tài liệu kiểm thử thay đổi trước khi đưa lên môi trường thật
- Thu thập tài liệu phê duyệt của cấp trên về việc cho phép các thay đổi khẩn cấp này

Kiểm soát A3.04.04 - Việc đóng và tài liệu hóa các thay đổi

Tiêu chí kiểm toán

Đảm bảo việc quản lý thay đổi hoạt động hiệu quả. Đơn vị có quy trình phù hợp sau để cập nhật các hệ thống liên quan và tài liệu người dùng sau khi một thay đổi được hoàn thiện.

Tài liệu yêu cầu

- Các tài liệu mô tả chức năng bị thay đổi
- Các tài liệu liên quan chức năng bị thay đổi trước và sau khi thay đổi.

Đánh giá thiết kế và triển khai

- Phòng vận lãnh đạo CNTT, thu thập các tài liệu mô tả chức năng bị thay đổi, xem xét các tài liệu để đảm bảo tính toàn diện và nhất quán của các chức năng bị thay đổi: thông tin cấu hình, tài liệu ứng dụng, màn hình trợ giúp, tài liệu đào tạo...

- Thu thập các tài liệu liên quan chức năng bị thay đổi trước và sau khi thay đổi, xác minh sau khi việc thay đổi hoàn thành, các tài liệu đó đã được cập nhật hay chưa.

- Dựa vào danh sách thay đổi, Kiểm toán viên nhà nước tiến hành chọn mẫu, thu thập các tài liệu liên quan chức năng bị thay đổi trước và sau khi thay đổi, xác minh sau khi việc thay đổi hoàn thành, các tài liệu đó đã được cập nhật hay chưa?

- Các tài liệu cần thu thập có thể như: thông tin cấu hình, tài liệu ứng dụng, màn hình trợ giúp, tài liệu đào tạo...

Thử nghiệm hiệu quả hoạt động

6. Chuyên đề A4 - Việc thuê khoán bên ngoài

a. Giới thiệu việc thuê khoán bên ngoài

Thuê khoán là một quá trình hợp đồng hóa những quy trình hoạt động hiện tại mà trước đây đơn vị thực hiện nội bộ hoặc một chức năng hoạt động mới với các đối tác

bên ngoài. Các đối tác được ký kết sẽ chịu trách nhiệm cung cấp các dịch vụ cần thiết với một mức phí đã được thỏa thuận. Đơn vị có thể chọn để khoán một phần (hoặc tất cả) cơ sở hạ tầng CNTT, dịch vụ CNTT hoặc các quy trình. Đơn vị nên có một chính sách hay tầm nhìn về những khía cạnh hoặc các chức năng hoạt động (thông thường là CNTT hoặc cũng có thể là lĩnh vực khác) có thể thuê khoán bên ngoài và chức năng nào cần được vận hành nội bộ. Tùy thuộc vào từng dịch vụ thuê ngoài, đơn vị có thể chọn cách kiểm soát phù hợp. Bộ phận CNTT có thể quyết định thuê ngoài một phần hoặc tất cả hạng mục liên quan đến CNTT nhằm tận dụng các ưu thế sau:

Nhân sự linh hoạt.

Đơn vị có thể tăng cường thuê khoán nhân sự bên ngoài khi cần thiết để thực hiện một số công việc mang tính thời vụ.

Phát triển nhân lực.

Đơn vị có thể thuê chuyên gia cấp cao cho một dự án CNTT thay vì đào tạo các nhân viên trong đơn vị để tiết kiệm thời gian và chi phí đào tạo. Sau đó, cử người của đơn vị theo sát các chuyên gia để học tập các kinh nghiệm và kỹ thuật chuyên môn..

Giảm chi phí.

Thuê khoán bên ngoài thông thường sẽ giúp cho đơn vị cắt giảm chi phí do nhà cung cấp có chi phí nhân công thấp hơn. Bộ phận CNTT không nên khoán những tác vụ tốn kém hơn so với khi thực hiện trong nội bộ. Thuê ngoài các lĩnh vực không phải là hoạt động chính của đơn vị cũng giúp cho đơn vị tập trung hơn vào các hoạt động kinh doanh cốt lõi, từ đó mang lại hiệu quả cao hơn.

Các chuyên gia tư vấn khi cần thiết.

Thuê khoán bên ngoài cho phép đơn vị có các chuyên gia túc trực hỗ trợ các vấn đề đang tồn tại hoặc đang nổi cộm. Đơn vị có thể nhanh chóng phản ứng với các nhu cầu thay đổi kinh doanh (yêu cầu mới hoặc thêm các chức năng) với sự trợ giúp của các chuyên gia.

b. Rủi ro thường gặp

Bản quyền sở hữu kiến thức kinh doanh và quy trình nghiệp vụ.

Việc phát triển phần mềm ứng dụng bên ngoài tổ chức có thể dẫn đến những nguy cơ mất quyền sở hữu quy trình hoạt động do nhà cung cấp dịch vụ có thể coi quy trình kinh doanh đó là quyền sở hữu trí tuệ của họ. Đơn vị cần có phương sách thích hợp để

giải quyết vấn đề này vào thời điểm ký kết hợp đồng và đảm bảo rằng đơn vị có tài liệu đầy đủ về quá trình phát triển cũng như thiết kế hệ thống. Điều này cũng sẽ giúp tổ chức chuyển đổi các nhà cung cấp dịch vụ nếu cần.

Nhà thầu không hoàn thành hợp đồng.

Có những trường hợp, nhà cung cấp không hoàn thành công việc bàn giao sản phẩm đúng hạn hay bàn giao những sản phẩm không sử dụng được do không đầy đủ chức năng. Nếu quá trình đấu thầu không được thực hiện đúng thủ tục, có khả năng cao hệ thống hoặc dịch vụ được mua không đáp ứng được nhu cầu người dùng, không đạt tiêu chuẩn, dẫn tới lãng phí. Thậm chí sản phẩm sẽ đòi hỏi nguồn lực đáng kể để duy trì hoạt động hoặc do chất lượng kém nên nó cần phải được thay thế trong tương lai gần. Hợp đồng sơ sài, không rõ ràng, quy trình lựa chọn nhà cung cấp không đầy đủ, các mốc thời gian không rõ ràng hay các điều kiện thị trường không thuận lợi là những lý do phổ biến khiến nhà thầu thất bại. Bộ phận CNTT cần có kế hoạch dự phòng cho một số vấn đề nêu trên. Khi xem xét việc thuê khoán xây dựng phần mềm, các phòng ban CNTT cần đánh giá mức độ ảnh hưởng trong việc không hoàn thành hợp đồng của nhà thầu (việc nhà thầu không hoàn thành hợp đồng có ảnh hưởng đáng kể đến hiệu quả hoạt động của đơn vị hay không?). Việc có đầy đủ các tài liệu hướng dẫn chi tiết về thiết kế hệ thống, phát triển hệ thống sẽ hỗ trợ tổ chức trong việc đảm bảo tính hoạt động liên tục thông qua một nhà cung cấp dịch vụ khác hoặc chính họ.

Các rủi ro về thay đổi phạm vi công việc.

Tất cả các hợp đồng thuê khoán đều có cơ sở và có giả định. Nếu các công việc thực tế thay đổi so với lúc ước tính ban đầu, khách hàng sẽ phải trả phần chênh lệch. Thực tế này là một trở ngại lớn cho các tổ chức CNTT khi giá cả không như cũ và nhà cung cấp luôn kỳ vọng sẽ được trả thêm cho phần phạm vi thay đổi. Hầu hết các dự án thay đổi khoảng 10-15% về thông số kỹ thuật trong suốt chu trình phát triển.

Luân chuyển nhân sự chủ chốt.

Các nhà cung cấp dịch vụ thuê khoán tăng trưởng nhanh chóng đã tạo ra một thị trường lao động năng động. Các nhân sự chủ chốt luôn được mời tham gia các dự án mới, dự án cao cấp, hoặc thậm chí được tuyển dụng bởi các nhà cung cấp khác. Tỷ lệ chuyển việc nằm trong bình quân khoảng 15-20%. Do vậy việc tạo ra các quy định trên hợp đồng về vấn đề thay đổi nhân sự chủ chốt là một yêu cầu hợp lý.

Rủi ro đến từ đối tác là đơn vị nước ngoài.

Sử dụng dịch vụ của các nhà cung cấp nước ngoài là một hình thức thông dụng, đặc biệt trong môi trường điện toán đám mây. Trong trường hợp này, rủi ro đối với việc thuê khoán bên ngoài sẽ liên quan tới các quy định của nước ngoài về việc lưu trữ thông tin, việc truyền tải có thể bị hạn chế, dữ liệu có thể được sử dụng bởi các cơ quan thực thi pháp luật nước ngoài mà không có hiểu biết về đơn vị, các tiêu chuẩn về bảo mật và ATTT có thể không tương xứng dẫn tới nảy sinh các tranh chấp liên quan đến thẩm quyền pháp lý.

c. Các vấn đề kiểm toán thành phần

Việc vận hành hệ thống CNTT của đơn vị được đánh giá thông qua việc kiểm toán các đối tượng: Chính sách thuê khoán dịch vụ bên ngoài; Đấu thầu; Giám sát nhà cung cấp và đối tác; Bảo vệ và quản lý dữ liệu; Nhà cung cấp nước ngoài; Giữ lại kiến thức kinh doanh và sở hữu quy trình kinh doanh; Hợp đồng các dịch vụ; Bảo mật thông tin với đối tác; Dự phòng và khắc phục thảm họa cho các dịch vụ thuê ngoài. Cụ thể như sau:

- Vấn đề A4.01 - Chính sách dịch vụ thuê ngoài nhằm kiểm tra đơn vị có đầy đủ các chính sách liên quan tới việc thuê khoán bên ngoài.
- Vấn đề A4.02 - Công tác đấu thầu nhằm kiểm tra đơn vị có đầy đủ các chính sách liên quan tới việc thuê khoán bên ngoài.
- Vấn đề A4.03 - Giám sát nhà cung cấp và đối tác nhằm kiểm tra và đánh giá việc đảm bảo chất lượng các dịch vụ thuê khoán thông qua các chỉ số KPI cùng các SLA.
- Vấn đề A4.04 - Bảo vệ và quản lý dữ liệu với đối tác nhằm kiểm tra và đánh giá việc bảo vệ và phân loại dữ liệu, cơ chế bảo mật và quyền truy cập đối với đối tác bên ngoài.
- Vấn đề A4.05 - Quản lý nhà cung cấp nước ngoài nhằm kiểm tra và đánh giá chính sách dự phòng về thuê khoán liên quan đến đại lý thuê khoán nước ngoài.
- Vấn đề A4.06 - Lưu giữ kiến thức kinh doanh và sở hữu quy trình nghiệp vụ nhằm kiểm tra và đánh giá việc đảm bảo quyền sở hữu kiến thức và quy trình kinh doanh và có thể tiếp tục tự hoạt động/tự xây dựng các chức năng quan trọng nếu nhà thầu hoặc nhà cung cấp không thể tiếp tục cung cấp dịch vụ.

- Vấn đề A4.07 - Kiểm soát và quản lý chi phí với đối tác nhằm kiểm tra nhằm kiểm tra chi phí thuê khoán được phân tích, tính toán theo các chuẩn mực và đạt được hiệu quả kinh tế cao nhất.

- Vấn đề A4.08 - SLA với đối tác nhằm đánh giá và kiểm tra SLA của đơn vị được xây dựng ở mức độ chi tiết, liệt kê tất cả các yêu cầu của đơn vị và là cơ sở để giám sát hoạt động của nhà cung cấp.

- Vấn đề A4.09 - Công tác bảo mật đối với đối tác nhằm kiểm tra các yêu cầu bảo mật đã được đề ra khi làm việc với đối tác và được thực hiện tuân theo các quy định.

- Vấn đề A4.10 - Sao lưu và khôi phục sau sự cố đối với các dịch vụ thuê ngoài nhằm kiểm tra các hợp đồng thuê khoán dịch vụ có các điều khoản về kế hoạch hoạt động liên tục (BCP) và kế hoạch phục hồi sau thảm họa (DRP).

d. Chương trình kiểm toán mẫu

Vấn đề A4.01 - Chính sách dịch vụ thuê ngoài

Mục tiêu kiểm toán:

Xác định đơn vị có đầy đủ các chính sách liên quan tới việc thuê khoán bên ngoài.

Kiểm soát A4.01.01 - Đơn vị có đầy đủ các chính sách liên quan tới việc thuê khoán bên ngoài

Tiêu chí kiểm toán

Xác định đơn vị có đầy đủ các chính sách liên quan tới việc thuê khoán bên ngoài

Tài liệu yêu cầu

- Các chính sách liên quan tới dịch vụ thuê khoán
- Các tài liệu phân tích lợi nhuận – chi phí khi thuê khoán chức năng dịch vụ bên ngoài
- Hồ sơ thuê ngoài
- SLA với bên ngoài

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phỏng vấn lãnh đạo CNTT của đơn vị để xác minh xem đơn vị có các chính sách liên quan tới dịch vụ thuê khoán bên ngoài hay không?
- Phỏng vấn lãnh đạo CNTT của đơn vị về quy trình phê duyệt đối với việc thuê khoán chức năng/dịch vụ bên ngoài

- Phòng vấn lãnh đạo CNTT của đơn vị để xác minh xem đơn vị có thực hiện phân tích lợi nhuận – chi phí khi thuê khoán chức năng dịch vụ bên ngoài hay không?
- Phòng vấn lãnh đạo CNTT của đơn vị để xác minh xem đơn vị có Phương thức đảm bảo tính liên tục trong trường hợp phải tiếp quản dịch vụ từ nhà cung cấp hay không?

Kiểm toán viên nhà nước tiến hành thu thập tài liệu và rà soát và xác minh các vấn đề sau:

- Rà soát chính sách thuê khoán để đảm bảo chính sách đã được thông qua. Ghi nhận thời điểm chính sách được ban hành và người ký quyết định ban hành. Bảo đảm người ký quyết định ban hành là lãnh đạo cấp cao có thẩm quyền trong đơn vị.
- Rà soát chính sách để bảo đảm chính sách bao gồm những thông tin liên quan đến việc các tài sản của tổ chức có thể thuê khoán hay không, xác định danh mục các dịch vụ/chức năng có thể thuê ngoài.
- Rà soát hồ sơ để đảm bảo đơn vị nhận thức được các rủi ro liên quan đến việc tiếp quản dịch vụ từ nhà cung cấp dịch vụ. Rà soát hồ sơ để đảm bảo tổ chức đảm bảo được khả năng hoạt động liên tục, quyền sở hữu dữ liệu, bảo mật, quyền sở hữu phần mềm ứng dụng và chi phí nằm trong thỏa thuận dịch vụ (SLA) trong trường hợp tiếp quản dịch vụ từ nhà cung cấp.

Thử nghiệm hiệu quả hoạt động

Dựa trên số lượng hồ sơ được phê duyệt, Kiểm toán viên nhà nước tiến hành chọn mẫu và kiểm tra các nội dung sau:

- Các khoản mục thuê ngoài được phê duyệt thuộc vào phạm vi/danh mục có thể thuê ngoài được quy định trong chính sách.
- Hồ sơ được phê duyệt đúng quy trình và được thực hiện bởi các nhà quản lý cấp cao.

Vấn đề A4.02 - Công tác đấu thầu

Mục tiêu kiểm toán:

Xác định đơn vị có đầy đủ các chính sách liên quan tới việc thuê khoán bên ngoài.

Kiểm soát A4.02.01 - Đơn vị có chính sách cụ thể trong công tác quản lý đấu thầu

Tiêu chí kiểm toán

Đơn vị có chính sách cụ thể trong công tác quản lý đấu thầu, trong đó:

- Có quy trình trong việc xác định và lựa chọn của nhà cung cấp dịch vụ không?
- Có các quy trình để chứng minh cho các kết luận đối với các yêu cầu/hợp đồng dịch vụ?

- Các quyết định có liên quan thực hiện ở các mức độ phù hợp không?

Tài liệu yêu cầu

- Chính sách liên quan đến đấu thầu hoặc mua lại
- Danh sách các điều luật quy định việc chuyển nhượng và thuê khoán phần mềm.

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo CNTT của đơn vị để kiểm tra xem đơn vị có chính sách cụ thể liên quan đến đấu thầu hoặc mua lại hay không.
- Kiểm toán viên nhà nước tham chiếu Luật đấu thầu cùng với các văn bản hướng dẫn của Nhà nước về công tác đấu thầu để xác định đơn vị có là đối tượng áp dụng của các văn bản này không. Lập danh mục các điều luật quy định việc chuyển nhượng và thuê khoán phần mềm.
- Thu thập chính sách đấu thầu, mua lại hoặc tương đương của đơn vị (nếu có) và kiểm tra tính tuân thủ theo luật định
- Thực hiện xuyên suốt một quy trình đấu thầu để xác minh tính tuân thủ đối với luật định hoặc chính sách cụ thể của đơn vị.

Thử nghiệm hiệu quả hoạt động

Dựa trên số lượng hợp đồng và các thỏa thuận dịch vụ, Kiểm toán viên nhà nước tiến hành lấy mẫu và xác minh các vấn đề sau:

- Rà soát lại quá trình lựa chọn nhà cung cho mỗi một hợp đồng dịch vụ thuê ngoài để bảo đảm nó phù hợp với quy định (đảm bảo quá trình lựa chọn là minh bạch, có tiêu chí, đội lựa chọn bao gồm các nhân viên hiểu các yêu cầu, các nhân viên làm công tác hợp đồng và tư vấn luật pháp cũng như tham khảo ý kiến với người sử dụng)
- Đảm bảo các yêu cầu về hợp đồng đã được thông qua bởi người dùng và các bên liên quan
- Đảm bảo công tác đấu thầu và hợp đồng được phê duyệt bởi lãnh đạo cấp cao

Vấn đề A4.03 - Giám sát nhà cung cấp và đối tác

Mục tiêu kiểm toán:

Các tham số và phương án dự phòng đã được quy định trong SLA và được thực hiện bởi đơn vị. Bao gồm:

- Các chỉ tiêu/tham số đo lường được định nghĩa dựa trên các hoạt động của tổ chức và thể hiện trong SLA
- Có thực hiện ký kết hợp đồng với nhà cung cấp dịch vụ không?
- Có thỏa thuận về việc giám sát với nhà cung cấp dịch vụ. Ví dụ: nhà thầu thuê ngoài có nhiệm vụ báo cáo tiến độ thường xuyên cho đơn vị, quyền được thanh tra/kiểm toán nhà thầu v.v..
- Mức độ dịch vụ được đảm bảo thông qua thỏa thuận này?
- Có các Phương án chế tài rõ ràng đối với nhà cung cấp dịch vụ khi không thực thi đầy đủ các quy định đã thỏa thuận trong SLA.

Kiểm soát A4.03.01- Đơn vị quản lý nhà thầu và nhà cung cấp một cách hiệu quả và có hành động thích hợp khi hiệu suất hoặc chất lượng sản phẩm CNTT lệch khỏi các tiêu chuẩn đã được quy định trong hợp đồng.

Tiêu chí kiểm toán

Trùng với mục tiêu kiểm toán

Tài liệu yêu cầu

- Chính sách hướng dẫn trong việc quản lý nhà thầu.
- Các SLA.
- Báo cáo tiến độ công việc, biên họp giữa nhà thầu và đơn vị.
- Hợp đồng giữa đơn vị và nhà thầu.

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Đơn vị có chính sách hướng dẫn trong việc quản lý nhà thầu.
- Phỏng vấn và xác minh lãnh đạo CNTT của đơn vị nhận thức đầy đủ về các điều khoản, điều kiện trong thỏa thuận cung cấp dịch vụ (SLA) của đơn vị, đặc biệt là các chế tài được quy định trong SLA hoặc trong hợp đồng khi nhà cung cấp dịch vụ không thực thi đầy đủ các quy định đã thỏa thuận trong hợp đồng hoặc SLA

- Các tình huống thực tế diễn ra trong kỳ kiểm toán khiến đơn vị phải thay đổi thỏa thuận, áp dụng các chế tài hoặc đổi nhà cung cấp dịch vụ.

Kiểm toán viên nhà nước tiến hành thu thập các tài liệu, rà soát và xác minh các vấn đề sau:

- Rà soát tài liệu để đảm bảo thỏa thuận dịch vụ được thiết lập và ký kết giữa hai bên
- Rà soát báo cáo tiến độ công việc của nhà cung cấp dịch vụ để đảm bảo rằng nó bao gồm các khoản mục báo cáo đã được quy định trong hợp đồng hoặc thỏa thuận dịch vụ (chi phí, kế hoạch, tiến độ, rủi ro, trạng thái, vấn đề, trạng thái các công việc thực hiện trong quá khứ)
- Rà soát báo cáo tiến độ công việc để xác định độ sai phạm trong việc triển khai các loại hình dịch vụ và tác động của các sai phạm đó
- Rà soát các thông báo và báo cáo các công việc cần được thực hiện khi nhà cung cấp không hoàn thành các nghĩa vụ được quy định trên SLA xem đã phù hợp, tương ứng với các tác động đến doanh nghiệp cũng như các điều khoản quy định trong hợp đồng hay chưa?

Thử nghiệm hiệu quả hoạt động

Dựa trên số lượng các thỏa thuận dịch vụ (SLA) và hợp đồng đã được phê duyệt, báo cáo tiến độ của nhà cung cấp, báo cáo xử lý sai phạm, Kiểm toán viên nhà nước tiến hành chọn mẫu và kiểm tra các nội dung sau:

- Bảo đảm báo cáo tiến độ bao hàm các khoản mục cần được báo cáo quy định trong thỏa thuận dịch vụ (SLA)
- Bảo đảm các chế tài được doanh nghiệp thực hiện đúng phù hợp với các tác động đến doanh nghiệp cũng như các điều khoản được quy định trong hợp đồng.

Vấn đề A4.04 - Bảo vệ và quản lý dữ liệu với đối tác

Mục tiêu kiểm toán:

- Các yêu cầu về bảo vệ dữ liệu và quyền truy cập của tổ chức đã được xác định và trở thành một phần của yêu cầu trong hợp đồng ký kết với đối tác bên ngoài.
- Các dữ liệu có được định nghĩa phù hợp để bao gồm cả dữ liệu nghiệp vụ cũng như của chương trình/phần mềm cung cấp dữ liệu (nếu có xảy ra).

- Có cơ chế đảm bảo rằng các yêu cầu bảo mật dữ liệu và theo thỏa thuận cấp độ dịch vụ đang áp dụng và thực hiện bởi các nhà cung cấp dịch vụ.

Kiểm soát A4.04.01 - Đơn vị đã thiết lập quyền bảo mật dữ liệu và bảo đảm các hợp đồng ký kết với các nhà thầu bên ngoài có quy định về bảo mật dữ liệu.

Tiêu chí kiểm toán

- Trùng với mục tiêu kiểm toán

Tài liệu yêu cầu

- Tài liệu quy định bảo mật dữ liệu và quyền truy cập đối với nhà thầu
- Hợp đồng giữa đơn vị và nhà thầu
- Các SLA.
- Các báo cáo kiểm toán của bên thứ ba hoặc kiểm toán nội bộ
- Các tài liệu giám sát, phản hồi, báo cáo xử lý sự cố nhằm đánh giá các hoạt động của đơn vị
- Danh sách các hồ sơ ghi nhận các dữ liệu nhà cung cấp dịch vụ được phép truy cập.
- Danh sách các thông tin bị tiết lộ bởi các đại lý thuê ngoài/bên thứ ba/các bên không liên quan (nếu có).

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phỏng vấn lãnh đạo CNTT của đơn vị để xác minh về phương thức truyền đạt các yêu cầu về bảo mật dữ liệu đến nhà cung cấp;
- Phỏng vấn lãnh đạo CNTT của đơn vị để xác minh xem việc bảo mật dữ liệu và quyền truy cập đã được bao hàm trong hợp đồng/thỏa thuận dịch vụ hay chưa? Phỏng vấn lãnh đạo CNTT về cơ chế đảm bảo các yêu cầu bảo mật dữ liệu quy định trong SLA đang được áp dụng và thực hiện bởi các nhà cung cấp dịch vụ;
- Phỏng vấn lãnh đạo CNTT về các tình huống vi phạm bảo mật trong kỳ kiểm toán.

Kiểm toán viên nhà nước thực hiện thủ tục và thu thập các bằng chứng kiểm toán sau:

- Thu thập các chính sách/yêu cầu bảo mật dữ liệu và quyền truy cập của đơn vị được lập thành văn bản và phê duyệt bởi lãnh đạo đơn vị.

- Thu thập hợp đồng với nhà cung cấp dịch vụ và xác minh vị trí trình bày phần định nghĩa về “Dữ liệu” (cho việc bảo mật và quyền truy cập) cũng như các yêu cầu về truy cập và bảo vệ dữ liệu và chế tài trên hợp đồng.

- Kiểm toán viên nhà nước xem xét báo cáo kiểm toán của bên thứ ba hoặc kiểm toán nội bộ với các đề xuất, đánh giá và xác định các ảnh hưởng lên đơn vị. Thu thập các tài liệu giám sát, phản hồi, báo cáo xử lý sự cố nhằm đánh giá các hoạt động của đơn vị.

- Danh sách các hồ sơ ghi nhận các dữ liệu nhà cung cấp dịch vụ được phép truy cập.

- Xác định thỏa thuận không tiết lộ thông tin (NDA) của đại lý thuê ngoài đã bao hàm tất cả các thông tin liên quan. Danh sách các thông tin bị tiết lộ bởi các đại lý thuê ngoài/bên thứ ba/các bên không liên quan.

- Dựa trên hợp đồng với các nhà cung cấp dịch vụ bên ngoài, tiến hành chọn mẫu và xem xét xem các yêu cầu về bảo mật dữ liệu để đảm bảo kiểm soát vận hành hiệu quả trong suốt kỳ kiểm toán.

Thử nghiệm hiệu quả hoạt động

Vấn đề A4.05 - Quản lý nhà cung cấp nước ngoài

Mục tiêu kiểm toán:

- Chính sách dự phòng về thuê khoán liên quan đến đại lý thuê khoán nước ngoài.
- Luật pháp của từng khu vực về kinh doanh với đại lý nước ngoài.

Kiểm soát A4.05.01 - Đơn vị có đầy đủ chính sách liên quan tới thuê khoán đại lý nước ngoài

Tiêu chí kiểm toán

Trùng với mục tiêu kiểm toán

Tài liệu yêu cầu

- Hợp đồng thuê khoán giữa nhà thầu và đơn vị
- Các thỏa thuận song phương giữa nước sở tại và nước của nhà cung cấp dịch vụ
- Báo cáo tiến độ của nhà cung cấp
- Báo cáo so sánh lợi ích chi phí của nhà cung cấp dịch vụ trong nước và nước ngoài
- Các SLA.

- Tài liệu liên quan tới thông tin về số tiền ký quỹ/bảo hiểm tài chính.
- Danh sách các sai lệch từ SLA và hợp đồng thuê khoán.
- Báo cáo giám sát về các hoạt động điều chỉnh chênh lệch bởi nhà cung cấp dịch vụ

vụ

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phòng vấn lãnh đạo CNTT của đơn vị để xác minh xem đơn vị có chiến lược/hoặc đã ký hợp đồng với đối tác nước ngoài hay không?
- Phòng vấn lãnh đạo CNTT của đơn vị để xác định xem đơn vị có nhận thức nào về các rủi ro liên quan tới thuê khoán đại lý nước ngoài?

Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán sau và thực hiện các thủ tục:

- Thu thập và rà soát các chính sách quy định của đơn vị liên quan tới thuê khoán đại lý nước ngoài được phê duyệt bởi lãnh đạo, luật và các thông lệ liên quan đến thuê khoán dịch vụ
- Thu thập thông tin về sự hiện diện của nhà cung cấp dịch vụ nước ngoài tại nước sở tại, cũng như danh các văn phòng ở nước ngoài của nhà cung cấp dịch vụ.
- Xem xét thỏa thuận song phương giữa nước sở tại và nước của nhà cung cấp dịch vụ và đánh giá ảnh hưởng lên các dịch vụ thuê khoán đơn vị đang sử dụng.
- Thu thập báo cáo tiến độ của nhà cung cấp về thời gian bàn giao và các vấn đề về chất lượng và bằng chứng về việc rà soát, kiểm tra chất lượng định kỳ của đơn vị đối với nhà cung cấp.
- Thu thập bảng so sánh lợi ích chi phí của nhà cung cấp dịch vụ trong nước và nước ngoài
- Thu thập và xem xét phê duyệt của lãnh đạo trên hợp đồng thuê khoán và thỏa thuận dịch vụ (SLA) là phù hợp.
- Thông tin về số tiền ký quỹ/bảo hiểm tài chính liên quan đến chất lượng dịch vụ
- Danh sách các sai lệch từ thỏa thuận dịch vụ (SLA) và hợp đồng thuê khoán
- Báo cáo giám sát về các hoạt động điều chỉnh chênh lệch bởi nhà cung cấp dịch vụ

vụ

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách các hợp đồng/SLA với nhà cung cấp nước ngoài, tiến hành chọn mẫu và thực hiện các thủ tục rà soát như ở bước đánh giá thiết kế và triển khai để đảm bảo kiểm soát vận hành hiệu quả trong suốt kỳ kiểm toán.

Vấn đề A4.06 - Lưu giữ kiến thức kinh doanh và sở hữu quy trình nghiệp vụ

Mục tiêu kiểm toán

Đảm bảo đơn vị có quyền sở hữu kiến thức và quy trình kinh doanh và có thể tiếp tục tự hoạt động/tự xây dựng các chức năng quan trọng nếu nhà thầu hoặc nhà cung cấp không thể tiếp tục cung cấp dịch vụ bằng việc:

- Duy trì việc sở hữu quy trình kinh doanh
- Duy trì các kiến thức chuyên ngành
- Thực hiện hoạt động liên tục trong hoàn cảnh nhà thầu dịch vụ dừng cung cấp

tại bất kỳ thời điểm

Kiểm soát A4.06.01 – Tài liệu hóa, bảo vệ và khẳng định sở hữu kiến thức kinh doanh và quy trình nghiệp vụ.

Tiêu chí kiểm toán

- Quyền sở hữu quy trình kinh doanh có được miêu tả và tài liệu hóa rõ ràng không?
- Có đảm bảo rằng việc mất kiến thức về kinh doanh do thuê khoán phần mềm sẽ không xảy ra?
- Có khả năng để thực hiện dịch vụ thuê khoán nội bộ?
- Có thể đảm bảo tính liên tục của hoạt động kinh doanh nếu nhà cung cấp không thể cung cấp dịch vụ tại bất kỳ thời điểm nào/trong tương lai?

Tài liệu yêu cầu

- Tài liệu quy trình liên quan tới phương thức lưu giữ quyền sở hữu quy trình kinh doanh, giữ lại kiến thức kinh doanh
- Tài liệu về quy trình kinh doanh, thiết kế hệ thống, dữ liệu, phần mềm ứng dụng.
- Hợp đồng giữa nhà thầu và đơn vị
- Các thỏa thuận dịch vụ (SLA) Các văn bản liên quan tới kiến thức kinh doanh, dữ liệu, phần mềm ứng dụng, thiết kế hệ thống
- Danh sách nhân viên của đơn vị tham gia vào quy trình cập nhật hệ thống

- Danh sách các dịch vụ liên quan đến quyền sở hữu hệ thống và dữ liệu.
- Biên bản cuộc họp với nhà thầu

Đánh giá thiết kế và triển khai

▪ Phòng vấn lãnh đạo CNTT của đơn vị về phương thức lưu giữ quyền sở hữu quy trình kinh doanh, giữ lại kiến thức kinh doanh. Đảm bảo đơn vị có ghi nhận các yêu cầu về quyền sở hữu kinh doanh, kiến thức kinh doanh trong hợp đồng hoặc các thỏa thuận dịch vụ. -Phòng vấn lãnh đạo CNTT của đơn vị về việc đào tạo nhân viên về quy trình kinh doanh, thiết kế hệ thống, dữ liệu, phần mềm ứng dụng.

▪ Phòng vấn lãnh đạo CNTT của đơn vị về khả năng thực hiện thuê khoán tại chỗ, khả năng tiếp tục tự hoạt động/tiếp tục xây dựng các chức năng quan trọng nếu nhà thầu hoặc nhà cung cấp không thể tiếp tục cung cấp dịch vụ

Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán và thực hiện các thủ tục sau:

- Thu thập hợp đồng/thỏa thuận để đánh giá rằng quyền sở hữu của quá trình, dữ liệu và phần mềm ứng dụng được duy trì bởi tổ chức thông qua các điều khoản phù hợp trong hợp đồng.
- Thu thập tài liệu để đánh giá kiến thức kinh doanh, dữ liệu, phần mềm ứng dụng, thiết kế hệ thống được tài liệu hóa đầy đủ và nhân viên được cập nhật thường xuyên thông qua đào tạo v.v...
- Thu thập tài liệu để đánh giá tổ chức và nhân viên của mình tham gia vào bất kỳ bản cập nhật hệ thống do cơ quan bên ngoài thực hiện và tài liệu cập nhật hệ thống được cung cấp cho tổ chức.
- Tài liệu để đánh giá rằng không có sự cố hoặc tranh chấp với nhà cung cấp dịch vụ liên quan đến quyền sở hữu hệ thống và dữ liệu.
- Xem xét biên bản cuộc họp với nhà thầu để đảm bảo rằng nếu có bất kỳ rủi ro lớn nào thì nó cũng được quản lý và theo dõi để đảm bảo tính liên tục của hoạt động.

Thử nghiệm hiệu quả hoạt động

Dựa trên số lượng hợp đồng, tiến hành lấy mẫu và xác minh các vấn đề sau:

▪ Đơn vị có quy định quyền sở hữu quy trình kinh doanh, dữ liệu và phần mềm ứng dụng được giữ lại đơn vị thông qua các điều khoản phù hợp trong hợp đồng hay

không Các kiến thức liên quan tới quy trình kinh doanh, dữ liệu, phần mềm ứng dụng, thiết kế hệ thống chi tiết được tài liệu hóa đầy đủ và nhân viên được cập nhật thường xuyên thông qua đào tạo định kỳ

- Đơn vị và nhân viên của đơn vị tham gia vào tất cả các bản cập nhật hệ thống do nhà thầu bên ngoài thực hiện và tài liệu cập nhật hệ thống được cung cấp đầy đủ cho đơn vị.

- Không có sự cố hoặc tranh chấp với nhà cung cấp dịch vụ liên quan đến quyền sở hữu hệ thống và dữ liệu. Xem xét biên bản cuộc họp với nhà thầu để đảm bảo rằng nếu có bất kỳ rủi ro lớn nào thì nó cũng được quản lý và theo dõi để đảm bảo khả năng hoạt động liên tục của đơn vị.

Vấn đề A4.07 - Kiểm soát và quản lý chi phí với đối tác

Mục tiêu kiểm toán

- Chi phí thuê khoán trong suốt thời gian hợp đồng đạt được hiệu quả kinh tế cao nhất.
- Các phân tích về chi phí và lợi ích phải mang tính thực tế và dựa vào các chương trình đang được đơn vị kiểm soát và quản lý.

Kiểm soát A4.07.01 – Kiểm soát và quản lý chi phí với đối tác

Tiêu chí kiểm toán

Kiểm soát nhằm đảm bảo đơn vị đạt được lợi ích kinh tế trong suốt thời gian hợp đồng thuê khoán bằng việc trả lời:

- Các chi phí (bao gồm cả các chi phí trong tương lai) dành cho thuê khoán đã được xác định chưa?
- Phân tích chi phí-lợi ích đã được thực hiện và lựa chọn đã là tối ưu nhất hay chưa?
- Xác định trách nhiệm trong tổ chức về việc thuê khoán và họ đã xác định được các yếu tố chi phí quan trọng và các tác động được xây dựng trong hợp đồng thuê khoán không?
- Có phải tính chi phí bổ sung hoặc chi phí leo thang cho đại lý?

Tài liệu yêu cầu

- Tài liệu liên quan tới kiểm soát và quản lý chi phí của đơn vị cho từng dịch vụ thuê khoán;

- Các báo cáo phân tích chi phí lợi nhuận và có lấy bản phân tích chi phí lợi nhuận;

- Các tài liệu liên quan quản lý leo thang;
- Bảng ước lượng chi phí cho hợp đồng thuê khoán;
- Báo cáo giám sát về các chức năng/hoạt động.

Đánh giá thiết kế và triển khai

- Thỏa thuận dịch vụ
- Các yêu cầu chi phí bổ sung/tăng giá bởi nhà cung cấp dịch vụ.
- Hợp đồng giữa nhà cung cấp dịch vụ và đơn vị
- Phòng vận lãnh đạo CNTT về cách kiểm soát và quản lý chi phí của đơn vị cho từng dịch vụ thuê khoán. Tất cả các chi phí (bao gồm cả các chi phí trong tương lai) dành cho thuê khoán đã được xác định chưa? Đơn vị có thực hiện phân tích chi phí lợi nhuận và có lấy bản phân tích chi phí lợi nhuận làm cơ sở trong quá trình lựa chọn nhà cung cấp hay không?

- Phòng vận lãnh đạo CNTT về cách xử lý trong trường hợp phát sinh chi phí bổ sung/chi phí leo thang. Trong trường hợp nào chi phí phát sinh thêm/chi phí leo thang được tính cho đại lý cung cấp dịch vụ?

Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán và thực hiện các thủ tục sau:

- Thu thập bảng phân tích chi phí lợi ích đã được phê duyệt và đánh giá tính thực tế của nó.
- Thu thập các ước lượng chi phí cho hợp đồng thuê khoán nhằm đảm bảo tất cả chi phí đã được nhận diện bởi tổ chức, rà soát và chấp thuận bởi lãnh đạo.
- Xem xét và ghi nhận quá trình lựa chọn của nhà cung cấp dịch vụ đối với yếu tố chi phí, quá trình phê duyệt các tài liệu liên quan đến lựa chọn
- Thu thập và rà soát các trường hợp của chi phí bổ sung/leo thang chi phí bởi nhà cung cấp dịch vụ. Xem xét lại bảng so sánh chi phí ước tính so với chi phí thực tế trong hợp đồng nhằm nhận diện các nguyên nhân.
- Báo cáo giám sát về các chức năng/hoạt động cụ thể đối với các chi phí bổ sung/chi phí leo thang được tìm kiếm.

- Thu thập hợp đồng và thỏa thuận dịch vụ để phân tích điều khoản, điều kiện, đánh giá về tổng chi phí được thể hiện trên hợp đồng và không có chi phí ẩn nào bao gồm cả chi phí trong tương lai.

- Tài liệu hành động về yêu cầu chi phí bổ sung/tăng giá bởi nhà cung cấp dịch vụ.

Thử nghiệm hiệu quả hoạt động

Dựa trên số lượng hợp đồng và thỏa thuận dịch vụ, Kiểm toán viên nhà nước tiến hành chọn mẫu và xác minh các vấn đề sau:

- Rà soát bản phân tích chi phí lợi nhuận ban đầu xem tất cả các chi phí (bao gồm các chi phí trong tương lai) đã được xác định đầy đủ, xem xét và phê duyệt bởi các bên liên quan hay chưa?

- Rà soát quy trình lựa chọn và phê duyệt nhà cung cấp để xác minh xem việc lựa chọn nhà cung cấp có dựa trên yếu tố chi phí hay bản phân tích chi phí lợi nhuận không?

- Rà soát hợp đồng để bảo đảm tất cả các chi phí được thể hiện trên hợp đồng và không có chi phí ẩn nào bao gồm cả chi phí trong tương lai

- Rà soát chi tiêu so với ngân sách sẵn có để bảo đảm đơn vị luôn xem xét chi tiêu trong mối liên hệ với ngân sách

- Đối với các khoản mục gây thay đổi chi phí/phát sinh chi phí/leo thang chi phí cần đánh giá sự cần thiết của thay đổi thông qua các báo cáo giám sát.

- Rà soát lại hành động của đơn vị liên quan tới chi phí bổ sung/chi phí leo thang bởi nhà cung cấp dịch vụ để bảo đảm các hành động của đơn vị là phù hợp theo quy định trong hợp đồng

Vấn đề A4.08 - SLA với đối tác

Mục tiêu kiểm toán:

SLA của đơn vị được xây dựng ở mức độ chi tiết, liệt kê tất cả các yêu cầu của đơn vị và là cơ sở để giám sát hoạt động của nhà cung cấp.

Kiểm soát A4.08.01 – SLA với đối tác hợp lý, đầy đủ

Tiêu chí kiểm toán

SLA là cơ sở để giám sát và kiểm soát nhà thầu/nhà cung cấp đối với các yêu cầu kỹ thuật và yêu cầu khác. Mức độ đầy đủ của Hợp đồng cung cấp dịch vụ dựa vào:

- Hợp đồng các dịch vụ đã thỏa thuận giữa tổ chức và nhà cung cấp dịch vụ?

- Hợp đồng các dịch vụ có đủ chi tiết để xác định tất cả vai trò và trách nhiệm giữa tổ chức và nhà cung cấp dịch vụ không?

- Hợp đồng các dịch vụ đã được thực hiện một cách tối ưu?
- Tổ chức có cơ chế giám sát việc thực hiện Hợp đồng các dịch vụ không?
- Có cơ chế để giải quyết các ngoại lệ đối với Hợp đồng các dịch vụ không?

Tài liệu yêu cầu

- Thỏa thuận dịch vụ giữa nhà cung cấp dịch vụ và đơn vị
- Tài liệu liên quan tới việc tuân thủ các thỏa thuận dịch vụ của nhà cung cấp
- Tài liệu yêu cầu kỹ thuật, các yêu cầu khác
- Thỏa thuận hoặc hợp đồng cấp dịch vụ/Bảng liệt kê trách nhiệm của tổ chức và nhà cung cấp

- Bộ tài liệu quy định cơ sở đánh giá mức độ hiệu quả

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo CNTT của đơn vị để xác định xem thỏa thuận dịch vụ có được coi là cơ sở dùng để đánh giá mức độ hiệu quả, là cơ sở giám sát nhà cung cấp bên ngoài dựa vào các yêu cầu kỹ thuật và các yêu cầu khác được quy định trong thỏa thuận khi triển khai các dịch vụ cho đơn vị

- Phòng văn lãnh đạo CNTT của đơn vị về mức độ chi tiết của thỏa thuận dịch vụ, thỏa thuận dịch vụ có bao hàm tất cả các yêu cầu của người sử dụng cũng như đủ chi tiết để xác định tất cả các trách nhiệm và vai trò của đơn vị cũng như của nhà cung cấp dịch vụ

- Phòng văn lãnh đạo CNTT của đơn vị để xác định xem đơn vị có các cơ chế nào để giám sát việc thực hiện thỏa thuận dịch vụ của nhà cung cấp. Ví dụ như yêu cầu nhà cung cấp báo cáo tiến độ/hiệu quả công việc định kỳ, thường xuyên. Rà soát thỏa thuận dịch vụ đảm bảo các cơ chế giám sát dịch vụ được xác lập và thống nhất và có những chế tài cụ thể giữa đơn vị và nhà cung cấp dịch vụ

Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán sau và thực hiện các thủ tục:

- Tài liệu yêu cầu kỹ thuật, các yêu cầu khác (danh sách các dịch vụ sẽ được thực hiện bởi nhà cung cấp) để đánh giá rằng tất cả các yêu cầu của người sử dụng được dịch sang các yêu cầu ở cấp độ dịch vụ.

- Thỏa thuận hoặc hợp đồng cấp dịch vụ/Bảng liệt kê trách nhiệm của tổ chức và nhà cung cấp để đánh giá vai trò và trách nhiệm của tổ chức và nhà cung cấp dịch vụ được xác định và phân tích một cách rõ ràng
- Bộ tài liệu quy định cơ sở đo lường để đánh giá rằng các thông số cho các mức hiệu suất được xác định rõ ràng và bao gồm trong Hợp đồng các dịch vụ.
- Tài liệu để đánh giá cơ chế giám sát mức dịch vụ được xác lập và thống nhất giữa tổ chức và nhà cung cấp dịch vụ.
- Xem xét báo cáo tình trạng nhà cung cấp để đánh giá rằng các thông số trong SLA đang được nhà thầu báo cáo và được nhân viên thích hợp trong tổ chức xem xét.

Thử nghiệm hiệu quả hoạt động

Dựa trên các thỏa thuận dịch vụ, Kiểm toán viên nhà nước tiến hành chọn mẫu và xác minh các vấn đề sau:

- Đảm bảo vai trò và trách nhiệm của đơn vị và nhà cung cấp dịch vụ được xác định một cách rõ ràng trong thỏa thuận dịch vụ
- Đảm bảo tất cả các yêu cầu của người sử dụng được chuyển hóa thành các yêu cầu trong thỏa thuận dịch vụ
- Thỏa thuận dịch vụ bao gồm các thông số xác định được độ hiệu quả của nhà cung cấp dịch vụ (ví dụ như tên các chức năng, thời gian triển khai...)
- Xem xét báo cáo tiến độ của nhà cung cấp để đảm bảo các thông số trong thỏa thuận dịch vụ (SLA) đang được nhà thầu báo cáo, cập nhật thường xuyên và được nhân viên thích hợp trong tổ chức xem xét.
- Đơn vị có những hành động phù hợp đối với những sai lệch mà nhà cung cấp gây ra

Vấn đề A4.09 - Công tác bảo mật đối với đối tác

Mục tiêu kiểm toán:

Các yêu cầu bảo mật đã được đề ra khi làm việc với đối tác và được thực hiện tuân theo các quy định.

Kiểm soát A4.09.01 - Các yêu cầu bảo mật chính đáng của đơn vị đã được đưa vào hợp đồng thuê khoán bên ngoài.

Tiêu chí kiểm toán

Trùng với mục tiêu kiểm toán

Tài liệu yêu cầu

- Thỏa thuận dịch vụ hoặc hợp đồng với nhà cung cấp
- Các tài liệu liên quan tới việc giám sát truy cập của nhà cung cấp dịch vụ
- Danh sách các phần mềm, ứng dụng, hệ thống mà nhà cung cấp được phép truy cập tại đơn vị

Đánh giá thiết kế và triển khai

- Phòng vận lãnh đạo CNTT của đơn vị và kiểm tra xem đơn vị có các quy định cụ thể liên quan tới bảo mật thông tin khi thuê khoán bên ngoài hay không?
- Phòng vận lãnh đạo CNTT của đơn vị và xác minh xem các yêu cầu về bảo mật thông tin được truyền thông tới nhà cung cấp dịch vụ thông qua hình thức nào, có ghi nhận trong thỏa thuận dịch vụ (SLA) hoặc hợp đồng với nhà cung cấp hay không?
- Phòng vận lãnh đạo CNTT của đơn vị về việc bảo đảm tính tuân thủ bảo mật thông tin của nhà cung cấp dịch vụ
- Phòng vận lãnh đạo CNTT của đơn vị về phương án bảo mật cho các trung tâm sao lưu dữ liệu và trung tâm khôi phục dữ liệu. Đảm bảo đơn vị có nhật ký truy cập (vật lý và logic) cho việc truy cập dữ liệu, phần mềm ứng dụng và phần cứng tại các địa điểm trên cũng như các địa điểm bên ngoài.

Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán và thực hiện các thủ tục sau:

- Tài liệu để đánh giá rằng các yêu cầu về an toàn đã được xác định bởi tổ chức và được xây dựng trong hợp đồng thuê khoán phần mềm hoặc SLA
- Xác minh xem tổ chức có kiểm kê các tệp dữ liệu, phần mềm ứng dụng hay không?
- Xác minh rằng tổ chức giám sát/nhận thức được rằng trạng thái của các tệp dữ liệu, phần mềm ứng dụng và phần cứng được lưu giữ trong quá trình sao lưu và quá trình khôi phục dữ liệu được thực hiện bởi cơ quan bên ngoài.

- Xác minh xem tổ chức có đảm bảo cho phép bất kỳ thay đổi nào về dữ liệu, phần mềm ứng dụng và phần cứng của cơ quan bên ngoài.
- Xác minh xem tổ chức có đảm bảo về việc truy cập dữ liệu, phần mềm ứng dụng và phần cứng tại địa điểm bên ngoài thông qua nghiên cứu nhật ký truy cập (vật lý và logic).
- Xác minh xem tổ chức có đảm bảo về cơ chế bảo mật được đưa ra bởi nhà cung cấp dịch vụ.
- Xác minh xem tổ chức có nhận được báo cáo định kỳ và hành động về thông tin trong báo cáo giám sát.

Thử nghiệm hiệu quả hoạt động

Dựa trên số lượng thỏa thuận dịch vụ và hợp đồng, Kiểm toán viên nhà nước tiến hành chọn mẫu và xác minh các vấn đề sau:

- Đảm bảo các yêu cầu về bảo mật, báo cáo của nhà cung cấp dịch vụ về bảo mật thông tin được xác định rõ ràng và ghi nhận trong hợp đồng thuê khoán hoặc SLA.
- Có đầy đủ các báo cáo giám sát về các vấn đề bảo mật thông tin

Vấn đề A4.10 - Sao lưu và khôi phục sau sự cố đối với các dịch vụ thuê ngoài

Mục tiêu kiểm toán

Hợp đồng thuê khoán dịch vụ có các điều khoản về kế hoạch hoạt động liên tục (BCP) và kế hoạch phục hồi sau thảm họa (DRP).

Kiểm soát A4.10.01 - Kiểm soát đảm bảo nhà cung cấp dịch vụ đáp ứng đủ các điều kiện về các kế hoạch BCP và DRP

Tiêu chí kiểm toán

Trùng với mục tiêu kiểm toán

Tài liệu yêu cầu

- SLA
- Hợp đồng giữa nhà cung cấp dịch vụ và đơn vị
- Tài liệu liên quan đến kế hoạch BCP và DRP
- Các báo cáo liên quan được gửi từ nhà cung cấp
- Các báo cáo rà soát định kỳ của dự án

Đánh giá thiết kế và triển khai

- Phòng vấn lãnh đạo CNTT để xác minh xem đơn vị có đưa các yêu cầu về kế hoạch BCP và DRP vào thỏa thuận dịch vụ/hợp đồng khi ký hợp đồng với nhà cung cấp dịch vụ hay không?

- Phòng vấn lãnh đạo CNTT để xác minh xem đơn vị có tiến hành kiểm tra khả năng thực hiện kế hoạch hoạt động liên tục (BCP) và kế hoạch phục hồi sau thảm họa (DRP) của nhà cung cấp hay không?

Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán sau và thực hiện các thủ tục:

- Thu thập và xác định trên hợp đồng hoặc SLA có trình bày yêu cầu liên quan đến kế hoạch BCP và DRP cho các dữ liệu, ứng dụng và máy chủ được khoán cho nhà cung cấp.

- Xem lại hợp đồng hoặc SLA để đảm bảo rằng nhà cung cấp dịch vụ sẽ đưa ra các báo cáo kiểm toán độc lập hoặc báo cáo kiểm toán nội bộ xác nhận họ sẵn sàng thực hiện Kế hoạch BCP và DRP và nhà cung cấp có thực hiện thử nghiệm các quy trình của họ theo định kỳ.

- Xem lại các báo cáo đã gửi từ nhà cung cấp để đảm bảo việc thử nghiệm đã được thực hiện phù hợp với các điều kiện của hợp đồng và/hoặc SLA.

- Rà soát các báo cáo định kỳ để đảm bảo rằng các thủ tục đã được cập nhật (nếu cần).

Thử nghiệm hiệu quả hoạt động

Dựa trên số lượng thỏa thuận dịch vụ và hợp đồng, Kiểm toán viên nhà nước tiến hành chọn mẫu và xác minh các vấn đề sau:

- Đảm bảo hợp đồng có các điều khoản về BCP và DRP.
- Đảm bảo nhà cung cấp có đủ điều kiện đáp ứng các điều khoản trên hợp đồng.

7. Chuyên đề A5 - Chính sách hoạt động liên tục và khắc phục thảm họa

a. Giới thiệu chính sách hoạt động liên tục và khắc phục thảm họa

Các cơ quan chính phủ ngày càng phụ thuộc vào khả năng hoạt động chính xác và tính sẵn sàng của hệ thống CNTT để thực thi các quyền hạn theo pháp luật. Hệ thống CNTT đóng một vai trò quan trọng trong nhiều hoạt động như xác định và thu thuế xuất nhập khẩu tại các cơ quan hải quan, thanh toán lương hưu và các trợ cấp an sinh xã hội

của nhà nước, tập hợp, lên danh sách các chỉ số thống kê quốc gia (tỉ lệ sinh, tỉ lệ tử, tội phạm, bệnh tật, v.v...). Trong thực tế, nhiều hoạt động không thể thực hiện được một cách hiệu quả nếu không có sự hỗ trợ của CNTT.

Mất điện, đình công, hỏa hoạn hay các thảm họa bất ngờ đều có thể ảnh hưởng đến tính sẵn sàng của hệ thống CNTT. Điều này sẽ khiến đơn vị mất thời gian rất dài để tiếp tục hoạt động có hiệu quả trở lại nếu không có một kế hoạch hoạt động liên tục (BCP) khả thi giúp ứng phó để có thể khôi phục hoạt động nhanh nhất.

Thuật ngữ kế hoạch hoạt động liên tục (BCP-Business Continuity Plan) và kế hoạch khắc phục thảm họa (DRP-Disaster Recovery Plan) đôi khi được sử dụng đồng nghĩa nhưng trên thực tế là hai thuật ngữ riêng biệt bổ sung cho nhau. Cả hai kế hoạch này đều rất quan trọng đối với Kiểm toán viên nhà nước, bởi vì sự kết hợp của hai kế hoạch giúp đơn vị có thể đảm bảo khả năng hoạt động hiệu quả ở một mức nhất định khi xảy ra sự cố gián đoạn do thiên nhiên hoặc do con người gây ra. Hai nội dung trên được diễn giải như sau:

- Kế hoạch BCP: là quy trình tổ chức sử dụng để lên kế hoạch và kiểm tra khả năng phục hồi hoạt động của tổ chức khi xảy ra sự cố làm gián đoạn. Nó cũng mô tả cách thức đơn vị sẽ tiếp tục hoạt động dưới những điều kiện bất lợi có thể nảy sinh như thế nào (ví dụ thiên tai hoặc các thảm họa khác).
- Kế hoạch DRP: là quy trình lên kế hoạch và kiểm tra khả năng khôi phục cơ sở hạ tầng CNTT sau thiên tai hoặc thảm họa. Kế hoạch DRP có thể coi là một bộ phận của kế hoạch BCP. Tuy nhiên, kế hoạch BCP áp dụng cho chức năng hoạt động của tổ chức trong khi kế hoạch DRP hướng tới tài nguyên CNTT để hỗ trợ hoạt động của đơn vị.

Về bản chất, kế hoạch BCP xác định khả năng tiếp tục hoạt động của tổ chức khi hoạt động thông thường bị gián đoạn. Kế hoạch này kết hợp các chính sách, thủ tục và tình huống thực tiễn cho phép khôi phục và tiếp tục các quy trình quan trọng sau khi xảy ra thiên tai hoặc khủng hoảng. Bên cạnh việc chỉ rõ các hoạt động phải tuân theo trong trường hợp bị gián đoạn, một số kế hoạch hoạt động liên tục bao gồm các thành phần khác như khắc phục thảm họa, ứng phó khẩn cấp, khôi phục quyền người dùng, và các hoạt động quản lý trong tình trạng khẩn cấp và bất ngờ. Như vậy, trong các đơn vị hoạt

động liên tục được xem như một khái niệm bao gồm cả việc khắc phục thảm họa và việc kết nối lại các hoạt động.

Dù là một phần của kế hoạch BCP hay một tài liệu riêng biệt thì kế hoạch DRP thường đề cập đến các vấn đề về nguồn lực, hành động, nhiệm vụ và dữ liệu cần thiết để quy trình khôi phục của đơn vị diễn ra trơn tru. Kế hoạch DRP hỗ trợ đơn vị trong việc khôi phục các quy trình hoạt động bị ảnh hưởng bằng cách vạch ra các bước cụ thể mà đơn vị phải thực hiện. Cụ thể, kế hoạch DRP giúp đơn vị chuẩn bị trước và lập kế hoạch cần thiết để giảm thiểu thiệt hại và để đảm bảo sự sẵn sàng hoạt động cho các hệ thống thông tin quan trọng của đơn vị. Trong khái niệm của CNTT, kế hoạch DRP tập trung khôi phục các tài sản công nghệ quan trọng, bao gồm hệ thống phần mềm ứng dụng, CSDL, thiết bị lưu trữ và các tài nguyên mạng.

b. Rủi ro thường gặp

Việc xây dựng quy trình DRP, BCP chưa bao quát hết các nhiệm vụ quan trọng. Cụ thể, nếu việc khôi phục thảm họa cho một số chức năng/ứng dụng quan trọng bị chậm chễ, tính hoạt động liên tục của đơn vị sẽ bị ảnh hưởng. Đồng thời nếu vai trò, trách nhiệm và sự nhận thức của các nhân viên liên quan không rõ ràng, một kế hoạch dù có tốt cũng có thể không hiệu quả.

Hiệu quả khi thực thi các kế hoạch BCP và DRP phụ thuộc vào quy trình đánh giá các tác động tới hoạt động kinh doanh khi xảy ra thảm họa, kiểm tra diễn tập kế hoạch ứng phó cũng như đào tạo cho các nhân viên ban ngành liên quan. Đồng thời nếu không có đầy đủ các quy định về đảm bảo về an toàn, bảo mật thông tin trong các kế hoạch BCP và DRP, sẽ dẫn đến nguy cơ mất dữ liệu, mất thời gian và các chi phí khác do phục hồi không hiệu quả trong trường hợp thảm họa xảy ra.

Đối với các rủi ro liên quan trong trường hợp thuê khoán bên ngoài, nơi mà các kế hoạch BCP và DRP khó quản lý do không nằm trực tiếp dưới sự kiểm soát của đơn vị. Cụ thể là các nguy cơ về tính bảo mật của dữ liệu, xử lý trái phép và rò rỉ dữ liệu. Đồng thời, việc phụ thuộc khả năng hoạt động liên tục vào các nhà cung cấp dịch vụ thuê ngoài cũng khiến đơn vị đối mặt với các nguy cơ như việc mất bí quyết kinh doanh, quyền sở hữu quy trình, cũng như không thể thay đổi nhà cung cấp dịch vụ trong trường hợp năng lực kém và trong các trường hợp khác như việc phá sản hoặc thay đổi chủ diễn ra ở phía nhà cung cấp dịch vụ.

c. Các vấn đề kiểm toán thành phần

Các vấn đề kiểm toán thuộc chủ đề kiểm toán khả năng BCP và DRP bao gồm:

- Vấn đề A5.01 - Chính sách BCP nhằm đánh giá đơn vị có thiết lập chính sách BCP hiệu quả hay không?
- Vấn đề A5.02 - Tổ chức thực hiện kế hoạch BCP nhằm đánh giá đơn vị có tổ chức các bộ phận/đội thực hiện kế hoạch.
- Vấn đề A5.03 - Đánh giá mức độ quan trọng các nghiệp vụ nhằm đánh giá việc đơn vị có thứ tự ưu tiên nghiệp vụ rõ ràng và có phương án khôi phục theo thứ tự ưu tiên phù hợp nhất.
- Vấn đề A5.04 - Kế hoạch DRP nhằm kiểm tra kế hoạch BCP đã đề cập đến kế hoạch DRP với các thủ tục cùng biện pháp khắc phục hiệu quả như sao lưu dự phòng dữ liệu, hệ thống máy chủ dự phòng ...
- Vấn đề A5.05 – Kiểm soát môi trường vật lý nhằm kiểm tra việc đơn vị có tiến hành các công tác kiểm soát môi trường vật lý phù hợp nhằm hạn chế các rủi ro khi thảm họa hoặc các sự cố diễn ra.
- Vấn đề A5.06 - Kiểm toán công tác tài liệu hóa các kế hoạch BCP và DRP nhằm đảm bảo các kế hoạch được soạn thảo và ban hành với các tài liệu được phê duyệt rõ ràng.
- Vấn đề A5.07 - Diễn tập, kiểm tra kế hoạch BCP và DRP nhằm đảm bảo sự sẵn sàng, mức độ tuân thủ cùng tính khả thi của các kế hoạch trên.
- Vấn đề A5.08 - Bảo mật khi xảy ra các thảm họa nhằm đảm bảo các thông tin quan trọng vẫn được bảo mật khi có thảm họa xảy ra.
- Vấn đề A5.09 - Lưu trữ dự phòng và khôi phục dịch vụ bên ngoài sau thảm họa nhằm đảm bảo các đối tác tham gia cung cấp dịch vụ cũng có vai trò trong việc khắc phục sau thảm họa.

d. Chương trình kiểm toán mẫu

Vấn đề A5.01 - Chính sách hoạt động liên tục (BCP)

Mục tiêu kiểm toán:

Đánh giá tính hiệu quả của kế hoạch và chính sách dự phòng của đơn vị.

Kiểm soát A5.01.01 - Đơn vị có kế hoạch và chính sách dự phòng đảm bảo sự hoạt động liên tục.

Tiêu chí kiểm toán

Đơn vị có kế hoạch và chính sách dự phòng được ban hành chính thức? Nếu có kế hoạch, chính sách đó có hoạt động hiệu quả hay không?

Tài liệu yêu cầu

- Các tài liệu về kế hoạch BCP của đơn vị.
- Các báo cáo biên bản họp xác minh kế hoạch BCP.
- Bảng chứng liên quan tới việc phổ biến, chia sẻ tài liệu BCP cho nhân viên trong đơn vị.

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo CNTT của đơn vị để xác minh: Đơn vị có thiết lập kế hoạch/chính sách dự phòng đảm bảo tính hoạt động liên tục của đơn vị hay không? Thu thập tài liệu về kế hoạch hoạt động liên tục và xác minh các tài liệu này được rà soát, xem xét và phê duyệt bởi các cấp lãnh đạo.
- Phòng văn lãnh đạo CNTT/nhân sự của đơn vị để xác minh tính hiệu quả của kế hoạch, chính sách đó đối với tính hoạt động liên tục của đơn vị.
- Thu thập các báo cáo, biên bản họp xác minh kế hoạch, chính sách đã được áp dụng vào thực tế hay chưa? Nếu có, thì các thủ tục áp dụng có theo đúng kế hoạch, chính sách dự phòng đó không?
- Phòng văn lãnh đạo CNTT để xác minh tài liệu đảm bảo tính hoạt động liên tục của đơn vị đó có được phổ biến tới các nhân sự trong đơn vị hay chỉ một số các bộ phận quan trọng? Nếu có, đơn vị áp dụng hình thức nào để phổ biến cho nhân sự liên quan (như gửi email thông báo, chia sẻ tài liệu lên các thư mục chung, website của đơn vị...)
- Thu thập bằng chứng liên quan tới việc phổ biến, chia sẻ tài liệu cho nhân viên trong đơn vị
- Phỏng vấn một số nhân viên nhằm đánh giá xem liệu chính sách có được tuyên truyền, phổ biến đầy đủ trong nội bộ đơn vị không?
- Rà soát tài liệu thu thập để đánh giá chính sách hoạt động liên tục của đơn vị đã đáp ứng các yêu cầu về hoạt động liên tục.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề A5.02 - Tổ chức kế hoạch BCP

Mục tiêu kiểm toán:

Đánh giá đội ngũ nhân sự đảm bảo tính hoạt động liên tục.

Kiểm soát A5.02.01 - Đơn vị có một đội ngũ nhân sự đảm bảo tính hoạt động liên tục khi có sự cố xảy ra.

Tiêu chí kiểm toán

Đội ngũ nhân sự đảm bảo tính hoạt động liên tục của đơn vị bao quát được hết các hoạt động quan trọng của tổ chức. Đội ngũ này luôn sẵn sàng hành động đảm bảo tính hoạt động liên tục của đơn vị khi có sự cố xảy ra.

Tài liệu yêu cầu

- Sơ đồ tổ chức đội ngũ nhân sự đảm bảo tính hoạt động liên tục của đơn vị.
- Giấy tờ/biên bản các cuộc họp về kế hoạch BCP.
- Kế hoạch BCP.
- Bảng chứng liên quan tới kiến thức chuyên môn của các thành viên trong nhóm.

Đánh giá thiết kế và triển khai

▪ Phòng văn lãnh đạo CNTT của đơn vị để xác minh danh sách các cá nhân tham gia và chịu trách nhiệm trực tiếp tới tính hoạt động liên tục của tổ chức? Vai trò trách nhiệm của mỗi thành viên trong nhóm. Rà soát và xác minh kiến thức chuyên môn của các thành viên trong nhóm đáp ứng được các yêu cầu công việc liên quan tới bảo đảm tính hoạt động liên tục của đơn vị.

▪ Rà soát sơ đồ tổ chức đội ngũ nhân sự đảm bảo tính hoạt động liên tục của đơn vị và xác minh vai trò, trách tương ứng của các cá nhân trong đội ngũ đó. Xác minh kiến thức chuyên môn của các thành viên trong nhóm đáp ứng được các yêu cầu công việc liên quan tới bảo đảm tính hoạt động liên tục của đơn vị.

▪ Rà soát giấy tờ/biên bản của các cuộc họp về kế hoạch hoạt động liên tục trong việc phân công vai trò trách nhiệm

- Rà soát Kế hoạch đảm bảo tính hoạt động liên tục để xác minh vai trò và nhiệm vụ của các cá nhân bộ phận đã được xác định rõ ràng.

- Phỏng vấn một số nhân sự chịu trách nhiệm về đảm bảo tính hoạt động liên tục của đơn vị và kiểm chứng xem họ có nhận thức được vai trò, nhiệm vụ và các thủ tục cần thực hiện nếu có sự cố xảy ra hay không?

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề A5.03 - Đánh giá các tác động, rủi ro tới hoạt động của đơn vị.

Mục tiêu kiểm toán:

Đánh giá các tác động, rủi ro tới hoạt động của đơn vị.

Kiểm soát A5.03.01 - Đơn vị thực hiện đánh giá các tác động, rủi ro tới hoạt động của đơn vị. Đơn vị triển khai hệ thống QLRR.

Tiêu chí kiểm toán

- Đơn vị có thực hiện đánh giá các tác động (bên trong, bên ngoài), rủi ro tới hoạt động của đơn vị.
- Đảm bảo hệ thống QLRR của đơn vị hoạt động một cách hiệu quả.

Tài liệu yêu cầu

- Các văn bản liên quan tới việc đánh giá các tác động, rủi ro ảnh hưởng tới hoạt động của đơn vị
 - Danh sách các phòng ban liên quan tham gia
 - Tài liệu để đánh giá tác động khẩn cấp tới hoạt động của đơn vị
 - Biên bản xử lý các rủi ro quan trọng được ưu tiên
 - Các biên bản liên quan tới việc đánh giá các tác động, rủi ro ảnh hưởng tới hoạt động của đơn vị

Đánh giá thiết kế và triển khai

- Phỏng vấn ban lãnh đạo CNTT để xác minh đơn vị có thực hiện đánh giá các tác động, rủi ro có thể ảnh hưởng tới hoạt động của đơn vị hay không. Tìm hiểu quy trình đánh giá ảnh hưởng của đơn vị.

- Rà soát các văn bản liên quan tới việc đánh giá các tác động, rủi ro ảnh hưởng tới hoạt động của đơn vị để xác minh xem các tác động, rủi ro này đã được phân công xử lý hoặc có áp dụng các biện pháp giảm thiểu mức độ ảnh hưởng và được theo dõi, cập nhật tình hình thường xuyên.

- Phòng văn ban lãnh đạo CNTT để xác định các bộ phận, phòng ban liên quan tham gia việc đánh giá, trách nhiệm và nghĩa vụ tương ứng của các bộ phận phòng ban đó trong quy trình đánh giá các ảnh hưởng của các tác động rủi ro tới hoạt động của đơn vị.

- Rà soát danh sách các phòng ban liên quan, xác minh vai trò và trách nhiệm của họ trong việc đánh giá các ảnh hưởng của các tác động, rủi ro tới hoạt động của đơn vị.

- Rà soát tài liệu để đánh giá tác động khẩn cấp tới hoạt động của đơn vị. Rà soát các rủi ro quan trọng có được ưu tiên xử lý hợp lý và kịp thời (ví dụ việc xử lý đúng theo quy trình đánh giá ảnh hưởng của rủi ro của đơn vị, các phòng ban liên quan phối hợp cùng đánh giá, các biện pháp lí được thực hiện nhanh chóng và kịp thời)

- Rà soát các biên bản liên quan tới các tác động, rủi ro ảnh hưởng tới hoạt động của đơn vị để xác minh xem các tác động, rủi ro này đã được phân công xử lý hoặc có áp dụng các biện pháp giảm thiểu mức độ ảnh hưởng, và được theo dõi, cập nhật tình hình thường xuyên.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát A5.03.02 - Quy trình QLRR bao quát việc đánh giá về ảnh hưởng của tác động, rủi ro. Các rủi ro hoặc các trường hợp khẩn cấp được ưu tiên xử lý kịp thời.

Tiêu chí kiểm toán

- Quy trình QLRR có bao quát việc đánh giá về ảnh hưởng của tác động, rủi ro hay không?

- Các rủi ro hoặc các trường hợp khẩn cấp có được ưu tiên xử lý nhanh chóng, kịp thời hay không?

Tài liệu yêu cầu

- Quy trình QLRR của đơn vị.

- Quy trình giải quyết rủi ro của đơn vị
- Danh sách nhân sự chịu trách nhiệm trong QLRR cùng với vai trò nhiệm vụ của họ.
- Danh sách các rủi ro, trường hợp khẩn cấp mà đơn vị đã giải quyết và chưa giải quyết trong giai đoạn kiểm toán.
- Các biên bản họp đánh giá, giải quyết rủi ro

Đánh giá thiết kế và triển khai

- Phòng vấn ban lãnh đạo CNTT về quy trình QLRR của đơn vị. Tìm hiểu các thủ tục tiến hành trong việc xác định các rủi ro, các trường hợp khẩn cấp cần ưu tiên được giải quyết ngay. Đồng thời tìm hiểu các thủ tục giải quyết của đơn vị, đánh giá các rủi ro, trường hợp khẩn cấp có được đơn vị giải quyết một cách nhanh chóng, kịp thời hay không?
- Thu thập các tài liệu liên quan tới các vấn đề cần được ưu tiên giải quyết cao, xác minh quy trình QLRR có xử lý được tất cả các vấn đề đó không? Phòng vấn ban lãnh đạo CNTT để tìm hiểu và nắm được danh sách nhân sự trực tiếp tham gia, chịu trách nhiệm trong QLRR và vai trò nhiệm vụ của họ.
- Thu thập tài liệu để đánh giá xem tất cả các nhân sự có liên quan, bao gồm cả việc xác minh của ban quản lý cấp cao cho nhân sự đó trong việc nhận thức được vai trò và trách nhiệm của mình thực hiện QLRR đảm bảo tính hoạt động liên tục cho đơn vị hay không?
- Phòng vấn ban lãnh đạo CNTT để nắm được danh sách các rủi ro, trường hợp khẩn cấp mà đơn vị đã giải quyết và chưa giải quyết trong giai đoạn kiểm toán. Thu thập tài liệu về các rủi ro, trường hợp khẩn cấp có được xử lý một cách hợp lý không?
- Thu thập các biên bản họp hay danh sách rủi ro để xác định xem các rủi ro này đã được phân công xử lý, các biện pháp giảm thiểu đã được xác định và rủi ro đã được theo dõi và cập nhật thường xuyên.
- Phòng vấn một vài cá nhân trong ban QLRR, xác minh xem họ có ý thức được vai trò, trách nhiệm của mình trong ban QLRR hay không?

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động (nếu cần thiết) nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề A5.04 - Kế hoạch phục hồi sau thảm họa (DRP)

Mục tiêu kiểm toán:

Đánh giá kế hoạch BCP bao gồm kế hoạch sao lưu và khôi phục phần cứng, dữ liệu, phần mềm ứng dụng và trung tâm dữ liệu (khôi phục).

Kiểm soát A5.04.01 - Thiết lập và thực hiện các thủ tục sao lưu dữ liệu, chương trình.

Tiêu chí kiểm toán

Đảm bảo kế hoạch hoạt động liên tục bao gồm kế hoạch sao lưu và khôi phục phần cứng, dữ liệu, phần mềm ứng dụng và trung tâm dữ liệu (khôi phục). Các nội dung đó được đơn vị thực hiện một cách đầy đủ và thích hợp.

Tài liệu yêu cầu

- Quy trình sao lưu và khôi phục các dữ liệu
- Tài liệu xác minh lịch sao lưu dữ liệu, cách thức sao lưu dữ liệu
- Tài liệu xác minh các thiết lập cảnh báo của hệ thống nếu như có sự cố liên quan tới việc sao lưu khôi phục dữ liệu
- Nhật ký kiểm thử việc khôi phục dữ liệu trên dữ liệu đã sao lưu
- Nhật ký sao lưu dữ liệu
- Các tài liệu, báo cáo liên quan tới sự cố, thảm họa ảnh hưởng tới quy trình sao lưu và khôi phục dữ liệu

Đánh giá thiết kế và triển khai

- Phòng vấn lãnh đạo CNTT, tìm hiểu về nhân sự chịu trách nhiệm trong quy trình sao lưu và khôi phục các dữ liệu quan trọng của đơn vị và đơn vị có tài liệu chính thức quy định về chính sách và thủ tục sao lưu
- Phòng vấn nhân sự liên quan, xem xét quan sát trực tiếp các cấu hình trên hệ thống xác minh lịch thực hiện sao lưu, thời gian kiểm thử khôi phục dữ liệu, loại sao lưu (sao lưu một phần, sao lưu nhiều phần...), cơ chế giám sát kết quả sao lưu (tự động hay thủ công?)

- Rà soát các tài liệu được thu thập xác minh lịch sao lưu dữ liệu, cách thức sao lưu dữ liệu (sao lưu một phần hay sao lưu toàn phần...) và các thủ tục thực hiện trong quá trình sao lưu dữ liệu.

- Rà soát các tài liệu được thu thập các thiết lập cảnh báo của hệ thống nếu như có sự cố liên quan tới việc sao lưu khôi phục dữ liệu (ví dụ Email gửi kết quả sao lưu, kiểm thử khôi phục dữ liệu về email, cảnh báo khi có sự cố xảy ra)

- Phỏng vấn nhân sự liên quan, tìm hiểu và xem xét cách hệ thống ghi lại lịch sử sao lưu và khôi phục dữ liệu.

- Rà soát các tài liệu được thu thập, nhật ký sao lưu dữ liệu xác minh việc sao lưu có được thực hiện đầy đủ không, đúng với thời gian và yêu cầu sao lưu dữ liệu hay không? (ví dụ sao lưu một phần hàng ngày lúc 2 giờ sáng, sao lưu toàn phần lúc 4 giờ sáng vào chủ nhật hàng tuần ...)

- Rà soát các tài liệu được thu thập, nhật ký kiểm thử việc khôi phục dữ liệu trên dữ liệu đã sao lưu

- Phỏng vấn lãnh đạo CNTT xác minh phiên bản sao lưu dữ liệu chính được sao lưu một cách an toàn và sẵn sàng được sử dụng trong trường hợp xảy ra sự cố về dữ liệu.

- Thu thập các tài liệu, báo cáo liên quan tới sự cố, thảm họa ảnh hưởng tới quy trình sao lưu và khôi phục dữ liệu, xác minh đơn vị có thực hiện đánh giá ảnh hưởng của sự cố thảm họa đó và có thực hiện các biện pháp khắc phục hiệu quả, kịp thời hay không?

Thử nghiệm hiệu quả hoạt động

Dựa vào quy trình sao lưu và các biên bản ghi lại lịch sao lưu, Kiểm toán viên nhà nước tiến hành chọn mẫu và thu thập bằng chứng xác minh kết quả thực hiện sao lưu của các mẫu được chọn thành công hay thất bại. Với các mẫu thất bại thì công tác xử lý sau đó ra sao?

Vấn đề A5.05 - Kiểm soát môi trường vật lý

Mục tiêu kiểm toán:

Xác định đơn vị có các kiểm soát môi trường.

Kiểm soát A5.05.01 - Các kiểm soát môi trường như mất điện cháy nổ, bão lũ...

Tiêu chí kiểm toán

Ngăn ngừa, phòng tránh và giảm thiểu các rủi ro liên quan tới môi trường như mất điện, cháy nổ, bão lũ...

Tài liệu yêu cầu

- Các văn bản liên quan đến nguồn điện dự phòng trong trường hợp xảy ra thảm họa; thiết bị phòng cháy chữa cháy; kiểm soát độ ẩm; nhiệt độ; điện áp, đặc biệt tại các khu vực quan trọng
- Kế hoạch phòng chống lũ lụt
- Các tài liệu ghi chép về việc đơn vị đã thực hiện, khắc phục sự cố do môi trường.

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phỏng vấn ban lãnh đạo CNTT tìm hiểu về các kiểm soát môi trường mà đơn vị thiết lập (như mất điện, phòng chống cháy nổ, phòng chống bão lũ...);
- Thu thập và xác minh nguồn điện dự phòng trong trường hợp xảy ra thảm họa
- Thu thập và xác minh thông tin các thiết bị phòng cháy chữa cháy của đơn vị sẵn sàng hoạt động trong trường hợp có thảm họa cháy nổ xảy ra;
- Thu thập thông tin về việc kiểm soát độ ẩm, nhiệt độ, điện áp đặc biệt tại các khu vực quan trọng;
- Thu thập thông tin về việc đơn vị thiết lập hệ thống phòng chống lũ lụt (nếu có tùy thuộc vào đặc điểm hoạt động của đơn vị, ví dụ vị trí của đơn vị gần các vùng hay có mưa bão lớn);
- Phỏng vấn ban lãnh đạo CNTT tìm hiểu về các thủ tục và đơn vị đã thực hiện để giảm thiểu rủi ro, khắc phục sự cố từ môi trường (nếu có);
- Thu thập các tài liệu ghi chép về việc đơn vị đã thực hiện, khắc phục sự cố từ môi trường (nếu có).

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề A5.06 - Công tác tài liệu hóa các kế hoạch BCP và DRP

Mục tiêu kiểm toán:

Xác minh kế hoạch khôi phục sau thảm họa được ban hành chính thức, cập nhật và phổ biến.

Kiểm soát A5.06.01 - Kế hoạch DRP được ban hành chính thức, cập nhật và phổ biến

Tiêu chí kiểm toán

Kiểm soát đảm bảo kế hoạch khôi phục sau thảm họa được đơn vị ban hành chính thức, rà soát cập nhật định kỳ, được sao lưu và lưu trữ và luôn sẵn sàng được sử dụng khi có thảm họa

Tài liệu yêu cầu

- Tài liệu về kế hoạch hoạt động liên tục và kế hoạch phục hồi sau thảm họa (phiên bản mới nhất)
- Các bằng chứng liên quan tới việc phổ biến các kế hoạch trên tới toàn thể nhân viên trong đơn vị

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phỏng vấn ban lãnh đạo CNTT và tìm hiểu kế hoạch hoạt động liên tục và kế hoạch phục hồi sau thảm họa có được ban hành chính thức, rà soát cập nhật định kỳ, được sao lưu và lưu trữ và luôn sẵn sàng được sử dụng khi có thảm họa.
- Tìm hiểu và nắm được các nội dung chính trong các bản kế hoạch đó. Tìm hiểu cách thức đơn vị phổ biến, truyền thông các kế hoạch đó tới nhân viên trong đơn vị (ví dụ: tài liệu kế hoạch được chia sẻ trên các thư mục chung hoặc trên website chung của đơn vị)
- Rà soát bản kế hoạch hoạt động liên tục (phiên bản mới nhất) bao gồm nội dung về vai trò và trách nhiệm của các nhân sự chính trong việc đảm bảo kế hoạch hoạt động liên tục;
- Thu thập kế hoạch khắc phục thảm họa (phiên bản mới nhất) bao gồm nội dung về vai trò và trách nhiệm của các nhân sự chính trong kế hoạch khắc phục thảm họa được thực thi (khi có thảm xảy ra). Phỏng vấn một số nhân sự để đánh giá xem liệu họ có hiểu và nắm bắt các thủ tục khắc phục thảm họa không?

- Thu thập các bằng chứng liên quan tới việc phổ biến các kế hoạch trên tới toàn thể nhân viên trong đơn vị (gửi email thông báo, chia sẻ trên các thư mục chung, đăng tải trên các website chung của đơn vị)
- Xác minh việc các kế hoạch trên được sao lưu và lưu trữ off-site nhằm đảm bảo bản kế hoạch luôn sẵn sàng được sử dụng khi có thảm họa xảy ra

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề A5.07 - Thử nghiệm các thủ tục trong kế hoạch BCP và DRP

Mục tiêu kiểm toán:

Xác minh các thủ tục trong kế hoạch BCP và DRP có được kiểm tra thử nghiệm.

Kiểm soát A5.07.01 - Đơn vị tiến hành kiểm tra thử nghiệm các thủ tục trong kế hoạch BCP và DRP.

Tiêu chí kiểm toán

Đảm bảo các thủ tục trong kế hoạch hoạt động liên tục và khôi phục sau thảm họa của đơn vị được thử nghiệm trước khi áp dụng thực tế. Giúp bộ phận, nhân sự liên quan ý thức được vai trò của họ trong việc thực hiện các thủ tục đảm bảo tính tục của hoạt động đơn vị

Tài liệu yêu cầu

- Chính sách, kế hoạch tiến hành kiểm tra thử nghiệm kế hoạch BCP và DRP
- Các bằng chứng liên quan tới việc thử nghiệm thường xuyên của đơn vị
- Danh sách các tiêu chí đánh giá kết quả thử nghiệm
- Các báo cáo tổng kết khuyến nghị, bài học rút ra được sau cuộc thử nghiệm.

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phỏng vấn ban lãnh đạo CNTT, tìm hiểu về việc liệu đơn vị có thực hiện các việc tiến hành thử nghiệm các thủ tục trong kế hoạch BCP và DRP ;
- Rà soát kế hoạch BCP và DRP của đơn vị, thu thập các thủ tục tiến hành thử nghiệm và đối chiếu mức độ bao quát của các thủ tục thử nghiệm với các thủ tục được xác định trong các bản kế hoạch.

- Phòng văn ban lãnh đạo CNTT để xác minh mức độ thường xuyên của việc thử nghiệm kế hoạch BCP và DRP (hàng năm hay hàng 2 năm thực hiện một lần)
- Thu thập và đánh giá các bằng chứng liên quan tới việc thử nghiệm thường xuyên của đơn vị
- Phòng văn ban lãnh đạo CNTT, tìm hiểu về các tiêu chí đánh giá kết quả của cuộc thử nghiệm đồng thời tìm hiểu về các bài học, kinh nghiệm rút ra sau cuộc thử nghiệm đó
- Thu thập danh sách các tiêu chí đánh giá kết quả thử nghiệm
- Thu thập các báo cáo tổng kết khuyến nghị, bài học rút ra được sau cuộc thử nghiệm.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề A5.08 - An toàn thông tin liên quan đến BCP và DCP

Mục tiêu kiểm toán:

Trong quá trình thực hiện các thủ tục sao lưu của kế hoạch khôi phục sau thảm họa, dữ liệu bảo mật cho CSDL, phần mềm ứng dụng, phần cứng, trung tâm dữ liệu được bảo đảm an toàn.

Kiểm soát A5.08.01 - Các kế hoạch BCP và DRP đảm bảo mật cho CSDL, phần mềm ứng dụng, phần cứng và trung tâm dữ liệu của đơn vị.

Tiêu chí kiểm toán

Dữ liệu bảo mật cho CSDL, phần mềm ứng dụng, phần cứng, trung tâm dữ liệu được bảo đảm an toàn trong quá trình thực hiện các thủ tục sao lưu của kế hoạch khôi phục sau thảm họa.

Tài liệu yêu cầu

- Quy trình/hướng dẫn việc bảo đảm an toàn cho các dữ liệu bảo mật, phần mềm ứng dụng, phần cứng và trung tâm dữ liệu trong kế hoạch BCP và DRP.
- Các danh sách các dữ liệu, phần mềm ứng dụng, phần cứng để xác định các dữ liệu cần được bảo vệ.
- Nhật ký sao lưu dữ liệu.

- Nhật ký kiểm soát truy cập.

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phòng vấn lãnh đạo CNTT tìm hiểu về quy trình/hướng dẫn việc bảo đảm an toàn cho các dữ liệu bảo mật, phần mềm ứng dụng, phần cứng và trung tâm dữ liệu trong kế hoạch hoạt động liên tục và kế hoạch khôi phục sau thảm họa của đơn vị
- Kiểm toán viên nhà nước tiến hành thu thập danh sách các dữ liệu, phần mềm ứng dụng, phần cứng để xác định các dữ liệu cần được bảo vệ trong suốt quá trình sao lưu và kiểm tra khôi phục dữ liệu, đánh giá vị trí sao lưu và vị trí khôi phục thảm họa.
- Phòng vấn lãnh đạo CNTT xác minh xem trong suốt quá trình sao lưu hoặc kiểm tra khôi phục dữ liệu, các dữ liệu bảo mật, phần mềm/phần cứng, trung tâm dữ liệu có phải chịu bất cứ sự thay đổi nào không?
- Kiểm toán viên nhà nước thu thập nhật ký sao lưu dữ liệu, kiểm tra và xác minh xem có sự thay đổi nào trong quá trình sao lưu, kiểm tra tính khôi phục của dữ liệu.
- Xác minh xem có bất kỳ sự vi phạm bảo mật nào thông qua việc kiểm tra nhật ký kiểm soát truy cập (vật lý và logic).

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề A5.09 - Sao lưu và khắc phục thảm họa cho các dịch vụ thuê ngoài

Mục tiêu kiểm toán:

Đánh giá các dịch vụ thuê ngoài có đảm bảo kế hoạch hoạt động liên tục và khôi phục thảm họa.

Kiểm soát A5.09.01 - Kiểm soát quy trình sao lưu và khắc phục thảm họa cho các dịch vụ thuê ngoài

Tiêu chí kiểm toán

Nhằm đánh giá xem liệu các dịch vụ thuê ngoài đảm bảo các kế hoạch hoạt động liên tục và khôi phục thảm họa.

Tài liệu yêu cầu

- Các thỏa thuận cung cấp dịch vụ giữa đơn vị và đối tác bên ngoài

- Nhật ký kiểm soát truy cập về các tệp dữ liệu, phần cứng, phần mềm ứng dụng với đối tác thuê ngoài
- Các kết quả thử nghiệm về kế hoạch sao lưu và kế hoạch khắc phục thảm họa tại tổ chức thuê ngoài
- Các tài liệu ghi chép về các rủi ro gắn với khả năng tiếp quản nhà cung ứng dịch vụ.

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phòng vấn ban lãnh đạo CNTT để tìm hiểu về các kế hoạch hoạt động liên tục và kế hoạch phục hồi sau thảm họa đối với các dịch vụ thuê ngoài và vấn đề này có được nêu trong thỏa thuận cung cấp dịch vụ không, các thủ tục của đơn vị khi đánh giá dữ liệu và chương trình của đơn vị sau khi sao lưu và khôi phục sau thảm họa.
- Rà soát các thỏa thuận cung cấp dịch vụ giữa đơn vị và đối tác để xác minh các nội dung chịu trách nhiệm sao lưu/khắc phục thảm họa của đối tác bên ngoài.
- Thu thập nhật ký kiểm soát truy cập về các tệp dữ liệu, phần cứng, phần mềm ứng dụng của đối tác thuê ngoài, rà soát các điều khoản hợp đồng và đánh giá sự truy cập của đối tác vào phần cứng, các phần mềm ứng dụng là được cho phép.
- Phòng vấn ban lãnh đạo, tìm hiểu, rà soát các kết quả thử nghiệm về kế hoạch sao lưu và kế hoạch khắc phục thảm họa tại tổ chức thuê ngoài. Rà soát việc đơn vị xác định tính toàn vẹn của dữ liệu và chương trình trong quy trình sao lưu và khôi phục thảm họa tại tổ chức thuê ngoài.
- Rà soát và thu thập các tài liệu xem liệu đơn vị có xác định được rằng thử nghiệm về sao lưu và khôi phục thảm họa có được đảm bảo tại tổ chức thuê ngoài. Rà soát và thu thập các tài liệu xem liệu đơn vị có nhận thức được các rủi ro gắn với các khả năng tiếp quản nhà cung ứng dịch vụ.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

8. Chuyên đề A6 - An toàn thông tin

a. Giới thiệu về an toàn thông tin

An toàn thông tin (ATTT) là khả năng của một hệ thống có thể bảo vệ thông tin và các nguồn tài nguyên để đảm bảo tính bảo mật và toàn vẹn. Cụ thể là:

- Bảo vệ thông tin và hệ thống thông tin chống lại sự truy cập và sửa đổi thông tin trái phép (kể cả trong lưu trữ, xử lý, hoặc trao đổi thông tin dữ liệu) nhưng phải luôn sẵn sàng cấp quyền truy cập cho người sử dụng hợp pháp.
- Những biện pháp cần thiết để đo lường, phát hiện, ghi nhận và chống lại các mối đe dọa thông tin.
- Bảo vệ cơ sở hạ tầng CNTT khỏi những người dùng trái phép.

ATTT bao gồm an toàn sử dụng máy tính và an toàn trong việc trao đổi thông tin.

Quản trị CNTT phải triển khai các giải pháp ATTT để đảm bảo tính sẵn sàng, tính tin cậy và tính toàn vẹn của hệ thống. ATTT rất quan trọng trong một tổ chức, vì giữ vai trò kiểm soát mọi tài sản CNTT. Vì vậy, cần phải triển khai ATTT song hành với các mục tiêu của tổ chức đáp ứng các tiêu chuẩn cần thiết. Thông tin được cung cấp cho những cá nhân có thẩm quyền kiểm soát, bảo vệ thông tin khỏi những người không có thẩm quyền.

b. Rủi ro thường gặp

Dưới đây là một số rủi ro phổ biến trong một tổ chức bất kỳ:

- Tiết lộ trái phép thông tin.
- Sửa đổi trái phép hoặc tiêu hủy thông tin.
- Bị bên ngoài xâm nhập vào lỗ hổng ATTT.
- Hệ thống nghiệp vụ không thể truy cập do yếu tố kỹ thuật.
- Hệ thống CNTT bị ngừng hoạt động do bị tấn công.
- Thông tin dữ liệu bị đánh cắp.

Nguyên nhân của các rủi ro trên xuất phát từ việc:

- Các chiến lược ATTT không phù hợp với trình độ CNTT hoặc yêu cầu nghiệp vụ.
- Các chính sách ATTT không được áp dụng thống nhất dẫn tới việc triển khai các biện pháp khác nhau gây nên xung đột, kẽ hở cho các sai phạm.

- Không thực hiện tuân thủ các yêu cầu an toàn bảo mật thông tin
- Công tác ATTT không kiểm soát quá trình bảo trì và phát triển sản phẩm để lọt các lỗ hổng ATTT.
- Thiết kế kiến trúc CNTT không hiệu quả Các biện pháp bảo mật và quản lý tài sản CNTT ở mức độ vật lý chưa phù hợp và đầy đủ.
- Cấu hình phần mềm ứng dụng, hệ thống phần cứng không đáp ứng đủ yếu tố an toàn bảo mật.
- Việc tổ chức và triển khai quy trình ATTT và HTTT không rõ ràng hoặc gây nhầm lẫn.
- Nhân sự CNTT còn yếu kém, chưa đáp ứng đủ yêu cầu đề ra. Việc đầu tư cho ATTT không hiệu quả chưa phù hợp với nhu cầu phát triển của đơn vị
- Không thực hiện giám sát ATTT hoặc công tác giám sát không thực hiện hiệu quả.

c. Các vấn đề kiểm toán thành phần

Các vấn đề kiểm toán thuộc chủ đề ATTT bao gồm:

- Vấn đề A60100 – Quản lý rủi ro ATTT nhằm đảm bảo các rủi ro ATTT được nhận diện và có phương án giảm thiểu hoặc hạn chế rủi ro.
- Vấn đề A60200 - Chính sách ATTT nhằm đảm bảo chính sách ATTT được ban hành, phổ biến đến tất cả nhân viên trong đơn vị, mọi người có trách nhiệm tuân thủ chính sách ATTT.
- Vấn đề A60300 - Chính sách bảo mật nhằm đảm bảo việc trao đổi thông tin nội bộ, với đối tác, nhà thầu và các đơn vị bên ngoài an toàn và bảo mật.
- Vấn đề A60400 - Bảo mật trao đổi thông tin và vận hành hệ thống nhằm đảm bảo tất cả thông tin trao đổi cũng như việc vận hành hệ thống đều được bảo đảm an toàn.
- Vấn đề A60500 - Quản lý tài sản CNTT nhằm đảm bảo toàn bộ tài sản CNTT được quản lý hợp lý.
- Vấn đề A60600 – Nâng cao nhận thức người dùng về ATTT nhằm đảm bảo nhận thức người dùng về ATTT được lên kế hoạch và thực hiện.
- Vấn đề A60700 – Bảo mật vật lý các tài sản CNTT nhằm đảm bảo đơn vị thiết lập cơ chế, hệ thống kiểm soát an toàn thông tin ở mức độ vật lý.

- Vấn đề A60800 - Quản lý việc truy cập vào hệ thống CNTT được kiểm soát hợp lý theo đúng chức năng nghiệp vụ của người dùng và phân quyền hợp lý.

d. Chương trình kiểm toán mẫu

Vấn đề A6.01 – Quản lý rủi ro an toàn thông tin

Mục tiêu kiểm toán:

Đảm bảo các rủi ro liên quan tới ATTT được nhận diện và đơn vị có phương án giảm thiểu rủi ro.

Kiểm soát A6.01.01 -Ban hành chính thức cơ chế đánh giá rủi ro ATTT.

Tiêu chí kiểm toán

Nhằm đảm bảo rằng các rủi ro liên quan tới ATTT được nhận diện và có phương án giảm thiểu rủi ro thích hợp.

Tài liệu yêu cầu

- Chính sách ATTT
- Các thủ tục chính thức về QLRR
- Danh sách nhân sự tham gia đánh giá rủi ro
- Báo cáo định kỳ về việc đánh giá rủi ro
- Biên bản cuộc họp khi xảy ra sự cố rủi ro

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phỏng vấn cán bộ chuyên trách tìm hiểu về quy trình/thủ tục quản lý và đánh giá rủi ro của đơn vị. Xác minh đơn vị có thực hiện đánh giá, phân tích rủi ro và có biện pháp ngăn ngừa, phòng tránh và khắc phục hậu quả.

Kiểm toán viên nhà nước thu thập các tài liệu sau:

- Chính sách ATTT
- Các thủ tục chính thức về QLRR
- Rà soát các tài liệu liên quản lý rủi ro, tài liệu phân tích đánh giá rủi ro xác minh:
 - Vai trò của đơn vị trong thủ tục đánh giá rủi ro;
 - Nguồn nhân lực tham gia vào quá trình đánh giá rủi ro;
 - Xác minh việc đánh giá rủi ro có được thực hiện và ghi chép định kỳ hoặc khi điều kiện thay đổi

Kiểm toán viên nhà nước tiến hành rà soát và xác minh các vấn đề sau:

- Rà soát tài liệu mô tả về những rủi ro trọng yếu đối với hệ thống, hoạt động kinh doanh, cơ sở hạ tầng của đơn vị
- Trong trường hợp không có thủ tục và các tài liệu đánh giá rủi ro, không nên đánh giá thấp các kiểm soát được thiết lập sẵn trong các quy trình hoạt động của đơn vị cần xác định cơ chế kiểm soát bổ sung hoạt động hiệu quả bằng cách đưa ra ví dụ cụ thể về hoạt động của kiểm soát này.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát A6.01.02 - Tất cả các rủi ro trọng yếu được nhận diện, xem xét và đánh giá

Tiêu chí kiểm toán

Kiểm soát, kiểm tra việc thực hiện đánh giá rủi ro (bao hàm tất cả các rủi ro trọng yếu) và đánh giá ảnh hưởng của những sai phạm ATTT

Tài liệu yêu cầu

- Quy trình đánh giá rủi ro;
- Tài liệu đánh giá rủi ro;
- Danh mục rủi ro;
- Các báo cáo xử lý sự cố.

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phỏng vấn lãnh đạo CNTT về hướng dẫn, quy trình đánh giá rủi ro, việc thực thi đánh giá rủi ro như thế nào?
- Phỏng vấn lãnh đạo CNTT về quy trình đánh giá ảnh hưởng khi có những sai phạm ATTT được phát hiện

Kiểm toán viên nhà nước tiến hành rà soát và xác minh các vấn đề sau:

- Rà soát tài liệu để kiểm tra xem liệu việc đánh giá rủi ro có được đơn vị thực hiện đầy đủ và toàn diện hay không?

- Rà soát các tài liệu đánh giá rủi ro đảm bảo tính thiết kế đánh giá rủi ro cho tính đầy đủ, phù hợp, kịp thời và có thể lường trước được.
- Rà soát các báo cáo xử lý sự cố và các tài liệu về rủi ro được định nghĩa trước xác minh đơn vị có thực hiện đánh giá rủi ro.
- Rà soát các sự cố đã xảy ra, xác minh xem các dữ liệu thu thập được về các sự cố trực tiếp trên hệ thống như: ID người dùng, loại sự kiện, dữ liệu và thời gian, kết quả thành công hay thất bại, nguồn gốc sự kiện, định danh hoặc tên của đối tượng bị ảnh hưởng.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát A6.01.03 - Đơn vị áp dụng các biện pháp giảm thiểu rủi ro phù hợp.

Tiêu chí kiểm toán

Mục tiêu của kiểm soát kiểm tra liệu đơn vị có thực hiện các biện pháp giảm thiểu rủi ro một cách hiệu quả và tối ưu đối với các rủi ro trọng yếu

Tài liệu yêu cầu

- Quy trình đơn vị thực hiện các biện pháp giảm thiểu rủi ro đối với các rủi ro trọng yếu
- Các báo cáo xử lý vấn đề/sự cố;
- Các báo cáo hoạt động định kỳ (trong trường hợp sự cố chưa được giải quyết, ảnh hưởng tới hoạt động của doanh nghiệp)

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phỏng vấn cán bộ chuyên trách về quy trình đơn vị thực hiện các biện pháp giảm thiểu rủi ro đối với các rủi ro trọng yếu

Kiểm toán viên nhà nước thu thập các tài liệu sau:

- Các báo cáo xử lý vấn đề/sự cố;
- Các báo cáo hoạt động định kỳ (trong trường hợp sự cố chưa được giải quyết, ảnh hưởng tới hoạt động của doanh nghiệp như thế nào?)

Kiểm toán viên nhà nước tiến hành rà soát và xác minh các vấn đề sau:

- Rà soát các báo cáo xử lý các sự cố và xác minh các thủ tục được áp dụng phòng ngừa, phát hiện và giảm thiểu rủi ro và các tài liệu có được ghi chép lưu trữ đầy đủ hay không?

- Rà soát sự cố nghiêm trọng, rủi ro đi kèm của các sự cố này và xác minh cách áp dụng các biện pháp giảm thiểu rủi ro đó. Rà soát sự cố vẫn còn tồn đọng chưa được giải quyết, xác minh lý do của việc xử lý chậm trễ.

- Rà soát báo cáo định kỳ về ảnh hưởng trực tiếp/gián tiếp của các sự cố chưa được giải quyết tới hoạt động của đơn vị (nếu có).

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề A6.02 - Chính sách bảo mật Công nghệ thông tin

Mục tiêu kiểm toán:

Đánh giá đơn vị có chính sách ATTT được rà soát phê duyệt bởi lãnh đạo cấp cao và được phổ biến tới toàn thể nhân viên.

Kiểm soát A6.02.01: Ban hành chính thức chính sách ATTT và nhất quán với kế hoạch bảo mật CNTT.

Tiêu chí kiểm toán

- Chính sách ATTT của đơn vị được ban hành, rà soát phê duyệt bởi lãnh đạo cấp cao và hỗ trợ kế hoạch bảo mật CNTT
- Chính sách ATTT của đơn vị được phổ biến rộng rãi tới toàn thể nhân viên.

Tài liệu yêu cầu

- Chính sách ATTT (bản cứng hoặc bản scan)
- Tài liệu đào tạo về ATTT cho nhân viên mới
- Tiêu chí đánh giá, báo cáo kết quả đào tạo về ATTT cho nhân viên mới
- Email, thông báo từ ban lãnh đạo liên quan tới vấn đề ATTT

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phòng vấn lãnh đạo CNTT về vai trò của ATTT trong đơn vị cũng như việc ban hành chính thức chính sách ATTT Phòng vấn lãnh đạo CNTT của đơn vị để xác minh đơn vị có thực hiện rà soát, cập nhật Chính sách ATTT thường xuyên hay không?

- Phòng vấn lãnh đạo CNTT để xác minh Chính sách ATTT có được phổ biến tới toàn thể nhân viên trong đơn vị hay không?

- Phòng vấn lãnh đạo CNTT về việc đào tạo cho nhân viên mới về Chính sách ATTT, cùng với tiêu chí đánh giá kiểm tra nhận thức của nhân viên mới về ATTT tại đơn vị.

- Phòng vấn lãnh đạo CNTT về các thông báo/cảnh báo từ ban lãnh đạo tới toàn thể đơn vị khi có sự cố ATTT xảy ra.

Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán sau:

- Thu thập Chính sách ATTT (bản cứng hoặc bản scan)
- Thu thập tài liệu đào tạo về ATTT cho nhân viên mới
- Thu thập tiêu chí đánh giá, báo cáo kết quả đào tạo về ATTT cho nhân viên mới
- Thu thập email, thông báo từ ban lãnh đạo liên quan tới vấn đề ATTT
- Kiểm toán viên nhà nước tiến hành rà soát và xác minh các vấn đề sau:
- Rà soát tài liệu chiến lược CNTT về việc đề cập tới vai trò quan trọng của ATTT.
- Rà soát kế hoạch an toàn CNTT và kiểm tra xem tài liệu có bao gồm các kế hoạch tác nghiệp CNTT, phân loại dữ liệu, các tiêu chuẩn công nghệ, các chính sách an toàn và kiểm soát và QLRR.

- Xác minh Chính sách ATTT được ban hành đã được rà soát và phê duyệt bởi các cấp lãnh đạo. Chính sách ATTT được rà soát thường xuyên (thông thường, một năm sẽ rà soát lại một lần và cập nhật nếu cần thiết)

- Rà soát nội dung Chính sách ATTT có bao hàm ít nhất các nội dung như: tầm quan trọng của ATTT đối với tổ chức; chính sách mật khẩu; chính sách truy cập vào các thiết bị mạng, máy tính; quy định về cấp phát/xóa bỏ quyền truy cập đối với người dùng...

- Rà soát tài liệu đào tạo cho nhân viên mới có bao gồm các nội dung chính trong Chính sách ATTT.

- Xác minh về việc phổ biến Chính sách ATTT được phổ biến tới tất cả nhân viên (cũ và mới). Chính sách được đưa lên những thư mục chung/website chung của đơn vị để nhân viên có đọc, tìm hiểu và sử dụng dễ dàng.

- Đánh giá về cảnh báo ATTT cho toàn bộ nhân viên được thực hiện một cách kịp thời và hiệu quả.

Thử nghiệm hiệu quả hoạt động

Lấy mẫu và kiểm tra:

- Dựa vào số lượng nhân viên mới trong năm: Kiểm toán viên nhà nước tiến hành chọn mẫu kiểm tra báo cáo tỉ lệ nhân viên được đào tạo, kết quả đào tạo, tỉ lệ phần trăm nhân viên hoàn thành ATTT theo tiêu chí đánh giá của đơn vị.

- Đối với nhân viên đang làm việc: xác minh xem nhân viên đó có thể dễ dàng tìm và đọc hiểu các thông tin về ATTT trên thư mục chung hoặc website của đơn vị.

Kiểm soát A6.02.02 - Đơn vị có yêu cầu cam kết không tiết lộ các thông tin cần được bảo vệ đối với người dùng nội bộ và đối tác bên ngoài.

Tiêu chí kiểm toán

Tổ chức có thể kiểm soát bảo vệ các thông tin nhạy cảm liên quan tới đối tác và các đơn vị liên quan

Tài liệu yêu cầu

- Cam kết bảo mật thông tin
- Hợp đồng giữa đơn vị và đối tác bên ngoài Các báo cáo về các trường hợp vi phạm bảo mật (nếu có)

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phỏng vấn lãnh đạo CNTT của đơn vị để xác minh: Đơn vị có yêu cầu nhân viên thực hiện cam kết bảo mật thông tin hay không? Trong kỳ kiểm toán, có trường hợp nhân viên vi phạm cam kết bảo mật thông tin không? Nếu có, cách xử lý như thế nào.

- Phỏng vấn lãnh đạo CNTT của đơn vị để xác minh: Đơn vị có yêu cầu đối tác/nhà thầu thực hiện cam kết bảo mật thông tin giữa đơn vị và đối tác/nhà thầu hay không? Trong giai đoạn kiểm toán, có trường hợp nhà thầu/đối tác vi phạm bảo mật thông tin giữa đơn vị và nhà thầu hay không? Nếu có, đưa ra cách xử lý của đơn vị.

Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán sau:

- Cam kết bảo mật thông tin
- Hợp đồng giữa đơn vị và đối tác bên ngoài

- Các báo cáo về các trường hợp vi phạm bảo mật (nếu có)

Kiểm toán viên nhà nước tiến hành rà soát và xác minh các vấn đề sau:

- Rà soát cam kết bảo mật thông tin được ký và xác nhận bởi nhân viên công ty (thông thường ban cam kết được ký ngay trong ngày làm việc chính thức của nhân viên).
- Rà soát các bản hợp đồng giữa đơn vị với các nhà thầu đối tác và xem xét trong đó có bao gồm các thỏa thuận về trách nhiệm và nghĩa vụ của các đơn vị đối tác khi sử dụng tài sản cũng như truy cập vào tài nguyên thông tin của đơn vị
- Rà soát báo cáo vi phạm bảo mật thông tin, đồng thời kiểm tra, đánh giá các hành động của cấp quản lý với các hành vi vi phạm (nếu có).

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề A6.03 - Cơ cấu tổ chức của bộ phận An toàn thông tin

Mục tiêu kiểm toán:

Đảm bảo đơn vị có bộ phận chuyên trách bảo mật CNTT.

Kiểm soát A6.03.01 - Chính sách CNTT quy định rõ ràng vai trò và nghĩa vụ của bộ phận CNTT

Tiêu chí kiểm toán

Đơn vị có bộ phận chuyên trách bảo mật CNTT với vai trò và nhiệm vụ được định nghĩa rõ ràng.

Tài liệu yêu cầu

- Sơ đồ cấu trúc tổ chức ban CNTT
- Quy định nội bộ về an toàn hệ thống CNTT;
- Mô tả công việc của từng vị trí;
- Biên bản về các cuộc họp với những người liên quan về việc phân công trách nhiệm của nhân viên/phòng ban trong việc bảo đảm ATTT

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phòng văn lãnh đạo CNTT của đơn vị về trách nhiệm và nghĩa vụ của ban CNTT (hoặc ban ATTT nếu có). Các nội dung này có được ban hành dưới dạng văn bản hoặc thông báo chính thức hay không?

- Phòng văn lãnh đạo CNTT của đơn vị để đánh giá mức độ ưu tiên và chú trọng của đơn vị về vấn đề ATTT

Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán sau:

- Sơ đồ cấu trúc tổ chức ban CNTT
- Quy định nội bộ về an toàn hệ thống CNTT;
- Mô tả công việc của từng vị trí;
- Biên bản về các cuộc họp với những người liên quan về việc phân công trách nhiệm của nhân viên/phòng ban trong việc bảo đảm ATTT.

Kiểm toán viên nhà nước tiến hành rà soát và xác minh các vấn đề sau:

- Rà soát sơ đồ cấu trúc tổ chức ban CNTT, mô tả nhiệm vụ chính, Quy định nội bộ về ATTT để xác minh vai trò nhiệm vụ của họ trong việc bảo đảm ATTT có chính thức và được trình bày một cách rõ ràng dễ hiểu không

- Rà soát các biên bản họp liên quan để xác minh trách nhiệm bảo đảm ATTT được rà soát và giao cho các cá nhân/phòng ban và trách nhiệm tương ứng.

- Xác minh quy trình, cách thức ban lãnh đạo quan tâm tới vấn đề ATTT trong đơn vị

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát A6.03.02 - Sự phối hợp khi thực hiện các hoạt động CNTT giữa phòng ban liên quan một cách hiệu quả

Tiêu chí kiểm toán

Sự phối hợp khi thực hiện các hoạt động CNTT giữa phòng ban liên quan một cách hiệu quả

Tài liệu yêu cầu

- Sơ đồ cấu trúc tổ chức ban CNTT
- Các yêu cầu pháp luật về việc phân loại thông tin

- Các quy định nội bộ về ATTT
- Biên bản cuộc họp của hội đồng ATTT
- Các báo cáo lỗi

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phỏng vấn lãnh đạo CNTT của đơn vị liệu có bất kỳ sự xung đột/trùng lặp/hay khoảng trống giữa các thủ tục/quy trình thực hiện ATTT giữa các phòng ban hay không
- Phỏng vấn cấp lãnh đạo CNTT về việc nhận thức bất cứ vấn đề về phối hợp hoạt động ATTT trong tổ chức
- Phỏng vấn lãnh đạo CNTT của đơn vị liệu có bất kỳ sự xung đột/trùng lặp/hay khoảng trống giữa các thủ tục/quy trình thực hiện ATTT giữa các phòng ban hay không?

Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán sau:

- Sơ đồ cấu trúc tổ chức ban CNTT
- Yêu cầu pháp luật về việc phân loại thông tin
- Các quy định nội bộ về ATTT
- Biên bản cuộc họp của hội đồng ATTT
- Các báo cáo lỗi

Kiểm toán viên nhà nước tiến hành rà soát và xác minh các vấn đề sau:

- Rà soát các văn bản, theo dõi thực tế để xác minh liệu có bất kỳ sự xung đột/trùng lặp/hay khoảng trống giữa các thủ tục/quy trình thực hiện ATTT giữa các phòng ban
- Rà soát quy trình thực hiện để xác minh xem có bất kỳ bước thực hiện nào dẫn tới việc truyền thông tin ra bên ngoài nhưng không được kiểm soát trách nhiệm.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề A6.04 - Bảo mật trao đổi thông tin nội bộ và bên ngoài

Mục tiêu kiểm toán

Đảm bảo việc trao đổi thông tin nội bộ và bên ngoài được an toàn.

Kiểm soát A6.04.01 - Đơn vị có ban hành quy định/chính sách về việc trao đổi thông tin nội bộ và bên ngoài một cách an toàn và hiệu quả

Tiêu chí kiểm toán

Nhằm đảm bảo việc trao đổi thông tin nội bộ và bên ngoài được an toàn.

Tài liệu yêu cầu

- Tài liệu chính thức về quy định trao đổi thông tin
- Bảng chứng xác minh tài liệu được phổ biến tới các nhân viên trong đơn vị
- Báo cáo, tài liệu liên quan tới việc xử lý các vi phạm

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

▪ Phỏng vấn lãnh đạo CNTT của đơn vị để xác minh: đơn vị có ban hành tài liệu về việc trao đổi thông tin? Tài liệu được có được phổ biến cho tất cả nhân viên trong đơn vị hay không? Tần suất rà soát và cập nhật quy trình.

▪ Phỏng vấn lãnh đạo CNTT của đơn vị để xác minh trong giai đoạn kiểm toán có trường hợp nào vi phạm trao đổi các thông tin không? Nếu có, cách xử lý của ban quản lý là gì?

▪ Phỏng vấn một số người dùng ở các vị trí khác nhau để xem họ có nắm được về thủ tục và nội dung trao đổi thông tin.

Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán sau:

- Tài liệu chính thức về quy định trao đổi thông tin
- Báo cáo, tài liệu liên quan tới việc xử lý các vi phạm

Kiểm toán viên nhà nước tiến hành rà soát và xác minh các vấn đề sau:

- Rà soát tài liệu về việc trao đổi thông tin;
- Xác minh tài liệu về việc chia sẻ thông tin có được phổ biến cho các nhân viên trong đơn vị (tài liệu được chia sẻ trên các thư mục chung hoặc website của đơn vị);
- Xác minh nhận thức của một số người dùng ở các vị trí khác nhau để xem họ có nắm được về chính sách và thủ tục trao đổi thông tin hay không?

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát A6.04.02 - Vận hành mạng được quản lý và thực hiện đảm bảo tính an toàn và hiệu quả.

Tiêu chí kiểm toán

Quản lý và kiểm soát rủi ro thông tin trên mạng.

Tài liệu yêu cầu

- Danh sách các thông tin bị hạn chế (ví dụ như danh sách các website bị chặn truy cập)
- Nhật ký quản trị mạng (ví dụ nhật ký tường lửa)
- Báo cáo phân tích nhật ký quản trị mạng (nếu có)

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phòng văn lãnh đạo CNTT của đơn vị về chính sách kiểm soát thông tin và xác minh: các công cụ thiết bị phần cứng/phần mềm mà đơn vị sử dụng cho việc giám sát và phân tích hoạt động người dùng thông qua mạng nội bộ và mạng Internet (tường lửa, phần mềm phòng chống Spam, phần mềm diệt virus...)
- Phòng văn lãnh đạo CNTT của đơn vị để xác minh: các công cụ thiết bị phần cứng/phần mềm mà đơn vị sử dụng có phát hiện và ghi lại những xâm nhập, tấn công trên mạng lưới; sự xâm nhập tấn công được phân tích đánh giá bởi chuyên gia góp phần đảm bảo ATTT trước những tấn công xâm nhập và tấn công trên mạng lưới.
- Phòng văn lãnh đạo CNTT, tìm hiểu cách thức bảo đảm an toàn cho việc truyền tải thông tin qua mạng lưới chung (Internet). Ví dụ như việc lưu hành/thông báo văn bản, thủ tục cho người dùng truy cập, sử dụng thông tin trên các trang thương mại điện tử/giao dịch trực tuyến.
- Phòng văn lãnh đạo CNTT, xác minh xem đơn vị có thực hiện các thủ tục mã hóa dữ liệu trước khi gửi thông tin cho đơn vị bên ngoài (khách hàng, đối tác, nhà thầu ...) hay không? Nếu có kỹ thuật mã hóa đơn vị sử dụng là gì (mã hóa đối xứng/mã hóa bất đối xứng).

Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán sau:

- Danh sách các thông tin bị hạn chế (ví dụ như danh sách các website bị chặn truy cập);
- Nhật ký quản trị mạng (ví dụ nhật ký tường lửa);

- Báo cáo phân tích nhật ký quản trị mạng (nếu có);

Kiểm toán viên nhà nước tiến hành rà soát và xác minh các vấn đề sau:

- Xác minh: các công cụ thiết bị phần cứng/phần mềm mà đơn vị sử dụng như: tường lửa, phần mềm phòng chống Spam, phần mềm diệt virus... có phát hiện và ghi lại những xâm nhập, tấn công trên mạng lưới.
- Xác minh: thống kê số lượng và các cuộc tấn công mã độc như: spam, hacking hay các phần mềm độc hại và bản đánh giá phân tích mức độ ảnh hưởng của các cuộc tấn công đó (nếu có) và các phản ứng của đơn vị trước các tấn công đó; Rà soát bản phân tích đánh giá của gia về các phát hiện xâm nhập, tấn công trên mạng lưới (nếu có).
- Rà soát các số lượng các cuộc tấn công mã độc như: spam, hacking hay các phần mềm độc hại và xác minh các phản ứng kịp thời của đơn vị.
- Xác minh cách thức bảo đảm an toàn cho việc truyền tải thông tin qua mạng lưới chung (Internet).
- Xác minh xem đơn vị có thực hiện các thủ tục mã hóa dữ liệu, kỹ thuật mã hóa dữ liệu mà đơn vị sử dụng để mã hóa thông tin trước khi gửi thông tin cho đơn vị bên ngoài (khách hàng, đối tác, nhà thầu ...). Nếu có, xác minh hoạt động hiệu quả của kiểm soát mã hóa thông tin (Quy trình quản lý "khóa key" mã hóa, việc hủy "khóa-key" mã hóa, phân quyền nắm giữ "khóa-key" "mã hóa"

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát A6.04.03 - Ban hành và thực thi quy trình quản lý cấu hình phù hợp.

Tiêu chí kiểm toán

Việc quản lý cấu hình góp phần hỗ trợ ATTT trong việc trao đổi thông tin và vận hành.

Tài liệu yêu cầu

- Rà soát trong bảng phân công nhiệm vụ để xác minh thông tin về cán bộ chuyên trách quản lý cấu hình
- Chính sách và thủ tục liên quan tới thay đổi cấu hình
- Danh mục lưu trữ các thay đổi cấu hình

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phòng vấn lãnh đạo CNTT về việc đơn vị giao cho các cán bộ chuyên trách thực hiện việc thay đổi cấu hình, phạm vi công việc, ghi chép lưu trữ thông tin về các thay đổi cấu hình.

- Phòng vấn cán bộ chuyên trách thực hiện việc thay đổi cấu hình về quy trình thực hiện, lưu trữ CSDL về các thay đổi cấu hình

Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán sau:

- Rà soát trong bảng phân công nhiệm vụ để xác minh thông tin về cán bộ chuyên trách quản lý cấu hình

- Chính sách và thủ tục liên quan tới thay đổi cấu hình

- Danh mục lưu trữ các thay đổi cấu hình

Kiểm toán viên nhà nước tiến hành rà soát và xác minh các vấn đề sau:

- Kiểm tra danh mục lưu trữ các thay đổi cấu hình có được thực hiện, cập nhật thường xuyên hay không?

- Xác nhận xem trong kỳ kiểm toán có bất kỳ vấn đề nào, lí do nào liên quan tới sai sót trong cấu hình? Nếu có thực hiện phỏng vấn các nhà quản lý về thủ tục thực hiện đối với thay đổi cấu hình đó.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề A6.05 - Quản lý tài sản Công nghệ thông tin

Mục tiêu kiểm toán:

Đảm bảo đơn vị có hệ thống quản lý tài sản CNTT.

Kiểm soát A6.05.01 - Đảm bảo rằng công tác bảo vệ tài sản CNTT được triển khai phù hợp

Tiêu chí kiểm toán

Đơn vị có hệ thống quản lý tài sản hỗ trợ công tác an ninh thông tin. Tham khảo Hệ thống quản lý ATTT ISO 2700, COBIT và các chính sách, thủ tục hoặc quy định khác.

Tài liệu yêu cầu

- Chính sách quản lý tài sản;
- Phân loại tài sản CNTT;
- Thủ tục thanh lý tài sản;
- Các báo cáo kiểm toán tài chính (nếu liên quan đến tài sản và hàng tồn kho).

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phòng văn lãnh đạo CNTT về việc ban hành chính sách quản lý tài sản của đơn vị: chính sách quản lý, cách thức phân loại tài sản của đơn vị, quy trình mua mới tài sản, quy trình quản lý tài sản (cấp phát, mua mới, thanh lý...)

Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán sau:

- Chính sách quản lý tài sản;
- Phân loại tài sản CNTT;
- Thủ tục thanh lý tài sản;
- Các báo cáo kiểm toán tài chính (nếu liên quan đến tài sản và hàng tồn kho)

Kiểm toán viên nhà nước tiến hành rà soát và xác minh các vấn đề sau:

- Rà soát chính sách quản lý tài sản, xác minh xem có bao gồm chính sách sử dụng chấp nhận được (AUP)? (ví dụ sử dụng máy tính xách tay cho các mục đích cá nhân, nếu nó không liên quan đến hoạt động kinh doanh tại đơn vị)

▪ Rà soát các danh sách thông tin tài sản có được cập nhật thường xuyên hay không?

▪ Kiểm tra xem các sổ sách ghi tài sản trong kho nhằm xác nhận xem liệu tài sản có được phân loại theo giá trị, mức độ nhạy cảm hoặc theo một cách phân loại khác hay không?

- Rà soát thủ tục thanh lý tài sản được giám sát bởi các cấp có thẩm quyền.
- Rà soát các yêu cầu thanh lý hoặc tái sử dụng tài sản.
- Xác minh với bộ phận chuyên trách nhằm đảm bảo rằng dữ liệu bên trong thiết bị đã được xóa trước khi thanh lý hoặc tái sử dụng.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề A6.06 – Nâng cao nhận thức người dùng về an ninh thông tin

Mục tiêu kiểm toán:

Nhân viên CNTT được đào tạo thích hợp để nắm rõ vai trò và trách nhiệm của mình trong công tác ATTT.

Kiểm soát A6.06.01 - Nhân viên CNTT được đào tạo thích hợp để nắm rõ vai trò và trách nhiệm của mình trong công tác ATTT.

Tiêu chí kiểm toán

Nhân viên CNTT được đào tạo thích hợp để nắm rõ vai trò và trách nhiệm của mình trong công tác ATTT

Tài liệu yêu cầu

- Chính sách nhân sự và quy trình tuyển dụng nhân sự đối với nhân viên phụ trách ATTT;
- Tiêu chuẩn về năng lực đối với nhân sự CNTT/nhân sự phụ trách ATTT;
- Các tài liệu đánh giá cá nhân (như bằng cấp, chứng chỉ nếu có).

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phòng vấn lãnh đạo phòng nhân sự về quy trình tuyển dụng nhân viên CNTT và các tiêu chí liên quan.
- Phòng vấn lãnh đạo nhân sự về việc thực hiện rà soát, kiểm tra, đánh giá lý lịch, đạo đức, chuyên môn của nhân sự CNTT.
- Phòng vấn lãnh đạo CNTT, xác minh các nhân viên CNTT tuyển dụng mới trong năm nay, vai trò trách nhiệm tương ứng của các nhân viên đó.
- Phòng vấn lãnh đạo CNTT xác minh danh sách các nhân viên nắm giữ vị trí quan trọng trong ban ATTT đã được cấp trên phê duyệt.

Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán sau:

- Chính sách nhân sự và quy trình tuyển dụng nhân sự đối với nhân viên phụ trách ATTT;

- Tiêu chuẩn về năng lực đối với nhân sự CNTT/nhân sự phụ trách ATTT; Các tài liệu đánh giá cá nhân (như bằng cấp, chứng chỉ nếu có)

Kiểm toán viên nhà nước tiến hành rà soát và xác minh các vấn đề sau:

- Rà soát danh sách nhân sự CNTT được tuyển dụng trong giai đoạn kiểm toán. Lấy một mẫu nhân viên CNTT (có tham gia công tác phụ trách ATTT của đơn vị) và rà soát thủ tục đánh giá trước khi tuyển dụng.

- Rà soát các tiêu chí đánh giá lý lịch, đạo đức, chuyên môn của đơn vị đối với nhân sự được tuyển chọn xem có phù hợp với mô tả yêu cầu công việc hay không?

- Rà soát các vị trí có vai trò quan trọng trong việc bảo đảm ATTT cần có văn bản phân công công việc và phê duyệt bởi ban quản lý.

- Rà soát và xác minh tính tách bạch trách nhiệm đối với nhân sự trong ban ATTT với bộ phận vận hành. (ví dụ: đội vận hành không được phép tự ý thực thi các quyết định liên quan tới ATTT mà không được cấp trên phê duyệt).

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát 60602 - Thực hiện đào tạo về thủ tục bảo mật ATTT hiệu quả nhằm nâng cao năng lực và kỹ năng của cán bộ.

Tiêu chí kiểm toán

Đảm bảo chương trình đào tạo có phạm vi phù hợp, được thực hiện theo định kỳ một cách đúng đắn.

Tài liệu yêu cầu

- Chính sách và quy trình đào tạo
- Nội dung đào tạo
- Mẫu về kết quả kiểm tra cuối kỳ
- Mẫu về việc đánh giá hiệu lực của công tác đào tạo

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phỏng vấn cán bộ chuyên trách có thẩm quyền về chính sách và quy trình đào tạo định kỳ nâng cao kiến thức và kỹ năng về ATTT: thời gian đào tạo, đối tượng đào

tạo, nội dung đào tạo và hình thức đào tạo, phương pháp đánh giá hiệu quả đào tạo sau khóa học...

Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán sau:

- Chính sách và quy trình đào tạo
- Nội dung đào tạo
- Mẫu về kết quả kiểm tra cuối kỳ
- Mẫu về việc đánh giá hiệu lực của công tác đào tạo

Kiểm toán viên nhà nước tiến hành đánh giá các vấn đề sau:

▪ Đánh giá quy trình đo lường tính hiệu quả của công tác đào tạo (nếu có) nhằm khẳng định rằng việc đào tạo an toàn CNTT và các yêu cầu về nhận thức đều bao gồm trong quy trình này.

▪ Rà soát nội dung chương trình đào tạo ATTT cả về tính đầy đủ và tính hợp lý. Kiểm tra cách thức giảng dạy, truyền đạt thông tin nhằm đánh giá xem liệu thông tin có được truyền tải đến tất cả các đối tượng bao gồm các nhà tư vấn, các nhà thầu và những nhân viên tạm thời cũng như khách hàng và các nhà cung ứng không. Kiểm tra nội dung chương trình đào tạo nhằm xác định xem liệu khuôn khổ kiểm soát nội bộ và các yêu cầu về an toàn có dựa trên chính sách an toàn và các thủ tục kiểm soát nội bộ của đơn vị không (ví dụ: tác động của việc không tuân thủ các yêu cầu về an toàn, việc sử dụng các nguồn lực của đơn vị, các trang thiết bị, xử lý các rắc rối, trách nhiệm của nhân viên đối với ATTT).

▪ Kiểm tra và xác nhận tài liệu đào tạo và chương trình đào tạo đã được thẩm định thường xuyên một cách đầy đủ.

▪ Kiểm tra chính sách về việc xác định yêu cầu đào tạo. Khẳng định xem chính sách này có đảm bảo rằng các yêu cầu quan trọng đã được phản ánh trong chương trình đào tạo.

▪ Phỏng vấn nhân viên nhằm đánh giá xem liệu họ đã được đào tạo và liệu họ có hiểu rõ trách nhiệm của mình trong việc duy trì ATTT và bảo mật thông tin không.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề A6.07 - Bảo mật vật lý các tài sản CNTT

Mục tiêu kiểm toán:

Đảm bảo vị trí đặt các tài sản CNTT được bảo vệ chống lại các rủi ro về vị trí địa lý và rủi ro môi trường.

Kiểm soát A6.07.01 - Vị trí đặt các tài sản CNTT được bảo vệ chống lại các rủi ro về vị trí địa lý và rủi ro môi trường.

Tiêu chí kiểm toán

Vị trí nơi chứa các tài sản CNTT của đơn vị có được bảo vệ trước các rủi ro về vật lý và môi trường không?

Tài liệu yêu cầu

- Sơ đồ hệ thống mạng;
- Kế hoạch bảo mật địa điểm lắp đặt tài sản CNTT
- Báo cáo kiểm tra thiết bị định kỳ (kiểm tra các thiết bị phòng cháy chữa cháy...);
- Báo cáo của các phòng ban liên quan khác (như báo cáo tình trạng hoạt động các thiết bị phòng cháy chữa cháy: vẫn hoạt động tốt hay đã hết thời hạn sử dụng).

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán sau:

- Sơ đồ hệ thống mạng;
- Kế hoạch bảo mật địa điểm lắp đặt tài sản CNTT
- Báo cáo kiểm tra thiết bị định kỳ (kiểm tra các thiết bị phòng cháy chữa cháy...);
- Báo cáo của các phòng ban liên quan khác (như báo cáo tình trạng hoạt động các thiết bị phòng cháy chữa cháy: vẫn hoạt động tốt hay đã hết thời hạn sử dụng).

Kiểm toán viên nhà nước tiến hành rà soát và xác minh các vấn đề sau:

- Đánh giá các kiểm soát đang được thực thi tại đơn vị có phù hợp với báo cáo phân tích rủi ro của đơn vị
- Rà soát các kiểm soát an toàn/biện pháp phòng ngừa của đơn vị trước những nguy cơ về mặt vật lý, môi trường như phòng cháy chữa cháy, báo động, thiết bị cung cấp điện ...; kiểm tra các báo cáo đánh giá định kỳ của các thiết bị.
- Rà soát các khuyến nghị của các bộ phận khác như phòng cháy chữa cháy, thanh tra, ban phòng ngừa thảm họa...có được thực hiện hay không?

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát A6.07.02 - Đơn vị thực hiện các kiểm soát đảm bảo an toàn phòng chống sự truy cập bất hợp pháp tới các trang thiết bị CNTT quan trọng (phòng server, kho dữ liệu...).

Tiêu chí kiểm toán

Kiểm soát phòng chống lại việc làm nguy hại tới tài sản CNTT, truy cập trái phép nhằm sao lưu hay xem xét các thông tin nhạy cảm.

Tài liệu yêu cầu

- Sơ đồ mạng lưới hệ thống thông tin;
- Báo cáo kiểm tra thiết bị định kỳ trung tâm dữ liệu;
- Lịch sử ra vào trung tâm dữ liệu được ghi lại trực tiếp trên hệ thống (thông thường đối với nhân viên ra vào bằng vân tay hoặc thẻ từ sẽ có lịch sử ra vào ghi lại trực tiếp trên hệ thống) trong giai đoạn kiểm toán;
 - Sổ ghi chép lịch sử ra vào trung tâm dữ liệu: Người ra vào, thời gian vào, thời gian ra, đơn vị trong giai đoạn kiểm toán;
 - Danh sách người dùng được phép ra vào trung tâm dữ liệu (danh sách được xem xét và phê duyệt bởi lãnh đạo cấp trên);
 - Ảnh chụp ghi lại lâu nhất có thể từ camera của trung tâm dữ liệu trong giai đoạn kiểm toán;
 - Các báo cáo sự cố liên quan tới trung tâm dữ liệu.

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phỏng vấn lãnh đạo CNTT tìm hiểu về vị trí lắp đặt của các tài sản CNTT quan trọng như trung tâm sao lưu dữ liệu, trung tâm dữ liệu dữ phòng cùng với các trang thiết bị được lắp đặt để bảo an toàn cho các tài sản CNTT đó: Số lượng camera, điều hòa, thiết bị phòng cháy chữa cháy, thiết bị báo khói, UPS... Phỏng vấn lãnh đạo CNTT về việc nguyên tắc ra vào phòng máy chủ ra vào bằng thẻ từ, chia khóa, vân tay...

- Phòng vận lãnh đạo CNTT tìm hiểu về nhân sự được phép ra trung tâm sao lưu dữ liệu/trung tâm dữ liệu dự phòng, công tác giám sát việc ra vào phòng máy chủ (giám sát qua camera, lịch sử ra vào phòng máy chủ được ghi lại trên hệ thống).

- Phòng vận lãnh đạo CNTT về thủ tục quy trình cấp phép ra vào trung tâm dữ liệu đối với những không được quyền ra vào như thanh tra, khách...

- Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán sau:

- Sơ đồ mạng lưới hệ thống thông tin;

- Báo cáo kiểm tra thiết bị định kỳ trung tâm dữ liệu;

- Danh sách người dùng được phép ra vào trung tâm dữ liệu (danh sách được xem xét và phê duyệt bởi lãnh đạo cấp trên);

- Lịch sử ra vào trung tâm dữ liệu được ghi lại trực tiếp trên hệ thống (thông thường đối với nhân viên ra vào bằng vân tay hoặc thẻ từ sẽ có lịch sử ra vào ghi lại trực tiếp trên hệ thống) trong giai đoạn kiểm toán;

- Sổ ghi chép lịch sử ra vào trung tâm dữ liệu: Người ra vào, thời gian vào, thời gian ra, đơn vị trong giai đoạn kiểm toán;

- Ảnh chụp ghi lại lâu nhất có thể từ camera của trung tâm dữ liệu trong giai đoạn kiểm toán;

- Các báo cáo sự cố liên quan tới trung tâm dữ liệu;

Kiểm toán viên nhà nước tiến hành rà soát và xác minh các vấn đề sau:

- Rà soát sơ đồ mạng lưới để xác định được vị trí, số lượng các trung tâm dữ liệu của đơn vị và xác định khoảng cách giữa trung tâm sao lưu dữ liệu và trung tâm dữ liệu dự phòng có đảm bảo an toàn hay không? (theo chuẩn mực là 30 km)

- Tham quan và xác minh trung tâm dữ liệu được trang bị đầy đủ các thiết bị bảo đảm an toàn: camera, thiết bị phòng cháy chữa cháy, thiết bị báo khói, UBS, điều hòa... đồng thời xác minh các thiết bị đó vẫn hoạt động ổn định, bình thường.

- Rà soát danh sách người dùng được phép ra vào trung tâm dữ liệu và đảm bảo những người trong danh sách là phù hợp, đã được xem xét và phê duyệt bởi cấp trên. Xác minh chỉ những người trong danh sách mới được phép ra vào trung tâm dữ liệu (có thể thử thẻ từ/vân tay của một vài nhân viên CNTT không được phép, xác minh hệ thống thẻ từ/vân tay không cho phép nhân viên đó ra vào trung tâm dữ liệu).

- Xác minh việc hệ thống thực hiện ghi lại hình ảnh, lịch sử ra vào, thời gian ra vào của những nhân viên được cấp quyền ra vào trung tâm dữ liệu.

- Xác minh các trường hợp khách/thanh tra vào kiểm tra và đánh giá trung tâm dữ liệu phải phê duyệt bởi các cấp lãnh đạo liên quan (ví dụ như tạo biểu mẫu yêu cầu ra vào phòng máy chủ cho khách, trình và xin chữ ký phê duyệt của lãnh đạo cấp trên). Lịch sử ra vào của khách/thanh tra được ghi lại đầy đủ trong nhật ký ra vào trung tâm dữ liệu. Khi khách/thanh tra vào trung tâm dữ liệu, phải có nhân viên CNTT đi theo và giám sát.

- Rà soát các báo cáo sự cố liên quan tới trung tâm dữ liệu và xác định các hành động của đơn vị đối với các sự cố đó.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát A6.07.03 - Đơn vị ban hành chính sách và thực hiện kiểm soát phát hiện và theo dõi việc đột nhập trái phép tới các tài nguyên CNTT

Tiêu chí kiểm toán

Phát hiện các đột nhập và có các biện pháp xử lý kịp thời

Tài liệu yêu cầu

- Chính sách/văn bản do đơn vị ban hành quy định về việc ngăn chặn các truy cập trái phép

- Các bằng chứng liên quan tới các trường hợp đột nhập trái phép

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phòng văn lãnh đạo CNTT về chính sách và việc thực thi các kiểm soát của đơn vị trong việc phát hiện và xử lý các đột nhập trái phép

- Phòng văn và tìm hiểu xem có trường hợp đột nhập trái phép nào xảy ra trong kỳ kiểm toán hay không và cách thức giải quyết của đơn vị.

Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán sau:

- Chính sách/văn bản do đơn vị ban hành quy định về việc ngăn chặn các truy cập trái phép

Kiểm toán viên nhà nước tiến hành rà soát và xác minh các vấn đề sau:

- Xác minh các thủ tục kiểm soát của đơn vị để phòng tránh, ngăn ngừa sự đột nhập trái phép và các khu vực bảo mật/trung tâm dữ liệu/văn phòng làm việc của đơn vị...
- Rà soát các trường hợp đột nhập trái phép và xác minh hành động đột nhập có được phát hiện và thông báo kịp thời, cách giải quyết của đơn vị đối với các đột nhập đó.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề A6.08 - Quản lý truy cập

Mục tiêu kiểm toán:

Đảm bảo đơn vị chính sách quản lý truy cập quy định việc cấp phát/thay đổi quyền truy cập cho người dùng trên các ứng dụng/phần mềm quan trọng của đơn vị.

Kiểm soát A6.08.01 - Đơn vị ban hành chính sách quản lý truy cập quy định việc cấp phát/thay đổi quyền truy cập cho người dùng trên các ứng dụng/phần mềm quan trọng của đơn vị.

Tiêu chí kiểm toán

Tổ chức ban hành chính sách rõ ràng và hiệu quả đối với việc kiểm soát truy cập

Tài liệu yêu cầu

- Chính sách quản lý truy cập
- Danh sách người sử dụng trên hệ thống
- Ma trận phân quyền/kiểm soát truy cập

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phỏng vấn cán bộ chuyên trách có thẩm quyền về việc liệu tổ chức có ban hành một chính sách về quản lý truy cập hay không? Chính sách này được phê duyệt, rà soát và cập nhật định kỳ như thế nào?

- Phòng văn cán bộ chuyên trách có thẩm quyền về việc áp dụng các quy định trong chính sách thực thi quản lý quyền truy cập của đơn vị và cách thức phân quyền cho người dùng.

Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán sau:

- Chính sách quản lý truy cập
- Danh sách người sử dụng trên hệ thống
- Ma trận phân quyền/kiểm soát truy cập

Kiểm toán viên nhà nước tiến hành rà soát và xác minh các vấn đề sau:

- Rà soát chính sách và thủ tục truy cập có quy định nhằm đảm bảo việc tách biệt phân quyền (SOD: Segregation Of Duties) giảm thiểu cơ hội truy cập bất hợp pháp và đặc quyền.

- Rà soát ma trận phân quyền người dùng cùng các quy định có đầy đủ thông tin hỗ trợ người quản trị hệ thống có đủ cơ sở để thực hiện việc phân quyền người dùng.

- Chọn mẫu người sử dụng cùng tài khoản hệ thống và quyền được gán để chứng minh cơ chế phân quyền đã được quy định.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát A6.08.02 - Đơn vị quản lý việc cấp phát/thay đổi quyền truy cập cho người dùng trên các ứng dụng/phần mềm quan trọng của đơn vị.

Tiêu chí kiểm toán

Đảm bảo chỉ có người có thẩm quyền mới có quyền truy cập vào hệ thống liên quan

Tài liệu yêu cầu

- Chính sách quản lý truy cập;
- Quy trình cấp phát quyền cho người dùng trên Domain, VPN (nếu có) và trên các ứng dụng/phần mềm quan trọng;
- Danh sách nhân sự tuyển dụng mới trong giai đoạn kiểm toán;

- Ma trận phân quyền/kiểm soát truy cập Báo cáo số lượng cấp phát quyền truy cập cho người dùng trong giai đoạn kiểm toán trên Domain/VPN (nếu có) và các ứng dụng/phần mềm quan trọng của đơn vị trong giai đoạn kiểm toán;

- Email/biểu mẫu yêu cầu cấp phát quyền truy cập (có phê duyệt từ cấp trên).

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán sau:

- Chính sách quản lý truy cập;
- Quy trình cấp phát quyền cho người dùng trên Domain, VPN (nếu có) và trên các ứng dụng/phần mềm quan trọng;
- Danh sách nhân sự tuyển dụng mới trong giai đoạn kiểm toán;
- Ma trận phân quyền/kiểm soát truy cập;
- Báo cáo số lượng cấp phát quyền truy cập cho người dùng trong giai đoạn kiểm toán trên Domain/VPN (nếu có) và các ứng dụng/phần mềm quan trọng của đơn vị trong giai đoạn kiểm toán;

- Email/biểu mẫu yêu cầu cấp phát quyền truy cập (có phê duyệt từ cấp trên);

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phỏng vấn cán bộ chuyên trách có thẩm quyền về chính sách và quy trình phát quyền truy cập cho người dùng trên hệ thống các ứng dụng/phần mềm quan trọng của đơn vị.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước tiến hành rà soát và xác minh các vấn đề sau:

- Xác minh lại thủ tục chính thức của đơn vị trong việc cấp phát quyền truy cập cho người dùng;
- Lấy một mẫu yêu cầu cấp phát/thay đổi quyền truy cập trong giai đoạn kiểm toán và xác minh việc cấp phát/thay đổi quyền theo đúng các thủ tục chính thức của đơn vị và kịp thời hay không;
- Với mẫu đã chọn, rà soát bảng phân quyền, rà soát các quyền của người dùng trên hệ thống, rà soát phiếu/email yêu cầu cấp phát quyền truy cập và xác minh rằng việc cấp phát/thay đổi quyền trên hệ thống đúng theo thủ tục cấp phát quyền của đơn vị;

- Dựa vào danh sách số lượng người dùng được cấp phát/thay đổi quyền trên từng hệ thống/ứng dụng trong giai đoạn kiểm toán. Kiểm toán viên nhà nước tiến hành chọn mẫu và xác minh các thông tin sau: Yêu cầu cấp phát/thay đổi quyền truy cập được sự phê duyệt từ cấp trên (thông thường là người quản lý trực tiếp của nhân viên đó, hoặc trưởng các phòng ban bộ phận của nhân viên đó);

- Đối chiếu phiếu yêu cầu với thực tế các quyền được cấp phát/thay đổi trên hệ thống có giống nhau hay không?

- Đối chiếu quyền của người được cấp/thay đổi quyền trên hệ thống có phù hợp, đúng với bảng ma trận phân quyền của từng hệ thống hay không (đảm bảo tính tách bạch trách nhiệm của người dùng)

- Đối chiếu với danh sách nhân sự thêm mới, chuyển chuyên rà soát ngày bắt đầu làm việc và ngày cấp quyền trên hệ thống, xác minh việc tạo cấp quyền được thực hiện hợp lý và phù hợp ngay sau thời gian yêu cầu cấp quyền/thời gian bắt đầu làm việc (đối với nhân sự được tuyển dụng mới)/thời gian bắt đầu công tác tại vị trí mới (đối với người dùng chuyển đơn vị)

** Lưu ý: Bên cạnh việc chọn mẫu thủ công, Kiểm toán viên nhà nước có thể sử dụng CAATs (ví dụ ACL, IDEA) để thực hiện việc kiểm tra xác minh xem liệu việc truy cập có được thực hiện một cách hợp lý và kịp thời không dựa trên dữ liệu xuất ra từ hệ thống*

Kiểm soát A6.08.03 - Hủy bỏ quyền truy cập hệ thống với người dùng nghỉ việc/chuyển bộ phận trên các ứng dụng/phần mềm quan trọng của đơn vị.

Tiêu chí kiểm toán

Tránh các rủi ro liên quan tới truy cập trái phép của người dùng trên hệ thống

Tài liệu yêu cầu

- Quy trình hủy bỏ quyền truy cập trên các ứng dụng/phần mềm quan trọng đối với người nghỉ việc/chuyển bộ phận công tác.

- Danh sách nhân sự chuyển và nghỉ việc trong giai đoạn kiểm toán

- Báo cáo số lượng hủy bỏ quyền truy cập cho người dùng trong giai đoạn kiểm toán trên Domain/VPN (nếu có) và các ứng dụng/phần mềm quan trọng của đơn vị trong giai đoạn kiểm toán

- Email/biểu mẫu yêu cầu hủy bỏ quyền truy cập

Đánh giá thiết kế và triển khai

Kiểm toán viên nhà nước tiến hành phỏng vấn và xác minh các vấn đề sau:

- Phỏng vấn cán bộ chuyên trách có thẩm quyền tìm hiểu quy trình hủy bỏ quyền truy cập trên hệ thống đối với người nghỉ việc/chuyển bộ phận công tác.

Kiểm toán viên nhà nước tiến hành thu thập các bằng chứng kiểm toán sau:

- Quy trình hủy bỏ quyền truy cập trên các ứng dụng/phần mềm quan trọng đối với người nghỉ việc/chuyển bộ phận công tác.

- Danh sách nhân sự chuyển và nghỉ việc trong giai đoạn kiểm toán

- Báo cáo số lượng hủy bỏ quyền truy cập cho người dùng trong giai đoạn kiểm toán trên Domain/VPN (nếu có) và các ứng dụng/phần mềm quan trọng của đơn vị trong giai đoạn kiểm toán

- Email/biểu mẫu yêu cầu hủy bỏ quyền truy cập

Kiểm toán viên nhà nước tiến hành rà soát và xác minh các vấn đề sau:

- Xác minh lại thủ tục chính thức của đơn vị trong việc cấp hủy quyền truy cập đối với người dùng

- Lấy một mẫu yêu cầu hủy bỏ quyền truy cập trong giai đoạn kiểm toán và xác minh việc hủy bỏ quyền theo đúng các thủ tục của đơn vị và kịp thời

- Với mẫu đã chọn, rà soát email/phiếu yêu cầu hủy quyền, so sánh giữa thời gian nghỉ việc/chuyển bộ phận với ngày hủy bỏ quyền trên hệ thống, đảm bảo quy trình hủy bỏ được thực hiện một cách hiệu quả

Thử nghiệm hiệu quả hoạt động

Dựa vào danh sách số lượng người dùng bị hủy bỏ quyền truy cập trên hệ thống trong giai đoạn kiểm toán, Kiểm toán viên nhà nước tiến hành chọn mẫu và xác minh các thông tin sau:

- Yêu cầu hủy bỏ quyền truy cập. Đối chiếu phiếu yêu cầu với thực tế hủy bỏ và ngày hủy bỏ quyền truy cập/ngày truy cập cuối cùng của các mẫu được chọn. Rà soát xác minh trạng thái tài khoản của các mẫu được chọn xem đã được xóa/không còn hoạt động (inactive) hay chưa?

- Đối chiếu với danh sách nhân sự nghỉ việc và chuyển, rà soát ngày nghỉ việc chính thức của các mẫu được chọn, xác minh rằng các việc hủy bỏ quyền được thực hiện kịp thời và hiệu quả ngay sau thời gian nghỉ việc/chuyển.

** Lưu ý: Bên cạnh việc chọn mẫu thủ công, Kiểm toán viên nhà nước có thể sử dụng CAATs (ví dụ ACL, IDEA) để thực hiện việc kiểm tra xác minh xem liệu việc truy cập có được thực hiện một cách hợp lý và kịp thời không dựa trên dữ liệu xuất ra từ hệ thống*

9. Chuyên đề A7 - Kiểm soát ứng dụng CNTT

a. Khái niệm

Phần mềm ứng dụng là phần mềm giúp thực hiện hoặc hỗ trợ một nghiệp vụ cụ thể. Phạm vi kiểm soát phần mềm ứng dụng bao gồm cả các thao tác nghiệp vụ xử lý thủ công cũng như thao tác nghiệp vụ được tin học hóa trong việc tổ chức sắp xếp các giao dịch, xử lý dữ liệu, lưu giữ dữ liệu và chuẩn bị các báo cáo. Đơn vị có thể có rất nhiều phần mềm ứng dụng với các quy mô khác nhau từ việc hệ thống phần mềm lớn phục vụ cho cả đơn vị đến các phần mềm chỉ phục vụ cho một cá nhân.

Ví dụ: Phần mềm tính lương, phần mềm tính hóa đơn, phần mềm quản lý kho hay hệ thống tích hợp quản lý các nguồn lực của đơn vị (ERP) dùng cho đơn vị. Hệ thống TABMIS, TMS, TCS và các hệ thống thông tin quốc gia khác được sử dụng trong các Bộ, Ban Ngành, cơ quan nhà nước.

Việc xem xét hệ thống kiểm soát phần mềm ứng dụng sẽ giúp Kiểm toán viên nhà nước đánh giá độ hiệu quả và hiệu lực của các chốt kiểm soát liên quan đến các nghiệp vụ kiểm toán nhằm nhận ra các vấn đề liên quan đến phần mềm cần phải chú ý.

Ví dụ: Nếu công tác nhập dữ liệu và lưu giữ hồ sơ nhập liệu không được tổ chức và kiểm soát chặt chẽ thì dữ liệu đầu vào có rủi ro là nhập dữ liệu trái phép. Hoặc nếu phần mềm BHXH không có chốt kiểm soát dữ liệu đầu vào của người hưởng BHXH thì việc cấp BHXH nhiều lần cho một cá nhân là hoàn toàn có thể xảy ra.

Mỗi phần mềm ứng dụng gắn chặt với các giao dịch nghiệp vụ cụ thể vì vậy việc thử nghiệm các chốt kiểm soát trên các phần mềm cụ thể sẽ đảm bảo cho việc xử lý chính xác của nghiệp vụ được chọn kiểm toán.

Ví dụ: Việc thử nghiệm công thức tính lương của phần mềm tính lương sẽ giúp trả lời khoản mục tiền lương trên BCTC có được xử lý chính xác.

Điều này chúng ta không thể có được nếu chỉ dừng ở mức độ kiểm soát chung CNTT.

Tùy theo mục tiêu kiểm toán cụ thể mà việc xem xét phần mềm ứng dụng sẽ có các cách tiếp cận khác nhau và được thực hiện nhiều cách thức khác nhau.

Ví dụ: Khi việc xem xét phần mềm tập trung vào tính tuân thủ pháp luật thì các chốt kiểm soát sẽ được thử nghiệm dưới góc độ tuân thủ. Khi xem xét phần mềm như là một phần của cuộc kiểm toán hoạt động thì cần tập trung vào quá trình tin học hóa các nghiệp vụ. Khi kiểm tra nội dung an toàn thông tin thì tập trung kiểm tra tính bảo mật, nhất quán và sẵn sàng của dữ liệu.

Việc xây dựng các bước thực hiện kiểm toán phần mềm ứng dụng nên là một quy trình xem xét xoay quanh các hoạt động. Nó có thể bắt đầu từ việc xem xét nghiệp vụ hoặc đi từ dữ liệu hoặc xem xét tài liệu phát triển. Vì vậy, sẽ không có một cấu trúc cố định giữa các bước thực hiện. Các hoạt động nên thực hiện như sau:

Hiểu về quy trình nghiệp vụ

Trước khi xem xét các vấn đề kỹ thuật của phần mềm cần xem xét các quy trình nghiệp vụ được tin học hóa liên quan đến phần mềm. Các vấn đề nghiệp vụ xem xét bao gồm các quy tắc, luồng xử lý công việc, các cá nhân sử dụng, vai trò của họ cùng các nguyên tắc phải tuân thủ. Việc tiến hành tìm hiểu nghiệp vụ cũng có cách tiếp cận đa dạng tùy thuộc vào mục đích của cuộc kiểm toán. Các việc thông thường phải thực hiện bao gồm nghiên cứu các thủ tục nghiệp vụ, luồng xử lý công việc dưới dạng biểu đồ hoặc các tài liệu liên quan. Kiểm toán viên nhà nước nên tiến hành gặp và phỏng vấn lãnh đạo mảng nghiệp vụ trên, đội vận hành hệ thống CNTT và những người sử dụng ứng dụng trọng yếu.

Nghiên cứu ứng dụng và môi trường hoạt động

Nghiên cứu thiết kế và các tính chất của phần mềm thông qua các tài liệu như sơ đồ tổ chức của đơn vị, luồng đi của dữ liệu, hướng dẫn sử dụng hoặc phỏng vấn các cá nhân quan trọng. Quan sát việc vận hành các nghiệp vụ trọng yếu trong thực tế và trao đổi với người dùng khi họ đang sử dụng phần mềm trên. Thông qua thảo luận và thực hiện xuyên suốt một nghiệp vụ từ dữ liệu đầu vào đến dữ liệu báo cáo cuối cùng, xác nhận lại nghiệp vụ để hiểu cách thức thật sự vận hành của các nghiệp vụ và phát hiện ra các nghiệp vụ xử lý thủ công liên quan đến phần mềm bắt buộc phải tuân thủ. Thảo luận với cấp quản lý, người vận hành và người phát triển nhằm có được các tài liệu liên quan đến hạ tầng kỹ thuật như: hệ điều hành, môi trường mạng, hệ thống quản lý CSDL, giao

thức giao tiếp với các phần mềm khác, lực lượng phát triển chính của phần mềm bên trong hay bên ngoài, việc chạy dữ liệu theo lô hay chạy trực tiếp. Công tác trên sẽ cung cấp được những chỉ dẫn về cách thức các yếu tố kỹ thuật ảnh hưởng lên ứng dụng.

Nhận diện rủi ro

Trả lời 2 câu hỏi “Cái gì có thể hoạt động sai sót?” nhằm xác định các rủi ro liên quan đến hoạt động nghiệp vụ, các chức năng của phần mềm; “Phần mềm kiểm soát hoạt động như thế nào?” nhằm phát hiện cách thức phần mềm xử lý các rủi ro trên. Đôi khi những rủi ro nghiệp vụ đã được phát hiện từ các cuộc kiểm toán trước, của bộ phận kiểm toán nội bộ hoặc bản thân quản lý của đơn vị. Trong trường hợp này, Kiểm toán viên nhà nước có thể sử dụng các phát hiện trên để đánh giá mức độ tin cậy của hệ thống kiểm soát nội bộ.

Kiểm tra các chốt kiểm soát

Sau khi đã xem xét các yếu tố nghiệp vụ và kỹ thuật, Kiểm toán viên nhà nước có thêm tự tin để đánh giá hệ thống kiểm soát nội bộ của đơn vị với các rủi ro đã xác định. Kiểm toán viên nhà nước cần công tâm và can trọng khi kiến nghị về cải tiến phần mềm.

Ví dụ: Một số kiến nghị về hệ thống lưu vết mọi hoạt động nghiệp vụ của Ngân hàng sẽ đẩy giá sản phẩm lên cao nhưng chưa chắc đã lưu vết thành công các thông tin trọng yếu của ngân hàng đó.

Việc đánh giá kiểm tra cần tiến hành toàn diện như những mô tả ở các phần tiếp theo của chương.

b. Rủi ro thường gặp

Các hậu quả của các kiểm soát ứng dụng thường phụ thuộc vào bản chất của phần mềm ứng dụng. Các rủi ro rất phong phú như sự không hài lòng của người sử dụng hoặc các thảm họa xảy ra trong thực tế. Đơn vị sẽ mất đi vị thế hoặc thị trường khi một dịch vụ công nghệ thông tin nào đó không hoạt động. Đơn vị cũng có thể mất tiền nếu hệ thống xử lý thiếu các đơn đặt hàng. Sự tin tưởng của nhân dân vào chính quyền bị giảm sút nếu dịch vụ không tốt. Sự không tuân thủ các quy định nhà nước có thể dẫn đến tham nhũng, trục lợi công quỹ gây hậu quả nghiêm trọng. Thậm chí đời sống chung của xã hội bị ảnh hưởng nếu hệ thống tài khoản ngân hàng bị ngừng hoạt động, hệ thống máy chủ của sân bay bị tấn công tê liệt.

Rủi ro lớn thường xảy ra trong việc thiếu đi kiểm soát dữ liệu đầu vào dẫn đến việc phần mềm xử lý sai và thất bại trong việc đạt được những nhiệm vụ đặt ra của tổ chức.

Việc xử lý dữ liệu thường phạm lỗi không nhất quán và cung cấp những dữ liệu đầu ra không chính xác. Đặc biệt khi người dùng được phép ghi đè hoặc xóa dữ liệu để đưa cách xử lý theo hướng khác. Trong các phần mềm quan trọng trên thì hệ thống lưu vết cũng như sự tuân thủ các quy tắc sửa chữa dữ liệu phải được áp dụng, nếu không việc sửa chữa dữ liệu tùy tiện sẽ dẫn đến tính không nhất quán trong xử lý cũng như hệ lụy khác.

Các thủ tục quản lý hồ sơ nhập liệu cùng các quyết định liên quan đến dữ liệu đầu vào cũng là chốt kiểm soát quan trọng việc nhập dữ liệu đầu vào. Nếu công tác quản lý hồ sơ nhập liệu không được thực hiện thì việc truy vết dữ liệu đầu vào không thể thực hiện được, không tuân thủ pháp luật, vi phạm các quy định về lưu trữ dữ liệu, dữ liệu trái phép có thể được đưa vào hệ thống. Mặt khác, các dữ liệu trái phép có thể dẫn đến các lỗi phần mềm và gian lận.

Thường thì nếu gặp lỗi trong quá trình kiểm soát quy trình xử lý lỗi dữ liệu sẽ dẫn đến lỗi xử lý và phần mềm sẽ không chạy đúng theo yêu cầu nghiệp vụ. Lỗi trong quá trình kiểm soát việc xử lý là do: việc ánh xạ quy tắc nghiệp vụ vào chương trình chưa chính xác; việc kiểm thử phần mềm không đầy đủ; lỗi điều chỉnh giữa các phiên bản phần mềm; việc phục hồi chương trình không chính xác sau một sự cố nào đó. Các lỗi này nếu không được phát hiện kịp thời sẽ tích lũy theo thời gian và có thể ảnh hưởng trọng yếu đến nghiệp vụ cũng như chất lượng của cả hệ thống.

Đối với hệ thống xử lý thời gian thật, một số kiểm soát không được cài đặt trong hệ thống như: xác định tính đúng đắn của dữ liệu đầu vào; đếm số lượng đầu vào và đầu ra để đảm bảo tính đầy đủ của dữ liệu; hệ thống lưu vết. Tuy nhiên, các hệ thống trên sẽ có những loại kiểm soát khác như kiểm tra tính đầy đủ của dữ liệu tương tác, các quy tắc xác nhận và lưu lại những lần cố gắng đăng nhập vào hệ thống để hạn chế các rủi ro như cố tình tấn công hệ thống, cố tình ăn cắp dữ liệu trực tuyến.

Việc thiếu kiểm soát dữ liệu đầu ra sẽ dẫn đến rủi ro của việc chỉnh sửa hoặc xóa dữ liệu mà không truy ra được nguồn gốc. Hậu quả là các quyết định, báo cáo quản lý

không chính xác. Mức độ nghiêm trọng của sự việc phụ thuộc vào cách thức dữ liệu được sử dụng trong nghiệp vụ.

Đối với an toàn bảo mật ứng dụng phần mềm thì sự thiếu vắng cơ chế lưu vết sẽ không thể phát hiện được ai đã làm thay đổi dữ liệu hoặc thao tác trên phần mềm. Ngoài ra, việc có hệ thống lưu vết dữ liệu cũng sẽ giúp cho người dùng tránh bớt chuyện dùng phần mềm sai mục đích. Hiển nhiên, việc dữ liệu bị sửa xóa có thể gây nên ảnh hưởng rất lớn đến các giao dịch.

Thật sự thì các lỗi an toàn bảo mật gây nên những hậu quả rất lớn như: mất thu nhập, hệ thống bị gián đoạn, mua bán thông tin, thay đổi tình trạng pháp lý hoặc vi phạm bản quyền. Những lỗi an toàn bảo mật, các biện pháp kiểm soát đã được thảo luận ở phần E.3.6 của Phần II.

c. Các vấn đề kiểm toán thành phần

Kiểm soát việc hoạt động của một phần mềm ứng dụng liên quan xoay quanh 04 đối tượng kiểm toán sau: Dữ liệu đầu vào; Dữ liệu đầu ra; Việc xử lý dữ liệu; Việc bảo đảm an toàn phần mềm. Cụ thể như sau:

- Vấn đề A7.01 - Dữ liệu đầu vào của phần mềm ứng dụng nhằm đảm bảo sự chính xác hợp lệ của dữ liệu đầu vào. Chú ý nội dung kiểm soát, đối chiếu hồ sơ nhập liệu cũng thuộc phạm vi kiểm soát trên. Khi thực hiện cần đối chiếu với các chứng từ nhập liệu gốc để đảm bảo tính hợp lệ của dữ liệu đầu vào.
- Vấn đề A7.02 – Quy trình xử lý dữ liệu chính xác để đảm bảo tính an toàn, bảo mật và sẵn sàng của dữ liệu.
- Vấn đề A7.03 - Dữ liệu đầu ra của phần mềm ứng dụng nhằm đảm bảo tính chính xác, đầy đủ và sử dụng đúng mục đích của dữ liệu đầu ra.
- Vấn đề A7.04 - An toàn của phần mềm ứng dụng nhằm đảm bảo phần mềm không bị dùng sai mục đích.

d. Chương trình kiểm toán mẫu

Vấn đề A7.01 - Dữ liệu đầu vào của ứng dụng

Mục tiêu kiểm toán

Đánh giá tính hợp lệ của dữ liệu nhập vào phần mềm ứng dụng.

Kiểm soát A7.01.01 - Tính hợp lệ của dữ liệu đầu vào.

Tiêu chí kiểm toán

- Các thông lệ, hướng dẫn kiểm soát nhập liệu phù hợp;
- Các quy tắc kiểm tra hợp lệ dữ liệu đầu vào đầy đủ, được mô tả trong các tài liệu kỹ thuật và hiện thực trong các giao diện nhập liệu của phần mềm;
- Các phương pháp và giao diện nhập liệu được mô tả trong các tài liệu kỹ thuật của phần mềm;
- Các quy tắc kiểm soát hợp lệ dữ liệu được cập nhật kịp thời, phù hợp với yêu cầu kiểm soát thực tế. Chú ý đến việc thay đổi chính sách kéo theo thay đổi quy cách dữ liệu đầu vào;
- Có hệ thống kiểm soát bổ sung thiết kế cho việc thay đổi dữ liệu đầu vào như sổ nhật ký ghi nhận ai đã thay đổi;
- Tồn tại hệ thống kiểm soát đúng đắn cùng tài liệu cho các giao diện nhập liệu cũng như giao thức tiếp nhận dữ liệu đến từ các phần mềm ứng dụng khác.

Tài liệu cần thu thập

- Tài liệu mô tả yêu cầu nghiệp vụ của phần mềm ứng dụng;
- Kiểu dữ liệu đầu vào của phần mềm ứng dụng;
- Yêu cầu tuân thủ của việc nhập dữ liệu đầu vào quy định trong các văn bản pháp quy và cơ quan quản lý;
- Giao thức và cấu trúc dữ liệu trao đổi với các phần mềm ứng dụng khác;
- Sơ đồ lưu chuyển dữ liệu toàn hệ thống phần mềm ứng dụng;
- Hướng dẫn sử dụng phần mềm;
- Các quy tắc quy định dữ liệu hợp lệ của phần mềm ứng dụng.

Thủ tục kiểm toán

- Rà soát yêu cầu nghiệp vụ, tài liệu phát triển ứng dụng cũng như xác nhận với chủ thể xử lý nghiệp vụ nhằm xác định các quy tắc quy định dữ liệu hợp lệ cần kiểm tra đánh giá.
- Kiểm tra xác nhận các quy tắc quy định dữ liệu đầu vào đã được thiết kế chính xác, mô tả đầy đủ trong tài liệu kỹ thuật.
- Xác nhận các chốt kiểm soát dữ liệu nhập vào hoạt động tốt trong thực tế. Việc xác nhận tiến hành thông qua: Quan sát thực tế việc nhập dữ liệu; Thử nghiệm phần

mềm với các kiểu dữ liệu vào khác nhau; hoặc Phân tích dữ liệu được lưu giữ trong cơ sở dữ liệu của đơn vị thông qua các phần mềm chuyên dụng.

- Rà soát và phân tích các tài liệu mô tả ý nghĩa nghiệp vụ, cảnh báo mâu thuẫn nghiệp vụ và các giao dịch liên quan đến dữ liệu đầu vào để đánh giá việc đảm bảo ý nghĩa nghiệp vụ của dữ liệu đầu vào.

- Đánh giá các tiêu chí hợp lệ và các tham số kỹ thuật phục vụ cho việc kiểm soát dữ liệu đầu vào đã phù hợp hay chưa với các quy tắc nghiệp vụ cũng như việc cương quyết loại trừ các dữ liệu không hợp lệ.

- Trong trường hợp dữ liệu trực tuyến, tiến hành kiểm tra các lỗi hỏng kỹ thuật bị khai thác thông qua việc cố tình nhập sai dữ liệu đầu vào được xử lý kịp thời.

- Kiểm tra đánh giá các tiêu chí, tham số liên quan đến việc kiểm soát dữ liệu đầu vào có được tiến hành xem xét định kỳ. Việc kiểm tra được tiến hành thông qua rà soát tài liệu, mã viết của chương trình hoặc phỏng vấn với các đối tượng liên quan.

- Kiểm tra và rà soát tài liệu, sổ nhật ký chỉnh sửa dữ liệu nhằm xác nhận các hoạt động chỉnh sửa được lưu giữ trong hệ thống thông qua hệ thống lưu vết; cá nhân chỉnh sửa dữ liệu được phân quyền hợp lý trong các tình huống nghiệp vụ hạn chế; việc chỉnh sửa theo đúng thủ tục, quy định nghiệp vụ.

- Xác định các giao thức giao tiếp dữ liệu của phần mềm ứng dụng với các hệ thống CNTT khác. Rà soát sơ đồ lưu chuyển dữ liệu, mã phần mềm, phỏng vấn người phát triển hoặc người quản trị nhằm đảm bảo tính chính xác, đầy đủ và được kiểm soát tốt của các dữ liệu được luân chuyển trong hệ thống.

Ví dụ: Kiểm tra người dùng có nhập dữ liệu rác vào hệ thống hay không, số CMND, số điện thoại nếu không nhập đúng theo quy định có bị hệ thống chặn lại hoặc cảnh báo hay không?

Kiểm soát A7.01.02 - Việc quản lý hồ sơ nhập liệu

Tiêu chí kiểm toán

- Tài liệu mô tả quy trình nhập liệu đầy đủ và được phổ biến cho người dùng;
- Tồn tại hệ thống lưu giữ hồ sơ nhập liệu từ lúc nhận được cho đến thời hạn hủy bỏ;
- Việc đánh số hồ sơ nhập liệu theo đúng từng giao dịch;

- Việc lưu giữ tài liệu gốc theo đúng các quy định của pháp luật về thời gian cũng như các yêu cầu khác.

Tài liệu cần thu thập

- Phân loại hồ sơ nhập liệu;
- Tiêu chí cho thời gian, đảm bảo đầy đủ và tính chính xác trong việc quản lý hồ sơ nhập liệu;
- Các thủ tục chuẩn bị hồ sơ nhập liệu;
- Giao thức trao đổi dữ liệu với các ứng dụng khác;
- Quy định việc lưu giữ hồ sơ nhập liệu;
- Sơ đồ lưu chuyển dữ liệu toàn hệ thống phần mềm ứng dụng;

Thủ tục kiểm toán

- Kiểm tra các quy trình về nhập liệu được xây dựng đầy đủ, tuân thủ các quy định và được phổ biến đến người dùng, các nguồn dữ liệu sử dụng cho việc nhập liệu là chính xác.

- Đánh giá việc quản lý nhóm nhập liệu trong đó tập trung vào việc lưu vết quá trình nhận tài liệu và nhập vào hệ thống cũng như các thao tác xử lý nghiệp vụ. Lưu ý đến số hồ sơ nhập cho từng nhóm, từng bộ phận phòng ban.

- Xác nhận tính đầy đủ, tuân thủ các tiêu chuẩn của các hồ sơ tài liệu bao gồm thời gian, đánh mã hồ sơ, cài đặt giá trị mặc định ... Các tiêu chuẩn trên được phê duyệt và xác nhận bởi cấp thẩm quyền.

- Kiểm tra việc đánh số các giao dịch theo đúng tuần tự không trùng lặp, không nhảy quãng, xử lý các tình huống phát sinh kỹ thuật liên quan đến việc đánh số giao dịch bằng phần mềm phân tích dữ liệu.

- Phỏng vấn nhân viên có trách nhiệm đến việc lưu giữ hồ sơ nhập liệu nhằm đảm bảo việc lưu trữ tài liệu được thực hiện theo đúng quy định. Chọn mẫu hồ sơ xem xét trong trường hợp cần thiết.

Ví dụ: Kiểm tra người dùng có nhập các bút toán không có hóa đơn chứng từ kèm theo hay không?

Kiểm soát A7.01.03 - Xử lý các lỗi nhập liệu

Tiêu chí kiểm toán

- Có một hệ thống thông báo lỗi rõ ràng, hướng dẫn người sử dụng sửa lỗi nhập liệu cho từng loại lỗi.
- Các lỗi nhập liệu phải được xử lý hoặc điều chỉnh hợp lý trước khi được đưa vào hệ thống.
- Nhật ký nhập liệu được xem xét định kỳ và có những hoạt động chỉnh sửa kịp thời nhằm giúp giảm thiểu lỗi nhập liệu.

Tài liệu cần thu thập

- Danh sách lỗi và các thông báo;
- Thủ tục cần thiết để xem xét các dữ liệu lưu vết;
- Chính sách và các thủ tục từ chối dữ liệu đầu vào;
- Thủ tục xem xét các tệp tin không được đưa vào hệ thống do các lỗi kỹ thuật.

Thủ tục kiểm toán

- Phòng vấn chuyên gia phát triển hoặc người vận hành hệ thống để xác định chính xác chính sách và các thủ tục từ chối dữ liệu đầu vào.
- Tiến hành thử nghiệm để xác nhận hệ thống sẽ cảnh báo và hướng dẫn xử lý các dữ liệu nhập vào vi phạm các nguyên tắc hợp lệ.
- Kiểm tra trường hợp dữ liệu bị từ chối thì chương trình sẽ xử lý ra sao. Cụ thể dữ liệu bị từ chối bị giữ lại hay vẫn đẩy thẳng vào cơ sở dữ liệu. Rà soát các dữ liệu bị giữ lại có ghi chú rõ lỗi, thời gian, người nhập dữ liệu.
- Đánh giá thủ tục xử lý khi dữ liệu nhập sai quá nhiều (khi người dùng cố ý nhập sai để dò dữ liệu chính xác).
- Phòng vấn cấp quản lý về việc xem xét dữ liệu lưu vết định kỳ để phát hiện các vấn đề liên quan đến việc nhập dữ liệu đầu vào và đo lường các lỗi phát sinh. Thu thập bằng chứng để hoạt động trên thực sự được thực hiện.

Kiểm soát A7.01.04 - Quy trình nhập và quản lý dữ liệu đầu vào

Tiêu chí kiểm toán

- Phân cấp xác nhận và phê duyệt theo chức năng nhiệm vụ trong xử lý giao dịch được thiết lập và hiện thực bởi những chốt kiểm soát đúng đắn;
- Có sự phân công trách nhiệm hợp lý trong việc nhập dữ liệu đầu vào;

- Có chốt kiểm soát bổ sung cho các trường hợp việc phân công trách nhiệm không thể thực hiện.

Tài liệu cần thu thập

- Yêu cầu tuân thủ của việc nhập dữ liệu đầu vào quy định trong các văn bản pháp quy và cơ quan quản lý;
- Tài liệu yêu cầu nghiệp vụ của phần mềm ứng dụng;
- Tài liệu hướng dẫn người sử dụng của phần mềm ứng dụng.

Thủ tục kiểm toán

▪ Tìm hiểu thiết kế của hệ thống đáp ứng việc xác nhận và phê duyệt theo chức năng nhiệm vụ trong xử lý giao dịch. Trên cơ sở đó xác nhận tính đúng đắn của việc xác nhận và phê duyệt theo đúng tính chất của các giao dịch trong thực tế. Đánh giá các quy tắc phân cấp xác nhận và phê duyệt liên quan đến nhập liệu, sửa dữ liệu, chấp nhận, từ chối được thiết kế tốt và mô tả đầy đủ trong các tài liệu.

▪ Quan sát việc phân cấp phân quyền hoạt động đúng trong môi trường thử nghiệm. Phân tích dữ liệu phân cấp phân quyền của đơn vị để xác nhận việc tuân thủ các quy định trên trong thực tế.

▪ Xác nhận việc tồn tại của bảng dữ liệu liên quan đến phân quyền phân cấp cho từng cá nhân. Rà soát dữ liệu trên với dữ liệu phân quyền người dùng của hệ thống. Kiểm tra sự tuân thủ trong việc một cá nhân không được phép vừa nhập dữ liệu, vừa xác nhận tính chính xác của dữ liệu. Xác nhận có chốt kiểm soát bổ sung trong trường hợp việc phân quyền phân cấp không thể thực hiện.

Vấn đề A7.02 - Quy trình xử lý dữ liệu của ứng dụng

Mục tiêu kiểm toán

Đánh giá việc phần mềm ứng dụng đảm bảo tính nhất quán, hợp lệ và tin cậy của dữ liệu trong quá trình xử lý các giao dịch nghiệp vụ.

Kiểm soát A7.02.01 - Việc tin học hóa các quy tắc nghiệp vụ

Tiêu chí kiểm toán

Các giao dịch của ứng dụng vận hành đáp ứng các yêu cầu nghiệp vụ mong đợi

Tài liệu cần thu thập

- Tài liệu phát triển hệ thống của phần mềm ứng dụng.
- Tài liệu yêu cầu nghiệp vụ của phần mềm ứng dụng.

- Sơ đồ luân chuyển dữ liệu của phần mềm ứng dụng.
- Danh sách các giao dịch quan trọng.
- Mã nguồn của chương trình.

Thủ tục kiểm toán

- Nghiên cứu phần mềm hệ thống thông qua sơ đồ luân chuyển dữ liệu và tài liệu liên quan đến những yêu cầu nghiệp vụ.
- Rà soát tài liệu phát triển hệ thống, kết hợp với phân tích dữ liệu, xem mã chương trình nhằm đánh giá tính đúng đắn, khả năng áp dụng của phần mềm. Cần phân tích dữ liệu để xác nhận tính chính xác của việc xử lý.
- Thử nghiệm trực tiếp phần mềm kết hợp với phân tích dữ liệu để đảm bảo danh sách các giao dịch quan trọng được vận hành đúng trong thực tế.

Kiểm soát A7.02.02 - Đảm bảo tính nhất quán và toàn vẹn của các giao dịch nghiệp vụ

Tiêu chí kiểm toán:

- Phần mềm nhận diện chính xác các lỗi giao dịch.
- Tính nhất quán của dữ liệu vẫn được đảm bảo ngay cả khi có những sự cố phát sinh làm dừng việc xử lý giao dịch ngoài ý muốn.
- Có cơ chế đầy đủ cho việc xử lý lỗi giao dịch, rà soát các tập tin bị treo do bị ngừng cũng như xóa bỏ các tập tin bị ngừng như trên.

Tài liệu cần thu thập:

- Tài liệu phát triển hệ thống.
- Tài liệu yêu cầu nghiệp vụ.
- Các báo cáo bị hỏng do không đảm bảo các quy tắc cân đối trong kế toán.
- Quy định đối chiếu dữ liệu.
- Thủ tục rà soát các báo cáo.
- Các tập tin dữ liệu bị dừng lại do lỗi hệ thống.

Thủ tục kiểm toán:

- Đánh giá phần mềm có đầy đủ các hàm kiểm tra tự động để đảm bảo tính nhất quán trong quá trình xử lý. Thu thập các thiết kế chức năng và hiện thực thực tế liên quan đến các lỗi xử lý tuần tự, bị trùng lặp dữ liệu hoặc các lỗi sai liên quan đến tham chiếu, ...

- Thu thập các quy định đối chiếu và các tài liệu liên quan phục vụ cho việc xác nhận tính toàn vẹn của quá trình xử lý dữ liệu dựa trên số lượng đầu vào khớp với số lượng đầu ra. Truy vết các giao dịch qua quá trình xử lý dữ liệu để đảm bảo các quy tắc cân đối tài chính của dữ liệu hoạt động hiệu quả. Thu thập các dữ liệu trong hệ thống phản ánh quá trình đảm bảo cân đối trên.

- Xác nhận khi các báo cáo xuất ra không đạt do dữ liệu tài chính mất cân đối thì có quy trình xử lý việc rà soát, phê duyệt của cấp có thẩm quyền.

- Tiến hành kiểm thử trực tiếp các dữ liệu đầu vào để đảm bảo dữ liệu đầu ra được xử lý chính xác. Chú ý tập trung vào các dữ liệu đầu vào sẽ tạo ra lỗi.

- Kiểm tra các công cụ kỹ thuật nếu có trong việc bảo đảm tính nhất quán của dữ liệu khi xảy ra sự cố kỹ thuật. Điều tra hệ thống truy vết, các tài liệu kế hoạch để đảm bảo khi xảy ra sự cố kỹ thuật bất ngờ, dữ liệu vẫn được đảm bảo tính nhất quán.

- Kiểm tra các tập tin chứa dữ liệu bị ngừng lại do một số lỗi kỹ thuật được xử lý đúng theo quy định nghiệp vụ.

Vấn đề A7.03 - Dữ liệu đầu ra của ứng dụng

Mục tiêu kiểm toán

Đánh giá tính đầy đủ và chính xác dữ liệu đầu ra của phần mềm ứng dụng trước khi sử dụng và việc bảo vệ dữ liệu đầu ra sử dụng đúng mục đích.

Kiểm soát A7.03.01 - Tính nhất quán và chính xác của dữ liệu đầu ra

Tiêu chí kiểm toán

- Các thủ tục được thiết kế nhằm đảm bảo tính chính xác và đầy đủ của dữ liệu đầu ra trước khi chuyển các bước xử lý tiếp theo và chuyển cho người dùng cuối;

- Việc theo dõi dữ liệu ra có thể bật/tắt đúng đắn;
- Dữ liệu đầu ra được rà soát nhằm đảm bảo tính chính xác và hợp lý;
- Các kiểm soát về tính đầy đủ và chính xác thông tin hoạt động hiệu quả.

Tài liệu cần thu thập

- Hệ thống kiểm soát đảm bảo tính đầy đủ và chính xác của dữ liệu;
- Thủ tục tạo cân bằng và rà soát dữ liệu đầu ra;
- Danh sách các báo cáo và dữ liệu đầu ra dưới dạng số hóa;
- Một số dữ liệu đầu ra được chọn mẫu.

Thủ tục kiểm toán

- Thu thập danh sách các báo cáo, dữ liệu đầu ra cung cấp cho người dùng. Xác nhận các dữ liệu đầu ra đã được thử nghiệm tính toán vẹn và chính xác trước khi được tái sử dụng hoặc chuyển cho bộ phận khác.

- Kiểm tra sự cân bằng và đối chiếu dữ liệu đầu ra được hướng dẫn cụ thể trong các tài liệu.

- Tiến hành thử nghiệm tính cân đối và đối chiếu trên một số dữ liệu đầu ra;

- Thực hiện lại các thủ tục kiểm soát về tính đầy đủ và chính xác của dữ liệu đầu ra.

- Kiểm tra tính hợp lý của một số thuộc tính của báo cáo đầu ra như tiêu đề, thời gian, địa điểm, người chuẩn bị, ...

- Xác nhận các lỗi kỹ thuật trọng yếu đều được ghi nhật ký và báo cáo đầy đủ.

Kiểm soát A7.03.02 - Bảo vệ dữ liệu đầu ra

Tiêu chí kiểm toán

- Dữ liệu đầu ra được phân loại và bảo vệ hợp lý.

- Việc phân phối các báo cáo được kiểm soát thích hợp.

Tài liệu cần thu thập

- Thủ tục xử lý và lưu trữ dữ liệu đầu ra;

- Chính sách phân loại thông tin của đơn vị.

Thủ tục kiểm toán

- Rà soát các thủ tục xử lý và lưu trữ dữ liệu đầu ra về tính bảo mật và cung cấp chính xác cho đối tượng được phép tiếp cận. Đánh giá các thủ tục trên được quy định rõ ràng và lưu giữ nhật ký các lỗi phát sinh. Đánh giá hệ thống đối chiếu giữa đầu ra và đầu vào để đảm bảo tính nhất quán trước khi phát hành báo cáo.

- Kiểm tra việc phân loại thông tin cho các dữ liệu đầu ra đặc biệt là các quy định kỹ thuật về thiết bị tiếp cận. Rà soát quy trình cung cấp thông tin nhạy cảm và xác nhận hệ thống trên hoạt động hiệu quả.

Vấn đề A7.04 - An toàn phần mềm ứng dụng.

Mục tiêu kiểm toán

Đánh giá việc đảm bảo thông tin của phần mềm ứng dụng không được dùng vào các mục đích trái phép.

Kiểm soát A7.04.01 - Hệ thống truy vết

Tiêu chí kiểm toán

- Có hệ thống truy vết lưu giữ việc thay đổi, tạo mới và thông tin người nhập của các giao dịch quan trọng;
- Hệ thống truy vết được rà soát nhằm giám sát những hoạt động bất thường;
- Hệ thống truy vết được bảo vệ và bảo trì đầy đủ;
- Mọi giao dịch đều được đánh số xác định theo tính tuần tự bởi một số duy nhất.

Tài liệu cần thu thập

- Cấu trúc và tài liệu hệ thống truy vết;
- Các chính sách quy định về việc thay đổi dữ liệu;
- Thủ tục rà soát dữ liệu phần mềm;
- Sơ đồ lưu chuyển dữ liệu toàn hệ thống phần mềm ứng dụng.

Thủ tục kiểm toán

- Thu thập tài liệu và đánh giá việc thiết kế, hiện thực, truy cập và rà soát hệ thống truy vết.
- Đánh giá cấu trúc hệ thống truy vết và các tài liệu khác nhằm xác nhận sự hiệu quả của hệ thống truy vết.
- Tìm hiểu ai có thể tắt hoặc xóa hệ thống giám sát.
- Xác nhận tính hiệu quả của việc rà soát định kỳ, giám sát hoạt động bất thường, cũng như rà soát của cấp trên dựa trên hệ thống lưu vết thông qua các thủ tục sau: Kiểm tra hệ thống truy vết, giao dịch, kết quả rà soát và các tài liệu khác; Quan sát các giao dịch hoặc phân tích dữ liệu; Thu thập các bằng chứng khác.
- Xem xét việc phân quyền cho việc tiếp cận dữ liệu lưu vết. Kiểm tra quyền truy cập cùng dữ liệu nhật ký truy cập đến dữ liệu lưu vết. Xác nhận chỉ có một số cá nhân được truy cập dữ liệu truy vết theo đúng chức năng nhiệm vụ. Đánh giá việc bảo vệ hệ thống lưu vết nhằm ngăn cản mọi sự thay đổi trái phép.
- Kiểm tra việc đánh số tuần tự cũng như tính hợp lý về thời gian của các giao dịch giám sát.

Kiểm soát A7.04.02 - Bảo vệ dữ liệu nghiệp vụ

Xem phần kiểm toán truy cập vật lý và truy cập phần mềm tại phần hướng dẫn kiểm toán An toàn thông tin.

Xem phần kiểm toán việc xây dựng kế hoạch khôi phục sau sự cố tại phần hướng dẫn kiểm toán Phát triển bền vững và khắc phục sự cố.

B. HƯỚNG DẪN CHI TIẾT KIỂM TOÁN DỰ ÁN CÔNG NGHỆ THÔNG TIN

1. Tóm tắt và cách sử dụng các chương trình kiểm toán mẫu B

a. Bố cục hướng dẫn

Hướng dẫn chi tiết kiểm toán dự án CNTT gồm 6 chuyên đề chia thành 2 nhóm:

- Nhóm 1 gồm 5 chuyên đề (chuyên đề B1 đến chuyên đề B5): Trình bày các chương trình kiểm toán mẫu của chuyên đề liên quan đến dự án CNTT nói chung.
- Nhóm 2 gồm duy nhất chuyên đề B6: Trình bày các chương trình kiểm toán mẫu của dự án CNTT sử dụng ngân sách nhà nước.

Ngoài ra, nên tham khảo thêm Chuyên đề A2 - Phát triển, mua sắm và tiếp nhận các sản phẩm CNTT như là nền móng cơ bản của kiểm toán dự án CNTT.

b. Cách áp dụng trong thực tế

Nếu kiểm toán dự án CNTT chỉ dừng ở mức cơ bản tập trung vào vấn đề phát triển, mua sắm và tiếp nhận các sản phẩm CNTT có thể tham khảo Chuyên đề A1200 Kiểm toán việc phát triển, mua sắm và tiếp nhận các sản phẩm CNTT.

Các cuộc kiểm toán dự án CNTT lĩnh vực Ngân sách thường sẽ sử dụng chương trình kiểm toán mẫu ở Chuyên đề 7 liên quan đến việc các dự án CNTT sử dụng ngân sách nhà nước. Các chương trình kiểm toán mẫu ở Chuyên đề 7 tập trung về tính tuân thủ theo các quy định của nhà nước liên quan đến việc đầu tư CNTT.

Các cuộc kiểm toán CNTT thông thường sẽ sử dụng chương trình kiểm toán mẫu ở Chuyên đề 2 đến 6 liên quan đến việc các dự án CNTT phục vụ cho tổ chức. Các chương trình kiểm toán mẫu ở các chuyên đề trên tập trung về tính đánh giá hiệu quả, hiệu lực và kinh tế từ các thông lệ quản lý CNTT tốt hoặc theo các chuẩn mực trên thế giới.

Các cuộc kiểm toán chuyên đề dự án CNTT có thể nên kết hợp cả hai nguồn chương trình kiểm toán mẫu ở cả 7 Chuyên đề phù hợp nhất với mục tiêu và loại hình của cuộc kiểm toán.

2. Chuyên đề B1 - Công tác khởi động dự án

a. Khái niệm

Giai đoạn khởi động dự án là giai đoạn tiến hành các bước chuẩn bị cơ bản và xin cấp phép chính thức thực hiện dự án.

Giai đoạn này thực hiện việc chuẩn bị phạm vi dự án, khởi tạo đội dự án, chuẩn bị và phê duyệt kinh phí, kịch bản kinh doanh. Thông thường giai đoạn khởi động này có thể bao gồm bước đánh giá tính khả thi của dự án (cho toàn bộ chương trình dự án hay một phần của dự án (ví dụ như giai đoạn thiết kế kỹ thuật).

b. Các rủi ro liên quan

- Các kịch bản kinh doanh không được ghi chép, phê duyệt một cách đầy đủ và chính thức
- Quy trình thực hiện việc tìm hiểu phạm vi, đánh giá tiền khả thi và phân tích khả thi dự án không được thực hiện một cách đúng đắn cũng như được văn bản hóa chính thức
- Không có quy trình văn bản chính thức cho việc lựa chọn/mua sắm, phân tích môi trường, phân tích tài chính hoặc các quy trình và phân tích không được thực sự thực hiện một cách đúng đắn
- Kinh phí lên kế hoạch cho dự án không đủ để hoàn thành dự án

c. Các vấn đề kiểm toán thành phần

Vấn đề đánh giá tính khả thi dự án

- Báo cáo phân tích tính khả thi của dự án có được văn bản hóa một cách rõ ràng và chi tiết?
- Trong giai đoạn phân tích tính khả thi của dự án có sự tham gia của các phòng ban liên quan như phòng triển khai và vận hành hệ thống không?
- Trong báo cáo phân tích tính khả thi có phản ánh bất kỳ thay đổi trọng yếu nào so với mục tiêu ban đầu?
- Thiết kế sơ bộ có đủ mức độ chi tiết để ước đoán chi phí, phân tích chi phí/lợi ích và đánh giá mức độ ảnh hưởng của dự án không?
- Thiết kế sơ bộ có đủ thông tin đáp ứng được yêu cầu của người dùng/người đọc hay không?
- Thiết kế sơ bộ có tuân theo các chuẩn mực của đơn vị quy định hay không?

- Đánh giá tính khả thi có hỗ trợ việc ra kết luận và đưa ra các khuyến nghị không?
- Các khuyến nghị có phù hợp với chính sách và văn hóa của đơn vị hay không?
- Báo cáo phân tích tính khả thi có được trình lên ban lãnh đạo của công ty hay không?
- Phòng ban nào chịu trách nhiệm phê duyệt báo cáo phân tích tính khả thi?
- Bộ phận kiểm soát nội bộ có xây dựng báo cáo đưa ra ý kiến và các khuyến nghị trên báo cáo phân tích tính khả thi dự án hay không?

Vấn đề thẩm định dự án

- Dự án có được thẩm định và phê duyệt một cách chính thức bởi cấp lãnh đạo có thẩm quyền hay không?
- Khi phê duyệt dự án, trong kế hoạch đánh giá tính khả thi dự án có xem xét tới lựa chọn thay thế không?
- Với mỗi lựa chọn có đánh giá xem xét trên đầy đủ các khía cạnh như lợi ích kinh doanh, chi phí và sự phù hợp với chiến lược của đơn vị không?
- Những đánh giá về lợi ích kinh doanh của dự án có thực sự khả thi và đo đạc tính toán được không? Phương pháp để thực hiện việc đo đạc tính toán đó là gì?
- Trong tình huống kinh doanh có bao gồm phần chi phí đào tạo nhân viên và việc phát triển kế hoạch vận hành liên tục hay không?
- Sự tồn tại của các tình huống kinh doanh có dựa chủ yếu trên sự đánh giá dài hạn hay không?
- Việc phân tích chi phí/lợi nhuận có xem xét phần tính toán dung sai (ví dụ 10%) trong trường hợp chi phí dưới mức dự đoán hay lợi nhuận vượt mức dự đoán hay chưa?
- Rủi ro của dự án đã được xác định, tính toán và cân nhắc bởi các cấp có thẩm quyền hay chưa?

Phạm vi và kế hoạch khởi động dự án

- Liệu dự án có sự kết nối một cách rõ ràng tới các yêu cầu của đơn vị trong hiện tại và tương lai không?
- Dự án có xác định được một cách rõ ràng:
 - Sản phẩm bàn giao tại mỗi giai đoạn của dự án
 - Khung thời gian và thời hạn cho mỗi giai đoạn của dự án
 - Phân bổ ngân sách và các tài nguyên cho mỗi giai đoạn của dự án

- Tổ chức dự án và vai trò trách nhiệm của từng vị trí
- Tổ chức theo dõi và báo cáo tiến độ dự án
- Các tiêu chuẩn bảo đảm chất lượng dự án được áp dụng tại mỗi giai đoạn của dự án
- Tổ chức thực hiện đánh giá các rủi ro ảnh hưởng tới sự hoàn thành của dự án

d. Chương trình kiểm toán mẫu

Vấn đề B1.01 - Công tác quản trị dự án tại giai đoạn khởi động dự án

Mục tiêu kiểm toán

Các thủ tục và quy trình trong dự án cần được kiểm tra và phê duyệt bởi ban lãnh đạo. Các nguồn lực cho dự án cần được phân bổ và tính toán hợp lý đảm bảo tiến độ của dự án. Đơn vị cần có những chính sách, quy định để bảo đảm ban quản lý dự án báo cáo liên tục lên ban lãnh đạo, giúp ban lãnh đạo đơn vị kịp thời ứng phó với các vấn đề của dự án phát sinh.

Kiểm soát B1.01.01 - Các kịch bản kinh doanh cần được rà soát đánh giá của cấp quản lý

Tiêu chí kiểm toán

Đảm bảo kịch bản kinh doanh của dự án được tài liệu hóa và được cấp quản lý đánh giá xem xét, và phê duyệt. Kịch bản kinh doanh này là cơ sở hợp lý cho việc khởi động dự án, các lợi ích mong đợi, ước tính chi phí và các thuộc tính cơ bản để đánh giá sự thành công của dự án

Tài liệu yêu cầu

- Kịch bản kinh doanh được phê duyệt
- Các tài liệu đính kèm kịch bản kinh doanh

Đánh giá thiết kế và triển khai

- Phòng văn giám đốc dự án nhằm xác định đơn vị có xây dựng kịch bản kinh doanh. Kịch bản này có được phê duyệt bởi ban lãnh đạo hay không?
- Phòng văn các bên liên quan dự án (Stakeholders) về việc tham gia của họ trong quá trình chuẩn bị kịch bản kinh doanh.
- Rà soát kịch bản kinh doanh liệu trong đó có mô tả lý do thực hiện dự án, các lợi ích dự án mang lại, chi phí dự trù, ROI và KPI dự án không?

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B1.01.02: Đánh giá phạm vi dự án phù hợp với kiến trúc CNTT của đơn vị.

Tiêu chí kiểm toán

Dự án khởi động thông qua bước đánh giá tính khả thi, sự tương thích của dự án với kiến trúc CNTT của đơn vị

Tài liệu yêu cầu

- Báo cáo nghiên cứu tính khả thi được duyệt
- Hoặc, tài liệu được duyệt thể hiện phạm vi dự án và dự án hỗ trợ các mục tiêu đơn vị.

Đánh giá thiết kế và triển khai

- Phòng vận quản lý dự án liệu báo cáo nghiên cứu tính khả thi của dự án có được thực hiện hay không?
- Nếu dự án có thực hiện nghiên cứu tính khả thi thì thu thập, rà soát báo cáo nghiên cứu tính khả thi của dự án.
- Phòng vận với cấp quản lý nhằm xác định xem liệu phạm vi của dự án có được định nghĩa một cách đúng đắn hay không?
- Nếu dự án không thực hiện báo cáo nghiên cứu tính khả thi thì cần phải làm rõ bằng cách nào có thể đưa ra được phạm vi của dự án và dự án có hỗ trợ các mục tiêu của đơn vị hay không?
- Trong cả hai trường hợp, xác định xem phạm vi dự án ban đầu có được phê duyệt bởi cấp quản lý có thẩm quyền hay không?

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B1.01.02: Đánh giá vai trò và trách nhiệm của ban chỉ đạo dự án và các bên tham gia dự án

Tiêu chí kiểm toán

Đánh giá vai trò và trách nhiệm của ban chỉ đạo dự án và các bên tham gia dự án

Tài liệu yêu cầu

- Quyết định thành lập ban chỉ đạo dự án

- Quyền hạn ban chỉ đạo dự án
- Cấu trúc, thành phần ban chỉ đạo dự án và phương thức báo cáo.

Đánh giá thiết kế và triển khai

- Phòng văn giám đốc dự án và xác nhận trong khuôn khổ dự án có thành lập ban chỉ đạo để giám sát dự án không?
- Xác nhận trong thành phần ban chỉ đạo dự án có nhà điều hành tài trợ và chủ tịch không?
- Xác nhận liệu chủ tịch của ban chỉ đạo có đủ quyền hạn để chỉ đạo dự án hay không?
- Xác nhận vai trò của ban chỉ đạo dự án, rà soát điều lệ dự án cũng như các văn bản tương tự.
- Xác nhận đội dự án cấp cao sẽ báo cáo lên ban chỉ đạo và nhận chỉ định công việc từ ban chỉ đạo.
- Đánh giá sự phù hợp của vị trí giám đốc dự án

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B1.01.03: Các thủ tục và quy trình trong dự án phải được phê duyệt

Tiêu chí kiểm toán

Xác minh các thủ tục, quy trình trong dự án được xem xét và phê duyệt bởi cấp chức năng có thẩm quyền.

Tài liệu yêu cầu

- Yêu cầu về nguồn vốn của dự án được phê duyệt
- Chính sách phê duyệt của đơn vị

Đánh giá thiết kế và triển khai

- Phòng văn giám đốc dự án để xác định ai là cấp quản lý có thẩm quyền chịu trách nhiệm dự án? Thu thập bằng chứng xem liệu dự án có được phê duyệt bởi cấp có thẩm quyền không?
- Thu thập, rà soát xem liệu yêu cầu về nguồn vốn dự án có được phê duyệt của cấp có thẩm quyền hay không?
- Rà soát xem việc phê duyệt đó có tuân thủ theo quy định và chính sách của đơn vị hay không?

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B1.01.04: Các chỉ số đánh giá mức độ thành công của dự án phải được xây dựng.

Tiêu chí kiểm toán

Dự án có xây dựng các chỉ số đánh giá mức độ thành công của dự án

Tài liệu yêu cầu

- Tài liệu xây dựng ROI (lợi tức đầu tư) và các KPI (chỉ số đo lường hiệu quả công việc)

- Kịch bản kinh doanh

Đánh giá thiết kế và triển khai

- Phòng vận giám đốc dự án liệu dự án có xây dựng ROI và KPI để tính toán mức độ thành công của dự án hay không?

- Rà soát kịch bản kinh doanh và xác định xem ROI có được đề cập trong kịch bản hay không?

- Thu thập bằng chứng về việc xây dựng các chỉ số KPI trong dự án

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B1.01.05: Quy trình quản lý cơ chế leo thang phải được ban hành chính thức.

Tiêu chí kiểm toán

Đơn vị ban hành chính thức quản lý cơ chế leo thang để giải quyết những vấn đề nghiêm trọng, cấp bách

Tài liệu yêu cầu

- Quy trình và thủ tục của cơ chế leo thang
- Cách thức phổ biến cơ chế của ban lãnh đạo
- Bằng chứng về các vấn đề được giải quyết

Đánh giá thiết kế và triển khai

- Phòng vận giám đốc dự án nhằm xác định xem đơn vị có ban hành quản lý cơ chế leo thang khi xảy ra vấn đề nghiêm trọng không? Sau khi áp dụng cơ chế leo thang, vấn đề sẽ được trình lên các cấp chức năng nào? Quy trình, thủ tục của cơ chế này?
- Phòng vận xác định cách thức mà ban lãnh đạo sẽ áp dụng để phổ biến cơ chế này tới toàn đội dự án (email, văn bản, thuyết trình...).
- Thu thập, rà soát các bằng chứng về các vấn đề đã được giải quyết theo cơ chế leo thang. Chi tiết của vấn đề giải quyết tuân theo quy chế leo thang được ghi chép đầy đủ.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B1.01.06: Đánh giá các tiêu chí ra quyết định mua mới hay đơn vị tự phát triển ứng dụng.

Tiêu chí kiểm toán

Xác định các tiêu chí được dùng để hỗ trợ việc ra quyết định mua mới hoặc tự xây dựng của ban lãnh đạo

Tài liệu yêu cầu

- Bảng chứng về các tiêu chí và yếu tố đã được phê duyệt
- Bảng chứng về các quyết định

Đánh giá thiết kế và triển khai

- Phòng vận giám đốc dự án nhằm xác định các thủ tục quy trình khi ra một quyết định tự mua hoặc tự xây dựng? (Quyết định bị ảnh hưởng bởi các tiêu chí, yếu tố đánh giá nào?)
- Thu thập, rà soát các bằng chứng về các tiêu chí và yếu tố đã được phê duyệt và tài liệu hóa để ra quyết định tự mua hoặc tự xây dựng
- Thu thập bằng chứng các chỉ tiêu đánh giá áp dụng cho dự án của đơn vị và xác định quyết định đó không bị ảnh hưởng bởi các yếu tố bên ngoài (như tiền thưởng, lợi ích cá nhân...)

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Vấn đề B1.02.00 - Công tác Quản lý dự án trong giai đoạn khởi động dự án

Mục tiêu kiểm soát

Quản lý dự án bao gồm các khía cạnh: quy mô dự án, giải quyết các vấn đề phát sinh theo quy chế đã ban hành, các yêu cầu phát sinh phục vụ dự án... Các cá nhân tổ chức có thẩm quyền (ban lãnh đạo, đội dự án, các bên tham gia) phải theo dõi giám sát các thông tin về dự án như: tài chính, ngân sách, tiến độ dự án, sự cố & rủi ro và cần có những biện pháp giải quyết kịp thời, cần thiết và hợp lý (ví dụ: cơ chế leo thang).

Kiểm soát B1.02.01: Vai trò và trách nhiệm của đội dự án

Tiêu chí kiểm toán

Các đội quản lý thông tin và nghiệp vụ được kết hợp, yêu cầu thông tin được tài liệu hóa một cách rõ ràng. Các mục tiêu của dự án phù hợp với chiến lược kinh doanh và các đơn vị kinh doanh chịu ảnh hưởng bởi dự án tham gia vào dự án.

Tài liệu yêu cầu

- Tài liệu về mục tiêu của đơn vị
- Sơ đồ tổ chức đội dự án
- Quy trình đảm bảo sự tham gia và thống nhất các đơn vị kinh doanh

Đánh giá thiết kế và triển khai

- Phòng văn giám đốc dự án xác định: đội dự án được thành lập có phù hợp với mục tiêu của đơn vị không?
- Thu thập sơ đồ tổ chức đội dự án;
- Phòng văn giám đốc dự án xác định trong trường hợp giám đốc dự án thuộc bên CNTT thì quy trình đảm bảo sự tham gia và thống nhất của các đơn vị kinh doanh.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B1.02.02: Năng lực và kinh nghiệm của các thành viên trong đội dự án phải được đánh giá.

Tiêu chí kiểm toán

Quản lý dự án và các thành viên của đội dự án có kinh nghiệm và năng lực phù hợp

Tài liệu yêu cầu

- Tài liệu, đánh giá các thành viên đội dự án
- Tài liệu về bổ nhiệm vị trí quản lý dự án

Đánh giá thiết kế và triển khai

▪ Thu thập rà soát các tài liệu được phê duyệt bởi ban lãnh đạo bổ nhiệm vị trí quản lý dự án. Đánh giá nhân sự được bổ nhiệm có phù hợp về năng lực và chuyên môn và kỹ năng lãnh đạo không?

▪ Đánh giá xem liệu có bất kỳ hạn chế hay rào cản nào bất lợi để thực hiện việc quản lý dự án một cách hiệu quả.

▪ Thu thập rà soát các tài liệu, đánh giá các thành viên đội dự án về năng lực, kiến thức nghiệp vụ, chuyên môn.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B1.02.03: Quy trình phân tích và đánh giá rủi ro phải được thiết lập và thực thi trong giai đoạn khởi động dự án

Tiêu chí kiểm toán

Đánh giá quy trình phân tích rủi ro trong giai đoạn khởi động dự án

Tài liệu yêu cầu

- Quy trình giám sát
- Biên bản việc đánh giá rủi ro

Đánh giá thiết kế và triển khai

▪ Phòng vận quản lý dự án để xác định xem đội dự án có thực hiện công tác đánh giá rủi ro ban đầu không, quy trình như thế nào?

▪ Rà soát việc đánh giá rủi ro để xác định xem việc đánh giá là toàn diện và rủi ro có được xác định rõ ràng. Xem xét các rủi ro sau: rủi ro thông thường, rủi ro trong kinh doanh, rủi ro khi hoạt động, rủi ro tài chính, quy định và tổ chức.

▪ Rà soát quy trình giám sát để đảm bảo ban chỉ đạo dự án đã rà soát việc đánh giá rủi ro

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B1.02.04: Quy trình quản lý chất lượng dự án cần được thiết lập

Tiêu chí kiểm toán

Nhà tài trợ dự án đưa ra các tiêu chuẩn chất lượng cụ thể cho dự án

Tài liệu yêu cầu

- Chỉ tiêu chấp nhận người dùng
- Mô hình tài chính
- Kế hoạch đảm bảo chất lượng

Đánh giá thiết kế và triển khai

- Phòng văn quản lý dự án về quy trình quản lý chất lượng, các yêu cầu quản lý chất lượng tại đơn vị.
- Thu thập và rà soát các chỉ tiêu chấp nhận người dùng, quy trình rà soát các mô hình tài chính;
- Rà soát các quyết định quan trọng, ...
- Thu thập và rà soát các phê duyệt của ban quản lý về kế hoạch đảm bảo chất lượng, giao tiếp với đội dự án và các bên liên quan.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B1.02.05: Kế hoạch truyền thông phải được thiết lập, đánh giá và phê duyệt.

Tiêu chí kiểm toán

Đánh giá kế hoạch truyền thông, đảm bảo các bên liên quan dự án và ban lãnh đạo luôn nhận được thông tin kịp thời chính xác.

Tài liệu yêu cầu

- Kế hoạch truyền thông
- Phương thức thực hiện kế hoạch truyền thông
- Danh sách phân phối bao gồm các bên liên quan, thành viên tham gia dự án và đơn vị tài trợ.

Đánh giá thiết kế và triển khai

- Phòng văn quản lý dự án kế hoạch truyền thông được áp dụng trong dự án theo các nguyên tắc và quy chế nào? Bộ phận nào thực hiện kế hoạch truyền thông? Năng

lực của mỗi thành viên thực hiện kế hoạch truyền thông có đáp ứng yêu cầu của dự án không?

- Kế hoạch truyền thông có được ban chỉ đạo và các bên liên quan đánh giá và phê duyệt không? Các phương thức được áp dụng để thực hiện kế hoạch truyền thông (email, bản trình bày, báo cáo...), Xác minh danh sách phân phối bao gồm các bên liên quan, thành viên tham gia dự án và đơn vị tài trợ
- Thu thập và rà soát xem kế hoạch truyền thông bao gồm các báo cáo ngoại lệ không?

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Vấn đề B1.03 - Công tác Quản lý chi phí trong giai đoạn khởi động dự án

Mục tiêu kiểm toán

Ngân sách và các quy trình kế toán phải chính xác, hoàn thiện và cung cấp thông tin cần thiết cho quản lý dự án.

Kiểm soát B1.03.01 – Các nguyên tắc kế toán phải được tuân thủ trong giai đoạn khởi động dự án

Tiêu chí kiểm toán

Đánh giá việc sử dụng nguồn vốn cho các chi phí dự án (bao gồm chi tiêu nguồn vốn và chi phí dự án khác) tuân theo các nguyên tắc kế toán.

Tài liệu yêu cầu

- Quy trình phê duyệt sử dụng nguồn vốn dự án
- Bản ghi nhận tài khoản chi tiêu nguồn vốn

Đánh giá thiết kế và triển khai

- Phòng văn quản lý dự án về quy trình phê duyệt sử dụng nguồn vốn dự án. Khi sử dụng nguồn vốn, phải được chấp thuận và phê duyệt bởi các cấp có thẩm quyền (ban lãnh đạo...). Phòng văn ban lãnh đạo, quản lý dự án, kế toán trưởng xác định dự án áp dụng các quy chuẩn kế toán chung để tiến hành công tác kế toán dự án
- Phòng văn ban lãnh đạo/trưởng nhóm dự án, quản lý dự án, kế toán trưởng xác định các chi phí ban đầu sẽ được ghi nhận vào tài khoản chi tiêu nguồn vốn, được tài liệu hóa và phê duyệt của ban lãnh đạo.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Vấn đề B1.04.00 - Quản lý Nhà cung cấp dịch vụ bên ngoài trong giai đoạn khởi động dự án

Mục tiêu kiểm toán

Các chỉ tiêu để đánh giá dịch vụ của nhà cung cấp bên ngoài cần được thiết lập và tài liệu hóa một cách khách quan.

Kiểm soát B1.04.01 - Các tiêu chí đánh giá năng lực của đơn vị cung cấp bên ngoài cần được thiết lập thực thi.

Tiêu chí kiểm toán

Lựa chọn các đơn vị cung cấp dịch vụ bên ngoài phải dựa theo các tiêu chí đã được định nghĩa, tài liệu hóa chính thức và tuân theo thủ tục đã được cấp trên phê duyệt, quy định

Tài liệu yêu cầu

- Tài liệu về tiêu chí mời thầu của dự án
- Giải pháp khắc phục của đơn vị trong trường hợp đơn vị bên ngoài yếu kém hoặc thay đổi đơn vị cung cấp dịch vụ bên ngoài

Đánh giá thiết kế và triển khai

- Phòng văn ban lãnh đạo/quản lý dự án về các đơn vị cung cấp dịch vụ bên ngoài cho dự án. Đơn vị dựa theo tiêu chí nào để lựa chọn đơn vị.
- Giải pháp khắc phục khi một đơn vị bên ngoài không có khả năng đáp ứng trong lúc dự án tiến hành có được thiết lập, tài liệu hóa và phê duyệt bởi ban lãnh đạo không?
- Thu thập, rà soát các tài liệu liên quan đến các tiêu chí mời thầu của dự án
- Thu thập rà soát các tài liệu liên quan đến giải pháp khắc phục trong trường hợp năng lực đơn vị bên ngoài yếu kém, thay đổi đơn vị cung cấp dịch vụ bên ngoài.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

3. Chuyên đề B2 - Công tác xây dựng kế hoạch dự án

a. Khái niệm

Giai đoạn lên kế hoạch là sự chuẩn bị cho kế hoạch chi tiết của dự án. Xuyên suốt giai đoạn này, việc định nghĩa yêu cầu, mô tả các thuộc tính dữ liệu cụ thể và quy trình kinh doanh sẽ được chuẩn bị.

Đối với dự án mua sắm và triển khai giải pháp thì tại giai đoạn lên kế hoạch dự án này quy trình mua sắm sẽ được khởi tạo: bao gồm chuẩn bị hồ sơ mời thầu, đánh giá hồ sơ thầu, lựa chọn nhà cung cấp và thương thảo hợp đồng.

b. Các rủi ro liên quan

- Quy trình lựa chọn nhà thầu không phù hợp hoặc không được thực hiện một cách nghiêm túc

- Các điều khoản và điều kiện hợp đồng không mang lại các lợi thế cho việc quản lý chi phí dự án cũng như cho phép đơn vị giám sát công việc của nhà thầu

Ví dụ: Như trong điều kiện thanh toán dự án 95% khi bàn giao sản phẩm và 5% còn lại trong bảo hành bảo trì. Rất nhiều dự án đơn vị nhà thầu sau khi nhận 95% đã bỏ 5% còn lại khi rất nhiều các lỗi phát sinh sau khi đơn vị tiến hành chạy thực tế nhưng không được nhà thầu giải quyết

- Nhà thầu không có đủ năng lực để hoàn thành chất lượng dự án đúng hạn và trong chi phí cấp phép

- Phạm vi dự án không được thống nhất rõ ràng và hợp lý

- Nhà thầu không có đủ nguồn lực cũng như chuyên gia để hoàn thành dự án theo đúng tiến độ và chi phí

- Kế hoạch dự án không đủ để giải quyết các rủi ro đã được xác định

- Chi phí dự án không được phê duyệt một cách đúng đắn và hợp lý

Ví dụ: Các cấu phần/chức năng là sản phẩm miễn phí của nhà cung cấp nhưng đơn vị vẫn bị tính phí cho việc triển khai cấu phần/chức năng đó

- Nguồn lực dự án không sẵn sàng để tham gia thực hiện/hoàn thành dự án

- Các tiêu chí đánh giá thầu không đưa ra đầy đủ và đúng đắn. Việc đánh giá thầu không được thực hiện một cách tuân theo các tiêu chí thầu đã đưa ra trong việc lựa chọn nhà thầu, giải pháp

Ví dụ: Trong việc đưa ra tiêu chí đánh giá sản phẩm không đề cập tới việc các sản phẩm phần mềm không có bản quyền dẫn đến rủi ro cho đơn vị trong vấn đề hiệu năng và luật pháp liên quan tới sản phẩm

- Các kiểm soát không được thiết kế hoặc thực hiện một cách đúng đắn để quản lý dòng tiền trong dự án
- Không có báo cáo tình hình dự án để hỗ trợ cấp quản lý giám sát dự án
- Các chính sách và thủ tục không được văn bản hóa và chính thức hóa có thể dẫn tới việc thực hiện không nhất quán, dẫn tới dự án không hiệu quả và đội chi phí
- Cơ cấu chi phí dự án không được thiết kế hợp lý dẫn đến phân bổ chi phí không hiệu quả

c. Các vấn đề kiểm toán thành phần

Kế hoạch chi tiết dự án

Mục tiêu của giai đoạn này nhằm xác định xem liệu đội dự án có xây dựng một kế hoạch dự án phù hợp và dự án có tuân theo kế hoạch đã định không? Trong trường hợp có những điều chỉnh thì việc chỉnh sửa đó cần phải được ghi chép lại, bao gồm cả việc kéo dài thêm kế hoạch ban đầu.

- Kế hoạch dự án có được văn bản hóa hay không?
- Các mốc dự án trong kế hoạch đưa ra có thực tế và khả thi hay không?
- Trong kế hoạch có yêu cầu công tác phê duyệt của cấp quản lý tại một số bước quan trọng không?
- Kế hoạch dự án có được xây dựng bao gồm tất cả các bước quan trọng bao gồm giai đoạn kiểm thử, giai đoạn đào tạo, và chuyển đổi dữ liệu.

Yêu cầu người dùng

- Các yêu cầu người dùng có được ghi chép, văn bản hóa một cách rõ ràng và chi tiết không?
- Các mục tiêu kinh doanh được trình bày một cách rõ ràng không?
- Các giải pháp cho mục tiêu kinh doanh có được đề xuất trong phân tích yêu cầu người dùng?
- Hệ thống mới có bao gồm các chức năng kiểm toán cần thiết?
- Phân tích yêu cầu có bao gồm cả các yêu cầu tương lai trong hệ thống mới không?

- Các yêu cầu về việc kết nối với các hệ thống sẵn có của đơn vị có được xác định rõ ràng không?
- Liệu hệ thống mới có tương thích với các hệ thống sẵn có của đơn vị không?
- Liệu hệ thống mới có khả năng phục hồi sau khi bị lỗi không?
- Có sự tham gia của các phòng ban liên quan trong quá trình chuẩn bị xây dựng yêu cầu chức năng hệ thống không?
- Các yêu cầu hệ thống có bao gồm tính năng bảo mật và kiểm soát chưa?
- Các yêu cầu người dùng có phản ánh đúng các yêu cầu thực tế tại đơn vị?

Hợp đồng

- Các hợp đồng có đưa ra các yêu cầu về sản phẩm đúng theo như yêu cầu hay không?
- Hợp đồng có đề cập tới việc đánh giá cụ thể sản phẩm như thế nào không?
- Hợp đồng có chỉ ra cụ thể ngày tháng sản phẩm được bàn giao hay không?
- Hợp đồng có chỉ ra các mức độ để đánh giá sản phẩm hay không?
- Các hợp đồng có đưa ra các biện pháp giải quyết sửa chữa nếu như sản phẩm không đạt được tiêu chuẩn đặt ra hay không?
- Các hợp đồng có đề cập đến các yêu cầu bổ sung cần thiết khác (ví dụ như hệ thống bảo mật, hệ thống mật khẩu và chức năng lưu vết kiểm toán) không?
- Hợp đồng có cung cấp những nâng cấp phần cứng cần thiết không?
- Hợp đồng có đưa ra vấn đề người sử dụng sẽ yêu cầu những thay đổi như thế nào với phần mềm không?
- Hợp đồng có quy định chi phí để nâng cấp phần mềm không?
- Hợp đồng có quy định đề cập tới chi phí liên quan tới việc duy trì hiệu năng hay không?
- Các hướng dẫn hoạt động có được cung cấp quy định trong hợp đồng hay không?
- Hợp đồng có quy định việc cung cấp các hướng dẫn cho người dùng không?
- Hợp đồng có quy định việc cung cấp tài liệu hướng dẫn các khách hàng theo dõi và sửa chữa các lỗi?
- Thời gian bảo hành có được đề cập cụ thể trong hợp đồng hay không?

- Hợp đồng như hiện tại có khuyến khích nhà cung cấp hoàn thành hết hợp đồng hay không?
- Hợp đồng có quy định luật cụ thể của các tỉnh hay cả nước sẽ quy định hợp đồng này hay không?
- Địa điểm nơi đào tạo có được cung cấp cụ thể trong hợp đồng hay không?
- Hợp đồng có cung cấp việc đào tạo người dùng trong việc chuẩn bị dữ liệu thông tin đầu vào và sử dụng kết quả đầu ra của hệ thống hay không?
- Nhà cung cấp dịch vụ có tiếp tục hỗ trợ cho người mua trong khoảng thời gian hợp lý hay không?
- Nhà cung cấp có đảm bảo sản phẩm sẽ hoạt động đúng như trong hợp đồng quy định hay không?
- Nhà cung cấp có cung cấp việc đào tạo hay không?
- Nhà cung cấp dịch vụ có tiếp tục hỗ trợ cho người mua trong khoảng thời gian hợp lý hay không?
- Nhà cung cấp có quyền truy cập vào dữ liệu mật của khách hàng để bảo trì hay không?
- Đơn vị có thể huỷ bỏ hợp đồng vào bất cứ thời gian nào hay không?
- Hình thức phạt như thế nào đối với nhà cung cấp trong trường hợp họ không hoàn thành các yêu cầu của hợp đồng?
- Những điều khoản trong hợp đồng có phù hợp với các điều khoản yêu cầu của đơn vị không?
- Nếu hợp đồng bị huỷ bỏ, hợp đồng đã có cụ thể các dự phòng cho trường hợp này chưa?
- Nếu là hợp đồng thuê thì trong đó có cung cấp một điều khoản việc thuê có thể trở thành hợp đồng mua bán hay không?

Nhà thầu

- Có tiêu chuẩn đánh giá người cung cấp dịch vụ hay không?
- Có quy trình mời thầu chính thức hay không?
- Có quy trình chọn người cung cấp dịch vụ hay không?
- Đơn vị có được quyền bảo trì sản phẩm bởi các nhà cung cấp khác không?
- Quá trình chọn lựa nhà cung cấp có công bằng hay không?

- Nhà cung cấp được lựa chọn có khả năng hoạt động tới hết thời gian của hợp đồng hay không?

d. Chương trình kiểm toán mẫu

Vấn đề B2.01 - Thiết lập công tác quản trị dự án

Mục tiêu kiểm toán

Ban lãnh đạo cần thực hiện giám sát dự án liên tục và đầy đủ. Các nguồn lực kỹ thuật và nghiệp vụ cần được quy hoạch đầy đủ đảm bảo tiến độ của dự án. Đơn vị cần có những chính sách, quy định để bảo đảm ban quản lý dự án kịp thời nhận được thông tin và đệ trình các vấn đề lên cấp quản lý cao hơn nhằm ứng phó với các vấn đề phát sinh.

Kiểm soát B2.01.01: Tiến độ và nội dung thực hiện dự án cần được báo cáo thường xuyên.

Tiêu chí kiểm toán

Đảm bảo dự án đang đi đúng hướng so với kế hoạch và kịch bản ban đầu.

Tài liệu yêu cầu

- Tài liệu tổng quan về dự án (mục tiêu, phạm vi, giá trị hoạt động)
- Biên bản cuộc họp
- Tài liệu liên quan đến trao đổi kết quả phân tích giữa tổ dự án

Đánh giá thiết kế và triển khai

- Phòng văn ban quản lý dự án/trưởng nhóm dự án và thu thập tài liệu tổng quan về dự án bao gồm: mục tiêu, phạm vi, giá trị hoạt động cơ bản của án được gửi cho các bên liên quan trước khi lập kế hoạch dự án.

- Thu thập, rà soát các biên bản cuộc họp/tài liệu liên quan để xác minh dự án được tiến hành giữa trên sự đồng thuận của các đại diện các bộ phận liên quan, đơn vị chủ quản dự án và ban quản lý, đơn vị chủ quản dự án và ban quản lý

- Phòng văn ban quản lý dự án, tìm hiểu và xác minh tổ dự án có những thủ tục phân tích được thực hiện thường xuyên nhằm đảm bảo dự án đúng hướng so với kế hoạch và phương án ban đầu hay không?

- Thu thập và rà soát các tài liệu liên quan đến trao đổi kết quả phân tích giữa tổ dự án, các bên liên quan, xác minh xem, dự án có đi đúng hướng so với kế hoạch và phương án ban đầu không?

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B2.01.02: Các thay đổi của phạm vi dự án phải được phê duyệt.

Tiêu chí kiểm toán

Đảm bảo sự thay đổi phạm vi của dự án phải được phê duyệt bởi ban chỉ đạo dự án hoặc đơn vị chủ quản dự án.

Tài liệu yêu cầu

- Kế hoạch chi tiết cho từng giai đoạn bao gồm ít nhất các thông tin sau: kế hoạch chi tiết cho từng giai đoạn, quy trình chung, quy trình con, mốc dự án và việc phân bổ.
- Danh sách các thay đổi phạm vi của dự án
- Văn bản chấp thuận phê duyệt thay đổi

Đánh giá thiết kế và triển khai

- Phòng văn ban quản lý dự án/trưởng nhóm dự án và thu thập kế hoạch dự án đang được tổ dự án áp dụng. Rà soát và xác minh kế hoạch dự án bao gồm ít nhất các thông tin sau: kế hoạch chi tiết cho từng giai đoạn, quy trình chung, quy trình con, mốc dự án và việc phân bổ.
- Phòng văn ban quản lý dự án, tìm hiểu, thu thập các tài liệu về quy trình, thủ tục trong việc thay đổi phạm vi dự án, thu thập danh sách các thay đổi phạm vi của dự án trong giai đoạn kiểm toán, xác minh việc thay đổi phạm vi dự án theo đúng quy trình và thủ tục đã định, việc thay đổi phạm vi được phê duyệt bởi ban chỉ đạo dự án và đơn vị chủ quản dự án.

Thử nghiệm hiệu quả hoạt động

Dựa vào danh sách các thay đổi phạm vi của dự chọn mẫu và tiến hành các bước sau:

- Thu thập các văn bản chấp thuận phê duyệt thay đổi phạm vi của ban dự án
- Xác minh phạm vi dự án có được thay đổi kịp thời hay không
- Kiểm tra các thành phần ngoài phạm vi dự án có được định nghĩa rõ ràng hay không?

Kiểm soát B2.01.03: Vai trò, trách nhiệm và tính tách bạch trách nhiệm của các thành viên trong tổ dự án được xác định rõ ràng.

Tiêu chí kiểm toán

Đảm bảo vai trò, trách nhiệm của các thành viên trong tổ dự án được xác định rõ ràng. Đảm bảo tính tách bạch trách nhiệm trong tổ dự án.

Tài liệu yêu cầu

- Danh sách đội dự án và vai trò của mỗi người

Đánh giá thiết kế và triển khai

- Phòng vận ban quản lý dự án/Trưởng nhóm dự án và thu thập và danh sách đội dự án, xác minh các nhân sự chính: chủ đầu tư/đơn vị chủ quản dự án, trưởng nhóm dự án, đại diện ban chỉ đạo dự án

- Rà soát danh sách tổ dự án, xác minh danh sách tổ dự án có các thành viên đến từ: đơn vị kinh doanh, đơn vị phát triển hệ thống, ban vận hành CNTT, ban an toàn thông tin, kiểm toán nội bộ, nhà cung cấp ...

- Rà soát vai trò trách nhiệm của từng người và từng phòng ban trong danh sách tổ dự án. Xác minh việc phân công vai trò và nhiệm vụ đảm bảo tính tách bạch trách nhiệm.

- Xác định nhân sự chính trong tổ dự án chịu trách nhiệm đảm bảo về mặt phạm vi, thời gian và ngân sách của dự án.

- Xác định nhân sự chính chịu trách nhiệm về việc bảo đảm chất lượng, được ủy quyền sử dụng ngân sách, tiếp nhận các sản phẩm bàn giao và đưa ra quyết định tiếp tục thực hiện/dừng thực hiện tại các mốc quan trọng của dự án.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B2.01.04: Công thức tính toán lợi tức đầu tư (ROI) và chỉ số đánh giá hoạt động hiệu quả (KPI) của dự án được thiết lập một cách khách quan và được phê duyệt

Tiêu chí kiểm toán

Đảm bảo công thức tính toán ROI và KPI được phê duyệt bởi ban chỉ đạo dự án và đơn vị chủ quản dự án và được sử dụng như một thước đo, đo lường sự thành công của dự án.

Tài liệu yêu cầu

- Công thức tính toán chỉ số đánh giá hiệu quả công việc và lợi tức đầu tư
- ROI
- KPI

Đánh giá thiết kế và triển khai

- Phòng vấn ban quản lý dự án/trưởng nhóm dự án, tìm hiểu công thức tính toán lợi tức đầu tư và xác minh các thuộc tính được sử dụng trong công thức đó. Rà soát các thuộc tính mang tính chất khách quan, lặp đi lặp lại và các thông tin liên quan giữa giai đoạn này với giai đoạn khác.

- Phòng vấn ban quản lý dự án/trưởng nhóm dự án, tìm hiểu về công thức tính toán chỉ số đánh giá hiệu quả công việc, xác minh các thuộc tính được sử dụng trong công thức đó.

Thử nghiệm hiệu quả hoạt động

Dựa và công thức tính ROI vs KPI của tổ dự án, Kiểm toán viên nhà nước tiến hành chọn mẫu các thuộc tính trong công thức và tính toán lại. Kiểm toán viên nhà nước so sánh kết quả tính toán được với kết quả tính toán của đơn vị, đảm bảo hai kết quả này bằng nhau.

Kiểm soát B2.01.05: Các vấn đề được đệ trình cần phải được tiếp nhận và xử lý kịp thời.

Tiêu chí kiểm toán

Đảm bảo các vấn đề được đệ trình bởi tổ dự án được xử lý một cách hiệu quả, kịp thời.

Tài liệu yêu cầu

- Thủ tục giải quyết vấn đề được đệ trình.

- Danh sách các vấn đề được đệ trình trong thời gian diễn ra dự án

Đánh giá thiết kế và triển khai

▪ Phòng văn ban quản lý dự án/trưởng nhóm dự án, tìm hiểu về các thủ tục giải quyết vấn đề được đệ trình. Thu thập tài liệu mô tả các thủ tục liên quan tới việc giải quyết vấn đề được đệ trình.

▪ Xác minh trong thủ tục xử lý, các vấn đề được đệ trình cần phải được thông báo kịp thời cho ban chỉ đạo dự án và đơn vị chủ quản dự án.

Thử nghiệm hiệu quả hoạt động

Dựa vào danh sách các vấn đề được đệ trình trong thời gian diễn ra dự án, Kiểm toán viên nhà nước chọn mẫu và rà soát nội dung, phương án giải quyết nhằm đảm bảo vấn đề được xử lý theo đúng quy trình.

Kiểm soát B2.01.06: Quyết định mua hoặc tự xây dựng dự án phải dựa trên nghiên cứu tính khả thi và yêu cầu chức năng nghiệp vụ.

Tiêu chí kiểm toán

Đảm bảo việc được ra quyết định mua sắm/tự xây dựng (phần mềm/hệ thống) một cách phù hợp

Tài liệu yêu cầu

- Quy trình đánh giá yêu cầu/chức năng.
- Quy trình thủ tục liên quan tới việc mời thầu, phương pháp lựa chọn nhà thầu
- Danh sách các thành viên trong tổ dự án
- Tài liệu nghiên cứu tính khả thi về việc mua/hay tự xây dựng
- Các phân tích đánh giá về chi phí – lợi ích – bất lợi của việc đưa ra quyết định mua/hay tự xây dựng.

Đánh giá thiết kế và triển khai

▪ Phòng văn ban quản lý dự án/trưởng nhóm dự án, tìm hiểu quy trình đánh giá yêu cầu/chức năng để đơn vị đưa ra quyết định mua hoặc tự xây dựng (phần mềm, hệ thống...)

▪ Nếu đơn vị thực hiện tự xây dựng, xác minh xem đơn vị đã có kế hoạch tự xây dựng và đã liệt kê, tính toán các chi phí tương ứng hay chưa?

- Nếu đơn vị thực hiện mua ngoài, xác minh xem đơn vị có quy trình thủ tục liên quan tới việc mời thầu, phương pháp lựa chọn nhà thầu và đưa ra các tiêu chí lựa chọn nhà thầu hay chưa?

- Phòng văn ban quản lý dự án/trưởng nhóm dự án: thu thập danh sách các thành viên trong tổ dự án, xác minh tổ dự án có bao gồm các phòng ban chức năng, nghiệp vụ, ban vận hành CNTT, ban tài chính kế toán, ban luật pháp – những bộ phận hiểu biết về dự án để cùng thống nhất đưa ra quyết định mua hay tự xây dựng (phần mềm, hệ thống...)

- Nếu đơn vị thực hiện mua ngoài, phòng văn ban quản lý dự án, thu thập các tài liệu, biên bản họp liên quan tới thủ tục mời thầu, phương pháp lựa chọn nhà thầu, các tiêu chí lựa chọn nhà thầu.

- Phòng văn ban quản lý dự án/trưởng nhóm dự án xác minh các yêu cầu mua mới/tự xây dựng (phần mềm, hệ thống) đảm bảo tuân theo cấu trúc hệ thống CNTT và chiến lược CNTT tại đơn vị.

- Phòng văn ban quản lý dự án/trưởng nhóm dự án thu thập tài liệu nghiên cứu tính khả thi về việc mua/hay tự xây dựng để đáp ứng yêu cầu nghiệp vụ và chức năng. Thu thập các phân tích đánh giá về chi phí – lợi ích – bất lợi của việc đưa ra quyết định mua/hay tự xây dựng (phần mềm, hệ thống)

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề B2.02 - Công tác quản lý dự án phục vụ việc lập kế hoạch dự án

Mục tiêu kiểm toán

Đảm bảo dự án được thực hiện đúng theo kế hoạch đã định, giảm thiểu rủi ro, các sự cố được giải quyết, vấn đề được đề trình được báo cáo tới ban quản lý/đơn vị chủ quản dự án một cách kịp thời, đảm bảo về mặt chất lượng, tối ưu chi phí dự án và đưa ra được quyết định tiếp tục thực hiện/dừng thực hiện tại các mốc trọng yếu của dự án.

Kiểm soát B2.02.01: Đội quản lý nghiệp vụ và quản lý thông tin phối hợp với nhau để cùng xây dựng kế hoạch dự án.

Tiêu chí kiểm toán

Đảm bảo đội quản lý nghiệp vụ và quản lý thông tin phối hợp xây dựng kế hoạch dự án hiệu quả.

Tài liệu yêu cầu

Biên bản họp

Đánh giá thiết kế và triển khai

Phòng văn ban quản lý dự án/trưởng nhóm dự án, thu thập và rà soát các biên bản họp, xác minh tổ dự án bao gồm cả đội nghiệp vụ và đội thông tin, xác minh trong các buổi họp cần thiết, cả hai đội đều tham gia, xác minh không có bất kỳ sự bất hòa nào xảy ra trong đội, ảnh hưởng đến dự án

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B2.02.02: Các thành viên xây dựng kế hoạch dự án cần được đánh giá về kiến thức nghiệp vụ.

Tiêu chí kiểm toán

Đảm bảo kế hoạch dự án được xây dựng một cách hiệu quả dựa trên các thành viên có kiến thức về nghiệp vụ và giải pháp.

Tài liệu yêu cầu

- Bảng cấp/văn bản liên quan tới việc đánh giá trình độ
- Kế hoạch nhân sự của tổ dự án

Đánh giá thiết kế và triển khai

- Phòng văn ban quản lý dự án/trưởng nhóm dự án, thu thập và rà soát danh sách các thành viên trong tổ dự án, thu thập bằng cấp/văn bản liên quan tới việc đánh giá kinh nghiệm, kiến thức chuyên môn của những thành viên đóng vai trò chủ chốt trong dự án
- Phòng văn quản lý dự án/Trưởng nhóm dự án, xác nhận tính sẵn sàng của thành viên trong tổ dự án, đảm bảo rằng mọi thành viên trong tổ dự án đều nắm được thông tin thời gian tham gia của mình trong dự án.

- Phòng văn quản lý dự án/Trưởng nhóm dự án thu thập các thông tin liên quan tới vấn đề nhân sự trong tổ dự án: như có kế hoạch thay người trong đội, thêm người trong đội...

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B2.02.03: Các rủi ro tiềm tàng cần phải được xác định, phân tích, giám sát và xử lý trong giai đoạn lên kế hoạch dự án.

Tiêu chí kiểm toán

Đảm bảo đơn vị lường trước được một số các rủi ro có thể xảy ra trong dự án. Các rủi ro được báo cáo, giám sát và xử lý. Góp phần làm giảm thiểu rủi ro của dự án.

Tài liệu yêu cầu

- Bản phân tích đánh giá rủi ro trước dự án
- Thông tin về việc đơn vị đang hoặc sẽ sử dụng hệ thống/văn bản để giám sát rủi ro của dự án

Đánh giá thiết kế và triển khai

- Phòng văn ban quản lý dự án/trưởng nhóm dự án, thu thập bản phân tích đánh giá rủi ro trước dự án của đơn vị. Rà soát các nơi có thể xảy ra rủi ro trong bản phân tích, và xác minh đơn vị đã có hướng giải quyết để giảm thiểu rủi ro.

- Phòng văn quản lý dự án/Trưởng nhóm dự án, xác nhận đơn vị có các thủ tục bao gồm: báo cáo, theo dõi, và xử lý các rủi ro.

- Thu thập thủ tục quản lý rủi ro của đơn vị, rà soát các rủi ro trong ngưỡng chấp nhận được. Nếu rủi ro vượt qua ngưỡng chấp nhận được, đơn vị có thủ tục thông báo tới các bên liên quan hay không?

- Thu thập thông tin đảm bảo rằng đơn vị đang hoặc sẽ sử dụng hệ thống/văn bản để giám sát các rủi ro của dự án.

Thử nghiệm hiệu quả hoạt động

Dựa vào danh sách các rủi ro được đưa ra trong bản phân tích rủi ro trong giai đoạn lên kế hoạch dự án. Kiểm toán viên nhà nước chọn mẫu và tiến hành rà soát hướng giải quyết của đơn vị.

Trong mẫu các rủi ro đã chọn, xác minh rủi ro nào là rủi ro chấp nhận được, rủi ro nào bắt buộc phải giải quyết triệt để.

Nếu rủi ro của dự án đang được giám sát trên hệ thống/phần mềm quản lý rủi ro của đơn vị, xác minh các rủi ro trên đã được lên trên hệ thống.

Kiểm soát B2.02.04: Các vấn đề được đệ trình cần phải được tiếp nhận và xử lý kịp thời.

Tiêu chí kiểm toán

Đảm bảo các vấn đề được đệ trình bởi tổ dự án được xử lý một cách hiệu quả, kịp thời.

Tài liệu yêu cầu

- Tài liệu mô tả các thủ tục liên quan tới giải quyết vấn đề được đệ trình
- Biên bản các vấn đề được đệ trình

Đánh giá thiết kế và triển khai

Phòng văn ban quản lý dự án/trưởng nhóm dự án, tìm hiểu về các thủ tục giải quyết vấn đề được đệ trình. Thu thập tài liệu mô tả các thủ tục liên quan tới việc giải quyết vấn đề được đệ trình. Xác minh trong thủ tục xử lý, các vấn đề được đệ trình cần phải được thông báo kịp thời cho ban chỉ đạo dự án và đơn vị chủ quản dự án.

Thử nghiệm hiệu quả hoạt động

Dựa vào danh sách các vấn đề được đệ trình trong thời gian diễn ra dự án, Kiểm toán viên nhà nước chọn mẫu và rà soát nội dung cũng như phương án giải quyết nhằm đảm bảo vấn đề được xử lý theo đúng quy trình.

Kiểm soát B2.02.05: Kế hoạch cho quy trình đảm bảo chất lượng cần phải được thiết lập.

Tiêu chí kiểm toán

Chất lượng được đảm bảo

Tài liệu yêu cầu

- Kế hoạch đảm bảo chất lượng của đơn vị
- Kế hoạch quản lý dự án
- Thông tin về vai trò của từng người trong nhóm đảm bảo chất lượng

Đánh giá thiết kế và triển khai

- Phòng văn trưởng nhóm quản bảo đảm chất lượng dự án, thu thập kế hoạch đảm bảo chất lượng của đơn vị, rà soát xác minh tại những nơi cần quyết định quan trọng trong bản kế hoạch có các yêu cầu như thuyết trình, tiêu chí và giả định.
- Xác minh rằng việc đảm bảo chất lượng dự án dự trên việc đáp ứng các yêu cầu nghiệp vụ và chức năng, các báo cáo nghiên cứu khả thi, và các tiêu chí được về chất lượng được đề ra trước đó.
- Đảm bảo kế hoạch quản lý dự án được rà soát và phê duyệt độc lập của đội ngũ kỹ thuật, đội ngũ kinh doanh và đơn vị chủ quản dự án.
- Phòng văn trưởng nhóm bảo đảm chất lượng dự án, đảm bảo tính thiết thực và hiệu quả của kế hoạch đảm bảo chất lượng. Xác minh bản kế hoạch có nêu ra yêu cầu phê duyệt cho sản phẩm bàn giao, các tài liệu cần rà soát, các giả định hợp lý và bám sát quy trình dự án hay không?
- Phòng văn trưởng nhóm bảo chất lượng dự án, thu thập và xác minh vai trò trách nhiệm của từng người trong nhóm đảm bảo chất lượng.
- Phòng văn trưởng nhóm đảm bảo chất lượng dự án, xác minh xem đơn vị có tiến hành đảm bảo chất lượng cho việc lên kế hoạch dự án hay không? Nếu có thu thập các tài liệu liên quan.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B2.02.06: Phương pháp luận phát triển của dự án cần phải được định nghĩa và đánh giá tính phù hợp.

Tiêu chí kiểm toán

Đảm bảo phương pháp luận phát triển được đưa ra, phù hợp với kích thước, phạm vi, và kiến trúc dự án

Tài liệu yêu cầu

- Phương pháp luận phát triển hệ thống
- Tài liệu đặc tả thiết kế dự án

Đánh giá thiết kế và triển khai

- Phòng văn ban quản lý dự án/trưởng nhóm dự án, thu thập và xác minh phương pháp luận phát triển hệ thống đang được sử dụng cho dự án (như Agile, Development Life Circle...)

- Phòng văn ban quản lý dự án/trưởng nhóm dự án, rà soát phương pháp luận phát triển hệ thống mà đơn vị đang sử dụng, xác minh các đặc tả thiết kế cấp cao được chuyển thể từ các yêu cầu nghiệp vụ cho việc phát triển phần mềm.

Dựa vào phương pháp luận phát triển mà đơn vị sử dụng, dựa vào đặc tả thiết kế của đơn vị, Kiểm toán viên nhà nước tiến hành xác minh

- Phương pháp luận mà đơn vị sử dụng là gì? Với kích thước, quy mô và cấu trúc dự án như vậy thì việc sử dụng phương pháp luận phát triển trên có phù hợp hay không?
- Tài liệu đặc tả thiết kế của dự án ở mức độ cao cấp có thể hiện các yêu cầu nghiệp vụ hay không?

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B2.02.07 – Các tài liệu liên quan tới việc thay đổi cần tuân thủ thủ tục quản lý thay đổi và được phê duyệt.

Tiêu chí kiểm toán

Đảm bảo các tài liệu liên quan tới việc thay đổi trong phạm vi, tình huống kinh doanh hay các thuộc tính quan trọng của dự án đều được tài liệu hóa và phê duyệt.

Tài liệu yêu cầu

- Tài liệu liên quan tới việc phân tích thay đổi

Đánh giá thiết kế và triển khai

- Phòng văn ban quản lý dự án/trưởng nhóm dự án về thủ tục quản lý thay đổi, xác minh rằng với mỗi yêu cầu thay đổi đều được tài liệu hóa và phê duyệt.

- Rà soát thủ tục quản lý thay đổi, xác minh những các phần của dự án mà chỉ cần phê duyệt của quản lý dự án và các phần bắt buộc phải có sự phê duyệt của ban chỉ đạo dự án và đơn vị chủ quản dự án

- Thu thập tài liệu liên quan tới việc phân tích thay đổi để đánh giá ảnh hưởng của các thay đổi đó tới dự án: các rủi ro trọng yếu có thể xảy ra, chi phí, ngày bàn giao sản phẩm...

Thử nghiệm hiệu quả hoạt động

Dựa vào danh sách các thay đổi của dự án, Kiểm toán viên nhà nước chọn mẫu và xác minh các thông tin về việc quản lý thay đổi trong giai đoạn lên kế hoạch dự án như sau:

- Xác minh yêu cầu thay đổi được tài liệu hóa và phê duyệt bởi các cấp tương ứng
- Xác minh đơn vị có thực hiện phân tích thay đổi, liệt kê ra ảnh hưởng của các thay đổi đó đối với dự án như các rủi ro trọng yếu, chi phí, ngày bàn giao sản phẩm.

Kiểm soát B2.02.08 – Các kiểm soát quan trọng cần phải được định nghĩa trong kế hoạch dự án.

Tiêu chí kiểm toán

Kế hoạch phải có các kiểm soát quan trọng bao gồm kiểm soát thời gian hiệu quả, kiểm soát kế hoạch dự án cùng với mốc dự án, sản phẩm bàn giao, chuỗi quy trình, nguồn lực dự kiến, và các hoạt động phụ thuộc (nếu có).

Tài liệu yêu cầu

- Kế hoạch dự án
- Tài liệu kế hoạch dự án

Đánh giá thiết kế và triển khai

- Phòng văn ban quản lý dự án/trưởng nhóm dự án, thu thập kế hoạch dự án, rà soát và xem xét mức độ chi tiết cho từng giai đoạn, các mục nhỏ và nhiệm vụ tương ứng, nguồn lực cần thiết, tài liệu/sản phẩm cần bàn giao, cột mốc thời gian, và các hoạt động phụ thuộc (nếu có)
- Xác minh các mốc dự án có trong kế hoạch và các nhiệm vụ cần phải hoàn thành.
- Xác minh rằng dự án tận dụng được tối đa nguồn nhân lực (như kế hoạch tăng ca ...)
- Xác minh các sản phẩm bàn giao cho từng hoạt động
- Xác minh các giả định, các ràng buộc và đưa vào trong kế hoạch dự án.
- Xác minh mỗi nhiệm vụ đều có một mục tiêu rõ ràng
- Xác minh với bất kì thay đổi nào trong tài liệu kế hoạch dự án đều có bộ phận quản lý chất lượng và bộ phận quản lý xem xét

- Xác minh thời gian sử dụng nguồn lực được thiết lập rõ ràng, không có nguồn lực dự án nào không được giao nhiệm vụ.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B2.02.09: Quyết định tiếp tục/dừng thực hiện các bước tiếp theo cần được đưa ra tại các mốc quan trọng của dự án.

Tiêu chí kiểm toán

Đảm bảo ban quản lý thực hiện rà soát các mốc quan trọng của dự án để đưa ra quyết định tiếp tục thực hiện/dừng thực hiện trong dự án

Tài liệu yêu cầu

Kế hoạch dự án

Đánh giá thiết kế và triển khai

Phòng văn ban quản lý dự án/trưởng nhóm dự án, thu thập kế hoạch dự án, rà soát tại các mốc quan trọng của dự án, có sự rà soát, xem xét kỹ lưỡng của ban lãnh đạo trước khi đưa ra quyết định tiếp tục thực hiện hay dừng thực hiện.

Thử nghiệm hiệu quả hoạt động

Dựa vào danh sách các mốc dự án quan trọng, Kiểm toán viên nhà nước chọn một vài mốc dự án, xác minh xem tại các mốc có thực hiện quy trình đánh giá đưa ra quyết định tiếp tục thực hiện hay dừng thực hiện không?

Nếu có, xác minh quyết định tiếp tục thực hiện/dừng thực hiện của đơn vị có ghi lại hợp lý, được phê duyệt bởi các cấp quản lý có thẩm quyền hay không?

Kiểm soát B2.02.10 - Đơn vị thực hiện lên kế hoạch cho việc kiểm soát tiến độ dự án, đảm bảo cho việc hoàn thành các mốc dự án và đảm bảo ngân sách dự án

Tiêu chí kiểm toán

- Góp phần bảo đảm việc hoàn thành các mốc dự án đúng thời hạn và sử dụng ngân sách dự án một cách hiệu quả.
- Đảm bảo thời gian sử dụng nguồn lực, phần trăm hoàn thành công việc, các tài liệu/sản phẩm bàn giao được ghi lại trong tài liệu quản lý dự án.

- Xác định chu kỳ báo cáo để kiểm soát tiến độ, mức độ đầy đủ của tài liệu cần báo cáo. Rà soát quy trình về việc báo cáo tiến độ dự án.

Tài liệu yêu cầu

- Kế hoạch báo cáo
- Tài liệu kiểm soát tiến độ dự án, xác minh trong đó có các nội dung chính cần kiểm soát như sau: nguồn lực dự án, phần trăm hoàn thành công việc, sản phẩm bàn giao dự án.
- Bản kế hoạch dự án

Đánh giá thiết kế và triển khai

- Phòng văn ban quản lý dự án/trưởng nhóm dự án, tìm hiểu về quy trình báo cáo tiến độ dự án, xác minh nhân sự phụ trách việc bảo đảm tiến độ dự án.
- Thu thập tài liệu kiểm soát tiến độ dự án, xác minh trong đó có các nội dung chính cần kiểm soát như sau: nguồn lực dự án, phần trăm hoàn thành công việc, sản phẩm bàn giao dự án, mốc thời gian...
- Thu thập bản kế hoạch dự án, xác minh chu kỳ báo cáo để kiểm soát tiến độ và các tài liệu cần báo cáo.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B2.02.11 – Vấn đề quản lý thời gian và chi phí cần được lên kế hoạch.

Tiêu chí kiểm toán

Góp phần đảm bảo dự án được hoàn thành đúng thời hạn và sử dụng ngân sách dự án một cách hiệu quả.

Tài liệu yêu cầu

- Tài liệu về cách quản lý thời gian và chi phí dự án
- Tài liệu về thời gian làm việc của các thành viên trong tổ dự án
- Tài liệu về thời gian làm việc của đơn vị tư vấn bên ngoài
- Chi phí của dự án

Đánh giá thiết kế và triển khai

- Phòng văn ban quản lý dự án/trưởng nhóm dự án, tìm hiểu cách quản lý thời gian và chi phí của dự án. Thu thập tài liệu liên quan và xác minh:
 - Thời gian làm việc của các thành viên trong tổ dự án đều được lưu lại
 - Thời gian làm việc của đơn vị tư vấn bên ngoài cũng sẽ được ghi lại
 - Mọi chi phí của dự án đều được lưu lại (hóa đơn, bản liệt kê...) và được phê duyệt bởi ban quản lý dự án.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B2.02.12: Kế hoạch truyền thông cho các bên liên quan và lãnh đạo dự án cần được thiết lập.

Tiêu chí kiểm toán

Góp phần đảm bảo rằng dự án đáp ứng các mục tiêu về chức năng, ngân sách và thời gian của dự án.

Tài liệu yêu cầu

- Kế hoạch truyền thông
- Yêu cầu về tần số trao đổi và nội dung truyền thông

Đánh giá thiết kế và triển khai

- Phòng văn ban quản lý dự án/trưởng nhóm dự án và thu thập các thông tin về kế hoạch truyền thông dựa án cho các bên liên quan và ban lãnh đạo, xác minh các yêu cầu về tần suất trao đổi và nội dung truyền thông đúng theo kế hoạch truyền thông. Ví dụ như việc trao đổi sẽ diễn ra vào cuối mỗi tuần, khoảng 15 phút, nội dung chính báo cáo tiến độ công việc, khó khăn, chi phí hoạt động...
 - Thu thập các báo cáo truyền thông được đẩy lên trên hệ thống quản lý dự án (hoặc thư mục chung của dự án), xác minh rằng các báo cáo về trạng thái dự án, báo cáo ngoại lệ cũng được đẩy lên trên hệ thống quản lý của dự án (hoặc thư mục quản lý chung của dự án)

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề B2.03 - Xây dựng ngân sách dự án

Mục tiêu kiểm toán

Kiểm toán quản lý ngân sách trong giai đoạn lên kế hoạch của dự án. Đảm bảo các quy trình liên quan tới ngân sách dự án và thủ tục của kế toán chính xác, hoàn thiện và cung cấp các thông tin quản lý dự án.

Kiểm soát B2.03.01: Ngân sách dự án được án được xác lập rõ ràng, tách bạch với dự án khác, và chỉ được sử dụng cho dự án.

Tiêu chí kiểm toán

Đảm bảo ngân sách dự án được sử dụng hiệu quả, rõ ràng, tách bạch với các dự án khác.

Tài liệu yêu cầu

Ngân sách dự án và tất cả tài liệu liên quan

Đánh giá thiết kế và triển khai

- Phòng vấn nhân sự phụ trách ngân sách dự án, thu thập các tài liệu liên quan đến ngân sách, xác minh các tài liệu này đã được phê duyệt bởi đơn vị chủ quản dự án và ban chỉ đạo dự án.
- Xác minh đơn vị thực hiện quy trình ước lượng chi phí dự án và ngân sách đưa ra dựa trên kết quả của quy trình ước lượng chi phí đó.
- Đảm bảo rằng kết quả của quy trình ước lượng chi phí bằng với ngân quỹ đưa ra. Nếu có sự sai khác, rà soát các sai khác đó đã được chấp nhận và phê duyệt bởi ban quản chỉ đạo dự án và đơn vị chủ quản dự án hay chưa?
- Phòng vấn nhân sự phụ trách ngân sách dự án, trong trường hợp sản phẩm bàn giao không đạt tiêu chuẩn đúng theo kế hoạch (chất lượng, thời gian và tiến độ), xác minh xem việc này có ảnh hưởng tới ngân sách hay không? Nếu có, rà soát và xác minh các ảnh hưởng đó.
- Xác minh rằng, ngân sách của dự án chỉ được sử dụng riêng cho dự án.

- Rà soát ngân sách dự án, xác minh xem các thành phần trong hoạt động của dự án nằm ngoài ngân sách hay không? (ví dụ như: thử nghiệm (bao gồm cả thử nghiệm chấp nhận người dùng [UAT]); triển khai và đào tạo; chuyển đổi; sửa đổi cơ sở hạ tầng...)

- Rà soát ngân sách dự án, xác minh dự án có thiết lập một quỹ dự phòng.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B2.03.01: Các nguyên tắc kế toán về chi phí và vốn hóa phải được tuân thủ

Tiêu chí kiểm toán

Đảm bảo các yêu cầu về chi phí và vốn hóa của dự án

Tài liệu yêu cầu

Thủ tục kế toán của đơn vị

Đánh giá thiết kế và triển khai

Phòng vấn nhân sự phụ trách kế toán của dự án, xác minh các thủ tục kế toán mà đơn vị thực hiện, đảm bảo công việc kế toán của đơn vị được tính và chi phí và vốn hóa tuân theo chuẩn mực kế toán.

Thử nghiệm hiệu quả hoạt động

Chọn một giai đoạn của dự án, theo dõi phân bổ chi phí nhân lực và các chi phí khác trên hệ thống kế toán. Xác minh việc phân bổ chi phí đúng theo chuẩn mực kế toán.

Vấn đề B2.03.02 - Thiết lập hệ thống kiểm soát nội bộ

Mục tiêu kiểm toán

Đơn vị nên thiết lập kiểm soát nội bộ trong giai đoạn lập kế hoạch nhằm đảm bảo rằng việc xử lý dữ liệu một cách chính xác và đầy đủ.

Kiểm soát B2.03.03: Các yêu cầu kiểm soát nội bộ được thiết lập trong giai đoạn lập kế hoạch.

Tiêu chí kiểm toán

Các kiểm soát nội bộ được thiết lập trong kế hoạch.

Tài liệu yêu cầu

- Báo cáo tài chính, hoạt động của đơn vị
- Tài liệu yêu cầu về kiểm soát thiết kế
- Tài liệu về các yêu cầu kiểm soát được phê duyệt

Đánh giá thiết kế và triển khai

- Phòng vấn nhân sự chịu trách nhiệm kiểm toán nội bộ, xác minh nhân sự hiểu được các chức năng sắp có của ứng dụng mới hay không?
- Phòng vấn lãnh đạo dự án/trưởng tổ dự án, thu thập danh sách các chức năng của ứng dụng, hãy xác định xem nhóm dự án đã xác định được các kiểm soát chính cần thực hiện giám sát chưa? Tham khảo báo cáo tài chính, hoạt động, các yêu cầu về an ninh và quy định của đơn vị để đảm bảo các kiểm soát cần giám sát là thực sự cần thiết.
- Thu thập và rà soát các tài liệu yêu cầu về kiểm soát thiết kế và xác định các trường hợp mà việc cấp phép, nhập thông tin đầu vào (input), xử lý thông tin đầu ra, kiểm soát biên, bảo mật, toàn vẹn dữ liệu, nhật ký kiểm toán, kiểm soát truy cập, kiểm soát toàn vẹn cơ sở dữ liệu ... chưa đầy đủ.
- Rà soát các kiểm soát tự động (trong phần mềm ứng dụng đóng gói) đã giải quyết được yêu cầu nghiệp vụ hay
- Rà soát yêu cầu kiểm soát đã được phê duyệt.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề B2.04.00 - Xây dựng kế hoạch kiểm thử

Mục tiêu kiểm toán

Đơn vị thực hiện kiểm thử ở các giai đoạn phát triển khác nhau, bao gồm việc định nghĩa các loại kiểm thử cần thực hiện, khung thời gian cho thử nghiệm và yêu cầu tài liệu. Đảm bảo thử nghiệm phải bao gồm ít nhất các bước sau: kiểm thử đơn vị, kiểm

tích hợp, kiểm thử chấp nhận người dùng, tích hợp kiểm thử thủ công và tự động, thử nghiệm chuyển đổi và kiểm tra độ tin cậy. Tiến hành kiểm thử song song hoặc kiểm thử trên nhiều hệ điều hành khác nhau trước khi triển khai.

Kiểm soát B2.04.01: Các yêu cầu về tài liệu và tiêu chuẩn kiểm thử cần được thiết lập.

Tiêu chí kiểm toán

Đảm bảo các yêu cầu kiểm thử được đưa ra trước khi thực hiện dự án

Tài liệu yêu cầu

- Kế hoạch kiểm thử dự án
- Yêu cầu kiểm thử như: mục đích kiểm thử, phạm vi kiểm thử, kích thước kiểm thử, thời gian kiểm thử, tài liệu liên quan và các yêu cầu về rà soát và phê duyệt kiểm thử

Đánh giá thiết kế và triển khai

- Phòng văn nhân sự chịu trách nhiệm lên kế hoạch kiểm thử dự án, thu thập rà soát kế hoạch kiểm thử, đảm bảo rằng đơn vị có thiết lập yêu cầu kiểm thử như: mục đích kiểm thử, phạm vi kiểm thử, kích thước kiểm thử, thời gian kiểm thử, tài liệu liên quan và các yêu cầu về rà soát và phê duyệt kiểm thử
- Rà soát quy trình kiểm thử, xác minh xem quy trình kiểm thử của đơn vị gồm những quy trình nào: kiểm thử đơn vị, kiểm thử tích hợp, kiểm thử chấp nhận, kiểm thử tin cậy, kiểm thử chuyển đổi
- Rà soát kế hoạch kiểm thử nhằm đảm bảo rằng, các yêu cầu được lên kế hoạch kiểm thử cả trên môi trường thật và môi trường kiểm thử
- Rà soát kế hoạch kiểm thử, xác minh đơn vị có đưa ra một bộ kiểm thử cho các phần/chức năng sẽ được phát triển và sẵn sàng kiểm thử hồi quy của hệ thống.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B2.04.02: Lên kế hoạch cho thời gian kiểm thử, và thời gian khắc phục các lỗi trong giai đoạn phát triển.

Tiêu chí kiểm toán

Đảm bảo việc lên kế hoạch dự án có bao gồm việc lên kế hoạch cho thời gian kiểm thử và thời gian khắc phục các lỗi trong giai đoạn phát triển

Tài liệu yêu cầu

- Kế hoạch kiểm thử
- Kế hoạch thời gian kiểm thử

Đánh giá thiết kế và triển khai

- Phòng vận nhân sự chịu trách nhiệm lên kế hoạch kiểm thử dự án, thu thập rà soát kế hoạch kiểm thử, đảm bảo rằng đơn vị có lên kế hoạch thời gian kiểm thử
- Rà soát quy trình kiểm thử, xác minh trong trường hợp sản phẩm bàn giao muộn hoặc quá trình khắc phục lỗi muộn, đơn vị có đưa ra các cách xử lý nào để đảm bảo tiến độ dự án.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B2.04.03: Lên kế hoạch cho kịch bản kiểm thử và khối lượng kiểm thử.

Tiêu chí kiểm toán

Góp phần đảm bảo kết quả kiểm thử đầy đủ và chính xác

Tài liệu yêu cầu

- Kế hoạch kiểm thử
- Kết quả kiểm thử

Đánh giá thiết kế và triển khai

- Phòng vận nhân sự chịu trách nhiệm lên kế hoạch kiểm thử dự án, thu thập rà soát kế hoạch kiểm thử, xác minh rằng việc kiểm thử được lên kế hoạch thực hiện đầy đủ trên các chức năng của hệ thống
- Rà soát kế hoạch kiểm thử, xác minh rằng kết quả dự kiến của việc kiểm thử được tính toán tự động hay thủ công

- Rà soát kế hoạch kiểm thử độ tin cậy của hệ thống, đảm bảo đơn vị đã chuẩn bị một khối lượng dữ liệu thực tế để tiến hành kiểm thử độ tin cậy cho hệ thống.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề B2.05 - Xây dựng kế hoạch triển khai

Mục tiêu kiểm toán

Đơn vị lên kế hoạch triển khai để giảm thiểu tối đa sự gián đoạn của dự án trong giai đoạn triển khai, đảm bảo hệ thống được tra kỹ lưỡng trước khi chuyển đổi hệ thống mới lên môi trường thật.

Kiểm soát B2.05.01: Kế hoạch triển khai thử nghiệm được thiết lập

Tiêu chí kiểm toán

Góp phần đảm bảo kết quả kiểm thử được đầy đủ và chính xác

Tài liệu yêu cầu

- Kế hoạch thử nghiệm dự án
- Quy trình rà soát

Đánh giá thiết kế và triển khai

- Phòng vấn nhân sự chịu trách nhiệm lên kế hoạch thử nghiệm dự án, thu thập kế hoạch thử nghiệm dự án, rà soát và phạm vi thử nghiệm và đánh giá hiệu quả của việc thử nghiệm
- Phòng vấn nhân sự chịu trách nhiệm lên kế hoạch thử nghiệm dự án, tìm hiểu về quy trình rà soát và xác minh rằng kết quả kiểm tra thử nghiệm giải quyết đầy đủ các vấn đề được xác định trong quá trình kiểm thử và những vấn đề này đã được đưa lên trên hệ thống giám sát các vấn đề
- Thu thập kế hoạch thử nghiệm, rà soát mục tiêu thử nghiệm có được nêu ra rõ ràng hay không? Rà soát xem việc đánh giá tiếp tục thực hiện/dừng thực hiện có được nêu ra trong bản kế hoạch thử nghiệm dự án hay không?

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B2.05.02: Tính sẵn sàng của hệ thống cho triển khai cần được đánh giá.

Tiêu chí kiểm toán

Đảm bảo hệ thống sẵn sàng cho giai đoạn triển khai

Tài liệu yêu cầu

- Danh sách các vấn đề phát sinh
- Bản phân tích rủi ro

Đánh giá thiết kế và triển khai

- Phòng văn ban quản lý dự án/trưởng tổ dự án, xác minh rằng đơn vị có các thủ tục đánh giá tính sẵn sàng trước khi chuyển sang giai đoạn tiếp theo của dự án.
- Thu thập các tài liệu về kế hoạch đánh giá tính sẵn sàng, xác minh các đầu mục yêu cầu cần đánh giá như: danh sách các vấn đề phát sinh, bản phân tích các rủi ro và tác động của chúng tới việc triển khai dự án, phê duyệt từ ban chỉ đạo dự án/nhân sự chủ chốt của dự án/đơn vị chủ quản dự án

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B2.05.03: Kế hoạch về nguồn lực cho dự án cần được thiết lập.

Tiêu chí kiểm toán

Giảm thiểu các rủi ro thiếu hụt nguồn lực cho dự án.

Tài liệu yêu cầu

- Kế hoạch chỉ ra khối lượng công việc
- Kế hoạch về nguồn lực
- Kế hoạch dự phòng cho nguồn nhân lực

Đánh giá thiết kế và triển khai

- Phòng vấn ban quản lý dự án/trưởng tổ dự án, thu thập kế hoạch về nguồn lực cần thiết trong việc chuyển đổi và triển khai hệ thống mới.
- Xác minh kế hoạch chỉ ra khối lượng công việc hiện tại cũng như khối lượng công việc quy trình mới và quy trình chuyển đổi.
- Xác minh đơn vị có kế hoạch dự phòng nguồn nhân lực trong trường hợp nhân viên nghỉ phép, bệnh tật...

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B2.05.04: Kế hoạch chuyển đổi trong giai đoạn lên kế hoạch của dự án cần được thiết lập.

Tiêu chí kiểm toán

Giảm thiểu các rủi ro trong quá trình chuyển đổi hệ thống

Tài liệu yêu cầu

- Kế hoạch chuyển đổi, rà soát
- Yêu cầu và đặc tả chuyển đổi
- Kế hoạch diễn tập chuyển đổi
- Kế hoạch quy hồi
- Kế hoạch đảm bảo hòa hợp dữ liệu

Đánh giá thiết kế và triển khai

- Phòng vấn ban quản lý dự án/trưởng tổ dự án, thu thập kế hoạch chuyển đổi, rà soát và xác minh xem các nhiệm vụ sau được đưa vào kế hoạch hay chưa:
 - Yêu cầu và đặc tả chuyển đổi,
 - Kế hoạch diễn tập chuyển đổi cho quy trình chuyển đổi thử nghiệm sử dụng đầy đủ các dữ liệu cần được chuyển đổi.
 - Kế hoạch quy hồi trong trường hợp chuyển đổi không thành công.
 - Kế hoạch đảm bảo sự hòa hợp dữ liệu giữa các hệ thống mới và cũ
- Xác minh kế hoạch chuyển đổi đã được ban chỉ đạo và /hoặc đơn vị chủ quản dự án đã thông qua và phê duyệt

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B2.05.05: Kế hoạch đào tạo về các chức năng thay đổi được thiết lập trước khi triển khai hệ thống.

Tiêu chí kiểm toán

Đảm bảo người dùng cùng nắm được các thông tin về chức năng bị thay đổi, tránh lỗi thao tác người dùng và phát hiện những lỗi chức năng trong quá trình sử dụng

Tài liệu yêu cầu

Kế hoạch đào tạo cho các phòng ban

Đánh giá thiết kế và triển khai

- Phòng văn ban quản lý dự án/trưởng tổ dự án, thu thập kế hoạch đào tạo cho các phòng ban liên quan. Xác minh các chức năng bị thay đổi đều có trong kế hoạch đào tạo cho nhân viên,
- Xác minh ban CNTT, bộ phận hỗ trợ được đào tạo trong việc lập kế hoạch và xử lý hệ thống mới.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B2.05.06: Kế hoạch khôi phục hệ thống/dữ liệu được thiết lập và phê duyệt

Tiêu chí kiểm toán

Chuẩn bị kế hoạch khôi phục, đảm bảo kế hoạch quy hồi được phê duyệt và chỉ định ngay từ bước khởi động dự án.

Tài liệu yêu cầu

Kế hoạch khôi phục

Đánh giá thiết kế và triển khai

- Phòng văn ban quản lý dự án/trưởng tổ dự án, thu thập kế hoạch khôi phục, đánh giá kế hoạch khôi phục tại các điểm cần chú trọng yêu cầu khôi phục khi cần thiết.

- Xác minh kế hoạch khôi phục có sự tham gia của ban quản lý dự án, cán bộ chủ chốt của các bên liên quan và đơn vị chủ quản dự án.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề B2.06 - Lập kế hoạch chọn lựa, quản lý các bên thứ 3 có liên quan

Mục tiêu kiểm toán

Đảm bảo việc lựa chọn nhà cung cấp dịch vụ bên ngoài hiệu quả, tối đa lợi tức đầu tư. Đơn vị cung cấp dịch vụ bên ngoài cần được kiểm tra, đánh giá và xem xét đầy đủ. Trong hợp đồng cung cấp dịch vụ với nhà cung cấp cần nêu rõ các sản phẩm bàn giao (có thể thấy được) và các điều khoản liên quan tới sở hữu trí tuệ.

Kiểm soát B2.06.01: Các tiêu chí và chính sách lựa chọn nhà thầu được định nghĩa

Tiêu chí kiểm toán

Góp phần đảm bảo việc lựa chọn nhà thầu được thực hiện một cách khách quan

Tài liệu yêu cầu

- Tài liệu các tiêu chí lựa chọn nhà cung cấp dịch vụ/nhà thầu
- Quá trình lựa chọn nhà thầu
- Hợp đồng ký kết với nhà thầu

Đánh giá thiết kế và triển khai

- Phòng văn ban quản lý dự án/trưởng tổ dự án, thu thập các tài liệu các tiêu chí lựa chọn nhà cung cấp dịch vụ bên ngoài. Tìm hiểu quá trình lựa chọn nhà thầu và xác minh quy trình lựa chọn đó bao gồm bao gồm việc đánh giá, so sánh các tiêu chí lựa chọn đối với đặc điểm của nhà cung cấp trong đề nghị mời thầu.

- Trong trường hợp đơn vị đã lựa chọn được nhà thầu rà soát lại quá trình ra quyết định và đưa ra giải thích lý do lựa chọn thầu đó.

- Thu thập hợp đồng ký kết với nhà thầu được chọn, rà soát hợp đồng ký kết, xác minh các chuẩn mực, điều khoản được đưa vào trong hợp đồng có bao gồm các sản phẩm bàn giao hay không?

- Xác minh việc ủy quyền hợp đồng có phù hợp với quy định của đơn vị về phạm vi và giá trị hay không?

- Rà soát hợp đồng mua lại phần mềm (nếu có) xác minh hợp đồng có các yêu cầu về: các quyền và nghĩa vụ của tất cả các bên về quyền sở hữu và cấp phép quyền sở hữu trí tuệ, bảo trì, bảo đảm, thủ tục trọng tài, điều khoản nâng cấp, quyền sử dụng, an ninh, bảo mật và quyền truy cập hay không?

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B2.06.02: Đơn vị đưa ra các thỏa thuận chất lượng dịch vụ với nhà thầu.

Tiêu chí kiểm toán

Đảm bảo nhà thầu tuân thủ theo đúng các điều khoản trong hợp đồng dịch vụ và có những cơ chế xử phạt tương ứng nếu không tuân thủ.

Tài liệu yêu cầu

- Thỏa thuận dịch vụ
- Hợp đồng với nhà thầu

Đánh giá thiết kế và triển khai

- Phòng vấn ban quản lý dự án/trưởng tổ dự án, thu thập thỏa thuận dịch vụ? Xác minh các thỏa thuận đó có được tài liệu hóa hay không? Xác minh thỏa thuận dịch vụ có được mô tả giống như trong hợp đồng hay không?

- Rà soát các thỏa thuận dịch vụ để xem liệu rằng đơn vị/tổ dự án đã sử dụng tối đa các chỉ số đang được theo dõi, đánh giá các hoạt động của nhà thầu hay chưa?

- Rà soát các thỏa thuận dịch vụ và xác minh xem các thỏa thuận này có cho phép đưa ra các hình phạt vì nhà thầu không tuân theo đúng điều khoản của hợp đồng hay không?

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B2.06.03: Quy trình quản lý truy cập đối với nhà cung cấp được thiết lập.

Tiêu chí kiểm toán

Nhà cung cấp ký các thỏa thuận về bảo mật, hạn chế quyền truy cập, sử dụng, phân phát tài sản trí tuệ của doanh nghiệp. Nhà cung cấp chỉ được truy cập các thông tin cần thiết để thực hiện các nghĩa vụ đã ký hợp đồng.

Tài liệu yêu cầu

Cam kết liên quan tới bảo mật thông tin, sở hữu trí tuệ

Đánh giá thiết kế và triển khai

- Phòng văn ban quản lý dự án/trưởng tổ dự án, thu thập các cam kết liên quan tới bảo mật thông tin, sở hữu trí tuệ... khi tham gia dự án.
- Thu thập các cam kết với nhà thầu, xác minh đại diện bảo nhà thầu, và các thành viên tham gia dự án của nhà thầu đều thực hiện ký các cam kết đó
- Xác minh rằng, đơn vị có các thủ tục quản lý rà soát truy cập của nhà thầu đối với các sản phẩm sở hữu trí tuệ của đơn vị

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

4. Chuyên đề B3 - Công tác thực hiện dự án

a. Khái niệm

Giai đoạn thực hiện dự án thường là giai đoạn kéo dài thời gian nhất, nó bao gồm tất các bước sau khi hoàn thành giai đoạn lên kế hoạch dự án tới giai đoạn dự án được đưa vào sử dụng trong môi trường thật. Giai đoạn thực hiện dự án có thể chia thành các giai đoạn con sau:

- Báo cáo phân tích khoảng trống (trong trường hợp dự án mua sắm phần mềm)
- Thiết kế hệ thống mới bao gồm:
 - Quy trình kinh doanh mới (cả thủ công và tự động)
 - Các kiểm soát mới
 - Phát triển phần kết nối giữa hệ thống mới với các hệ thống đang sử dụng tại đơn vị

- Phát triển các quy trình tạm thời trong trường hợp hệ thống mới phải vận hành song song cùng hệ thống cũ cho tới khi tất cả các quy trình mới được hoàn thiện
- Các tiện ích chuyển đổi qua hệ thống mới
- Thiết lập việc chuyển đổi qua quy trình, và xác nhận quy trình là chính xác và hoàn thiện
 - Kiểm thử
 - Quy trình kinh doanh (kiểm thử đơn vị và kiểm thử tích hợp)
 - Kiểm thử người dùng cuối
 - Chuyển đổi dữ liệu
 - Kiểm thử tải trọng các quy trình và thiết bị
 - Kế hoạch dự phòng (backout) nếu việc chuyển đổi dữ liệu phải trì hoãn
 - Triển khai
 - Kiểm tra việc chuyển đổi dữ liệu

b. Các rủi ro liên quan

- Cơ chế xử lý leo thang trong dự án không được quy định dẫn đến các vấn đề không được xử lý kịp thời
 - Dự án không thành lập kiểm soát nội bộ trong suốt quá trình thực hiện
 - Dự án không có thiết lập các thủ tục quản lý đảm bảo chất lượng dự án
 - Việc kiểm thử hệ thống không được tiến hành một cách đầy đủ và đúng đắn
 - Dự án không thực hiện việc triển khai thử nghiệm trước khi tiến hành triển khai trên quy mô lớn
- Dự án không có sự chuẩn bị cho kế hoạch chuyển giao
- Dự án không có sự chuẩn bị cho kế hoạch dự phòng (backout) sử dụng khi cần thiết
 - ROI và KPI của dự án không được tính toán và cập nhật khi có thay đổi
 - Các yêu cầu thay đổi không được rà soát và phê duyệt phù hợp để xác định/xem xét các thay đổi tới phạm vi, điều khoản, nguồn lực và các khía cạnh khác của hợp đồng cũng như dự án. Các yêu cầu thay đổi có thể bao gồm những công việc đã nằm trong phạm vi dự án ban đầu.
- Hợp đồng không thể tiếp cận và không được lưu trữ ở vị trí có thể tiếp cận được

- Hóa đơn không được rà soát kiểm tra đảm bảo việc tuân thủ theo các điều khoản và điều kiện hợp đồng trước khi thực hiện chi trả
- Cấp quản lý có thể không thực hiện việc rà soát chất lượng và tiến độ hoàn thành công việc trước khi phê duyệt việc trả tiền dự án

c. Các vấn đề thực hiện kiểm toán

Cơ chế leo thang trong dự án

- Đơn vị có ban hành quy trình về cơ chế leo thang để giải quyết vấn đề trong dự án hay không? Quy trình này có được văn bản hóa và phê duyệt bởi cấp có thẩm quyền hay không?
- Việc thực thi theo quy trình cơ chế leo thang có được tuân thủ một cách nghiêm túc hay không?

Chất lượng dự án

- ROI và KPI có được tính toán và cập nhật báo cáo tới ban giám đốc khi mà phạm vi dự án hay các cấu phần thay đổi ảnh hưởng tới hiệu quả và ROI
- Đơn vị có quy trình quản lý chất lượng dự án không?

Kiểm thử dự án

- Xác định xem liệu hệ thống có được kiểm thử thích hợp trước khi đi vào triển khai, kịch bản kiểm thử bao gồm tất cả khía cạnh của một hệ thống mới và tất cả các kết quả không như mong đợi sẽ được giải quyết triệt để. Kế hoạch kiểm thử có được văn bản hóa và có đầy đủ các thông tin sau không:
 - Kiểm thử đơn vị
 - Kiểm thử tích hợp
 - Kiểm thử hệ thống
 - Kiểm thử thí điểm
 - Kiểm thử song song
 - Người dùng có tham gia vào giai đoạn kiểm thử không?
 - Việc kiểm thử có được thực hiện trên một thiết bị kiểm thử phù hợp hay không?
 - Người dùng có ký xác nhận trên kết quả kiểm thử không?
 - Kịch bản kiểm thử nêu chi tiết các yêu cầu và đảm bảo tất cả các khía cạnh của hệ thống được kiểm thử

- Kết quả kiểm thử có được rà soát chi tiết hay không?
- Đơn vị có quy trình xử lý khi mà các kết quả kiểm thử không đạt được như mong đợi?
- Các kết quả của kịch bản kiểm thử có đạt như mong đợi không?

Quản lý thay đổi

- Đơn vị có quy trình và chính sách quản lý thay đổi chính thức không?
- Tất cả những thay đổi so với các tính năng ban đầu có được đánh giá, rà soát, thực hiện, kiểm thử, lưu vết và phê duyệt?
- Tất cả các thay đổi trước và sau khi triển khai có được kiểm thử và lưu văn bản hay không?
- Các thay đổi của dự án có tuân theo quy trình và chính sách ban hành về quản lý thay đổi của đơn vị hay không?
- Liệu những nhân viên trong doanh nghiệp có đủ thẩm quyền hiệu quả và nguồn lực để thực hiện vai trò và nhiệm vụ không?
- Những người thực hiện việc phê duyệt chỉ thực hiện những công tác liên quan tới công việc và vị trí của họ

d. Chương trình kiểm toán mẫu

Vấn đề B3.01 - Quản trị dự án trong giai đoạn thực hiện dự án

Mục tiêu kiểm toán

Ban lãnh đạo cần thực hiện giám sát dự án liên tục và đầy đủ. Các nguồn lực kỹ thuật cần được phân công đầy đủ đảm bảo tiến độ của dự án. Đơn vị cần có những chính sách, quy định để bảo đảm ban quản lý dự án báo cáo liên tục lên ban lãnh đạo, để ban lãnh đạo đơn vị kịp thời ứng phó với các vấn đề phát sinh.

Kiểm soát 3411: Quản lý dự án cần liên tục theo dõi và báo cáo cho các cấp lãnh đạo và nhà tài trợ dự án.

Tiêu chí kiểm toán

Đảm bảo dự án đang đi đúng hướng so với kế hoạch và kịch bản kinh doanh ban đầu

Tài liệu yêu cầu

- Văn bản ghi chép lại các thay đổi ảnh hưởng đến kế hoạch và kịch bản kinh doanh của dự án

- Biên bản cuộc họp liên quan đến các thay đổi kế hoạch và kịch bản kinh doanh trong dự án.

Đánh giá thiết kế và triển khai

- Phòng vận ban quản lý dự án và thu thập lịch sử thay đổi của dự án.
- Phòng vận ban quản lý dự án và rà soát các thay đổi, xác định xem có thay đổi nào ảnh hưởng đến kịch bản kinh doanh không.

- Thu thập, rà soát các báo cáo của quản lý dự án lên ban lãnh đạo, đảm bảo các thay đổi được báo cáo đầy đủ lên ban lãnh đạo

- Nếu các thay đổi đã được thực hiện, rà soát các biên bản họp với lãnh đạo đơn vị, đảm bảo các thay đổi đã được phê duyệt một cách hợp lý từ các cấp có thẩm quyền

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách các thay đổi, Kiểm toán viên nhà nước thực hiện chọn mẫu và tiến hành các bước tương tự như phần đánh giá thiết kế và triển khai để đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán

Kiểm soát B3.01.02: Phạm vi của dự án được xác định rõ ràng, giám sát và cập nhật thường xuyên.

Tiêu chí kiểm toán

Đảm bảo phạm vi dự án được xác định rõ ràng. Tất cả các thay đổi liên quan đến phạm vi dự án cần phải được phê duyệt bởi các cấp lãnh đạo có thẩm quyền.

Tài liệu yêu cầu

- Văn bản ghi chép lại các thay đổi ảnh hưởng đến phạm vi của dự án
- Biên bản cuộc họp liên quan đến các thay đổi phạm vi trong dự án.

Đánh giá thiết kế và triển khai

- Phòng vận ban quản lý dự án/trưởng dự án và thu thập danh sách thay đổi của dự án.

- Phòng vận ban quản lý dự án và rà soát các thay đổi, xác định xem có thay đổi nào ảnh hưởng đến phạm vi của dự án hay không

- Nếu phạm vi dự án thay đổi, rà soát các biên bản họp với lãnh đạo đơn vị, đảm bảo các thay đổi về mặt phạm vi đã được thông báo và phê duyệt một cách hợp lý từ các cấp có thẩm quyền.

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách các thay đổi về mặt phạm vi, Kiểm toán viên nhà nước thực hiện chọn mẫu và tiến hành thu thập các tài liệu liên quan tới văn bản phê duyệt của ban quản lý, xác minh thời gian quy trình phê duyệt được hoàn thành, đảm bảo các bước phê duyệt và thời gian phê duyệt phù hợp với các quy định của đơn vị

Kiểm soát B3.01.03 - Các chỉ số đo lường hiệu quả hoạt động của dự án được cập nhật, báo cáo thường xuyên cho ban lãnh đạo và đơn vị tài trợ dự án.

Tiêu chí kiểm toán

Đảm bảo ban quản lý dự án thường xuyên cập nhật, báo cáo các chỉ số đo lường hiệu quả hoạt động của dự án lên các cấp lãnh đạo và đơn vị tài trợ dự án khi có những thay đổi tác động đến hiệu quả và ROI của dự án

Tài liệu yêu cầu

- Báo cáo, biên bản cuộc họp liên quan đến các chỉ số đo lường hiệu quả khi có sự thay đổi
- Tài liệu ghi chép tính toán các chỉ số đo lường hiệu quả

Đánh giá thiết kế và triển khai

- Phòng văn trưởng dự án/ban quản lý dự án về việc đơn vị có thực hiện việc báo cáo các chỉ số đo lường hiệu quả của dự án lên các cấp lãnh đạo, đơn vị tài trợ dự án khi những thay đổi tác động đến hiệu quả và ROI của dự án
- Thu thập các báo cáo, các biên bản họp với lãnh đạo đơn vị, rà soát báo cáo bảo đảm nhóm dự án báo cáo thường xuyên lên các cấp lãnh đạo và các đơn vị tài trợ dự án theo quy định. Các thông số trong báo cáo bao gồm đầy đủ các chỉ số đã được thống nhất.
- Trong trường hợp các thuộc tính để tính toán các chỉ số hoạt động thay đổi do dự án thay đổi (phạm vi, thời gian thực hiện dự án), đảm bảo các chỉ số được cập nhật theo các thuộc tính mới.

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách các báo cáo, Kiểm toán viên nhà nước thực hiện chọn mẫu (lưu ý trong trường hợp các thuộc tính để tính toán thay đổi) và tiến hành các bước tương tự như phần đánh giá thiết kế và triển khai để đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán

Kiểm soát B3.01.04: Quy trình quản lý leo thang cần được thiết lập

Tiêu chí kiểm toán

Ban chỉ đạo dự án và các đơn vị tài trợ tiếp nhận và xử lý các vấn đề được báo cáo lên của đội dự án

Tài liệu yêu cầu

- Tài liệu về quy trình thủ tục quản lý sự cố leo thang
- Danh sách công cụ/phần mềm được sử dụng trong cơ chế leo thang
- Các tài liệu liên quan tới quy trình, thủ tục và cả tiêu chí cho việc ghi lại thông tin của sự cố

Đánh giá thiết kế và triển khai

- Phỏng vấn quản lý dự án về quy trình quản lý leo thang của dự án như thế nào? Trong suốt dự án có bất kỳ vấn đề leo thang được đưa ra mà không có cách xử lý thích hợp và kịp thời không?
- Thu thập tài liệu mô tả các thủ tục liên quan tới giải quyết vấn đề leo thang.
- Xác minh trong thủ tục xử lý, các vấn đề leo thang cần phải được thông báo kịp thời cho ban chỉ đạo dự án và nhà tài trợ., đảm bảo không có vấn đề leo thang nào được đưa ra mà không có cách xử lý thích hợp.
- Trong trường hợp có bất kỳ vấn đề leo thang được đưa ra mà chưa có cách xử lý thích hợp, đảm bảo đơn vị đang giám sát vấn đề này thường xuyên và cập nhật khi có phương án xử lý.

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách các vấn đề xử lý leo thang, Kiểm toán viên nhà nước thực hiện chọn mẫu và tiến hành bước tương tự như phần đánh giá thiết kế và triển khai để đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán

Vấn đề B3.02 - Quản lý dự án trong giai đoạn thực hiện dự án

Mục tiêu kiểm toán

Hoạt động quản lý dự án cần có sự giám sát và xử lý thích hợp để đảm bảo kế hoạch dự án được thực hiện, giảm nhẹ rủi ro đã định trước, các vấn đề được giải quyết hoặc báo cáo lên các cấp quản lý thích hợp, duy trì chất lượng dự án, giám sát và tối ưu các chi phí và đưa ra quyết định tiếp tục/dừng lại tại các mốc quan trọng của dự án.

Kiểm soát B3.02.01: Việc phối hợp giữa nhóm nghiệp vụ và thông tin trong dự án cần được giám sát.

Tiêu chí kiểm toán

Đảm bảo nhóm quản lý thông tin và nghiệp vụ và các bên liên quan luôn tham gia vào dự án cùng với nhóm dự án. Ban chỉ đạo dự án giám sát hiệu quả của việc hoạt động chung của nhóm nghiệp vụ và nhóm dự án.

Tài liệu yêu cầu

- Cơ cấu tổ chức/Danh sách các thành viên của nhóm quản lý thông tin và nhóm nghiệp vụ
- Biên bản cuộc họp giữa ban lãnh đạo dự án và nhóm quản lý thông tin & nhóm nghiệp vụ
- Báo cáo ghi chép lại những sự cố, vấn đề do không thống nhất giữa 2 nhóm (nếu có)

Đánh giá thiết kế và triển khai

- Phòng vận Trưởng dự án/ban quản lý dự án xem nhóm quản lý thông tin và nghiệp vụ có thuộc vào thành phần nhóm dự án hay không?
- Rà soát biên bản các cuộc họp, đảm bảo các thành viên trong nhóm, bao gồm nhóm quản lý thông tin và nghiệp vụ đều tham gia đầy đủ, các thông tin liên quan tới nghiệp vụ đều có sự đóng góp từ bên quản lý nghiệp vụ
- Rà soát các biên bản họp, các báo cáo lên các cấp lãnh đạo, đảm bảo tất cả những bất đồng trong quá trình phối hợp thực hiện giữa nhóm dự án và nhóm quản lý nghiệp vụ đều được báo cáo lên ban chỉ đạo dự án.
- Rà soát các biên bản chỉ đạo của ban chỉ đạo dự án, đảm bảo các vấn đề bất đồng nêu trên được ban chỉ đạo quan tâm và xử lý kịp thời.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B3.02.02: Thành phần của nhóm dự án cần được đánh giá về kiến thức và năng lực

Tiêu chí kiểm toán

Đảm bảo nhóm dự án bao gồm các nguồn lực phù hợp, có kiến thức về quy trình nghiệp vụ và giải pháp

Tài liệu yêu cầu

- Quy trình tuyển chọn nhân sự dự án
- Hồ sơ nhân sự dự án
- Kế hoạch dự phòng về nhân sự của dự án

Đánh giá thiết kế và triển khai

- Phòng vận Trường dự án/Ban quản lý dự án về cách lựa chọn các nhân sự tham gia dự án, các thành viên của nhóm dự án,
 - Rà soát hồ sơ các thành viên nhóm dự án và đánh giá tính phù hợp về kinh nghiệm, kiến thức của các thành viên dự án.
 - Phỏng vấn các thành viên nhóm dự án xem có tham gia vào các công việc khác không? Đảm bảo việc tham gia vào các công việc khác không làm ảnh hưởng đến tiến độ của dự án.
- Phòng vận Trường dự án/Ban quản lý dự án về các kế hoạch dự phòng về nguồn nhân sự cho dự án, đảm bảo luôn có sự tham gia của các nhân sự chủ chốt.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B3.02.03: Quy trình phân tích và giám sát rủi ro được thiết lập.

Tiêu chí kiểm toán

Đảm bảo phân tích rủi ro tiếp tục được áp dụng cho dự án trong giai đoạn thực hiện. Đảm bảo có một quy trình thích hợp cho để giảm thiểu và giám sát rủi ro.

Tài liệu yêu cầu

- Thủ tục/quy trình phân tích, giám sát rủi ro
- Tài liệu ghi chép về các rủi ro có thể xảy ra và các ảnh hưởng của nó trong giai đoạn thực hiện dự án
 - Kế hoạch dự phòng khi rủi ro thay đổi hoặc xuất hiện mới
 - Biên bản cuộc họp giữa ban quản lý dự án và các bên liên quan
 - Báo cáo về sự thay đổi rủi ro lên ban quản lý và các báo cáo liên quan khác.

Đánh giá thiết kế và triển khai

- Phỏng vấn Trưởng dự án/ban quản lý dự án về quy trình phân tích giám sát rủi ro trong giai đoạn thực hiện dự án như thế nào?

- Nếu rủi ro có thay đổi, phòng vấn Trường dự án/Ban quản lý dự án xem ảnh hưởng của các rủi ro đó đến các vấn đề liên quan (tài chính, ngày hoàn thành, quy định....), xác suất xảy ra rủi ro cũng như các tác động đã được phân tích hay chưa?

- Phòng vấn Trường dự án/ban quản lý dự án và xác minh xem ban chỉ đạo dự án và các bên liên quan có tham gia vào quá trình đánh giá rủi ro trong bước thực hiện dự án hay không

- Rà soát các báo cáo lên ban chỉ đạo, đảm bảo mọi sự thay đổi về rủi ro đều được cập nhật và báo cáo lên ban chỉ đạo dự án và các bên liên quan và được phê duyệt một cách hợp lý.

Thử nghiệm hiệu quả hoạt động

Dựa trên các rủi ro mới đã được xác định trong quá trình thực hiện, Kiểm toán viên nhà nước tiến hành chọn mẫu và xác minh xem các tác động và khả năng xảy ra rủi ro đã được đánh giá như thế nào, các bên liên quan được thông báo và xử lý rủi ro (bằng cách chấp nhận và thông qua rủi ro hoặc giảm nhẹ rủi ro) như thế nào.

Kiểm soát B3.02.04: Quy trình quản lý và xử lý sự cố được thiết lập

Tiêu chí kiểm toán

Đảm bảo các vấn đề trong quá trình thực hiện dự án được tài liệu hóa, thông báo, đánh giá và xử lý bởi các cấp theo quy định thông qua hệ thống quản lý các vấn đề.

Tài liệu yêu cầu

- Thủ tục, quy trình xử lý sự cố trong quá trình thực hiện dự án
- Nhật ký ghi chép các sự cố

Đánh giá thiết kế và triển khai

- Phòng vấn Trường dự án/ban quản lý dự án về Phương thức đơn vị ghi nhận và xử lý các vấn đề trong quá trình thực hiện dự án.

- Phòng vấn Trường dự án/ban quản lý dự án/thành viên nhóm dự án về các vấn đề đã được ghi nhận. Rà soát nhật ký các vấn đề và xác minh xem các vấn đề đã được ghi nhận đầy đủ hay chưa

- Rà soát nhật ký các vấn đề, đảm bảo các vấn đề đã được rà soát và xử lý bởi các cấp có thẩm quyền. Nếu vấn đề vẫn còn tồn đọng, đảm bảo nó đang được giám sát thường xuyên bởi các bộ phận liên quan.

Thử nghiệm hiệu quả hoạt động

Dựa trên nhật ký các vấn đề, Kiểm toán viên nhà nước tiến hành chọn mẫu và xác minh xem các vấn đề đã được ghi nhận như thế nào, đảm bảo quy trình tham gia và xử lý vấn đề của các bên phù hợp với quy định

Kiểm soát B3.02.05: Thủ tục quy định về quản lý chất lượng được thiết lập.

Tiêu chí kiểm toán

Đảm bảo dự án thiết lập các thủ tục, quy định về quản lý chất lượng và các thủ tục quản lý chất lượng được thực thi trong khâu thực hiện dự án.

Tài liệu yêu cầu

- Thủ tục, quy định về quản lý chất lượng
- Danh sách các thành viên trong nhóm đánh giá chất lượng
- Tài liệu liên quan ghi chép về công tác rà soát chất lượng

Đánh giá thiết kế và triển khai

- Phòng vấn Trưởng dự án/Ban quản lý dự án và xác minh xem liệu rằng dự án có thiết lập các thủ tục, quy định về quản lý chất lượng hay không, công tác quản lý chất lượng có được thực hiện trong giai đoạn này hay không.

- Phòng vấn Trưởng dự án/Ban quản lý dự án xác minh thành phần nhóm thực hiện đánh giá chất lượng, đảm bảo nhóm thực hiện đánh giá chất lượng độc lập với nhóm phát triển.

- Rà soát các tài liệu liên quan, đảm bảo công tác rà soát chất lượng được thực hiện thường xuyên, xuyên suốt trong giai đoạn thực hiện dự án bởi các thành viên bên ngoài nhóm phát triển

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B3.02.06: Quy trình quản lý thay đổi được thiết lập.

Tiêu chí kiểm toán

Quy trình quản lý thay đổi đang được đơn vị sử dụng để ghi nhận toàn bộ các thay đổi liên quan tới phạm vi, Kịch bản kinh doanh và các thuộc tính quan trọng của dự án.

Tài liệu yêu cầu

- Tài liệu, chính sách quản lý thay đổi

- Nhật ký ghi lại các thay đổi trong dự án

Đánh giá thiết kế và triển khai

- Phòng văn quản lý dự án và xác nhận đơn vị có một quy trình chính thức cho việc quản lý thay đổi hay không
- Rà soát quy trình và xác minh rằng quy trình được áp dụng cho các thay đổi liên quan tới phạm vi, kích bản kinh doanh hay các thuộc tính quan trọng của dự án cần được phê duyệt

- Lựa chọn một yêu cầu thay đổi và xác nhận thay đổi tuân theo quy trình quản lý thay đổi của đơn vị

Thử nghiệm hiệu quả hoạt động

Dựa trên nhật ký các thay đổi, Kiểm toán viên nhà nước tiến hành chọn mẫu và xác minh các vấn đề sau:

- Đảm bảo mô tả thay đổi đã được tài liệu hóa
- Đảm bảo tất cả các thay đổi tác động tới tình huống kinh doanh và dự án đã được tài liệu hóa
- Đối với các thay đổi có yêu cầu đánh giá lại rủi ro, đảm bảo việc đánh giá rủi ro được thực hiện
- Tất cả các thay đổi đều được phê duyệt theo đúng quy trình (thực hiện theo ngưỡng phê duyệt)

Kiểm soát B3.02.07: Đánh giá công tác lập kế hoạch và kiểm soát dự án

Tiêu chí kiểm toán

Việc lập kế hoạch và kiểm soát dự án bao gồm kiểm soát thời gian hiệu quả, kế hoạch dự án bao gồm các mốc dự án quan trọng, các sản phẩm bàn giao, trình tự các bước, nguồn lực dự kiến và các hoạt động phụ thuộc

Tài liệu yêu cầu

- Kế hoạch dự án
- Báo cáo định kỳ về kế hoạch dự án
- Biên bản cuộc họp ban lãnh đạo dự án với trưởng dự án và ban quản lý dự án

Đánh giá thiết kế và triển khai

- Phòng văn ban quản lý dự án/trưởng dự án tìm hiểu việc quản lý kế hoạch dự án với các thay đổi về phạm vi công việc, nguồn lực và các mốc dự án

- Thu thập và rà soát kế hoạch dự án có bao gồm các thông tin về mốc dự án quan trọng, các sản phẩm bàn giao, trình tự các bước, nguồn lực dự kiến và các hoạt động phụ thuộc, giả định và các ràng buộc của dự án đã được tài liệu hóa và đảm bảo mỗi nhiệm vụ đều gắn với một mục tiêu rõ ràng.

- Thu thập, rà soát các báo cáo của Trưởng dự án/ban quản lý dự án lên ban lãnh đạo, đảm bảo các thay đổi cập nhật được báo cáo đầy đủ lên ban lãnh đạo

- Phỏng vấn ban quản lý dự án và rà soát các thay đổi, xác định xem có thay đổi nào ảnh hưởng đến Kế hoạch kinh doanh không. Nếu các thay đổi đã được thực hiện, rà soát các biên bản họp với lãnh đạo đơn vị, đảm bảo các thay đổi đã được phê duyệt một cách hợp lý từ các cấp có thẩm quyền.

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách các thay đổi, Kiểm toán viên nhà nước thực hiện chọn mẫu và tiến hành các bước tương tự như phần đánh giá thiết kế và triển khai để đảm bảo tính hiệu quả hoạt động trong suốt quá trình kiểm toán.

Kiểm soát B3.02.08: Đánh giá các mốc dự án để quyết định tiếp tục tiến hành dự án hay dừng lại.

Tiêu chí kiểm toán

Ban quản lý kiểm tra đánh giá trạng thái của dự án tại các mốc dự án để ra quyết định dự án tiếp tục thực hiện hoặc dừng lại

Tài liệu yêu cầu

- Báo cáo đánh giá tại các mốc dự án
- Tài liệu, văn bản về các quyết định dừng lại hoặc tiếp tục sau mỗi mốc dự án

Đánh giá thiết kế và triển khai

- Phỏng vấn ban quản lý/trưởng nhóm dự án đảm bảo rằng các nhiệm vụ và mục tiêu tại mỗi mốc dự án được thực hiện đầy đủ và hiệu quả nhằm đánh giá tổng thể dự án nên tiếp tục hay dừng lại.

- Thu thập rà soát các báo cáo đánh giá tại mỗi mốc dự án

- Phỏng vấn ban lãnh đạo/trưởng nhóm trong các trường hợp tiếp tục dự án hoặc dừng lại, có sự tham gia và sự phê duyệt của ban lãnh đạo, đội dự án và các bên tham gia không.

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách mốc dự án đã thực hiện, Kiểm toán viên nhà nước tiến hành chọn mẫu và thực hiện các quy trình như phân đánh giá thiết kế và triển khai để đảm bảo tính hữu hiệu trong suốt giai đoạn kiểm toán.

Kiểm soát B3.02.09: Tiến độ dự án cần được giám sát và báo cáo thường xuyên.

Tiêu chí kiểm toán

Đảm bảo tiến độ dự án được duy trì và báo cáo thường xuyên lên ban quản lý.

Tài liệu yêu cầu

- Báo cáo tiến độ dự án/tình trạng dự án
- Văn bản, kết quả đánh giá tiến độ dự án
- Các hoạt động cần thực hiện để cải thiện tiến độ dự án (nếu có)

Đánh giá thiết kế và triển khai

- Phòng văn ban quản lý/trưởng nhóm dự án về quy trình báo cáo tiến độ dự án.
- Thu thập, rà soát báo cáo tiến độ dự án đánh giá liệu dự án có hoàn thành các mốc dự án với mức chi phí, nguồn lực và thời gian cho phép và được ghi chép lại không
- Thu thập các bằng chứng về tính định kỳ của báo cáo kiểm soát tiến độ. Rà soát các báo cáo, đảm bảo nó bao gồm những thông tin theo quy định

Thử nghiệm hiệu quả hoạt động

Dựa trên các báo tiến độ đã thực hiện, Kiểm toán viên nhà nước thực hiện chọn mẫu và tiến hành các bước tương tự như phân đánh giá thiết kế và triển khai để đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán

Kiểm soát B3.02.10: Quản lý thời gian và chi phí thực hiện dự án.

Tiêu chí kiểm toán

Nguồn lực thời gian và chi phí được ghi chép, phê duyệt và tài liệu hóa đầy đủ

Tài liệu yêu cầu

- Lịch/thời gian làm việc cho các thành viên trong đội dự án và đơn vị tư vấn bên ngoài
- Tài liệu liên quan đến chi phí thực hiện dự án

Đánh giá thiết kế và triển khai

- Phòng vấn Trường dự án/ban quản lý dự án về việc quản lý thời gian thực hiện dự án của mỗi thành viên trong đội đảm bảo thời gian và chi phí thực hiện dự án. Công tác này có được giám sát chặt chẽ và được tài liệu hóa đầy đủ không
- Thu thập, rà soát các phương thức ghi chép lại thời gian làm việc của mỗi thành viên và chi phí thực hiện cho dự án
- Phòng vấn Trường dự án/ban quản lý dự án xác minh các đơn vị tư vấn bên ngoài ghi chép lại thời gian làm việc và được phê duyệt định kỳ bởi cấp chức năng có thẩm quyền
- Phòng vấn Trường dự án/ban quản lý dự án và xác minh các chi phí của dự án đã được ban chỉ đạo dự án phê duyệt và thông qua. Tiến hành thu thập và rà soát các bằng chứng có liên quan.

Thử nghiệm hiệu quả hoạt động

Dựa trên việc thu thập các tài liệu ghi chép lại thời gian làm việc của mỗi thành viên và chi phí thực hiện dự án, Kiểm toán viên nhà nước thực hiện chọn mẫu và tiến hành các bước tương tự như phần đánh giá thiết kế và triển khai để đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán

Kiểm soát B3.02.11: Đánh giá kế hoạch truyền thông

Tiêu chí kiểm toán

Đảm bảo công tác truyền thông được thiết lập để cung cấp cho các bên liên quan và lãnh đạo dự án những thông tin phù hợp để đảm bảo rằng dự án đáp ứng được các chức năng, mục tiêu về thời gian và ngân sách của dự án.

Tài liệu yêu cầu

- Báo cáo kế hoạch truyền thông dự án
- Danh sách nhân sự tham gia công tác truyền thông của đội dự án và các bên liên quan
- Báo cáo đánh giá công tác truyền thông

Đánh giá thiết kế và triển khai

- Phòng vấn Trường dự án/ban chỉ đạo dự án về Phương thức, nội dung và tần suất thực hiện truyền thông, đảm bảo nội dung truyền thông bao hàm các thông tin về

dự án như trạng thái dự án, các vấn đề ngoại lệ... tất cả các báo cáo truyền thông đều được ghi nhận trên hệ thống quản lý dự án

- Thu thập, rà soát báo cáo truyền thông, để đánh giá chức năng của nó theo các tiêu chí sau: kế hoạch truyền thông được phổ biến tới các bộ phận tham gia dự án được cập nhật thường xuyên và chính xác, tần suất trao đổi nội dung diễn ra theo đúng kế hoạch truyền thông
- Phỏng vấn ban lãnh đạo/trưởng nhóm xác định sự tham gia của các bên trong kế hoạch truyền thông, được tài liệu hóa và phê duyệt.

Thử nghiệm hiệu quả hoạt động

Dựa trên các báo cáo về kế hoạch truyền thông, Kiểm toán viên nhà nước thực hiện chọn mẫu và tiến hành các bước tương tự như phần đánh giá thiết kế và triển khai để đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán

Vấn đề B3.03 – Quản lý ngân sách trong giai đoạn thực hiện dự án

Mục tiêu kiểm toán

Các quy trình ngân sách và kế toán phải chính xác, đầy đủ và cung cấp các thông tin cần thiết trong việc quản lý dự án.

Kiểm soát B3.03.01: Ngân sách dự án được xác định, tác biệt với các dự án khác và phù hợp với tình huống kinh doanh.

Tiêu chí kiểm toán

Giám sát chặt chẽ chi tiêu ngân sách dự án, đảm bảo chi tiêu phù hợp với tình huống kinh doanh

Tài liệu yêu cầu

- Tài liệu ghi chép chi tiêu ngân sách trong thực tế và được ước tính trong tình huống kinh doanh
- Các biện pháp cần thực hiện khi có sự chênh lệch
- Biên bản cuộc họp của đơn vị về vấn đề trên

Đánh giá thiết kế và triển khai

- Phỏng vấn Trưởng dự án/ban quản lý dự án và xác minh rằng ngân sách được cập nhật thường xuyên và phản ánh tất cả các thay đổi so với phạm vi ban đầu.
- Tiến hành thu thập các tài liệu liên quan chi tiêu ngân sách dự án rà soát và bảo đảm chi tiêu ngân sách thực tế phù hợp với chi tiêu ngân sách đã ước tính trong tình

huống kinh doanh. Nếu có sự chênh lệch, thu thập bằng chứng thể hiện sự chênh lệch và được phê duyệt bởi các bên liên quan (Ban lãnh đạo, đơn vị tài trợ, ban chỉ đạo)

Thử nghiệm hiệu quả hoạt động

Dựa trên các tài liệu thu thập được, Kiểm toán viên nhà nước thực hiện chọn mẫu và tiến hành các bước tương tự như phần đánh giá thiết kế và triển khai để đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán

Kiểm soát B3.03.02: Trạng thái ngân sách cần được theo dõi, đánh giá và cập nhật.

Tiêu chí kiểm toán

Chi phí thực tế và ngân sách phù hợp với tỷ lệ hoàn thành dự án

Tài liệu yêu cầu

- Tài liệu, sổ ngân sách và các chi phí
- Các biện pháp cần thực hiện khi có sự chênh lệch
- Biên bản cuộc họp của đơn vị về vấn đề trên

Đánh giá thiết kế và triển khai

- Phòng văn Trưởng dự án /ban quản lý dự án và xác minh xem các chi phí thực tế có dựa trên tỷ lệ phần trăm hoàn thành dự án hay không?
- Thu thập ngân tài liệu, sổ sách ngân sách và các chi phí, rà soát tài liệu đảm bảo chi phí thực tế phù hợp với các khoản ngân sách đã được lên kế hoạch theo từng giai đoạn dự án
- Đảm bảo tất cả các chi phí đều được phê duyệt bởi các cấp có thẩm quyền.
- Trong trường hợp chi thực tế khác với ngân sách kế hoạch ban đầu, đảm bảo ban quản lý dự án báo cáo lên các cấp lãnh đạo có thẩm quyền để rà soát và phê duyệt.

Thử nghiệm hiệu quả hoạt động

Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B3.03.03: Các tiêu chuẩn kế toán về chi phí và vốn hóa cần được tuân thủ.

Tiêu chí kiểm toán

Đảm bảo kế toán dự án tuân thủ tiêu chuẩn về chi phí và vốn hóa

Tài liệu yêu cầu

- Văn bản liên quan tới quy chuẩn kết toán
- Sổ kế toán định kỳ

Đánh giá thiết kế và triển khai

- Phòng vấn Trưởng dự án/ban quản lý dự án và xác minh xem kế toán dự án có áp dụng theo các quy chuẩn kế toán và được tài liệu hóa thành văn bản với sự phê duyệt của các cấp chức năng có thẩm quyền hay không
- Rà soát thu thập số kế toán xác định chi phí có được vốn hóa hoặc tính vào chi phí một cách hợp lý theo luật định hay không

Thử nghiệm hiệu quả hoạt động

Dựa trên các lần phân bổ chi phí và vốn hóa, Kiểm toán viên nhà nước thực hiện chọn mẫu và xác minh xem việc phân bổ vào chi phí hay vốn hóa có phù hợp với các tiêu chuẩn kế toán, có nằm trong hướng dẫn kế toán hay không?

Vấn đề B3.04 - Kiểm soát nội bộ trong giai đoạn thực hiện dự án

Mục tiêu kiểm toán

Kiểm soát nội bộ cần có một cách tiếp cận hiệu quả, hợp lý và toàn diện để kiểm soát dữ liệu và quy trình ứng dụng.

Kiểm soát B3.04.01: Thiết lập hệ thống kiểm soát rủi ro trong giai đoạn lập kế hoạch

Tiêu chí kiểm toán

Kiểm soát đánh giá rủi ro được chuẩn bị trong giai đoạn lập kế hoạch được cập nhật để xác định các yêu cầu kiểm soát nội bộ chi tiết dựa trên các rủi ro về xử lý, vận hành và tài chính.

Tài liệu yêu cầu

- Quy trình đánh giá và xử lý rủi ro
- Văn bản ghi chép công tác đánh giá rủi ro dự án

Đánh giá thiết kế và triển khai

- Phòng vấn quản lý dự án về công tác cập nhật đánh giá rủi ro kiểm soát được thực hiện từ giai đoạn lên kế hoạch dự án, về các kiểm soát thiết kế tương ứng với các rủi ro
- Rà soát bản đánh giá rủi ro của nhóm dự án để xác định xem các kiểm soát được xác định một cách hợp lý hay không và việc đánh giá đã hoàn tất hay chưa.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Vấn đề B3.04 – Tổ chức kiểm thử trong giai đoạn thực hiện dự án

Mục tiêu kiểm toán

Dự án cần phải bảo đảm được kiểm thử đầy đủ trước khi nhận bàn giao và đưa lên môi trường thật (môi trường vận hành). Kiểm thử cần phải bao hàm ít nhất Kiểm thử chấp nhận người dùng, tích hợp các quy trình thủ công và tự động, kiểm thử chuyển đổi dữ liệu... Đơn vị cũng cần xem xét việc kiểm thử trên một nền tảng riêng biệt, chạy thử song song trước khi tiến hành chạy hoàn toàn trên môi trường thật.

Kiểm soát B3.04.03 – Quy trình kiểm thử cần được thiết lập.

Tiêu chí kiểm toán

Quy trình kiểm thử được thực hiện theo chuẩn dự án và đơn vị, quy trình kiểm thử cần phải được tài liệu hóa ra và rà soát bởi các cấp theo thẩm quyền

Tài liệu yêu cầu

- Kế hoạch kiểm thử
- Nhật ký kiểm thử trong quá trình thực hiện dự án
- Danh sách các thành viên phụ trách kiểm thử

Đánh giá thiết kế và triển khai

- Phòng vấn Trưởng dự án/Ban quản lý dự án và xác minh kế hoạch kiểm thử đã được thông qua bởi ban lãnh đạo đơn vị.
- Rà soát kế hoạch kiểm thử và đảm bảo kế hoạch kiểm thử đã đưa ra những yêu cầu kiểm thử cho các hạng mục của dự án. Xác minh xem kế hoạch kiểm thử đã bao gồm ít nhất các phần như kiểm thử chấp nhận người dùng, kiểm thử chuyển đổi dữ liệu, kiểm thử với dữ liệu lớn/số lượng người dùng lớn... hay chưa
- Rà soát kế hoạch kiểm thử đảm bảo các bước kiểm thử được tài liệu hóa và phê duyệt bởi các cấp có thẩm quyền
- Rà soát kịch bản và kết quả kiểm thử đảm bảo được phê duyệt bởi các cấp có thẩm quyền
- Phòng vấn Trưởng dự án/Ban quản lý dự án và xác minh xem liệu rằng tất cả các loại kiểm thử đã được thực hiện cho các hạng mục của dự án, đã được rà soát và thông qua bởi các cấp lãnh đạo đơn vị hay chưa?

Thử nghiệm hiệu quả hoạt động

Dựa trên các hạng mục của dự án, Kiểm toán viên nhà nước tiến hành chọn mẫu và xác minh các vấn đề sau:

- Đảm bảo hạng mục của dự án đã được kiểm thử, quy trình và kết quả kiểm thử được tài liệu hóa đầy đủ, được phê duyệt bởi các cấp có thẩm quyền
- Đảm bảo tất cả các phần việc yêu cầu chỉnh sửa được xem xét bởi ban quản lý dự án và bên phát triển dự án

Kiểm soát B3.04.04: Thời gian tiến hành kiểm thử cần được đánh giá

Tiêu chí kiểm toán

Đảm bảo kế hoạch dự án ban đầu xác định được đầy đủ thời gian để tiến hành kiểm thử và khắc phục dựa trên kết quả kiểm thử

Tài liệu yêu cầu

- Bản kế hoạch dự án ban đầu
- Báo cáo đánh giá kết quả kiểm thử chấp nhận người dùng

Đánh giá thiết kế và triển khai

- Phòng vận Trưởng dự án/Ban quản lý dự án và xác minh Phương thức đơn vị xác định thời gian cho chương trình kiểm thử. Rà soát bản kế hoạch dự án ban đầu và xác minh xem dự án có đầy đủ thời gian cho kế hoạch kiểm thử hay không,
- Phòng vận Trưởng dự án/Ban quản lý dự án và xác minh xem việc bắt đầu giai đoạn Kiểm thử chấp nhận người dùng có bị chậm hay không? Việc bắt đầu giai đoạn kiểm thử chấp nhận người dùng muộn hơn so với kế hoạch có ảnh hưởng tới việc không kiểm thử hết các hạng mục hoặc không chỉnh sửa hết các hạng mục hay không?

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B3.04.05: Kết quả kiểm thử cần được đánh giá về tính hiệu quả

Tiêu chí kiểm toán

Kịch bản kiểm thử và tài kiểm thử là đầy đủ để bảo đảm tính chính xác, hiệu quả của kết quả kiểm thử

Tài liệu yêu cầu

- Văn bản ghi chép kết quả kiểm thử
- Quy trình kiểm thử

Đánh giá thiết kế và triển khai

- Kiểm toán viên nhà nước tiến hành rà soát kết quả kiểm thử để đảm bảo việc kiểm thử được hoàn thành một cách đầy đủ
- Rà soát kết quả kiểm tra tải đảm bảo tải kiểm thử thực tế được sử dụng để kiểm tra tải của hệ thống trong hiện tại và tương lai.

Thử nghiệm hiệu quả hoạt động

Dựa trên các hạng mục kiểm thử của dự án, Kiểm toán viên nhà nước tiến hành bốc mẫu và xác minh các vấn đề sau:

- Rà soát lại kết quả kiểm thử, thực hiện kiểm thử độc lập bảo đảm hạng mục đó đã được kiểm thử và kết quả kiểm thử là đúng theo quy trình
- Kiểm tra tải với hạng mục kiểm thử, đảm bảo tính ổn định của hệ thống ở trong mức tải cho phép.

Vấn đề B3.05 – Việc triển khai hệ thống

Mục tiêu kiểm toán

Kế hoạch triển khai cần được xây dựng để đảm bảo sự gián đoạn tối thiểu trong quá trình triển khai hệ thống mới. Kế hoạch triển khai cần bao hàm việc kiểm tra kỹ lưỡng các quy trình trước khi chuyển đổi sang hệ thống mới.

Kiểm soát B3.05.01 – Thử nghiệm thí điểm cần được lên kế hoạch, triển khai và đánh giá

Tiêu chí kiểm toán

Đơn vị tiến hành triển khai thí điểm các quy trình mới để giảm thiểu rủi ro khi triển khai toàn bộ ứng dụng

Tài liệu yêu cầu

- Kế hoạch thử nghiệm thí điểm
- Quy trình, thủ tục thử nghiệm thí điểm
- Kết quả thử nghiệm thí điểm
- Biên bản cuộc họp/báo cáo đánh giá kết quả thử nghiệm thí điểm

Đánh giá thiết kế và triển khai

- Phòng vấn Trưởng dự án/Ban quản lý dự án và xác minh xem đơn vị có tiến hành việc triển khai thí điểm trước khi triển khai toàn bộ ứng dụng hay không? Rà soát kết quả triển khai thí điểm, đảm bảo toàn bộ phạm vi triển khai thí điểm được hoàn thành

- Đánh giá hiệu quả của quy trình triển khai thí điểm, đảm bảo kết quả của chương trình triển khai thí điểm đã vạch ra được tất cả những vấn đề phát sinh trong quá trình triển khai thí điểm, và những vấn đề đó được ghi nhận trong hệ thống quản lý các vấn đề và được phê duyệt bởi các bên có thẩm quyền

- Phòng vận Trường dự án/Ban quản lý dự án và xác minh xem mục tiêu của việc triển khai thí điểm có đạt được sau khi kết thúc quy trình triển khai thí điểm hay không?

- Phòng vận Trường dự án/Ban quản lý dự án và xác minh xem đơn vị có phải xem xét việc ra quyết định tiếp tục hay dừng lại dự án sau khi hoàn thành triển khai thí điểm hay không

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B3.05.02 - Đánh giá sự sẵn sàng của hệ thống.

Tiêu chí kiểm toán

Đảm bảo kế hoạch dự án ban đầu của đơn vị có bao hàm quy trình về đánh giá tính sẵn sàng của hệ thống

Tài liệu yêu cầu

- Quy trình đánh giá tính sẵn sàng của hệ thống trước khi đưa hệ thống lên môi trường thật

- Danh sách các vấn đề và danh sách các rủi ro của dự án

- Danh sách nhân sự tham gia vào quá trình đưa hệ thống lên môi trường thật

Đánh giá thiết kế và triển khai

- Phòng vận Trường dự án/Ban chỉ đạo dự án và xác minh xem đơn vị có thực hiện quy trình đánh giá tính sẵn sàng của hệ thống trong kế hoạch ban đầu của dự án trước khi đưa hệ thống lên môi trường thật hay không.

- Phòng vận Trường dự án/Ban chỉ đạo dự án và xác minh xem quy trình đánh giá tính sẵn sàng của hệ thống bao gồm những hạng mục, công việc nào. Đảm bảo quy trình cần bao hàm những công việc sau:

- Danh sách các vấn đề còn tồn đọng khi đưa lên môi trường thật
- Đánh giá rủi ro của các tác động đến đơn vị khi sử dụng hệ thống mới
- Phê duyệt của các bên liên quan và lãnh đạo đơn vị về khả năng sẵn sàng của hệ thống và chuyển giao lên môi trường thật

- Rà soát danh sách các vấn đề và danh sách các rủi ro của dự án và xác minh tính chính xác của báo cáo đánh giá sự sẵn sàng của hệ thống

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B3.05.03 - Kế hoạch nguồn lực của dự án cần được giám sát và cập nhật thường xuyên

Tiêu chí kiểm toán

Kế hoạch nguồn lực của dự án được giám sát, theo dõi trong suốt quá trình thực thi dự án để bảo đảm đơn vị phân bổ đầy đủ các nguồn lực theo kế hoạch cho các quy trình quan trọng khi đưa hệ thống lên môi trường thật

Tài liệu yêu cầu

- Kế hoạch nguồn lực của dự án
- kế hoạch dự phòng nguồn nhân sự trong giai đoạn triển khai hệ thống mới
- Các rủi ro có thể xảy ra và các kiểm soát

Đánh giá thiết kế và triển khai

- Phòng vấn trưởng dự án/ban quản lý dự án và xác minh xem kế hoạch nguồn lực của dự án có thay đổi so với kế hoạch ban đầu hay không, đảm bảo nguồn lực dành cho dự án được duy trì và giám sát thường xuyên, không có tình trạng thiếu hụt nguồn lực.

- Phòng vấn Trưởng dự án/ban quản lý dự án về kế hoạch dự phòng về nguồn nhân sự trong giai đoạn triển khai hệ thống mới, đảm bảo luôn có nhân sự chủ chốt tham gia.

- Phòng vấn trưởng dự án/ban quản lý dự án và xác minh xem có vấn đề nào liên quan tới nguồn lực dự án xảy ra trong quá trình đưa hệ thống mới lên môi trường thật hay không? Đánh giá các rủi ro cho dự án khi không được đảm bảo về mặt nguồn lực.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B3.05.04 - Kế hoạch chuyển đổi dữ liệu cần được thiết lập và đánh giá kết quả thực hiện

Tiêu chí kiểm toán

Kế hoạch chuyển đổi đã được kiểm tra kỹ lưỡng và dữ liệu đã được đối chiếu trước khi đưa hệ thống mới lên môi trường thật

Tài liệu yêu cầu

- Quy trình, thủ tục chuyển đổi dữ liệu
- Báo cáo đánh giá kết quả chuyển đổi dữ liệu

Đánh giá thiết kế và triển khai

▪ Phòng vấn Trưởng dự án/ban quản lý dự án và xác minh xem kế hoạch dự án ban đầu có bao gồm kế hoạch chuyển đổi dữ liệu hay không? Thu thập danh sách các bước thực hiện trong quy trình chuyển đổi dữ liệu, đảm bảo ban quản lý dự án cũng như các cấp có thẩm quyền đã rà soát và phê duyệt kế hoạch chuyển đổi dữ liệu.

▪ Rà soát kết quả của quá trình chuyển đổi, đối chiếu dữ liệu, đảm bảo toàn bộ các dữ liệu đã được đối chiếu đầy đủ trước khi đưa hệ thống lên vận hành ở môi trường thật.

▪ Rà soát kết quả của quá trình chuyển đổi/đối chiếu dữ liệu, đảm bảo ban chỉ đạo dự án/cơ quan tài trợ dự án đã xem xét và phê duyệt đồng ý đưa hệ thống lên vận hành ở môi trường thật.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên xem xét thực hiện kiểm thử độc lập cho quy trình chuyển đổi/đối chiếu dữ liệu nếu đánh giá quy trình chuyển đổi/đối chiếu dữ liệu có rủi ro cao để bảo đảm tính hữu hiệu hoạt động của kiểm soát.

Kiểm soát B3.05.05 - Kế hoạch truyền thông cần được thiết lập.

Tiêu chí kiểm toán

Đơn vị có kế hoạch truyền thông cho tất cả các bên liên quan về tiến độ đưa hệ thống lên vận hành ở môi trường thật

Tài liệu yêu cầu

▪ Kế hoạch truyền thông đến các bên liên quan khi đưa hệ thống lên vận hành ở môi trường thật

- Nội dung truyền thông

Đánh giá thiết kế và triển khai

- Phòng vấn Trưởng dự án/ban quản lý dự án và xác minh xem đơn vị có kế hoạch truyền thông cho các bên liên quan về tiến độ đưa hệ thống lên vận hành ở môi trường thật hay không?
- Rà soát chương trình truyền thông của đơn vị, đảm bảo bao gồm các quy định về tần suất, kênh truyền thông và nội dung truyền thông.

Thử nghiệm hiệu quả hoạt động

Dựa trên các truyền thông mà ban quản lý dự án đã thực hiện, Kiểm toán viên nhà nước tiến hành chọn mẫu và xác minh các truyền thông đó là phù hợp với các quy định được ban hành trong kế hoạch truyền thông (về tần suất, các kênh truyền thông và nội dung truyền thông)

Kiểm soát B3.05.06 - Kế hoạch đào tạo cần được thiết lập

Tiêu chí kiểm toán

Chương trình đào tạo cho tất cả các phòng ban liên quan của dự án trước khi hệ thống mới đưa môi trường thật

Tài liệu yêu cầu

- Kế hoạch, nội dung đào tạo về hệ thống mới
- Danh sách người tham gia đào tạo
- Danh sách nhân viên chịu trách nhiệm đào tạo
- Tài liệu hỗ trợ đào tạo, công cụ, phần mềm.

Đánh giá thiết kế và triển khai

- Rà soát kế hoạch đào tạo, nội dung đào tạo đảm bảo tất cả các chức năng liên quan tới vận hành hệ thống mới trên hệ thống thật được đưa vào chương trình đào tạo cho nghiệp vụ, CNTT, helpdesk....
- Rà soát kết quả đào tạo, danh sách những người tham gia đào tạo, đảm bảo tất cả các bên liên quan tham gia vào quá trình đào tạo.
- Rà soát các tài liệu hỗ trợ (tài liệu đào tạo, hướng dẫn sử dụng, các quy trình thủ công, quy trình hỗ trợ...), đảm bảo các thông tin đầy đủ để đơn vị có thể vận hành hệ thống mới.

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách những người tham gia đào tạo, Kiểm toán viên nhà nước tiến hành chọn mẫu và xác minh các vấn đề sau:

- Phòng vận nhân viên xử lý giao dịch và xác minh họ đã được đào tạo đúng cách trong việc sử dụng hệ thống mới
- Phòng vận nhân viên vận hành hệ thống và xác minh họ đã được đào tạo đúng cách về việc lập kế hoạch và xử lý hệ thống mới
- Phòng vận nhân viên hỗ trợ và xác minh họ đã được đào tạo và chuẩn bị để hỗ trợ người dùng trong việc sử dụng hệ thống mới.

Kiểm soát B3.05.07 - Kế hoạch chuyển giao cần được thiết lập

Tiêu chí kiểm toán

Kế hoạch chuyển giao quy định các quy trình trung gian cần thực hiện cho tới khi hệ thống mới được vận hành hoàn toàn và tích hợp với các hệ thống khác

Tài liệu yêu cầu

- Quy trình, thủ tục chuyển giao hệ thống mới
- Danh sách nhân sự tham gia chuyển giao hệ thống
- Báo cáo đánh giá kết quả chuyển giao

Đánh giá thiết kế và triển khai

- Phòng vận quản lý dự án liệu dự án có xây dựng một kế hoạch chuyển giao chính thức hay không? Kế hoạch này có được ghi chép, đánh giá bởi cấp có thẩm quyền hay không?
- Thu thập kế hoạch chuyển giao và xác nhận xem trong kế hoạch đó các quy trình tạm thời khi hệ thống chưa được tích hợp một cách hoàn toàn các chức năng và quy trình

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B3.05.08: Kế hoạch khôi phục được rà soát và phê duyệt ngay từ bước khởi động dự án.

Tiêu chí kiểm toán

Đảm bảo đơn vị có kế hoạch khôi phục. Kế hoạch khôi phục được rà soát và phê duyệt ngay từ bước khởi động dự án.

Tài liệu yêu cầu

- Kế hoạch khôi phục
- Nhân sự chịu trách nhiệm thực hiện kế hoạch khôi phục

Đánh giá thiết kế và triển khai

- Phòng vận trưởng dự án/ban quản lý dự án và xác minh kế hoạch khôi phục được rà soát và phê duyệt ngay từ bước khởi động dự án hay không.
- Rà soát kế hoạch khôi phục, đảm bảo kế hoạch khôi phục chỉ rõ các quy trình để đưa hệ thống về trạng thái ổn định, sử dụng hệ thống cũ.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Vấn đề B3.06 – Quản lý Nhà cung cấp dịch vụ bên ngoài trong giai đoạn thực hiện dự án

Mục tiêu kiểm toán

Đảm bảo việc lựa chọn nhà cung cấp dịch vụ bên ngoài hiệu quả, tối đa lợi tức đầu tư. Đơn vị cung cấp dịch vụ bên ngoài cần được kiểm tra, đánh giá và xem xét đầy đủ. Trong hợp đồng cung cấp dịch vụ với nhà cung cấp cần nêu rõ các sản phẩm bàn giao (có thể thấy được) và các điều khoản liên quan tới sở hữu trí tuệ.

Kiểm soát B3.06.01 Các cam kết trong thỏa thuận chất lượng dịch vụ được thực hiện đầy đủ và có chế tài xử phạt trong trường hợp không tuân thủ.

Tiêu chí kiểm toán

Đơn vị có chế tài phù hợp với các trường hợp nhà cung cấp dịch vụ không tuân thủ các quy định trong thỏa thuận chất lượng dịch vụ và hợp đồng để đảm bảo nhà cung cấp dịch vụ đúng các điều khoản trong thỏa thuận dịch vụ và hợp đồng

Tài liệu yêu cầu

- Các chính sách liên quan tới dịch vụ thuê khoán
- Các tài liệu phân tích lợi nhuận – chi phí khi thuê khoán chức năng dịch vụ bên ngoài
- Hồ sơ thuê ngoài
- Các thỏa thuận dịch vụ (SLA)

Đánh giá thiết kế và triển khai

- Phòng vận Truởng dự án/ban quản lý dự án và xác minh rằng các khoản mục trong Thỏa thuận dịch vụ đã được hoàn thành.
- Thu thập Thỏa thuận dịch vụ và các hồ sơ quản lý thỏa thuận dịch vụ, rà soát, so sánh thỏa thuận dịch vụ với các hồ sơ quản lý và xác minh tất cả các khoản mục trong thỏa thuận dịch vụ đã được hoàn thành
- Phòng vận Truởng dự án/Ban quản lý dự án và xác minh xem thủ tục bổ sung có được thực hiện khi nhà cung cấp không hoàn thành được các quy định trong thỏa thuận dịch vụ
- Rà soát Thỏa thuận dịch vụ và xác minh tất cả các khoản mục nhà cung cấp không hoàn thành theo quy định trong thỏa thuận dịch vụ đều được bao hàm trong kế hoạch bổ sung với nhà cung cấp
- Phòng vận Truởng dự án/Ban quản lý dự án và xác minh xem các hình phạt có được thiết lập, đánh giá và thu tiền về đơn vị khi nhà cung cấp dịch vụ không tuân thủ theo thỏa thuận dịch vụ hay không. Rà soát quy trình đánh giá các hình phạt và xác minh xem đơn vị đã thu tiền về chưa, xác định trạng thái của hình phạt nếu đơn vị chưa thu tiền về

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B3.06.02: Việc thanh toán cho nhà cung cấp được rà soát thường xuyên.

Tiêu chí kiểm toán

Đảm bảo việc xuất hóa đơn/thanh toán cho nhà cung ứng dịch vụ được rà soát/thực hiện thường xuyên theo các quy định trong hợp đồng

Tài liệu yêu cầu

- Bảng chấm công của nhà cung cấp dịch vụ
- Hóa đơn thanh toán của đơn vị cho nhà cung cấp

Đánh giá thiết kế và triển khai

- Phòng vận Truởng dự án/ban quản lý dự án và xác minh xem nhà cung cấp có gửi bảng chấm công cho đơn vị để phản ánh các phần việc nhà cung cấp đã hoàn thành theo như trong hợp đồng hay không?

- Rà soát bảng chấm công của nhà cung cấp và đảm bảo nó đã được rà soát và thông qua bởi bản quản lý dự án

- Rà soát các thanh toán của đơn vị cho nhà cung cấp và đảm bảo việc xuất hóa đơn và thanh toán cho nhà cung cấp là chính xác dựa trên các quy định của hợp đồng, thời gian đóng góp cho dự án của nhà cung cấp cũng như các sản phẩm bàn giao khác.

Thử nghiệm hiệu quả hoạt động

Dựa trên các lần xuất hóa đơn/thanh toán của đơn vị cho nhà cung cấp, Kiểm toán viên nhà nước tiến hành chọn mẫu và đánh giá xem việc xuất hóa đơn/thanh toán của đơn vị cho nhà cung cấp đã phù hợp với các quy định trong hợp đồng, khối lượng công việc hoàn thành của nhà cung cấp hay chưa?

5. Chuyên đề B4 - Công tác kết thúc dự án

a. Khái niệm

Đây là giai đoạn thực hiện công tác đóng dự án, tổng kết chi phí và công tác kế toán cũng như chuyển giao các quy trình còn lại cho bộ phận vận hành

b. Các rủi ro liên quan

- Các yêu cầu thay đổi liên quan tới kịch bản kinh doanh không được phê duyệt chính thức
- Các văn bản đóng dự án không được phê duyệt chính thức bởi nhà điều hành tài trợ
- Các vấn đề phát sinh cần giải quyết không được xử lý kịp thời
- Các sản phẩm dự án không được bàn giao toàn bộ
- Chi phí phát sinh sau khi đóng dự án chính thức
- Công tác truyền thông về việc đóng dự án không được thực hiện một cách toàn diện
- Công tác tổng kết chi phí phát sinh thực tế của dự án không được thực hiện một cách đúng đắn
- Kế toán dự án không tuân thủ theo các chuẩn mực kế toán về hoạch toán chi phí và vốn hóa
- Việc hoàn thiện hợp đồng không được rà soát và đánh giá phù hợp của các cấp liên quan trong đơn vị

- Đối tác tiếp tục truy cập vào các nguồn tài nguyên thông tin của đơn vị sau khi đóng dự án

c. Các vấn đề thực hiện kiểm toán

- Các văn bản đóng dự án có được phê duyệt chính thức bởi nhà điều hành tài trợ không
- Các vấn đề phát sinh cần giải quyết có được chuyển tới bộ phận vận hành có thẩm quyền giải quyết không?
- Có sự xác nhận của ban quản lý dự án về việc đơn vị thầu cung cấp đầy đủ các sản phẩm bàn giao của dự án không?
- Dự án có phát sinh thêm các yêu cầu về nguồn lực và chi phí sau khi đóng chính thức dự án hay không?
- Các đơn vị liên quan có được truyền thông về việc đóng dự án không?
- Công tác tổng kết chi phí phát sinh thực tế của dự án cùng với các phân tích về chênh lệch giữa chi phí thực tế và kế hoạch chi phí có được thực hiện không?
- Kế toán dự án có tuân thủ theo các chuẩn mực kế toán về hoạch toán chi phí và vốn hóa cho các chi phí dự án không?
- Quản lý dự án có thực hiện công tác rà soát các sản phẩm bàn giao của dự án không?
- Đối tác có còn quyền truy cập vào các nguồn tài nguyên thông tin của đơn vị sau khi kết thúc dự án hay không?

d. Chương trình kiểm toán mẫu

Vấn đề B4.01 - Quản trị dự án trong giai đoạn kết thúc dự án

Mục tiêu kiểm toán

Ban lãnh đạo cần thực hiện giám sát dự án liên tục và đầy đủ. Các nguồn lực kỹ thuật cần được phân công đầy đủ đảm bảo tiến độ của dự án. Đơn vị cần có những chính sách, quy định để bảo đảm ban quản lý dự án báo cáo liên tục lên ban lãnh đạo, để ban lãnh đạo đơn vị kịp thời ứng phó với các vấn đề phát sinh.

Kiểm soát B4.01.01: Các phần chỉnh sửa của kịch bản kinh doanh phải được phê duyệt.

Tiêu chí kiểm toán

Đảm bảo đơn vị chủ quản dự án và ban chỉ đạo dự án đều đã thông qua và phê duyệt các phần chỉnh sửa kịch bản doanh

Tài liệu yêu cầu

- Lịch sử thay đổi phạm vi dự án, kịch bản kinh doanh
- Tài liệu liên quan tới việc chấp nhận hoặc không chấp nhận thay đổi từ phía ban lãnh đạo dự án

Đánh giá thiết kế và triển khai

- Phòng vận đơn vị chủ quản dự án và xác minh rằng tình huống hoạt động, quy trình kinh doanh, các thuộc tính kinh doanh đề đã được bàn giao cùng với ứng dụng hệ thống.
- Phòng vận trưởng nhóm dự án, thu thập lịch sử thay đổi phạm vi dự án, rà soát các yêu cầu thay đổi lớn ảnh hưởng tới tình huống hoạt động, và xác minh những thay đổi đó cũng đã được thực hiện, bàn giao cùng với ứng dụng hệ thống.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B4.01.02: Đơn vị chủ quản dự án đã thông qua và xác nhận chính thức kết thúc dự án.

Tiêu chí kiểm toán

Xác minh dự án đã kết thúc

Tài liệu yêu cầu

Tài liệu, báo cáo kết thúc dự án

Đánh giá thiết kế và triển khai

Phòng vận trưởng nhóm dự án, thu thập tài liệu đóng dự án, xác minh đơn vị chủ quản dự án đã xác nhận chính thức đóng dự án. (như kí văn bản xác nhận...)

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề B4.02 - Quản lý dự án trong giai đoạn kết thúc dự án CNTT

Mục tiêu kiểm toán

Hoạt động quản lý dự án chính thức kết thúc, mọi hoạt động của dự án đều đã được chuyển giao cho bộ phận vận hành hoặc đơn vị kinh doanh.

Kiểm soát B4.01.01: Các vấn đề phát sinh sau dự án được chuyển giao sang cho bộ phận vận hành.

Tiêu chí kiểm toán

Xác minh các vấn đề phát sinh sau dự án được chuyển giao sang cho bộ phận vận hành

Tài liệu yêu cầu

- Tài liệu kết thúc dự án
- Quy trình xử lý vấn đề phát sinh sau khi kết thúc dự án

Đánh giá thiết kế và triển khai

Phòng vấn trưởng nhóm dự án, thu thập tài liệu kết thúc dự án, rà soát các vấn đề phát sinh và xác minh đều được chuyển giao cho bộ phận vận hành. (Ví dụ như các bản sửa đổi cần thiết, các bản sửa lỗi bản vá)

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B4.01.02: Ban quản lý dự án xác minh tất cả những sản phẩm bàn giao đều đã được hoàn thành

Tiêu chí kiểm toán

Tất cả các sản phẩm bàn giao của dự án đều đã được hoàn thành

Tài liệu yêu cầu

- Tài liệu danh sách các sản phẩm bàn giao

- Văn bản liên quan tới việc ban quản lý xác nhận đầy đủ sản phẩm bàn giao

Đánh giá thiết kế và triển khai

▪ Phòng văn trưởng nhóm dự án, thu thập tài liệu danh sách các sản phẩm bàn giao, thu thập văn bản liên quan tới việc xác nhận đơn vị đã tiếp nhận đầy đủ các sản phẩm bàn giao.

- Xác minh ban quản lý dự án đã thực hiện xác nhận đủ sản phẩm bàn giao. (Ví dụ ký xác nhận bằng văn bản, hoặc gửi email thông báo cho cả đội dự án...)

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B4.01.03: Mọi quy trình liên quan tới chi phí và thời gian của dự án đều kết thúc.

Tiêu chí kiểm toán

Đảm bảo không có chi phí, thời gian, nguồn lực được phân bổ vào dự án.

Tài liệu yêu cầu

Tài liệu kết thúc dự án liên quan tới thời gian và chi phí dự án

Đánh giá thiết kế và triển khai

▪ Phòng văn trưởng nhóm dự án, thu thập tài liệu kết thúc dự án, xác minh thời gian và chi phí dự án đã được kết thúc lại.

- Xác minh rằng không có khoản phí nào được tính vào chi phí dự án sau khi đã kết thúc dự án

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B4.01.04: Các bên liên quan đều được thông báo về việc kết thúc dự án

Tiêu chí kiểm toán

Đảm bảo các bên liên quan đều được thông báo việc kết thúc dự án

Tài liệu yêu cầu

Email/tài liệu về việc kết thúc dự án được gửi tới các bên

Đánh giá thiết kế và triển khai

Phòng văn trưởng nhóm dự án, thu thập email/tài liệu thông báo được gửi cho tất cả các bên liên quan về việc kết thúc dự án.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề B4.03 - Quản lý ngân sách trong giai đoạn kết thúc dự án

Mục tiêu kiểm toán

Các quy trình liên quan tới kế toán đảm bảo chính xác và cung cấp đầy đủ thông tin về việc phân bổ chi phí cho toàn dự án.

Kiểm soát B4.03.01 – Những chênh lệch giữa chi phí thực tế với dự trù ngân sách cần phải được đánh giá.

Tiêu chí kiểm toán

Sau khi kết thúc dự án, các phí của dự án đều được tập hợp lại. Có sự giải thích về các chênh lệch giữa ngân sách ban đầu và chi phí thực tế đều có

Tài liệu yêu cầu

Bản tổng hợp ngân sách và chi phí dự án

Đánh giá thiết kế và triển khai

- Phòng văn nhân sự phụ trách ngân sách của dự án, thu thập bản tổng hợp ngân sách và chi phí dự án, xác minh ngân sách còn lại sau dự án, và tất cả các chi phí dự án.
- Rà soát và xác minh các phạm vi thay đổi trong báo cáo tài chính của dự án
- Đảm bảo đơn vị thực hiện thủ tục kết thúc kiểm toán nội bộ để đảm bảo tất cả các chi phí đã được đưa vào trong báo cáo
- Xác minh rằng ngân sách được sử dụng của dự án trùng với kết quả ước tính trong tình huống hoạt động. Nếu như có sự chênh lệch, rà soát các chênh lệch đó, kiểm tra lý do chênh lệch và xác minh các chênh lệch đã được phê duyệt bởi ban chỉ đạo dự án và nhà tài trợ.

- Phòng văn quản lý dự án/đơn vị chủ quản dự án, xác nhận thông tin về ngân sách và các sản phẩm bàn giao của dự án và đúng như mong đợi.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B4.03.02 – Các nguyên tắc kế toán về chi phí và vốn hóa cần phải được tuân thủ.

Tiêu chí kiểm toán

Đảm bảo kế toán của dự án tuân theo yêu cầu về chi phí và vốn hóa.

Tài liệu yêu cầu

- Báo cáo kế toán của dự án
- Tài liệu yêu cầu cung cấp thêm vốn cho dự án (nếu có)

Đánh giá thiết kế và triển khai

- Phòng văn nhân sự phụ trách kế toán của dự án, thu thập báo cáo kế toán của dự án, rà soát và xác minh chi phí phù hợp của dự án đều được vốn hóa và ghi vào danh mục chi phí theo đúng chuẩn mực kế toán.
- Xác minh các yêu cầu cung cấp thêm vốn cho dự án đều được phê duyệt và được ghi lại trong báo cáo kế toán của dự án. (nếu có)

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề B4.04 – Quản lý Nhà cung cấp dịch vụ bên ngoài trong giai đoạn kết thúc dự án

Mục tiêu kiểm toán

Việc chi trả cho nhà cung cấp dịch vụ bên ngoài đều tuân theo hợp đồng. Các thủ tục bổ sung bao gồm thu lại các khoản tiền phạt và tất cả các sản phẩm bàn giao chậm từ nhà cung cấp.

Kiểm soát B4.04.01: Sản phẩm bàn giao và các điều khoản hợp đồng cần phải được rà soát và phê duyệt.

Tiêu chí kiểm toán

Đảm bảo các điều khoản của hợp đồng đều được rà soát, tất cả các sản phẩm bàn giao đều được rà soát và chấp nhận, các vấn đề phát sinh trong hợp đồng đều được xem xét bởi quản lý dự án và nhà tài trợ (khi cần)

Tài liệu yêu cầu

- Tài liệu liên quan tới sản phẩm bàn giao

Đánh giá thiết kế và triển khai

- Phòng văn quản lý dự án, thu thập các tài liệu liên quan tới sản phẩm bàn giao và xác minh rằng các tài sản phẩm bàn giao đều được xem xét và chấp thuận.
- Xác minh rằng bộ phận chịu trách nhiệm về pháp luật của đơn vị đã rà soát các sản phẩm chuyển giao theo hợp đồng và xác nhận hợp đồng đã thực hiện.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B4.04.02: Việc truy cập thông tin doanh nghiệp của nhà cung cấp cần được vô hiệu hóa sau khi kết thúc dự án.

Tiêu chí kiểm toán

Đảm bảo việc truy cập thông tin doanh nghiệp của nhà cung cấp bị vô hiệu hóa và sau khi kết thúc dự án.

Tài liệu yêu cầu

Tài liệu liên quan tới việc chấm dứt quyền truy cập của nhà cung cấp sau khi hoàn thành dự án,

Đánh giá thiết kế và triển khai

- Phòng văn quản lý dự án, thu thập các tài liệu liên quan tới việc chấm dứt quyền truy cập của nhà cung cấp sau khi hoàn thành dự án, xác minh rằng nhà cung cấp đã trả lại đơn vị các tài sản liên quan tới dự án (ví dụ như tài liệu dự án)

- Phòng văn quản lý dự án, thu thập danh sách các thành viên của nhà cung cấp, kiểm tra trực tiếp trên hệ thống, đảm bảo quyền truy cập của tất cả các tài khoản từ phía nhà cung cấp đã được khóa hoặc xóa.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

6. Chuyên đề B5 - Công tác rà soát sau triển khai

a. Khái niệm

Giai đoạn rà soát sau triển khai là giai đoạn cuối cùng của dự án. Mục đích thực hiện các công tác đánh giá và rà soát như sau:

- Rà soát sự thành công của dự án
- Rà soát tài chính của các tình huống kinh doanh và kết quả
- Bài học kinh nghiệm và các cải tiến trong tương lai

b. Các rủi ro liên quan

- Đơn vị không có cơ chế đánh giá tính hiệu quả của dự án
- Dự án không thực hiện một cách định kỳ việc kiểm soát và báo cáo cho nhà điều hành tài trợ về sự phù hợp giữa kế hoạch dự án và các kịch bản kinh doanh
- ROI và KPI của dự án không được rà soát bởi ban lãnh đạo và nhà điều hành tài trợ
- Bản báo cáo ROI và ma trận hiệu quả không được gửi tới những người liên quan
- Kinh phí dự án không được tính toán một cách chính xác, dẫn đến sự chênh lệch giữa chi phí thực tế và kế hoạch không được giải thích rõ ràng và hợp lý
- Chi phí dự án không được phân bổ hợp lý vào chi phí vận hành hay chi phí vốn dự án
- Các yêu cầu kiểm soát nội bộ không được rà soát và thực thi trong suốt dự án dẫn đến các rủi ro kiểm soát nội bộ không được phát hiện

c. Các vấn đề thực hiện kiểm toán

Hiệu quả của dự án

- Đơn vị có quy trình giám sát để đánh giá tính hiệu quả của hệ thống mới hay không?
- Hệ thống mới có được chứng minh là ổn định sau khi đưa vào vận hành thực tế?
- Hệ thống mới có thỏa thuận cung cấp dịch vụ hay không?
- Nếu dự án có sự tham gia của nhiều đơn vị thì việc hợp tác giữa các đơn vị có hiệu quả hay không?
- Dự án có thực hiện kiểm soát và báo cáo định kỳ cho nhà điều hành tài trợ (executive sponsor) về sự phù hợp giữa kế hoạch dự án và các kịch bản kinh doanh không?
- ROI và KPI của dự án có được gửi ban lãnh đạo và nhà điều hành tài trợ xem xét và đánh giá không?
- Bản báo cáo ROI và ma trận hiệu quả có được gửi tới những người liên quan hay không?

Bảo trì sau triển khai

- Nhà cung cấp sản phẩm có hỗ trợ đơn vị một cách kịp thời và hiệu quả không?

Phân tích chi phí

- Cấp quản lý có phân tích sự chênh lệch giữa chi phí thực tế và kế hoạch đặt ra, bài học được rút ra cho các dự án tương lai không?
- Chi phí dự án có được phân bổ hợp lý vào chi phí vận hành hay chi phí vốn dự án hay không?

d. Chương trình kiểm toán mẫu

Vấn đề B5.01 - Quản trị dự án trong giai đoạn rà soát dự án

Mục tiêu kiểm toán

Xác minh tình hướng hoạt động ban đầu đã được thực hiện.

Kiểm soát B5.01.01: Kiểm toán công tác đánh giá chỉ số lợi tức đầu tư và chỉ số đánh giá hiệu quả hoạt động của dự án.

Tiêu chí kiểm toán

Đảm bảo các thông tin liên quan tới lợi tức đầu tư và chỉ số đánh giá hiệu quả hoạt động của dự án đều được xem xét bởi ban chỉ đạo dự án và nhà tài trợ.

Tài liệu yêu cầu

- Văn bản ghi chép việc tính toán các chỉ số đo lường: chỉ số lợi tức đầu tư, chỉ số đánh giá hiệu quả.
- Danh sách nhân sự tham gia tính toán các chỉ số đo lường

Đánh giá thiết kế và triển khai

- Phòng văn nhân sự chịu trách nhiệm theo thực hiện tính toán chỉ số lợi tức đầu tư và hiệu quả hoạt động của dự án, thu thập các báo cáo tính toán liên quan, Kiểm toán viên nhà nước thực hiện tính toán lại và xác minh tính chính xác của 2 chỉ số trên
- Xác minh rằng các chỉ số trên đều đã được xem xét và phê duyệt bởi ban chỉ đạo dự án và nhà tài trợ.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề B5.02 - Quản lý dự án trong giai đoạn rà soát dự án

Mục tiêu kiểm toán

Hoạt động quản lý dự án chính thức kết thúc, mọi hoạt động của dự án đều đã được chuyển giao cho bộ phận vận hành hoặc đơn vị kinh doanh.

Kiểm soát B5.02.01: Tài liệu các chỉ số đánh giá hiệu quả hoạt động của dự án được gửi cho các bên liên quan.

Tiêu chí kiểm toán

Tất cả các bên liên quan đều nhận được tài liệu về các chỉ số lợi tức đầu tư và các chỉ số đánh giá hiệu quả hoạt động của dự án.

Tài liệu yêu cầu

- Email/văn bản truyền thông công tác tính toán các chỉ số đo lường

- Danh sách nhân sự tham gia phân tích và truyền thông

Đánh giá thiết kế và triển khai

- Phòng văn nhân sự chịu trách nhiệm theo thực hiện tính toán chỉ số lợi tức đầu tư và hiệu quả hoạt động của dự án, thu thập các tài liệu liên quan tới 2 chỉ số này.
- Thu thập email/điện tín... của ban quản lý dự án gửi đi cho các đơn vị đơn quan.
- Phòng văn quản lý dự án, xác minh xác có cách nào xác nhận các bên liên quan đã xem các tài liệu liên quan chưa? Nếu có thu thập bằng chứng xác nhận (nếu có)

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề B5.03 – Quyết toán ngân sách dự án

Mục tiêu kiểm toán

Các quy trình liên quan tới kế toán đảm bảo chính xác và cung cấp đầy đủ thông tin về việc phân bổ chi phí cho toàn dự án.

Kiểm soát B5.03.01: Ngân sách dự án được quyết toán, phân tích và đánh giá.

Tiêu chí kiểm toán

Đảm bảo ngân sách dự án được quyết toán với tất cả các chi phí liên quan. Đơn vị hoàn thành bản so sánh giữa ngân sách ban đầu so với chi phí thực tế cùng với các giải thích cho các sự chênh lệch. Quản lý dự án phân tích và đánh giá các khoản chênh lệch đó để có thể tối ưu các chênh lệch đó trong tương lai (nếu có)

Tài liệu yêu cầu

- Danh sách nhân sự chịu trách nhiệm ngân sách dự án
- Báo cáo chi tiêu ngân sách dự án
- Tài liệu giải thích sự chênh lệch trong báo cáo ngân sách (nếu có)

Đánh giá thiết kế và triển khai

- Phòng văn nhân sự chịu trách nhiệm ngân sách dự án, thu thập báo cáo ngân sách dự án, xác minh ban quản lý đã xem xét báo cáo đó (bằng cách ký xác nhận hoặc ký nháy)
- Rà soát phần giải thích chênh lệch trong báo cáo ngân sách của dự án, xem xét và đánh giá mức độ chi tiết của các phần giải thích

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả và hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Vấn đề B5.04 – Quản lý Nhà cung cấp bên ngoài trong giai đoạn rà soát dự án

Mục tiêu kiểm toán

Việc chi trả cho nhà cung cấp dịch vụ bên ngoài đều tuân theo hợp đồng. Các thủ tục bổ sung bao gồm thu lại các khoản tiền phạt và tất cả các sản phẩm bàn giao chậm từ nhà cung cấp.

Kiểm soát B5.04.01: Các vấn đề còn tồn đọng và phát sinh cần phải được xem xét và giải quyết

Tiêu chí kiểm toán

Đảm bảo các điều khoản của hợp đồng đều được thực hiện, tất cả các sản phẩm bàn giao đều được rà soát và chấp nhận, các vấn đề phát sinh trong hợp đồng đều được xem xét bởi quản lý dự án và nhà tài trợ (khi cần)

Tài liệu yêu cầu

- Danh sách các vấn đề còn tồn đọng với nhà cung cấp
- Quy trình giải quyết các vấn đề tồn đọng trên.

Đánh giá thiết kế và triển khai

- Phòng vấn Trưởng dự án/ban quản lý dự án và xác minh xem còn vấn đề nào còn tồn đọng chưa giải quyết với nhà cung cấp dịch vụ hay không.
- Thu thập danh sách các vấn đề còn tồn đọng với nhà cung cấp, rà soát và xác minh xem đơn vị có cần đưa các thủ tục bổ sung để giảm thiểu tác động rủi ro của các vấn đề còn tồn đọng hay không
- Rà soát tài liệu và đảm bảo các vấn đề còn tồn đọng cũng như các thủ tục bổ sung được rà soát và thông qua bởi ban chỉ đạo dự án/nhà tài trợ dự án

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách các vấn đề còn tồn đọng, Kiểm toán viên nhà nước tiến hành chọn mẫu và thực hiện các bước tương tự như phần đánh giá thiết kế và triển khai để bảo đảm tính hiệu quả hoạt động của kiểm soát

7. Chuyên đề B6 - Kiểm toán dự án phần mềm CNTT sử dụng ngân sách nhà nước

a. Khái niệm

Đối với các dự án CNTT sử dụng ngân sách nhà nước thì vấn đề tuân thủ theo các chính sách, thông tư, nghị định... được ban hành của Nhà nước, các bộ ban ngành liên quan là đặc biệt quan trọng đối với công tác thực hiện kiểm toán CNTT của kiểm toán viên nhà nước. Nội dung của chuyên đề này nêu một số các vấn đề và kiểm soát trọng yếu trong quá trình thực hiện đầu tư dự án CNTT đã được ban hành chính thức trong các văn bản của nhà nước

b. Các rủi ro liên quan

- Rủi ro trong việc phân loại dự án không chính xác dẫn đến rủi ro trong việc áp dụng các thủ tục hướng dẫn thực hiện dự án tương ứng
- Đội ngũ tham gia dự án không đủ chuyên môn và năng lực để thực hiện cũng như giải quyết các vấn đề liên quan trong suốt quá trình thực hiện dự án đầu tư CNTT
- Kế hoạch chi phí và các chi phí phát sinh vượt quá định mức quy định của nhà nước ban hành một cách không hợp lý

Ngoài ra các kiểm toán viên cần tham khảo thêm các rủi ro ở chuyên đề từ B1 tới B5

c. Các vấn đề thực hiện kiểm toán

- Việc phân loại dự án có tuân theo quy định của Nhà nước hay không?
- Chủ trương đầu tư dự án và các bước thực hiện dự án phân loại theo các dự án trọng điểm quốc gia, dự án nhóm A, dự án nhóm B và dự án nhóm C có tuân theo các quy định hướng dẫn hay không?
- Quy định về bằng cấp, kinh nghiệm chuyên môn của các vị trí tham gia đội dự án có được tuân thủ theo không?
- Các chi phí dự án có tuân thủ theo các quy định về định mức được ban hành hay không?

d. Chương trình kiểm toán mẫu

Vấn đề B6.01.00 - Kiểm toán việc áp dụng khung tham số quản lý, phân loại dự án CNTT sử dụng NSNN

Kiểm soát B6.01.01: Đối tượng áp dụng việc quản lý và thực hiện đầu tư ứng dụng CNTT trong khuôn khổ 102/2009/NĐ-CP theo nguồn vốn

Tiêu chí kiểm toán

Đảm bảo tính đúng đắn đối với đối tượng áp dụng công tác quản lý và thực hiện đầu tư ứng dụng CNTT tuân theo 102/2009/NĐ-CP theo nguồn vốn.

Dẫn chứng quy định ban hành

Điều 1 Chương 1 102/2009/NĐ-CP

Tài liệu yêu cầu

- Danh sách đầu tư ứng dụng CNTT
- Thông tin chi tiết về nguồn vốn đầu tư ứng với từng ứng dụng CNTT.

Đánh giá thiết kế và triển khai

▪ Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có thực hiện quy định về quản lý và thực hiện đầu tư ứng dụng CNTT sử dụng nguồn vốn ngân sách nhà nước hay không.

▪ Thu thập, rà soát danh sách đầu tư ứng dụng CNTT cùng thông tin chi tiết về nguồn vốn nhằm xác định ứng dụng CNTT thỏa mãn một trong các điều kiện dưới đây phải tuân thủ theo 102/2009/NĐ-CP:

- Các dự án ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước do các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, các tổ chức chính trị, tổ chức chính trị xã hội, tổ chức xã hội, tổ chức xã hội nghề nghiệp (được xác định trong Luật Ngân sách nhà nước), các tỉnh, thành phố trực thuộc Trung ương (sau đây gọi chung là tỉnh), các quận, huyện, thị xã, thành phố thuộc tỉnh (sau đây gọi chung là huyện) và cấp xã quản lý;

- Các dự án ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước hỗ trợ cho các doanh nghiệp nhà nước, các quỹ do Tập đoàn kinh tế nhà nước, Tổng công ty nhà nước, công ty nhà nước độc lập và các tổ chức quản lý Quỹ khác (được xác định trong Luật Ngân sách nhà nước) quản lý;

- Dự án ứng dụng công nghệ thông tin sử dụng hỗn hợp nhiều nguồn vốn khác nhau trong đó vốn ngân sách nhà nước chiếm tỷ lệ từ 30% trở lên hoặc lớn nhất trong tổng mức đầu tư của dự án;
- Phần ứng dụng công nghệ thông tin sử dụng vốn ngân sách nhà nước trong các dự án đầu tư xây dựng công trình và các dự án đầu tư không có xây dựng công trình được quản lý như đối với một dự án ứng dụng công nghệ thông tin độc lập theo quy định tại Nghị định này;
- Các dự án ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước thuộc diện bí mật quốc gia không thuộc phạm vi điều chỉnh của Nghị định này;
- Các dự án ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước phải thu hồi vốn, Chủ đầu tư có trách nhiệm thu hồi và hoàn trả vốn đầu tư;
- Các dự án ứng dụng công nghệ thông tin sử dụng nguồn vốn hỗ trợ phát triển chính thức (gọi tắt là ODA), Chủ đầu tư thực hiện theo thỏa thuận tín dụng, cùng các điều ước quốc tế có liên quan mà Việt Nam là thành viên, và các quy định hiện hành về quản lý và sử dụng nguồn vốn ODA;
- Các dự án ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước của cơ quan đại diện Việt Nam tại nước ngoài.

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách đầu tư ứng dụng CNTT, Kiểm toán viên nhà nước tiến hành chọn mẫu và thực hiện các thủ tục như ở phần Đánh giá thiết kế và triển khai để bảo đảm tính hoạt động hữu hiệu của kiểm soát.

Kiểm soát B6.01.02: Đối tượng áp dụng việc quản lý và thực hiện đầu tư ứng dụng CNTT trong khuôn khổ 102/2009/NĐ-CP theo quy mô tổng mức vốn đầu tư

Tiêu chí kiểm toán

Đảm bảo tính đúng đắn đối với đối tượng áp dụng công tác quản lý và thực hiện đầu tư ứng dụng CNTT tuân theo 102/2009/NĐ-CP theo quy mô tổng mức vốn đầu tư

Dẫn chứng quy định ban hành

Điều 1 Chương 1 102/2009/NĐ-CP

Tài liệu yêu cầu

- Danh sách đầu tư ứng dụng CNTT
- Thông tin chi tiết về tổng mức vốn đầu tư ứng với từng ứng dụng CNTT

Đánh giá thiết kế và triển khai

▪ Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có thực hiện quy định về phân nhóm dự án CNTT: dự án quan trọng quốc gia, nhóm A, nhóm B, nhóm C hay không.

Thu thập, rà soát danh sách đầu tư ứng dụng CNTT cùng thông tin chi tiết về tổng mức vốn đầu tư nhằm xác định việc phân nhóm dự án tuân thủ theo quy định của nhà nước ban hành theo Điều 1 Chương 1 102/2009/NĐ-CP

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách đầu tư ứng dụng CNTT, Kiểm toán viên nhà nước tiến hành chọn mẫu và thực hiện các thủ tục như ở phần Đánh giá thiết kế và triển khai để bảo đảm tính hoạt động hữu hiệu của kiểm soát.

Vấn đề B6.02.00 - Trình kế hoạch trung hạn và xin chủ trương đầu tư dự án CNTT sử dụng NSNN

Kiểm soát B6.02.01: Chủ trương đầu tư dự án nhóm B, nhóm C được thực hiện theo đúng trình tự và thủ tục quy định.

Tiêu chí kiểm toán

Đảm bảo đơn vị thực hiện theo đúng trình tự và thủ tục quyết định cho các chủ trương đầu tư dự án nhóm B, nhóm C sử dụng vốn NS TW, vốn công trái quốc gia, vốn trái phiếu Chính phủ do địa phương quản lý.

Dẫn chứng quy định ban hành

Điều 27 luật đầu tư công 49/2014/QH13

Tài liệu yêu cầu

- Quy định về trình tự và thủ tục quyết định cho các chủ trương đầu tư nhóm B, nhóm C sử dụng vốn Ngân sách Trung ương, vốn công trái Quốc gia, vốn Trái phiếu Chính phủ do địa phương quản lý (nếu có)
- Các quyết định liên quan tới chủ trương đầu tư các dự án nhóm B, nhóm C sử dụng nguồn vốn Ngân sách Trung ương, vốn công trái quốc gia, vốn Trái phiếu Chính phủ do địa phương quản lý

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có ban hành văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định về trình tự và thủ tục quyết định cho các chủ trương đầu tư nhóm B, nhóm C sử dụng vốn Ngân sách Trung ương, vốn công trái Quốc gia, vốn Trái phiếu Chính phủ do địa phương quản lý hay không.

- Thu thập, rà soát các văn bản quy định nội bộ (nếu có)

- Thu thập, rà soát các quyết định liên quan tới chủ trương đầu tư các dự án nhóm B, nhóm C, sử dụng nguồn vốn Ngân sách Trung ương, vốn công trái quốc gia, vốn Trái phiếu Chính phủ do địa phương quản lý và đảm bảo trình tự và thủ tục quyết định được thực hiện tuân theo quy định nội bộ ban hành (nếu có) và tuân theo điều 27 luật đầu tư công (trong trường hợp không có quy định ban hành nội bộ) như sau:

- Đối với dự án nhóm B và dự án trọng điểm nhóm C:

- Đối với dự án nhóm B và dự án trọng điểm nhóm C do Ủy ban nhân dân cấp tỉnh quản lý, Ủy ban nhân dân cấp tỉnh giao Sở Kế hoạch và Đầu tư thẩm định nguồn vốn và khả năng cân đối vốn trước khi trình Hội đồng nhân dân cấp tỉnh cho ý kiến về Báo cáo đề xuất chủ trương đầu tư.

- Sau khi Hội đồng nhân dân cấp tỉnh chấp thuận, Ủy ban nhân dân cấp tỉnh gửi Bộ Kế hoạch và Đầu tư Báo cáo đề xuất chủ trương đầu tư;

- Đối với dự án nhóm B và dự án trọng điểm nhóm C do Ủy ban nhân dân cấp huyện, cấp xã quản lý, Ủy ban nhân dân trình Hội đồng nhân dân cùng cấp cho ý kiến về Báo cáo đề xuất chủ trương đầu tư.

- Sau khi Hội đồng nhân dân cùng cấp chấp thuận, Ủy ban nhân dân cấp huyện, cấp xã gửi Ủy ban nhân dân cấp tỉnh Báo cáo đề xuất chủ trương đầu tư. Ủy ban nhân dân cấp tỉnh giao Sở Kế hoạch và Đầu tư thẩm định nguồn vốn và khả năng cân đối vốn trước khi gửi Bộ Kế hoạch và Đầu tư Báo cáo đề xuất chủ trương đầu tư;

- Bộ Kế hoạch và Đầu tư chủ trì, phối hợp với Bộ Tài chính thẩm định nguồn vốn và khả năng cân đối vốn;

- Ủy ban nhân dân cấp tỉnh chỉ đạo hoàn chỉnh Báo cáo đề xuất chủ trương đầu tư theo ý kiến thẩm định của Bộ Kế hoạch và Đầu tư;

- Ủy ban nhân dân trình Hội đồng nhân dân cùng cấp quyết định chủ trương đầu tư của dự án, bao gồm mục tiêu, quy mô, tổng mức đầu tư, cơ cấu nguồn vốn, địa điểm, thời gian, tiến độ thực hiện.
- Đối với các dự án nhóm C khác:
 - Đối với dự án do Ủy ban nhân dân cấp tỉnh quản lý, Ủy ban nhân dân cấp tỉnh giao Sở Kế hoạch và Đầu tư thẩm định nguồn vốn và khả năng cân đối vốn trước khi gửi Bộ Kế hoạch và Đầu tư Báo cáo đề xuất chủ trương đầu tư;
 - Đối với dự án do Ủy ban nhân dân cấp huyện, cấp xã quản lý, Chủ tịch Ủy ban nhân dân cấp Huyện, cấp xã gửi Ủy ban nhân dân cấp tỉnh Báo cáo đề xuất chủ trương đầu tư. Ủy ban nhân dân cấp tỉnh giao Sở Kế hoạch và Đầu tư thẩm định nguồn vốn và khả năng cân đối vốn trước khi gửi Bộ Kế hoạch và Đầu tư Báo cáo đề xuất chủ trương đầu tư;
 - Bộ Kế hoạch và Đầu tư chủ trì, phối hợp với Bộ Tài chính thẩm định nguồn vốn và khả năng cân đối vốn;
 - Ủy ban nhân dân cấp tỉnh chỉ đạo hoàn chỉnh Báo cáo đề xuất chủ trương đầu tư theo ý kiến thẩm định của Bộ Kế hoạch và Đầu tư;
 - Ủy ban nhân dân các cấp quyết định chủ trương đầu tư, bao gồm mục tiêu, quy mô, tổng mức đầu tư, cơ cấu nguồn vốn, địa điểm, thời gian, tiến độ thực hiện.

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách các quyết định liên quan tới chủ trương đầu tư các dự án nhóm B, nhóm C, sử dụng vốn Ngân sách Trung ương, vốn công trái quốc gia, vốn Trái phiếu Chính phủ do địa phương quản lý, Kiểm toán viên nhà nước tiến hành chọn mẫu và thực hiện các thủ tục như ở phần Đánh giá thiết kế và triển khai để bảo đảm tính hoạt động hữu hiệu của kiểm soát.

Kiểm soát B6.02.02: Báo cáo đề xuất chủ trương đầu tư chương trình đầu tư công cần đầy đủ nội dung theo quy định.

Tiêu chí kiểm toán

Đảm bảo các báo cáo đề xuất chủ trương đầu tư chương trình đầu tư công bao gồm đầy đủ các nội dung theo quy định

Dẫn chứng quy định ban hành

Điều 34 luật đầu tư công 49/2014/QH13

Tài liệu yêu cầu

- Văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định về trình tự và thủ tục quyết định nội dung Báo cáo đề xuất chủ trương đầu tư chương trình đầu tư công (nếu có).

- Các báo cáo đề xuất chủ trương đầu tư chương trình đầu tư công.

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có ban hành văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định về trình tự và thủ tục quyết định nội dung Báo cáo đề xuất chủ trương đầu tư chương trình đầu tư công hay không.

- Thu thập, rà soát các văn bản quy định (nếu có).

- Thu thập, rà soát các báo cáo đề xuất chủ trương đầu tư chương trình đầu tư công, và đảm bảo trình tự và thủ tục quyết định được thực hiện tuân theo quy định nội bộ ban hành (nếu có) và tuân theo điều 34 luật đầu tư công (trong trường hợp không có quy định ban hành nội bộ) đảm bảo nội dung các báo cáo bao gồm các khoản mục sau:

- Sự cần thiết của chương trình để thực hiện các mục tiêu chiến lược, quy hoạch, kế hoạch phát triển kinh tế – xã hội;

- Mục tiêu, phạm vi và quy mô chương trình;

- Dự kiến tổng mức vốn và cơ cấu nguồn lực thực hiện chương trình, bao gồm danh mục dự án hoặc đối tượng đầu tư, khả năng cân đối nguồn vốn đầu tư công, huy động các nguồn vốn và nguồn lực khác;

- Dự kiến tiến độ thực hiện chương trình phù hợp với điều kiện thực tế và khả năng huy động các nguồn lực theo thứ tự ưu tiên hợp lý bảo đảm đầu tư tập trung, có hiệu quả;

- Xác định chi phí liên quan trong quá trình thực hiện và chi phí vận hành sau khi chương trình kết thúc;

- Phân tích, đánh giá sơ bộ những ảnh hưởng, tác động về môi trường, xã hội của chương trình, tính toán hiệu quả đầu tư về mặt kinh tế – xã hội của chương trình;

- Phân chia các dự án thành phần của chương trình theo quy định của pháp luật;

- Các giải pháp tổ chức thực hiện

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách các báo cáo đề xuất chủ trương đầu tư chương trình đầu tư công, Kiểm toán viên nhà nước tiến hành chọn mẫu và thực hiện các thủ tục như ở phần Đánh giá thiết kế và triển khai để bảo đảm tính hoạt động hữu hiệu của kiểm soát.

Kiểm soát B6.02.03: Nội dung Báo cáo nghiên cứu tiền khả thi của dự án quan trọng quốc gia và dự án nhóm A

Tiêu chí kiểm toán

Đảm bảo các dự án quan trọng quốc gia và các dự án nhóm A được tiến hành nghiên cứu tiền khả thi và nội dung báo cáo nghiên cứu tiền khả thi bao gồm các khoản mục theo quy định

Dẫn chứng quy định ban hành

Điều 35 luật đầu tư công 49/2014/QH13

Tài liệu yêu cầu

Quy định nội bộ về nội dung Báo cáo nghiên cứu tiền khả thi dự án quan trọng quốc gia và dự án nhóm A (nếu có)

Đánh giá thiết kế và triển khai

- Báo cáo nghiên cứu tiền khả thi dự án quan trọng quốc gia, dự án nhóm A
- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có ban hành văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định về nội dung Báo cáo nghiên cứu tiền khả thi dự án quan trọng quốc gia và dự án nhóm A hay không
- Thu thập, rà soát các văn bản quy định (nếu có)
- Thu thập, rà soát các báo cáo nghiên cứu tiền khả thi dự án quan trọng quốc gia, dự án nhóm A, và đảm bảo trình tự và thủ tục quyết định được thực hiện tuân theo quy định nội bộ ban hành (nếu có) và tuân theo điều 35 luật đầu tư công (trong trường hợp không có quy định ban hành nội bộ) đảm bảo nội dung các báo cáo bao gồm các khoản mục sau:
 - Sự cần thiết đầu tư, các điều kiện để thực hiện đầu tư, đánh giá về sự phù hợp với quy hoạch, kế hoạch đầu tư;
 - Dự báo nhu cầu, phạm vi phục vụ và dự kiến mục tiêu đầu tư, quy mô và hình thức đầu tư;

- Khu vực, địa điểm đầu tư, dự kiến nhu cầu diện tích sử dụng đất và nhu cầu sử dụng tài nguyên khác;
- Phân tích, lựa chọn sơ bộ về công nghệ, kỹ thuật và các điều kiện cung cấp vật tư, thiết bị, nguyên liệu, năng lượng, dịch vụ, hạ tầng;
- Phân tích, lựa chọn sơ bộ các phương án đầu tư và quy mô các hạng mục đầu tư;
- Phương án tổng thể đền bù, giải phóng mặt bằng, tái định cư, biện pháp bảo vệ môi trường;
- Phân tích, đánh giá sơ bộ tác động về môi trường, xã hội của dự án;
- Xác định sơ bộ tổng mức đầu tư, phương án huy động vốn, cơ cấu nguồn vốn;
- Xác định sơ bộ chi phí vận hành, bảo dưỡng, duy tu, sửa chữa lớn trong giai đoạn khai thác dự án;
- Dự kiến tiến độ thực hiện dự án, phân chia giai đoạn đầu tư;
- Xác định sơ bộ hiệu quả đầu tư về kinh tế – xã hội của dự án;
- Phân chia các dự án thành phần hoặc tiểu dự án (nếu có);
- Các giải pháp tổ chức thực hiện.

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách các báo cáo nghiên cứu tiền khả thi dự án quan trọng Quốc gia, dự án nhóm A, Kiểm toán viên nhà nước tiến hành chọn mẫu và thực hiện các thủ tục như ở phần Đánh giá thiết kế và triển khai để bảo đảm tính hoạt động hữu hiệu của kiểm soát.

Kiểm soát B6.02.04: Nội dung Báo cáo đề xuất chủ trương đầu tư dự án nhóm B, nhóm C

Tiêu chí kiểm toán

Đảm bảo nội dung báo cáo đề xuất chủ trương đầu tư dự án nhóm B, nhóm C bao gồm các khoản mục theo quy định

Dẫn chứng quy định ban hành

Điều 36 luật đầu tư công 49/2014/QH13

Tài liệu yêu cầu

- Quy định nội bộ về nội dung Báo cáo nghiên cứu tiền khả thi dự án quan trọng quốc gia và dự án nhóm B, nhóm C (nếu có)
- Báo cáo đề xuất chủ trương đầu tư dự án nhóm B, nhóm C

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có ban hành văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định về nội dung Báo cáo đề xuất chủ trương đầu tư dự án nhóm B, nhóm C hay không
- Thu thập, rà soát các văn bản quy định (nếu có)
- Thu thập, rà soát các báo cáo đề xuất chủ trương đầu tư dự án nhóm B, nhóm C, và đảm bảo trình tự và thủ tục quyết định được thực hiện tuân theo quy định nội bộ ban hành (nếu có) và tuân theo điều 36 luật đầu tư công (trong trường hợp không có quy định ban hành nội bộ) đảm bảo nội dung các báo cáo bao gồm các khoản mục sau:
 - Sự cần thiết đầu tư, các điều kiện để thực hiện đầu tư, đánh giá về sự phù hợp với quy hoạch, kế hoạch đầu tư;
 - Mục tiêu, quy mô, địa điểm và phạm vi đầu tư;
 - Dự kiến tổng mức đầu tư và cơ cấu nguồn vốn đầu tư, khả năng cân đối nguồn vốn đầu tư công và việc huy động các nguồn vốn, nguồn lực khác để thực hiện dự án;
 - Dự kiến tiến độ triển khai thực hiện đầu tư phù hợp với điều kiện thực tế và khả năng huy động các nguồn lực theo thứ tự ưu tiên hợp lý bảo đảm đầu tư tập trung, có hiệu quả;
 - Xác định sơ bộ chi phí liên quan trong quá trình thực hiện và chi phí vận hành dự án sau khi hoàn thành;
 - Phân tích, đánh giá sơ bộ tác động về môi trường, xã hội; xác định sơ bộ hiệu quả đầu tư về kinh tế – xã hội;
 - Phân chia các dự án thành phần (nếu có);
 - Các giải pháp tổ chức thực hiện

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách các báo cáo nghiên cứu tiền khả thi dự án quan trọng Quốc gia, dự án nhóm B và nhóm C, Kiểm toán viên nhà nước tiến hành chọn mẫu và thực

hiện các thủ tục như ở phần Đánh giá thiết kế và triển khai để bảo đảm tính hoạt động hữu hiệu của kiểm soát.

Kiểm soát B6.02.05: Các dự án đầu tư CNTT sử dụng nguồn vốn NSNN giai đoạn 2016 – 2020 nằm trong danh mục hỗ trợ theo quy định của nhà nước

Tiêu chí kiểm toán

Đảm bảo các dự án đầu tư CNTT sử dụng nguồn vốn NSNN giai đoạn 2016 – 2020 nằm trong danh mục ưu tiên hỗ trợ theo quy định của nhà nước

Dẫn chứng quy định ban hành

Mục 13, phần 1 trong quy định đính kèm 40/2015/QĐ-TTg

Tài liệu yêu cầu

Các dự án đầu tư CNTT sử dụng nguồn vốn NSNN nằm trong phạm vi kiểm toán giai đoạn 2016 – 2020

Đánh giá thiết kế và triển khai

- Thu thập, rà soát các dự án đầu tư CNTT sử dụng nguồn vốn NSNN được phê duyệt giai đoạn 2016 – 2020 tại đơn vị, đảm bảo các dự án nằm trong danh mục các dự án được hỗ trợ theo quy định của nhà nước như sau:

- Về ngành/ lĩnh vực: cần thuộc vào một trong các lĩnh vực sau: Các dự án đầu tư hạ tầng ứng dụng công nghệ thông tin; bảo mật và an toàn thông tin điện tử trong cơ quan nhà nước; hạ tầng công nghệ thông tin cung cấp dịch vụ công trực tuyến phục vụ người dân và doanh nghiệp; hạ tầng thương mại điện tử, giao dịch điện tử.

- Về phạm vi hỗ trợ:

- Các Bộ có các dự án xây dựng cơ sở dữ liệu được Thủ tướng Chính phủ phê duyệt theo Quyết định số 714/QĐ-TTg ngày 22 tháng 5 năm 2015, trong đó ưu tiên các cơ sở dữ liệu quốc gia;

- Các địa phương có các dự án xây dựng khu công nghệ thông tin tập trung theo Quyết định số 2407/QĐ-TTg ngày 31 tháng 12 năm 2014 và Quyết định số 392/QĐ-TTg ngày 27 tháng 3 năm 2015 của Thủ tướng Chính phủ; có các dự án ứng dụng công nghệ thông tin trong quản lý, điều hành đảm bảo kết nối liên thông với các cơ quan Trung ương, kết nối liên thông vào hệ thống thông tin và cơ sở dữ liệu quốc gia theo quyết định của Thủ tướng Chính phủ, trong đó ưu tiên các địa phương khó khăn, chưa tự cân đối được ngân sách.

- Đối tượng hỗ trợ:
 - Các dự án hệ thống thông tin quốc gia, các cơ sở dữ liệu quốc gia, các cơ sở dữ liệu chuyên ngành và các hệ thống kết nối thông tin trực tuyến thuộc nền tảng Chính phủ điện tử.
 - Các dự án đầu tư xây dựng hạ tầng ứng dụng công nghệ thông tin tại địa phương đáp ứng yêu cầu khung về kiến trúc Chính phủ điện tử; đảm bảo tính bảo mật, an toàn thông tin và kết nối liên thông giữa các hệ thống thông tin của địa phương với các hệ thống thông tin, cơ sở dữ liệu quốc gia.
 - Các dự án hạ tầng và giải pháp công nghệ đảm bảo an toàn, an ninh mạng tập trung đối với các hệ thống thông tin, cơ sở dữ liệu và mạng máy tính của các cơ quan nhà nước.
 - Đầu tư hạ tầng cơ bản trong các Khu Công nghệ thông tin tập trung, phát triển các sản phẩm công nghiệp công nghệ thông tin trọng điểm, sản phẩm an toàn thông tin và các sản phẩm công nghệ thông tin phục vụ các hệ thống thông tin quốc gia theo mục tiêu cụ thể tại Quyết định số 392/QĐ-TTg ngày 27 tháng 3 năm 2015 của Thủ tướng Chính phủ.

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách các dự án đầu tư CNTT sử dụng nguồn vốn NSNN giai đoạn 2016 – 2020, Kiểm toán viên nhà nước tiến hành chọn mẫu và thực hiện các thủ tục như ở phần Đánh giá thiết kế và triển khai để bảo đảm tính hoạt động hữu hiệu của kiểm soát.

Kiểm soát B6.02.06: Chủ đầu tư dự án được chỉ định bởi Người có thẩm quyền quyết định đầu tư trước khi lập dự án.

Tiêu chí kiểm toán

Đảm bảo Chủ đầu tư dự án được chỉ định trước khi lập dự án bởi Người có thẩm quyền quyết định đầu tư theo quy định

Dẫn chứng quy định ban hành

Điều 7 NĐ102/2009/NĐ-CP

Tài liệu yêu cầu

Quyết định bổ nhiệm Chủ đầu tư

Đánh giá thiết kế và triển khai

- Thu thập và rà soát quyết định bổ nhiệm Chủ đầu tư, đảm bảo Chủ đầu tư được bổ nhiệm bởi Người có thẩm quyền quyết định đầu tư theo quy định:

- Đối với dự án ứng dụng công nghệ thông tin do Thủ tướng Chính phủ quyết định đầu tư thì Chủ đầu tư là một trong các cơ quan, tổ chức sau: Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, tổ chức chính trị, tổ chức chính trị xã hội, tổ chức xã hội, tổ chức xã hội nghề nghiệp (gọi chung là cơ quan cấp Bộ), Ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương (gọi chung là cấp tỉnh);

- Đối với dự án ứng dụng công nghệ thông tin do Bộ trưởng, Thủ trưởng cơ quan cấp Bộ, Chủ tịch Ủy ban nhân dân các cấp quyết định đầu tư thì Người quyết định đầu tư giao cho đơn vị quản lý, sử dụng sản phẩm của dự án làm Chủ đầu tư;

- Trường hợp đơn vị quản lý, sử dụng sản phẩm của dự án không đủ điều kiện về tổ chức, nhân lực, thời gian và các điều kiện cần thiết khác để thực hiện nhiệm vụ, quyền hạn của Chủ đầu tư hoặc chưa xác định được đơn vị quản lý, sử dụng sản phẩm của dự án thì Người có thẩm quyền quyết định đầu tư lựa chọn đơn vị có đủ điều kiện làm Chủ đầu tư.

- Đối với dự án ứng dụng công nghệ thông tin sử dụng vốn hỗn hợp thì Chủ đầu tư do các thành viên góp vốn thỏa thuận cử ra hoặc là đại diện của bên có tỷ lệ góp vốn cao nhất.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Vấn đề B6.03.00 - Lập, phê duyệt nhiệm vụ khảo sát

Kiểm soát B6.03.01: Việc khảo sát dự án được thực hiện bởi cá nhân có đủ bằng cấp, kinh nghiệm và chuyên môn phù hợp

Tiêu chí kiểm toán

Đảm bảo công tác khảo sát dự án được thực hiện bởi nhóm khảo sát có đủ năng lực

Dẫn chứng quy định ban hành

Điều 66 102/2009/NĐ-CP

Tài liệu yêu cầu

- Danh sách nhóm thực hiện khảo sát dự án

- Bằng cấp / văn bản liên quan tới kinh nghiệm, kiến thức chuyên môn của nhóm khảo sát dự án

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có ban hành văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt văn bản nào quy định về bằng cấp, kinh nghiệm và năng lực chuyên môn của các thành viên nhóm thực hiện khảo sát hay không

- Thu thập và rà soát danh sách các thành viên trong nhóm thực hiện khảo sát cũng như bằng cấp văn bản liên quan tới kinh nghiệm và kiến thức chuyên môn của các thành viên thực hiện khảo sát, đảm bảo các thành viên trong nhóm thực hiện khảo sát tuân theo quy định nội bộ ban hành (nếu có) và tuân theo điều 66 102/2009/NĐ-CP (trong trường hợp không có quy định ban hành nội bộ) như sau:

- Chủ trì khảo sát phải có trình độ đại học chuyên ngành công nghệ thông tin, đã được bồi dưỡng nghiệp vụ về quản lý, đầu tư ứng dụng công nghệ thông tin (bộ môn lập và quản lý dự án)

- Đối với dự án nhóm A, chủ trì khảo sát cần có kinh nghiệm tham gia ít nhất 2 nhiệm vụ khảo sát đối với dự án nhóm A, hoặc 3 nhiệm vụ khảo sát đối với dự án nhóm B, C

- Đối với dự án nhóm B, C, chủ trì khảo sát cần có kinh nghiệm tham gia ít nhất 2 nhiệm vụ khảo sát đối với dự án nhóm B, C.

- Trong trường hợp đơn vị thuê ngoài tổ chức tư vấn khảo sát, rà soát danh sách các thành viên tư vấn khảo sát, đảm bảo đáp ứng các yêu cầu sau:

- Có ít nhất 10 người trình độ đại học chuyên ngành công nghệ thông tin phù hợp với yêu cầu của nhiệm vụ khảo sát, trong đó có người có đủ điều kiện làm chủ trì khảo sát nhóm dự án phù hợp với yêu cầu của nhiệm vụ khảo sát.

- Có đủ thiết bị phù hợp với từng loại khảo sát.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Vấn đề B6.04.00- Thực hiện khảo sát, lập Báo cáo Khảo sát

Kiểm soát B6.04.01: Đơn vị thực hiện lập nhiệm vụ khảo sát và tổ chức thực hiện công tác khảo sát

Tiêu chí kiểm toán

Đảm bảo các dự án ứng dụng CNTT sử dụng nguồn vốn NSNN được khảo sát trước khi triển khai và khảo sát bổ sung

Dẫn chứng quy định ban hành

Điều 12, 13 – 102/2009/NĐ-CP

Tài liệu yêu cầu

- Báo cáo khảo sát trong giai đoạn chuẩn bị dự án
- Báo cáo khảo sát bổ sung trong giai đoạn thực hiện dự án (nếu có)

Đánh giá thiết kế và triển khai

▪ Phòng văn lãnh đạo đơn vị, chủ đầu tư dự án và xác minh xem đơn vị có thực hiện lập nhiệm vụ khảo sát và tổ chức thực hiện công tác khảo sát trước khi triển khai dự án hay không.

▪ Thu thập, rà soát báo cáo kết quả khảo sát của dự án, đảm bảo báo cáo kết quả khảo sát dự án bao gồm đầy đủ các nội dung sau:

▪ Nhiệm vụ khảo sát: Nhiệm vụ khảo sát cần được đưa ra trước khi tiến hành khảo sát, nhiệm vụ khảo sát bao gồm:

- i) Mục đích khảo sát
- ii) Phạm vi khảo sát
- iii) Các loại công tác khảo sát dự kiến
- iv) Tiêu chuẩn, kỹ thuật khảo sát dự kiến áp dụng
- v) Thời gian thực hiện khảo sát dự kiến

▪ Đặc điểm, quy mô đầu tư;

▪ Vị trí và hiện trạng mặt bằng của khu vực được khảo sát (đối với lắp đặt thiết bị và phụ kiện liên quan);

▪ Mô tả yêu cầu người sử dụng (đối với phần mềm nội bộ);

▪ Tiêu chuẩn kỹ thuật khảo sát được áp dụng;

▪ Khối lượng công tác khảo sát thực tế;

▪ Quy trình, phương pháp và thiết bị (nếu có) dùng cho khảo sát;

- Đánh giá về độ tin cậy của kết quả khảo sát thu được;
 - Đề xuất giải pháp kỹ thuật công nghệ (nếu có) phục vụ cho việc thiết kế sơ bộ, hoặc thiết kế thi công (trong trường hợp khảo sát bổ sung);
 - Kết luận và kiến nghị (nếu có);
 - Nhật ký khảo sát;
 - Các phụ lục có liên quan để minh họa cho kết quả khảo sát thu được (nếu có).
- Rà soát Báo cáo kết quả khảo sát trong giai đoạn chuẩn bị đầu tư, đảm bảo báo cáo đã được chủ đầu tư kiểm tra, nghiệm thu và là cơ sở cho triển khai lập thiết kế sơ bộ của dự án.
- Phòng vận ban chỉ đạo dự án và xác minh xem đơn vị có tiến hành khảo sát bổ sung trong giai đoạn thực hiện dự án hay không
- Thu thập và rà soát các báo cáo khảo sát bổ sung, đảm bảo các báo cáo khảo sát bổ sung được Chủ đầu tư kiểm tra, nghiệm thu và là cơ sở cho triển khai lập, hoặc thay đổi, bổ sung thiết kế thi công, hoặc thiết kế sơ bộ của dự án.

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cân nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B6.04.02: Tổ chức tư vấn khảo sát có đủ bằng cấp chuyên môn phù hợp

Tiêu chí kiểm toán

Đảm bảo tổ chức tư vấn khảo sát cho đơn vị đáp ứng đầy đủ các quy định theo luật định.

Dẫn chứng quy định ban hành

Điều 66 102/2009/NĐ-CP

Tài liệu yêu cầu

- Đơn vị tổ chức tư vấn khảo sát
- Thông tin tổ chức tư vấn khảo sát
- Biên bản nghiệm thu kết quả khảo sát.

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có ban hành văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định về năng lực của tổ chức tư vấn khảo sát hay không
- Thu thập, rà soát thông tin về tổ chức tư vấn khảo sát cho đơn vị và xác định đơn vị có thực hiện tuân theo quy định nội bộ ban hành (nếu có) và tuân theo điều 66 102/2009/NĐ-CP (trong trường hợp không có quy định ban hành nội bộ) đảm bảo tổ chức tư vấn khảo sát đáp ứng các yêu cầu sau:
 - Có ít nhất 10 người trình độ đại học chuyên ngành công nghệ thông tin phù hợp với yêu cầu của nhiệm vụ khảo sát, trong đó có người có đủ điều kiện làm chủ trì khảo sát nhóm dự án phù hợp với yêu cầu của nhiệm vụ khảo sát.
 - Có đủ thiết bị phù hợp với từng loại khảo sát.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Vấn đề B6.05.00- Lập dự án đầu tư, trình thẩm định, phê duyệt

Kiểm soát B6.05.01: Đơn vị có lập Dự án khả thi ứng dụng CNTT/ Báo cáo nghiên cứu tính khả thi theo quy định

Tiêu chí kiểm toán

Đảm bảo đơn vị tiến hành đánh giá tính khả thi của dự án trước khi triển khai dự án

Dẫn chứng quy định ban hành

Điều 16 102/2009/NĐ-CP

Tài liệu yêu cầu

Dự án khả thi ứng dụng công nghệ thông tin/ Báo cáo tính khả thi của dự án

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có tiến hành đánh giá tính khả thi của dự án trước khi triển khai dự án hay không
- Thu thập và rà soát Dự án khả thi ứng dụng CNTT (đối với dự án nhóm A) hoặc báo cáo nghiên cứu tính khả thi (đối với dự án nhóm B, C), và xác minh các vấn đề sau:
 - Đảm bảo Chủ đầu tư tổ chức lập Dự án khả thi ứng dụng CNTT cho các dự án quan trọng quốc gia và dự án nhóm A.

- Đảm bảo Chủ đầu tư tổ chức lập Báo cáo nghiên cứu tính khả thi cho dự án nhóm B và các dự án nhóm C có số vốn đầu tư > 3 tỉ đồng.
- Đảm bảo chủ đầu tư thực hiện lập Báo cáo đầu tư cho các dự án nhóm C < 3 tỉ đồng. Tuy nhiên, trường hợp khi lập đề cương và dự toán chi tiết, tổng dự toán dưới 03 tỷ đồng nhưng trong quá trình thực hiện phải điều chỉnh dẫn tới thay đổi tổng dự toán thành từ 03 tỷ đồng trở lên phải thực hiện lại các thủ tục đầu tư theo quy định.
- Đảm bảo thời gian lập dự án đối với dự án nhóm B không quá 5 tháng, dự án nhóm C không quá 3 tháng.
- Thời gian thực hiện dự án không quá 2 năm đối với dự án nhóm C, không quá 4 năm đối với dự án nhóm B

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách các dự án Kiểm toán viên nhà nước tiến hành chọn mẫu và thực hiện các thủ tục như ở phần Đánh giá thiết kế và triển khai để bảo đảm tính hoạt động hữu hiệu của kiểm soát.

Kiểm soát B6.05.02: Nội dung Dự án khả thi ứng dụng CNTT/ Báo cáo nghiên cứu tính khả thi bao gồm đầy đủ các khoản mục theo quy định

Tiêu chí kiểm toán

Đảm bảo đơn vị tiến hành đánh giá tính khả thi của dự án trước khi triển khai dự án

Dẫn chứng quy định ban hành

Điều 17, 19 102/2009/NĐ-CP

Tài liệu yêu cầu

Dự án khả thi ứng dụng công nghệ thông tin/ Báo cáo tính khả thi của dự án

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem các nội dung trong dự án khả thi ứng dụng CNTT/báo cáo nghiên cứu khả thi.
- Thu thập và rà soát Dự án khả thi ứng dụng CNTT (đối với dự án nhóm A) hoặc báo cáo nghiên cứu tính khả thi (đối với dự án nhóm B, C), đảm bảo nội dung Dự án khả thi ứng dụng CNTT, hoặc báo cáo tính khả thi bao gồm đầy đủ các hạng mục sau:

- -Dự án khả thi ứng dụng CNTT cho các dự án quốc gia hoặc dự án nhóm A phục vụ cho mục đích mua sắm thiết bị không cần lắp đặt, cần có các nội dung sau:
 - Sự cần thiết phải đầu tư, các điều kiện thuận lợi và khó khăn.
 - Xác định Chủ đầu tư, hình thức đầu tư.
 - Phân tích, lựa chọn sơ bộ về công nghệ, kỹ thuật; thiết kế sơ bộ của phương án chọn; điều kiện cung cấp vật tư thiết bị, dịch vụ, hạ tầng kỹ thuật, phòng chống cháy nổ và an toàn vận hành, bảo đảm an ninh, quốc phòng.
 - Xác định sơ bộ tổng mức đầu tư, loại nguồn vốn, thời hạn thực hiện dự án, hiệu quả kinh tế xã hội của dự án và phân kỳ đầu tư (nếu có), phương án hoàn trả vốn đầu tư (đối với dự án có yêu cầu thu hồi vốn đầu tư).
 - Các mốc thời gian chính thực hiện đầu tư.
 - Kiến nghị áp dụng hình thức quản lý dự án.
- Đối với các dự án quốc gia hoặc dự án nhóm A khác, ngoài các nội dung trên cần có thêm các nội dung sau:
 - Dự kiến quy mô đầu tư: các yếu tố công nghệ, kỹ thuật phải đáp ứng; dự kiến về địa điểm đầu tư (bao gồm cả tài liệu về sự lựa chọn địa điểm).
 - Quy mô lắp đặt, cài đặt thiết bị.
 - Xác định tính độc lập khi vận hành, khai thác của các hạng mục đầu tư hoặc tiểu dự án thành phần (nếu có).
- Báo cáo nghiên cứu tính khả thi cho các dự án nhóm B, hoặc các dự án nhóm C có số vốn đầu tư > 3 tỉ phục vụ cho mục đích mua sắm thiết bị không cần lắp đặt, cần có các nội dung sau:
 - a) Sự cần thiết và mục tiêu đầu tư;
 - b) Lựa chọn hình thức đầu tư và xác định Chủ đầu tư;
 - d) Quy mô lắp đặt, cài đặt thiết bị;
 - e) Thiết kế sơ bộ của phương án chọn;
 - g) Điều kiện cung cấp vật tư thiết bị, dịch vụ, hạ tầng kỹ thuật, phòng chống cháy nổ và an toàn vận hành, bảo đảm an ninh, quốc phòng;
 - h) Loại nguồn vốn, khả năng tài chính, tổng mức đầu tư và nhu cầu vốn theo tiến độ. Phương án hoàn trả vốn đầu tư (đối với dự án có yêu cầu thu hồi vốn đầu tư). Chi phí quản lý dự án cho toàn bộ quá trình thực hiện;

- i) Phân tích hiệu quả đầu tư;
 - k) Các mốc thời gian chính thực hiện đầu tư;
 - l) Kiến nghị áp dụng hình thức quản lý dự án;
 - m) Mỗi quan hệ và trách nhiệm của các cơ quan liên quan đến dự án.
- Báo cáo tính khả thi cho dự án khác thuộc nhóm B, hoặc nhóm C có số vốn đầu tư >3 tỉ đồng, ngoài các nội dung trên cần có các nội dung sau
- Dự kiến quy mô đầu tư: các yêu cầu kỹ thuật đối với các hạng mục đầu tư chính và phụ; dự kiến về địa điểm đầu tư (bao gồm cả tài liệu về sự lựa chọn địa điểm);
 - Phân tích lựa chọn phương án kỹ thuật, công nghệ;

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách các dự án Kiểm toán viên nhà nước tiến hành chọn mẫu và thực hiện các thủ tục như ở phần Đánh giá thiết kế và triển khai để bảo đảm tính hoạt động hữu hiệu của kiểm soát.

Kiểm soát B6.05.03: Thành viên tiến hành thiết kế sơ bộ có đủ bằng cấp, kinh nghiệm chuyên môn phù hợp

Tiêu chí kiểm toán

Đảm bảo quá trình thiết kế sơ bộ được thực hiện, chủ trì bởi các thành viên có đầy đủ bằng cấp, kiến thức và kinh nghiệm phù hợp

Dẫn chứng quy định ban hành

Chương 6 102/2009/NĐ-CP

Tài liệu yêu cầu

- Danh sách nhóm thiết kế sơ bộ
- Bằng cấp / văn bản liên quan tới việc đánh giá kinh nghiệm, kiến thức chuyên môn của nhóm thiết kế sơ bộ

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có ban hành văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định về bằng cấp, kinh nghiệm và năng lực chuyên môn của các thành viên nhóm thiết kế sơ bộ hay không.
- Thu thập và rà soát danh sách các thành viên trong nhóm thiết kế sơ bộ cũng như bằng cấp văn bản liên quan tới kinh nghiệm và kiến thức chuyên môn của các thành

viên thuộc nhóm thiết kế sơ bộ, và đảm bảo trình tự và thủ tục quyết định được thực hiện tuân theo quy định nội bộ ban hành (nếu có) và tuân theo 102/2009/NĐ-CP (trong trường hợp không có quy định ban hành nội bộ) đảm bảo các yêu cầu sau:

- Phải có trình độ đại học chuyên ngành CNTT, đã được bồi dưỡng nghiệp vụ lập, quản lý đầu tư ứng dụng công nghệ thông tin (bộ môn lập và quản lý dự án)
- Đối với dự án ứng dụng công nghệ thông tin quan trọng cấp quốc gia, dự án nhóm A, B, C thì Chủ trì thiết kế sơ bộ cần có thời gian liên tục làm công tác lập dự án ứng dụng CNTT tối thiểu 7 năm, đã từng tham gia lập tối thiểu 5 thiết kế sơ bộ của dự án ứng dụng CNTT nhóm A, B, C hoặc đã là Chủ trì thiết kế sơ bộ đối với dự án có quy mô đầu tư tương tự.
- Đối với các dự án nhóm C, chủ trì thiết kế sơ bộ cần có thời gian liên tục làm công tác lập dự án ứng dụng CNTT tối thiểu 5 năm, đã từng tham gia lập tối thiểu 3 Báo cáo đầu tư hoặc 2 Báo cáo nghiên cứu khả thi dự án ứng dụng CNTT nhóm C.
- Riêng đối với các dự án ở vùng sâu, vùng xa, chủ trì thiết kế sơ bộ dự án chỉ lập báo cáo đầu tư thì chủ trì thiết kế sơ bộ cần có bằng cao đẳng, trung cấp chuyên ngành CNTT, Có thời gian liên tục làm công tác lập dự án ứng dụng CNTT tối thiểu 3 năm, và đã tham gia lập ít nhất 1 Báo cáo đầu tư dự án ứng dụng CNTT nhóm C.
- Đối với cá nhân chưa đủ điều kiện để phân cấp độ thì không được làm chủ trì thiết kế sơ bộ nhưng được tham gia lập thiết kế sơ bộ

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B6.05.04: Tổ chức tư vấn lập dự án có đủ bằng cấp chuyên môn phù hợp

Tiêu chí kiểm toán

Đảm bảo tổ chức tư vấn lập dự án cho đơn vị đáp ứng đầy đủ các quy định theo luật định.

Dẫn chứng quy định ban hành

Điều 62 102/2009/NĐ-CP

Tài liệu yêu cầu

- Văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định về năng lực của tổ chức tư vấn lập dự án

- Đơn vị tổ chức tư vấn lập dự án
- Bản đánh giá đơn vị tổ chức tư vấn lập dự án

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có ban hành văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định về năng lực của tổ chức tư vấn lập dự án hay không

- Thu thập, rà soát danh sách bản đánh giá đơn vị tổ chức tư vấn lập dự án và đảm bảo tổ chức tư vấn lập dự án tuân theo quy định nội bộ ban hành (nếu có) và tuân theo điều 62 -102/2009/NĐ-CP (trong trường hợp không có quy định ban hành nội bộ) như sau:

- Đối với dự án nhóm C, đơn vị tổ chức tư vấn lập dự án cần có ít nhất 7 người trình độ: đại học chuyên ngành công nghệ thông tin, đại học chuyên ngành kinh tế, tài chính phù hợp với yêu cầu của dự án; trong đó có người có đủ điều kiện làm Chủ trì thiết kế sơ bộ Cấp độ 2
- Đối với các dự án quan trọng quốc gia, nhóm A, B, C tổ chức tư vấn lập dự án cần có ít nhất 10 người trình độ: đại học chuyên ngành công nghệ thông tin, đại học chuyên ngành kinh tế, tài chính phù hợp với yêu cầu của dự án; trong đó có người có đủ điều kiện làm Chủ trì thiết kế sơ bộ Cấp độ 1
- Đối với tổ chức chưa đủ điều kiện để phân cấp độ thì phải liên kết, liên danh với tổ chức tư vấn có đủ năng lực để lập dự án.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B6.05.05: Đơn vị đầu mối tổ chức thẩm định dự án là đơn vị chuyên môn phân cấp theo đúng quy định

Tiêu chí kiểm toán

Đảm bảo đơn vị thẩm định dự án được phân cấp theo đúng quy định

Dẫn chứng quy định ban hành

Điều 26 NĐ102/2009/NĐ-CP

Tài liệu yêu cầu

Quy định về thẩm định dự án

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có quy định nào liên quan tới việc phải thực hiện thẩm định dự án trước khi phê duyệt hay không.
- Thu thập các tài liệu liên quan xác minh xem đơn vị chuyên trách thẩm định dự án đáp ứng yêu cầu như sau:
 - Đối với các cơ quan cấp Bộ, được phép tổ chức thẩm định dự án do mình quyết định đầu tư. Đầu mỗi tổ chức thẩm định dự án là đơn vị chuyên môn trực thuộc Người có thẩm quyền quyết định đầu tư theo phân cấp ủy quyền;
 - Đối với Ủy ban nhân dân cấp tỉnh, được phép tổ chức thẩm định dự án do mình quyết định đầu tư. Đầu mỗi tổ chức thẩm định dự án là đơn vị chuyên môn giúp việc theo phân cấp ủy quyền;
 - Đối với Ủy ban nhân dân cấp huyện, được phép tổ chức thẩm định dự án do mình quyết định đầu tư. Đầu mỗi thẩm định dự án là đơn vị có chức năng quản lý kế hoạch ngân sách trực thuộc Người có thẩm quyền quyết định đầu tư;
 - Đối với Ủy ban nhân dân cấp xã, chỉ được tổ chức thẩm định dự án do mình quyết định đầu tư theo thẩm quyền được Ủy ban nhân dân cấp tỉnh giao. Đầu mỗi thẩm định dự án là đơn vị có chức năng quản lý kế hoạch ngân sách.
- Đơn vị đầu mỗi thẩm định dự án không đồng thời làm Chủ đầu tư dự án mà mình được giao thẩm định.
- Trường hợp cần thiết đơn vị đầu mỗi thẩm định dự án có thể thuê các tổ chức, cá nhân có đủ điều kiện năng lực, kinh nghiệm để tư vấn thẩm định dự án.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B6.05.06: Đơn vị đầu mỗi tổ chức thẩm định thiết kế sơ bộ được phân cấp theo đúng quy định

Tiêu chí kiểm toán

Đảm bảo đơn vị đầu mỗi tổ chức thẩm định thiết kế sơ bộ được phân cấp theo đúng thẩm quyền

Dẫn chứng quy định ban hành

Điều 26 NĐ102/2009/NĐ-CP

Tài liệu yêu cầu

- Đơn vị thẩm định thiết kế sơ bộ
- Quy định về đơn vị được thực hiện thẩm định thiết kế sơ bộ

Đánh giá thiết kế và triển khai

▪ Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có ban hành văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định bộ phận chuyên trách thẩm định thiết kế sơ bộ hay không

▪ -Thu thập, rà soát thông tin đơn vị thẩm định thiết kế sơ bộ đảm bảo trình tự và thủ tục quyết định được thực hiện tuân theo quy định nội bộ ban hành (nếu có) và tuân theo điều 26 NĐ102/2009/NĐ-CP như sau:

▪ Thẩm quyền thẩm định thiết kế sơ bộ cho các dự án thuộc Chương trình Quốc gia về ứng dụng CNTT trong hoạt động của cơ quan nhà nước giai đoạn 2011 – 2015 là của Bộ Thông tin và Truyền thông. (Theo QĐ 1605/QĐ-TTg ngày 27/8/2010)

▪ Thẩm quyền thẩm định các dự án quan trọng quốc gia và các dự án nhóm A là của Bộ Thông tin và Truyền thông

▪ Đối với dự án do Ủy ban nhân dân cấp tỉnh, cấp huyện, cấp xã quyết định đầu tư, Sở Thông tin và Truyền thông thẩm định thiết kế sơ bộ;

▪ Đối với dự án do cơ quan cấp Bộ, các Tập đoàn kinh tế nhà nước, Tổng công ty nhà nước, công ty nhà nước độc lập quyết định đầu tư, đơn vị chuyên môn về công nghệ thông tin trực thuộc Người quyết định đầu tư thẩm định thiết kế sơ bộ;

▪ Trường hợp cần thiết, đơn vị thẩm định thiết kế sơ bộ có thể thuê các tổ chức, cá nhân có đủ điều kiện năng lực, kinh nghiệm để tư vấn thẩm định.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B6.05.07: Chi phí thẩm định dự án/ Chi phí thuê tư vấn thẩm định được tính vào chi phí khác trong tổng mức đầu tư

Tiêu chí kiểm toán

Đảm bảo chi phí thẩm định dự án/ chi phí thuê tư vấn thẩm định được phản ánh đúng trong tổng mức đầu tư

Dẫn chứng quy định ban hành

- Điều 26 NĐ102/2009/NĐ-CP
- Điều 7 TT06/2011/TT-BTTTT
- Điều 4 TT 209/2016/ TT-BTC

Tài liệu yêu cầu

- Đơn vị thẩm định dự án
- Chi phí thẩm định dự án

Đánh giá thiết kế và triển khai

▪ Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có quy định nào liên quan tới chi phí thẩm định dự án (bao gồm chi phí thẩm định dự án do đơn vị thực hiện/ chi phí thuê tư vấn thẩm định) hay không.

▪ Thu thập thông tin về tổng mức đầu tư, rà soát và xác minh xem chi phí thẩm định dự án/ chi phí thuê tư vấn thẩm định được ghi nhận trong khoản mục nào trong tổng đầu tư, đảm bảo chi phí thuê tư vấn thẩm định được trích từ lệ phí thẩm định dự án, thuộc vào chi phí khác trong tổng mức đầu tư.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B6.05.08: Thời gian thẩm định dự án được hoàn thành theo đúng quy định

Tiêu chí kiểm toán

Đảm bảo đơn vị thực hiện thẩm định dự án hoàn thành quy trình thẩm định trong khung thời gian được quy định

Dẫn chứng quy định ban hành

Điều 26 NĐ102/2009/NĐ-CP

Tài liệu yêu cầu

Hồ sơ thẩm định dự án

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có văn bản nào quy định về thời gian thẩm định dự án cho đơn vị tổ chức thẩm định dự án hay không.
- Thu thập, rà soát hồ sơ thẩm định dự án, đảm bảo thời gian thẩm định dự án ở trong mức cho phép như sau:
 - Đối với dự án nhóm A, thời gian thẩm định dự án (kể cả thời gian thẩm định thiết kế sơ bộ) không quá 60 ngày làm việc kể từ ngày nhận đủ hồ sơ hợp lệ.
 - Thời gian thẩm định sơ bộ (kể cả thời gian thẩm định thiết kế sơ bộ) là không quá 30 ngày với dự án nhóm B kể từ ngày nhận đủ hồ sơ hợp lệ.
 - Thời gian thẩm định dự án (kể cả thời gian thẩm định thiết kế sơ bộ) là không quá 20 ngày với dự án nhóm C kể từ ngày nhận đủ hồ sơ hợp lệ.
- Trường hợp đặc biệt, thời gian thẩm định dự án có thể dài hơn nhưng phải được người có thẩm quyền quyết định đầu tư cho phép.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B6.05.09: Thời gian thẩm định thiết kế sơ bộ được hoàn thành theo đúng quy định

Tiêu chí kiểm toán

Đảm bảo đơn vị thực hiện thẩm định thiết kế sơ bộ hoàn thành quy trình thẩm định trong khung thời gian được quy định

Dẫn chứng quy định ban hành

Điều 26 NĐ102/2009/NĐ-CP

Tài liệu yêu cầu

Hồ sơ thẩm định thiết kế sơ bộ

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có văn bản nào quy định về thời gian thẩm định thiết kế sơ bộ cho đơn vị tổ chức thẩm định thiết kế sơ bộ hay không.
- Thu thập, rà soát hồ sơ thẩm định thiết kế sơ bộ, đảm bảo thời gian thẩm định thiết kế sơ bộ ở trong mức cho phép như sau:
 - Đối với dự án nhóm A, thời gian thẩm định thiết kế sơ bộ không quá 30 ngày làm việc kể từ ngày nhận đủ hồ sơ hợp lệ.

- Thời gian thẩm định thiết kế sơ bộ là không quá 15 ngày với dự án nhóm B kể từ ngày nhận đủ hồ sơ hợp lệ.
- Thời gian thẩm định thiết kế sơ bộ là không quá 10 ngày với dự án nhóm C kể từ ngày nhận đủ hồ sơ hợp lệ.
- Trường hợp đặc biệt, thời gian thẩm định có thể dài hơn nhưng phải được Người có thẩm quyền quyết định đầu tư cho phép.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B6.05.10: Dự án được quyết định đầu tư theo đúng thẩm quyền quy định

Tiêu chí kiểm toán

Đảm bảo dự án được quyết định đầu tư theo đúng thẩm quyền quy định

Dẫn chứng quy định ban hành

Điều 6 ND102/2009/NĐ-CP

Tài liệu yêu cầu

Quyết định đầu tư dự án ứng dụng CNTT

Đánh giá thiết kế và triển khai

Thu thập và rà soát quyết định đầu tư dự án ứng dụng CNTT, đảm bảo quyết định đầu tư dự án ứng dụng CNTT được thực hiện bởi các bên có thẩm quyền như sau:

- Các dự án ứng dụng công nghệ thông tin quan trọng quốc gia đã được Quốc hội thông qua chủ trương và cho phép đầu tư phải được quyết định đầu tư bởi Thủ tướng Chính phủ
- Bộ trưởng, Thủ trưởng cơ quan ngang Bộ, cơ quan thuộc Chính phủ, cơ quan quản lý tài chính của Trung ương Đảng, cơ quan Trung ương của tổ chức chính trị xã hội, các tổ chức chính trị, tổ chức xã hội, tổ chức xã hội nghề nghiệp, Tổng công ty nhà nước, Tập đoàn kinh tế nhà nước, công ty nhà nước độc lập (được xác định trong Luật Ngân sách nhà nước), Chủ tịch ủy ban nhân dân cấp tỉnh quyết định đầu tư các dự án ứng dụng công nghệ thông tin các nhóm A, B, C đã có trong kế hoạch ứng dụng công nghệ thông tin được duyệt hoặc đã có quyết định chủ trương đầu tư.
- Trường hợp dự án nhóm A chưa nằm trong kế hoạch ứng dụng công nghệ thông tin được duyệt, hoặc chưa có quyết định chủ trương đầu tư thì trước khi lập dự án phải

được Thủ tướng Chính phủ xem xét, đồng ý về chủ trương đầu tư. Việc xem xét chủ trương đầu tư được thực hiện theo quy chế làm việc của Chính phủ.

- Đối với các dự án nhóm B, C chưa nằm trong kế hoạch ứng dụng công nghệ thông tin được duyệt thì trước khi lập dự án phải có quyết định chủ trương đầu tư của Người có thẩm quyền quyết định đầu tư.

- Đối với doanh nghiệp nhà nước do Thủ tướng Chính phủ quyết định thành lập (Tổng công ty nhà nước, Tập đoàn kinh tế nhà nước), Hội đồng quản trị Tổng công ty, Tập đoàn kinh tế có thể ủy quyền cho giám đốc các đơn vị thành viên quyết định đầu tư các dự án ứng dụng công nghệ thông tin nhóm C.

- Tùy theo điều kiện cụ thể của từng Bộ, ngành, địa phương, Người có thẩm quyền quyết định đầu tư được phép ủy quyền cho các đối tượng quy định tại khoản 5 Điều này quyết định đầu tư các dự án ứng dụng công nghệ thông tin nhóm B, C. Người ủy quyền phải chịu trách nhiệm trước pháp luật về sự ủy quyền của mình. Người được ủy quyền phải chịu trách nhiệm về quyết định của mình trước pháp luật và người ủy quyền.

- Đối tượng được ủy quyền quyết định đầu tư:

- i) Đối với cấp Bộ:

- Tổng cục trưởng, Cục trưởng, Chủ tịch Hội đồng quản trị Tổng công ty nhà nước, Tập đoàn kinh tế nhà nước, Giám đốc doanh nghiệp nhà nước trực thuộc, Thủ trưởng cơ quan, đơn vị trực thuộc Bộ;

- ii) Đối với cấp tỉnh:

- Giám đốc Sở, Chủ tịch ủy ban nhân dân quận, huyện, thị xã, thành phố thuộc cấp tỉnh (sau đây gọi là cấp huyện), Chủ tịch Hội đồng quản trị Tổng công ty nhà nước, Giám đốc doanh nghiệp nhà nước trực thuộc, Thủ trưởng cơ quan trực thuộc ủy ban nhân dân cấp tỉnh;

- Chủ tịch ủy ban nhân dân cấp huyện, cấp xã được quyết định đầu tư các dự án trong phạm vi ngân sách của địa phương mình (bao gồm cả các khoản bổ sung từ ngân sách cấp trên) có mức vốn đầu tư đến 05 tỷ đồng (đối với cấp huyện) và đến 03 tỷ đồng (đối với cấp xã) tùy theo điều kiện cụ thể của từng địa phương do ủy ban nhân dân cấp tỉnh quy định cụ thể trên cơ sở kế hoạch ứng dụng công nghệ thông tin được

duyet của địa phương và năng lực thực hiện của các đối tượng được phân cấp.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B6.05.11: Tổng mức đầu tư/ tổng dự toán bao gồm các khoản mục theo quy định

Tiêu chí kiểm toán

Đảm bảo tổng mức đầu tư/ tổng dự toán bao gồm các khoản mục theo quy định

Dẫn chứng quy định ban hành

Điều 6 -21/2010/TT-BTTTT

Tài liệu yêu cầu

- Tổng mức đầu tư dự án
- Tổng dự toán của dự án

Đánh giá thiết kế và triển khai

Thu thập các tài liệu xác định tổng dự toán của đơn vị, đảm bảo tổng dự toán bao gồm các khoản mục sau (không bao gồm các khoản mục không phát sinh):

- Chi phí xây lắp: Chi phí lắp đặt phụ kiện mạng, đi dây cho mạng công nghệ thông tin và các chi phí khác phục vụ cho lắp đặt mạng và các chi phí xây lắp trực tiếp khác có liên quan;

- Chi phí thiết bị:

- Chi phí mua sắm thiết bị công nghệ thông tin: Thiết bị phải lắp đặt và cài đặt, thiết bị không phải lắp đặt và cài đặt, thiết bị đặc biệt là phần mềm nội bộ, các thiết bị phụ trợ và thiết bị ngoại vi;

- Chi phí mua sắm tài sản vô hình: Phần mềm thương mại, tạo lập cơ sở dữ liệu ban đầu, chuẩn hoá phục vụ cho nhập dữ liệu, mua sắm các tài sản vô hình khác;

- Chi phí đào tạo chuyển giao công nghệ;

- Chi phí lắp đặt thiết bị, cài đặt phần mềm, kiểm tra và hiệu chỉnh thiết bị và phần mềm;

- Chi phí quản lý: Gồm các chi phí cần thiết để cơ quan, đơn vị tổ chức quản lý thực hiện;

- Chi phí tư vấn: Gồm các chi phí tư vấn triển khai và thực hiện các công việc tư vấn khác có liên quan;
- Chi phí khác có liên quan: Phí và lệ phí; bảo hiểm, di chuyển thiết bị và lực lượng lao động; kiểm toán; thẩm tra, phê duyệt quyết toán; nghiên cứu khoa học công nghệ liên quan; lắp đặt và thuê đường truyền; lệ phí đăng ký và duy trì tên miền; và các chi phí đặc thù khác;
- Chi phí dự phòng: Cho khối lượng công việc phát sinh chưa lường trước được khi lập đề cương và dự toán chi tiết. Chi phí dự phòng không vượt quá 10% tổng dự toán các chi phí nêu trên

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Vấn đề B6.06.00- Thành lập Ban QLDA

Kiểm soát B6.05.01 Thành viên ban quản lý dự án đầu tư ứng dụng CNTT có đủ bằng cấp chuyên môn phù hợp

Tiêu chí kiểm toán

Đảm bảo các thành viên của tổ dự án có đủ bằng cấp, kiến thức, kinh nghiệm và kỹ năng phù hợp, góp phần xây dựng kế hoạch dự án một cách hiệu quả

Dẫn chứng quy định ban hành

Điều 63 -102/2009/NĐ-CP

Tài liệu yêu cầu

- Văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định về bằng cấp, kinh nghiệm và năng lực chuyên môn của các thành viên ban quản lý dự án
- Danh sách ban quản lý dự án
- Bằng cấp / văn bản liên quan tới kinh nghiệm, kiến thức chuyên môn của thành viên quản lý dự án

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có ban hành văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định về bằng cấp, kinh nghiệm và năng lực chuyên môn của các thành viên ban quản lý dự án hay không.
- Thu thập, rà soát danh sách các thành viên trong ban quản lý dự án cũng như bằng cấp văn bản liên quan tới kinh nghiệm và kiến thức chuyên môn của các thành viên

bản quản lý dự án đảm bảo tuân theo quy định nội bộ ban hành (nếu có) và tuân theo điều 63 -102/2009/NĐ-CP (trong trường hợp không có quy định ban hành nội bộ) các thành viên trong ban quản lý đáp ứng được các yêu cầu sau:

- Giám đốc, các phó giám đốc và những người phụ trách về công nghệ thông tin, kinh tế, tài chính phải có trình độ đại học thuộc chuyên ngành phù hợp với lĩnh vực phụ trách. Được bồi dưỡng nghiệp vụ về quản lý, đầu tư ứng dụng công nghệ thông tin (bộ môn lập và quản lý dự án).
- Riêng đối với các dự án nhóm C ở vùng sâu, vùng xa thì các chức danh nêu trên có thể giao cho những người có trình độ cao đẳng hoặc trung cấp thuộc các chuyên ngành phù hợp.
- Các cá nhân đảm nhận trách nhiệm Giám đốc dự án, Trưởng dự án, Giám sát dự án không được đồng thời đảm nhận quá một công việc theo chức danh trong cùng một thời gian. Cá nhân đảm nhận các chức danh theo quy định phải ký hợp đồng với một tổ chức theo quy định của pháp luật. Thời hạn hợp đồng phải đảm bảo đủ dài để cá nhân đó có thời gian thực hiện hoàn tất nhiệm vụ được giao theo chức danh mình đảm nhận.
- Các thành viên ban quản lý dự án cần có kinh nghiệm làm việc chuyên môn tối thiểu 3 năm.

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách các thành viên ban quản lý dự án, Kiểm toán viên nhà nước tiến hành chọn mẫu và thực hiện các thủ tục như phần Đánh giá thiết kế và triển khai để đảm bảo tính hoạt động hiệu quả của kiểm soát

Kiểm soát B6.05.02 Tổ chức tư vấn quản lý dự án có đủ bằng cấp chuyên môn phù hợp

Tiêu chí kiểm toán

Đảm bảo tổ chức tư vấn quản lý dự án cho đơn vị đáp ứng đầy đủ các quy định theo luật định.

Dẫn chứng quy định ban hành

Điều 64 102/2009/NĐ-CP

Tài liệu yêu cầu

- Văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định về năng lực của tổ chức tư vấn quản lý dự án

- Tổ chức tư vấn quản lý dự án
- Bản đánh giá đơn vị tổ chức tư vấn quản lý dự án

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có ban hành văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định về năng lực của tổ chức tư vấn quản lý dự án hay không

- Thu thập, rà soát danh sách bản đánh giá đơn vị tổ chức tư vấn lập dự án và đảm bảo tổ chức tư vấn quản lý dự án tuân theo quy định nội bộ ban hành (nếu có) và tuân theo điều 64 -102/2009/NĐ-CP (trong trường hợp không có quy định ban hành nội bộ) như sau:

- Đối với dự án nhóm C, đơn vị tổ chức tư vấn quản lý dự án cần có giám đốc tư vấn quản lý dự án Cấp độ 2 đồng thời có ít nhất 7 người trình độ: đại học chuyên ngành CNTT, đại học chuyên ngành kinh tế, tài chính phù hợp với yêu cầu của dự án; trong đó có người có đủ điều kiện làm chủ trì khảo sát; chủ trì thiết kế thi công, chỉ huy thi công xây lắp tại hiện trường và có năng lực giám sát thi công cấp độ 2

- Đối với các dự án quan trọng quốc gia, nhóm A, B, C tổ chức tư vấn quản lý dự án cần có Giám đốc tư vấn quản lý dự án Cấp độ 1 đồng thời có ít nhất 10 người trình độ: đại học chuyên ngành công nghệ thông tin, đại học chuyên ngành kinh tế, tài chính phù hợp với yêu cầu của dự án; trong đó có người có đủ điều kiện làm chủ trì khảo sát; chủ trì thiết kế thi công, chỉ huy thi công xây lắp tại hiện trường và có năng lực giám sát thi công cấp độ 1

- Đối với tổ chức chưa đủ điều kiện để phân cấp độ thì phải liên kết, liên danh với tổ chức tư vấn có đủ năng lực để thực hiện tư vấn quản lý dự án.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B6.05.03 Giám đốc dự án có đủ bằng cấp, năng lực chuyên môn phù hợp

Tiêu chí kiểm toán

Đảm bảo Giám đốc dự án cho đơn vị đáp ứng đầy đủ các quy định theo luật định.

Dẫn chứng quy định ban hành

Điều 63 102/2009/NĐ-CP

Tài liệu yêu cầu

- Văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định về năng lực của Giám đốc dự án
- Bản đánh giá năng lực giám đốc dự án

Đánh giá thiết kế và triển khai

- Phòng vấn lãnh đạo đơn vị và xác minh xem đơn vị có ban hành văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định về năng lực của Giám đốc dự án hay không
- Thu thập, rà soát danh sách các thành viên trong ban quản lý dự án cũng như bằng cấp văn bản liên quan tới kinh nghiệm và kiến thức chuyên môn của các thành viên ban quản lý dự án đảm bảo tuân theo quy định nội bộ ban hành (nếu có) và tuân theo điều 63 -102/2009/NĐ-CP (trong trường hợp không có quy định ban hành nội bộ) đảm bảo giám đốc dự án đáp ứng các yêu cầu sau:
 - Có trình độ đại học chuyên ngành CNTT trở lên, đã được bồi dưỡng nghiệp vụ về quản lý, đầu tư ứng dụng CNTT (bộ môn lập và quản lý dự án)
 - Đối với dự án nhóm C, Giám đốc dự án cần Có thời gian liên tục làm công tác lập, quản lý dự án tối thiểu 5 năm, đã tham gia quản lý dự án của 1 dự án nhóm B hoặc 2 dự án nhóm C
 - Đối với các dự án quan trọng quốc gia, nhóm A, B, C Giám đốc dự án cần Có thời gian liên tục làm công tác lập, quản lý dự án tối thiểu 7 năm, đã tham gia quản lý dự án của 1 dự án nhóm A hoặc 2 dự án nhóm B, hoặc 5 dự án nhóm C và đã là chỉ huy thi công xây lắp tại hiện trường của dự án nhóm C

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Vấn đề B6.07.00- Lập, thẩm định, phê duyệt kế hoạch đấu thầu cho công việc chuẩn bị thực hiện dự án

Kiểm soát B6.07.01: Đơn vị sử dụng Phương thức Chỉ định thầu trong các trường hợp theo đúng quy định

Tiêu chí kiểm toán

Đảm bảo tất cả các dự án sử dụng Phương thức chỉ định thầu là phù hợp với quy định

Dẫn chứng quy định ban hành

Điều 22 Luật đấu thầu 43/2013/QH13

Tài liệu yêu cầu

- Hồ sơ thầu
- Quy định sử dụng các phương thức mời thầu (nếu có)

Đánh giá thiết kế và triển khai

▪ Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có ban hành văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định về các điều kiện mà qua đó đơn vị xác định được Phương thức lựa chọn nhà thầu.

▪ Đối với dự án sử dụng Phương thức chỉ định thầu, rà soát hồ sơ dự án và bảo đảm dự án thuộc một trong các trường hợp sau:

▪ a) Gói thầu cần thực hiện để khắc phục ngay hoặc để xử lý kịp thời hậu quả gây ra do sự cố bất khả kháng; gói thầu cần thực hiện để bảo đảm bí mật nhà nước; gói thầu cần triển khai ngay để tránh gây nguy hại trực tiếp đến tính mạng, sức khỏe và tài sản của cộng đồng dân cư trên địa bàn hoặc để không ảnh hưởng nghiêm trọng đến công trình liền kề; gói thầu mua thuốc, hóa chất, vật tư, thiết bị y tế để triển khai công tác phòng, chống dịch bệnh trong trường hợp cấp bách;

▪ b) Gói thầu cấp bách cần triển khai nhằm mục tiêu bảo vệ chủ quyền quốc gia, biên giới quốc gia, hải đảo;

▪ c) Gói thầu cung cấp dịch vụ tư vấn, dịch vụ phi tư vấn, mua sắm hàng hóa phải mua từ nhà thầu đã thực hiện trước đó do phải bảo đảm tính tương thích về công nghệ, bản quyền mà không thể mua được từ nhà thầu khác; gói thầu có tính chất nghiên cứu, thử nghiệm; mua bản quyền sở hữu trí tuệ;

- d) Gói thầu cung cấp dịch vụ tư vấn lập báo cáo nghiên cứu khả thi, thiết kế xây dựng được chỉ định cho tác giả của thiết kế kiến trúc công trình trúng tuyển hoặc được tuyển chọn khi tác giả có đủ điều kiện năng lực theo quy định; gói thầu thi công xây dựng tượng đài, phù điêu, tranh hoành tráng, tác phẩm nghệ thuật gắn với quyền tác giả từ khâu sáng tác đến thi công công trình;
- đ) Gói thầu di dời các công trình hạ tầng kỹ thuật do một đơn vị chuyên ngành trực tiếp quản lý để phục vụ công tác giải phóng mặt bằng; gói thầu rà phá bom, mìn, vật nổ để chuẩn bị mặt bằng thi công xây dựng công trình;
- e) Gói thầu cung cấp sản phẩm, dịch vụ công, gói thầu có giá gói thầu trong hạn mức được áp dụng chỉ định thầu theo quy định của Chính phủ phù hợp với điều kiện kinh tế xã hội trong từng thời kỳ.
- Việc thực hiện chỉ định thầu đối với gói thầu quy định tại các điểm b, c, d, đ và e khoản 1 Điều này phải đáp ứng đủ các điều kiện sau đây:
 - a) Có quyết định đầu tư được phê duyệt, trừ gói thầu tư vấn chuẩn bị dự án;
 - b) Có kế hoạch lựa chọn nhà thầu được phê duyệt;
 - c) Đã được bố trí vốn theo yêu cầu tiến độ thực hiện gói thầu;
 - d) Có dự toán được phê duyệt theo quy định, trừ trường hợp đối với gói thầu EP, EC, EPC, gói thầu chìa khóa trao tay;
 - đ) Có thời gian thực hiện chỉ định thầu kể từ ngày phê duyệt hồ sơ yêu cầu đến ngày ký kết hợp đồng không quá 45 ngày; trường hợp gói thầu có quy mô lớn, phức tạp không quá 90 ngày;
 - e) Nhà thầu được đề nghị chỉ định thầu phải có tên trong cơ sở dữ liệu về nhà thầu của cơ quan quản lý nhà nước về hoạt động đấu thầu.
- Chỉ định thầu đối với nhà đầu tư được áp dụng trong các trường hợp sau đây:
 - a) Chỉ có một nhà đầu tư đăng ký thực hiện;
 - b) Chỉ có một nhà đầu tư có khả năng thực hiện do liên quan đến sở hữu trí tuệ, bí mật thương mại, công nghệ hoặc thu xếp vốn;
 - c) Nhà đầu tư đề xuất dự án đáp ứng yêu cầu thực hiện dự án khả thi và hiệu quả cao nhất theo quy định của Chính phủ

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B6.07.02: Đơn vị sử dụng Phương thức chào hàng cạnh tranh trong các trường hợp theo đúng quy định

Tiêu chí kiểm toán

Đảm bảo tất cả các dự án sử dụng Phương thức chào hàng cạnh tranh là phù hợp với quy định

Dẫn chứng quy định ban hành

Điều 23 Luật đấu thầu 43/2013/QH13

Tài liệu yêu cầu

- Hồ sơ thầu
- Quy định sử dụng các phương thức mời thầu (nếu có)

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có văn bản nào quy định về các điều kiện mà qua đó đơn vị xác định được Phương thức lựa chọn nhà thầu.

- Đối với dự án sử dụng Phương thức Chào hàng cạnh tranh, rà soát hồ sơ thầu của dự án và bảo đảm dự án có giá trị trong hạn mức theo quy định. Cụ thể:

- Gói thầu dịch vụ phi tư vấn thông dụng, đơn giản được áp dụng Phương thức Chào hàng cạnh tranh theo quy trình rút gọn nếu gói thầu có giá trị không quá 500 triệu đồng.

- Gói thầu mua sắm hàng hóa thông dụng, sẵn có trên thị trường với đặc tính kỹ thuật được tiêu chuẩn hóa và tương đương nhau về chất lượng; Gói thầu xây lắp công trình đơn giản đã có thiết kế bản vẽ thi công được phê duyệt được áp dụng Phương thức chào hàng cạnh tranh theo quy trình rút gọn nếu gói thầu có giá trị không quá 01 tỉ đồng, gói thầu đối với mua sắm thường xuyên có giá trị không quá 200 triệu đồng.

- Các gói thầu trên được thực hiện Phương thức chào hàng cạnh tranh theo quy trình thông thường nếu giá trị thầu không quá 5 tỉ đồng.

- Bên cạnh những yêu cầu trên, để áp dụng Phương thức chào hàng cạnh tranh, dự án cần đáp ứng các yêu cầu:

- Có kế hoạch lựa chọn nhà thầu được phê duyệt

- Có dự toán được phê duyệt theo quy định
- Đã được bố trí vốn theo yêu cầu tiến độ thực hiện gói thầu

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B6.07.03: Đơn vị sử dụng Phương thức Mua sắm trực tiếp trong các trường hợp theo đúng quy định.

Tiêu chí kiểm toán

Đảm bảo tất cả các dự án sử dụng Phương thức Mua sắm trực tiếp là phù hợp với quy định

Dẫn chứng quy định ban hành

Điều 60 của Nghị định 63/2014/NĐ-CP

Tài liệu yêu cầu

- Hồ sơ thầu
- Quy định sử dụng các phương thức mời thầu (nếu có)

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có văn bản nào quy định về các điều kiện mà qua đó đơn vị xác định được Phương thức lựa chọn nhà thầu.

- Đối với dự án sử dụng Phương thức Mua sắm trực tiếp, rà soát hồ sơ thầu của dự án và đảm bảo Mua sắm trực tiếp chỉ được áp dụng đối với gói thầu mua sắm hàng hóa tương tự thuộc cùng một dự án, dự toán mua sắm hoặc thuộc dự án, dự toán mua sắm khác đồng thời thỏa mãn các yêu cầu sau:

- Nhà thầu đã trúng thầu thông qua đấu thầu rộng rãi hoặc đấu thầu hạn chế và đã ký hợp đồng thực hiện gói thầu trước đó;
- Gói thầu có nội dung, tính chất tương tự và quy mô nhỏ hơn 130% so với gói thầu đã ký hợp đồng trước đó;
- Đơn giá của các phần việc thuộc gói thầu áp dụng mua sắm trực tiếp không được vượt đơn giá của các phần việc tương ứng thuộc gói thầu tương tự đã ký hợp đồng trước đó;
- Thời hạn từ khi ký hợp đồng của gói thầu trước đó đến ngày phê duyệt kết quả mua sắm trực tiếp không quá 12 tháng.

- Trong trường hợp nhà thầu thực hiện hợp đồng trước đó không có khả năng tiếp tục thực hiện gói thầu mua sắm trực tiếp thì được áp dụng mua sắm trực tiếp đối với nhà thầu khác nếu đáp ứng các yêu cầu về năng lực, kinh nghiệm, kỹ thuật và giá theo hồ sơ mời thầu và kết quả lựa chọn nhà thầu trước đó.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B6.07.04: Đơn vị sử dụng Phương thức Tự thực hiện trong các trường hợp theo đúng quy định

Tiêu chí kiểm toán

Đảm bảo tất cả các dự án sử dụng Phương thức Tự thực hiện là phù hợp với quy định.

Dẫn chứng quy định ban hành

Điều 61 Nghị định số 63/2014/NĐ-CP

Tài liệu yêu cầu

- Hồ sơ thầu
- Quy định sử dụng các phương thức mời thầu (nếu có)

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có văn bản nào quy định về các điều kiện mà qua đó đơn vị xác định được Phương thức lựa chọn nhà thầu.

- Đối với dự án sử dụng Phương thức Tự thực hiện, rà soát hồ sơ thầu của dự án và đảm bảo chỉ áp dụng đối với gói thầu thuộc dự án, dự toán mua sắm trong trường hợp tổ chức trực tiếp quản lý, sử dụng gói thầu có năng lực kỹ thuật, tài chính và kinh nghiệm đáp ứng yêu cầu của gói thầu. Cụ thể:

- Đơn vị có chức năng, nhiệm vụ, lĩnh vực hoạt động và ngành nghề kinh doanh phù hợp với yêu cầu của gói thầu;
- Đơn vị phải chứng minh và thể hiện trong phương án tự thực hiện về khả năng huy động nhân sự, máy móc, thiết bị đáp ứng yêu cầu về tiến độ thực hiện gói thầu;
- Đơn vị được giao thực hiện gói thầu không được chuyển nhượng khối lượng công việc với tổng số tiền từ 10% giá gói thầu trở lên hoặc dưới 10% giá gói thầu nhưng trên 50 tỷ đồng.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Vấn đề B6.08.00- Lập, thẩm định, phê duyệt TKTC TDT, HSMT/HSYC và tổ chức đấu thầu các gói thầu dự án CNTT sử dụng NSNN

Kiểm soát B6.08.01 Nhà thầu tham dự thầu phải độc lập về pháp lý và độc lập về tài chính với các bên liên quan

Tiêu chí kiểm toán

Đảm bảo nhà thầu tham dự thầu độc lập về pháp lý và độc lập về tài chính với các bên liên quan, việc lựa chọn nhà thầu được thực hiện một cách khách quan

Dẫn chứng quy định ban hành

- Điều 6 Luật đấu thầu 43/2013/QH13
- Điều 2 Nghị định 63/2014/NĐ-CP

Tài liệu yêu cầu

- Hồ sơ mời thầu
- Danh sách các nhà thầu tham dự thầu
- Thông tin về các nhà thầu tham dự

Đánh giá thiết kế và triển khai

▪ Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có tiến hành đánh giá tính độc lập về mặt pháp lý và tính độc lập về mặt tài chính của các nhà thầu tham dự thầu hay không

▪ Thu thập và rà soát Hồ sơ mời thầu, danh sách các nhà thầu tham dự thầu, và xác minh xem các nhà thầu tham dự thầu có đáp ứng đủ các điều kiện sau không:

- Nhà thầu không cùng thuộc một cơ quan hoặc tổ chức quản lý trực tiếp với đơn vị sự nghiệp;
- Nhà thầu với chủ đầu tư, bên mời thầu không có cổ phần hoặc vốn góp trên 30% của nhau;
- Nhà thầu không có cổ phần hoặc vốn góp trên 20% của nhau khi cùng tham dự thầu trong một gói thầu đối với đấu thầu hạn chế;
- Nhà thầu tham dự thầu với nhà thầu tư vấn cho gói thầu đó không có cổ phần hoặc vốn góp của nhau; không cùng có cổ phần hoặc vốn góp trên 20% của một tổ chức, cá nhân khác với từng bên.

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách các nhà thầu tham dự thầu, Kiểm toán viên nhà nước tiến hành chọn mẫu và thực hiện các thủ tục như phần Đánh giá thiết kế và triển khai để đảm bảo tính hoạt động hiệu quả của kiểm soát.

Vấn đề B6.09.00 - Tổ chức triển khai dự án

Kiểm soát B6.09.01: Việc lập và gửi báo cáo định kỳ cho các đơn vị chủ quản

Tiêu chí kiểm toán

Đảm bảo các dự án ứng dụng CNTT sử dụng nguồn vốn NSNN phải chịu sự giám sát, đánh giá đầu tư định kỳ thông qua việc thực hiện lập và gửi báo cáo định kỳ cho các cơ quan chủ quản

Dẫn chứng quy định ban hành

Điều 10102/2009/NĐ-CP

Tài liệu yêu cầu

- Danh sách nhóm thiết kế sơ bộ
- Bảng cấp / văn bản liên quan tới việc đánh giá kinh nghiệm, kiến thức chuyên môn của nhóm thiết kế sơ bộ

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có ban hành văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt văn bản nào quy định liên quan tới việc gửi báo cáo dự án cho cơ quan chủ quản, các cơ quan thực hiện giám sát, đánh giá đầu tư có liên quan hay không

- Thu thập, rà soát các báo cáo theo quy định và xác minh tần suất báo cáo, đảm bảo tần suất báo cáo lên cơ quan chủ quản, các cơ quan thực hiện giám sát, đánh giá đầu tư có liên quan như sau:

- Báo cáo tháng, chậm nhất 10 ngày sau khi hết tháng (chỉ áp dụng đối với dự án ứng dụng công nghệ thông tin thuộc thẩm quyền phê duyệt của Thủ tướng Chính phủ);
- Báo cáo sáu tháng, chậm nhất vào ngày 15 tháng 07 của năm kế hoạch;
- Báo cáo năm, chậm nhất vào ngày 31 tháng 01 năm sau;
- Báo cáo kết thúc, chậm nhất 6 tháng sau khi kết thúc dự án;

Thử nghiệm hiệu quả hoạt động

Kiểm toán viên nhà nước cần nhắc thực hiện thử nghiệm hiệu quả hoạt động nếu cần thiết nhằm đảm bảo kiểm soát trên hoạt động hiệu quả trong suốt giai đoạn kiểm toán.

Kiểm soát B6.09.02: Mức vốn tạm ứng cho nhà thầu ở trong mức theo quy định

Tiêu chí kiểm toán

- Đảm bảo đơn vị tạm ứng vốn cho nhà thầu đầy đủ và không vượt quá định mức cho phép

Dẫn chứng quy định ban hành

- Điều 6 Luật đấu thầu 43/2013/QH13
- Điều 2 Nghị định 63/2014/NĐ-CP

Tài liệu yêu cầu

- Thỏa thuận dịch vụ/ Hợp đồng
- Vốn tạm ứng cho nhà thầu

Đánh giá thiết kế và triển khai

- Phòng vấn lãnh đạo đơn vị và xác minh xem đơn vị có quy định nào liên quan đến mức vốn tạm ứng cho nhà thầu hay không
- Thu thập và rà soát Thỏa thuận dịch vụ/ Hợp đồng, và xác minh xem mức vốn tạm ứng cho nhà thầu là bao nhiêu, đảm bảo mức vốn tạm ứng đáp ứng yêu cầu như sau:
 - Đối với hợp đồng thi công xây lắp:
 - Mức tạm ứng phải $\geq 20\%$ GTHĐ với các HĐ có giá trị < 10 tỉ đồng
 - Mức tạm ứng phải $\geq 15\%$ GTHĐ với các HĐ có giá trị từ $10 - 50$ tỉ đồng
 - Mức tạm ứng phải $\geq 10\%$ GTHĐ với các HĐ có giá trị > 50 tỉ đồng
 - Đối với HĐ cung cấp thiết bị công nghệ, HĐ EPC, hợp đồng chìa khóa trao tay và các loại HĐ xây dựng khác thì mức tạm ứng phải $\geq 10\%$ GTHĐ
 - Đối với các HĐ tư vấn thì mức tạm ứng phải $\geq 25\%$ GTHĐ
 - Mức tạm ứng tối đa không được vượt quá 50% GTHĐ. Nếu mức tạm ứng $\geq 50\%$ GTHĐ, kiểm tra xem đã có quyết định cho phép của người quyết định đầu tư hay chưa

- Ngoài mức vốn tạm ứng tối đa theo các hợp đồng nêu trên, đối với một số cấu kiện, bán thành phẩm có giá trị lớn phải sản xuất trước để đảm bảo tiến độ và một số loại vật tư phải dự trữ theo mùa, mức vốn tạm ứng theo nhu cầu cần thiết và do chủ đầu tư thống nhất với nhà thầu.
- Việc tạm ứng vốn được thực hiện sau khi HĐ có hiệu lực.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B6.09.03: Thời gian thực hiện đầu tư cho các hoạt động ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước nhưng không yêu cầu phải lập dự án theo đúng quy định

Tiêu chí kiểm toán

Đảm bảo các hoạt động ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước nhưng không yêu cầu phải lập dự án được hoàn thành trong khoảng thời gian theo quy định

Dẫn chứng quy định ban hành

Điều 5 -21/2010/TT-BTTTT

Tài liệu yêu cầu

Danh sách hoạt động ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước nhưng không yêu cầu phải lập dự án

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có hoạt động ứng dụng CNTT nhưng không lập dự án không
- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có văn bản nào quy định về thời gian thực hiện đối với các hoạt động CNTT sử dụng nguồn vốn NSNN nhưng không phải lập dự án hay không
- Thu thập, rà soát các hoạt động ứng dụng CNTT sử dụng nguồn vốn NSNN, đảm bảo thời gian thực hiện đầu tư các hoạt động đó không kéo dài quá 2 năm kể từ khi đề cương và dự toán chi tiết được phê duyệt

Thử nghiệm hiệu quả hoạt động

Dựa trên danh sách các hoạt động CNTT không lập dự án, mà chỉ lập đề cương và dự toán chi tiết, Kiểm toán viên nhà nước tiến hành chọn mẫu và thực hiện các thủ

tục như ở phần Đánh giá thiết kế và triển khai để bảo đảm tính hoạt động hữu hiệu của kiểm soát.

Vấn đề B6.10 - Bàn giao/nghiệm thu các hợp đồng dự án

Kiểm soát B6.10.01: Báo cáo quyết toán được hoàn thành trong thời gian quy định.

Tiêu chí kiểm toán

Đảm bảo đơn vị hoàn thành báo cáo quyết toán trong thời gian theo quy định

Dẫn chứng quy định ban hành

Điều 19/2011/TT-BTC

Tài liệu yêu cầu

- Biên bản bàn giao sử dụng
- Báo cáo quyết toán

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có ban hành văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định nào liên quan đến thời gian hoàn thành báo cáo quyết toán hay không.

- Thu thập, rà soát biên bản bàn giao sử dụng cũng như báo cáo quyết toán, và đảm bảo trình tự và thủ tục quyết định được thực hiện tuân theo quy định nội bộ ban hành (nếu có) và tuân theo điều 19/2011/TT-BTC (trong trường hợp không có quy định ban hành nội bộ) đảm bảo đáp ứng yêu cầu như sau:

- Đối với dự án quan trọng quốc gia, dự án nhóm A, thời gian lập báo cáo quyết toán không quá 12 tháng. Thời gian lập báo cáo quyết toán dự án hoàn thành được tính từ ngày ký biên bản bàn giao đưa vào sử dụng.

- Đối với dự án nhóm B, thời gian lập báo cáo quyết toán không quá 9 tháng.

Dự án nhóm C không quá 6 tháng

- Đối với các dự án chỉ phải lập Đề cương dự toán chi tiết thì thời gian lập báo cáo quyết toán dự án không quá 3 tháng.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B6.10.02: Dự án được bảo hành bởi nhà thầu theo quy định

Tiêu chí kiểm toán

Đảm bảo dự án được bảo hành bởi nhà thầu theo quy định

Dẫn chứng quy định ban hành

Điều 48 NĐ102/2009/NĐ-CP

Tài liệu yêu cầu

Hồ sơ bảo hành của nhà thầu

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có ban hành văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định về nhà thầu có thực hiện nộp tiền bảo hành dự án hay không
- Thu thập, rà soát hồ sơ bảo hành của nhà thầu cũng như chứng từ liên quan tới việc nộp tiền hoặc bảo lãnh ngân hàng cho chủ đầu tư đảm bảo trình tự và thủ tục quyết định được thực hiện tuân theo quy định nội bộ ban hành (nếu có) và tuân theo Điều 48 NĐ102/2009/NĐ-CP (trong trường hợp không có quy định ban hành nội bộ) đảm bảo nhà thầu thực hiện bảo hành các dự án theo các quy định như sau:
 - Bảo hành 24 tháng đối với sản phẩm của dự án quan trọng quốc gia, dự án nhóm A;
 - Bảo hành 12 tháng đối với sản phẩm của dự án nhóm B, C.
 - Mức tiền bảo hành tối thiểu được tính bằng tỷ lệ phần trăm (%) giá trị sản phẩm của dự án theo quy định. Cụ thể:
 - i) Đối với sản phẩm có thời hạn bảo hành 24 tháng là 3%;
 - ii) Đối với sản phẩm có thời hạn bảo hành 12 tháng là 5%.
 - Nhà thầu có trách nhiệm nộp tiền bảo hành vào tài khoản của Chủ đầu tư trước khi Chủ đầu tư ký biên bản nghiệm thu. Tiền bảo hành sản phẩm được tính lãi suất như tiền gửi ngân hàng. Nhà thầu và Chủ đầu tư có thể thỏa thuận việc thay thế tiền bảo hành bằng thư bảo lãnh của ngân hàng có giá trị tương đương. Nhà thầu chỉ được hoàn trả tiền bảo hành sau khi kết thúc thời hạn bảo hành và được Chủ đầu tư xác nhận đã hoàn thành công việc bảo hành.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Vấn đề B6.11 - Quyết toán dự án đầu tư

Kiểm soát B6.11.01: Chi phí quản lý dự án và chi phí tư vấn đầu tư ứng dụng CNTT được đơn vị xác định theo QĐ 2378 hoặc QĐ993/ QĐ-BTTTT

Tiêu chí kiểm toán

Đảm bảo chi phí quản lý dự án và chi phí tư vấn đầu tư ứng dụng CNTT sử dụng NSNN tuân theo các QĐ của Bộ Thông tin và Truyền thông.

Dẫn chứng quy định ban hành

QĐ 2378 /QĐ993/ QĐ-BTTTT

Tài liệu yêu cầu

Văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định việc tính toán chi phí quản lý dự án và chi phí tư vấn đầu tư ứng dụng CNTT

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có ban hành văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định việc tính toán chi phí quản lý dự án và chi phí tư vấn đầu tư ứng dụng CNTT sử dụng NSNN khi lập dự toán/ tính tổng mức đầu tư hay không. Trong trường hợp đơn vị không có quy định nội bộ thì:
 - Đơn vị có dựa vào QĐ 2378/QĐ-BTTTT để xác định chi phí QLDA và chi phí tư vấn đầu tư để lập dự toán/ tính tổng mức đầu tư cho các dự án mà dự toán được lập sau ngày 1/3/2017 hay không?
 - Đơn vị có dựa vào QĐ 993/QĐ-BTTTT để xác định chi phí QLDA và chi phí tư vấn đầu tư để lập dự toán/ tính tổng mức đầu tư cho các dự án mà dự toán được lập trước ngày 1/3/2017 hay không?
 - Thu thập quy trình được lập thành văn bản, được phê duyệt bởi lãnh đạo.
 - Phỏng vấn người quản lý và những người có trách nhiệm khác đối với lập dự toán để bảo đảm họ đã tuân theo các quy định của đơn vị.

Thử nghiệm hiệu quả hoạt động

- Hiệu quả hoạt động đã được thử nghiệm ở phần đánh giá thiết kế và triển khai.

Kiểm soát B6.11.02: Chi phí quản lý dự án được xác định theo các quy tắc và điều chỉnh phù hợp theo quy định

Tiêu chí kiểm toán

Đảm bảo chi phí quản lý dự án được xác định theo các quy tắc và điều chỉnh theo quy định

Dẫn chứng quy định ban hành

QĐ2378/QĐ-BTTTT

Tài liệu yêu cầu

Dự toán/ tổng mức đầu tư của dự án

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đơn vị có ban hành văn bản nội bộ được cấp quản lý có thẩm quyền phê duyệt quy định việc tính toán chi phí quản lý dự án và chi phí tư vấn đầu tư ứng dụng CNTT sử dụng NSNN khi lập dự toán/ tính tổng mức đầu tư hay không.
- Trong trường hợp đơn vị không ban hành quy định nội bộ, phòng văn lãnh đạo đơn vị và xác minh xem đối với các dự án lập dự toán/ lập tổng mức đầu tư sau ngày 1/3/2017 đơn vị có áp dụng Định mức chi phí quản lý dự án được quy định trong QĐ 2378/QĐ-BTTTT hay không?
- Rà soát Dự toán chi phí quản lý dự án và đảm bảo Dự toán chi phí quản lý dự án đáp ứng các yêu cầu sau:
 - Chi phí quản lý dự án được xác định là nguồn kinh phí cần thiết cho chủ đầu tư để tổ chức quản lý việc thực hiện các công việc quản lý dự án từ giai đoạn chuẩn bị đầu tư, thực hiện đầu tư đến khi hoàn thành, nghiệm thu bàn giao, đưa dự án vào khai thác sử dụng và phê duyệt quyết toán;
 - Chi phí quản lý dự án trong tổng mức đầu tư (chưa có thuế giá trị gia tăng) xác định theo định mức tỷ lệ phần trăm (%) và nhân với chi phí xây lắp và chi phí thiết bị (chưa có thuế giá trị gia tăng) trong tổng mức đầu tư được duyệt.
 - Chi phí quản lý dự án trong dự toán (chưa có thuế giá trị gia tăng) xác định theo định mức tỷ lệ phần trăm (%) (cùng định mức tỷ lệ % sử dụng để tính chi phí quản lý dự án trong tổng mức đầu tư nói trên) và nhân với chi phí xây lắp và thiết bị (chưa có thuế giá trị gia tăng) của dự toán được duyệt.

- Chi phí quản lý dự án của các dự án đầu tư hoặc hạng mục ứng dụng công nghệ thông tin được điều chỉnh trong các trường hợp sau:
 - Dự án được thực hiện tại vùng hải đảo, tại vùng biên giới được xác định theo định mức công bố tại Quyết định này và điều chỉnh với hệ số $k = 1,35$.
 - Dự án được thực hiện trải dài trên địa bàn nhiều tỉnh thì chi phí quản lý dự án được xác định theo định mức công bố tại Quyết định này và điều chỉnh với hệ số $k = 1,25$. Trường hợp dự án triển khai trên phạm vi rộng, có những yêu cầu quản lý đặc thù, định mức không đáp ứng yêu cầu quản lý thì chủ đầu tư lập dự toán, kèm giải trình chi tiết và trình cấp có thẩm quyền phê duyệt theo chế độ hiện hành.
 - Dự án đầu tư mua sắm dự phòng, thay thế một phần các thiết bị phần cứng thuộc hệ thống hạ tầng kỹ thuật hiện có; mua sắm thiết bị không cần lắp đặt, phần mềm thương mại thì chi phí quản lý dự án được xác định theo định mức công bố tại Quyết định này và điều chỉnh với hệ số $k = 0,8$.
 - Trường hợp dự án bao gồm các dự án thành phần thì chi phí quản lý dự án được xác định riêng theo quy mô của từng dự án thành phần. Trường hợp dự án gồm các công trình riêng biệt được xây lắp trên địa bàn các tỉnh khác nhau thì chi phí quản lý dự án được xác định theo quy mô chi phí xây lắp và chi phí thiết bị trong dự toán của từng công trình được duyệt.

Thử nghiệm hiệu quả hoạt động

Dựa trên dự toán/ tổng mức đầu tư của các dự án, Kiểm toán viên nhà nước tiến hành chọn mẫu mà thực hiện các thủ tục như trong phần Đánh giá thiết kế và triển khai để bảo đảm tính hữu hiệu của hoạt động.

Kiểm soát B6.11.03: Chi phí quản lý dự án được xác định theo định mức cận trên và cận dưới phù hợp

Tiêu chí kiểm toán

Đảm bảo Chi phí quản lý dự án được xác định theo định mức cận trên và cận dưới phù hợp theo quy định tại QĐ2378/QĐ-BTTTT

Dẫn chứng quy định ban hành

QĐ2378/QĐ-BTTTT

Tài liệu yêu cầu

Dự toán/ tổng mức đầu tư của dự án

Đánh giá thiết kế và triển khai

Rà soát Dự toán chi phí quản lý dự án và đảm bảo Dự toán/ Chi phí quản lý dự án trong tổng mức đầu tư được tính toán theo hướng dẫn của BTTT

$$N_t = N_b - \frac{N_b - N_a}{G_a - G_b} \times (G_t - G_b)$$

Áp dụng cận trên và cận dưới theo đúng quy định như sau:

+ Dự án hạ tầng kỹ thuật công nghệ thông tin

Đơn vị tính: tỷ lệ %

Chi phí xây lắp và thiết bị (chưa có thuế GTGT) (tỷ đồng)									
≤ 7	15	20	30	50	100	150	200	500	1000
2,644	2,184	1,913	1,747	1,324	1,045	1,007	0,975	0,841	0,696

+ Trường hợp báo cáo kinh tế kỹ thuật thì định mức chi phí quản lý dự án tính bằng 0,84 lần định mức chi phí quản lý dự án của dự án đầu tư, tương ứng với quy mô giá trị xây lắp và thiết bị.

+ Dự án phần mềm nội bộ, cơ sở dữ liệu

Đơn vị tính: tỷ lệ %

Giá trị thiết bị phần mềm nội bộ (chưa có thuế GTGT) (tỷ đồng)							
≤ 7	15	20	30	50	100	150	200
2,809	2,133	1,964	1,782	1,710	1,346	1,287	1,248
1,855	1,532						

+ Báo cáo kinh tế kỹ thuật phần mềm nội bộ, cơ sở dữ liệu

≤ 7	15
1,855	1,532

Thử nghiệm hiệu quả hoạt động

Dựa trên dự toán/ tổng mức đầu tư của các dự án, Kiểm toán viên nhà nước tiến hành chọn mẫu mà thực hiện các thủ tục như trong phần Đánh giá thiết kế và triển khai để bảo đảm tính hữu hiệu của hoạt động.

Kiểm soát B6.11.04 Chi phí lập dự án đầu tư trong lập dự toán/ tổng mức đầu tư được xác định theo các quy tắc và điều chỉnh phù hợp theo quy định

Tiêu chí kiểm toán

Đảm bảo Chi phí lập dự án đầu tư trong lập dự toán/ tổng mức đầu tư được xác định theo các quy tắc và điều chỉnh phù hợp theo quy định

Dẫn chứng quy định ban hành

QĐ 2378/QĐ-BTTTT

Tài liệu yêu cầu

Dự toán/ tổng mức đầu tư của dự án

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đối với các dự án lập dự toán/ lập tổng mức đầu tư sau ngày 1/3/2017 đơn vị có áp dụng Định mức chi phí lập dự án đầu tư được quy định trong QĐ 2378/QĐ-BTTTT hay không?

- Rà soát Dự toán chi phí lập dự án đầu tư, đảm bảo Chi phí lập dự án đầu tư đáp ứng các yêu cầu sau:

- Chi phí lập dự án đầu tư xác định theo định mức tỉ lệ phần trăm (%) và nhân với chi phí xây lắp và chi phí thiết bị trong tổng mức đầu tư của dự án được duyệt.

- Chi phí lập dự án đầu tư chưa gồm chi phí để thực hiện điều tra, khảo sát phục vụ lập dự án.

- Chi phí lập dự án đầu tư điều chỉnh trong các trường hợp sau:

- Trường hợp cải tạo, sửa chữa, mở rộng, nâng cấp có tính toán kết nối với hạ tầng, công nghệ của dự án hiện có: điều chỉnh định mức chi phí với hệ số $k = 1,2$.

- Trường hợp sử dụng thiết kế mẫu, thiết kế điển hình do cơ quan có thẩm quyền ban hành: điều chỉnh định mức chi phí với hệ số $k = 0,75$.

- Dự án có các phần tử mạng phân bố ở các khu vực khác nhau thì chi phí lập dự án được xác định theo định mức công bố tại Quyết định này và điều chỉnh với hệ số $k = 1,3$.
- Dự án đầu tư mua sắm dự phòng, thay thế một phần các thiết bị phần cứng thuộc hệ thống hạ tầng kỹ thuật hiện có; mua sắm thiết bị không cần lắp đặt, phần mềm thương mại thì chi phí lập dự án được xác định theo định mức công bố tại Quyết định này và điều chỉnh với hệ số $k = 0,7$.

Thử nghiệm hiệu quả hoạt động

Dựa trên dự toán/ tổng mức đầu tư của các dự án, Kiểm toán viên nhà nước tiến hành chọn mẫu mà thực hiện các thủ tục như trong phần Đánh giá thiết kế và triển khai để bảo đảm tính hữu hiệu của hoạt động.

Kiểm soát B6.11.05: Chi phí thiết kế thi công và dự toán trong lập dự toán/ tổng mức đầu tư được xác định theo các quy tắc và điều chỉnh phù hợp theo quy định

Tiêu chí kiểm toán

Đảm bảo chi phí thiết kế thi công và dự toán trong lập dự toán/ tổng mức đầu tư được xác định theo các quy tắc và điều chỉnh phù hợp theo quy định

Dẫn chứng quy định ban hành

Mục 3, 4 phần 3 QĐ 2378/QĐ-BTTTT

Tài liệu yêu cầu

Dự toán/ tổng mức đầu tư của dự án

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đối với các dự án lập dự toán/ lập tổng mức đầu tư sau ngày 1/3/2017 đơn vị có áp dụng Định mức chi phí thiết kế thi công và dự toán được quy định trong QĐ 2378/QĐ-BTTTT hay không?

- Rà soát Dự toán chi phí thiết kế thi công và dự toán, xác minh chi phí có được tính theo công thức:

- $C_{tk} = (C_{xl} + C_{tb}) \times N_t \times k$
- Trong đó:
 - C_{tk} : Chi phí thiết kế thi công và dự toán; đơn vị tính: giá trị;
 - C_{xl} : Chi phí xây lắp tương ứng; đơn vị tính: giá trị;

- Ctb: Chi phí thiết bị tương ứng; đơn vị tính: giá trị;
 - Nt: Định mức chi phí thiết kế thi công và dự toán theo công bố; đơn vị tính: tỷ lệ %;
 - k: Hệ số điều chỉnh định mức chi phí thiết kế thi công và dự toán;
- Trong đó các chi phí định mức và hệ số điều chỉnh được sử dụng theo hướng dẫn của Mục 4 phần 3 QĐ 2378/QĐ-BTTTT không?

Thử nghiệm hiệu quả hoạt động

Dựa trên dự toán/ tổng mức đầu tư của các dự án, Kiểm toán viên nhà nước tiến hành chọn mẫu mà thực hiện các thủ tục như trong phần Đánh giá thiết kế và triển khai để bảo đảm tính hữu hiệu của hoạt động.

Kiểm soát B6.11.06: Chi phí thẩm tra thiết kế thi công trong lập dự toán/ tổng mức đầu tư được xác định theo các quy tắc và điều chỉnh phù hợp theo quy định

Tiêu chí kiểm toán

Đảm bảo chi phí thẩm tra thiết kế thi công trong lập dự toán/ tổng mức đầu tư được xác định theo các quy tắc và điều chỉnh phù hợp theo quy định

Dẫn chứng quy định ban hành

Mục 5 phần 3 QĐ 2378/QĐ-BTTTT

Tài liệu yêu cầu

- Dự toán/ tổng mức đầu tư của dự án

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đối với các dự án lập dự toán/ lập tổng mức đầu tư sau ngày 1/3/2017 đơn vị có áp dụng Định mức chi phí thẩm tra thiết kế thi công được quy định trong QĐ 2378/QĐ-BTTTT hay không?
- Rà soát Dự toán chi phí thiết kế thi công và dự toán, xác minh chi phí có được xác định như sau:
 - Chi phí thẩm tra thiết kế thi công xác định theo định mức phí cần thiết để hoàn thành toàn bộ công việc, đầy đủ nội dung và đạt yêu cầu chất lượng thẩm tra theo quy định hiện hành.
 - Chi phí thẩm tra thiết kế thi công (chưa có thuế giá trị gia tăng) xác định theo định mức tỷ lệ phần trăm (%) (định mức công bố tại Bảng số 5 QĐ 2378/QĐ-

BTTTT và nhân với chi phí xây lắp và thiết bị (chưa có thuế giá trị gia tăng) trong dự toán được duyệt.

- Trường hợp công việc thiết kế được thực hiện theo gói thầu thì chi phí thẩm tra thiết kế thi công xác định theo định mức quy định tại quyết định này và nhân với hệ số điều chỉnh $k = 0,9$.

Thử nghiệm hiệu quả hoạt động

Dựa trên dự toán/ tổng mức đầu tư của các dự án, Kiểm toán viên nhà nước tiến hành chọn mẫu mà thực hiện các thủ tục như trong phần Đánh giá thiết kế và triển khai để bảo đảm tính hữu hiệu của hoạt động.

Kiểm soát B6.11.07: Chi phí thẩm tra dự án trong lập dự toán/ tổng mức đầu tư được xác định theo các quy tắc và điều chỉnh phù hợp theo quy định

Tiêu chí kiểm toán

Đảm bảo chi phí thẩm tra dự án trong lập dự toán/ tổng mức đầu tư được xác định theo các quy tắc và điều chỉnh phù hợp theo quy định

Dẫn chứng quy định ban hành

Mục 6 phần 3 QĐ 2378/QĐ-BTTTT

Tài liệu yêu cầu

- Dự toán/ tổng mức đầu tư của dự án

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đối với các dự án lập dự toán/ lập tổng mức đầu tư sau ngày 1/3/2017 đơn vị có áp dụng Định mức chi phí thẩm tra dự toán công được quy định trong QĐ 2378/QĐ-BTTTT hay không?

- Rà soát Dự toán chi phí thẩm tra dự toán, xác minh chi phí có được xác định như sau:

- Chi phí thẩm tra dự toán xác định theo định mức là mức chi phí cần thiết để hoàn thành toàn bộ công việc, đầy đủ nội dung và đạt yêu cầu chất lượng thẩm tra theo quy định hiện hành.

- Chi phí thẩm tra dự toán (chưa có thuế giá trị gia tăng) xác định theo định mức tỷ lệ phần trăm (%) (Định mức công bố tại Bảng số 6/QĐ 2378/QĐ-BTTTT) và nhân với chi phí xây lắp và thiết bị (chưa có thuế giá trị gia tăng) trong dự toán được duyệt hoặc dự toán gói thầu được duyệt.

- Chi phí thẩm tra dự toán điều chỉnh, bổ sung, sửa đổi hoặc thẩm tra lại dự toán (không do lỗi của nhà thầu tư vấn thẩm tra dự toán) được xác định bằng lập dự toán.

Thử nghiệm hiệu quả hoạt động

Dựa trên dự toán/ tổng mức đầu tư của các dự án, Kiểm toán viên nhà nước tiến hành chọn mẫu mà thực hiện các thủ tục như trong phần Đánh giá thiết kế và triển khai để bảo đảm tính hữu hiệu của hoạt động.

Kiểm soát B6.11.08: Chi phí lập hồ sơ mời thầu, đánh giá hồ sơ dự thầu xây lắp trong lập dự toán/ tổng mức đầu tư được xác định theo các quy tắc và điều chỉnh phù hợp theo quy định

Tiêu chí kiểm toán

Đảm bảo chi phí hồ sơ mời thầu, đánh giá hồ sơ dự thầu xây lắp trong lập dự toán/ tổng mức đầu tư được xác định theo các quy tắc và điều chỉnh phù hợp theo quy định

Dẫn chứng quy định ban hành

Mục 7 phần 3 QĐ 2378/QĐ-BTTTT

Tài liệu yêu cầu

- Dự toán/ tổng mức đầu tư của dự án

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đối với các dự án lập dự toán/ lập tổng mức đầu tư sau ngày 1/3/2017 đơn vị có áp dụng Định mức chi phí hồ sơ mời thầu, đánh giá hồ sơ dự thầu xây lắp được quy định trong QĐ 2378/QĐ-BTTTT hay không?

- Rà soát Dự toán chi phí hồ sơ mời thầu, đánh giá hồ sơ dự thầu xây lắp, xác minh chi phí có được xác định như sau:

- Định mức chi phí lập hồ sơ mời thầu và đánh giá hồ sơ dự thầu mua sắm thiết bị tính theo định mức tại bảng 8 và phân chia như sau:

- Lập hồ sơ mời thầu: 40%;
- Phân tích đánh giá hồ sơ dự thầu: 60%.

- Trường hợp phải sơ tuyển thì bổ sung thêm chi phí bằng 15% của chi phí lập hồ sơ mời thầu và phân tích đánh giá hồ sơ dự thầu tính theo định mức tại bảng này.

- Chi phí lập hồ sơ mời thầu và đánh giá hồ sơ dự thầu mua sắm thiết bị xác định theo định mức nhưng tối thiểu không nhỏ hơn 5.000.000 đồng (chưa bao gồm Thuế GTGT).

Thử nghiệm hiệu quả hoạt động

Dựa trên dự toán/ tổng mức đầu tư của các dự án, Kiểm toán viên nhà nước tiến hành chọn mẫu mà thực hiện các thủ tục như trong phần Đánh giá thiết kế và triển khai để bảo đảm tính hữu hiệu của hoạt động.

Kiểm soát B6.11.09: Chi phí giám sát thi công lắp đặt phần cứng, cài đặt phần mềm trong lập dự toán/ tổng mức đầu tư được xác định theo các quy tắc và điều chỉnh phù hợp theo quy định

Tiêu chí kiểm toán

Đảm bảo Chi phí giám sát thi công lắp đặt phần cứng, cài đặt phần mềm trong lập dự toán/ tổng mức đầu tư được xác định theo các quy tắc và điều chỉnh phù hợp theo quy định

Dẫn chứng quy định ban hành

Mục 8 phần 3 QĐ 2378/QĐ-BTTTT

Tài liệu yêu cầu

- Dự toán/ tổng mức đầu tư của dự án

Đánh giá thiết kế và triển khai

- Phòng văn lãnh đạo đơn vị và xác minh xem đối với các dự án lập dự toán/ lập tổng mức đầu tư sau ngày 1/3/2017 đơn vị có áp dụng Định mức chi phí giám sát thi công lắp đặt phần cứng, cài đặt phần mềm được quy định trong QĐ 2378/QĐ-BTTTT hay không?

- Rà soát Dự toán chi phí giám sát thi công lắp đặt phần cứng, cài đặt phần mềm, xác minh chi phí có được xác định như sau:

- Chi phí giám sát thi công lắp đặt phần cứng, cài đặt phần mềm xác định theo định mức bảng 9QĐ 2378/QĐ-BTTTT là mức chi phí cần thiết để hoàn thành toàn bộ công việc, đầy đủ nội dung và đạt yêu cầu chất lượng giám sát thi công lắp đặt phần cứng, cài đặt phần mềm theo quy định hiện hành.

- Chi phí giám sát thi công lắp đặt phần cứng, cài đặt phần mềm (chưa có thuế giá trị gia tăng) xác định theo định mức tỷ lệ phần trăm (%) (định mức công

bổ tại Bảng số 9 QĐ 2378/QĐ-BTTTT) và nhân với chi phí xây lắp và chi phí thiết bị (chưa có thuế giá trị gia tăng) trong dự toán gói thầu thi công lắp đặt phần cứng, cài đặt phần mềm được duyệt.

- Chi phí giám sát xây dựng phần mềm nội bộ (chưa có thuế giá trị gia tăng) xác định theo định mức tỷ lệ phần trăm (%) (định mức công bố tại Bảng số 9 trong Quyết định này) và nhân với Giá trị thiết bị phần mềm nội bộ (chưa có thuế giá trị gia tăng) trong dự toán gói thầu xây dựng phần mềm nội bộ được duyệt.

- Chi phí giám sát dự án ứng dụng công nghệ thông tin ở hải đảo, biên giới hoặc dự án có các phần tử mạng phân bố ở các khu vực khác nhau hoặc dự án trải dài trên nhiều địa bàn thì chi phí giám sát được xác định theo định mức công bố tại Quyết định này và điều chỉnh với hệ số $k = 1,2$. Trường hợp dự án triển khai trên phạm vi rộng, có những yêu cầu quản lý đặc thù, định mức không đáp ứng yêu cầu quản lý thì chủ đầu tư lập dự toán, kèm giải trình chi tiết và trình cấp có thẩm quyền phê duyệt theo chế độ hiện hành.

- Chi phí giám sát thi công lắp đặt phần cứng, cài đặt phần mềm tính theo định mức công bố tại Quyết định này chưa bao gồm chi phí thuê hoặc xây dựng văn phòng làm việc tại hiện trường của nhà thầu tư vấn giám sát.

Thử nghiệm hiệu quả hoạt động

Dựa trên dự toán/ tổng mức đầu tư của các dự án, Kiểm toán viên nhà nước tiến hành chọn mẫu mà thực hiện các thủ tục như trong phần Đánh giá thiết kế và triển khai để bảo đảm tính hữu hiệu của hoạt động.

C. HƯỚNG DẪN CHI TIẾT KIỂM TOÁN TRONG MÔI TRƯỜNG CNTT

1. Tóm tắt và cách sử dụng các hướng dẫn chi tiết

a. Bố cục hướng dẫn

Hướng dẫn chi tiết kiểm toán trong môi trường CNTT trình bày các thủ tục kiểm toán mẫu sử dụng CAATs áp dụng cho kiểm toán báo cáo tài chính doanh nghiệp.

b. Cách áp dụng trong thực tế

Các cuộc kiểm toán CNTT trong môi trường CNTT cần lưu ý các nội dung sau:

- Vận dụng các thủ tục kiểm toán mẫu trình bày ở mục 2 khi kiểm tra xác nhận các báo cáo tài chính.
- Vận dụng các căn cứ pháp lý rút ra từ chuẩn mực KTNN tại Phụ lục.E để đề nghị đơn vị cung cấp dữ liệu, hoặc thực hiện các thủ tục kiểm toán cần thiết giảm thiểu rủi ro kiểm toán trong trường hợp đơn vị sử dụng các hệ thống CNTT xử lý thông tin nghiệp vụ chính cũng như lập các báo cáo tài chính.
- Áp dụng các thủ tục kiểm soát chung và kiểm soát ứng dụng CNTT thích hợp với cuộc kiểm toán trình bày ở phần II.A.

2. Thủ tục kiểm toán CNTT mẫu áp dụng cho kiểm toán báo cáo tài chính doanh nghiệp

a. Phân tích chỉ tiêu tài chính theo các tiêu chí khác nhau

Phân tích theo chiều ngang

So sánh các chỉ tiêu BCTC hoặc các tài khoản theo các kỳ nhằm tìm ra các biến động lớn. Kỹ thuật này có thể áp dụng cho từng tháng, quý, năm thậm chí ngày tùy thuộc vào mục tiêu kiểm toán và hệ thống kế toán máy của đơn vị.

Ví dụ: So sánh mức tăng trưởng doanh thu, tổng tài sản giữa năm nay với năm trước.

Phân tích theo chiều dọc

So sánh sự biến động cơ cấu các chỉ tiêu trên BCTC với một chỉ tiêu gốc nhằm xác định những thay đổi lớn.

Ví dụ: Các nội dung phân tích có thể là:

- *Phân tích tỷ lệ lãi gộp, lãi thuần trên Báo cáo kết quả hoạt động kinh doanh để đánh giá hiệu quả kinh doanh của đơn vị.*
- *Phân tích tỷ lệ nợ dài hạn trên tổng tài sản ở Bảng cân đối kế toán nhằm đánh giá mức độ rủi ro tài chính của đơn vị.*

Phân tích xu hướng biến động

Xem xét biến động của cặp chỉ tiêu tài chính biến động qua từng kỳ thời gian.

Ví dụ: Phân tích số dư hàng tồn kho quý trong năm, phân tích sự biến động của doanh thu hàng tháng trong năm

b. Phân tích chỉ tiêu tài chính theo từng khoản mục

Kiểm toán khoản mục tiền

- Kiểm tra tính liên tục của số phiếu thu/chi tiền mặt, tiền gửi ngân hàng đảm bảo tất cả các phí thu/chi đều được hạch toán một cách đầy đủ vào sổ sách kế toán. Thực hiện bằng cách áp dụng kỹ thuật kiểm tra khoảng trống của CAATs trên các bảng kê phiếu thu/chi của đơn vị.
- Kiểm tra việc đánh giá lại tỷ giá cuối kỳ đảm bảo các số dư tiền mặt và tiền gửi ngân hàng bằng ngoại tệ được đánh giá lại một cách chính xác theo quy định. Thực hiện bằng cách áp dụng CAATs tính toán lại chính xác số hạch toán.
- Kiểm tra tính hiệu quả của nguồn tiền nhàn rỗi nhằm đảm bảo: (i) Số dư tiền mặt chỉ được duy trì ở mức tối thiểu so với nhu cầu của đơn vị, phần phụ trội phải nộp tài khoản ngân hàng sớm nhất có thể; (ii) Số dư tiền gửi ngân hàng cũng chỉ được duy trì ở mức tối thiểu so với nhu cầu của đơn vị, phần phụ trội phải được chuyển sang một hình thức đầu tư sinh lời khác có hiệu quả cao hơn. Thực hiện bằng cách áp dụng CAATs tính toán lại toàn bộ số dư cuối ngày của các tài khoản tiền mặt để xác định đơn vị có sử dụng hiệu quả nguồn tiền nhàn rỗi.
- Kiểm tra các nghiệp vụ giao dịch tiền bất thường như: Giao dịch tiền lớn chuyển sang tài khoản cá nhân; Giao dịch ghi với giá trị âm; Giao dịch số lớn gần cuối tháng; Giao dịch với giá trị lớn một cách khác thường. Thực hiện bằng cách áp dụng CAATs lọc dữ liệu có điều kiện trên sao kê tài khoản tiền gửi của Ngân hàng cũng như sổ chi tiết tài khoản tiền gửi.

Kiểm toán khoản mục phải thu

- Kiểm tra số dư phải thu trọng yếu nhằm kiểm tra tính chính xác của khoản phải thu. Áp dụng CAATs để lọc ra các khoản phải thu lớn được thực hiện cuối kỳ, sau đó kết nối với sổ phụ tiền gửi Ngân hàng ở kỳ tiếp theo để kiểm tra số tiền phải thu có thực sự được thanh toán trong kỳ tiếp theo.

- Phân tích số dư phải thu của từng khách hàng kỳ này với kỳ trước dựa vào quy luật là khách hàng lớn thì tương ứng số dư lớn, khách hàng nhỏ tương ứng với số dư nhỏ. Quy mô của một khách hàng thông thường là tương đối ổn định, do vậy số dư phải thu từ mỗi khách hàng cũng sẽ là tương đối ổn định. Áp dụng CAATs để tính số dư phải thu của từng khách hàng qua hai kỳ liên tiếp nhằm phát hiện các trường hợp có số dư phải thu tăng đột biến để tiến hành kiểm tra chi tiết.

- Phân tích số ngày phải thu cho từng khách hàng dựa trên quy luật tỷ lệ “số dư phải thu”/“doanh thu bán hàng trong kỳ” giữa các khách hàng sẽ tương ứng với thời hạn tín dụng của khách hàng đó. Áp dụng CAATs để tính số ngày phải thu của từng khách hàng để phát hiện nếu có bất thường thì chọn mẫu kiểm tra.

- Kiểm tra tính chính xác của dự phòng khó đòi đảm bảo các khoản phải thu quá hạn cần được lập dự phòng phù hợp với quy định để đảm bảo chi phí được phản ánh kịp thời. Vì khoản mục này ảnh hưởng trực tiếp đến chi phí và lãi ròng của đơn vị nên trong nhiều trường hợp dự phòng được lập không đúng với thực tế nhằm làm tăng/giảm lãi ròng. Áp dụng CAATs để tính lại dự phòng cho từng khách hàng nhằm đảm bảo việc lập dự phòng là hoàn toàn chính xác

- Kiểm tra hạn mức phải thu khách hàng nhằm đảm bảo đơn vị không cho khách hàng vay nợ quá hạn mức phải thu tránh rủi ro nợ khó đòi. Áp dụng CAATs để kiểm tra: (i) So sánh số dư cuối kỳ với hạn mức tín dụng cấp cho khách hàng áp dụng tại thời điểm cuối kỳ; (ii) So sánh số dư lũy kế của các khách hàng lớn trong suốt năm với hạn mức tín dụng tương ứng.

Kiểm toán khoản mục TSCĐ

- Đối chiếu sổ chi tiết TSCĐ với bảng cân đối thử, BCTC nhằm đảm bảo tính chính xác của khoản mục này. Áp dụng CAATs tính toán toàn bộ tài sản cố định với cả 3 chỉ tiêu: giá vốn, khấu hao lũy kế và giá trị còn lại nhằm đảm bảo tính chính xác.

- Đối chiếu sổ chi tiết TSCĐ với biên bản kiểm kê TSCĐ nhằm đảm bảo tính tồn tại của TSCĐ. Áp dụng CAATs so khớp số liệu của hai bảng kê trên dựa trên mã của tài sản.

- Kiểm tra tính hợp lý của sổ chi tiết TSCĐ dựa trên giả thiết: TSCĐ là khoản mục có tính ổn định cao, sau khi mua về TSCĐ thường được duy trì trên sổ kế toán và khấu hao đều cho đến khi hết nguyên giá hoặc bị bán thanh lý. Hầu hết các đơn vị áp dụng khá nhất quán một số chính sách khấu hao. Trên cơ sở này có thể giả định tỷ lệ giữa chi phí khấu hao trong năm của đơn vị so với bình nguyên giá TSCĐ giữa đầu kỳ và cuối kỳ là tương đối ổn định. Tỷ lệ này có thể được so sánh với tỷ lệ tương ứng của năm trước hoặc đối chiếu với chính sách khấu hao của đơn vị. Việc phân tích có thể được chia nhỏ trên các tài khoản con để đạt độ chính xác cao hơn.

Ví dụ: Phân tích có thể tiến hành riêng trên từng nhóm chính của TSCĐ như: Nhà cửa, vật kiến trúc; Máy móc, thiết bị; Phương tiện vận tải, thiết bị truyền dẫn;

- Tính toán lại hao mòn lũy kế của TSCĐ dựa vào: Nguyên giá TSCĐ; Thời gian khấu hao; Phương pháp khấu hao. Áp dụng CAATs tính toán lại hao mòn lũy kế của TSCĐ để đảm bảo tính khớp đúng.

Kiểm toán khoản mục hàng tồn kho

- Kiểm tra số dư cuối kỳ các mặt hàng tồn kho trọng yếu nhằm phát hiện giá trị hàng tồn kho không phân bổ một cách đồng đều trên các mã hàng mà tập trung vào một số lượng nhỏ các mã hàng chính có thể là kết quả của một sai lỗi nào đó. Áp dụng CAATs vào việc chọn mẫu.

- Kiểm tra đơn giá hàng tồn kho thông qua việc tính toán lại đơn giá tồn kho theo phương pháp tính của đơn vị. Áp dụng CAATs tính toán lại toàn bộ đơn giá.

- Kiểm tra dự phòng giảm giá hàng tồn kho theo chuẩn mực kế toán hàng tồn kho không được phép phản ánh vượt quá giá trị thuần có thể thu hồi được. Áp dụng CAATs tính toán lại giá trị dự phòng dựa vào đơn giá cùng giá trị có thể thực hiện được.

- Thủ tục phân tích hàng tồn kho dựa vào đặc thù kinh doanh, mỗi đơn vị thường có một cơ cấu hàng tồn kho tương đối ổn định. Áp dụng CAATs phân tích cơ cấu trên theo các giả thiết:

- Một số mã hàng nguyên vật liệu thường xuyên chiếm tỷ trọng cao hơn hẳn trong số dư hàng tồn kho do đơn giá cao hoặc do lượng tiêu thụ trong kỳ lớn dẫn đến lượng tồn kho cao.

- Hàng bán thành phẩm có giá trị tương đối ổn định do bản chất là lượng hàng đang nằm trên dây chuyền sản xuất, nếu dây chuyền sản xuất không thay đổi quy mô thì càng không có lý do để con số này thay đổi một cách đáng kể.

- Hàng thành phẩm phục vụ cho các đơn hàng của khách hàng. Trừ khi doanh thu có biến động lớn hoặc tình hình thị trường thay đổi bất ngờ, số dư hàng thành phẩm nhìn chung cũng khá ổn định.

- Việc phân tích số lượng cũng như giá trị hàng tồn kho theo các mã hàng, phân nhóm giữa năm nay và năm trước có thể hé lộ một số biến động bất thường, nhiều khả năng là do sai sót từ phía đơn vị

- Kiểm tra tính liên tục của phiếu nhập xuất hàng tồn kho bằng cách áp dụng CAATs tìm ra các khoảng trống trong phiếu nhập xuất hàng tồn kho.

Kiểm toán khoản mục phải trả

- Kiểm tra số dư phải trả trọng yếu. Áp dụng CAATs để lọc ra các khoản phải trả lớn được thực hiện cuối kỳ, sau đó kết nối với số phụ tiền gửi Ngân hàng ở kỳ tiếp theo để kiểm tra số tiền phải trả có thực sự được thanh toán trong kỳ tiếp theo.

- Phân tích số dư phải trả của từng khách hàng kỳ này với kỳ trước. Cách làm tương tự như với số phải thu ở mục trước.

- Phân tích số ngày phải trả cho từng nhà cung cấp. Cách làm tương tự như với số phải thu ở mục trước.

- Kiểm tra hóa đơn trùng lặp nhằm phát hiện việc xuất hiện 2 hóa đơn trùng nhau trên sổ sách (bao gồm hóa đơn đã thanh toán và chưa thanh toán). Đây là dấu hiệu bất thường của một trong hai khả năng: (i) Sai sót; (ii) Gian lận (hóa đơn thanh toán 2 lần cho cùng một nhà cung cấp, 1 hóa đơn được gán cho 2 nhà cung cấp).

Kiểm toán khoản mục doanh thu

- Phân tích doanh thu của đơn vị theo từng tháng dựa vào CAATs. Trong đó tập trung phân tích vào tháng cuối kỳ của kỳ này và tháng đầu kỳ của kỳ sau nhằm phát hiện các danh thu không.

- Phân tích doanh thu theo từng khách hàng dựa vào quy mô của khách hàng đó. Áp dụng CAATs cho từng khoản mục doanh thu, phải thu qua từng năm để xem có biến động bất thường hay không?

- Kiểm tra chọn mẫu giao dịch doanh thu dựa vào CAATs để chọn mẫu tập trung vào hai tiêu chí: Mẫu lớn và của khách hàng có liên quan để đưa vào điều kiện lọc.

- Kiểm tra ghi nhận doanh thu sai niên độ kế toán thủ tục kiểm toán phải dựa trên các thời điểm xung quanh ngày 31/12 trước sau trong thời gian nhất định. Áp dụng CAATs phân tích trên tài khoản doanh thu trước sau 31/12 và các sổ phụ kế toán liên quan.

Kiểm toán giá vốn hàng bán.

- CAATs có thể được ứng dụng để tính toán lại chi phí nguyên vật liệu theo định mức nguyên vật liệu (Bill of Materials) và số lượng thành phẩm sản xuất trong kỳ, tính toán lại việc phân bổ chênh lệch giữa chi phí thực tế và định mức chi phí.

- Đối với chi phí nhân công và chi phí sản xuất chung, Kiểm toán viên Nhà nước có thể ứng dụng CAATs để tính toán lại việc phân bổ chi phí vào từng đơn vị sản phẩm.

Kiểm toán các hạng mục chi phí phát sinh.

CAATs có thể được ứng dụng để phân tích các giao dịch phát sinh chi phí trong kỳ nhằm phát hiện ra các giao dịch bất thường. Kiểm toán viên Nhà nước cũng cần phải phân tích các giao dịch phát sinh trong tháng liền kề sau năm tài chính để phát hiện ra các khoản mục chi phí hạch toán sai niên độ tài chính.

Kiểm toán viên Nhà nước cũng có thể dùng CAATs để phân tích biến động chi phí giữa các thời kỳ, tỉ trọng của từng khoản mục chi phí trên tổng chi phí.

Thuế TNDN

Kiểm toán viên Nhà nước có thể sử dụng CAATs để hỗ trợ trong việc kiểm toán khoản mục thuế TNCN. Dựa vào các định nghĩa thuế suất đang được thiết lập trong hệ thống, Kiểm toán viên Nhà nước có thể trích xuất các thông tin và sử dụng CAATs để thực hiện việc tính toán loại và so sánh với các nghiệp vụ ghi nhận thuế TNCN trong hệ thống.

Thuế GTGT

Kiểm toán viên Nhà nước có thể sử dụng CAATs để hỗ trợ trong việc kiểm toán khoản mục thuế GTGT. Dựa vào các định nghĩa thuế suất tương ứng cho từng loại hàng

hóa/dịch vụ đang được thiết lập trong hệ thống, Kiểm toán viên Nhà nước có thể trích xuất các thông tin về các nghiệp vụ bán hàng/cung cấp dịch vụ trong kỳ kiểm toán (loại giao dịch, giá trị giao dịch v.v...), và sử dụng CAATs để thực hiện việc tính toán loại và so sánh với các nghiệp vụ ghi nhận thuế GTGT trong hệ thống. Ngoài ra Kiểm toán viên Nhà nước cũng có thể sử dụng CAATs để đối chiếu sự phù hợp giữa thuế suất thuế GTGT đầu ra và thuế suất thuế GTGT đầu vào cho cùng một loại hàng hóa/dịch vụ.

Hạch toán các bút toán thủ công

Thủ tục kiểm tra các bút toán hạch toán có thể được thực hiện với sự trợ giúp của CAATs. Trong các ứng dụng Quản trị nguồn lực doanh nghiệp, sẽ có 2 loại bút toán, bao gồm:

- Bút toán thủ công: được kế toán trực tiếp định khoản. Các bút toán này thường liên quan đến các ước tính, chỉnh sửa... ở cấp độ sổ cái tổng hợp.
- Bút toán tự động: được hệ thống tạo ra ở sổ chi tiết, dựa vào loại nghiệp vụ được thiết lập trong hệ thống.

CAATs giúp Kiểm toán viên Nhà nước rà soát các bút toán hạch toán dựa trên nguyên tắc đã được định trước nhằm phát hiện các sai sót hoặc gian lận...

Ví dụ: Khi nhân viên tạo phiếu xuất kho cho một đơn hàng, hệ thống tự tạo hạch toán ghi nhận Doanh thu/Công nợ vào các số hiệu tài khoản tương ứng cho Nghiệp vụ bán hàng nội bộ, Bán cho đối tác trong nước hay xuất khẩu...

Kiểm toán viên Nhà nước có thể thu thập bảng ánh xạ tài khoản doanh thu tương ứng với từng loại nghiệp vụ bán hàng đang được cài đặt trên hệ thống, sử dụng CAATs để đối chiếu hàng loạt các bút toán trên sổ kế toán để nhận diện các nghiệp vụ bán hàng hạch toán sai tài khoản, nhận diện các bút toán thủ công v.v... để tiếp tục điều tra và mở rộng phạm vi rà soát.

Phần III – PHỤ LỤC

A. CÁC VÍ DỤ THỰC TẾ MINH HỌA CÁC KHÁI NIỆM CĂN BẢN

1. Các ví dụ thực tế về khung kiểm toán CNTT

Ví dụ 1.01 – Một số đối tượng kiểm toán của cuộc kiểm toán hệ thống TABMIS.

Các đối tượng kiểm toán có thể là:

- Hệ thống và dữ liệu của hệ thống TABMIS.
- Các kiểm soát: kiểm soát nhập liệu, kiểm soát cài đặt quy tắc cảnh báo và lưu

vết các nghiệp vụ hạch toán thu sau 31/12, cấp dự toán sau ngày 25/12 của năm ngân sách; cài đặt các tài khoản quản lý nguồn ngân sách; lưu trữ hồ sơ nhập liệu, lưu giữ các báo cáo kiểm tra định kỳ nhằm phục vụ cho việc rà soát dữ liệu đầu vào, đầu ra của TABMIS.

Ví dụ 1.02 – Kiểm toán CNTT thực hiện trong Đoàn kiểm toán báo cáo quyết toán ngân sách của một tỉnh.

Khi kiểm toán báo cáo quyết toán ngân sách của một tỉnh, kiểm toán CNTT có mục tiêu là đảm bảo tất cả thông tin tạo nên báo cáo thu chi đều lấy từ dữ liệu gốc của hệ thống như: TABMIS của KBNN, hệ thống TMS của TCT và hệ thống HQĐT của TCHQ và các hệ thống liên quan; Các thao tác hạch toán kế toán nghiệp vụ tuân theo luật Ngân sách và các văn bản pháp luật liên quan.

Ví dụ 1.03 - Kiểm toán CNTT khi kết hợp với kiểm toán tuân thủ việc xác định lượng xe đi qua trạm thu phí đường cao tốc thuộc dự án BOT.

Khi kiểm toán một trạm thu phí đường cao tốc thuộc một dự án BOT, mục tiêu kiểm toán CNTT là kiểm tra các hệ thống giám sát nội bộ (như: dữ liệu của phần mềm in vé, dữ liệu trên camera giám sát, dữ liệu giám sát trực tiếp của Tổng cục Đường bộ; Doanh số thu từ việc bán vé phải thống nhất với dữ liệu của các tài khoản tiền gửi của Ngân hàng cho vay vốn; Số hóa đơn bán vé phải liên tục tăng tuần tự không nhảy quãng theo quy định về hóa đơn do Bộ Tài chính quản lý; Các chủng loại xe gắn với bảng số xe qua trạm cũng phải thống nhất với CSDL bảng số xe của Tổng cục Đường bộ. Ngoài ra, cần xác định các dữ liệu trên có cho phép cập nhật, thay đổi hay không? Hệ thống CNTT có lưu vết mọi sự thay đổi để bảo đảm độ tin cậy và bảo mật của tài liệu gốc không?

Ví dụ 1.04 - Kiểm toán CNTT khi kết hợp với kiểm toán hoạt động dự án đầu tư Chính phủ điện tử của một Tỉnh.

Khi kiểm toán dự án Chính phủ điện tử của một tỉnh, ngoài việc kiểm tra tính tuân thủ các thủ tục triển khai dự án, mục tiêu của kiểm toán CNTT là đánh giá mức độ hiệu quả, hài lòng của hệ thống đem lại cho người dân. Cuộc kiểm toán CNTT cũng cần chỉ ra những rủi ro nếu có trong trường hợp hệ thống CNTT bị đối tượng bên ngoài tấn công kể cả tình huống nảy sinh chiến tranh mạng.

Ví dụ 1.05 - Kiểm toán CNTT hỗ trợ xây dựng CSDL chuyên ngành về các hóa đơn bất hợp pháp khi kiểm toán hệ thống CNTT của cơ quan Thuế.

Khi kiểm toán định kỳ hệ thống CNTT của cơ quan Thuế với nội dung đánh giá công tác kiểm soát danh sách các “công ty ma” lập ra để chuyên phục vụ mua bán hóa đơn bất hợp pháp, Kiểm toán viên nhà nước cần kiểm tra danh sách các công ty trên trong phần mềm chuyên dụng của cơ quan Thuế và cập nhật chúng vào CSDL chuyên ngành của Kiểm toán nhà nước phục vụ các công tác kiểm toán khác của Ngành.

Ví dụ 1.06 – Tính bảo mật, trung thực, tin cậy, khả dụng và tuân thủ theo văn bản pháp luật và các quy định của các hệ thống CNTT

Ví dụ 1.06.01 - Tính bảo mật thông tin khách hàng đi máy bay

Số điện thoại của hành khách đi máy bay cũng được xem là một dạng thông tin cần được bảo mật thay vì hiện tại đang được cung cấp cho các hãng taxi sai quy định.

Ví dụ 1.06.02 - Tính trung thực việc hạch toán trên hệ thống TABMIS

Báo cáo lưu vết các nghiệp vụ hạch toán thu sau 31/12 của năm ngân sách trên TABMIS thể hiện đầy đủ số lượng nghiệp vụ và chính xác giá trị so với thời điểm các nghiệp vụ được hạch toán trên hệ thống. Việc báo cáo lưu vết xuất từ hệ thống thể hiện thông tin không đầy đủ (thừa/thiếu nghiệp vụ) hoặc sai khác giá trị so với các nghiệp vụ đang được hạch toán trên hệ thống cho thấy hệ thống không đáng tin cậy và việc sử dụng báo cáo lưu vết để thực hiện công tác rà soát có thể dẫn đến sai sót, đặc biệt khi áp dụng phương pháp chọn mẫu kiểm tra.

Ví dụ 1.06.03 - Tính khả dụng của phần mềm kế toán dùng lập BCTC

Đơn vị sử dụng phần mềm kế toán cần lập BCTC vào cuối mỗi tháng; yêu cầu hoạt động là các dữ liệu/thông tin trong hệ thống Tài chính - Kế toán phải sẵn sàng để kế toán viên có thể thực hiện việc lập báo cáo. Khi hệ thống xảy ra sự cố (ví dụ như

cháy nổ), thông tin đó sẽ không khả dụng và mức độ ảnh hưởng đến hoạt động tùy thuộc vào kế hoạch ứng phó của từng đơn vị.

Ví dụ 1.06.04 - Tính tin cậy của hệ thống đếm xe của dự án BOT

Hệ thống đếm xe của dự án BOT không đáng tin cậy nếu số lượt xe đếm được mỗi ngày nhiều hoặc ít hơn với thực tế; và sai sót này vượt qua tỷ lệ sai sót cho phép.

Ví dụ 1.06.05 – Việc tuân thủ theo văn bản pháp luật và quy định của hệ thống CNTT lõi của ngân hàng

Hệ thống ngân hàng lõi (Core-banking) không tuân theo các quy định về phân loại nhóm nợ và xếp hạng tín dụng của Ngân hàng Nhà nước.

Ví dụ 1.07 – Các nhóm hệ thống CNTT quan trọng đối với hoạt động kiểm toán CNTT của KTNN

Các hệ thống CNTT thuộc phạm vi kiểm toán của KTNN có thể là: Phần mềm kế toán, phần mềm nhân sự của đơn vị thuộc các đầu mối kiểm toán; Hệ thống quản lý cơ sở dữ liệu của Sở Tài nguyên và Môi trường; Hệ thống CNTT của các Ngân hàng thương mại có vốn sở hữu của nhà nước; Hệ thống TABMIS của KBNN.

Ví dụ 1.07.01 - Ví dụ các hệ thống CNTT quản lý ngân sách nhà nước

- Hệ thống thông tin Quản lý Ngân sách và Kho bạc TABMIS (Treasury and Budget Management Information System) được triển khai ở các Cơ quan tài chính, KBNN và một số đơn vị sử dụng ngân sách nhà nước phục vụ công tác quản lý thông tin Ngân sách.
- Hệ thống thông tin điện tử VNACCS/VCIS (HQĐT) được triển khai ở các cơ quan hải quan.
- Hệ thống quản lý thuế tập trung TMS (Tax Management System) được triển khai ở các cơ quan Thuế.
- Hệ thống quản lý thu ngân sách TCS – được triển khai ở KBNN quản lý các thông tin thu ngân sách.

Ví dụ 1.07.02 - Thực trạng các hệ thống thông tin và cơ sở dữ liệu quốc gia

Theo thống kê của Bộ Thông tin và Truyền thông vào ngày 18/08/2015 hiện đang có 49 HTTTQG đã triển khai xong; 38 HTTTQG đang triển khai và 16 HTTTQG dự kiến triển khai trong thời gian ngắn. Ngoài ra, các hệ thống Chính phủ điện tử sẽ kết nối với các CSDL Quốc gia tập trung (Chi tiết tại Phụ lục III.C).

Ví dụ 1.07.03 - Ví dụ các hệ thống CNTT của đầu mối kiểm toán quan trọng

- Các ngân hàng đều có: hệ thống lõi xử lý nghiệp vụ ngân hàng, hệ thống lập báo cáo tài chính, hệ thống kho dữ liệu phục vụ các báo cáo quản trị.
- Các tập đoàn doanh nghiệp nhà nước lớn đều áp dụng hệ thống kế toán toàn Ngành tích hợp với các nghiệp vụ lõi để quản lý tập trung.
- Hệ thống tính tiền điện của EVN, hệ thống quản lý mua bán vé máy bay và điều hành chuyến bay của Vietnam Airline, hệ thống quản lý mua bán xăng đến từng đại lý của Petrolimex.

Thực tế, hầu hết các tỉnh thành phố đều triển khai phần mềm quản lý hồ sơ công việc tập trung toàn tỉnh. Ngoài ra, còn có phần mềm quản lý tài sản công, quản lý nhân sự tập trung toàn tỉnh.

Ví dụ 1.07.04 - Ví dụ các hệ thống CNTT được xã hội quan tâm

- Hệ thống phần mềm đếm lưu lượng xe của các dự án BOT: Đang được công luận quan tâm vì việc đếm chính xác lưu lượng xe qua trạm ảnh hưởng đến thời gian và mức phí.
- Hệ thống phần mềm liên quan đến việc tính tiền điện, nước, cước viễn thông: Đang được công luận quan tâm vì đôi khi còn tính không đúng cước và phí dịch vụ hoặc minh bạch thông tin tính cước.
- Hệ thống phần mềm liên quan đến việc tính toán chính xác nghĩa vụ tài chính liên quan đến đất đai: Đang được công luận quan tâm vì tính không chính xác các nghĩa vụ tài chính liên quan đến đất đai.
- Hệ thống phần mềm đấu thầu giá thuốc: Đang được công luận quan tâm vì hiện tượng có các công ty thuốc chất lượng và giá cả chưa hợp lý nhưng vẫn thắng thầu ...
- Hệ thống phần mềm liên quan đến việc phân phối các sản phẩm xăng dầu.

Ví dụ 1.08 – Các mục tiêu khác nhau của cuộc kiểm toán hệ thống CNTT

Ví dụ 1.08.01 - Mục tiêu khác khi tiến hành kiểm toán các Hệ thống thông tin quản lý Ngân sách nhà nước

- Cập nhật kiến thức của Kiểm toán nhà nước về hệ thống kiểm soát, cách thức lưu trữ các dữ liệu thông tin liên quan đến Ngân sách. Ví dụ: Nếu đã có kinh nghiệm và am hiểu về cách thức vận hành hệ thống TABMIS, Kiểm toán viên nhà nước có thể yêu

cầu chính xác dữ liệu từ đơn vị hoặc có thể phát hiện các sai sót trong việc cung cấp dữ liệu liên quan đến kế toán ngân sách.

- Cung cấp và cập nhật CSDL kiểm toán chuyên ngành phục vụ cho các Đoàn kiểm toán Ngân sách cần các dữ liệu liên quan. Ví dụ: Dữ liệu BCTC của tất cả các doanh nghiệp được truy xuất từ hệ thống quản lý thông tin BCTC doanh nghiệp của cơ quan thuế hoặc dữ liệu tín dụng của tất cả các doanh nghiệp được truy xuất từ hệ thống quản lý thông tin tín dụng doanh nghiệp của Ngân hàng nhà nước.

Ví dụ 1.08.02 - Mục tiêu của việc kiểm toán chuyên đề các hệ thống thông tin và CSDL quốc gia và các hệ thống CNTT được xã hội quan tâm

Mục tiêu kiểm toán:

- Đánh giá tính trung thực, đầy đủ và tuân thủ của việc xử lý thông tin nghiệp vụ xác định thuế phi nông nghiệp của các hệ thống CNTT của Cục Thuế và Sở TNMT thuộc tỉnh X.

- Đánh giá tính trung thực, đầy đủ và tuân thủ của các hệ thống CNTT của các đơn vị liên quan trong việc đếm số xe qua Trạm thu phí X.

- Đánh giá tính trung thực và tuân thủ của việc cấp phát thẻ bảo hiểm của các hệ thống CNTT thuộc cơ quan Bảo hiểm và CSDL Dân cư của tỉnh X.

- Đánh giá tính trung thực, đầy đủ và tuân thủ của việc chặn tin nhắn rác của Tổng công ty viễn thông X.

Mục tiêu chuyên môn khác có thể là:

- Khi kiểm toán phần mềm quản lý CSDL đất đai của Sở Tài Nguyên môi trường, Kiểm toán nhà nước hoàn toàn có thể vận dụng kiến thức có được để phục vụ cho các cuộc kiểm toán liên quan đến chủ đề đất đai.

- Làm giàu các CSDL chuyên ngành của Kiểm toán nhà nước. Ví dụ: Nếu Kiểm toán nhà nước tiến hành kiểm toán Ngân hàng nhà nước về các hệ thống CNTT cùng các CSDL liên quan đến tín dụng thì ngoài mục tiêu kiểm toán còn có mục tiêu riêng cho Ngành, đó là: Cập nhật thông tin tín dụng của các doanh nghiệp trên toàn quốc phục vụ cho công tác kiểm toán của Ngành từ việc kiểm toán Ngân hàng cho đến kiểm toán Thu ngân sách khi cần tra cứu thông tin tín dụng của doanh nghiệp.

Ví dụ 1.08.03 Các công ty kiểm toán danh tiếng đang đẩy mạnh kiểm toán các hệ thống CNTT liên quan đến việc xử lý thông tin tài chính của các khách hàng lớn

Trong thực tế, các công ty kiểm toán Big4 khi kiểm toán BCTC các doanh nghiệp lớn trong môi trường CNTT thường luôn tiến hành kiểm toán CNTT hệ thống CNTT quan trọng của đơn vị trước, sau đó mới tiến hành kiểm toán BCTC với sự am hiểu nhất định về môi trường CNTT của đơn vị cũng như hệ thống kiểm soát liên quan.

Ví dụ 1.09 – Các mục tiêu thực tế của dự án CNTT lĩnh vực Chính phủ điện tử

Các mục tiêu của dự án CNTT lĩnh vực Chính phủ điện tử có thể là:

- Xây dựng hệ thống điện tử thông suốt, kết nối và liên thông văn bản điện tử, dữ liệu điện tử từ Chính phủ đến cấp tỉnh, cấp huyện, cấp xã.
- Tạo lập môi trường điện tử để người dân giám sát và đóng góp cho hoạt động của chính quyền các cấp. v.v...

Ví dụ 1.10 – Các ví dụ khác nhau về kiểm toán dự án CNTT

- Kiểm toán các chương trình quốc gia về CNTT: Kiểm toán dự án CNTT thực hiện chương trình quốc gia về chứng thực điện tử và chữ ký số trong các cơ quan thuộc hệ thống nhà nước.
- Kiểm toán các dự án CNTT triển khai các hệ thống thông tin quốc gia: Kiểm toán dự án CNTT triển khai hệ thống cổng thông tin một cửa quốc gia.
- Kiểm toán việc đầu tư xây dựng Chính quyền điện tử ở các cơ quan Ngang Bộ/ Tỉnh: Kiểm toán dự án CNTT xây dựng Hệ thống thông quan tự động (VNACCS/VCIS) tại Tổng cục Hải Quan.
- Kiểm toán các dự án đầu tư CNTT thuộc các doanh nghiệp/ đơn vị sự nghiệp nhà nước: Kiểm toán dự án đầu tư hệ thống quản trị doanh nghiệp tại tập đoàn X.
- Kiểm toán các đề án nghiên cứu liên quan đến CNTT: Kiểm toán đề án nghiên cứu xây dựng thành phố thông minh của thành phố X.

Ví dụ 1.11 – Một số nội dung kiểm toán trong môi trường CNTT trong Đoàn Kiểm toán Ngân sách địa phương.

Cuộc kiểm toán báo cáo quyết toán ngân sách địa phương trong môi trường CNTT sẽ bao gồm các nội dung chính sau đây:

- Thử nghiệm hệ thống kiểm soát chung của các phần mềm liên quan đến việc lập báo cáo quyết toán ngân sách địa phương. Liên quan đến phần mềm TABMIS lập

các báo cáo thu chi, một số công việc cụ thể phải thực hiện là: Kiểm tra rà soát việc cài đặt hệ thống tài khoản dự toán quản lý các nguồn ngân sách; Kiểm tra rà soát các tỷ lệ phân chia mức thu giữa các cấp ngân sách cài đặt trong hệ thống; Kiểm tra việc lưu vết các giao dịch trong thời kỳ chính dữ liệu...

- Thử nghiệm hệ thống kiểm soát nghiệp vụ của các phần mềm liên quan đến việc lập báo cáo quyết toán ngân sách địa phương. Liên quan đến phần mềm TABMIS, một số công việc cần thực hiện là: Kiểm tra tất cả các bút toán ghi nhận khoản thu sau khi đã loại trừ ghi thu ghi chi sau ngày 31/12; Kiểm tra tất cả các bút toán cấp dự toán sau ngày 25/12; Kiểm tra tất cả các bút toán có giao dịch lớn diễn ra sau ngày 31/12; Kiểm tra tất cả các bút toán thay đổi nguồn ngân sách; ...

- Thực hiện các kỹ thuật kiểm toán với sự hỗ trợ của máy tính. Liên quan đến phần mềm TABMIS, mọi tài khoản được mã hóa bởi 12 đoạn mã và tổng số các tài khoản của 1 tỉnh có thể lên đến hàng trăm nghìn tài khoản. Việc xử lý phân tích và tiếp cận không thể thực hiện với các phần mềm xử lý thông thường mà phải có sự tham gia của các chuyên gia kiểm toán CNTT cùng phần mềm xử lý dữ liệu chuyên dụng phân tích biến động của các tài khoản gồm 12 đoạn mã qua từng năm ngân sách, qua từng thời điểm nhạy cảm của năm ngân sách bao gồm: 31/21, 31/1 năm sau, 31/03 năm sau và thời điểm lập dự thảo báo cáo quyết toán ngân sách địa phương.

2. Các ví dụ thực tế về các yếu tố cơ bản của kiểm toán CNTT

Ví dụ 2.01 – Các chốt kiểm soát thủ công, tự động và thủ công có yếu tố tự động

- Kiểm soát thủ công: Nhân viên bảo vệ phải yêu cầu người vào phòng máy chủ khai rõ họ tên và mục đích vào sổ đăng ký.
- Kiểm soát tự động: Hệ thống khóa bằng thẻ từ sẽ không mở cửa khi thẻ của nhân viên chưa được cấp quyền tiếp cận các khu vực hạn chế.
- Kiểm soát thủ công có yếu tố tự động: Định kỳ nhân viên quản lý xuất danh sách lưu vết các thay đổi trên hệ thống và yêu cầu chủ sở hữu tài khoản xác nhận có thực hiện các nội dung thay đổi đó để phòng tránh rủi ro tài khoản bị chiếm đoạt/lạm dụng, kịp thời phát hiện và xử lý các vi phạm.

Ví dụ 2.02 – Các kiểm soát chung CNTT

- Các nội dung kiểm soát chung CNTT có thể là việc phát triển và thực hiện chiến lược phát triển hệ thống CNTT và chiến lược phát triển an toàn thông tin; thiết lập hội

đồng tư vấn về CNTT; tổ chức hệ thống nhân sự vận hành hệ thống CNTT để tách bạch chồng chéo về nhiệm vụ; hoặc như lập kế hoạch cho việc phòng chống thảm họa và các sự cố bất thường.

Ví dụ 2.03 - Các ví dụ tổng quát và chi tiết về kiểm soát ứng dụng CNTT

- Tổng quát: Hệ thống tự động kiểm tra định dạng dữ liệu được nhập vào để ngăn chặn các khả năng sai sót khi nhập liệu; hoặc hệ thống tăng cường các kiểm soát giao dịch để (1) ngăn chặn người dùng thực hiện các giao dịch nằm ngoài trách nhiệm, (2) hệ thống lập ra các báo cáo chi tiết và (3) hệ thống kiểm soát giao dịch theo trị và lượng bằng việc tham chiếu tới các nguồn dữ liệu bởi các đơn vị khác nhau nhằm đảm bảo các giao dịch đã được ghi nhận đầy đủ và chính xác.

- Cụ thể: Các hệ thống thanh toán trực tuyến phải có chốt kiểm soát dữ liệu đầu vào như đảm bảo số tiền nhập vào là một số nguyên dương, không chứa chữ hoặc ký tự đặc biệt, mã hóa mọi thông tin liên quan đến thẻ thanh toán, phải kiểm tra thẻ còn hạn thanh toán hay không. Đối chiếu xem giao dịch đã được gửi/nhận đầy đủ.

Ví dụ 2.04 - Các ví dụ tiêu chí kiểm toán

- Tiêu chí của cuộc kiểm toán hệ thống CNTT của một ngân hàng nên căn cứ trên các quy định, hướng dẫn của Ngân hàng nhà nước liên quan đến các tiêu chuẩn về an toàn thông tin (ví dụ thông tư 31..), yêu cầu nghiệp vụ của các hệ thống CNTT của Ngân hàng thương mại hoạt động trên lãnh thổ Việt Nam.

- Tiêu chí có thể là các tiêu chuẩn về An toàn thông tin ISO 27001, chuẩn PCI-DSS trong trường hợp đơn vị cam kết thực hiện theo các chuẩn mực trên.

- Tiêu chí có thể là hệ thống tiêu chuẩn về quản trị CNTT COBIT 5 hiện đang được các cộng đồng doanh nghiệp lớn trên thế giới, cộng đồng kiểm toán viên nhà nước chuyên về kiểm toán CNTT, tổ chức INTOSAI công nhận.

Ví dụ 2.05 – Các ví dụ rủi ro kiểm toán CNTT.

Ví dụ 2.05.01 - Rủi ro CNTT liên quan đến Ngành

- Khi đánh giá rủi ro liên quan tới hệ thống CNTT của các bệnh viện, một trong những rủi ro ngành (y tế) là việc thông tin khám chữa của bệnh nhân đang được sử dụng để khai khống để yêu cầu bồi thường bảo hiểm xã hội. Rủi ro ngành cùng các yếu tố rủi ro khác sẽ ảnh hưởng tới nhận định và đánh giá rủi ro của kiểm toán viên kiểm toán hệ thống CNTT.

Ví dụ 2.05.02 - Rủi ro CNTT tiềm tàng

- Hệ thống CNTT lạc hậu gây nên các phép tính tự động sai. Hoặc hệ thống phần mềm hoạt động trên mạng LAN lạc hậu có rủi ro bị vi rút máy tính tấn công làm tê liệt hệ thống.

Ví dụ 2.05.03 - Rủi ro kiểm soát CNTT

- Rủi ro kiểm soát liên quan tới việc rà soát thủ công các bản lưu vết máy tính có thể cao vì những hoạt động cần được điều tra dễ bị bỏ qua do số lượng bản ghi quá lớn.