INTERNATIONAL STANDARD
TIÊU CHUẨN QUỐC TẾ

ISO/IEC 27001

First edition
2005-10-15

Second edition
2013-10-01

Third edition
2022-10-25

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

AN TOÀN THÔNG TIN, AN NINH MẠNG VÀ BẢO VỆ QUYỀN RIÊNG TƯ - HỆ THỐNG QUẢN LÝ AN TOÀN THÔNG TIN - CÁC YÊU CẦU

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

Reference number

ISO/IEC 27001 :2022 (E-V)
[BẢN DỊCH CHỈ DÙNG CHO MỤC ĐÍCH THAM KHẢO]

Lời nói đầu

ISO/IEC 27001:2022 (EV) hoàn toàn tương đương với ISO/IEC 27001:2022

Bản dịch tiếng Việt được thực hiện chỉ dùng cho mục đích tham khảo

0 Introduction

0.1 General

This document has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS). The adoption of an ISMS is a strategic decision for an organization. The establishishment and implementation of an organization's ISMS is influenced by organization's needs and objectives, security requirements, the processes employed and the size and structure of the organization. All of there influencing factors are expected to change over time.

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

This document can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.

The order in which requirements are presented in this document does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the ISMS family of standards (including ISO/IEC 27003, ISO/IEC 27004 and ISO/IEC 27005), with related terms and definitions.

0. Giới thiệu

0.1 Tổng quan

Tài liệu này được chuẩn bị nhằm cung cấp các yêu cầu cho việc thiết lập, áp dụng, duy trì và cải tiến liên tục Hệ thống quản lý An toàn thông tin (ISMS). Việc áp dụng ISMS là quyết định mang tính chiến lược của một tổ chức. Việc thiết lập và triển khai thực hiện hệ thống quản lý an toàn thông tin của một tổ chức chịu ảnh hưởng bởi các nhu cầu và các mục tiêu của tổ chức, các yêu cầu an toàn, các quá trình được sử dụng và bởi quy mô, cấu trúc của tổ chức. Tất cả các yếu tố ảnh hưởng đó có thể xảy ra sự thay đổi theo thời gian.

Hệ thống quản lý an toàn thông tin duy trì tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin bằng cách áp dụng một quá trình quản lý rủi ro và mang lại sự tin cậy cho các bên quan tâm rằng các rủi ro đã được quản lý đầy đủ.

Điều quan trọng là hệ thống quản lý an toàn thông tin phải là một phần, và được tích hợp với các quá trình và cấu trúc quản lý tổng thể của tổ chức, và an toàn thông tin cần được quan tâm trong thiết kế các quá trình, các hệ thống thông tin, và các biện pháp kiểm soát. Chắc rằng việc triển khai một hệ thống quản lý an toàn thông tin sẽ được mở rộng, thu hẹp theo nhu cầu của tổ chức.

Tài liệu này có thể được sử dụng bởi nội bộ hoặc các tổ chức bên ngoài để đánh giá khả năng của tổ chức đáp ứng các yêu cầu an toàn thông tin của tổ chức.

Thứ tự của các yêu cầu được trình bày trong tài liệu này không phản ảnh tầm quan trọng của chúng cũng như không phản ảnh hàm ý về thứ tự mà chúng trình bày. Danh sách các mục là được liệt kê dành cho mục đích tham khảo.

ISO/IEC 27000 mô tả tổng quan và từ vựng của hệ thống quản lý an toàn thông tin, viện dẫn các tiêu chuẩn của bộ tiêu chuẩn về Hệ thống quản lý an toàn thông tin (bao gồm ISO/IEC 27003, ISO/IEC 27004 and ISO/IEC 27005), với các thuật ngữ và định nghĩa liên quan.

0.2 Compatibility with other management system standards

This document applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement, and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

0.2 Tương thích với các tiêu chuẩn hệ thống quản lý khác

Tài liệu này áp dụng cấu trúc cao cấp, đồng nhất giống nhau tiêu đề các điều khoản phụ, đồng nhất về văn bản, các thuật ngữ chung, và các định nghĩa cốt lõi được định nghĩa trong Phụ lục SL của Chỉ thị ISO/IEC, Phần 1, Phụ lục hợp nhất ISO, và do đó đảm bảo duy trì khả năng tương thích với các tiêu chuẩn hệ thống quản lý khác đã áp dụng theo Phụ lục SL.

Cách tiếp cận chung được quy định tại Phụ lục SL sẽ hữu ích cho các tổ chức lựu chọn để vận hành một hệ thống quản lý duy nhất đáp ứng các yêu cầu của hai hoặc nhiều tiêu chuẩn hệ thống quản lý.

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

An toàn thông tin, an ninh mạng và bảo vệ quyền riêng tư - Hệ thống quản lý An toàn thông tin - Các yêu cầu

1 Scope

This document specifies the requirements for establishing, implementing, maintaining and continually improving an ISMS within the context of the organization. This document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

The requirements set out in this document are generic and are intended to be applicable to all organizations, regardless of type, size and nature. Excluding any of the requirements specified in Clauses 4, to 10 is not acceptable when an organization claims conformity to this document.

1. Phạm vi

Tài liệu này chỉ định rõ các yêu cầu đối với hoạt động thiết lập, áp dụng, duy trì và cải tiến liên tục một Hệ thống quản lý An toàn thông tin trong bối cảnh của tổ chức. Tài liệu này cũng bao gồm các yêu cầu cho hoạt động đánh giá và xử lý các rủi ro an toàn thông tin đáp ứng nhu cầu của tổ chức.

Các yêu cầu trình bày trong tài liệu này mang tính tổng quát và nhằm áp dụng cho tất cả các tổ chức, bất kể loại hình, qui mô, tính chất. Việc loại trừ bất kỳ yêu cầu nào trong điều 4 đến 10 đều không được chấp nhận khi tổ chức tuyên bố phù hợp với tài liệu này.

2 Normative references

The following documents, are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, Information technology — Security Techniques — Information security management systems – Overview and vocabulary

2. Tài liệu viện dẫn

Các tài liệu dưới đây, được đề cập đến trong văn bản theo cách mà một số hoặc tất cả nội dung của chúng tạo thành các yêu cầu của văn bản này. Với các trích dẫn ghi ngày tháng, chỉ có các trích dẫn được nêu mới áp dụng. Các trích dẫn không ghi ngày tháng, bản mới nhất của tài liệu trích dẫn (bao gồm cả bổ sung) được áp dụng.

ISO/IEC 27000, Công nghệ thông tin – Các kỹ thuật an toàn – Hệ thống quản lý an toàn thông tin – Tổng quan và Từ vựng

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at https://www.electropedia.org/

3. Thuật ngữ và định nghĩa

Tài liệu này sử dụng các thuật ngữ và định nghĩa của ISO/IEC 27000

ISO và IEC duy trì cơ sở dữ liệu thuật ngữ để sử dụng trong hoạt động tiêu chuẩn hóa tại các địa chỉ sau:

- Nền tảng ISO Online: có tại https://www.iso.org/obp
- IEC Electropedia: có tại https://www.electropedia.org/

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

NOTE: Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.4.1 of ISO 31000.

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

a) interested parties that are relevant to the information security management system; and

b) the relevant requirements of these interested parties;

c) which of these requirements will be addressed through the information security management system.

NOTE: The requirements of interested parties can include legal and regulatory requirements and contractual obligations.

4.3 Determining the scope of the information security management system

The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

When determining this scope, the organization shall consider:

a) the external and internal issues referred to in 4.1;

b) the requirements referred to in 4.2;

c) interfaces and dependencies between activities performed by the organisation, and those that are performed by other organisations.

The scope shall be available as documented information.

4. Bối cảnh của tổ chức

4.1 Hiểu tổ chức và bối cảnh của tổ chức

Tổ chức phải xác định các vấn đề bên ngoài và nội bộ liên quan đến mục đích của tổ chức và ảnh hưởng đến khả năng đạt được (các) kết quả dự kiến của hệ thống quản lý an toàn thông tin của tổ chức.

Chú thích: Xác định các vấn đề liên quan đến việc thiết lập bối cảnh bên ngoài và nội bộ của các tổ chức có thể xem xét tại khoản 5.4.1 của ISO 31000.

4.2 Hiểu nhu cầu và mong đợi của các bên quan tâm

Tổ chức phải xác định:

a) các bên quan tâm có liên quan đến hệ thống quản lý an toàn thông tin; và

b) các yêu cầu liên quan của các bên quan tâm này;

c) yêu cầu nào trong số này sẽ được giải quyết thông qua hệ thống quản lý an toàn thông tin.

CHÚ THÍCH: Các yêu cầu của các bên quan tâm có thể bao gồm các yêu cầu pháp lý và nghĩa vụ hợp đồng.

4.3 Xác định phạm vi của hệ thống quản lý an toàn thông tin

Tổ chức phải xác định ranh giới và phạm vi áp dụng hệ thống quản lý an toàn thông tin để thiết lập phạm vi của nó.

Khi xác định phạm vi này, tổ chức phải xem xét:

a) các vấn đề bên ngoài và nội bộ được đề cập trong 4.1;

b) các yêu cầu nêu trong 4.2;

c) những cái chung và những phần phụ thuộc giữa các hoạt động được thực hiện bởi tổ chức, và các hoạt động được thực hiện bởi các tổ chức khác.

Phạm vi sẽ phải sẵn có như một thông tin được lập văn bản.

4.4 Information security management system

The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document.

5. Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the information security management system by:

a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

b) ensuring the integration of the information security management system requirements into the organization's processes;

c) ensuring that the resources needed for the information security management system are available;

d) communicating the importance of effective information security management and of conforming to the information security management system requirements ;

e) ensuring that the information security management system achieves its in intended outcome(s);

f) directing and supporting persons to contribute to the effectiveness of the information security management system;

g) promoting continual improvement; and

h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

NOTE: Reference to "business" in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence

4.4 Hệ thống quản lý an toàn thông tin

Tổ chức phải thiết lập, áp dụng, duy trì và cải tiến liên tục hệ thống quản lý an toàn thông tin, bao gồm các quá trình cần thiết và các tương tác giữa các quá trình, phù hợp với các yêu cầu của tài liệu này.

5. Sự lãnh đạo

5.1 Sự lãnh đạo và sự cam kết

Lãnh đạo cao nhất phải chứng minh sự lãnh đạo và sự cam kết liên quan đến hệ thống quản lý an toàn thông tin thông qua việc:

a) đảm bảo chính sách an toàn thông tin và các mục tiêu an toàn thông tin được thiết lập và tương thích với các định hướng chiến lược của tổ chức;

b) đảm bảo sự tích hợp của các yêu cầu hệ thống quản lý an toàn thông tin vào các quá trình của tổ chức;

c) đảm bảo rằng các nguồn lực cần thiết cho hệ thống quản lý an toàn thông tin được đáp ứng;

d) truyền đạt tầm quan trọng của hiệu lực quản lý an toàn thông tin và sự tuân thủ với các yêu cầu hệ thống quản lý an toàn thông tin;

e) đảm bảo hệ thống quản lý an toàn thông tin đạt được (các) kết quả mong muốn;

f) chỉ đạo và hỗ trợ nhân sự tạo nên sự hiệu lực của hệ thống quản lý an toàn thông tin;

g) thúc đẩy cải tiến liên tục, và

h) hỗ trợ các vai trò quản lý khác có liên quan để chứng minh sự lãnh đạo của ban lãnh đạo tương ứng với vai trò, trách nhiệm của từng vị trí.

CHÚ THÍCH: Việc tham chiếu đến "kinh doanh" trong tài liệu này có thể được hiểu theo nghĩa rộng có nghĩa là những hoạt động cốt lõi cho mục đích tồn tại của tổ chức

5.2 Policy

Top management shall establish an information security policy that:

a) is appropriate to the purpose of the organization;

b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;

c) includes a commitment to satisfy applicable requirements related to information security; and

d) includes a commitment to continual improvement of the information security management system.

The information security policy shall:

e) be available as documented information;

f) be communicated within the organization;

g) be available to interested parties, as appropriate.

5.3 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.

Top management shall assign the responsibility and authority for:

a) ensuring that the information security management system conforms to the requirements of this document; and

b) reporting on the performance of the information security management system to top management.

NOTE: Top management can also assign responsibilities and authorities for reporting performance of the information security management system within the organization.

5.2 Chính sách

Lãnh đạo cao nhất phải thiết lập một chính sách an toàn thông tin:

a) phù hợp với mục đích của tổ chức;

b) bao gồm các mục tiêu an toàn thông tin (xem 6.2) hoặc cung cấp khuôn khổ cho việc thiết lập các mục tiêu an toàn thông tin;

c) bao gồm việc cam kết đáp ứng các yêu cầu áp dụng liên quan đến an toàn thông tin; và

d) bao gồm việc cam kết cải tiến liên tục hệ thống quản lý an toàn thông tin.

Chính sách an toàn thông tin phải:

e) sẵn có như một thông tin được lập văn bản;

f) được truyền đạt trong tổ chức;

g) sẵn có cho các bên quan tâm, hoặc khi thấy thích hợp.

5.3 Vai trò, trách nhiệm và quyền hạn

Lãnh đạo cao nhất phải đảm bảo rằng các trách nhiệm và quyền hạn cho các vai trò liên quan đến an toàn thông tin được xác định và truyền đạt.

Lãnh đạo cao nhất phải phân công trách nhiệm và quyền hạn cho việc:

a) đảm bảo rằng hệ thống quản lý an toàn thông tin phù hợp với các yêu cầu của tài liệu này, và

b) báo cáo về việc thực hiện hệ thống quản lý an toàn thông tin cho lãnh đạo cao nhất.

CHÚ THÍCH: Lãnh đạo cao nhất cũng có thể phân công các trách nhiệm và quyền hạn đối với việc báo cáo kết quả hoạt động của hệ thống quản lý an toàn thông tin trong tổ chức.

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

a) ensure the information security management system can achieve its intended outcome(s);

b) prevent, or reduce, undesired effects; and

c) achieve continual improvement.

The organization shall plan:

d) actions to address these risks and opportunities, and

e) how to

1) integrate and implement these actions into its information security management system processes; and

2) evaluate the effectiveness of these actions.

6.1.2 Information security risk assessment

The organization shall define and apply an information security risk assessment process that:

a) establishes and maintains information security risk criteria, that include:

1) the risk acceptance criteria; and

2) criteria for performing information security risk assessments;

b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;

c) identify the information security risks:

1) apply the information security risk assessment process to identify risks associated with the loss of

6. Hoạch định

6.1 Hành động để giải quyết rủi ro và các cơ hội cải tiến

6.1.1 Khái quát

Khi hoạch định hệ thống quản lý an toàn thông tin, tổ chức phải quan tâm các vấn đề được đề cập trong 4.1 và các yêu cầu nêu trong 4.2 và xác định những rủi ro và các cơ hội cải tiến cần được giải quyết để:

a) đảm bảo hệ thống quản lý an toàn thông tin có thể đạt được (các) kết quả mong muốn;

b) ngăn chặn, hoặc giảm, các tác động không mong muốn, và

c) được cải tiến liên tục.

Tổ chức phải lập kế hoạch:

d) các hành động để giải quyết các rủi ro và các cơ hội này, và

e) làm thế nào để

1) tích hợp và triển khai các hành động này vào các quá trình hệ thống quản lý an toàn thông tin của tổ chức, và

2) đánh giá tính hiệu lực của các hành động này.

6.1.2 Đánh giá rủi ro an toàn thông tin

Tổ chức phải xác định và áp dụng một quá trình đánh giá rủi ro an toàn thông tin trong đó:

a) thiết lập và duy trì các tiêu chí rủi ro an toàn thông tin, bao gồm:

1) tiêu chí chấp nhận rủi ro; và

2) tiêu chí thực hiện các cuộc đánh giá rủi ro an toàn thông tin;

b) đảm bảo rằng các cuộc đánh giá rủi ro an toàn thông tin lặp đi lặp lại tạo ra kết quả nhất quán, hợp lệ và có thể so sánh được;

c) xác định các rủi ro an toàn thông tin:

1) áp dụng quá trình đánh giá rủi ro an toàn thông tin để xác định các rủi ro liên quan tới sự mất mát của tính bảo mật, tính toàn

confidentiality, integrity and availability for information within the scope of the ISMS, and

2) identify the risk owners;

d) analyse the information security risks:

1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;

2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and.

3) determine the levels of risk;

e) evaluate the information security risks:

1) compare the rusults of risk analysis with the risk criteria established in 6.1.2 a) and

2) prioritize the analysed for risk treatment.

The organization shall retain documented information about the information security risk assessment process.

6.1.3 Information security risk treatment

The organization shall difine and apply an information security risk treatment process to:

a) select appropriate information security risk treatment options, taking account of the risk assessment results;

b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;

NOTE 1: Organizations can design controls as required, or identify them from any source.

c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;

vẹn và tính sẵn sàng của thông tin trong phạm vi của hệ thống ISMS, và

2) xác định các chủ sở hữu rủi ro;

d) phân tích các rủi ro an toàn thông tin:

1) đánh giá các hậu quả tiềm tàng sẽ xảy ra nếu các rủi ro được xác định trong 6.1.2 c) 1) trở thành hiện thực;

2) đánh giá khả năng thực tế sự xuất hiện của các rủi ro đã được xác định trong 6.1.2 c) 1); và

3) xác định các mức độ của rủi ro;

e) ước lượng rủi ro an toàn thông tin:

1) so sánh các kết quả phân tích rủi ro với các tiêu chí rủi ro đã được thiết lập trong 6.1.2 a) và

2) phân tích mức độ ưu tiên cho việc xử lý rủi ro.

Tổ chức phải lưu giữ thông tin được lập văn bản về quá trình đánh giá rủi ro an toàn thông tin.

6.1.3 Xử lý rủi ro an toàn thông tin

Tổ chức phải xác định và áp dụng một quá trình xử lý rủi ro an toàn thông tin để:

a) lựa chọn các phương pháp xử lý rủi ro an toàn thông tin thích hợp, có tính đến kết quả đánh giá rủi ro;

b) xác định tất cả các biện pháp kiểm soát cần thiết để thực hiện (các) phương án xử lý rủi ro an toàn thông tin đã lựa chọn;

CHÚ THÍCH 1: Các tổ chức có thể thiết kế các biện pháp kiểm soát theo yêu cầu, hoặc xác định chúng từ bất cứ nguồn nào.

c) so sánh các biện pháp kiểm soát đã xác định trong 6.1.3 b) ở trên với những biện pháp kiểm soát trong Phụ lục A và xác minh rằng không có biện pháp kiểm soát cần thiết nào bị bỏ qua;

NOTE 2: Annex A contains a list of possible information security controls. Users of this document are directed to Annex A to ensure that no necessary information security controls are overlooked.. Users of this document are directed to Annex A to ensure that no important control options are overlooked.

CHÚ THÍCH 2: Phụ lục A chứa một danh sách các biện pháp kiểm soát an toàn thông tin có thể có. Người sử dụng Tài liệu này được định hướng đến Phụ lục A để đảm bảo rằng không có biện pháp kiểm soát quan trọng nào bị bỏ qua.

NOTE 3: The information security controls listed in Annex A are not exhaustive and additional information security controls can be included if needed.

CHÚ THÍCH 3: Các biện pháp kiểm soát an toàn thông tin được liệt kê trong Phụ lục A là chưa đầy đủ và các biện pháp kiểm soát an toàn thông tin bổ sung có thể được đưa vào nếu cần.

d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 a), b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls in Annex A;

d) đưa ra một bản Tuyên bố áp dụng có chứa các biện pháp kiểm soát cần thiết (xem 6.1.3 a), b) và c)) và bao gồm các giải thích, cho dù chúng được triển khai hay không, và lý giải cho việc loại trừ các biện pháp kiểm soát trong Phụ lục A;

e) formulate an information security risk treatment plan;

e) xây dựng một kế hoạch xử lý rủi ro an toàn thông tin;

f) obtain risk owner’s approval of the information security risk treatment plan and the acceptance of the residual information security risks.

f) đạt được sự chấp thuận của các chủ sở hữu rủi ro về kế hoạch xử lý rủi ro an toàn thông tin và sự chấp nhận các rủi ro an toàn thông tin còn lại.

The organization shall retain documented information about the information security risk treatment process.

Tổ chức phải có trách nhiệm lưu giữ thông tin được lập văn bản về quá trình **xử lý rủi ro an toàn thông tin**.

NOTE 4: The information security risk assessment and treatment process in this document aligns with the principles and generic guidelines provided in ISO 31000.

CHÚ THÍCH 4: Quá trình đánh giá và xử lý rủi ro an toàn thông tin trong tài liệu này gắn với các nguyên tắc và hướng dẫn chung được cung cấp trong tiêu chuẩn ISO 31000.

6.2 Information security objectives and plans to achieve them

6.2 Mục tiêu an toàn thông tin và hoạch định để đạt được mục tiêu

The organization shall establish information security objectives at relevant functions and levels.

Tổ chức phải thiết lập các mục tiêu an toàn thông tin tại các cấp và bộ phận chức năng thích hợp có liên quan.

The information security objectives shall:

Các mục tiêu an toàn thông tin phải:

a) be consistent with the information security policy;

a) nhất quán với chính sách an toàn thông tin;

b) be measurable (if practicable);

b) có thể đo lường được (nếu có thể);

c) take into account applicable information

c) xem xét các yêu cầu an toàn thông tin, và các kết

security requirements, and risk assessment and treatment results;

d) be monitored;

e) be communicated;

f) be updated as appropriate;

g) be available as documented information.

The organization shall retain documented information on the information security objectives.

When planning how to achieve its information security objectives, the organization shall determine:

f) what will be done;

g) what resources will be required;

h) who will be responsible;

i) when it will be completed; and

j) how the results will be evaluated.

quả đánh giá và xử lý rủi ro;

d) được theo dõi;

e) được truyền đạt;

f) được cập nhật thích hợp.

g) sẵn có dưới dạng thông tin dạng văn bản.

Tổ chức phải lưu giữ thông tin được lập văn bản các mục tiêu an toàn thông tin.

Khi lập kế hoạch để đạt được các mục tiêu an toàn thông tin, tổ chức phải xác định:

f) những gì sẽ được thực hiện;

g) những nguồn lực sẽ được yêu cầu;

h) người sẽ chịu trách nhiệm;

i) khi nào sẽ được hoàn thành, và

j) kết quả sẽ được đo lường như thế nào.

6.3 Planning of changes

When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.

6.3 Hoạch định các thay đổi

Khi tổ chức xác định sự cần thiết phải thay đổi đối với hệ thống quản lý an toàn thông tin, thì các thay đổi này phải được thực hiện một cách có kế hoạch.

7 Support

7. Hỗ trợ

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

7.1 Nguồn lực

Tổ chức phải xác định và cung cấp các nguồn lực cần thiết cho việc thiết lập, áp dụng, duy trì và cải tiến liên tục hệ thống quản lý an toàn thông tin.

7.2 Competence

The organization shall:

a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;

b) ensure that these persons are competent on the basis of appropriate education, training, or experience;

c) where applicable, take actions to acquire the

7.2 Năng lực

Tổ chức phải:

a) xác định năng lực cần thiết của (những) người đang làm công việc mà dưới sự quản lý của họ có ảnh hưởng đến hoạt động an toàn thông tin;

b) đảm bảo rằng những người đó có đủ năng lực dựa trên cơ sở được giáo dục, đào tạo, hoặc kinh nghiệm;

c) khi thích hợp, tiến hành các hành động để có được

necessary competence, and evaluate the effectiveness of the actions taken; and

d) retain appropriate documented information as evidence of competence.

NOTE: Applicable actions can include, for example: the provision of training to, the mentoring of, or the re-assignment of current employees; or the hiring or contracting of competent persons.

7.3 Awareness

Persons doing work under the organization's control shall be aware of:

a) the information security policy;

b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and

c) the implications of not conforming with the information security management system requirements.

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the information security management system including:

a) on what to communicate;

b) when to communicate;

c) with whom to communicate;

d) how to communicate.

7.5 Documented information

7.5.1 General

The organization's information security management system shall include:

a) documented information required by this document; and

b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.

các năng lực cần thiết, và đánh giá hiệu lực của các hành động đã thực hiện; và

d) lưu giữ thông tin được lập văn bản thích hợp như bằng chứng về năng lực.

CHÚ THÍCH: Áp dụng các hành động có thể bao gồm, ví dụ: cung cấp các khóa đào tạo, các cố vấn, hoặc phân công lại vai trò của người lao động hiện hành; hoặc tuyển dụng hoặc ký hợp đồng với người đủ năng lực.

7.3 Nhận thức

Người làm công việc dưới sự quản lý của tổ chức phải có nhận thức về:

a) chính sách an toàn thông tin;

b) việc đóng góp của họ vào hiệu lực của hệ thống quản lý an toàn thông tin, bao gồm cả các lợi ích của sự cải tiến hoạt động thực hiện an toàn thông tin; và

c) những hệ quả của việc không thực hiện phù hợp với các yêu cầu của hệ thống quản lý an toàn thông tin.

7.4 Trao đổi thông tin

Tổ chức phải xác định nhu cầu trao đổi thông tin nội bộ và bên ngoài có liên quan đến hệ thống quản lý an toàn thông tin bao gồm:

a) trao đổi thông tin gì;

b) trao đổi thông tin khi nào;

c) trao đổi thông tin với ai;

d) cách thức trao đổi thông tin.

7.5 Thông tin được lập văn bản

7.5.1 Khái quát

Hệ thống quản lý an toàn thông tin của tổ chức phải bao gồm:

a) thông tin được lập văn bản theo yêu cầu của tài liệu này, và

b) thông tin được lập văn bản được xác định bởi tổ chức như là sự cần thiết cho tính hiệu lực của hệ thống quản lý an toàn thông tin.

NOTE: The extent of documented information for an information security management system can differ from one organization to another due to:

1) the size of organization and its type of activities, processes, products and services;

2) the complexity of processes and their interactions; and

3) the competence of persons.

7.5.2 Creating and updating

When creating and updating documented information the organization shall ensure appropriate:

a) identification and description (e.g. a title, date, author, or reference number);

b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and

c) review and approval for suitability and adequacy.

7.5.3 Control of documented information

Documented information required by the information security management system and by this document shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed; and

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:

c) distribution, access, retrieval and use;

d) storage and preservation, including the preservation of legibility;

e) control of changes (e.g. version control); and

f) retention and disposition.

Documented information of external origin, determined by the organization to be necessary for

CHÚ THÍCH: Mức độ thông tin được lập văn bản cho một hệ thống quản lý an toàn thông tin có thể khác nhau giữa các tổ chức phụ thuộc vào:

1) quy mô của tổ chức và loại hình hoạt động, quy trình, sản phẩm và dịch vụ của tổ chức;

2) sự phức tạp và sự tương tác của các quá trình; và

3) năng lực của con người.

7.5.2 Khởi tạo và cập nhật

Khi khởi tạo và cập nhật thông tin được lập văn bản tổ chức phải đảm bảo thích hợp:

a) định danh và mô tả (ví dụ như tiêu đề, ngày tháng, tác giả, hoặc mã số tài liệu);

b) định dạng (ví dụ như ngôn ngữ, phiên bản phần mềm, đồ họa) và phương tiện (ví dụ như giấy, điện tử); và

c) xem xét và phê duyệt cho thích hợp và thỏa đáng.

7.5.3 Quản lý thông tin được lập văn bản

Thông tin được lập văn bản theo yêu cầu của hệ thống quản lý an toàn thông tin và tài liệu này phải được kiểm soát để đảm bảo:

a) sẵn có và phù hợp để sử dụng bất kỳ ở đâu và khi nào cần thiết; và

b) được bảo vệ đầy đủ (ví dụ bảo vệ khỏi mất tính bảo mật, sử dụng không đúng cách, hoặc mất tính toàn vẹn).

Đối với việc kiểm soát thông tin được lập văn bản, tổ chức phải quan tâm đến các hoạt động sau đây, có thể áp dụng:

c) phân phối, truy cập, thu hồi và sử dụng;

d) lưu trữ và bảo quản, bao gồm cả việc duy trì tính rõ ràng;

e) kiểm soát các thay đổi (ví dụ như kiểm soát phiên bản); và

f) duy trì và hủy bỏ.

Thông tin lập văn bản có nguồn gốc bên ngoài mà tổ chức xác định là cần thiết cho việc hoạch định và vận hành hệ

the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

NOTE: Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

thống quản lý an toàn thông tin, phải được nhận biết thích hợp, và được kiểm soát.

CHÚ THÍCH: Thuật ngữ Truy cập bao hàm ý nghĩa một quyết định liên quan đến việc cho phép chỉ xem thông tin được lập văn bản, hoặc sự cho phép và thẩm quyền để xem và thay đổi thông tin được lập văn bản, vv

8 Operation

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in Clause 6, by:

- establishing criteria for processes;
- implementing control of processes in accordance with the criteria.

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.

8.2 Information security risk assessment

The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a).

The organization shall retain documented information of the results of the information security risk assessments.

8.3 Information security risk treatment

The organization shall implement the information security risk treatment plan.

The organization shall retain documented information of the results of the information security risk treatment.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization shall evaluate the information

8. Điều hành

8.1 Hoạch định và kiểm soát hoạt động

Tổ chức phải lập kế hoạch, thực hiện và kiểm soát các quy trình cần thiết để đáp ứng yêu cầu an toàn thông tin, và triển khai các hoạt động đã xác định trong Điều 6, thông qua:

- thiết lập các tiêu chí cho các quá trình;
- thực hiện kiểm soát các quá trình phù hợp với các tiêu chí.

Thông tin dạng văn bản sẽ sẵn có ở mức độ cần thiết để đảm bảo tin cậy rằng các quá trình đã được tiến hành theo kế hoạch.

Tổ chức phải kiểm soát các thay đổi kế hoạch và xem xét các hậu quả của sự thay đổi ngoài ý muốn, có hành động để giảm thiểu bất kỳ tác dụng phụ nào, khi cần thiết.

Tổ chức phải đảm bảo rằng các quá trình, sản phẩm hoặc dịch vụ được cung cấp bởi bên ngoài có liên quan đến hệ thống quản lý an toàn thông tin được kiểm soát.

8.2 Đánh giá rủi ro an toàn thông tin

Tổ chức phải thực hiện đánh giá rủi ro an toàn thông tin trong khoảng thời gian theo kế hoạch hoặc khi có những thay đổi quan trọng theo dự kiến hoặc đã xảy ra, có tính đến các tiêu chí thiết lập trong 6.1.2 a).

Tổ chức có trách nhiệm lưu giữ thông tin được lập văn bản các kết quả của đánh giá rủi ro an toàn thông tin.

8.3 Xử lý rủi ro an toàn thông tin

Tổ chức phải triển khai kế hoạch xử lý rủi ro an toàn thông tin.

Tổ chức phải lưu giữ thông tin được lập văn bản các kết quả của các quá trình xử lý rủi ro an toàn thông tin.

9. Đánh giá hiệu quả

9.1 Giám sát, đo lường, phân tích và đánh giá

Tổ chức phải đánh giá sự thực thi và tính hiệu lực của hệ

security performance and the effectiveness of the information security management system.

The organization shall determine:

a) what needs to be monitored and measured, including information security processes and controls;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results; The methods selected should produce comparable and reproducible results to be considered valid.

c) when the monitoring and measuring shall be performed;

d) who shall monitor and measure;

e) when the results from monitoring and measurement shall be analyzed and evaluated; and

f) who shall analyse and evaluate these results.

Documented information shall be available as evidence of the results.

The organization shall evaluate the information security performance and the effectiveness of the information security management system.

9.2 Internal audit

9.2.1 General

The organization shall conduct internal audits at planned intervals to provide information on whether the ISMS:

a) conform to 1) the organization's own requirements for its information security management system; and 2) the requirements of this document;

b) are effectively implemented and maintained.

9.2.2 Internal audit programme

The organization shall plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s)

thống quản lý an toàn thông tin.

Tổ chức phải xác định:

a) những gì cần phải được giám sát và đo lường, bao gồm các quá trình và các biện pháp kiểm soát an toàn thông tin;

b) các phương pháp giám sát, đo lường, phân tích và đánh giá, nếu có, để đảm bảo kết quả hợp lệ; Các phương pháp được lựa chọn cần tạo ra kết quả có thể so sánh được và có thể tái sử dụng, được coi là hợp lệ.

c) khi nào hoạt động giám sát và đo lường được thực hiện;

d) ai phải thực hiện giám sát và đo lường;

e) khi nào các kết quả từ giám sát và đo lường được phân tích và đánh giá; và

f) ai phải phân tích và đánh giá các kết quả này.

Thông tin dạng văn bản phải sẵn có làm bằng chứng về kết quả giám sát và đo lường.

Tổ chức phải đánh giá việc thực hiện an toàn thông tin và tính hiệu lực của hệ thống quản lý an toàn thông tin.

9.2 Đánh giá nội bộ

9.2.1 Khái quát

Tổ chức phải tiến hành các hoạt động đánh giá nội bộ định kỳ theo kế hoạch để cung cấp thông tin xem hệ thống ISMS có:

a) phù hợp với 1) yêu cầu của chính tổ chức về hệ thống quản lý an toàn thông tin của mình, và 2) với các yêu cầu của Tài liệu này.

b) được thực hiện và duy trì có hiệu lực.

9.2.2 Chương trình đánh giá nội bộ

Tổ chức phải lập kế hoạch, thiết lập, triển khai và duy trì (các) chương trình đánh giá, bao gồm tần suất, phương pháp, trách nhiệm, yêu cầu lập kế hoạch và báo cáo. Chương trình đánh giá có tính đến tầm quan trọng của các

shall take into consideration the importance of the processes concerned and the results of previous audits;

quá trình có liên quan và kết quả các cuộc đánh giá trước đó;

The organization shall

a) define the audit criteria and scope for each audit;

b) select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;

c) ensure that the results of the audits are reported to relevant management; and

Tổ chức phải:

a) xác định các tiêu chí đánh giá và phạm vi cho từng cuộc đánh giá;

b) lựa chọn đánh giá viên và thực hiện việc đánh giá đảm bảo tính khách quan và công bằng của quá trình đánh giá;

c) đảm bảo rằng các kết quả của cuộc đánh giá được báo cáo đến các cấp quản lý có liên quan; và

Documented information shall be available as evidence of the audit programme(s) and the audit results.

Thông tin được lập văn bản phải sẵn có làm bằng chứng về việc thực hiện (các) chương trình đánh giá và các kết quả đánh giá.

9.3 Management review

9.3 Xem xét của lãnh đạo

9.3.1 General

Top Management shall review the organization's ISMS at planned intervals to ensure itscontinuing suitability, adequacy and effectiveness.

9.3.1 Khái quát

Lãnh đạo cao nhất phải xem xét định kỳ theo kế hoạch hệ thống ISMS của tổ chức để đảm bảo nó luôn phù hợp, thoả đáng và có hiệu lực.

9.3.2 Management review inputs

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the information security management system;

c) changes in needs and expectations of interested parties that are relevant to the information security management system;

d) feedback on the information security performance, including trends in:

1) nonconformities and corrective actions;

2) monitoring and measurement results;

3) audit results; and

4) fulfilment of information security

9.3.2 Đầu vào xem xét của lãnh đạo

Việc xem xét của lãnh đạo phải bao gồm sự xem xét:

a) tình trạng của các hành động từ lần xem xét lãnh đạo trước đó;

b) các thay đổi trong các vấn đề bên ngoài và nội bộ có liên quan đến hệ thống quản lý an toàn thông tin;

c) những thay đổi về nhu cầu và mong đợi của các bên quan tâm có liên quan đến hệ thống quản lý an toàn thông tin;

d) phản hồi về việc thực hiện an toàn thông tin, bao gồm:

1) các sự không phù hợp và các hành động khắc phục;

2) các kết quả giám sát và đo lường;

3) các kết quả đánh giá; và

4) sự đáp ứng các mục tiêu an toàn thông tin;

objectives;

e) feedback from interested parties;

f) results of risk assessment and status of risk treatment plan; and

g) opportunities for continual improvement.

9.3.3 Management review results

The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

Documented information shall be available as evidence of the results of management reviews.

e) thông tin phản hồi từ các bên quan tâm;

f) kết quả đánh giá rủi ro và tình trạng của kế hoạch xử lý rủi ro; và

g) các cơ hội cải tiến liên tục.

9.3.3 Kết quả xem xét của lãnh đạo

Kết quả xem xét của lãnh đạo phải bao gồm những quyết định liên quan đến các cơ hội cải tiến liên tục và bất cứ nhu cầu cần thiết nào cho các thay đổi đối với hệ thống quản lý an toàn thông tin.

Thông tin được lập văn bản phải sẵn có làm bằng chứng về kết quả của các cuộc xem xét của lãnh đạo.

10 Improvement

10.1 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the ISMS.

10.2 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:

1) take action to control and correct it; and

2) deal with the consequences;

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:

1) reviewing the nonconformity;

2) determining the causes of the nonconformity; and

3) determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken; and

e) make changes to the information security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

Documented information shall be available as evidence of:

f) the nature of the nonconformities and any subsequent actions taken, and

g) the results of any corrective action.

10. Cải tiến

10.1 Cải tiến liên tục

Tổ chức phải liên tục cải tiến nâng cao tính thích hợp, đầy đủ và hiệu lực của hệ thống quản lý an toàn thông tin.

10.2 Sự không phù hợp và hành động khắc phục

Khi xảy ra sự không phù hợp, tổ chức phải:

a) phản ứng với sự không phù hợp, và có thể áp dụng:

1) có hành động để kiểm soát và sửa chữa nó; và

2) giải quyết các hậu quả;

b) đánh giá sự cần thiết phải hành động để loại bỏ nguyên nhân của sự không phù hợp, để nó không tái xuất hiện hay xảy ra ở những nơi khác, bằng cách:

1) xem xét sự không phù hợp;

2) xác định nguyên nhân của sự không phù hợp; và

3) xác định nếu có sự không phù hợp tương tự tồn tại, hoặc có khả năng có thể xảy ra;

c) thực hiện bất kỳ hành động cần thiết nào;

d) xem xét hiệu lực của bất kỳ hành động khắc phục đã thực hiện; và

e) thay đổi hệ thống quản lý an toàn thông tin, nếu cần thiết.

Hành động khắc phục phải phù hợp với ảnh hưởng của sự không phù hợp gặp phải.

Thông tin được lập văn bản phải sẵn có làm bằng chứng về:

f) bản chất của sự không phù hợp và bất kỳ hành động tiếp theo nào được thực hiện, và

g) kết quả của các hành động khắc phục.

Annex A

(normative)

Information Security controls reference

The Information Security controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2022, Clauses 5 to 8, and shall be used in context with Clause 6.1.3.

Phụ lục A

(quy định)

Các biện pháp kiểm soát an toàn thông tin tham khảo

Các biện pháp kiểm soát an toàn thông tin được liệt kê trong bảng A.1 bắt nguồn trực tiếp và có liên kết với các mục từ mục 5 đến 8 được liệt kê trong ISO/IEC27002:2022 và phải được sử dụng trong bối cảnh của điều khoản 6.1.3.

Table A.1 – Information Security controls

Bảng A.1- Các biện pháp kiểm soát an toàn thông tin

A.5 Organizational controls – ***Các biện pháp kiểm soát về tổ chức***		
A.5.1	Policies for information security	Chính sách an toàn thông tin
A.5.2	Information security roles and responsibilities	Vai trò và trách nhiệm an toàn thông tin
A.5.3	Segregation of duties	Phân tách nhiệm vụ
A.5.4	Management responsibilities	Trách nhiệm của lãnh đạo
A.5.5	Contact with authorities	Thiết lập và duy trì liên lạc với các cơ quan chức năng
A.5.6	Contact with special interest groups	Liên lạc thường xuyên với các nhóm chuyên gia
A.5.7	Threat intelligence	Cập nhật thông tin tình báo về các mối đe dọa
A.5.8	Information security in project management	An toàn thông tin trong quản lý dự án
A.5.9	Inventory of information and other associated assets	Kiểm kê thông tin và các tài sản liên quan khác
A.5.10	Acceptable use of information and other associated assets	Việc sử dụng thông tin và các tài sản liên quan khác được chấp nhận
A.5.11	Return of assets	Hoàn trả tài sản
A.5.12	Classification of information	Phân loại thông tin
A.5.13	Labelling of information	Ghi nhãn thông tin
A.5.14	Information transfer	Chuyển giao thông tin
A.5.15	Access control	Kiểm soát truy cập
A.5.16	Identity management	Quản lý danh tính
A.5.17	Authentication information	Thông tin xác thực
A.5.18	Access rights	Quyền truy cập

A.5.19	Information security in supplier relationships	An toàn thông tin trong các mối quan hệ với nhà cung cấp
A.5.20	Addressing information security within supplier agreements	Giải quyết vấn đề an toàn thông tin trong các thỏa thuận với nhà cung cấp
A.5.21	Managing information security in the ICT supply chain	Quản lý an toàn thông tin trong chuỗi cung ứng CNTT-TT
A.5.22	Monitoring, review and change management of supplier services	Giám sát, xem xét và quản lý thay đổi các dịch vụ của nhà cung cấp
A.5.23	Information security for use of cloud services	An toàn thông tin khi sử dụng các dịch vụ đám mây
A.5.24	Information security incident management planning and preparation	Lập kế hoạch và chuẩn bị quản lý sự cố an toàn thông tin
A.5.25	Assessment and decision on information security events	Đánh giá và quyết định các sự kiện an toàn thông tin
A.5.26	Response to information security incidents	Ứng phó sự cố an toàn thông tin
A.5.27	Learning from information security incidents	Rút kinh nghiệm từ các sự cố an toàn thông tin
A.5.28	Collection of evidence	Thu thập bằng chứng
A.5.29	Information security during disruption	An toàn thông tin trong thời gian gián đoạn
A.5.30	ICT readiness for business continuity	Sẵn sàng về CNTT-TT cho hoạt động kinh doanh liên tục
A.5.31	Legal, statutory, regulatory and contractual requirements	Các yêu cầu pháp lý, luật định, quy định và hợp đồng
A.5.32	Intellectual property rights	Quyền sở hữu trí tuệ
A.5.33	Protection of records	Bảo vệ hồ sơ
A.5.34	Privacy and protection of PII	Quyền riêng tư và bảo vệ thông tin định danh cá nhân
A.5.35	Independent review of information security	Xem xét độc lập về an toàn thông tin
A.5.36	Compliance with policies, rules and standards for information security	Tuân thủ các chính sách, quy tắc và tiêu chuẩn về an toàn thông tin
A.5.37	Documented operating procedures	Quy trình vận hành được lập thành văn bản

A.6 People controls – *Các biện pháp kiểm soát về con người*		
A.6.1	Screening	Sàng lọc
A.6.2	Terms and conditions of employment	Điều khoản và điều kiện làm việc
A.6.3	Information security awareness, education and training	Nhận thức, giáo dục và đào tạo về an toàn thông tin
A.6.4	Disciplinary process	Quy trình xử lý kỷ luật
A.6.5	Responsibilities after termination or change of employment	Trách nhiệm sau khi thôi việc hoặc thay đổi công việc
A.6.6	Confidentiality or non-disclosure agreements	Thỏa thuận bảo mật hoặc không tiết lộ thông tin
A.6.7	Remote working	Làm việc từ xa
A.6.8	Information security event reporting	Báo cáo sự kiện an toàn thông tin
A.7 Physical controls – *Các biện pháp kiểm soát về vật lý*		
A.7.1	Physical security perimeters	Các vành đai an ninh vật lý
A.7.2	Physical entry	Cổng ra vào vật lý
A.7.3	Securing offices, rooms and facilities	Bảo vệ văn phòng, phòng và cơ sở vật chất
A.7.4	Physical security monitoring	Giám sát an ninh vật lý
A.7.5	Protecting against physical and environmental threats	Bảo vệ chống lại các mối đe dọa vật lý và môi trường
A.7.6	Working in secure areas	Làm việc trong các khu vực an toàn
A.7.7	Clear desk and clear screen	Bàn sạch và màn hình sạch
A.7.8	Equipment siting and protection	Bố trí và bảo vệ thiết bị
A.7.9	Security of assets off-premises	An toàn tài sản bên ngoài trụ sở
A.7.10	Storage media	Phương tiện lưu trữ
A.7.11	Supporting utilities	Các tiện ích hỗ trợ
A.7.12	Cabling security	An toàn dây cáp
A.7.13	Equipment maintenance	Bảo trì thiết bị
A.7.14	Secure disposal or re-use of equipment	Xử lý hoặc tái sử dụng thiết bị an toàn

A.8 Technological controls – *Các biện pháp kiểm soát về kỹ thuật*		
A.8.1	User endpoint devices	Thiết bị đầu cuối của người dùng
A.8.2	Privileged access rights	Quyền truy cập đặc quyền
A.8.3	Information access restriction	Hạn chế truy cập thông tin
A.8.4	Access to source code	Truy cập mã nguồn
A.8.5	Secure authentication	Xác thực an toàn
A.8.6	Capacity management	Quản lý năng lực
A.8.7	Protection against malware	Bảo vệ chống lại phần mềm độc hại
A.8.8	Management of technical vulnerabilities	Quản lý các lỗ hổng kỹ thuật
A.8.9	Configuration management	Quản lý cấu hình
A.8.10	Information deletion	Xóa thông tin
A.8.11	Data masking	Che dấu dữ liệu
A.8.12	Data leakage prevention	Ngăn chặn rò rỉ dữ liệu
A.8.13	Information backup	Sao lưu thông tin
A.8.14	Redundancy of information processing facilities	Dự phòng các phương tiện xử lý thông tin
A.8.15	Logging	Ghi nhật ký
A.8.16	Monitoring activities	Các hoạt động giám sát
A.8.17	Clock synchronization	Đồng bộ thời gian
A.8.18	Use of privileged utility programs	Sử dụng các chương trình tiện ích đặc quyền
A.8.19	Installation of software on operational systems	Cài đặt phần mềm trên các hệ điều hành
A.8.20	Networks security	An toàn mạng
A.8.21	Security of network services	An toàn các dịch vụ mạng
A.8.22	Segregation of networks	Phân tách mạng
A.8.23	Web filtering	Lọc web
A.8.24	Use of cryptography	Sử dụng mật mã
A.8.25	Secure development life cycle	Vòng đời phát triển an toàn
A.8.26	Application security requirements	Yêu cầu an toàn ứng dụng
A.8.27	Secure system architecture and engineering principles	Kiến trúc hệ thống an toàn và các nguyên tắc kỹ thuật

A.8.28	Secure coding	Mã hóa an toàn
A.8.29	Security testing in development and acceptance	Kiểm tra bảo mật trong quá trình phát triển và chấp nhận
A.8.30	Outsourced development	Phát triển thuê ngoài
A.8.31	Separationofdevelopment,testandproductionenvironments	Phân tách môi trường phát triển, kiểm thử và sản xuất
A.8.32	Change management	Quản lý thay đổi
A.8.33	Test information	Thông tin kiểm tra
A.8.34	Protection of information systems during audit testing	Bảo vệ hệ thống thông tin trong quá trình kiểm tra đánh giá

**Nội dung chi tiết các biện pháp kiểm soát và các hướng dẫn thực hiện kiểm soát, xin tham khảo bản dịch Tiếng Việt của ISO/IEC 27002:2022.*

Bibliography

[1] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

[2] ISO/IEC 27003, *Information technology — Security techniques — Information security management systems — Guidance*

[3] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*

[4] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[5] ISO 31000:2018, *Risk management — Guidelines*