BA tài liệu sau đây, toàn bộ hoặc một phần, được tham chiếu theo chuẩn mực với nhau trong từng tài liệu và không thể thiếu cho việc áp dụng từng tài liệu:

TIÊU CHUẨN ISO/IEC 27000, ISO/IEC 27001 và ISO/IEC 27002

INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

INTERNATIONAL STANDARD

ISO/IEC 27002

Second edition
2013-10-01

Information technology — Security techniques — Code of practice for information security controls

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information

INTERNATIONAL STANDARD

ISO/IEC 27000

Fifth edition
2018-02

Information technology — Security techniques — Information security management systems — Overview and vocabulary

Annex A
(normative)
Reference control objectives and controls

The control objectives and controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2013[1], Clauses 5 to 18 and are to be used in context with Clause 6.1.3.

Table A.1 — Control objectives and controls

ISO/IEC 27001:2013		**Trang 10**
A.5 Information security policies		
A.5.1 Management direction for information security		
Objective *(mục tiêu)* **: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.**		
A.5.1.1	**Policies for information security**	**Control** *(biện pháp kiểm soát)* **A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.**
…	*(còn nữa)*	

ĐỐI CHIẾU ISO 27001 VỚI ISO 27002 KHI KIỂM TOÁN ATTT / TRIỂN KHAI ATTT

ISO/IEC 27002:2013		**Trang 2**
5.1.1 Policies for information security **Control** *(biện pháp kiểm soát)* **A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.** **Implementation guidance** ***(Hướng dẫn (cách) thực hiện/triển khai)*** **At the highest level, organizations should define an "information security policy" which is approved by management and which sets out the organization's approach to managing its information security objectives. Information security policies should address requirements created by:** **a) business strategy;** **b) regulations, legislation and contracts;** **c) the current and projected information security threat environment.** *[Tạm dịch: **Ở cấp độ cao nhất, các tổ chức nên xác định "chính sách bảo mật thông tin" được ban quản lý phê duyệt và nêu rõ cách tiếp cận của tổ chức đối với việc quản lý các mục tiêu bảo mật thông tin của mình. Các chính sách bảo mật thông tin nên giải quyết các yêu cầu do:*** ***a) chiến lược kinh doanh;*** ***b) các quy định, luật pháp và hợp đồng tạo ra;*** ***c) môi trường đe dọa bảo mật thông tin hiện tại và dự kiến.]*** ... *(còn nữa)*		
…		

(*)Xem slide số 45, 46 và 47 tập tin giáo trình Chương 2 - QLRRATTT_Ch.02_v4.2.pdf

ISO/IEC 27001:2013		Trang 10
A.6 Organization of information security		
A.6.1 Internal organization		
Objective *(mục tiêu)*: **To establish a management framework to initiate and control the implementation and operation of information security within the organization.**		
A.6.1.1	**Information security roles and responsibilities**	**Control** *(biện pháp kiểm soát)* **All information security responsibilities shall be defined and allocated.**
	(còn nữa)	

ĐỐI CHIẾU ISO 27001 VỚI ISO 27002 KHI KIỂM TOÁN ATTT / TRIỂN KHAI ATTT

ISO/IEC 27002:2013	Trang 4
6.1.1 Information security roles and responsibilities **Control** *(biện pháp kiểm soát)* **All information security responsibilities should be defined and allocated.** **Implementation guidance** ***(Hướng dẫn (cách) thực hiện/triển khai)*** **Allocation of information security responsibilities should be done in accordance with the information security policies (see 5.1.1). Responsibilities for the protection of individual assets and for carrying out specific information security processes should be identified. Responsibilities for information security risk management activities and in particular for acceptance of residual risks should be defined....** *(còn nữa)*	
…	

ISO/IEC 27001:2013		Trang 10 và 11
A.6.2 Mobile devices and teleworking		
Objective *(mục tiêu)*: **To ensure the security of teleworking and use of mobile devices.**		
A.6.2.1	**Mobile device policy**	**Control** *(biện pháp kiểm soát)* **A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.**
	(còn nữa)	

ĐỐI CHIẾU ISO 27001 VỚI ISO 27002 KHI KIỂM TOÁN ATTT / TRIỂN KHAI ATTT

ISO/IEC 27002:2013	Trang 6
6.2 Mobile devices and teleworking **Objective** *(mục tiêu)*: **To ensure the security of teleworking and use of mobile devices.** **6.2.1 Mobile device policy** **Control** *(biện pháp kiểm soát)* **A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.** **Implementation guidance** ***(Hướng dẫn (cách) thực hiện/triển khai)*** **When using mobile devices, special care should be taken to ensure that business information is not compromised. The mobile device policy should take into account the risks of working with mobile devices in unprotected environments. The mobile device policy should consider:** **a) registration of mobile devices;** **b) requirements for physical protection;** **c) restriction of software installation;** **d) …** *(còn nữa)*	
…	

(*)Xem slide số 48, 49, 50, 51 và 52 tập tin giáo trình Chương 2 - QLRRATTT_Ch.02_v4.2.pdf

ISO/IEC 27001:2013		Trang 11
A.7 Human resource security		
A.7.2 During employment		
Objective *(mục tiêu)*: **To ensure that employees and contractors are aware of and fulfil their information security responsibilities**		
A.7.2.2	**Information security awareness, education and training**	**Control** *(biện pháp kiểm soát)* **All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function**
…	*(còn nữa)*	

ĐỐI CHIẾU ISO 27001 VỚI ISO 27002 KHI KIỂM TOÁN ATTT / TRIỂN KHAI ATTT

ISO/IEC 27002:2013	Trang 11

7.2.2 Policies for information security

Control *(biện pháp kiểm soát)*

All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

Implementation guidance ***(Hướng dẫn (cách) thực hiện/triển khai)***

An information security awareness programme should aim to make employees and, where relevant, contractors aware of their responsibilities for information security and the means by which those responsibilities are discharged.

An information security awareness programme should be established in line with the organization's information security policies and relevant procedures, taking into consideration the organization's information to be protected and the controls that have been implemented to protect the information.

*[Tạm dịch: **Một chương trình nâng cao nhận thức về an ninh thông tin phải hướng đến mục tiêu giúp nhân viên và, nếu có thể, các nhà thầu nhận thức được trách nhiệm của họ đối với an ninh thông tin và các phương tiện để thực hiện các trách nhiệm đó.***

Một chương trình nâng cao nhận thức về an ninh thông tin phải được thiết lập phù hợp với các chính sách an ninh thông tin và các quy trình có liên quan của tổ chức, đồng thời xem xét thông tin cần được bảo vệ của tổ chức và các biện pháp kiểm soát đã được triển khai để bảo vệ thông tin.]

...

(còn nữa)

…		

(*)Xem slide số 53, 54 và 55 tập tin giáo trình Chương 2 - QLRRATTT_Ch.02_v4.2.pdf

ISO/IEC 27001:2013		Trang 11 và 12
A.8 Asset management		
A.8.1 Responsibility for assets		
Objective *(mục tiêu)*: **To identify organizational assets and define appropriate protection responsibilities.**		
A.8.1.4	**Return of assets**	**Control** *(biện pháp kiểm soát)* **All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement**
	(còn nữa)	

ĐỐI CHIẾU ISO 27001 VỚI ISO 27002 KHI KIỂM TOÁN ATTT / TRIỂN KHAI ATTT

ISO/IEC 27002:2013	Trang 15

8.1.4 Return of assets

Control *(biện pháp kiểm soát)*

All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement.

Implementation guidance ***(Hướng dẫn (cách) thực hiện/triển khai)***

The termination process should be formalized to include the return of all previously issued physical and electronic assets owned by or entrusted to the organization.

(còn nữa)

…

ISO/IEC 27001:2013	Trang 12

A.8.2 Information classification

Objective *(mục tiêu)*: **To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.**

A.8.2.1	**Classification of information**	**Control** *(biện pháp kiểm soát)* **Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification**
	(còn nữa)	

ĐỐI CHIẾU ISO 27001 VỚI ISO 27002 KHI KIỂM TOÁN ATTT / TRIỂN KHAI ATTT

ISO/IEC 27002:2013	Trang 15 và 16

8.2 Information classification

Objective *(mục tiêu)*: **To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.**

8.2.1 Classification of information

Control *(biện pháp kiểm soát)*

Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

Implementation guidance ***(Hướng dẫn (cách) thực hiện/triển khai)***

(…) Owners of information assets should be accountable for their classification.

Classification should be included in the organization's processes, and be consistent and coherent across the organization. Results of classification should indicate value of assets depending on their sensitivity and criticality to the organization, e.g. in terms of confidentiality, integrity and availability.

*[**Tạm dịch:** (…) Chủ sở hữu tài sản thông tin phải chịu trách nhiệm về việc phân loại thông tin. Phân loại phải được đưa vào các quy trình của tổ chức và phải nhất quán và mạch lạc trong toàn tổ chức. Kết quả phân loại phải chỉ ra giá trị của tài sản tùy thuộc vào mức độ nhạy cảm và tính quan trọng của chúng đối với tổ chức, ví dụ về tính bảo mật, tính toàn vẹn và tính khả dụng.*

(còn nữa)

…

(*)Xem slide số 56, 57 và 58 tập tin giáo trình Chương 2 - QLRRATTT_Ch.02_v4.2.pdf