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*

Reference number
ISO/IEC 27002:2013(E)

ISO/IEC 27002

# 信息技术–安全技术–信息安全控制实用规则

Information technology-Security techniques

-Code of practice for information security controls

# Contents

Page

**Foreword** ρ

**0 Introduction** σ

**1 Scope** χ

**2 Normative references** χ

**3 Terms and definitions** χ

**4 Structure of this standard** χ
4.1 Clauses 7
4.2 Control categories 7

**5 Information security policies** ω
5.1 Management direction for information security 9

**6 Organization of information security** ρσ
6.1 Internal organization 13
6.2 Mobile devices and teleworking 17

**7 Human resource security** 23
7.1 Prior to employment 23
7.2 During employment 25
7.3 Termination and change of employment 31

**8 Asset management** 31
8.1 Responsibility for assets 31
8.2 Information classification 35
8.3 Media handling 39

**9 Access control** 43
9.1 Business requirements of access control 43
9.2 User access management 47
9.3 User responsibilities 53
9.4 System and application access control 55

**10 Cryptography** 61
10.1 Cryptographic controls 61

**11 Physical and environmental security** 65
11.1 Secure areas 65
11.2 Equipment 71

**12 Operations security** 81
12.1 Operational procedures and responsibilities 81
12.2 Protection from malware 87
12.3 Backup 89
12.4 Logging and monitoring 91
12.5 Control of operational software 95
12.6 Technical vulnerability management 97
12.7 Information systems audit considerations 101

**13 Communications security** 103
13.1 Network security management 103
13.2 Information transfer 105

**14 System acquisition, development and maintenance** 113
14.1 Security requirements of information systems 113
14.2 Security in development and support processes 119
14.3 Test data 129

**15 Supplier relationships** 129
15.1 Information security in supplier relationships 129

# 目　　次


前言 ..... 2
引言 ..... 4
0 简介 ..... 4
0.1 背景和环境 ..... 4
0.2 信息安全要求 ..... 4
0.3 选择控制措施 ..... 6
0.4 编制组织的指南 ..... 6
0.5 生命周期的考虑 ..... 6
0.6 相关标准 ..... 6
1 范围 ..... 8
2 规范性引用文件 ..... 8
3 术语和定义 ..... 8
4 本标准的结构 ..... 8
4.1 章节 ..... 8
4.2 控制类别 ..... 8
5 信息安全策略 ..... 10
5.1 信息安全的管理方向 ..... 10
6 信息安全组织 ..... 14
6.1 内部组织 ..... 14
6.2 移动设备和远程工作 ..... 18
7 人力资源安全 ..... 24
7.1 任用之前 ..... 24
7.2 任用中 ..... 26
7.3 任用的终止或变更 ..... 32
8 资产管理 ..... 32
8.1 对资产负责 ..... 32
8.2 信息分类 ..... 36
8.3 介质处置 ..... 40
9 访问控制 ..... 44
9.1 访问控制的业务要求 ..... 44
9.2 用户访问管理 ..... 48
9.3 用户职责 ..... 54
9.4 系统和应用访问控制 ..... 56
10 密码学 ..... 62
10.1 密码控制 ..... 62
11 物理和环境安全 ..... 66
11.1 安全区域 ..... 66
11.2 设备 ..... 72
12 操作安全 ..... 82
12.1 操作规程和职责 ..... 82
12.2 恶意软件防护 ..... 88
12.3 备份 ..... 90

15.2 Supplier service delivery management ..... 137

**16 Information security incident management ..... 139**
16.1 Management of information security incidents and improvements ..... 139

**17 Information security aspects of business continuity management ..... 147**
17.1 Information security continuity ..... 147
17.2 Redundancies ..... 151

**18 Compliance ..... 153**
18.1 Compliance with legal and contractual requirements ..... 153
18.2 Information security reviews ..... 159

**Bibliography ..... 163**

12.4 日志和监视 ..... 92
12.5 运行软件的控制 ..... 96
12.6 技术脆弱性管理 ..... 98
12.7 信息系统审计考虑 ..... 102
13 通信安全 ..... 104
13.1 网络安全管理 ..... 104
13.2 信息传递 ..... 106
14 系统获取、开发和维护 ..... 114
14.1 信息系统的安全要求 ..... 114
14.2 开发和支持过程中的安全 ..... 120
14.3 测试数据 ..... 130
15 供应商关系 ..... 130
15.1 供应商关系的信息安全 ..... 130
15.2 供应商服务交付管理 ..... 138
16 信息安全事件管理 ..... 140
16.1 信息安全事件和改进的管理 ..... 140
17 业务连续性管理的信息安全方面 ..... 148
17.1 信息安全连续性 ..... 148
17.2 冗余 ..... 152
18 符合性 ..... 154
18.1 符合法律和合同要求 ..... 154
18.2 信息安全评审 ..... 160
参考文献 ..... 164

# Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

ISO/IEC 27002 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

This second edition cancels and replaces the first edition (ISO/IEC 27002:2005), which has been technically and structurally revised.

# 前　言

ISO（国际标准化组织）和IEC（国际电工委员会）是为国际标准化制定专门体制的国际组织。国家机构是ISO或IEC的成员，他们通过各自的组织建立技术委员会参与国际标准的制定，来处理特定领域的技术活动。ISO和IEC技术委员会在共同感兴趣的领域合作。其他国际组织、政府和非政府等机构，通过联络ISO和IEC参与这项工作。

国际标准的制定遵循ISO/IEC 导则第2部分的规则。

ISO和IEC已经在信息技术领域建立了一个联合技术委员会ISO/IEC JTC1。

ISO/IEC 27002由联合技术委员会ISO/IEC JTC1（信息技术）分委员会SC27（安全技术）起草。

ISO/IEC 27002中的某些内容有可能涉及一些专利权问题，这一点应该引起注意。ISO和IEC不负责识别任何这样的专利权问题。

第二版进行了技术上的修订，并取消和替代第一版（ISO/IEC 27002:2005）。

# 0 Introduction

## 0.1 Background and context

This International Standard is designed for organizations to use as a reference for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001[10] or as a guidance document for organizations implementing commonly accepted information security controls. This standard is also intended for use in developing industry- and organization-specific information security management guidelines, taking into consideration their specific information security risk environment(s).

Organizations of all types and sizes (including public and private sector, commercial and non-profit) collect, process, store and transmit information in many forms including electronic, physical and verbal (e.g. conversations and presentations).

The value of information goes beyond the written words, numbers and images: knowledge, concepts, ideas and brands are examples of intangible forms of information. In an interconnected world, information and related processes, systems, networks and personnel involved in their operation, handling and protection are assets that, like other important business assets, are valuable to an organization's business and consequently deserve or require protection against various hazards.

Assets are subject to both deliberate and accidental threats while the related processes, systems, networks and people have inherent vulnerabilities. Changes to business processes and systems or other external changes (such as new laws and regulations) may create new information security risks. Therefore, given the multitude of ways in which threats could take advantage of vulnerabilities to harm the organization, information security risks are always present. Effective information security reduces these risks by protecting the organization against threats and vulnerabilities, and then reduces impacts to its assets.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. An ISMS such as that specified in ISO/IEC 27001[10] takes a holistic, coordinated view of the organization's information security risks in order to implement a comprehensive suite of information security controls under the overall framework of a coherent management system.

Many information systems have not been designed to be secure in the sense of ISO/IEC 27001[10] and this standard. The security that can be achieved through technical means is limited and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. A successful ISMS requires support by all employees in the organization. It can also require participation from shareholders, suppliers or other external parties. Specialist advice from external parties can also be needed.

In a more general sense, effective information security also assures management and other stakeholders that the organization's assets are reasonably safe and protected against harm, thereby acting as a business enabler.

## 0.2 Information security requirements

It is essential that an organization identifies its security requirements. There are three main sources of security requirements:

a) the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated;

b) the legal, statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and service providers have to satisfy, and their socio-cultural environment;

# 引　　言

## 0　简介

### 0.1　背景和环境

本标准可作为组织基于 ISO/IEC 27001 实施信息安全管理体系（ISMS）的过程中选择控制措施时的参考，或作为组织实施通用信息安全控制措施时的指南文件。本标准还可以用于开发行业和组织特定的信息安全管理指南，考虑其特定信息安全风险环境。

所有类型和规模的组织（包括公共和私营部门、商业和非盈利组织）都要采用不同方式（包括电子方式、物理方式、会谈和陈述等口头方式）收集、处理、存储和传输信息。

信息的价值超越了文字、数字和图像：无形的信息可能包括知识、概念、观念和品牌等。在互联的世界里，信息和相关过程、系统、网络及其操作、处理和保护的过程中所涉及的人员都是资产，与其它重要的业务资产一样，对组织的业务至关重要，因此需要防护各种危害。

因相关过程、系统、网络和人员具有固有的脆弱性，资产易受到故意或意外的威胁。对业务过程和系统的变更或其他外部变更（例如新的法律和规章）可能产生新的信息安全风险。因此，考虑到威胁利用脆弱性损害组织会有大量方式，信息安全风险是一直存在的。有效的信息安全可以通过保护组织免受威胁和脆弱性，从而减少这些风险，进一步降低对组织资产的影响。

信息安全是通过实施一组合适的控制措施而达到的，包括策略、过程、规程、组织结构以及软件和硬件功能。在必要时需建立、实施、监视、评审和改进这些控制措施，以确保满足该组织的特定安全和业务目标。为在一个一致的管理体系总体框架下实施一套全面的信息安全控制措施，信息安全管理体系（例如 ISO/IEC 27001 所指定的）从整体、协调的角度看待组织的信息安全风险。

从 ISO/IEC 27001 和本标准的意义上说，许多信息系统并没有被设计成是安全的。通过技术手段可获得的安全性是有限的，宜通过适当的管理和规程给予支持。确定哪些控制措施宜实施到位需要仔细规划并注意细节。成功的信息安全管理体系需要组织所有员工的参与，还要求利益相关者、供应商或其他外部方的参与。外部方的专家建议也是需要的。

就一般意义而言，有效的信息安全还可以向管理者和其他利益相关者保证，组织的资产是适当安全的，并能防范损害。因此，信息安全可承担业务使能者的角色。

### 0.2　信息安全要求

组织识别出其安全要求是非常重要的，安全要求有三个主要来源：

a)　对组织的风险进行评估，考虑组织的整体业务策略与目标。通过风险评估，识别资产受到的威胁，评价易受威胁利用的脆弱性和威胁发生的可能性，估计潜在的影响；

b)　组织、贸易伙伴、承包方和服务提供者必须满足的法律、法规、规章和合同要求，以及他们的社会文化环境；

c) the set of principles, objectives and business requirements for information handling, processing, storing, communicating and archiving that an organization has developed to support its operations.

Resources employed in implementing controls need to be balanced against the business harm likely to result from security issues in the absence of those controls. The results of a risk assessment will help guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.

ISO/IEC 27005[11] provides information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review.

## 0.3 Selecting controls

Controls can be selected from this standard or from other control sets, or new controls can be designed to meet specific needs as appropriate.

The selection of controls is dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options and the general risk management approach applied to the organization, and should also be subject to all relevant national and international legislation and regulations. Control selection also depends on the manner in which controls interact to provide defence in depth.

Some of the controls in this standard can be considered as guiding principles for information security management and applicable for most organizations. The controls are explained in more detail below along with implementation guidance. More information about selecting controls and other risk treatment options can be found in ISO/IEC 27005.[11]

## 0.4 Developing your own guidelines

This International Standard may be regarded as a starting point for developing organization-specific guidelines. Not all of the controls and guidance in this code of practice may be applicable. Furthermore, additional controls and guidelines not included in this standard may be required. When documents are developed containing additional guidelines or controls, it may be useful to include cross-references to clauses in this standard where applicable to facilitate compliance checking by auditors and business partners.

## 0.5 Lifecycle considerations

Information has a natural lifecycle, from creation and origination through storage, processing, use and transmission to its eventual destruction or decay. The value of, and risks to, assets may vary during their lifetime (e.g. unauthorized disclosure or theft of a company's financial accounts is far less significant after they have been formally published) but information security remains important to some extent at all stages.

Information systems have lifecycles within which they are conceived, specified, designed, developed, tested, implemented, used, maintained and eventually retired from service and disposed of. Information security should be taken into account at every stage. New system developments and changes to existing systems present opportunities for organizations to update and improve security controls, taking actual incidents and current and projected information security risks into account.

## 0.6 Related standards

While this standard offers guidance on a broad range of information security controls that are commonly applied in many different organizations, the remaining standards in the ISO/IEC 27000 family provide complementary advice or requirements on other aspects of the overall process of managing information security.

Refer to ISO/IEC 27000 for a general introduction to both ISMSs and the family of standards. ISO/IEC 27000 provides a glossary, formally defining most of the terms used throughout the ISO/IEC 27000 family of standards, and describes the scope and objectives for each member of the family.

c） 组织开发的支持其运行的信息处理、加工、存储、沟通和存档的原则、目标和业务要求的特定集合。

实施控制措施所用资源需要根据缺乏这些控制措施时由安全问题导致的业务损害加以平衡。

风险评估的结果将帮助指导和确定适当的管理措施、管理信息安全风险以及实现所选择的用以防范这些风险的控制措施的优先级。

ISO/IEC 27005 提供了信息安全风险管理的指南，包括风险评估、风险处置、风险接受、风险沟通、风险监视和风险评审的建议。

### 0.3 选择控制措施

控制措施可以从本标准或其他控制措施集合中选择，或者当合适时设计新的控制措施以满足特定需求。

控制措施的选择依赖于组织基于风险接受准则、风险处置选项以及所应用的通用风险管理方法做出的决策，同时还宜遵守所有相关的国家和国际法律法规。控制措施的选择还依赖于控制措施为提供深度防御而相互作用的方式。

本标准中的某些控制措施可被当作信息安全管理的指导原则，并且可用于大多数组织。在下面的实施指南中，将更详细的解释这些控制措施。更多的关于选择控制措施和其他风险处置选项的信息见 ISO/IEC 27005。

### 0.4 编制组织的指南

本标准可作为是组织开发其详细指南的起点。对一个组织来说，本标准中的控制措施和指南并非全部适用，此外，很可能还需要本标准中未包括的另外的控制措施和指南。为便于审核员和业务伙伴进行符合性核查，当开发包含另外的指南或控制措施的文件时，对本标准中条款的引用可能是有用的。

### 0.5 生命周期的考虑

信息具有自然的生命周期，从创建和产生，经存储、处理、使用和传输，到最后的销毁或衰退。资产的价值和风险可能在其生命期中是变化的（例如公司**财务报表**的泄露或被盗在他们被正式公布后就不那么重要了），但在某种程度上信息安全对于所有阶段而言都是非常重要的。

信息系统也具有生命周期，他们被构想、指定、设计、开发、测试、实施、使用、维护，并最终退出服务进行处置。在每一个阶段最好都要考虑信息安全。新系统的开发和现有系统的变更为组织更新和改进安全控制带来了机会，可将现实事件、当前和预计的信息安全风险考虑在内。

### 0.6 相关标准

虽然本标准提供了通常适用于不同组织的大范围信息安全控制措施的指南，ISO/IEC 27000 标准族的其他部分提供了信息安全管理全过程其他方面的补充建议或要求。

ISO/IEC 27000 作为信息安全管理体系和标准族的总体介绍，提供了一个词汇表，正式定义了整个 ISO/IEC 27000 标准族中的大部分术语，并描述了族中每个成员的范围和目标。

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

## 1 Scope

This International Standard gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

This International Standard is designed to be used by organizations that intend to:

a) select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;[10]

b) implement commonly accepted information security controls;

c) develop their own information security management guidelines.

## 2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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*

## 3 Terms and definitions

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

## 4 Structure of this standard

This standard contains 14 security control clauses collectively containing a total of 35 main security categories and 114 controls.

### 4.1 Clauses

Each clause defining security controls contains one or more main security categories.

The order of the clauses in this standard does not imply their importance. Depending on the circumstances, security controls from any or all clauses could be important, therefore each organization applying this standard should identify applicable controls, how important these are and their application to individual business processes. Furthermore, lists in this standard are not in priority order.

### 4.2 Control categories

Each main security control category contains:

a) a control objective stating what is to be achieved;

b) one or more controls that can be applied to achieve the control objective.

# 信息技术-安全技术-信息安全控制实用规则

## 1 范围

本标准为组织的信息安全标准和信息安全管理实践提供了指南，包括考虑组织信息安全风险环境前提下控制措施的选择、实施和管理。

本标准可被组织用于下列目的：

a) 在基于ISO/IEC 27001实施信息安全管理体系过程中选择控制措施；

b) 实施通用信息安全控制措施；

c) 开发组织自身的信息安全管理指南。

## 2 规范性引用文件

下列参考文件对于本文件的应用是必不可少的。凡是注日期的引用文件，只有引用的版本适用于本标准；凡是不注日期的引用文件，其最新版本（包括任何修改）适用于本标准。

ISO/IEC 27000，信息技术—安全技术—信息安全管理体系—概述和词汇

## 3 术语和定义

ISO/IEC 27000 中的术语和定义适用于本标准。

## 4 本标准的结构

本标准包括 14 个安全控制措施的章节，共含有 35 个主要安全类别和 113 项安全控制措施。

### 4.1 章节

定义安全控制的每个章节含一个或多个主要安全类别。

本标准中章节的顺序不表示其重要性。根据不同的环境，任何或所有章节的安全控制措施都可能是重要的，因此使用本标准的每一个组织宜识别适用的控制措施及其重要性，以及它们对各个业务过程的适用性。另外，本标准的排列没有优先顺序。

### 4.2 控制类别

每一个主要安全控制类别包含：

a) 一个控制目标，声明要实现什么；

b) 一个或多个控制措施，可被用于实现该控制目标。

Control descriptions are structured as follows:

Control

Defines the specific control statement, to satisfy the control objective.

Implementation guidance

Provides more detailed information to support the implementation of the control and meeting the control objective. The guidance may not be entirely suitable or sufficient in all situations and may not fulfil the organization's specific control requirements. .

Other information

Provides further information that may need to be considered, for example legal considerations and references to other standards. If there is no other information to be provided this part is not shown.

# 5 Information security policies

## 5.1 Management direction for information security

| Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. |
|---|

### 5.1.1 Policies for information security

Control

A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.

Implementation guidance

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.

The information security policy should contain statements concerning:

a) definition of information security, objectives and principles to guide all activities relating to information security;

b) assignment of general and specific responsibilities for information security management to defined roles;

c) processes for handling deviations and exceptions.

At a lower level, the information security policy should be supported by topic-specific policies, which further mandate the implementation of information security controls and are typically structured to address the needs of certain target groups within an organization or to cover certain topics.

Examples of such policy topics include:

a) access control (see Clause 9);

控制措施的描述结构如下：

控制措施

定义满足控制目标的特定的控制措施的陈述。

实施指南

为支持控制措施的实施和满足控制目标，提供更详细的信息。本指南可能不能全部适用或满足所有情况，也可能不满足组织的特定控制要求。

其他信息

提供需要考虑的进一步的信息，例如法律方面的考虑和对其他标准的引用。如果没有其他信息需要提供，将不显示本部分。

# 5 信息安全策略

## 5.1 信息安全的管理方向

| |
|---|
| 目标：依据业务要求和相关法律法规提供管理方向并支持信息安全。 |

### 5.1.1 信息安全策略

控制措施

信息安全策略集宜由管理者定义、批准、发布并传达给员工和相关外部方。

实施指南

在最高级别上，组织宜定义“信息安全方针”，由管理者批准，制定组织管理其信息安全目标的方法。

信息安全方针宜解决下列方面创建的要求：

a) 业务战略；

b) 规章、法规和合同；

c) 当前和预期的信息安全威胁环境。

信息安全方针宜包括以下声明：

a) 指导所有信息安全相关活动的信息安全、目标和原则的定义；

b) 已定义角色信息安全管理一般和特定职责的分配；

c) 处理偏差和意外的过程。

在较低级别，信息安全方针宜由特定主题的策略加以支持，这些策略进一步强化了信息安全控制措施的执行，并且在组织内通常以结构化的形式处理某些目标群体的需求或涵盖某些主题。

这些细化的策略主题包括：

a) 访问控制（见 9）；

b) information classification (and handling) (see 8.2);

c) physical and environmental security (see Clause 11);

d) end user oriented topics such as:

   1) acceptable use of assets (see 8.1.3);

   2) clear desk and clear screen (see 11.2.9);

   3) information transfer (see 13.2.1);

   4) mobile devices and teleworking (see 6.2);

   5) restrictions on software installations and use (see 12.6.2);

e) backup (see 12.3);

f) information transfer (see 13.2);

g) protection from malware (see 12.2);

h) management of technical vulnerabilities (see 12.6.1);

i) cryptographic controls (see Clause 10);

j) communications security (see Clause 13);

k) privacy and protection of personally identifiable information (see 18.1.4);

l) supplier relationships (see Clause 15).

These policies should be communicated to employees and relevant external parties in a form that is relevant, accessible and understandable to the intended reader, e.g. in the context of an "information security awareness, education and training programme" (see 7.2.2).

Other information

The need for internal policies for information security varies across organizations. Internal policies are especially useful in larger and more complex organizations where those defining and approving the expected levels of control are segregated from those implementing the controls or in situations where a policy applies to many different people or functions in the organization. Policies for information security can be issued in a single "information security policy" document or as a set of individual but related documents.

If any of the information security policies are distributed outside the organization, care should be taken not to disclose confidential information.

Some organizations use other terms for these policy documents, such as "Standards", "Directives" or "Rules".

### 5.1.2 Review of the policies for information security

Control

The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Implementation guidance

Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

b) 信息分类（和处理）（见 8.2）；

c) 物理和环境安全（见 11）；

d) 面向终端用户的主题，例如：

1) 资产的可接受使用（见 8.1.3）；

2) 清空桌面和清空屏幕（见 11.2.9）；

3) 信息传递（见 13.2.1）；

4) 移动设备和远程工作（见 6.2）；

5) 软件安装和使用的限制（见 12.6.2）；

e) 备份（见 12.3）；

f) 信息传递（见 13.2）；

g) 恶意软件防范（见 12.2）；

h) 技术脆弱性管理（见 12.6.1）；

i) 密码控制（见 10）；

j) 通信安全（见 13）；

k) 隐私和个人可识别信息的保护（见 18.1.4）；

l) 供应商关系（见 15）。

这些策略宜采用预期读者适合的、可访问的和可理解的形式传达给员工和相关外部方，例如在“信息安全意识、教育和培训方案”（见 7.2.2）的情况下。

其他信息

信息安全内部策略的需求因组织而异。内部策略对于大型和复杂的组织而言更加有用，这些组织中，定义和批准控制预期水平的人员与实施控制措施的人员或策略应用于组织中不同人员或职能的情境是隔离的。信息安全策略可以以单一《信息安全方针》文件的形式发布，或作为各不相同但相互关联的一套文件。

如果任何信息安全策略要分发至组织外部，宜注意不要泄露保密信息。

一些组织使用其他术语定义这些策略文件，例如“标准”、“导则”或“规则”。

### 5.1.2 信息安全策略的评审

控制措施

信息安全策略宜按计划的时间间隔或当重大变化发生时进行评审，以确保其持续的适宜性、充分性和有效性。

实施指南

每个策略宜有专人负责，他负有授权的策略开发、评审和评价的管理职责。评审宜包括评估组织策略改进的机会和管理信息安全适应组织环境、业务状况、法律条件或技术环境变化的方法。

The review of policies for information security should take the results of management reviews into account.

Management approval for a revised policy should be obtained.

# 6 Organization of information security

## 6.1 Internal organization

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

### 6.1.1 Information security roles and responsibilities

Control

All information security responsibilities should be defined and allocated.

Implementation guidance

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. These responsibilities should be supplemented, where necessary, with more detailed guidance for specific sites and information processing facilities. Local responsibilities for the protection of assets and for carrying out specific security processes should be defined.

Individuals with allocated information security responsibilities may delegate security tasks to others. Nevertheless they remain accountable and should determine that any delegated tasks have been correctly performed.

Areas for which individuals are responsible should be stated. In particular the following should take place:

a) the assets and information security processes should be identified and defined;

b) the entity responsible for each asset or information security process should be assigned and the details of this responsibility should be documented (see 8.1.2);

c) authorization levels should be defined and documented;

d) to be able to fulfil responsibilities in the information security area the appointed individuals should be competent in the area and be given opportunities to keep up to date with developments;

e) coordination and oversight of information security aspects of supplier relationships should be identified and documented.

Other information

Many organizations appoint an information security manager to take overall responsibility for the development and implementation of information security and to support the identification of controls.

However, responsibility for resourcing and implementing the controls will often remain with individual managers. One common practice is to appoint an owner for each asset who then becomes responsible for its day-to-day protection.

### 6.1.2 Segregation of duties

Control

信息安全策略评审宜考虑管理评审的结果。

宜获得管理者对修订的策略的批准。

# 6 信息安全组织

## 6.1 内部组织

| |
|---|
| 目标：建立管理框架，以启动和控制组织范围内的信息安全的实施和运行。 |

### 6.1.1 信息安全角色和职责

控制措施

所有的信息安全职责宜予以定义和分配。

实施指南

信息安全职责的分配宜与信息安全策略（见 5.1.1）相一致。宜识别各个资产的保护和执行特定信息安全过程的职责。宜定义信息安全风险管理活动，特别是残余风险接受的职责。这些职责宜在必要时加以补充，来为特定地点和信息处理设施提供更详细的指南。资产保护和执行特定安全过程的局部职责宜予以定义。

分配有信息安全职责的人员可以将安全任务委托给其他人员。尽管如此，他们仍然负有责任，并且他们宜能够确定任何被委托的任务是否已被正确地执行。

个人负责的领域宜予以规定；特别是，宜进行下列工作：

a) 宜识别和定义资产和信息安全过程；

b) 宜分配每一资产或信息安全过程的实体职责，并且该职责的细节宜形成文件（见 8.1.2）；

c) 宜定义授权级别，并形成文件；

d) 能够履行信息安全领域的职责，领域内被任命的人员宜有能力，并给予他们机会，使其能够紧跟发展的潮流；

e) 宜识别供应商关系信息安全方面的协调和监督措施，并形成文件。

其他信息

在许多组织中，将任命一名信息安全管理人员全面负责信息安全的开发和实施，并支持控制措施的识别。

然而，提供控制措施资源并实施这些控制措施的职责通常归于各个管理人员。一种通常的做法是为每一项资产指定一名责任人负责该项资产的日常保护。

### 6.1.2 职责分离

控制措施

Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

Implementation guidance

Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls.

Small organizations may find segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered.

Other information

Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of an organization's assets.

### 6.1.3 Contact with authorities

Control

Appropriate contacts with relevant authorities should be maintained.

Implementation guidance

Organizations should have procedures in place that specify when and by whom authorities (e.g. law enforcement, regulatory bodies, supervisory authorities) should be contacted and how identified information security incidents should be reported in a timely manner (e.g. if it is suspected that laws may have been broken).

Other information

Organizations under attack from the Internet may need authorities to take action against the attack source.

Maintaining such contacts may be a requirement to support information security incident management (see Clause 16) or the business continuity and contingency planning process (see Clause 17). Contacts with regulatory bodies are also useful to anticipate and prepare for upcoming changes in laws or regulations, which have to be implemented by the organization. Contacts with other authorities include utilities, emergency services, electricity suppliers and health and safety, e.g. fire departments (in connection with business continuity), telecommunication providers (in connection with line routing and availability) and water suppliers (in connection with cooling facilities for equipment).

### 6.1.4 Contact with special interest groups

Control

Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.

Implementation guidance

Membership in special interest groups or forums should be considered as a means to:

a) improve knowledge about best practices and stay up to date with relevant security information;

b) ensure the understanding of the information security environment is current and complete;

c) receive early warnings of alerts, advisories and patches pertaining to attacks and vulnerabilities;

d) gain access to specialist information security advice;

宜分离相冲突的责任及职责范围，以降低未授权或无意识的修改或者不当使用组织资产的机会。

实施指南

宜注意，在无授权或监测时，个人不能访问、修改或使用资产。事件的启动宜与其授权分离。勾结的可能性宜在设计控制措施时予以考虑。

小型组织可能感到难以实现这种职责分离，但只要具有可能性和可行性，宜尽量应用该原则。如果难以分离，宜考虑其他控制措施，例如对活动、审核踪迹和管理监督的监视等。

其他信息

职责分离是一种减少意外或故意组织资产误用的风险的方法。

### 6.1.3 与政府部门的联系

控制措施

宜保持与政府相关部门的适当联系。

实施指南

组织宜有规程指明什么时候与哪个部门（例如，执法部门、监管机构、监督部门）联系、已识别的信息安全事件如何及时报告（例如，如果怀疑可能触犯了法律时）

其他信息

受到来自互联网攻击的组织可能需要政府部门采取措施以应对攻击源。

保持这样的联系可能是支持信息安全事件管理（见 16）或业务连续性和应急计划过程（见 17）的要求。与监管机构的联系还有助于预先知道组织必须遵循的法律法规方面即将出现的变化，并为这些变化做好准备。与其他部门的联系包括公共设施、紧急服务、电力供应和健康安全（safety）部门，例如消防局（与业务连续性有关）、电信提供商（与路由和可用性有关）、供水部门（与设备的冷却设施有关）。

### 6.1.4 与特定利益集团的联系

控制措施

宜保持与特定利益集团、其他安全论坛和专业协会的适当联系。

实施指南

宜考虑成为特定利益集团或论坛的成员，以便：

a) 增进关于最佳实践的知识，保持对最新相关安全信息的了解；

b) 确保全面了解当前的信息安全环境；

c) 尽早收到关于攻击和脆弱性的预警、建议和补丁；

d) 获得信息安全专家的建议；

e) share and exchange information about new technologies, products, threats or vulnerabilities;

f) provide suitable liaison points when dealing with information security incidents (see Clause 16).

Other information

Information sharing agreements can be established to improve cooperation and coordination of security issues. Such agreements should identify requirements for the protection of confidential information.

### 6.1.5 Information security in project management

Control

Information security should be addressed in project management, regardless of the type of the project.

Implementation guidance

Information security should be integrated into the organization's project management method(s) to ensure that information security risks are identified and addressed as part of a project. This applies generally to any project regardless of its character, e.g. a project for a core business process, IT, facility management and other supporting processes. The project management methods in use should require that:

a) information security objectives are included in project objectives;

b) an information security risk assessment is conducted at an early stage of the project to identify necessary controls;

c) information security is part of all phases of the applied project methodology.

Information security implications should be addressed and reviewed regularly in all projects. Responsibilities for information security should be defined and allocated to specified roles defined in the project management methods.

## 6.2 Mobile devices and teleworking

| Objective: To ensure the security of teleworking and use of mobile devices. |
|---|

### 6.2.1 Mobile device policy

Control

A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.

Implementation guidance

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) requirements for mobile device software versions and for applying patches;

e) restriction of connection to information services;

e) 分享和交换关于新的技术、产品、威胁或脆弱性的信息；

f) 提供处理信息安全事件时适当的联络点（见 16）。

其他信息

建立信息共享协议来改进安全问题的协作和协调。这种协议宜识别出保护保密信息的要求。

### 6.1.5 项目管理中的信息安全

控制措施

无论项目是什么类型，在项目管理中都宜处理信息安全问题。

实施指南

信息安全宜整合到组织的项目管理方法中，以确保将识别并处理信息安全风险作为项目的一部分。这通常可应用于所有项目，无论其特性是什么，例如核心业务过程、IT、设施管理和其他支持过程等方面的项目。在用的项目管理方法宜要求：

a) 信息安全目标纳入项目目标；

b) 在项目的早期阶段进行信息安全风险评估，以识别必要的控制措施；

c) 对于适用的项目方法论而言，信息安全是其每个阶段的组成部分。

在所有项目中，宜定期处理和评审信息安全影响。信息安全职责宜加以定义，并分配给项目管理方法中定义的指定角色。

## 6.2 移动设备和远程工作

| |
|---|
| 目标：确保远程工作和使用移动设备时的安全。 |

### 6.2.1 移动设备策略

控制措施

宜采用策略和支持性安全措施来管理由于使用移动设备带来的风险。

实施指南

当使用移动设备时，宜特别小心确保业务信息不被损害。移动设备策略宜考虑到在不受保护的环境下使用移动设备工作的风险。

移动设备策略宜考虑：

a) 移动设备的注册；

b) 物理保护的要求；

c) 软件安装的限制；

d) 移动设备软件版本和补丁应用的要求；

e) 连接信息服务的限制；

f) access controls;

g) cryptographic techniques;

h) malware protection;

i) remote disabling, erasure or lockout;

j) backups;

k) usage of web services and web apps.

Care should be taken when using mobile devices in public places, meeting rooms and other unprotected areas. Protection should be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these devices, e.g. using cryptographic techniques (see Clause 10) and enforcing use of secret authentication information (see 9.2.4).

Mobile devices should also be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centres and meeting places. A specific procedure taking into account legal, insurance and other security requirements of the organization should be established for cases of theft or loss of mobile devices. Devices carrying important, sensitive or critical business information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the devices.

Training should be arranged for personnel using mobile devices to raise their awareness of the additional risks resulting from this way of working and the controls that should be implemented.

Where the mobile device policy allows the use of privately owned mobile devices, the policy and related security measures should also consider:

a) separation of private and business use of the devices, including using software to support such separation and protect business data on a private device;

b) providing access to business information only after users have signed an end user agreement acknowledging their duties (physical protection, software updating, etc.), waiving ownership of business data, allowing remote wiping of data by the organization in case of theft or loss of the device or when no longer authorized to use the service. This policy needs to take account of privacy legislation.

Other information

Mobile device wireless connections are similar to other types of network connection, but have important differences that should be considered when identifying controls. Typical differences are:

a) some wireless security protocols are immature and have known weaknesses;

b) information stored on mobile devices may not be backed-up because of limited network bandwidth or because mobile devices may not be connected at the times when backups are scheduled.

Mobile devices generally share common functions, e.g. networking, internet access, e-mail and file handling, with fixed use devices. Information security controls for the mobile devices generally consist of those adopted in the fixed use devices and those to address threats raised by their usage outside the organization's premises.

### 6.2.2 Teleworking

Control

A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites.

Implementation guidance

f) 访问控制；

g) 密码技术；

h) 恶意软件防范；

i) 远程关闭、擦除或锁定；

j) 备份；

k) web 服务和 web 应用的用法。

当在公共场所、会议室和其他不受保护的区域使用移动设备时，宜加以小心。为避免未授权访问或泄露这些设备所存储和处理的信息，宜有适当的保护措施，例如，使用密码技术（见 10）、强制使用秘密鉴别信息（见 9.2.3）。

还宜对移动设备进行物理保护，以防被偷窃，例如，特别是遗留在汽车和其他形式的运输工具上、旅馆房间、会议中心和会议室。宜为移动设备的被窃或丢失等情况建立一个符合法律、保险和组织的其他安全要求的特定规程。携带重要、敏感或关键业务信息的设备不宜无人值守，若有可能，宜以物理的方式锁起来，或使用专用锁来保护设备。

对于使用移动设备的人员宜安排培训，以提高他们对这种工作方式导致的附加风险的意识，并且宜实施控制措施。

当移动设备策略允许使用私人移动设备时，策略及相关安全措施宜考虑：

a) 分离设备的私人使用和业务使用，包括使用软件来支持这种分离，保护私人设备上的业务数据；

b) 只有当用户签署了终端用户协议，确认其职责（物理保护、软件更新等）后，方可提供对业务信息的访问，一旦设备被盗或丢失，或当不再授权使用服务时，组织放弃业务数据的所有权、允许远程的数据擦除。这个策略需要考虑隐私方面的法律。

其他信息

移动设别无线连接类似于其他类型的网络连接，但在识别控制措施时，宜考虑两者的重要区别。典型的区别有：

a) 一些无线安全协议是不成熟的，并有已知的弱点；

b) 在移动设备上存储的信息因受限的网络带宽可能不能备份，或因为移动设备在规定的备份时间不能进行连接。

移动设备通常与固定使用的设备分享其常用功能，例如联网、互联网访问、电子邮件和文件处理。移动设备的信息安全控制措施通常包含在固定使用的设备中所用的控制措施，以及处理由于其在组织场所外使用所引发威胁的控制措施。

### 6.2.2 远程工作

控制措施

宜实施策略和支持性安全措施来保护在远程工作场地访问、处理或存储的信息。

实施指南

Organizations allowing teleworking activities should issue a policy that defines the conditions and restrictions for using teleworking. Where deemed applicable and allowed by law, the following matters should be considered:

a) the existing physical security of the teleworking site, taking into account the physical security of the building and the local environment;

b) the proposed physical teleworking environment;

c) the communications security requirements, taking into account the need for remote access to the organization's internal systems, the sensitivity of the information that will be accessed and passed over the communication link and the sensitivity of the internal system;

d) the provision of virtual desktop access that prevents processing and storage of information on privately owned equipment;

e) the threat of unauthorized access to information or resources from other persons using the accommodation, e.g. family and friends;

f) the use of home networks and requirements or restrictions on the configuration of wireless network services;

g) policies and procedures to prevent disputes concerning rights to intellectual property developed on privately owned equipment;

h) access to privately owned equipment (to verify the security of the machine or during an investigation), which may be prevented by legislation;

i) software licensing agreements that are such that organizations may become liable for licensing for client software on workstations owned privately by employees or external party users;

j) malware protection and firewall requirements.

The guidelines and arrangements to be considered should include:

a) the provision of suitable equipment and storage furniture for the teleworking activities, where the use of privately owned equipment that is not under the control of the organization is not allowed;

b) a definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the teleworker is authorized to access;

c) the provision of suitable communication equipment, including methods for securing remote access;

d) physical security;

e) rules and guidance on family and visitor access to equipment and information;

f) the provision of hardware and software support and maintenance;

g) the provision of insurance;

h) the procedures for backup and business continuity;

i) audit and security monitoring;

j) revocation of authority and access rights, and the return of equipment when the teleworking activities are terminated.

Other information

Teleworking refers to all forms of work outside of the office, including non-traditional work environments, such as those referred to as "telecommuting", "flexible workplace", "remote work" and "virtual work" environments.

组织宜在定义使用远程工作的条件及限制的策略发布后，才允许远程工作活动。当认为适用，法律允许的情况下，宜考虑下列事项：

a) 远程工作场地的现有物理安全，要考虑到建筑物和本地环境的物理安全；
b) 推荐的物理的远程工作环境；
c) 通信安全要求，要考虑远程访问组织内部系统的需要、被访问的并在通信链路上传递的信息的敏感性以及内部系统的敏感性；
d) 虚拟桌面访问的规定，防止在私有设备处理或存储信息；
e) 住处的其他人员（例如，家人和朋友）未授权访问信息或资源的威胁；
f) 家庭网络的使用和无线网络服务配置的要求或限制；
g) 针对私有设备开发的预防知识产权争论的策略和规程；
h) 法律禁止的对私有设备的访问（核查机器安全或在调查期间）；
i) 使组织对雇员或外部方人员等私人拥有的工作站上的客户端软件负责的软件许可协议；
j) 防病毒保护和防火墙要求。

要考虑的指南和安排宜包括：

a) 当不允许使用不在组织控制下的私有设备时，对远程工作活动提供合适的设备和存储设施；
b) 定义允许的工作、工作小时数、可以保持的信息分类和授权远程工作者访问的内部系统和服务；
c) 提供适合的通信设备，包括使远程访问安全的方法；
d) 物理安全；
e) 有关家人和来宾访问设备和信息的规则和指南；
f) 硬件和软件支持和维护的规定；
g) 保险的规定；
h) 用于备份和业务连续性的规程；
i) 审核和安全监视；
j) 当远程工作活动终止时，撤销授权和访问权限，并归还设备。

其他信息

远程工作是利用通信技术来使得人员可以在其组织之外的固定地点进行远程工作的。

远程工作是指在办公场所外工作的所有形式，包括非传统的工作环境，例如被称为“远程办公”、“弹性工作点”、“远程工作”和“虚拟工作”等的环境。

# 7 Human resource security

## 7.1 Prior to employment

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

### 7.1.1 Screening

Control

Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

Implementation guidance

Verification should take into account all relevant privacy, protection of personally identifiable information and employment based legislation, and should, where permitted, include the following:

a) availability of satisfactory character references, e.g. one business and one personal;

b) a verification (for completeness and accuracy) of the applicant's curriculum vitae;

c) confirmation of claimed academic and professional qualifications;

d) independent identity verification (passport or similar document);

e) more detailed verification, such as credit review or review of criminal records.

When an individual is hired for a specific information security role, organizations should make sure the candidate:

a) has the necessary competence to perform the security role;

b) can be trusted to take on the role, especially if the role is critical for the organization.

Where a job, either on initial appointment or on promotion, involves the person having access to information processing facilities, and, in particular, if these are handling confidential information, e.g. financial information or highly confidential information, the organization should also consider further, more detailed verifications.

Procedures should define criteria and limitations for verification reviews, e.g. who is eligible to screen people and how, when and why verification reviews are carried out.

A screening process should also be ensured for contractors. In these cases, the agreement between the organization and the contractor should specify responsibilities for conducting the screening and the notification procedures that need to be followed if screening has not been completed or if the results give cause for doubt or concern.

Information on all candidates being considered for positions within the organization should be collected and handled in accordance with any appropriate legislation existing in the relevant jurisdiction. Depending on applicable legislation, the candidates should be informed beforehand about the screening activities.

### 7.1.2 Terms and conditions of employment

Control

The contractual agreements with employees and contractors should state their and the organization's responsibilities for information security.

# 7 人力资源安全

## 7.1 任用之前

| |
|---|
| 目标：确保雇员和承包方人员理解其职责、适于考虑让其承担的角色。 |

### 7.1.1 审查

控制措施

关于所有任用候选者的背景验证核查宜按照相关法律、法规、道德规范和对应的业务要求、被访问信息的类别和察觉的风险来执行。

实施指南

验证宜考虑所有相关的隐私、个人可识别信息的保护以及与任用相关的法律，并宜包括以下内容（允许时）：

a) 令人满意的个人资料的可用性（例如，一项业务和一个个人）；

b) 申请人履历的核查（针对完备性和准确性）；

c) 声称的学术、专业资质的证实；

d) 个人身份核查（护照或类似文件）；

e) 更多细节的核查，例如信用卡核查或犯罪记录核查。

当人员聘用为特定的信息安全角色时，组织宜弄清楚候选者：

a) 有执行安全角色所必需的能力；

b) 可被信任从事该角色，特别是当该角色对组织来说是十分关键时。

当一个职务（最初任命的或提升的）涉及到对信息处理设施进行访问的人时，特别是，如果这些设施正在处理保密信息，例如，财务信息或高度保密的信息，那么，该组织还宜考虑进一步的、更详细的核查。

宜有规程确定验证核查的准则和限制，例如谁有资格审查人员，以及如何、何时、为什么执行验证核查。

对于承包方人员也宜执行审查过程。在这样的情况下，组织与承包方人员的协议宜指定进行审查的职责以及如果审查没有完成或结果给出需要怀疑或关注的理由时需遵循的通告规程。

被考虑在组织内录用的所有候选者的信息宜按照相关管辖范围内存在的合适的法律来收集和处理。依据适用的法律，宜将审查活动提前通知候选者。

### 7.1.2 任用条款和条件

控制措施

与雇员和承包方人员的合同协议宜声明他们和组织的信息安全职责。

Implementation guidance

The contractual obligations for employees or contractors should reflect the organization's policies for information security in addition to clarifying and stating:

a) that all employees and contractors who are given access to confidential information should sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities (see 13.2.4);

b) the employee's or contractor's legal responsibilities and rights, e.g. regarding copyright laws or data protection legislation (see 18.1.2 and 18.1.4);

c) responsibilities for the classification of information and management of organizational assets associated with information, information processing facilities and information services handled by the employee or contractor (see Clause 8);

d) responsibilities of the employee or contractor for the handling of information received from other companies or external parties;

e) actions to be taken if the employee or contractor disregards the organization's security requirements (see 7.2.3).

Information security roles and responsibilities should be communicated to job candidates during the pre-employment process.

The organization should ensure that employees and contractors agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services.

Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment (see 7.3).

Other information

A code of conduct may be used to state the employee's or contractor's information security responsibilities regarding confidentiality, data protection, ethics, appropriate use of the organization's equipment and facilities, as well as reputable practices expected by the organization. An external party, with which a contractor is associated, can be required to enter into contractual arrangements on behalf of the contracted individual.

## 7.2 During employment

Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

### 7.2.1 Management responsibilities

Control

Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.

Implementation guidance

Management responsibilities should include ensuring that employees and contractors:

a) are properly briefed on their information security roles and responsibilities prior to being granted access to confidential information or information systems;

b) are provided with guidelines to state information security expectations of their role within the organization;

实施指南

雇员或承包方人员的合同义务除澄清和声明以下内容外，还宜反映组织的信息安全策略：

a) 所有访问保密信息的雇员和承包方人员宜在给予访问信息处理设施权限之前签署保密或不泄露协议；

b) 雇员和承包方人员的法律责任和权利，例如关于版权法、数据保护法（见 18.1.4）；

c) 与雇员和承包方人员处理的信息、信息处理设施和信息服务有关的信息分类和组织资产管理的职责（见 8）；

d) 雇员和承包方人员处理来自其他公司或外部方的信息的职责；

e) 如果雇员和承包方人员漠视组织的安全要求所要采取的措施（见 7.2.3）。

信息安全角色和职责宜在任用前的过程中传达给职务的候选者。

组织宜确保雇员和承包方人员同意适用于他们将访问的与信息系统和服务有关的组织资产的性质和程度的信息安全条款和条件。

若适用，包含于任用条款和条件中的职责宜在任用结束后持续一段规定的时间（见 7.3）。

其他信息

一个行为细则可声明雇员和承包方人员关于保密性、数据保护、道德规范、组织设备和设施的适当使用以及组织期望的最佳实践的信息安全职责。承包方人员与之有关的外部方、可被要求代表已签约的人遵守合约的安排。

## 7.2 任用中

| |
|---|
| 目标：确保雇员和承包方人员知悉并履行其信息安全职责。 |

### 7.2.1 管理职责

控制措施

管理者宜要求所有雇员和承包方人员按照组织已建立的策略和规程对信息安全尽心尽力。

实施指南

管理职责宜包括确保雇员和承包方人员：

a) 在被允许访问保密信息或信息系统前了解其信息安全角色和职责；

b) 获得声明在组织中他们角色的信息安全期望的指南；

c) are motivated to fulfil the information security policies of the organization;

d) achieve a level of awareness on information security relevant to their roles and responsibilities within the organization (see 7.2.2);

e) conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working;

f) continue to have the appropriate skills and qualifications and are educated on a regular basis;

g) are provided with an anonymous reporting channel to report violations of information security policies or procedures ("whistle blowing").

Management should demonstrate support of information security policies, procedures and controls, and act as a role model.

Other information

If employees and contractors are not made aware of their information security responsibilities, they can cause considerable damage to an organization. Motivated personnel are likely to be more reliable and cause fewer information security incidents.

Poor management can cause personnel to feel undervalued resulting in a negative information security impact on the organization. For example, poor management can lead to information security being neglected or potential misuse of the organization's assets.

### 7.2.2 Information security awareness, education and training

Control

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

Implementation guidance

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. The awareness programme should include a number of awareness-raising activities such as campaigns (e.g. an "information security day") and issuing booklets or newsletters.

The awareness programme should be planned taking into consideration the employees' roles in the organization, and, where relevant, the organization's expectation of the awareness of contractors. The activities in the awareness programme should be scheduled over time, preferably regularly, so that the activities are repeated and cover new employees and contractors. The awareness programme should also be updated regularly so it stays in line with organizational policies and procedures, and should be built on lessons learnt from information security incidents.

Awareness training should be performed as required by the organization's information security awareness programme. Awareness training can use different delivery media including classroom-based, distance learning, web-based, self-paced and others.

Information security education and training should also cover general aspects such as:

a) stating management's commitment to information security throughout the organization;

c) 被激励以实现组织的信息安全策略；

d) 对于在组织内他们角色和职责相关信息安全的意识程度达到一定级别；

e) 遵守任用的条款和条件，包括组织的信息安全策略和工作的适当方法；

f) 持续拥有适当的技能和资质，定期接受培训；

g) 获知匿名报告途径，可报告信息安全策略或规程的违规行为（“举报”）。

管理者宜对信息安全策略、规程和控制措施表达支持，并充当榜样。

其他信息

如果雇员和承包方人员没有意识到他们的信息安全职责，他们会对组织造成相当大的破坏。被激励的人员更可靠并能减少信息安全事件的发生。

缺乏有效的管理会使员工感觉被低估，并由此导致对组织的负面信息安全影响。例如，缺乏有效的管理可能导致信息安全被忽视或组织资产的潜在误用。

### 7.2.2 信息安全意识、教育和培训

控制措施

组织的所有雇员，适当时，包括承包方人员，宜受到与其工作职能相关的适当的意识培训和组织策略及规程的定期更新培训。

实施指南

信息安全意识培训方案旨在使雇员，适当时，包括承包方人员，意识到他们的信息安全职责以及履行职责的方法。

信息安全意识培训方案宜按照组织的信息安全策略和相关规程建立，考虑组织要保护的信息以及为保护这些信息所实施的控制措施。意识方案宜包括一些意识提升活动，像组织宣传活动（例如“信息安全日”）、发布宣传单或制作简报等。

意识方案宜考虑雇员在组织中的角色，适当时，还要考虑组织对承包方人员在意识方面的期望。意识方案的活动宜不断开展，最好能定期实施，使得这些活动是可重复的，并能够涵盖新的雇员和承包方人员。意识方案还宜定期更新，使它保持与组织策略和规程的一致，并建立在信息安全事件所积累教训的基础上。

意识培训宜按照组织的信息安全意识培训方案的要求执行。意识培训可使用不同的交付媒介，包括课堂教学、远程教学、网络教学、自学及其他方式。

信息安全教育和培训还宜覆盖的一般方面包括：

a) 在整个组织范围内声明信息安全管理承诺；

b) the need to become familiar with and comply with applicable information security rules and obligations, as defined in policies, standards, laws, regulations, contracts and agreements;

c) personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to the organization and external parties;

d) basic information security procedures (such as information security incident reporting) and baseline controls (such as password security, malware controls and clear desks);

e) contact points and resources for additional information and advice on information security matters, including further information security education and training materials.

Information security education and training should take place periodically. Initial education and training applies to those who transfer to new positions or roles with substantially different information security requirements, not just to new starters and should take place before the role becomes active.

The organization should develop the education and training programme in order to conduct the education and training effectively. The programme should be 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. The programme should consider different forms of education and training, e.g. lectures or self-studies.

Other information

When composing an awareness programme, it is important not only to focus on the 'what' and 'how', but also the 'why'. It is important that employees understand the aim of information security and the potential impact, positive and negative, on the organization of their own behaviour.

Awareness, education and training can be part of, or conducted in collaboration with, other training activities, for example general IT or general security training. Awareness, education and training activities should be suitable and relevant to the individual's roles, responsibilities and skills.

An assessment of the employees' understanding could be conducted at the end of an awareness, education and training course to test knowledge transfer.

### 7.2.3 Disciplinary process

Control

There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

Implementation guidance

The disciplinary process should not be commenced without prior verification that an information security breach has occurred (see 16.1.7).

The formal disciplinary process should ensure correct and fair treatment for employees who are suspected of committing breaches of information security. The formal disciplinary process should provide for a graduated response that takes into consideration factors such as the nature and gravity of the breach and its impact on business, whether or not this is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required.

The disciplinary process should also be used as a deterrent to prevent employees from violating the organization's information security policies and procedures and any other information security breaches. Deliberate breaches may require immediate actions.

Other information

The disciplinary process can also become a motivation or an incentive if positive sanctions are defined for remarkable behaviour with regards to information security.

b) 熟悉并遵从信息安全规则和义务的需求，正如策略、标准、法律、法规、合同和协议中所定义的那样；

c) 对自己行为和不作为的人员责任、保护组织和外部方信息的一般责任；

d) 基本信息安全规程（例如信息安全事件报告）和基线控制（例如口令安全、恶意软件控制措施和清空桌面）；

e) 联络点和其他信息资源以及信息安全事项的建议，包括进一步的信息安全教育和培训材料。

信息安全教育和培训宜定期开展。最初的教育和培训可针对那些调任新岗位或角色，且与原来的信息安全要求相比有很大不同的人员展开，不要只是针对新员工，而且宜在进入角色之前实施。

为有效进行教育和培训，组织宜开发信息安全意识培训方案。方案宜与组织的信息安全策略和相关规程保持一致，方案宜考虑教育和培训的不同形式，例如演讲或自学。

其他信息

当组成意识方案时，重要的是，不仅要关注“做什么”和“怎么做”，还要关注“为什么”。雇员理解信息安全的目的以及由于他们在组织内的行为（正面的或负面的）所带来的潜在影响是十分重要的。

意识教育和培训可以是其他培训活动的一部分，或与之协同实施，例如通用 IT 或通用安全培训。意识教育和培训活动宜适于并与个人的角色、职责和技能相关（见 7.2.2）。

可在意识教育和培训课程结束时，对雇员的理解程度进行评估，以测试知识的传递效果。

### 7.2.3 纪律处理过程

控制措施

宜有一个正式的、已传达的纪律处理过程，来对信息安全违规的雇员采取措施。

实施指南

纪律处理过程之前宜有一个信息安全违规的验证过程（见 16.1.7）。

正式的纪律处理过程宜确保正确和公平的对待被怀疑信息安全违规的雇员。无论违规是第一次或是已发生过，无论违规者是否经过适当的培训，正式的纪律处理过程宜规定一个分级的响应，要考虑例如违规的性质、重要性及对于业务的影响等因素，相关法律、业务合同和其他因素也是需要考虑的。

纪律处理过程也可用于对雇员的一种威慑，防止他们违反组织的信息安全策略和规程及其他信息安全违规。故意的违规需要立即采取措施。

其他信息

如果对信息安全有关的异常行为定义了肯定的处罚，纪律处理过程还可以变为一种动力或刺激。

## 7.3 Termination and change of employment

Objective: To protect the organization's interests as part of the process of changing or terminating employment.

### 7.3.1 Termination or change of employment responsibilities

Control

Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced.

Implementation guidance

The communication of termination responsibilities should include on-going information security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement (see 13.2.4) and the terms and conditions of employment (see 7.1.2) continuing for a defined period after the end of the employee's or contractor's employment.

Responsibilities and duties still valid after termination of employment should be contained in the employee's or contractor's terms and conditions of employment (see 7.1.2).

Changes of responsibility or employment should be managed as the termination of the current responsibility or employment combined with the initiation of the new responsibility or employment.

Other information

The human resources function is generally responsible for the overall termination process and works together with the supervising manager of the person leaving to manage the information security aspects of the relevant procedures. In the case of a contractor provided through an external party, this termination process is undertaken by the external party in accordance with the contract between the organization and the external party.

It may be necessary to inform employees, customers or contractors of changes to personnel and operating arrangements.

# 8 Asset management

## 8.1 Responsibility for assets

Objective: To identify organizational assets and define appropriate protection responsibilities.

### 8.1.1 Inventory of assets

Control

Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained.

Implementation guidance

An organization should identify assets relevant in the lifecycle of information and document their importance. The lifecycle of information should include creation, processing, storage, transmission, deletion and destruction. Documentation should be maintained in dedicated or existing inventories as appropriate.

The asset inventory should be accurate, up to date, consistent and aligned with other inventories.

For each of the identified assets, ownership of the asset should be assigned (see 8.1.2) and the classification should be identified (see 8.2).

### 7.3 任用的终止或变更

| |
|---|
| 目标：将保护组织利益作为变更或终止任用过程的一部分。 |

#### 7.3.1 任用终止或变更的职责

控制措施

宜定义信息安全职责和义务在任用终止或变更后保持有效的要求，并传达给雇员或承包方人员，予以执行。

实施指南

终止职责的传达宜包括正在进行的信息安全要求和法律职责，适当时，还包括任何保密协议包含的职责（见 13.2.4），并且在雇员和承包方人员任用结束后持续一段时间仍然有效的任用条款和条件（见 7.1.2）。

规定职责和义务在任用终止后仍然有效的内容宜包含在雇员和承包方人员的任用条款和条件中。

职责或任用的变更宜加以管理，当前职责或任用的终止要结合新的职责或任用的初始化。

其他信息

人力资源的职能通常是与管理相关规程的信息安全方面的监督管理员一块负责总体的任用终止处理。在由外部方提供承包方人员的情况下，终止 的处理按照组织与外部方的合同，由外部方完成，

有必要通知雇员、顾客、承包方人员关于组织人员的变更和运营上的安排。

## 8 资产管理

### 8.1 对资产负责

| |
|---|
| 目标：识别组织资产，并定义适当的保护职责。 |

#### 8.1.1 资产清单

控制措施

宜识别与信息和信息处理设施的资产，编制并维护这些资产的清单。

实施指南

组织宜识别与信息生命周期有关的资产，并将其重要性形成文件。信息的生命周期宜包括创建、处理、存储、传输、删除和销毁。文件宜以专用清单进行维护，适当时，或以现有清单进行维护。

资产清单宜是准确的、最新的，并与其它清单保持一致和匹配。

对于所识别的每个资产，需要指定资产的所有权（见 8.1.2）、识别其类别（见 8.2）。

Other information

Inventories of assets help to ensure that effective protection takes place, and may also be required for other purposes, such as health and safety, insurance or financial (asset management) reasons.

ISO/IEC 27005[11] provides examples of assets that might need to be considered by the organization when identifying assets. The process of compiling an inventory of assets is an important prerequisite of risk management (see also ISO/IEC 27000 and ISO/IEC 27005[11]).

### 8.1.2 Ownership of assets

Control

Assets maintained in the inventory should be owned.

Implementation guidance

Individuals as well as other entities having approved management responsibility for the asset lifecycle qualify to be assigned as asset owners.

A process to ensure timely assignment of asset ownership is usually implemented. Ownership should be assigned when assets are created or when assets are transferred to the organization. The asset owner should be responsible for the proper management of an asset over the whole asset lifecycle.

The asset owner should:

a) ensure that assets are inventoried;

b) ensure that assets are appropriately classified and protected;

c) define and periodically review access restrictions and classifications to important assets, taking into account applicable access control policies;

d) ensure proper handling when the asset is deleted or destroyed.

Other information

The identified owner can be either an individual or an entity who has approved management responsibility for controlling the whole lifecycle of an asset. The identified owner does not necessarily have any property rights to the asset.

Routine tasks may be delegated, e.g. to a custodian looking after the assets on a daily basis, but the responsibility remains with the owner.

In complex information systems, it may be useful to designate groups of assets which act together to provide a particular service. In this case the owner of this service is accountable for the delivery of the service, including the operation of its assets.

### 8.1.3 Acceptable use of assets

Control

Rules for the acceptable use of information and of assets associated with information and information processing facilities should be identified, documented and implemented.

Implementation guidance

Employees and external party users using or having access to the organization's assets should be made aware of the information security requirements of the organization's assets associated with information and information processing facilities and resources. They should be responsible for their use of any information processing resources and of any such use carried out under their responsibility.

其他信息

资产清单有助于确保有效的资产保护，其他目的也可能需要资产清单，例如健康与安全(safety)、保险或财务（资产管理）等原因。

ISO/IEC 27005 提供了组织在识别资产时需要考虑的资产示例，编制资产清单的过程是风险管理的重要前提条件（见 ISO/IEC 27000 和 ISO/IEC 27005）。

### 8.1.2 资产所有权

控制措施

清单中所维护的资产宜分配所有权。

实施指南

已批准对资产生命周期具有管理职责的个人和其他实体，有资格被指定为资产所有者。

通常要实施确保及时分配资产所有权的过程。宜当资产被创建或资产转移至组织时分配所有权。资产所有者宜负责在整个资产生命周期内对资产进行适当管理。

资产所有人宜：

a) 确保资产列入清单；

b) 确保资产进行了适当的分类和保护；

c) 确定并定期评审对重要资产的访问限制和分类，考虑适用的访问控制策略；

d) 当资产被删除或销毁时，确保进行适当处理。

其他信息

确定的所有者或者为个人，或者为实体，他们具备批准的控制资产整个生命周期的管理职责。确定的所有者不一定具备资产的产权。

日常任务可以委派给其他人，例如委派给一个保管人员每天照看资产，但所有者仍保留职责。

在复杂的信息系统中，将一组资产指派给一个所有者可能是比较有用的，它们一起工作来提供特定服务。在这种情况下，服务责任人负责服务的交付，包括资产的运行。

### 8.1.3 资产的可接受使用

控制措施

信息及与信息和信息处理设施有关的资产的可接受使用规则宜被确定、形成文件并加以实施。

实施指南

使用或访问组织资产的雇员和外部方人员宜意识到组织中与信息、信息处理设施和资源相关的资产的信息安全要求。他们宜对其所有信息处理资源的使用行为负责，这种使用不能超出其职责范围。

### 8.1.4 Return of assets

Control

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

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.

In cases where an employee or external party user purchases the organization's equipment or uses their own personal equipment, procedures should be followed to ensure that all relevant information is transferred to the organization and securely erased from the equipment (see 11.2.7).

In cases where an employee or external party user has knowledge that is important to ongoing operations, that information should be documented and transferred to the organization.

During the notice period of termination, the organization should control unauthorized copying of relevant information (e.g. intellectual property) by terminated employees and contractors.

## 8.2 Information classification

Objective: 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

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

Implementation guidance

Classifications and associated protective controls for information should take account of business needs for sharing or restricting information, as well as legal requirements. Assets other than information can also be classified in conformance with classification of information which is stored in, processed by or otherwise handled or protected by the asset.

Owners of information assets should be accountable for their classification.

The classification scheme should include conventions for classification and criteria for review of the classification over time. The level of protection in the scheme should be assessed by analysing confidentiality, integrity and availability and any other requirements for the information considered. The scheme should be aligned to the access control policy (see 9.1.1).

Each level should be given a name that makes sense in the context of the classification scheme's application.

The scheme should be consistent across the whole organization so that everyone will classify information and related assets in the same way, have a common understanding of protection requirements and apply the appropriate protection.

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. Results of classification should be updated in accordance with changes of their value, sensitivity and criticality through their life-cycle.

Other information

### 8.1.4 资产的归还

控制措施

所有的雇员和外部方人员在终止任用、合同或协议时，宜归还他们使用的所有组织资产。

实施指南

终止过程宜被正式化以包括归还所有先前发放的组织拥有或交托的物理和电子资产。

当雇员或第三方人员购买了组织的设备或使用他们自己的个人设备时，宜遵循规程确保所有相关的信息已转移给组织，并且已从设备中安全地删除（见 11.2.7）。

当一个雇员或第三方人员拥有的知识对正在进行的操作具有重要意义时，此信息宜形成文件并转移给组织。

在终止的离职通知期内，组织宜控制已终止的雇员和第三方人员未授权复制有关信息（例如知识产权）。

## 8.2 信息分类

| |
|---|
| 目标：确保信息按照其对组织的重要性受到适当级别的保护。 |

### 8.2.1 信息的分类

控制措施

信息宜按照法律要求、价值、关键性以及它对未授权泄露或修改的敏感性予以分类。

实施指南

信息的分类及相关保护控制措施宜考虑到共享或限制信息的业务需求以及法律要求。除信息之外的资产也能按照所存储、加工及由其处理或保护的信息的类别予以分类。

信息资产的所有者宜对他们的分类负有责任。

分类机制宜包括分类的约定及一段时间后对分类进行评审的准则。机制中的保护级别宜通过分析被考虑信息的保密性、完整性、可用性及其他要求予以评估。机制宜与访问控制策略（见 9.1.1）结合起来。

每个级别宜给定一个名称，使其在分类机制应用的环境中是有意义的。

整个组织的分类机制宜是一致的，以便于每个人使用同样的方式对信息和相关资产进行分类，并对保护要求达成共识，从而应用适当的保护。

分类宜纳入组织的过程中，在整个组织中是一致和连贯的。分类的结果宜基于其对组织的敏感性和关键性表明资产的价值，例如根据保密性、完整性和可用性。分类的结果宜在资产的生命周期中按照他们价值、敏感性和关键性的变化予以更新。

其他信息

Classification provides people who deal with information with a concise indication of how to handle and protect it. Creating groups of information with similar protection needs and specifying information security procedures that apply to all the information in each group facilitates this. This approach reduces the need for case-by-case risk assessment and custom design of controls.

Information can cease to be sensitive or critical after a certain period of time, for example, when the information has been made public. These aspects should be taken into account, as over-classification can lead to the implementation of unnecessary controls resulting in additional expense or on the contrary under-classification can endanger the achievement of business objectives.

An example of an information confidentiality classification scheme could be based on four levels as follows:

a) disclosure causes no harm;

b) disclosure causes minor embarrassment or minor operational inconvenience;

c) disclosure has a significant short term impact on operations or tactical objectives;

d) disclosure has a serious impact on long term strategic objectives or puts the survival of the organization at risk.

### 8.2.2 Labelling of information

Control

An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.

"Implementation guidance"

Procedures for information labelling need to cover information and its related assets in physical and electronic formats. The labelling should reflect the classification scheme established in 8.2.1. The labels should be easily recognizable. The procedures should give guidance on where and how labels are attached in consideration of how the information is accessed or the assets are handled depending on the types of media. The procedures can define cases where labelling is omitted, e.g. labelling of non-confidential information to reduce workloads. Employees and contractors should be made aware of labelling procedures.

Output from systems containing information that is classified as being sensitive or critical should carry an appropriate classification label.

Other information

Labelling of classified information is a key requirement for information sharing arrangements. Physical labels and metadata are a common form of labelling.

Labelling of information and its related assets can sometimes have negative effects. Classified assets are easier to identify and accordingly to steal by insiders or external attackers.

### 8.2.3 Handling of assets

Control

Procedures for handling assets should be developed and implemented in accordance with the information classification scheme adopted by the organization.

Implementation guidance

Procedures should be drawn up for handling, processing, storing and communicating information consistent with its classification (see 8.2.1).

分类为处理信息的人员提供了一个如何处理和保护信息的简明指示。为具有类似保护需求的信息创建组，指定信息安全规程并应用到每个组设施中的所有信息。这个方法减少了逐一进行风险评估的需求，可定制控制措施的设计。

在一段时间后，信息不再是敏感的或关键的，例如，当该信息已经公开时。这些方面宜予以考虑，因为过度分类致使实施不必要的控制措施，从而导致附加成本，反之，适度分类可促使实现业务目标。

信息保密性分类机制的示例可基于以下四个级别：

a) 泄露不会导致损害；

b) 泄露可导致轻微的困窘或轻微的操作不便；

c) 泄露对操作或战术目标有显著的短期影响；

d) 泄露有对长期战略目标有严重的影响，或使组织的生存处于风险之中。

### 8.2.2 信息的标记

控制措施

宜按照组织所采纳的信息分类机制建立和实施一组合适的信息标记规程。

实施指南

信息标记的规程需要涵盖物理和电子格式的信息及其相关资产。标记宜反映 8.2.1 中建立的分类机制。标记宜易于识别。规程宜给出关于在哪儿及如何附加标记的指南，基于介质的类型考虑信息如何被访问或资产如何被处理。规程可定义当可省略标记的情况，例如为减少工作量，可省略非保密信息的标记。宜使雇员和承包方人员知悉标记规程。

包含分类为敏感或关键信息的系统输出宜在该输出中携带合适的分类标记。

其他信息

分类信息的标记是信息共享布置的一个关键要求。物理标记和元数据是常用的标记形式。

信息及其相关资产的标记有时具有负面的影响。分类的资产易于识别，导致被入侵者或外部攻击者盗取。

### 8.2.3 信息的处理

控制措施

宜按照组织所采纳的信息分类机制建立和实施处理资产的规程。

实施指南

宜为处理、加工、存储和沟通信息制定规程，与其分类一致（见 8.2.1）。

The following items should be considered:

a) access restrictions supporting the protection requirements for each level of classification;

b) maintenance of a formal record of the authorized recipients of assets;

c) protection of temporary or permanent copies of information to a level consistent with the protection of the original information;

d) storage of IT assets in accordance with manufacturers' specifications;

e) clear marking of all copies of media for the attention of the authorized recipient.

The classification scheme used within the organization may not be equivalent to the schemes used by other organizations, even if the names for levels are similar; in addition, information moving between organizations can vary in classification depending on its context in each organization, even if their classification schemes are identical.

Agreements with other organizations that include information sharing should include procedures to identify the classification of that information and to interpret the classification labels from other organizations.

## 8.3 Media handling

| Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media. |
|---|

### 8.3.1 Management of removable media

Control

Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

Implementation guidance

The following guidelines for the management of removable media should be considered:

a) if no longer required, the contents of any re-usable media that are to be removed from the organization should be made unrecoverable;

b) where necessary and practical, authorization should be required for media removed from the organization and a record of such removals should be kept in order to maintain an audit trail;

c) all media should be stored in a safe, secure environment, in accordance with manufacturers' specifications;

d) if data confidentiality or integrity are important considerations, cryptographic techniques should be used to protect data on removable media;

e) to mitigate the risk of media degrading while stored data are still needed, the data should be transferred to fresh media before becoming unreadable;

f) multiple copies of valuable data should be stored on separate media to further reduce the risk of coincidental data damage or loss;

g) registration of removable media should be considered to limit the opportunity for data loss;

h) removable media drives should only be enabled if there is a business reason for doing so;

i) where there is a need to use removable media the transfer of information to such media should be monitored.

宜考虑下列事项：

a) 访问限制支持每个分类级别的保护要求；

b) 维护资产授权接收的正式记录；

c) 与原始信息的保护级别一样，对信息的临时或永久拷贝进行保护；

d) 按照制造商说明保存 IT 资产；

e) 为引起授权接收者的注意，所有介质拷贝都有清晰的标志。

即使级别的名字类似，组织内部所用的分类机制也可能不同于其他组织所用的机制；此外，信息在组织间转移时可能类别会发生变化，这主要基于每个组织的环境，即使他们的分类机制是一样的。

与其他组织签署的包括信息共享的协议宜有规程来识别信息的类别，并解释其他组织的分类标记。

## 8.3 介质处置

| |
|---|
| 目标：防止存储在介质上的信息遭受未授权泄露、修改、移动或销毁。 |

### 8.3.1 可移动介质的管理

控制措施

宜按照组织所采纳的分类机制实施可移动介质的管理规程。

实施指南

对于可移动介质的管理，宜考虑下列指南：

a） 对于从组织取走的任何可重用的介质中的内容，如果不再需要，要使其不可重现；

b） 如果必要并可行，对于从组织取走的所有介质要要求授权，所有这种移动的记录要加以保持，以保持审核踪迹；

c） 要将所有介质存储在符合制造商说明的安全、保密的环境中；

d） 如果数据保密性或完整性是重要的考虑事项，宜使用加密技术来保护在可移动介质中的数据；

e） 当仍然需要存储于介质中的数据时，为减缓介质退化风险，宜在其变的不可读之前，将数据转移到新的介质中；

f） 重要数据的多份拷贝宜存储于单独的介质中，进一步降低数据同时损坏或丢失的风险；

g） 宜考虑可移动介质的登记，以减少数据丢失的机会；

h） 只要在有业务要求时，才使用可移动介质；

i） 当有需求使用可移动介质时，宜监视信息转移到介质的过程。

Procedures and authorization levels should be documented.

### 8.3.2 Disposal of media

Control

Media should be disposed of securely when no longer required, using formal procedures.

Implementation guidance

Formal procedures for the secure disposal of media should be established to minimize the risk of confidential information leakage to unauthorized persons. The procedures for secure disposal of media containing confidential information should be proportional to the sensitivity of that information. The following items should be considered:

a) media containing confidential information should be stored and disposed of securely, e.g. by incineration or shredding, or erasure of data for use by another application within the organization;

b) procedures should be in place to identify the items that might require secure disposal;

c) it may be easier to arrange for all media items to be collected and disposed of securely, rather than attempting to separate out the sensitive items;

d) many organizations offer collection and disposal services for media; care should be taken in selecting a suitable external party with adequate controls and experience;

e) disposal of sensitive items should be logged in order to maintain an audit trail.

When accumulating media for disposal, consideration should be given to the aggregation effect, which can cause a large quantity of non-sensitive information to become sensitive.

Other information

Damaged devices containing sensitive data may require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded (see 11.2.7).

### 8.3.3 Physical media transfer

Control

Media containing information should be protected against unauthorized access, misuse or corruption during transportation.

Implementation guidance

The following guidelines should be considered to protect media containing information being transported:

a) reliable transport or couriers should be used;

b) a list of authorized couriers should be agreed with management;

c) procedures to verify the identification of couriers should be developed;

d) packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications, for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields;

e) logs should be kept, identifying the content of the media, the protection applied as well as recording the times of transfer to the transit custodians and receipt at the destination.

Other information

规程和授权级别宜形成文件。

### 8.3.2 介质的处置

控制措施

不再需要的介质，宜使用正式的规程可靠并安全地处置。

实施指南

宜建立安全处置介质的正式规程，以使保密信息泄露给未授权人员的风险减至最小。安全处置包含保密信息的介质的规程宜与信息的敏感性相对应。宜考虑下列条款：

a) 包含有保密信息的介质宜安全地存储和处置，例如，利用焚化或切碎的方法，或者将数据删除供组织内其他应用使用；

b) 宜有规程识别可能需要安全处置的项目；

c) 安排把所有介质部件收集起来并进行安全处置，比试图分离出敏感部件可能更容易；

d) 许多组织对介质提供收集和处置服务；宜注意选择具有足够控制措施和经验的合适的外部方；

e) 处置敏感部件宜做记录，以便保持审核踪迹。

当处置堆积的介质时，对集合效应宜予以考虑，它可使大量不敏感信息变成敏感信息。

其他信息

已损坏的包含敏感数据的设备可能需要实施风险评估以确定物品是否需要进行物理毁坏，而不是送去修理或丢弃（见 11.2.7）。

### 8.3.3 物理介质传输

控制措施

包含信息的介质在运送时，宜防止未授权的访问、不当使用或毁坏。

实施指南

为保护传输的包含信息的介质，宜考虑下列指南：

a) 要使用可靠的运输或送信人；

b) 授权的送信人列表要经管理者批准；

c) 要开发验证送信人身份信息的规程；

d) 包装要足以保护信息免遭在运输期间可能出现的任何物理损坏，并且符合制造商的规范，例如防止可能减少介质恢复效力的任何环境因素，例如暴露于过热、潮湿或电磁区域；

e) 宜保存日志，确定介质的内容、所应用的保护手段并记录交付给传输保管人的时间和在目的地接收的时间。

其他信息

Information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending media via the postal service or via courier. In this control, media include paper documents.

When confidential information on media is not encrypted, additional physical protection of the media should be considered.

# 9 Access control

## 9.1 Business requirements of access control

| Objective: To limit access to information and information processing facilities. |
|---|

### 9.1.1 Access control policy

Control

An access control policy should be established, documented and reviewed based on business and information security requirements.

Implementation guidance

Asset owners should determine appropriate access control rules, access rights and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls reflecting the associated information security risks.

Access controls are both logical and physical (see Clause 11) and these should be considered together. Users and service providers should be given a clear statement of the business requirements to be met by access controls.

The policy should take account of the following:

a) security requirements of business applications;

b) policies for information dissemination and authorization, e.g. the need-to-know principle and information security levels and classification of information (see 8.2);

c) consistency between the access rights and information classification policies of systems and networks;

d) relevant legislation and any contractual obligations regarding limitation of access to data or services (see 18.1);

e) management of access rights in a distributed and networked environment which recognizes all types of connections available;

f) segregation of access control roles, e.g. access request, access authorization, access administration;

g) requirements for formal authorization of access requests (see 9.2.1 and 9.2.2);

h) requirements for periodic review of access rights (see 9.2.5);

i) removal of access rights (see 9.2.6);

j) archiving of records of all significant events concerning the use and management of user identities and secret authentication information;

k) roles with privileged access (see 9.2.3).

Other information

信息在物理传输期间（例如通过邮政服务或送信人传送）易遭受未授权访问、不当使用或破坏。在此项控制中，介质包括纸质文件。

当介质中的保密信息没有加密时，宜考虑附加的物理保护手段。

# 9 访问控制

## 9.1 访问控制的业务要求

| |
|---|
| 目标：限制对信息和信息处理设施的访问。 |

### 9.1.1 访问控制策略

控制措施

访问控制策略宜建立、形成文件，并基于业务和信息安全要求进行评审。

实施指南

资产所有者宜为特定用户角色访问其资产确定适当的访问控制规则、访问权限和限制，反映相关信息安全风险的控制措施要具备足够的细节和严格性。

访问控制包括逻辑的和物理的（见 11），它们宜一起考虑。宜给用户和服务提供商提供一份访问控制要满足的业务要求的清晰说明。

策略宜考虑到下列内容：

a） 业务应用的安全要求；

b） 信息分发和授权的策略，例如“需要则知道”的原则、信息安全级别和信息分类（见 8.2）；

c） 不同系统和网络的访问权限和信息分类策略之间的一致性；

d） 关于限制访问数据或服务的相关法律和合同义务（见 18.1）；

e） 在认可各种可用连接类型的分布式和网络化环境中的访问权限的管理；

f） 访问控制角色的分离，例如访问请求、访问授权、访问管理；

g） 访问请求的正式授权要求（见 9.2.1）；

h） 访问权限的定期评审要求（见 9.2.5）；

i） 访问权限的撤销（见 9.2.6）；

j） 关于用户身份和秘密鉴别信息使用和管理的所有重大事件记录的存档；

k） 具有特权的访问角色（见 9.2.3）。

其他信息

Care should be taken when specifying access control rules to consider:

a) establishing rules based on the premise "Everything is generally forbidden unless expressly permitted" rather than the weaker rule "Everything is generally permitted unless expressly forbidden";

b) changes in information labels (see 8.2.2) that are initiated automatically by information processing facilities and those initiated at the discretion of a user;

c) changes in user permissions that are initiated automatically by the information system and those initiated by an administrator;

d) rules which require specific approval before enactment and those which do not.

Access control rules should be supported by formal procedures (see 9.2, 9.3, 9.4) and defined responsibilities (see 6.1.1, 9.3).

Role based access control is an approach used successfully by many organisations to link access rights with business roles.

Two of the frequent principles directing the access control policy are:

a) Need-to-know: you are only granted access to the information you need to perform your tasks (different tasks/roles mean different need-to-know and hence different access profile);

b) Need-to-use: you are only granted access to the information processing facilities (IT equipment, applications, procedures, rooms) you need to perform your task/job/role.

### 9.1.2 Access to networks and network services

Control

Users should only be provided with access to the network and network services that they have been specifically authorized to use.

Implementation guidance

A policy should be formulated concerning the use of networks and network services. This policy should cover:

a) the networks and network services which are allowed to be accessed;

b) authorization procedures for determining who is allowed to access which networks and networked services;

c) management controls and procedures to protect access to network connections and network services;

d) the means used to access networks and network services (e.g. use of VPN or wireless network);

e) user authentication requirements for accessing various network services;

f) monitoring of the use of network services.

The policy on the use of network services should be consistent with the organization's access control policy (see 9.1.1).

Other information

Unauthorized and insecure connections to network services can affect the whole organization. This control is particularly important for network connections to sensitive or critical business applications or to users in high-risk locations, e.g. public or external areas that are outside the organization's information security management and control.

在规定访问控制规则时，宜认真考虑下列内容：

a） 在“未经明确允许，则一律禁止”的前提下，而不是“未经明确禁止，一律允许”的弱规则的基础上建立规则；

b） 信息处理设施自动启动的信息标记（见 8.2.2）和用户任意启动的信息标记的变更；

c） 信息系统自动启动的用户许可变更和由管理员启动的那些用户许可变更；

d） 在颁发之前，需要特别批准的规则以及无须批准的那些规则。

访问控制规则宜有正式的规程支持（见 9.2、9.3、9.4），并定义职责（见 6.1.1、9.2、15.1）。

基于访问控制的规则是成功用于许多组织、联系访问权限和业务角色的方法。

指导访问控制策略的两个常用原则是：

a） 需要则知道：用户仅被授权访问执行其任务所需要的信息（不同的任务/角色意味着不同的需要知道的内容，因此具有不同的访问轮廓）

b） 需要则使用：用户仅被授权访问执行其任务/工作/角色所需要的信息处理设施（IT 设备、应用、规程、房间）。

### 9.1.2 网络和网络服务的访问

控制措施

用户宜仅能访问已获专门授权使用的网络和网络服务。

实施指南

宜制定关于使用网络和网络服务的策略。这一策略宜包括：

a） 允许被访问的网络和网络服务；

b） 确定允许哪个人访问哪些网络和网络服务的授权规程；

c） 保护访问网络连接和网络服务的管理控制措施和规程；

d） 访问网络和网络服务使用的手段（例如，VPN 或无线网络的使用）。

e） 访问各种网络服务的用户鉴别要求；

f） 监视网络服务的使用。

网络服务使用策略宜与组织的访问控制策略相一致（见 9.1.1）。

其他信息

与网络服务的未授权和不安全连接可以影响整个组织。对于到敏感或关键业务应用的网络连接或与高风险位置（例如，超出组织安全管理和控制的公共区域或外部区域）的用户的网络连接而言，这一控制措施特别重要。

## 9.2 User access management

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

### 9.2.1 User registration and de-registration

Control

A formal user registration and de-registration process should be implemented to enable assignment of access rights.

Implementation guidance

The process for managing user IDs should include:

a) using unique user IDs to enable users to be linked to and held responsible for their actions; the use of shared IDs should only be permitted where they are necessary for business or operational reasons and should be approved and documented;

b) immediately disabling or removing user IDs of users who have left the organization (see 9.2.6);

c) periodically identifying and removing or disabling redundant user IDs;

d) ensuring that redundant user IDs are not issued to other users.

Other information

Providing or revoking access to information or information processing facilities is usually a two-step procedure:

a) assigning and enabling, or revoking, a user ID;

b) providing, or revoking, access rights to such user ID (see 9.2.2).

### 9.2.2 User access provisioning

Control

A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.

Implementation guidance

The provisioning process for assigning or revoking access rights granted to user IDs should include:

a) obtaining authorization from the owner of the information system or service for the use of the information system or service (see control 8.1.2); separate approval for access rights from management may also be appropriate;

b) verifying that the level of access granted is appropriate to the access policies (see 9.1) and is consistent with other requirements such as segregation of duties (see 6.1.2);

c) ensuring that access rights are not activated (e.g. by service providers) before authorization procedures are completed;

d) maintaining a central record of access rights granted to a user ID to access information systems and services;

e) adapting access rights of users who have changed roles or jobs and immediately removing or blocking access rights of users who have left the organization;

## 9.2 用户访问管理

| |
|---|
| 目标：确保授权用户访问系统和服务，并防止未授权的访问。 |

### 9.2.1 用户注册及注销

控制措施

宜实施正式的用户注册及注销规程，使访问权限得以分配。

实施指南

管理用户 ID 的过程宜包括：

a） 使用唯一用户 ID，使得用户与其行为链接起来，并对其行为负责；在对于业务或操作而言必要时，才允许使用组 ID，并宜经过批准和形成文件；

b） 立即禁用或取消已离开组织的用户的用户 ID（见 9.2.5）；

c） 定期识别并撤销或禁用多余的用户 ID；

d） 确保多余的用户 ID 不会分发给其他用户。

其他信息

提供或撤销对信息或信息处理设施的访问通常分两个步骤：

a） 分配并启动，或撤销，一个用户 ID（本控制项）；

b） 给这些用户 ID 提供，或撤销，访问权限（见 9.2.2）。

### 9.2.2 用户访问开通

控制措施

宜实施正式的用户访问开通过程，以分配或撤销所有系统和服务所有用户类型的访问权限。

实施指南

分配或撤销授予用户 ID 的访问权限的开通过程宜包括：

a） 为使用信息系统或服务，从信息系统或服务的所有者获得授权（见 8.1.2）；取得管理者对访问权限的单独批准也是合适的；

b） 验证授予访问的级别是否适于访问策略（见 9.1），且与其他要求一致，例如职责分离（见 6.1.5）；

c） 在授权过程完成之前确保访问权限不会被激活（例如，被服务提供商）；

d） 维护授予用户 ID 访问信息系统和服务的访问权限的主要记录；

e） 修改已变更角色或职位的用户的访问权限，立即 撤销或封锁离开组织的用户的访问权限；

f) periodically reviewing access rights with owners of the information systems or services (see 9.2.5).

Other information

Consideration should be given to establishing user access roles based on business requirements that summarize a number of access rights into typical user access profiles. Access requests and reviews (see 9.2.4) are easier managed at the level of such roles than at the level of particular rights.

Consideration should be given to including clauses in personnel contracts and service contracts that specify sanctions if unauthorized access is attempted by personnel or contractors (see 7.1.2, 7.2.3, 13.2.4, 15.1.2).

### 9.2.3 Management of privileged access rights

Control

The allocation and use of privileged access rights should be restricted and controlled.

Implementation guidance

The allocation of privileged access rights should be controlled through a formal authorization process in accordance with the relevant access control policy (see control 9.1.1). The following steps should be considered:

a) the privileged access rights associated with each system or process, e.g. operating system, database management system and each application and the users to whom they need to be allocated should be identified;

b) privileged access rights should be allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy (see 9.1.1), i.e. based on the minimum requirement for their functional roles;

c) an authorization process and a record of all privileges allocated should be maintained. Privileged access rights should not be granted until the authorization process is complete;

d) requirements for expiry of privileged access rights should be defined;

e) privileged access rights should be assigned to a user ID different from those used for regular business activities. Regular business activities should not be performed from privileged ID;

f) the competences of users with privileged access rights should be reviewed regularly in order to verify if they are in line with their duties;

g) specific procedures should be established and maintained in order to avoid the unauthorized use of generic administration user IDs, according to systems' configuration capabilities;

h) for generic administration user IDs, the confidentiality of secret authentication information should be maintained when shared (e.g. changing passwords frequently and as soon as possible when a privileged user leaves or changes job, communicating them among privileged users with appropriate mechanisms).

Other information

Inappropriate use of system administration privileges (any feature or facility of an information system that enables the user to override system or application controls) is a major contributory factor to failures or breaches of systems.

### 9.2.4 Management of secret authentication information of users

Control

The allocation of secret authentication information should be controlled through a formal management process.

f） 定期与信息系统或服务的所有者评审访问权限（见 9.2.4）。

其他信息

宜考虑基于业务要求建立用户访问角色，将大量的访问权限归结到典型的用户访问轮廓中。在这种角色级别上对访问请求和评审（见 9.2.4）进行管理要比在特定的权限级别上容易些。

宜考虑在人员合同和服务合同中将在员工或承包方人员试图进行未授权访问时的有关处罚措施的条款包括进去（见 7.1.2、7.2.3、13.2.4 和 15.1.2）。

### 9.2.3 特殊访问权限管理

控制措施

宜限制和控制特殊访问权限的分配及使用。

实施指南

宜采取相关控制策略（见 9.1.1）通过正式的授权过程控制特殊访问权限的分配。宜考虑下列步骤：

a） 要标识出与每个系统或程序（例如，操作系统、数据库管理系统和每个应用程序）相关的特殊访问权限和所需分配的用户；

b） 特殊访问权限要按照访问控制策略（见 9.1.1）在“按需使用”和“一事一议”的基础上分配给用户，即仅当需要时，才为其职能角色分配最低要求；

c） 宜维护所分配的各个特殊访问权限的授权过程及其记录。在未完成授权过程之前，不要授予特殊访问权限；

d） 宜定义特殊访问权限的期限要求；

e） 特殊访问权限宜分配给非日常业务活动的用户 ID，日常业务活动不宜使用特权账户执行；

f） 具有特殊访问权限的用户的能力宜定期实施评审，以验证他们是否与其责任相一致；

g） 宜按照系统配置能力建立和维护特定规程，以避免通用管理用户 ID 的未授权使用；

h） 对于通用管理用户 ID，当共享时宜维护秘密鉴别信息的保密性（例如经常变更口令、尽可能当一个特权用户离开或变化职位时也变更口令，使用适当的机制在特权用户中进行传达）。

其他信息

系统管理特殊权限（使用户无视系统或应用控制措施的信息系统的任何特性或设施）的不恰当使用可能是一种导致系统故障或违规的主要因素。

### 9.2.4 用户秘密鉴别信息管理

控制措施

宜通过正式的管理过程控制秘密鉴别信息的分配。

Implementation guidance

The process should include the following requirements:

a) users should be required to sign a statement to keep personal secret authentication information confidential and to keep group (i.e. shared) secret authentication information solely within the members of the group; this signed statement may be included in the terms and conditions of employment (see 7.1.2);

b) when users are required to maintain their own secret authentication information they should be provided initially with secure temporary secret authentication information`, which they are forced to change on first use;

c) procedures should be established to verify the identity of a user prior to providing new, replacement or temporary secret authentication information;

d) temporary secret authentication information should be given to users in a secure manner; the use of external parties or unprotected (clear text) electronic mail messages should be avoided;

e) temporary secret authentication information should be unique to an individual and should not be guessable;

f) users should acknowledge receipt of secret authentication information;

g) default vendor secret authentication information should be altered following installation of systems or software.

Other information

Passwords are a commonly used type of secret authentication information and are a common means of verifying a user's identity. Other types of secret authentication information are cryptographic keys and other data stored on hardware tokens (e.g. smart cards) that produce authentication codes.

### 9.2.5 Review of user access rights

Control

Asset owners should review users' access rights at regular intervals.

Implementation guidance

The review of access rights should consider the following:

a) users' access rights should be reviewed at regular intervals and after any changes, such as promotion, demotion or termination of employment (see Clause 7);

b) user access rights should be reviewed and re-allocated when moving from one role to another within the same organization;

c) authorizations for privileged access rights should be reviewed at more frequent intervals;

d) privilege allocations should be checked at regular intervals to ensure that unauthorized privileges have not been obtained;

e) changes to privileged accounts should be logged for periodic review.

Other information

This control compensates for possible weaknesses in the execution of controls 9.2.1, 9.2.2 and 9.2.6.

### 9.2.6 Removal or adjustment of access rights

Control

实施指南

此过程宜包括下列要求：

a） 要求用户签署一份声明，以保证个人秘密鉴别信息的保密性和组信息（例如共享）秘密鉴别信息仅在该组成员范围内使用；签署的声明可包括在任用条款和条件中（见 7.1.2）；

b） 若需要用户维护自己的秘密鉴别信息，要在初始时提供给他们一个安全的临时秘密鉴别信息，并强制其在首次使用时改变；

c） 在提供一个新的、代替的或临时的秘密鉴别信息之前，宜建立验证用户身份的规程；

d） 宜以安全的方式将临时秘密鉴别信息给予用户；宜避免使用外部方或未保护的（明文）电子邮件消息；

e） 临时秘密鉴别信息对个人而言宜是唯一的、不可猜测的；

f） 用户宜确认收到秘密鉴别信息；

g） 宜在系统或软件安装后改变提供商的默认秘密鉴别信息。

其他信息

口令是秘密鉴别信息的通常使用的一种类型，是验证用户身份的一种常用手段。其他类型的秘密鉴别信息包括密钥和存储于硬件令牌（例如智能卡）可产生鉴别码的其他数据。

### 9.2.5 用户访问权限的复查

控制措施

资产所有者宜定期复查用户的访问权限。

实施指南

访问权限的复查宜考虑下列指南：

a) 宜定期和在任何变更之后（例如提升、降级或雇用终止（见 7)），对用户的访问权限进行复查；

b) 当在同一个组织中从一个角色换到另一个时，宜复查和重新分配用户的访问权限；

c) 对于特殊访问权限的授权宜在更频繁的时间间隔内进行复查；

d) 要定期核查特殊权限的分配，以确保不能获得未授权的特殊权限；

e) 具有特殊权限的帐户的变更要在周期性复查时记入日志。

其他信息

本控制补偿了在执行控制措施 9.2.1、9.2.2 和 9.2.6 时可能存在的弱点。

### 9.2.6 撤销或调整访问权限

控制措施

The access rights of all employees and external party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.

Implementation guidance

Upon termination, the access rights of an individual to information and assets associated with information processing facilities and services should be removed or suspended. This will determine whether it is necessary to remove access rights. Changes of employment should be reflected in removal of all access rights that were not approved for the new employment. The access rights that should be removed or adjusted include those of physical and logical access. Removal or adjustment can be done by removal, revocation or replacement of keys, identification cards, information processing facilities or subscriptions. Any documentation that identifies access rights of employees and contractors should reflect the removal or adjustment of access rights. If a departing employee or external party user has known passwords for user IDs remaining active, these should be changed upon termination or change of employment, contract or agreement.

Access rights for information and assets associated with information processing facilities should be reduced or removed before the employment terminates or changes, depending on the evaluation of risk factors such as:

a) whether the termination or change is initiated by the employee, the external party user or by management, and the reason for termination;

b) the current responsibilities of the employee, external party user or any other user;

c) the value of the assets currently accessible.

Other information

In certain circumstances access rights may be allocated on the basis of being available to more people than the departing employee or external party user, e.g. group IDs. In such circumstances, departing individuals should be removed from any group access lists and arrangements should be made to advise all other employees and external party users involved to no longer share this information with the person departing.

In cases of management-initiated termination, disgruntled employees or external party users can deliberately corrupt information or sabotage information processing facilities. In cases of persons resigning or being dismissed, they may be tempted to collect information for future use.

## 9.3 User responsibilities

Objective: To make users accountable for safeguarding their authentication information.

### 9.3.1 Use of secret authentication information

Control

Users should be required to follow the organization's practices in the use of secret authentication information.

Implementation guidance

All users should be advised to:

a) keep secret authentication information confidential, ensuring that it is not divulged to any other parties, including people of authority;

b) avoid keeping a record (e.g. on paper, software file or hand-held device) of secret authentication information, unless this can be stored securely and the method of storing has been approved (e.g. password vault);

所有雇员、外部方人员对信息和信息处理设施的访问权限宜在任用、合同或协议终止时撤销，或在变化时调整。

实施指南

任用终止时，个人对与信息处理设施和服务有关的信息和资产的访问权限宜被撤销或暂停。这将决定撤销访问权限是否是必要的。任用的变更宜体现在不适用于新岗位的访问权限的撤销上。宜撤销或调整的访问权限包括物理和逻辑访问的权限。撤销或调整可通过撤销、取消或替换密钥、识别卡、信息处理设施或订阅来实现。识别员工和承包方人员访问权限的任何文件宜反映访问权限的撤销或调整。如果一个已离开的雇员或外部方人员知道仍保持活动状态的用户 ID 的密码，则宜在任用、合同或协议终止或变更后改变口令。

对与信息处理设施有关的信息和资产的访问权限在任用终止或变更前是否减少或删除，依赖于对风险因素的评价，例如：

a) 终止或变更是由雇员、外部方人员发起还是由管理者发起，以及终止的原因；

b) 雇员、外部方人员或任何其他用户的现有职责；

c) 当前可访问资产的价值。

其他信息

在某些情况下，访问权限的分配基于对多人可用而不是只基于离开的雇员或外部方人员，例如组 ID。在这种情况下，离开的人员宜从组访问列表中删除，还宜建议所有相关的其他雇员和外部方人员不宜再与已离开的人员共享信息。

在管理者发起终止的情况下，不满的雇员或外部方人员会故意破坏信息或破坏信息处理设施。在员工辞职或被解雇的情况下，他们可能为将来的使用而收集必要的信息。

## 9.3 用户职责

| |
|---|
| 目标：使用户承担保护鉴别信息的责任。 |

### 9.3.1 使用秘密鉴别信息

控制措施

宜要求用户在使用秘密鉴别信息时，遵循组织的实践。

实施指南

建议所有用户宜：

a） 保密秘密鉴别信息，确保不泄露给其他人，包括授权的人；

b） 避免保留秘密鉴别信息的记录（例如在纸上、软件文件中或手持设备中），除非可以对其进行安全地存储及存储方法得到批准（例如口令保管库）；

c) change secret authentication information whenever there is any indication of its possible compromise;

d) when passwords are used as secret authentication information, select quality passwords with sufficient minimum length which are:

   1) easy to remember;

   2) not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers and dates of birth etc.;

   3) not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries);

   4) free of consecutive identical, all-numeric or all-alphabetic characters;

   5) if temporary, changed at the first log-on;

e) not share individual user's secret authentication information;

f) ensure proper protection of passwords when passwords are used as secret authentication information in automated log-on procedures and are stored;

g) not use the same secret authentication information for business and non-business purposes.

Other information

Provision of Single Sign On (SSO) or other secret authentication information management tools reduces the amount of secret authentication information that users are required to protect and thus can increase the effectiveness of this control. However, these tools can also increase the impact of disclosure of secret authentication information.

## 9.4 System and application access control

| Objective: To prevent unauthorized access to systems and applications. |
|---|

### 9.4.1 Information access restriction

Control

Access to information and application system functions should be restricted in accordance with the access control policy.

Implementation guidance

Restrictions to access should be based on individual business application requirements and in accordance with the defined access control policy.

The following should be considered in order to support access restriction requirements:

a) providing menus to control access to application system functions;

b) controlling which data can be accessed by a particular user;

c) controlling the access rights of users, e.g. read, write, delete and execute;

d) controlling the access rights of other applications;

e) limiting the information contained in outputs;

f) providing physical or logical access controls for the isolation of sensitive applications, application data, or systems.

c） 每当有任何迹象表明秘密鉴别信息受到损害时就变更秘密鉴别信息；

d） 当用口令作为秘密鉴别信息时，选择具有最小长度的优质口令，这些口令：

1） 要易于记忆；

2） 不能基于别人容易猜测或获得的与使用人相关的信息，例如，名字、电话号码和生日等等；

3） 不容易遭受字典攻击（即，不是由字典中的词所组成的）；

4） 避免连续相同的，全数字的或全字母的字符；

e） 在初次登录时更换临时口令；不要共享个人的用户加密鉴别信息；

f） 当口令作为加密鉴别信息在任何自动登录过程和存储中，宜确保口令得到恰当保护；

g） 不在业务目的和非业务目的中使用相同的加密鉴别信息。

通过单点登录（SSO）或者其他加密鉴别信息管理工具减少了要求用户保护的加密鉴别信息量，增加了这一控制措施的有效性。然而，这些工具也提高了加密鉴别信息披露的影响。

## 9.4 系统和应用访问控制

| |
|---|
| 目标：防止对系统和应用的未授权访问。 |

### 9.4.1 信息访问限制

控制措施

宜依照访问控制策略限制对信息和应用系统功能的访问。

实施指南

对访问的限制宜基于各个业务应用要求和已定义的访问控制策略。

为支持访问限制要求，宜做如下考虑：

a） 提供应用系统控制访问功能的选择菜单；

b） 控制可被特定用户访问的数据；

c） 控制用户的访问权限，如，读、写、删除和执行；

d） 控制其他应用的访问权限；

e） 限制输出所包含的的信息;

f） 为隔离敏感的应用程序、应用数据或系统，提供物理或逻辑访问控制。

### 9.4.2 Secure log-on procedures

Control

Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.

Implementation guidance

A suitable authentication technique should be chosen to substantiate the claimed identity of a user.

Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens or biometric means, should be used.

The procedure for logging into a system or application should be designed to minimize the opportunity for unauthorized access. The log-on procedure should therefore disclose the minimum of information about the system or application, in order to avoid providing an unauthorized user with any unnecessary assistance. A good log-on procedure should:

a) not display system or application identifiers until the log-on process has been successfully completed;

b) display a general notice warning that the computer should only be accessed by authorized users;

c) not provide help messages during the log-on procedure that would aid an unauthorized user;

d) validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect;

e) protect against brute force log-on attempts;

f) log unsuccessful and successful attempts;

g) raise a security event if a potential attempted or successful breach of log-on controls is detected;

h) display the following information on completion of a successful log-on:

   1) date and time of the previous successful log-on;

   2) details of any unsuccessful log-on attempts since the last successful log-on;

i) not display a password being entered;

j) not transmit passwords in clear text over a network;

k) terminate inactive sessions after a defined period of inactivity, especially in high risk locations such as public or external areas outside the organization's security management or on mobile devices;

l) restrict connection times to provide additional security for high-risk applications and reduce the window of opportunity for unauthorized access.

Other information

Passwords are a common way to provide identification and authentication based on a secret that only the user knows. The same can also be achieved with cryptographic means and authentication protocols. The strength of user authentication should be appropriate for the classification of the information to be accessed.

If passwords are transmitted in clear text during the log-on session over a network, they can be captured by a network "sniffer" program.

### 9.4.3 Password management system

Control

Password management systems should be interactive and should ensure quality passwords.

### 9.4.2 安全登录规程

控制措施

在访问控制策略要求下，访问操作系统和应用宜通过安全登录规程加以控制。

实施指南

宜选择适当的鉴别方法，以证明用户所宣称的身份。

当要求强鉴别和身份验证时，宜利用加密、智能卡、令牌或生物特征等方式代替口令。

登录到操作系统或应用程序的规程宜设计成使未授权访问的机会减到最小。因此，登录规程宜公开最少有关系统或应用的信息，以避免给未授权用户提供任何不必要的帮助。良好的登录规程宜：

a） 不显示系统或应用标识符，直到登录过程已成功完成为止；

b） 显示只有已授权的用户才能访问计算机的一般性的告警通知；

c） 在登录规程中，不提供对未授权用户有帮助作用的帮助消息；

d） 仅在所有输入数据完成时才验证登录信息。如果出现差错情况，系统不宜指出数据的哪一部分是正确的或不正确的；

e） 防止暴力尝试登录；

f） 记录不成功的尝试和成功的尝试登录；

g） 如果检测到违反控制措施尝试登录或已成功登录，则引发安全事态;

h） 在成功登录完成时，显示下列信息：

1） 前一次成功登录的日期和时间；

2） 上次成功登录之后的任何不成功登录尝试的细节；

i） 不显示输入的口令；

j） 不在网络上以明文方式传输口令；

k） 不活动会话宜在一个设定的休止期后关闭，特别是在高风险地点（例如组织安全管理范围外的公共区域或外部区域）或使用移动设备上；

l） 宜使用联机时间的限制，为高风险应用程序提供额外的安全，同时降低非授权访问的机会。

其他信息

口令是一种非常通用的提供标识和鉴别的方法，这种标识和鉴别是建立在只有用户知悉的秘密的基础上的。使用密码手段和鉴别协议也可以获得同样的效果。用户标识和鉴别的强度宜和所访问信息的敏感程度相适应。

在网络上登录会话期间，如果口令以明文方式传输，它们可能会被网络上的网络“嗅探器”程序捕获。

### 9.4.3 口令管理系统

控制措施

口令管理系统宜是交互式的，并宜确保优质的口令。

Implementation guidance

A password management system should:

a) enforce the use of individual user IDs and passwords to maintain accountability;

b) allow users to select and change their own passwords and include a confirmation procedure to allow for input errors;

c) enforce a choice of quality passwords;

d) force users to change their passwords at the first log-on;

e) enforce regular password changes and as needed;

f) maintain a record of previously used passwords and prevent re-use;

g) not display passwords on the screen when being entered;

h) store password files separately from application system data;

i) store and transmit passwords in protected form.

Other information

Some applications require user passwords to be assigned by an independent authority; in such cases, points b), d) and e) of the above guidance do not apply. In most cases the passwords are selected and maintained by users.

### 9.4.4 Use of privileged utility programs

Control

The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.

Implementation guidance

The following guidelines for the use of utility programs that might be capable of overriding system and application controls should be considered:

a) use of identification, authentication and authorization procedures for utility programs;

b) segregation of utility programs from applications software;

c) limitation of the use of utility programs to the minimum practical number of trusted, authorized users (see 9.2.3);

d) authorization for ad hoc use of utility programs;

e) limitation of the availability of utility programs, e.g. for the duration of an authorized change;

f) logging of all use of utility programs;

g) defining and documenting of authorization levels for utility programs;

h) removal or disabling of all unnecessary utility programs;

i) not making utility programs available to users who have access to applications on systems where segregation of duties is required.

Other information

实施指南

一个口令管理系统宜：

a） 强制使用个人用户 ID 和口令，以保持可核查性；

b） 允许用户选择和变更他们自己的口令，并且包括一个确认规程，以便考虑到输入出错的情况；

c） 强制选择优质口令；

d） 在第一次登录时强制用户变更临时口令；

e） 根据需要，强制定期变更口令；

f） 维护用户以前使用的口令的记录，并防止重复使用；

g） 在输入口令时，不在屏幕上显示；

h） 口令文件与应用系统数据分开存储；

i） 以保护的形式存储和传输口令。

其他信息

某些应用要求由某个独立授权机构来分配用户口令；在这种情况下，上述指南 b)、d)和 e)不适用。在大多数情况下，口令由用户选择和维护。

### 9.4.4 特殊权限实用工具软件的使用

控制措施

对于可能超越系统和应用程序控制措施的适用工具软件的使用宜加以限制并严格控制。

实施指南

对于可能适用于整个系统或应用控制措施的适用工具软件的使用，宜考虑下列指南：

a） 对适用工具软件使用标识、鉴别和授权规程；

b） 将适用工具软件和应用软件分开；

c） 将使用适用工具软件的用户限制到可信的、已授权的最小实际用户数（也见 9.2.2）；

d） 对适用工具软件的特别使用进行授权；

e） 限制系统实用工具的可用性，例如，在授权变更的期间内；

f） 记录适用工具软件的所有使用；

g） 对适用工具软件的授权级别进行定义并形成文件；

h） 移去或禁用所有不必要的实用工具软件；

i） 当要求责任分割时，禁止访问系统中应用程序的用户使用实用工具软件。

其他信息

Most computer installations have one or more utility programs that might be capable of overriding system and application controls.

### 9.4.5 Access control to program source code

Control

Access to program source code should be restricted.

Implementation guidance

Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) should be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes as well as to maintain the confidentiality of valuable intellectual property. For program source code, this can be achieved by controlled central storage of such code, preferably in program source libraries. The following guidelines should then be considered to control access to such program source libraries in order to reduce the potential for corruption of computer programs:

a) where possible, program source libraries should not be held in operational systems;

b) the program source code and the program source libraries should be managed according to established procedures;

c) support personnel should not have unrestricted access to program source libraries;

d) the updating of program source libraries and associated items and the issuing of program sources to programmers should only be performed after appropriate authorization has been received;

e) program listings should be held in a secure environment;

f) an audit log should be maintained of all accesses to program source libraries;

g) maintenance and copying of program source libraries should be subject to strict change control procedures (see 14.2.2).

If the program source code is intended to be published, additional controls to help getting assurance on its integrity (e.g. digital signature) should be considered.

# 10 Cryptography

## 10.1 Cryptographic controls

| Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information. |
|---|

### 10.1.1 Policy on the use of cryptographic controls

Control

A policy on the use of cryptographic controls for protection of information should be developed and implemented.

Implementation guidance

When developing a cryptographic policy the following should be considered:

a) the management approach towards the use of cryptographic controls across the organization, including the general principles under which business information should be protected;

大多数计算机安装有一个或多个可能超越系统和应用控制措施的实用工具软件。

#### 9.4.5 对程序源代码的访问控制

控制措施

宜限制访问程序源代码。

实施指南

对程序源代码和相关事项（例如设计、说明书、验证计划和确认计划）的访问宜严格控制，以防引入非授权功能和避免无意识的变更，也为了维护有价值知识产权的机密性。对于程序源代码的保存，可以通过这种代码的中央存储控制来实现，更好的是放在源程序库中。为了控制对源程序库的访问以减少潜在的计算机程序的破坏，宜考虑下列指南：

a) 若有可能，在运行系统中不要保留源程序库；

b) 程序源代码和源程序库要根据制定的规程进行管理；

c) 要限制支持人员访问源程序库；

d) 更新源程序库和有关事项，向程序员发布程序源码要在获得适当的授权之后进行；

e) 程序列表要保存在安全的环境中；

f) 要维护对源程序库所有访问的审计日志；

g) 维护和拷贝源程序库要受严格变更控制规程的制约（见 14.2.2）。

如果企图公布程序源代码，宜考虑确保程序源代码完整性的附加控制措施（例如数字签名）。

## 10 密码学

### 10.1 密码控制

| |
|---|
| 目标：恰当和有效的利用密码学保护信息的保密性、真实性或完整性。 |

#### 10.1.1 使用密码控制的策略

控制措施

宜开发和实施使用密码控制措施来保护信息的策略。

实施指南

制定密码策略时，宜考虑下列内容：

a) 组织间使用密码控制的管理方法，包括保护业务信息的一般原则；

b) based on a risk assessment, the required level of protection should be identified taking into account the type, strength and quality of the encryption algorithm required;

c) the use of encryption for protection of information transported by mobile or removable media devices or across communication lines;

d) the approach to key management, including methods to deal with the protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys;

e) roles and responsibilities, e.g. who is responsible for:

   1) the implementation of the policy;

   2) the key management, including key generation (see 10.1.2);

f) the standards to be adopted for effective implementation throughout the organization (which solution is used for which business processes);

g) the impact of using encrypted information on controls that rely upon content inspection (e.g. malware detection).

When implementing the organization's cryptographic policy, consideration should be given to the regulations and national restrictions that might apply to the use of cryptographic techniques in different parts of the world and to the issues of trans-border flow of encrypted information (see 18.1.5).

Cryptographic controls can be used to achieve different information security objectives, e.g.:

a) confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted;

b) integrity/authenticity: using digital signatures or message authentication codes to verify the authenticity or integrity of stored or transmitted sensitive or critical information;

c) non-repudiation: using cryptographic techniques to provide evidence of the occurrence or non-occurrence of an event or action;

d) authentication: using cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources.

Other information

Making a decision as to whether a cryptographic solution is appropriate should be seen as part of the wider process of risk assessment and selection of controls. This assessment can then be used to determine whether a cryptographic control is appropriate, what type of control should be applied and for what purpose and business processes.

A policy on the use of cryptographic controls is necessary to maximize the benefits and minimize the risks of using cryptographic techniques and to avoid inappropriate or incorrect use.

Specialist advice should be sought in selecting appropriate cryptographic controls to meet the information security policy objectives.

### 10.1.2 Key management

Control

A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle.

Implementation guidance

The policy should include requirements for managing cryptographic keys though their whole lifecycle including generating, storing, archiving, retrieving, distributing, retiring and destroying keys.

b) 基于风险评估，宜确定需要的保护级别，并考虑需要的加密算法的类型、强度和质量；

c) 使用加密保护通过可移动或可拆卸的介质、设备或者通信线路传输的敏感信息；

d) 密钥管理方法，包括应对密钥保护的方法，以及在密钥丢失、损害或毁坏后加密信息的恢复方法；

e) 角色和职责，例如，谁负责：

1） 策略的实施；

2） 密钥管理，包括密钥生成（见 10.1.2）；

f) 为在整个组织内有效实施而采用的标准（哪种解决方案用于哪些业务过程）；

g) 使用加密后的信息对依赖于内容检查的控制措施（例如，恶意软件检测）的影响。

当实施组织的密码策略时，宜考虑我国应用密码技术的规定和限制，以及加密信息跨越国界时的问题（见 18.1.5）。

可以使用密码控制措施实现不同的安全目标，例如：

a) 保密性：使用信息加密以保护存储或传输中的敏感或关键信息；

b) 完整性/真实性：使用数字签名或消息鉴别码以保护存储和传输中的敏感或关键信息的真实性和完整性；

c) 抗抵赖性：使用密码技术以提供一个事态或行为发生或未发生的证据；

d) 可认证性：使用密码技术对请求访问实体和资源的用户以及与系统用户有交互的其他系统实体进行身份鉴别。

其他信息

有关一个密码解决方案是否合适的决策，宜被看作更广的风险评估和选择控制措施过程的一部分。该评估可以用来判定一个密码控制措施是否合适，宜运用什么类型的控制措施以及应用于什么目的和业务过程。

使用密码控制措施的策略对于使利益最大化，使利用密码技术的风险最小化，以及避免不合适或不正确的使用而言，十分必要。

宜征求专家建议以选择适当的、满足信息安全策略目标的密码控制。

### 10.1.2 密钥管理

控制措施

宜开发和实施贯穿整个密钥生命周期的关于密钥使用、保护和生存期的策略。

实施指南

策略宜包括的密钥管理要求，其贯穿密钥的整个生命周期，包括密钥的生成、存储、归档、检索、分发、回收和销毁。

Cryptographic algorithms, key lengths and usage practices should be selected according to best practice. Appropriate key management requires secure processes for generating, storing, archiving, retrieving, distributing, retiring and destroying cryptographic keys.

All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorized use as well as disclosure. Equipment used to generate, store and archive keys should be physically protected.

A key management system should be based on an agreed set of standards, procedures and secure methods for:

a) generating keys for different cryptographic systems and different applications;

b) issuing and obtaining public key certificates;

c) distributing keys to intended entities, including how keys should be activated when received;

d) storing keys, including how authorized users obtain access to keys;

e) changing or updating keys including rules on when keys should be changed and how this will be done;

f) dealing with compromised keys;

g) revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an organization (in which case keys should also be archived);

h) recovering keys that are lost or corrupted;

i) backing up or archiving keys;

j) destroying keys;

k) logging and auditing of key management related activities.

In order to reduce the likelihood of improper use, activation and deactivation dates for keys should be defined so that the keys can only be used for the period of time defined in the associated key management policy.

In addition to securely managing secret and private keys, the authenticity of public keys should also be considered. This authentication process can be done using public key certificates, which are normally issued by a certification authority, which should be a recognized organization with suitable controls and procedures in place to provide the required degree of trust.

The contents of service level agreements or contracts with external suppliers of cryptographic services, e.g. with a certification authority, should cover issues of liability, reliability of services and response times for the provision of services (see 15.2).

Other information

The management of cryptographic keys is essential to the effective use of cryptographic techniques. ISO/IEC 11770[2][3][4] provides further information on key management.

Cryptographic techniques can also be used to protect cryptographic keys. Procedures may need to be considered for handling legal requests for access to cryptographic keys, e.g. encrypted information can be required to be made available in an unencrypted form as evidence in a court case.

# 11 Physical and environmental security

## 11.1 Secure areas

| Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities. |
|---|

宜根据最佳实践，选择加密算法、密钥长度和使用规则，恰当的密钥管理要求安全过程包括密钥的生成、存储、归档、检索、分发、回收和销毁等。

宜保护所有的密钥免遭修改、丢失和毁坏。另外，秘密和私有密钥需要防范非授权的泄露。用来生成、存储和归档密钥的设备宜进行物理保护。

密钥管理系统宜基于已商定的标准、规程和安全方法，以便：

a) 生成用于不同密码系统和不同应用的密钥；

b) 生成和获得公开密钥证书；

c) 分发密钥给预期用户，包括在收到密钥时要如何激活；

d) 存储密钥，包括已授权用户如何访问密钥；

e) 变更或更新密钥，包括要何时变更密钥和如何变更密钥的规则；

f) 处理已损害的密钥；

g) 撤销密钥，包括要如何撤消或解除激活的密钥，例如，当密钥已损害时或当用户离开组织时（在这种情况下，密钥也要归档）；

h) 恢复已丢失或损坏的密钥；

i) 备份或归档密钥；

j) 销毁密钥；

k) 记录和审核与密钥管理相关的活动。

为了减少不恰当使用的可能性，宜规定密钥的激活日期和解除激活日期，以使它们只能用于相关密钥管理策略定义的时间段。

除了安全地管理秘密和私有密钥外，还宜考虑公开密钥的真实性。这一鉴别过程可以由证书认证机构正式颁发的公钥证书来完成，该认证机构宜是一个具有合适的控制措施和规程以提供所需的信任度的公认组织。

与外部密码服务提供者（例如与认证机构）签订的服务级别协议或合同的内容，宜涵盖服务责任、服务可靠性和提供服务的响应次数等若干问题（见 15.2）。

其他信息

密钥的管理对有效使用密码技术来说是必需的。GB/T 17901 提供了更多密钥管理的信息。

密码技术还可以用来保护密钥。可能需要考虑处理访问密钥的法律请求的规程，例如，加密的信息可能要求以未加密的形式提供，以作为法庭案例的证据。

## 11 物理和环境安全

### 11.1 安全区域

| |
|---|
| 目标：防止对组织场所和信息的未授权物理访问、损坏和干扰。 |

### 11.1.1 Physical security perimeter

Control

Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

Implementation guidance

The following guidelines should be considered and implemented where appropriate for physical security perimeters:

a) security perimeters should be defined, and the siting and strength of each of the perimeters should depend on the security requirements of the assets within the perimeter and the results of a risk assessment;

b) perimeters of a building or site containing information processing facilities should be physically sound (i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur); the exterior roof, walls and flooring of the site should be of solid construction and all external doors should be suitably protected against unauthorized access with control mechanisms, (e.g. bars, alarms, locks); doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level;

c) a manned reception area or other means to control physical access to the site or building should be in place; access to sites and buildings should be restricted to authorized personnel only;

d) physical barriers should, where applicable, be built to prevent unauthorized physical access and environmental contamination;

e) all fire doors on a security perimeter should be alarmed, monitored and tested in conjunction with the walls to establish the required level of resistance in accordance with suitable regional, national and international standards; they should operate in accordance with the local fire code in a failsafe manner;

f) suitable intruder detection systems should be installed to national, regional or international standards and regularly tested to cover all external doors and accessible windows; unoccupied areas should be alarmed at all times; cover should also be provided for other areas, e.g. computer room or communications rooms;

g) information processing facilities managed by the organization should be physically separated from those managed by external parties.

Other information

Physical protection can be achieved by creating one or more physical barriers around the organization's premises and information processing facilities. The use of multiple barriers gives additional protection, where the failure of a single barrier does not mean that security is immediately compromised.

A secure area may be a lockable office or several rooms surrounded by a continuous internal physical security barrier. Additional barriers and perimeters to control physical access may be needed between areas with different security requirements inside the security perimeter. Special attention to physical access security should be given in the case of buildings holding assets for multiple organizations.

The application of physical controls, especially for the secure areas, should be adapted to the technical and economic circumstances of the organization, as set forth in the risk assessment.

### 11.1.2 Physical entry controls

Control

Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

### 11.1.1 物理安全周边

控制措施

宜定义安全周边和所保护的区域，包括敏感或关键的信息和信息处理设施的区域。

实施指南

对于物理安全周边，若合适，下列指南宜予以考虑和实施：

a) 安全周边宜予以定义，各个周边的设置地点和强度取决于周边内资产的安全要求和风险评估的结果；

b) 包含信息处理设施的建筑物或场地的周边要在物理上是安全的（即，在周边或区域内不要存在可能易于闯入的任何缺口）；场所外部屋顶、墙和地板均是坚固结构，所有外部的门要使用控制机制来适当保护，以防止未授权进入，例如，门闩、报警器、锁等；无人看管的门和窗户要上锁，还要考虑窗户的外部保护，尤其是地面一层的窗户；

c) 对场所或建筑物的物理访问手段要到位（如有人管理的接待区域或其他控制）；进入场所或建筑物要仅限于已授权人员；

d) 如果可行，要建立物理屏障以防止未授权进入和环境污染；

e) 安全周边的所有防火门要可发出报警信号、被监视并经过测试，与墙一起按照合适的我国标准建立所需的防卫级别；它们要使用故障保护方式按照当地防火规则来运行。

f) 要按照我国标准安装适当的安防监测系统，并定期测试以覆盖所有的外部门窗；要一直警惕空闲区域；其他区域要提供掩护方法，例如计算机室或通信室；

g) 组织管理的信息处理设施要在物理上与第三方管理的设施分开。

其他信息

物理保护可以通过在组织边界和信息处理设施周围设置一个或多个物理屏障来实现。多重屏障的使用将提供附加保护，一个屏障的失效不意味着立即危及到安全。

一个安全区域可以是一个可上锁的办公室，或是被连续的内部物理安全屏障包围的几个房间。在安全边界内具有不同安全要求的区域之间需要控制物理访问的附加屏障和周边。

具有多个组织资产的建筑物宜考虑专门的物理访问安全。

特别是对于安全区域而言，宜在适合组织技术和经济条件下，按照风险评估应用物理控制措施。

### 11.1.2 物理入口控制

控制措施

安全区域宜由适合的入口控制所保护，以确保只有授权的人员才允许访问。

Implementation guidance

The following guidelines should be considered:

a) the date and time of entry and departure of visitors should be recorded, and all visitors should be supervised unless their access has been previously approved; they should only be granted access for specific, authorized purposes and should be issued with instructions on the security requirements of the area and on emergency procedures. The identity of visitors should be authenticated by an appropriate means;

b) access to areas where confidential information is processed or stored should be restricted to authorized individuals only by implementing appropriate access controls, e.g. by implementing a two-factor authentication mechanism such as an access card and secret PIN;

c) a physical log book or electronic audit trail of all access should be securely maintained and monitored;

d) all employees, contractors and external parties should be required to wear some form of visible identification and should immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification;

e) external party support service personnel should be granted restricted access to secure areas or confidential information processing facilities only when required; this access should be authorized and monitored;

f) access rights to secure areas should be regularly reviewed and updated, and revoked when necessary (see 9.2.5 and 9.2.6).

### 11.1.3 Securing offices, rooms and facilities

Control

Physical security for offices, rooms and facilities should be designed and applied.

Implementation guidance

The following guidelines should be considered to secure offices, rooms and facilities:

a) key facilities should be sited to avoid access by the public;

b) where applicable, buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building, identifying the presence of information processing activities;

c) facilities should be configured to prevent confidential information or activities from being visible and audible from the outside. Electromagnetic shielding should also be considered as appropriate;

d) directories and internal telephone books identifying locations of confidential information processing facilities should not be readily accessible to anyone unauthorized.

### 11.1.4 Protecting against external and environmental threats

Control

Physical protection against natural disasters, malicious attack or accidents should be designed and applied.

Implementation guidance

Specialist advice should be obtained on how to avoid damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster.

实施指南

宜考虑下列指南：

a) 记录访问者进入和离开的日期和时间，所有的访问者要予以监督，除非他们的访问事前已经经过批准；只允许他们访问特定的、已授权的目标，并要向他们宣布关于该区域的安全要求和应急规程的说明。访问者的身份宜通过恰当的方式认证。

b) 访问处理保密信息或储存保密信息的区域宜限于已授权的人员，并且采取的恰当访问控制措施；例如采取访问卡及加密的个人识别码构成的双因素认证机制。

c) 所有访问的物理登记薄或者电子审计单宜被安全的保留并监视；

d) 所有雇员和承包方人员以及外部各方要佩带某种形式的可视标识，如果遇到无人护送的访问者和未佩带可视标识的任何人要立即通知保安人员。

e) 外部方支持服务人员只有在需要时才能有限制的访问安全区域或敏感信息处理设施；这种访问要被授权并受监视；

f) 对安全区域的访问权限要定期地予以评审和更新，并在必要时废除（见 9.2.4 和 9.2.5）。

### 11.1.3 办公室、房间和设施的安全保护

控制措施

宜为办公室、房间和设施设计并采取物理安全措施。

实施指南

为保护办公室、房间和设施，宜考虑下列指南：

a) 关键设施要坐落在可避免公众进行访问的场地；

b) 如果可行，建筑物要不引人注目，并且在建筑物内侧或外侧用不明显的标记给出其用途的最少指示，以标识信息处理活动的存在；

c) 避免保密信息或活动对外部可视或可见，处理设施宜被包围，适当的采取电磁屏蔽措施；

d) 标识敏感信息处理设施位置的目录和内部电话簿不要轻易被公众得到。

### 11.1.4 外部和环境威胁的安全防护

控制措施

为防止自然灾难、恶意攻击或事件，宜设计和采取物理保护措施。

实施指南

宜获取如何避免火灾、洪水、地震、爆炸、社会动荡和其他形式的自然或人为灾难引起破坏的专家建议。

### 11.1.5 Working in secure areas

Control

Procedures for working in secure areas should be designed and applied.

Implementation guidance

The following guidelines should be considered:

a) personnel should only be aware of the existence of, or activities within, a secure area on a need-to-know basis;

b) unsupervised working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities;

c) vacant secure areas should be physically locked and periodically reviewed;

d) photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed, unless authorized.

The arrangements for working in secure areas include controls for the employees and external party users working in the secure area and they cover all activities taking place in the secure area.

### 11.1.6 Delivery and loading areas

Control

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

Implementation guidance

The following guidelines should be considered:

a) access to a delivery and loading area from outside of the building should be restricted to identified and authorized personnel;

b) the delivery and loading area should be designed so that supplies can be loaded and unloaded without delivery personnel gaining access to other parts of the building;

c) the external doors of a delivery and loading area should be secured when the internal doors are opened;

d) incoming material should be inspected and examined for explosives, chemicals or other hazardous materials, before it is moved from a delivery and loading area;

e) incoming material should be registered in accordance with asset management procedures (see Clause 8) on entry to the site;

f) incoming and outgoing shipments should be physically segregated, where possible;

g) incoming material should be inspected for evidence of tampering en route. If such tampering is discovered it should be immediately reported to security personnel.

## 11.2 Equipment

| Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations. |
|---|

### 11.1.5 在安全区域工作

控制措施

宜设计和应用工作在安全区域的规程。

实施指南

宜考虑下列指南：

a） 只在有必要知道的基础上，员工才应知道安全区域的存在或其中的活动；

b） 为了安全原因和减少恶意活动的机会，均要避免在安全区域内进行不受监督的工作；

c） 未使用的安全区域在物理上要上锁并周期地予以核查；

d） 除非授权，不要允许携带摄影、视频、声频或其他记录设备，例如移动设备中的照相机。

在安全区域工作的安排包括对工作在安全区域内的雇员和外部方人员的控制，以及对其他发生在安全区域的所有活动的控制。

### 11.1.6 交接区安全

控制措施

访问点（例如交接区）和未授权人员可进入办公场所的其他点宜加以控制，如果可能，宜与信息处理设施隔离，以避免未授权访问。

实施指南

宜考虑下列指南：

a） 由建筑物外进入交接区的访问要局限于已标识的和已授权的人员；

b） 交接区要设计成在无需交货人员获得对本建筑物其他部分的访问权限的情况下就能装载或卸下物资；

c） 当内部的门打开时，交接区的外部门要得到安全保护；

d） 在进来的物资从交接区运到使用地点之前，要检查是否存在易爆、化学和易燃物资；

e） 进来的物资要按照资产管理规程（见 8）在场所的入口处进行登记；

f） 如果可能，进入和外出的货物要在物理上予以隔离；

g） 进来的物资宜检查途中损坏的证据，如果发现损坏宜立即向安全人员报告。

## 11.2 设备

| |
|---|
| 目标：防止资产的丢失、损坏、失窃或危及资产安全以及组织活动的中断。 |

### 11.2.1 Equipment siting and protection

Control

Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

Implementation guidance

The following guidelines should be considered to protect equipment:

a) equipment should be sited to minimize unnecessary access into work areas;

b) information processing facilities handling sensitive data should be positioned carefully to reduce the risk of information being viewed by unauthorized persons during their use;

c) storage facilities should be secured to avoid unauthorized access;

d) items requiring special protection should be safeguarded to reduce the general level of protection required;

e) controls should be adopted to minimize the risk of potential physical and environmental threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation and vandalism;

f) guidelines for eating, drinking and smoking in proximity to information processing facilities should be established;

g) environmental conditions, such as temperature and humidity, should be monitored for conditions which could adversely affect the operation of information processing facilities;

h) lightning protection should be applied to all buildings and lightning protection filters should be fitted to all incoming power and communications lines;

i) the use of special protection methods, such as keyboard membranes, should be considered for equipment in industrial environments;

j) equipment processing confidential information should be protected to minimize the risk of information leakage due to electromagnetic emanation.

### 11.2.2 Supporting utilities

Control

Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.

Implementation guidance

Supporting utilities (e.g. electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning) should:

a) conform to equipment manufacturer's specifications and local legal requirements;

b) be appraised regularly for their capacity to meet business growth and interactions with other supporting utilities;

c) be inspected and tested regularly to ensure their proper functioning;

d) if necessary, be alarmed to detect malfunctions;

e) if necessary, have multiple feeds with diverse physical routing.

### 11.2.1 设备安置和保护

控制措施

宜安置或保护设备，以减少由环境威胁和危险所造成的各种风险以及未授权访问的机会。

实施指南

为保护设备，宜考虑下列指南：

a) 设备要进行适当安置，以尽量减少不必要的对工作区域的访问；

b) 要把处理敏感数据的信息处理设施放在适当的限制观测的位置，以减少在其使用期间信息被非授权人员窥视的风险；

c) 还要保护储存设施以防止未授权访问；

d) 要求特殊保护的部件要予以防护，以降低所要求的总体保护等级；

e) 要采取控制措施以最小化潜在的物理和环境威胁的风险，例如偷窃、火灾、爆炸、烟雾、水（或供水故障）、尘埃、振动、化学影响、电源干扰、通信干扰、电磁辐射和故意破坏；

f) 要建立在信息处理设施附近进食、喝饮料和抽烟的指南；

g) 对于可能对信息处理设施运行状态产生负面影响的环境条件（例如温度和湿度）要予以监视；

h) 所有建筑物都要采用避雷保护，所有进入的电源和通信线路都要装配雷电保护过滤器；

i) 对于工业环境中的设备，要考虑使用专门的保护方法，例如键盘保护膜；

j) 要保护处理敏感信息的设备，以最小化因辐射而导致信息泄露的风险；

### 11.2.2 支持性设施

控制措施

宜保护设备使其免于由支持性设施的失效而引起的电源故障和其他中断。

实施指南

支持性设施（例如电、通信、供水、供气、排污、通风和空调）宜：

a) 宜遵从设备制造商的说明书和本地法规要求；

b) 定期扩容满足业务增长和其他支持性设施的交互；

c) 定期检查和测试确保支持性设施功能正常；

d) 如果必要，检测到故障发出报警；

e) 如果必要，采取不同物理线路的多路供电 g。

Emergency lighting and communications should be provided. Emergency switches and valves to cut off power, water, gas or other utilities should be located near emergency exits or equipment rooms.

Other information

Additional redundancy for network connectivity can be obtained by means of multiple routes from more than one utility provider.

### 11.2.3 Cabling security

Control

Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage.

Implementation guidance

The following guidelines for cabling security should be considered:

a) power and telecommunications lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection;

b) power cables should be segregated from communications cables to prevent interference;

c) for sensitive or critical systems further controls to consider include:

   1) installation of armoured conduit and locked rooms or boxes at inspection and termination points;

   2) use of electromagnetic shielding to protect the cables;

   3) initiation of technical sweeps and physical inspections for unauthorized devices being attached to the cables;

   4) controlled access to patch panels and cable rooms.

### 11.2.4 Equipment maintenance

Control

Equipment should be correctly maintained to ensure its continued availability and integrity.

Implementation guidance

The following guidelines for equipment maintenance should be considered:

a) equipment should be maintained in accordance with the supplier's recommended service intervals and specifications;

b) only authorized maintenance personnel should carry out repairs and service equipment;

c) records should be kept of all suspected or actual faults, and of all preventive and corrective maintenance;

d) appropriate controls should be implemented when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the organization; where necessary, confidential information should be cleared from the equipment or the maintenance personnel should be sufficiently cleared;

e) all maintenance requirements imposed by insurance policies should be complied with;

f) before putting equipment back into operation after its maintenance, it should be inspected to ensure that the equipment has not been tampered with and does not malfunction.

宜提供应急照明和应急通信，切断电源、水、气及其他设施的电源开关或阀门宜安置在应急出口或设备间附件。

其他信息

网络连接冗余可以通过不同设施供应商的方式实现。

### 11.2.3 布缆安全

控制措施

宜保证传输数据或支持信息服务的电源布缆和通信布缆免受窃听或损坏。

实施指南

对于布缆安全，宜考虑下列指南：

a) 进入信息处理设施的电源和通信线路宜在地下，若可能，或提供足够的可替换的保护；

b) 为了防止干扰，电源电缆要与通信电缆分开；

c) 对于敏感的或关键的系统，更进一步的控制措施考虑要包括：

1） 在检查点和终接点处安装铠装电缆管道和上锁的房间或盒子；

2） 使用电磁防辐射装置保护电缆；

3） 对于电缆连接的未授权装置要主动实施技术清除和物理检查；

4） 控制对配线盘和电缆室的访问。

### 11.2.4 设备维护

控制措施

设备宜予以正确地维护，以确保其持续的可用性和完整性。

实施指南

对于设备维护，宜考虑下列指南：

a) 要按照供应商推荐的服务时间间隔和规范对设备进行维护；

b) 只有已授权的维护人员才可对设备进行修理和服务；

c) 要保存所有可疑的或实际的故障以及所有预防和纠正维护的记录；

d) 当对设备安排维护时，要实施适当的控制，并考虑到维护是由场所内部人员执行还是由组织外部人员执行；当必要时，敏感信息要从设备中删除或者维护人员要是足够可靠的；

e) 要遵守由保险策略所施加的所有要求；

f) 在设备维护之后返回运行之前，宜检查设备确保设备没有损坏和失效。

### 11.2.5 Removal of assets

Control

Equipment, information or software should not be taken off-site without prior authorization.

Implementation guidance

The following guidelines should be considered:

a) employees and external party users who have authority to permit off-site removal of assets should be identified;

b) time limits for asset removal should be set and returns verified for compliance;

c) where necessary and appropriate, assets should be recorded as being removed off-site and recorded when returned;

d) the identity, role and affiliation of anyone who handles or uses assets should be documented and this documentation returned with the equipment, information or software.

Other information

Spot checks, undertaken to detect unauthorized removal of assets, can also be performed to detect unauthorized recording devices, weapons, etc., and to prevent their entry into and exit from, the site. Such spot checks should be carried out in accordance with relevant legislation and regulations. Individuals should be made aware that spot checks are carried out, and the verifications should only be performed with authorization appropriate for the legal and regulatory requirements.

### 11.2.6 Security of equipment and assets off-premises

Control

Security should be applied to off-site assets taking into account the different risks of working outside the organization's premises.

Implementation guidance

The use of any information storing and processing equipment outside the organization's premises should be authorized by management. This applies to equipment owned by the organization and that equipment owned privately and used on behalf of the organization.

The following guidelines should be considered for the protection of off-site equipment:

a) equipment and media taken off premises should not be left unattended in public places;

b) manufacturers' instructions for protecting equipment should be observed at all times, e.g. protection against exposure to strong electromagnetic fields;

c) controls for off-premises locations, such as home-working, teleworking and temporary sites should be determined by a risk assessment and suitable controls applied as appropriate, e.g. lockable filing cabinets, clear desk policy, access controls for computers and secure communication with the office (see also ISO/IEC 27033[15][16][17][18][19]);

d) when off-premises equipment is transferred among different individuals or external parties, a log should be maintained that defines the chain of custody for the equipment including at least names and organizations of those who are responsible for the equipment.

Risks, e.g. of damage, theft or eavesdropping, may vary considerably between locations and should be taken into account in determining the most appropriate controls.

Other information

### 11.2.5 资产的移动

控制措施

设备、信息或软件在授权之前不宜带出组织场所。

实施指南

宜考虑下列指南：

a) 要明确识别有权允许资产移动，离开办公场所的雇员和外部方用户；

b) 要设置设备移动的时间限制，并在返还时执行符合性验证；

c) 若必要并合适，要对资产作出移出记录，当返回时，要作出送回记录；

d) 处理和使用资产的人员身份、角色和归属宜被记录，记录文档宜与设备、信息或软件一起归还。

其他信息

宜执行检测未授权资产移动的抽查，以检测未授权的记录装置、武器等等，防止他们进入和带出办公场所。这样的抽查宜按照相关法律和规章执行。宜让每个人都知道将进行抽查，并且只能在法律法规要求的适当授权下执行验证。

### 11.2.6 组织场外设备和资产的安全

控制措施

宜对组织场所外的设备采取安全措施，要考虑工作在组织场所以外的不同风险。

实施指南

在组织场所外使用任何信息存储和处理设备都宜通过管理者授权。这适用于组织拥有的设备、私有设备和代表组织的设备。

对于离开场所的设备的保护，宜考虑下列指南：

a） 离开建筑物的设备和介质在公共场所不应无人看管；

b） 制造商的设备保护说明要始终加以遵守，例如，防止暴露于强电磁场内；

c） 家庭工作、远程办公和临时场所办公的场外控制措施要根据风险评估确定，当适合时，要施加合适的控制措施，例如，可上锁的存档柜、清理桌面策略、对计算机的访问控制以及与办公室的安全通信（参见 ISO/IEC 18028 网络安全）；

d） 当场外设备在不同的人或外部方之间传递时，宜维护对设备一系列监督的记录，包括最终名称、设备的责任组织。

安全风险在不同场所可能有显著不同，例如，损坏、盗窃和截取，要考虑确定最合适的控制措施。

其他信息

Information storing and processing equipment includes all forms of personal computers, organizers, mobile phones, smart cards, paper or other form, which is held for home working or being transported away from the normal work location.

More information about other aspects of protecting mobile equipment can be found in 6.2.

It may be appropriate to avoid the risk by discouraging certain employees from working off-site or by restricting their use of portable IT equipment;

### 11.2.7 Secure disposal or re-use of equipment

Control

All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Implementation guidance

Equipment should be verified to ensure whether or not storage media is contained prior to disposal or re-use.

Storage media containing confidential or copyrighted information should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

Other information

Damaged equipment containing storage media may require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded. Information can be compromised through careless disposal or re-use of equipment.

In addition to secure disk erasure, whole-disk encryption reduces the risk of disclosure of confidential information when equipment is disposed of or redeployed, provided that:

a) the encryption process is sufficiently strong and covers the entire disk (including slack space, swap files, etc.);

b) the encryption keys are long enough to resist brute force attacks;

c) the encryption keys are themselves kept confidential (e.g. never stored on the same disk).

For further advice on encryption, see Clause 10.

Techniques for securely overwriting storage media differ according to the storage media technology. Overwriting tools should be reviewed to make sure that they are applicable to the technology of the storage media.

### 11.2.8 Unattended user equipment

Control

Users should ensure that unattended equipment has appropriate protection.

Implementation guidance

All users should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users should be advised to:

a) terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;

b) log-off from applications or network services when no longer needed;

用于家庭工作或从正常工作地点运走的信息存储和处理设备包括所有形式的个人计算机、管理设备、移动电话、智能卡、纸张或其他形式的设备。

关于保护移动设备的其他方面的更多信息在 6.2 中可以找到。

通过劝阻员工不要场外办公或者限制他们使用手提 IT 设备适当的避免风险。

### 11.2.7 设备的安全处置或再利用

控制措施

包含储存介质的设备的所有项目宜进行验证，以确保在处置之前，任何敏感信息和注册软件已被删除或安全地写覆盖。

实施指南

在设备处置和再利用之前宜验证是否保留存储介质。

包含保密或版权信息的存储介质在物理上宜予以摧毁，或者采用使原始信息不可获取的技术破坏、删除或写覆盖，而不能采用标准的删除或格式化功能。

其他信息

包含存储介质的已损坏的设备可能需要实施风险评估，以确定这些设备是否要进行销毁、而不是送去修理或丢弃。信息可能通过对设备的草率处置或重用而被泄漏。

当设备被处置或重用时，除了安全磁盘擦除，整个磁盘加密可降低保密信息泄露的风险，假如保证以下方面：

a) 加密过程足够强壮并且覆盖整个磁盘（包括剩余空间、交换文件等）；

b) 加密密钥的长度足够抵制暴力破解攻击；

c) 保证加密密钥的保密性（例如，不存储在同一磁盘）。

关于密码的进一步建议，见 10。

不同的存储介质技术，安全复写存储介质的技术方法则不同。为确保复写工具适用于存储介质技术，宜对其进行评审。

### 11.2.8 无人值守的用户设备

控制措施

用户宜确保无人值守的用户设备有适当的保护。

实施指南

所有用户宜了解保护无人值守的设备的安全要求和规程，以及他们对实现这种保护所负有的职责。建议用户宜：

a） 结束时终止活动的会话，除非采用一种合适的锁定机制保证其安全，例如，有口令保护的屏幕保护程序；

b） 当不再使用时，退出应用或网络服务；

c) secure computers or mobile devices from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use.

### 11.2.9 Clear desk and clear screen policy

Control

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.

Implementation guidance

The clear desk and clear screen policy should take into account the information classifications (see 8.2), legal and contractual requirements (see 18.1) and the corresponding risks and cultural aspects of the organization. The following guidelines should be considered:

a) sensitive or critical business information, e.g. on paper or on electronic storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated.

b) computers and terminals should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and should be protected by key locks, passwords or other controls when not in use;

c) unauthorised use of photocopiers and other reproduction technology (e.g. scanners, digital cameras) should be prevented;

d) media containing sensitive or classified information should be removed from printers immediately.

Other information

A clear desk/clear screen policy reduces the risks of unauthorized access, loss of and damage to information during and outside normal working hours. Safes or other forms of secure storage facilities might also protect information stored therein against disasters such as a fire, earthquake, flood or explosion.

Consider the use of printers with PIN code function, so the originators are the only ones who can get their print-outs and only when standing next to the printer.

# 12 Operations security

## 12.1 Operational procedures and responsibilities

| Objective: To ensure correct and secure operations of information processing facilities. |
|---|

### 12.1.1 Documented operating procedures

Control

Operating procedures should be documented and made available to all users who need them.

Implementation guidance

Documented procedures should be prepared for operational activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, backup, equipment maintenance, media handling, computer room and mail handling management and safety.

The operating procedures should specify the operational instructions, including:

a) the installation and configuration of systems;

c） 当不使用设备时，用带钥匙的锁或与之效果等同的控制措施来保护计算机或移动设备免遭未授权使用，例如，口令访问。

#### 11.2.9 清空桌面和屏幕策略

控制措施

宜采取清空桌面上文件、可移动存储介质的策略和清空信息处理设施屏幕的策略。

实施指南

清空桌面和清空屏幕策略宜考虑信息分类（见 8.2）、法律和合同要求（见 18.1）、相 应的风险和组织的文化方面。宜考虑下列指南：

a） 当不用时，特别是当离开办公室时，要将敏感或关键业务信息，例如在纸质或电子存储介质中的，锁起来（理想情况下，在保险柜或保险箱或者其他形式的安全设备中）；

b） 当无人值守时，计算机和终端要注销，或使用由口令、令牌或类似的用户鉴别机制控制的屏幕和键盘锁定机制进行保护；当不使用时，要使用带钥匙的锁、口令或其他控制措施进行保护；

c） 要防止复印机或其他复制技术（例如扫描仪、数字照相机）的未授权使用；

d） 包含敏感或涉密信息的煤质要立即从打印机中清除。

其他信息

清空桌面/清空屏幕策略降低了正常工作时间之中和之外对信息的未授权访问、丢失、破坏的风险。保险箱或其他形式的安全存储设施也可保护存储于其中的信息免受灾难（例如火灾、地震、洪水或爆炸）的影响。

要考虑使用带有个人识别码功能的打印机，使得原始操作人员是能获得打印输出的唯一人员，和站在打印机边的唯一人员。

## 12 操作安全

### 12.1 操作规程和职责

| |
|---|
| 目标：确保正确、安全的操作信息处理设施。。 |

#### 12.1.1 文件化的操作规程

控制措施

操作规程宜形成文件并对所有需要的用户可用。

实施指南

与信息处理和通信设施相关的操作活动宜具备形成文件的规程，例如计算机启动和关机规程、备份、设备维护、介质处理、计算机机房、邮件处置管理和安全等。

操作规程宜说明操作指导，其内容包括：

a）系统安装和配置；

b) processing and handling of information both automated and manual;

c) backup (see 12.3);

d) scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;

e) instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities (see 9.4.4);

f) support and escalation contacts including external support contacts in the event of unexpected operational or technical difficulties;

g) special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output from failed jobs (see 8.3 and 11.2.7);

h) system restart and recovery procedures for use in the event of system failure;

i) the management of audit-trail and system log information (see 12.4);

j) monitoring procedures.

Operating procedures and the documented procedures for system activities should be treated as formal documents and changes authorized by management. Where technically feasible, information systems should be managed consistently, using the same procedures, tools and utilities.

### 12.1.2 Change management

Control

Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled.

Implementation guidance

In particular, the following items should be considered:

a) identification and recording of significant changes;

b) planning and testing of changes;

c) assessment of the potential impacts, including information security impacts, of such changes;

d) formal approval procedure for proposed changes;

e) verification that information security requirements have been met;

f) communication of change details to all relevant persons;

g) fall-back procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events;

h) provision of an emergency change process to enable quick and controlled implementation of changes needed to resolve an incident (see 16.1).

Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes. When changes are made, an audit log containing all relevant information should be retained.

Other information

b）信息自动或手动处理和处置；

c）备份（见 12.3）；

d）时间安排要求，包括与其他系统的相互关系、最早工作开始时间和最后工作完成期限；

e）对在工作执行期间可能出现的处理差错或其他异常情况的指导，包括对使用系统实用工具的限制（见 9.4.4）；

f）支持性和上报联络，包括出现不期望操作或技术困难时的外部支持性联络；

g）特定输出及介质处理的指导，例如使用特殊信纸或管理保密输出，包括任务失败时输出的安全处置规程（见 8.3 和 11.2.7）；

h）供系统失效时使用的系统重启和恢复规程；

i）审核踪迹和系统日志信息的管理（见 12.4）；

j）监视规程（见 12.4）。

宜将操作规程和系统活动的文件化规程看作正式的文件，其变更由管理者授权。技术上可行时，信息系统宜使用相同的规程、工具和实用程序进行一致的管理。

### 12.1.2 变更管理

控制措施

若组织、业务过程、信息处理设施和系统等的变更影响了组织信息安全，则宜加以控制。

实施指南

运行系统和应用软件宜有严格的变更管理控制。

特别是，宜考虑下列条款：

a）重大变更的标识和记录；

b）变更的策划和测试；

c）对这种变更的潜在影响的评估，包括信息安全影响；

d）对建议变更的正式批准规程；

e）验证得到满足的信息安全要求；

f）向所有有关人员传达变更细节；

g）基本维持运行的规程，包括从不成功变更和未预料事态中退出和恢复的规程与职责；

h）规定紧急变更过程，使之能够在快速和受控状态下实施所需变更来处理事件。

正式的管理者职责和规程宜到位，以确保所有变更有令人满意的控制。当发生变更时，包含所有相关信息的审核日志宜予以保留。

其他信息

Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Changes to the operational environment, especially when transferring a system from development to operational stage, can impact on the reliability of applications (see 14.2.2).

### 12.1.3 Capacity management

Control

The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

Implementation guidance

Capacity requirements should be identified, taking into account the business criticality of the concerned system. System tuning and monitoring should be applied to ensure and, where necessary, improve the availability and efficiency of systems. Detective controls should be put in place to indicate problems in due time. Projections of future capacity requirements should take account of new business and system requirements and current and projected trends in the organization's information processing capabilities.

Particular attention needs to be paid to any resources with long procurement lead times or high costs; therefore managers should monitor the utilization of key system resources. They should identify trends in usage, particularly in relation to business applications or information systems management tools.

Managers should use this information to identify and avoid potential bottlenecks and dependence on key personnel that might present a threat to system security or services, and plan appropriate action.

Providing sufficient capacity can be achieved by increasing capacity or by reducing demand. Examples of managing capacity demand include:

a) deletion of obsolete data (disk space);

b) decommissioning of applications, systems, databases or environments;

c) optimising batch processes and schedules;

d) optimising application logic or database queries;

e) denying or restricting bandwidth for resource-hungry services if these are not business critical (e.g. video streaming).

A documented capacity management plan should be considered for mission critical systems.

Other information

This control also addresses the capacity of the human resources, as well as offices and facilities.

### 12.1.4 Separation of development, testing and operational environments

Control

Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.

Implementation guidance

The level of separation between operational, testing, and development environments that is necessary to prevent operational problems should be identified and implemented.

The following items should be considered:

a) rules for the transfer of software from development to operational status should be defined and documented;

对信息处理设施和系统的变更缺乏控制是系统故障或安全失效的常见原因。对运行环境的变更，特别是当系统从开发阶段向运行阶段转移时，可能影响应用的可靠性。（见 14.2.2）。

### 12.1.3 容量管理

控制措施

资源的使用宜加以监视、调整，并作出对于未来容量要求的预测，以确保拥有所需的系统性能。

实施指南

宜根据所关注系统的业务关键性识别容量要求。宜使用系统调整和监视以确保和改进（必要时）系统的可用性和效率。宜有检测控制措施以及时地指出问题。未来容量要求的推测宜考虑新业务、系统要求以及组织信息处理能力的当前和预计的趋势。

需要特别关注与长订货交货周期或高成本相关的所有资源；因此管理人员宜监视关键系统资源的利用。他们宜识别出使用的趋势，特别是与业务应用或管理信息系统工具相关的使用。

管理人员宜使用该信息来识别和避免可能威胁到系统安全或服务的潜在的瓶颈及对关键员工的依赖，并策划适当的措施。

提供充足的容量可以通过增加容量或降低需求来实现，管理容量需求的例子包括：

a) 删除过时数据（磁盘空间）；

b) 停止使用应用、系统、数据库或环境；

c) 优化应用逻辑或数据库查询；

d) 如果是非关键业务（例如影音串流），则拒绝或限制其资源服务带宽的使用。

对于关键任务系统，宜考虑文件化的容量管理方案。

其他信息

这一控制措施也涉及人力资源、办公室以及设施的容量。

### 12.1.4 开发、测试和运行环境分离

控制措施

开发、测试和运行环境宜分离，以减少未授权访问或运行环境变更的风险。

实施指南

为防止运行问题，宜识别运行、测试和开发环境之间的分离级别，并实施适当的控制措施。

宜考虑下列条款：

a) 要规定从开发状态到运行状态的软件传递规则并形成文件；

b) development and operational software should run on different systems or computer processors and in different domains or directories;

c) changes to operational systems and applications should be tested in a testing or staging environment prior to being applied to operational systems;

d) other than in exceptional circumstances, testing should not be done on operational systems;

e) compilers, editors and other development tools or system utilities should not be accessible from operational systems when not required;

f) users should use different user profiles for operational and testing systems, and menus should display appropriate identification messages to reduce the risk of error;

g) sensitive data should not be copied into the testing system environment unless equivalent controls are provided for the testing system (see 14.3).

Other information

Development and testing activities can cause serious problems, e.g. unwanted modification of files or system environment or system failure. There is a need to maintain a known and stable environment in which to perform meaningful testing and to prevent inappropriate developer access to the operational environment.

Where development and testing personnel have access to the operational system and its information, they may be able to introduce unauthorized and untested code or alter operational data. On some systems this capability could be misused to commit fraud or introduce untested or malicious code, which can cause serious operational problems.

Development and testing personnel also pose a threat to the confidentiality of operational information. Development and testing activities may cause unintended changes to software or information if they share the same computing environment. Separating development, testing and operational environments is therefore desirable to reduce the risk of accidental change or unauthorized access to operational software and business data (see 14.3 for the protection of test data).

## 12.2 Protection from malware

Objective: To ensure that information and information processing facilities are protected against malware.

### 12.2.1 Controls against malware

Control

Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.

Implementation guidance

Protection against malware should be based on malware detection and repair software, information security awareness and appropriate system access and change management controls. The following guidance should be considered:

a) establishing a formal policy prohibiting the use of unauthorized software (see 12.6.2 and 14.2.);

b) implementing controls that prevent or detect the use of unauthorized software (e.g. application whitelisting);

c) implementing controls that prevent or detect the use of known or suspected malicious websites (e.g. blacklisting);

b) 开发和运行软件要在不同的系统或计算机处理器上以及在不同的域或目录内运行；

c) 若运行系统和应用发生变更宜进行测试，并且在测试或过渡环境中测试优于在运行环境中测试；

d) 除非特殊情况下，不宜针对运行系统进行测试。

e) 用户要在运行和测试系统中使用不同的用户轮廓，菜单要显示合适的标识消息以减少出错的风险；

f) 除非针对测试系统提供了相关的控制措施，否则敏感数据不要拷贝到测试系统环境中（见 14.3）。

其他信息

开发和测试活动可能引起严重的问题，例如，文件或系统环境的不期望修改或者系统故障。在这种情况下，有必要保持一种已知的和稳定的环境，在此环境中可执行有意义的测试并防止不适当的开发者访问。

若开发和测试人员访问运行系统及其信息，那么他们可能会引入未授权和未测试的代码或改变运行数据。在某些系统中，这种能力可能被误用于实施欺诈，或引入未测试的、恶意的代码，从而导致严重的运行问题。

开发者和测试者还造成对运行信息保密性的威胁。如果开发和测试活动共享同一计算环境，那么可能引起非故意的软件和信息的变更。因此，为了减少意外变更或未授权访问运行软件和业务数据的风险，分离开发、测试和运行环境是有必要的（见 14.3 的测试数据保护）。

## 12.2 恶意软件防护

| |
|---|
| 目标：确保对信息和信息处理设施进行恶意软件防护。 |

### 12.2.1 控制恶意软件

控制措施

宜实施恶意软件的检测、预防和恢复的控制措施，以及适当的提高用户安全意识。

实施指南

防范恶意软件宜基于恶意代码检测、修复软件、安全意识、适当的系统访问和变更管理控制措施。宜考虑下列指南：

a） 建立禁止使用未授权软件的正式策略（见 14.2）；

b） 实施防止或检测使用非授权软件的控制措施（例如，应用程序白名单）；

c） 实施防止或检测已知的及可疑的恶意网站的使用（例如，黑名单）；

d) establishing a formal policy to protect against risks associated with obtaining files and software either from or via external networks or on any other medium, indicating what protective measures should be taken;

e) reducing vulnerabilities that could be exploited by malware, e.g. through technical vulnerability management (see 12.6);

f) conducting regular reviews of the software and data content of systems supporting critical business processes; the presence of any unapproved files or unauthorized amendments should be formally investigated;

g) installation and regular update of malware detection and repair software to scan computers and media as a precautionary control, or on a routine basis; the scan carried out should include:

   1) scan any files received over networks or via any form of storage medium, for malware before use;

   2) scan electronic mail attachments and downloads for malware before use; this scan should be carried out at different places, e.g. at electronic mail servers, desk top computers and when entering the network of the organization;

   3) scan web pages for malware;

h) defining procedures and responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks;

i) preparing appropriate business continuity plans for recovering from malware attacks, including all necessary data and software backup and recovery arrangements (see 12.3);

j) implementing procedures to regularly collect information, such as subscribing to mailing lists or verifying websites giving information about new malware;

k) implementing procedures to verify information relating to malware, and ensure that warning bulletins are accurate and informative; managers should ensure that qualified sources, e.g. reputable journals, reliable Internet sites or suppliers producing software protecting against malware, are used to differentiate between hoaxes and real malware; all users should be made aware of the problem of hoaxes and what to do on receipt of them;

l) isolating environments where catastrophic impacts may result.

Other information

The use of two or more software products protecting against malware across the information processing environment from different vendors and technology can improve the effectiveness of malware protection.

Care should be taken to protect against the introduction of malware during maintenance and emergency procedures, which may bypass normal malware protection controls.

Under certain conditions, malware protection might cause disturbance within operations.

Use of malware detection and repair software alone as a malware control is not usually adequate and commonly needs to be accompanied by operating procedures that prevent introduction of malware.

## 12.3 Backup

| Objective: To protect against loss of data. |
|---|

### 12.3.1 Information backup

Control

d） 建立防范风险的正式策略，该风险与来自或经由外部网络或在其他介质上获得的文件和软件相关，此策略指示要采取什么保护措施；

e） 降低可能被恶意软件利用的技术脆弱性，例如通过技术脆弱性管理（见 12.6）；

f） 对支持关键业务过程的系统中的软件和数据内容进行定期评审。要正式调查存在的任何未批准的文件或未授权的修正；

g） 安装和定期更新恶意软件检测和修复软件来扫描计算机和介质，以作为预防控制或作为例行程序的基础；执行的扫描要包括：

1） 从网络上或通过任何形式存储介质接收的文件在使用之前，宜进行恶意软件扫描；

2） 电子邮件附件和下载内容在使用之前，宜进行恶意软件扫描；该扫描要在不同位置进行，例如，在电子邮件服务器、台式计算机或进入组织的网络时；

3） 对 Web 页面进行恶意软件扫描；

h） 定义关于系统恶意软件防护、它们使用的培训、恶意软件攻击报告和从中恢复的管理规程和职责；

i） 制定适当的从恶意软件攻击中恢复的业务连续性计划，包括所有必要的数据和软件的备份以及恢复安排（见 12.3）；

j） 实施规程定期收集信息，例如订阅邮件列表和/或核查提供新恶意软件的 web 站点；

k） 实施检验与恶意软件相关信息的规程，并确保报警公告是准确情报；管理人员宜确保使用合格的来源（例如，声誉好的期刊、可靠的 Internet 网站或防范恶意软件的供应商），以区分虚假的和实际的恶意软件；要让所有用户了解欺骗问题，以及在收到它们时要做什么；

l） 隔离可能导致灾难性影响的环境。

其他信息

在信息处理环境中使用来自不同供应商的防范恶意软件的两个或多个软件产品，能改进恶意软件防护的有效性。

宜注意防止在实施维护和紧急规程期间引入恶意软件，因为它们可能旁路正常的恶意软件防护的控制措施。

在某种情况下，恶意软件防护可能会对运行造成干扰。

单独使用恶意软件检测或修复软件作为恶意软件控制措施是不充分的，通常需要配有防止恶意软件引入的操作规程。

## 12.3 备份

| |
|---|
| 目标：为了防止数据丢失。 |

### 12.3.1 信息备份

控制措施

Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.

Implementation guidance

A backup policy should be established to define the organization's requirements for backup of information, software and systems.

The backup policy should define the retention and protection requirements.

Adequate backup facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

When designing a backup plan, the following items should be taken into consideration:

a) accurate and complete records of the backup copies and documented restoration procedures should be produced;

b) the extent (e.g. full or differential backup) and frequency of backups should reflect the business requirements of the organization, the security requirements of the information involved and the criticality of the information to the continued operation of the organization;

c) the backups should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site;

d) backup information should be given an appropriate level of physical and environmental protection (see Clause 11) consistent with the standards applied at the main site;

e) backup media should be regularly tested to ensure that they can be relied upon for emergency use when necessary; this should be combined with a test of the restoration procedures and checked against the restoration time required. Testing the ability to restore backed-up data should be performed onto dedicated test media, not by overwriting the original media in case the backup or restoration process fails and causes irreparable data damage or loss;

f) in situations where confidentiality is of importance, backups should be protected by means of encryption.

Operational procedures should monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups according to the backup policy.

Backup arrangements for individual systems and services should be regularly tested to ensure that they meet the requirements of business continuity plans. In the case of critical systems and services, backup arrangements should cover all systems information, applications and data necessary to recover the complete system in the event of a disaster.

The retention period for essential business information should be determined, taking into account any requirement for archive copies to be permanently retained.

## 12.4 Logging and monitoring

| Objective: To record events and generate evidence. |
|---|

### 12.4.1 Event logging

Control

Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.

Implementation guidance

宜按照已设的备份策略，定期备份和测试信息、软件及系统镜像。

实施指南

宜建立备份策略，以定义组织信息、软件和系统备份的要求。

备份策略宜明确保留和保护要求。

宜提供足够的备份设施，以确保所有必要的信息和软件能在灾难或介质故障后进行恢复。

当设计备份方案时，宜考虑下列条款：

a） 要建立备份拷贝的准确完整的记录和文件化的恢复规程；

b） 备份的程度（例如全部备份或部分备份）和频率要反映组织的业务要求、涉及信息的安全要求和信息对组织持续运作的关键度；

c） 备份要存储在一个远程地点，有足够距离，以避免主办公场所灾难时受到损坏；

d） 要给予备份信息一个与主办公场所应用标准相一致的适当的物理和环境保护等级（见第 11 章 。

e） 宜定期测试备份介质，以确保当必要的应急使用时可以依靠这些备份介质；测试过程宜结合恢复测试规程执行并查验恢复所要求的时间。恢复备份数据能力的测试宜通过专用测试介质进行，不能靠复写原始介质进行，以防止恢复过程出现故障造成不可修复的损坏或数据丢失；

f） 在保密性十分重要的情况下，备份要通过加密方法进行保护。

操作规程宜监视备份的执行过程，并处理定期备份中的故障，以确保按照备份策略完成备份。

各个系统和服务的备份安排宜定期测试以确保它们满足业务连续性计划的要求。对于关键的系统和服务，备份安排宜包括在发生灾难时恢复整个系统所必要的所有系统信息、应用和数据。

宜确定最重要业务信息的保存周期以及对要永久保存的档案拷贝的任何要求。

## 12.4 日志和监视

| |
|---|
| 目标：记录事态和生成证据。 |

### 12.4.1 事态记录

控制措施

宜产生记录用户活动、异常情况、故障和信息安全事态的事态日志，并保持定期评审。

实施指南

Event logs should include, when relevant:

a) user IDs;

b) system activities;

c) dates, times and details of key events, e.g. log-on and log-off;

d) device identity or location if possible and system identifier;

e) records of successful and rejected system access attempts;

f) records of successful and rejected data and other resource access attempts;

g) changes to system configuration;

h) use of privileges;

i) use of system utilities and applications;

j) files accessed and the kind of access;

k) network addresses and protocols;

l) alarms raised by the access control system;

m) activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems;

n) records of transactions executed by users in applications.

Event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.

Other information

Event logs can contain sensitive data and personally identifiable information. Appropriate privacy protection measures should be taken (see 18.1.4).

Where possible, system administrators should not have permission to erase or de-activate logs of their own activities (see 12.4.3).

### 12.4.2 Protection of log information

Control

Logging facilities and log information should be protected against tampering and unauthorized access.

Implementation guidance

Controls should aim to protect against unauthorized changes to log information and operational problems with the logging facility including:

a) alterations to the message types that are recorded;

b) log files being edited or deleted;

c) storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.

Some audit logs may be required to be archived as part of the record retention policy or because of requirements to collect and retain evidence (see 16.1.7).

Other information

事态日志宜在需要时包括：

a） 用户 ID；

b） 系统活动；

c） 日期、时间和关键事态的细节，例如登录和退出；

d） 若有可能，设备身份或位置以及系统身份；

e） 成功的和被拒绝的对系统尝试访问的记录；

f） 成功的和被拒绝的对数据以及其他资源尝试访问的记录；

g） 系统配置的变更；

h） 特殊权限的使用；

i） 系统实用工具和应用程序的使用；

j） 访问的文件和访问类型；

k） 网络地址和协议；

l） 访问控制系统引发的警报；

m） 防护系统的激活和停用，例如防病毒系统和入侵检测系统；

n） 应用系统中用户执行的交易记录。

事态记录成为自动监视系统的基础，该系统可以提供综合报告并且能够针对系统安全提供告警。

其他信息

事态日志包含敏感数据和个人身份信息，宜采取适当的隐私保护措施（见 18.1.4）。

可能时，系统管理员不宜有删除或停用他们自己活动日志的权利（见 12.4.3）。

### 12.4.2 日志信息的保护

控制措施

记录日志的设施和日志信息宜加以保护，以防止篡改和未授权的访问。

实施指南

宜实施控制措施以防止日志信息被未授权更改以及日志设施出现操作问题，包括：

a) 更改已记录的消息类型；

b) 日志文件被编辑或删除；

c) 超越日志文件介质的存储容量，导致不能记录事态或过去记录事态被写覆盖。

一些审计日志可能需要被存档，以作为记录保持策略的一部分或由于收集和保留证据的要求（见 16.1.7）。

其他信息

System logs often contain a large volume of information, much of which is extraneous to information security monitoring. To help identify significant events for information security monitoring purposes, the copying of appropriate message types automatically to a second log, or the use of suitable system utilities or audit tools to perform file interrogation and rationalization should be considered.

System logs need to be protected, because if the data can be modified or data in them deleted, their existence may create a false sense of security. Real-time copying of logs to a system outside the control of a system administrator or operator can be used to safeguard logs.

### 12.4.3 Administrator and operator logs

Control

System administrator and system operator activities should be logged and the logs protected and regularly reviewed.

Implementation guidance

Privileged user account holders may be able to manipulate the logs on information processing facilities under their direct control, therefore it is necessary to protect and review the logs to maintain accountability for the privileged users.

Other information

An intrusion detection system managed outside of the control of system and network administrators can be used to monitor system and network administration activities for compliance.

### 12.4.4 Clock synchronisation

Control

The clocks of all relevant information processing systems within an organization or security domain should be synchronised to a single reference time source.

Implementation guidance

External and internal requirements for time representation, synchronisation and accuracy should be documented. Such requirements can be legal, regulatory, contractual requirements, standards compliance or requirements for internal monitoring. A standard reference time for use within the organization should be defined.

The organization's approach to obtaining a reference time from external source(s) and how to synchronise internal clocks reliably should be documented and implemented.

Other information

The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence. A clock linked to a radio time broadcast from a national atomic clock can be used as the master clock for logging systems. A network time protocol can be used to keep all of the servers in synchronisation with the master clock.

## 12.5 Control of operational software

| Objective: To ensure the integrity of operational systems. |
|---|

### 12.5.1 Installation of software on operational systems

Control

系统日志通常包含大量的信息，其中许多与信息安全监视无关。为帮助识别出对信息安全监视目的有重要意义的事态，宜考虑将相应的消息类型自动地拷贝到第二份日志和/或使用适合的系统实用工具或审计工具执行文件查询及规范化。

需要保护系统日志，因为如果其中的数据被修改或删除，可能导致一个错误的安全判断。实时复制日志到系统管理员和操作员控制范围外的系统，可用于日志防护。

### 12.4.3 管理员和操作员日志

控制措施

系统管理员和系统操作员的活动宜记入日志，保护日志并定期评审。

实施指南

特权用户账户持有人可操作其直接控制下的信息处理设施日志。因此，为保持特权用户的可稽核性，保护和评审日志是必要的。

其他信息

对在系统和网络管理员控制之外进行管理的入侵检测系统可以用来监视系统和网络管理活动的符合性。

### 12.4.4 时钟同步

控制措施

一个组织或安全域内的所有相关信息处理设施的时钟宜使用单一参考时间源进行同步。

实施指南

宜记录时间表示、同步和精确的内部及外部要求，这些要求符合法律、法规及合同要求，同时也符合标准一致性或内部监视要求。宜定义标准参考时间用于组织内。

宜记录和实施组织从外部源获取参考时间的方法以及如何同步内部时钟并保证可靠性。

其他信息

正确设置计算机时钟对确保审计记录的准确性是重要的，审计日志可用于调查或作为法律、纪律处理的证据。不准确的审计日志可能妨碍调查，并损害这种证据的可信性。链接到国家原子钟无线电广播时间的时钟可用于记录系统的主时钟。可以用网络时间协议保持所有服务器与主时钟同步。

## 12.5 运行软件的控制

| |
|---|
| 目标：确保运行系统的完整性。 |

### 12.5.1 在运行系统上安装软件

控制措施

Procedures should be implemented to control the installation of software on operational systems.

Implementation guidance

The following guidelines should be considered to control changes of software on operational systems:

a) the updating of the operational software, applications and program libraries should only be performed by trained administrators upon appropriate management authorization (see 9.4.5);

b) operational systems should only hold approved executable code and not development code or compilers;

c) applications and operating system software should only be implemented after extensive and successful testing; the tests should cover usability, security, effects on other systems and user-friendliness and should be carried out on separate systems (see 12.1.4); it should be ensured that all corresponding program source libraries have been updated;

d) a configuration control system should be used to keep control of all implemented software as well as the system documentation;

e) a rollback strategy should be in place before changes are implemented;

f) an audit log should be maintained of all updates to operational program libraries;

g) previous versions of application software should be retained as a contingency measure;

h) old versions of software should be archived, together with all required information and parameters, procedures, configuration details and supporting software for as long as the data are retained in archive.

Vendor supplied software used in operational systems should be maintained at a level supported by the supplier. Over time, software vendors will cease to support older versions of software. The organization should consider the risks of relying on unsupported software.

Any decision to upgrade to a new release should take into account the business requirements for the change and the security of the release, e.g. the introduction of new information security functionality or the number and severity of information security problems affecting this version. Software patches should be applied when they can help to remove or reduce information security weaknesses (see 12.6).

Physical or logical access should only be given to suppliers for support purposes when necessary and with management approval. The supplier's activities should be monitored (see 15.2.1).

Computer software may rely on externally supplied software and modules, which should be monitored and controlled to avoid unauthorized changes, which could introduce security weaknesses.

## 12.6 Technical vulnerability management

| Objective: To prevent exploitation of technical vulnerabilities. |
|---|

### 12.6.1 Management of technical vulnerabilities

Control

Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

Implementation guidance

A current and complete inventory of assets (see Clause 8) is a prerequisite for effective technical vulnerability management. Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment (e.g. what software is installed on what systems) and the person(s) within the organization responsible for the software.

宜实施规程来控制在运行系统上安装软件。

实施指南

为控制运行系统的软件变更，宜考虑下列指南：

a) 要仅由受过培训的管理员，根据合适的管理授权（见 9.4.5），进行运行软件、应用和程序库的更新；

b) 运行系统要仅安装经过批准的可执行代码，不安装开发代码和编译程序；

c) 应用和操作系统软件要在大范围的、成功的测试之后才能实施；这种测试腰要包括实用性、安全性、对其他系统的影响和用户友好性的测试，且测试要在独立的系统上完成（见 12.1.4）；要确保所有对应的程序源库已经更新；

d) 要使用配置控制系统对所有已开发的软件和系统文件进行控制；

e) 在变更实施之前要有还原的策略；

f) 要维护对运行程序库的所有更新的审计日志；

g) 要保留应用软件的先前版本作为应急措施；

h) 软件的旧版本，连同所有需要的信息和参数、规程、配置细节以及支持软件，以及进行与归档数据具有相同保留期的归档。

在运行系统中所使用的由厂商供应的软件宜在供应商支持的级别上加以维护。一段时间后，软件供应商停止支持旧版本的软件。组织宜考虑依赖于这种不再支持的软件的风险。

升级到新版的任何决策宜考虑变更的业务要求和新版的安全，即引入的新安全功能或影响该版本安全问题的数量和严重程度。当软件补丁有助于消除或减少安全弱点（见 12.6）时宜使用软件补丁。

必要时在管理者批准的情况下，仅为了支持目的，才授予供应商物理或逻辑访问权。宜监督供应商的活动（见 15.2.1）。

计算机软件可能依赖于外部提供的软件和模块，宜对这些产品进行监视和控制，以避免可能引入安全弱点的非授权的变更。

## 12.6 技术脆弱性管理

| |
|---|
| 目标：防止技术脆弱性被利用。 |

### 12.6.1 技术脆弱性的控制

控制措施

宜及时得到现用信息系统技术脆弱性的信息，评价组织对这些脆弱性的暴露程度，并采取适当的措施来处理相关的风险。

实施指南

当前的、完整的资产清单（见 8）是进行有效技术脆弱性管理的先决条件。支持技术脆弱性管理所需的特定信息包括软件供应商、版本号、部署的当前状态（例如，在什么系统上安装什么软件），以及组织内负责软件的人员。

Appropriate and timely action should be taken in response to the identification of potential technical vulnerabilities. The following guidance should be followed to establish an effective management process for technical vulnerabilities:

a) the organization should define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking and any coordination responsibilities required;

b) information resources that will be used to identify relevant technical vulnerabilities and to maintain awareness about them should be identified for software and other technology (based on the asset inventory list, see 8.1.1); these information resources should be updated based on changes in the inventory or when other new or useful resources are found;

c) a timeline should be defined to react to notifications of potentially relevant technical vulnerabilities;

d) once a potential technical vulnerability has been identified, the organization should identify the associated risks and the actions to be taken; such action could involve patching of vulnerable systems or applying other controls;

e) depending on how urgently a technical vulnerability needs to be addressed, the action taken should be carried out according to the controls related to change management (see 12.1.2) or by following information security incident response procedures (see 16.1.5);

f) if a patch is available from a legitimate source, the risks associated with installing the patch should be assessed (the risks posed by the vulnerability should be compared with the risk of installing the patch);

g) patches should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls should be considered, such as:

   1) turning off services or capabilities related to the vulnerability;

   2) adapting or adding access controls, e.g. firewalls, at network borders (see 13.1);

   3) increased monitoring to detect actual attacks;

   4) raising awareness of the vulnerability;

h) an audit log should be kept for all procedures undertaken;

i) the technical vulnerability management process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency;

j) systems at high risk should be addressed first;

k) an effective technical vulnerability management process should be aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide technical procedures to be carried out should an incident occur;

l) define a procedure to address the situation where a vulnerability has been identified but there is no suitable countermeasure. In this situation, the organization should evaluate risks relating to the known vulnerability and define appropriate detective and corrective actions.

Other information

Technical vulnerability management can be viewed as a sub-function of change management and as such can take advantage of the change management processes and procedures (see 12.1.2 and 14.2.2).

Vendors are often under significant pressure to release patches as soon as possible. Therefore, there is a possibility that a patch does not address the problem adequately and has negative side effects. Also, in some cases, uninstalling a patch cannot be easily achieved once the patch has been applied.

宜采取适当的、及时的措施以响应潜在的技术脆弱性。建立有效的技术脆弱性管理过程宜遵循下列指南：

a) 组织要定义和建立与技术脆弱性管理相关的角色和职责，包括脆弱性监视、脆弱性风险评估、打补丁、资产追踪和任意需要的协调责任；

b) 用于识别相关的技术脆弱性和维护有关这些脆弱性的认识的信息资源，要被识别用于软件和其他技术（基于资产清单，见 8.1.1）；这些信息资源要根据清单的变更而更新，或当发现其他新的或有用的资源时，也要更新；

c) 要制定时间表对潜在的相关技术脆弱性的通知做出反映；

d) 一旦潜在的技术脆弱性被确定，组织要识别相关的风险并采取措施；这些措施可能包括对脆弱的系统打补丁和/或应用其他控制措施；

e) 按照技术脆弱性需要解决的紧急程度，要根据变更管理相关的控制措施（见 12.1.2），或者遵照信息安全事件响应规程（见 16.1.5），采取措施；

f) 如果有可用的补丁，则要评估与安装该补丁相关的风险（脆弱性引起的风险要与安装补丁带来的风险进行比较）；

g) 在安装补丁之前，要进行测试与评价，以确保它们是有效的，且不会导致不能容忍的负面影响；如果没有可用的补丁，要考虑其他控制措施，例如：

   1） 关闭与脆弱性有关的服务和功能；

   2） 调整或增加访问控制措施，例如在网络边界上添加防火墙（见 13.1）；

   3） 增加监视以检测实际的攻击；

   4） 提高脆弱性意识；

h) 要对所有执行的规程进行日志审计；

i) 要定期对技术脆弱性管理过程进行监视和评价，以确保其有效性和效率；

j) 处于高风险中的系统要首先解决；

k) 一个有效的技术脆弱性管理过程宜符合事件管理活动，沟通事件响应的功能脆弱性数据，并提供处置所发生事件的技术规程；

l) 宜定义一个规程说明脆弱性已经被识别但没有适当防范措施的情况。在这种情况下，组织宜评估已知脆弱性的相关风险并确定适当的检测或纠正措施。

其他信息

技术脆弱性管理可被看作是变更管理的一个子功能，因此可以利用变更管理的过程和规程（见 12.1.2 和 14.2.2）。

供应商往往是在很大的压力下发布补丁。因此，补丁可能不足以解决该问题，并且可能存在负作用。而且，在某些情况下，一旦补丁被安装后，很难被卸载。

If adequate testing of the patches is not possible, e.g. because of costs or lack of resources, a delay in patching can be considered to evaluate the associated risks, based on the experience reported by other users. The use of ISO/IEC 27031[14] can be beneficial.

### 12.6.2 Restrictions on software installation

Control

Rules governing the installation of software by users should be established and implemented.

Implementation guidance

The organization should define and enforce strict policy on which types of software users may install.

The principle of least privilege should be applied. If granted certain privileges, users may have the ability to install software. The organization should identify what types of software installations are permitted (e.g. updates and security patches to existing software) and what types of installations are prohibited (e.g. software that is only for personal use and software whose pedigree with regard to being potentially malicious is unknown or suspect). These privileges should be granted having regard to the roles of the users concerned.

Other information

Uncontrolled installation of software on computing devices can lead to introducing vulnerabilities and then to information leakage, loss of integrity or other information security incidents, or to violation of intellectual property rights.

## 12.7 Information systems audit considerations

| Objective: To minimise the impact of audit activities on operational systems. |
|---|

### 12.7.1 Information systems audit controls

Control

Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes.

Implementation guidance

The following guidelines should be observed:

a) audit requirements for access to systems and data should be agreed with appropriate management;

b) the scope of technical audit tests should be agreed and controlled;

c) audit tests should be limited to read-only access to software and data;

d) access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements;

e) requirements for special or additional processing should be identified and agreed;

f) audit tests that could affect system availability should be run outside business hours;

g) all access should be monitored and logged to produce a reference trail.

如果不能对补丁进行充分的测试，如由于成本或资源缺乏，那么可以考虑推迟打补丁，以便基于其他用户报告的经验来评价相关的风险。使用 ISO/IEC 27031 是有益的。

### 12.6.2 限制软件安装

控制措施

宜建立和实施软件安装的用户管理规则。

实施指南

组织宜定义和加强用户可安装软件类型的限制策略。

宜应用最小授权原则，如果授予一定的权限，用户则有安装软件的能力。组织宜确定什么类型软件允许安装（例如，现有软件的更新和安全补丁）和什么类型软件禁止安装（例如仅为个人使用的软件以及其谱系可能存在未知或可疑恶意代码的软件）。宜根据用户的角色进行权限的授予。

其他信息

若计算机设备上的软件安装失控，则可能导致脆弱性，进而导致信息泄露、完整性破坏或其他信息安全事件，或者是侵犯知识产权。

## 12.7 信息系统审计考虑

| 目标：将运行系统审计活动的影响最小化。 |
| --- |

### 12.7.1 信息系统审计控制措施

控制措施

涉及对运行系统验证的审计要求和活动，宜谨慎地加以规划并取得批准，以便使造成业务过程中断最小化。

实施指南

宜遵守下列指南：

a) 要与合适的管理者商定访问系统和数据的审计要求；

b) 要商定和控制技术审计测试的范围；

c) 审计测试仅限于对软件和数据的只读访问；

d) 非只读的访问要仅用于对系统文件的单独拷贝，当审计完成时，要擦除这些拷贝，或者按照审计文件要求，具有保留这些文件的义务，则要给予适当的保护；

e) 要识别和商定特定的或另外的处理要求；

f) 若审计测试会影响系统的可用性，则宜在非业务时间进行测试；

g) 要监视和记录所有访问，以产生参照踪迹。

# 13 Communications security

## 13.1 Network security management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

### 13.1.1 Network controls

Control

Networks should be managed and controlled to protect information in systems and applications.

Implementation guidance

Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorized access. In particular, the following items should be considered:

a) responsibilities and procedures for the management of networking equipment should be established;

b) operational responsibility for networks should be separated from computer operations where appropriate (see 6.1.2);

c) special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (see Clause 10 and 13.2); special controls may also be required to maintain the availability of the network services and computers connected;

d) appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security;

e) management activities should be closely coordinated both to optimize the service to the organization and to ensure that controls are consistently applied across the information processing infrastructure;

f) systems on the network should be authenticated;

g) systems connection to the network should be restricted.

Other information

Additional information on network security can be found in ISO/IEC 27033.[15][16][17][18][19]

### 13.1.2 Security of network services

Control

Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.

Implementation guidance

The ability of the network service provider to manage agreed services in a secure way should be determined and regularly monitored, and the right to audit should be agreed.

The security arrangements necessary for particular services, such as security features, service levels and management requirements, should be identified. The organization should ensure that network service providers implement these measures.

Other information

## 13 通信安全

### 13.1 网络安全管理

| |
|---|
| 目标：确保网络中信息的安全性并保护支持性信息处理设施。 |

#### 13.1.1 网络控制

控制措施

宜管理和控制网络，以保护系统中信息和应用程序的安全。

实施指南

宜实施控制措施，以确保网络上的信息安全、防止未授权访问所连接的服务。特别是，宜考虑下列条款：

a） 要建立网络设备管理的职责和规程；

b） 若合适，网络的操作职责要与计算机操作分开（见 6.1.5）；

c） 要建立专门的控制，以防护在公用网络上或无线网络上传递数据的保密性和完整性，并且保护已连接的系统及应用（见 10 和 13.2）；为维护所连接的网络服务和计算机的可用性，还可以要求专门的控制；

d） 为记录和检测可能影响信息安全或与之相关的活动，要使用适当的日志记录和监视措施；

e） 为优化对组织的服务和确保在信息处理基础设施上始终如一地应用若干控制措施，要紧密地协调管理活动；

f） 网络系统宜被鉴别；

g） 系统接入网络宜被限制。

其他信息

关于网络安全的另外信息参见ISO/IEC 27033 网络安全。

#### 13.1.2 网络服务安全

控制措施

安全机制、服务级别以及所有网络服务的管理要求宜予以确定并包括在所有网络服务协议中，无论这些服务是由内部提供的还是外包的。

实施指南

网络服务提供商以安全方式管理商定服务的能力宜予以确定并定期监视，还宜商定审核的权利。

宜识别特殊服务的安全安排，例如安全特性、服务级别和管理要求。组织宜确保网络服务提供商实施了这些措施。

其他信息

Network services include the provision of connections, private network services and value added networks and managed network security solutions such as firewalls and intrusion detection systems. These services can range from simple unmanaged bandwidth to complex value-added offerings.

Security features of network services could be:

a) technology applied for security of network services, such as authentication, encryption and network connection controls;

b) technical parameters required for secured connection with the network services in accordance with the security and network connection rules;

c) procedures for the network service usage to restrict access to network services or applications, where necessary.

### 13.1.3 Segregation in networks

Control

Groups of information services, users and information systems should be segregated on networks.

Implementation guidance

One method of managing the security of large networks is to divide them into separate network domains. The domains can be chosen based on trust levels (e.g. public access domain, desktop domain, server domain), along organizational units (e.g. human resources, finance, marketing) or some combination (e.g. server domain connecting to multiple organizational units). The segregation can be done using either physically different networks or by using different logical networks (e.g.virtual private networking).

The perimeter of each domain should be well defined. Access between network domains is allowed, but should be controlled at the perimeter using a gateway (e.g. firewall, filtering router). The criteria for segregation of networks into domains, and the access allowed through the gateways, should be based on an assessment of the security requirements of each domain. The assessment should be in accordance with the access control policy (see 9.1.1), access requirements, value and classification of information processed and also take account of the relative cost and performance impact of incorporating suitable gateway technology.

Wireless networks require special treatment due to the poorly defined network perimeter. For sensitive environments, consideration should be made to treat all wireless access as external connections and to segregate this access from internal networks until the access has passed through a gateway in accordance with network controls policy (see 13.1.1) before granting access to internal systems.

The authentication, encryption and user level network access control technologies of modern, standards based wireless networks may be sufficient for direct connection to the organization's internal network when properly implemented.

Other information

Networks often extend beyond organizational boundaries, as business partnerships are formed that require the interconnection or sharing of information processing and networking facilities. Such extensions can increase the risk of unauthorized access to the organization's information systems that use the network, some of which require protection from other network users because of their sensitivity or criticality.

## 13.2 Information transfer

| Objective: To maintain the security of information transferred within an organization and with any external entity. |
|---|

网络服务包括接入服务、私有网络服务、增值网络和受控的网络安全解决方案，例如防火墙和入侵检测系统。这些服务既包括简单的未受控的带宽也包括复杂的增值的提供。

网络服务的安全特性可以是：

a) 为网络服务应用的安全技术，例如鉴别、加密和网络连接控制；

b) 按照安全和网络连接规则，网络服务的安全连接需要的技术参数；

c) 若必要，网络服务使用规程，以限制对网络服务或应用的访问。

### 13.1.3 网络隔离

控制措施

宜在网络中隔离信息服务、用户及信息系统。

实施指南

管理大型网络安全的一种方法是将该网络分成独立的网络域，选择网络域可基于可信级别（例如，公共访问域、桌面终端域、服务器域），也可基于独立的组织单元（例如，人力资源、财务、市场）或一些组合（例如，连接多个组织单元的服务器域）。不同的网络之间或者通过物理方式或者通过逻辑方式隔离（例如，虚拟专用网络）。

宜明确每个域的边界。网络域之间的访问是允许的，但宜通过在边界安装网关（例如，防火墙、过滤路由器）进行控制。宜基于对每个域安全要求的评估结果，确定网络域隔离准则和通过网关所允许的访问。评估宜遵循访问控制策略（见 9.1.1）、访问要求、所处理信息的价值和类别，还宜考虑到相关成本和加入适合的网关技术的性能影响。

由于无线网络的周边不好定义，因此其要求宜特别处理。对于敏感环境，宜考虑将所有无线访问作为外部连接处理（见 9.4.2），并且在允许访问内部网络之前，从内网中隔离无线访问，直到已经按照网络控制策略（见 13.1.1）通过网关访问。

当正确实施基于无线网络的身份鉴别、加密和用户层网络访问控制现代技术标准时，对于直接接入组织内部网络可能是充分的。

其他信息

正在日益扩展的网络超出了组织边界，因为形成的业务伙伴可能需要信息处理和网络设施的互连或共享。这样的扩展可能增加对使用此网络的组织的信息系统进行未授权访问的风险，其中的某些系统由于其敏感性或关键性可能需要防范其他的网络用户。

## 13.2 信息传递

| |
|---|
| 目标：保持组织内以及与组织外信息传递的安全。 |

### 13.2.1 Information transfer policies and procedures

Control

Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities.

Implementation guidance

The procedures and controls to be followed when using communication facilities for information transfer should consider the following items:

a) procedures designed to protect transferred information from interception, copying, modification, mis-routing and destruction;

b) procedures for the detection of and protection against malware that may be transmitted through the use of electronic communications (see 12.2.1);

c) procedures for protecting communicated sensitive electronic information that is in the form of an attachment;

d) policy or guidelines outlining acceptable use of communication facilities (see 8.1.3);

e) personnel, external party and any other user's responsibilities not to compromise the organization, e.g. through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.;

f) use of cryptographic techniques e.g. to protect the confidentiality, integrity and authenticity of information (see Clause 10);

g) retention and disposal guidelines for all business correspondence, including messages, in accordance with relevant national and local legislation and regulations;

h) controls and restrictions associated with using communication facilities, e.g. automatic forwarding of electronic mail to external mail addresses;

i) advising personnel to take appropriate precautions not to reveal confidential information;

j) not leaving messages containing confidential information on answering machines since these may be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialling;

k) advising personnel about the problems of using facsimile machines or services, namely:

   1) unauthorized access to built-in message stores to retrieve messages;

   2) deliberate or accidental programming of machines to send messages to specific numbers;

   3) sending documents and messages to the wrong number either by misdialling or using the wrong stored number.

In addition, personnel should be reminded that they should not have confidential conversations in public places or over insecure communication channels, open offices and meeting places.

Information transfer services should comply with any relevant legal requirements (see 18.1).

Other information

Information transfer may occur through the use of a number of different types of communication facilities, including electronic mail, voice, facsimile and video.

Software transfer may occur through a number of different mediums, including downloading from the Internet and acquisition from vendors selling off-the-shelf products.

### 13.2.1 信息传递策略和规程

控制措施

宜有正式的传递策略、规程和控制措施，以保护通过使用各种类型通信设施的信息传递。

实施指南

使用通信设施进行信息传递的规程和控制宜考虑下列条款：

a) 设计用来防止传递信息遭受截取、复制、修改、错误寻址和破坏的规程；

b) 检测和防止可能通过使用电子通信传输的恶意软件的规程（见 12.2.1）；

c) 保护以附件形式传输的敏感电子信息的规程；

d) 简述通信设施可接受使用的策略或指南（见 8.1.3）；

e) 个人、外部方和所有其他使用人员不危害组织的职责，例如诽谤、扰乱、扮演、连锁信寄送、未授权购买等；

f) 密码技术的使用，例如保护信息的保密性、完整性和真实性（见 10）；

g) 所有业务通信（包括消息）的保持和处理指南，要与相关国家和地方法律法规一致；

h) 与通信设施相关的控制措施和限制，例如将电子邮件自动转发到外部邮件地址；

i) 建议工作人员，为不泄露敏感信息他们要采取相应预防措施：

j) 不要将包含机密信息的消息留在应答机上，因为可能被未授权个人重放，也不能留在公用系统或者由于误拨号而被不正确地存储；

k) 建议工作人员关于传真机或传真服务的使用问题，即：

1） 未授权访问内置消息存储器，以检索消息；

2） 有意的或无意的对传真机编程，将消息发送给特定的电话号码；

3） 由于误拨号或使用错误存储的号码将文件和消息发送给错误的电话号码。

另外，宜提醒工作人员，不要在公共场所、开放办公室和会场以及不要通过不安全的通信渠道进行保密会谈。

信息传递服务宜符合所有相关的法律要求（见 18.1）。

其他信息

可能通过使用多种不同类型的通信设施进行信息传递，例如电子邮件、声音、传真和视频。

可能通过多种不同类型的介质进行软件传递，包括从互联网下载和从出售现货的供应商处获得。

The business, legal and security implications associated with electronic data interchange, electronic commerce and electronic communications and the requirements for controls should be considered.

### 13.2.2 Agreements on information transfer

Control

Agreements should address the secure transfer of business information between the organization and external parties.

Implementation guidance

Information transfer agreements should incorporate the following:

a) management responsibilities for controlling and notifying transmission, dispatch and receipt;

b) procedures to ensure traceability and non-repudiation;

c) minimum technical standards for packaging and transmission;

d) escrow agreements;

e) courier identification standards;

f) responsibilities and liabilities in the event of information security incidents, such as loss of data;

g) use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected (see 8.2);

h) technical standards for recording and reading information and software;

i) any special controls that are required to protect sensitive items, such as cryptography (see Clause 10);

j) maintaining a chain of custody for information while in transit;

k) acceptable levels of access control.

Policies, procedures and standards should be established and maintained to protect information and physical media in transit (see 8.3.3), and should be referenced in such transfer agreements.

The information security content of any agreement should reflect the sensitivity of the business information involved.

Other information

Agreements may be electronic or manual, and may take the form of formal contracts. For confidential information, the specific mechanisms used for the transfer of such information should be consistent for all organizations and types of agreements.

### 13.2.3 Electronic messaging

Control

Information involved in electronic messaging should be appropriately protected.

Implementation guidance

Information security considerations for electronic messaging should include the following:

a) protecting messages from unauthorized access, modification or denial of service commensurate with the classification scheme adopted by the organization;

b) ensuring correct addressing and transportation of the message;

宜考虑与电子数据交换、电子商务、电子通信和控制要求相关的业务、法律和安全含义。

### 13.2.2 信息传递协议

控制措施

协议宜解决组织与外部方之间业务信息的安全传递。

实施指南

信息传递协议宜考虑以下安全条款：

a) 控制和通知传输、分派和接收的管理职责；

b) 确保可追溯性和不可抵赖性的规程；

c) 打包和传输的最低技术标准；

d) 有条件转让契约；

e) 送信人标识标准；

f) 如果发生信息安全事件的职责和义务，例如数据丢失；

g) 商定的标记敏感或关键信息的系统的使用，确保标记的含义能直接理解，信息受到适当的保护（见 8.2）；

h) 记录和阅读信息和软件的技术标准；

i) 为保护敏感项，可以要求任何专门的控制措施，例如加密（见 10）；

j) 维护传输中信息的保管链；

k) 可接受的访问控制级别。

宜建立和保持策略、规程和标准，以保护传输中的信息和物理介质（见 8.3.3），这些 还宜在传递协议中进行引用。

任何协议的安全内容宜反映涉及的业务信息的敏感度。

其他信息

协议可以是电子的或手写的，可能采取正式合同的形式。对机密信息而言，信息传递使用的特定机制对于所有组织和各种协议宜是一致的。

### 13.2.3 电子消息发送

控制措施

包含在电子消息发送中的信息宜给予适当的保护。

实施指南

电子消息发送的信息安全考虑宜包括以下方面：

a) 防止消息遭受未授权访问、修改或拒绝服务攻击，与组织采取的分类方案对应；

b) 确保正确的寻址和消息传输；

c) reliability and availability of the service;

d) legal considerations, for example requirements for electronic signatures;

e) obtaining approval prior to using external public services such as instant messaging, social networking or file sharing;

f) stronger levels of authentication controlling access from publicly accessible networks.

Other information

There are many types of electronic messaging such as email, electronic data interchange and social networking which play a role in business communications.

### 13.2.4 Confidentiality or non-disclosure agreements

Control

Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, regularly reviewed and documented.

Implementation guidance

Confidentiality or non-disclosure agreements should address the requirement to protect confidential information using legally enforceable terms. Confidentiality or non-disclosure agreements are applicable to external parties or employees of the organization. Elements should be selected or added in consideration of the type of the other party and its permissible access or handling of confidential information. To identify requirements for confidentiality or non-disclosure agreements, the following elements should be considered:

a) a definition of the information to be protected (e.g. confidential information);

b) expected duration of an agreement, including cases where confidentiality might need to be maintained indefinitely;

c) required actions when an agreement is terminated;

d) responsibilities and actions of signatories to avoid unauthorized information disclosure;

e) ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information;

f) the permitted use of confidential information and rights of the signatory to use information;

g) the right to audit and monitor activities that involve confidential information;

h) process for notification and reporting of unauthorized disclosure or confidential information leakage;

i) terms for information to be returned or destroyed at agreement cessation;

j) expected actions to be taken in case of a breach of the agreement.

Based on an organization's information security requirements, other elements may be needed in a confidentiality or non-disclosure agreement.

Confidentiality and non-disclosure agreements should comply with all applicable laws and regulations for the jurisdiction to which they apply (see 18.1).

Requirements for confidentiality and non-disclosure agreements should be reviewed periodically and when changes occur that influence these requirements.

Other information

c) 服务的可靠性和可用性；

d) 法律方面的考虑，例如电子签名的要求；

e) 在使用外部公共服务（例如即时消息、社交网络或文件共享）前获得批准；

f) 更强的用以控制从公开可访问网络进行访问的鉴别级别。

其他信息

电子消息（例如电子邮件、电子数据交换（EDI）、社交网络）在业务通信中充当一个日益重要的角色。

### 13.2.4 保密性或不泄露协议

控制措施

宜识别、定期评审并记录反映组织信息保护需要的保密性或不泄露协议的要求。

实施指南

保密或不泄露协议宜使用合法可实施条款来解决保护保密信息的要求。保密或不泄露协议适用于外部各方和组织的员工。宜根据其他团体的类型以及允许起访问或处理的机密信息选择或增加条款。要识别保密或不泄露协议的要求，宜考虑下列因素：

a) 定义要保护的信息（例如如保密信息）；

b) 协议的期望持续时间，包括不确定地需要维持保密性的情形；

c) 协议终止时所需的措施；

d) 签署者的职责和行为，以避免未授权信息泄露；

e) 信息、商业秘密和知识产权的所有权，及其如何与保密信息保护相关；

f) 保密信息的许可使用，及签署者使用信息的权力；

g) 对涉及保密信息的活动的审核和监视权力；

h) 未授权泄露或保密信息破坏的通知和报告过程；

i) 关于协议终止时信息归档或销毁的条款；

j) 违反协议时期望采取的措施。

基于一个组织的信息安全要求，在保密性或不泄露协议中可能需要其他因素。

保密性和不泄露协议宜针对它适用的管辖范围遵循所有适用的法律法规（见 18.1）。保密性和不泄露协议的要求宜进行周期性评审，当发生影响这些要求的变更时，也宜进行评审。

其他信息

Confidentiality and non-disclosure agreements protect organizational information and inform signatories of their responsibility to protect, use and disclose information in a responsible and authorized manner.

There may be a need for an organization to use different forms of confidentiality or non-disclosure agreements in different circumstances.

# 14 System acquisition, development and maintenance

## 14.1 Security requirements of information systems

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

### 14.1.1 Information security requirements analysis and specification

Control

The information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems.

Implementation guidance

Information security requirements should be identified using various methods such as deriving compliance requirements from policies and regulations, threat modelling, incident reviews, or use of vulnerability thresholds. Results of the identification should be documented and reviewed by all stakeholders.

Information security requirements and controls should reflect the business value of the information involved (see 8.2) and the potential negative business impact which might result from lack of adequate security.

Identification and management of information security requirements and associated processes should be integrated in early stages of information systems projects. Early consideration of information security requirements, e.g. at the design stage can lead to more effective and cost efficient solutions.

Information security requirements should also consider:

a) the level of confidence required towards the claimed identity of users, in order to derive user authentication requirements;

b) access provisioning and authorization processes, for business users as well as for privileged or technical users;

c) informing users and operators of their duties and responsibilities;

d) the required protection needs of the assets involved, in particular regarding availability, confidentiality, integrity;

e) requirements derived from business processes, such as transaction logging and monitoring, non-repudiation requirements;

f) requirements mandated by other security controls, e.g. interfaces to logging and monitoring or data leakage detection systems.

For applications that provide services over public networks or which implement transactions, the dedicated controls 14.1.2 and 14.1.3 should be considered.

If products are acquired, a formal testing and acquisition process should be followed. Contracts with the supplier should address the identified security requirements. Where the security functionality

保密性和不泄密协议保护组织信息，并告知签署者他们的职责，以授权、负责的方式保护、使用和公开信息。

对于一个组织来说，可能需要在不同环境中使用保密性或不泄密协议的不同格式。

## 14 系统获取、开发和维护

### 14.1 信息系统的安全要求

| |
|---|
| 目标：确保信息安全是信息系统整个生命周期中的一个有机组成部分。这也包括提供公共网络服务的信息系统的要求。 |

#### 14.1.1 信息安全要求分析和说明

控制措施

信息安全相关要求宜包括新的信息系统要求或增强已有信息系统的要求。

实施指南

宜采用不同方法识别信息安全要求，例如遵从策略和法规要求、威胁模型、事件评审以及脆弱性阀值等方法。宜记录识别结果并确保通过利益相关者评审。

信息安全要求和控制措施宜反映出所涉及的信息资产的业务价值（见 8.2），和可能由于安全措施不足引起的潜在的业务负面影响。

信息安全要求的识别和处理以及相关的过程宜在信息系统项目的早期阶段被集成。越早考虑信息安全要求（例如在设计阶段）则越可能产生更有效及更符合成本效益的结果。

信息安全要求宜考虑：

a） 为了获得用户身份鉴别要求，需要确认用户所宣称身份的信任级别；

b） 访问资源调配与授权过程，对于业务用户与特权用户或技术用户是相同的；

c） 告知用户和操作员他们的权限及职责；

d） 涉及的资产需要所要求的保护，特别是可用性、保密性和完整性；

e） 源自业务过程的要求，例如交易记录、监视和抗抵赖等要求；

f） 其他安全控制强制的要求，例如日志记录和监视或数据泄露检测系统之间的接口。

通过公共网络提供服务或者实施交易的应用，其专用控制措施宜在 14.1.2 和 14.1.3 考虑。

如果购买产品，则宜遵循一个正式的测试和获取过程。与供应商签订的合同宜给出已确定的安全要求。如果推荐的产品的安全功能不能满足安全要求，那么在购买产品之前宜重新考虑引入的风险和相关控制措施。

in a proposed product does not satisfy the specified requirement, the risk introduced and associated controls should be reconsidered prior to purchasing the product.

Available guidance for security configuration of the product aligned with the final software / service stack of that system should be evaluated and implemented.

Criteria for accepting products should be defined e.g. in terms of their functionality, which will give assurance that the identified security requirements are met. Products should be evaluated against these criteria before acquisition. Additional functionality should be reviewed to ensure it does not introduce unacceptable additional risks.

Other information

ISO/IEC 27005[11] and ISO 31000[27] provide guidance on the use of risk management processes to identify controls to meet information security requirements.

### 14.1.2 Securing application services on public networks

Control

Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

Implementation guidance

Information security considerations for application services passing over public networks should include the following:

a) the level of confidence each party requires in each other's claimed identity, e.g. through authentication;

b) authorization processes associated with who may approve contents of, issue or sign key transactional documents;

c) ensuring that communicating partners are fully informed of their authorizations for provision or use of the service;

d) determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key documents and the non-repudiation of contracts, e.g. associated with tendering and contract processes;

e) the level of trust required in the integrity of key documents;

f) the protection requirements of any confidential information;

g) the confidentiality and integrity of any order transactions, payment information, delivery address details and confirmation of receipts;

h) the degree of verification appropriate to verify payment information supplied by a customer;

i) selecting the most appropriate settlement form of payment to guard against fraud;

j) the level of protection required to maintain the confidentiality and integrity of order information;

k) avoidance of loss or duplication of transaction information;

l) liability associated with any fraudulent transactions;

m) insurance requirements.

Many of the above considerations can be addressed by the application of cryptographic controls (see Clause 10), taking into account compliance with legal requirements (see Clause 18, especially see 18.1.5 for cryptography legislation).

系统中承载最终软件或服务的产品的安全配置指南宜被评估和实施。

宜定义所接收产品的准则，例如产品的功能条款，以确保满足已识别的安全要求。在获取产品之前宜对准则进行评估。宜对附加功能进行评审，以确保没有引入不可接受的、另外的风险。

其他信息

ISO/IEC 27005 和 ISO3100 提供了使用风险管理过程确定安全控制措施满足信息安全要求的指南。

### 14.1.2 公共网络应用服务安全

控制措施

宜保护公共网络中的应用服务信息，以防止欺骗行为、合同纠纷、未授权泄露和修改。

实施指南

通过公共网络的应用服务的信息安全，宜考虑下列条款：

a） 在彼此声称的身份中，每一方要求的信任级别，例如通过鉴别;；

b） 与谁确定批准内容、发布或签署关键交易文件相关的授权过程；

c） 确保合作伙伴完全接到他们所提供或使用服务的授权通知；

d） 决定并满足保密性、完整性和关键文件的分发和接收的证明以及合同不可抵赖性方面的要求，例如关于提出和订约过程；

e） 关键文档完整性所要求的可信级别；

f） 任何保密信息的保护要求；

g） 任何订单交易、支付信息、交付地址细节和接收确认的保密性和完整性；

h） 适于验证用户提供的支付信息的验证程度；

i） 为防止欺诈，选择最适合的支付解决形式；

j） 为保持订单信息的保密性和完整性要求的保护级别；

k） 避免交易信息的丢失或复制；

l） 与所有欺诈交易相关的责任；

m） 保险要求。

上述许多考虑可以通过应用密码技术来实现（见第十章），还要考虑符合法律要求（见第十八章，特别是 18.1.5 密码法规）。

Application service arrangements between partners should be supported by a documented agreement which commits both parties to the agreed terms of services, including details of authorization (see b) above).

Resilience requirements against attacks should be considered, which can include requirements for protecting the involved application servers or ensuring the availability of network interconnections required to deliver the service.

Other information

Applications accessible via public networks are subject to a range of network related threats, such as fraudulent activities, contract disputes or disclosure of information to the public. Therefore, detailed risk assessments and proper selection of controls are indispensable. Controls required often include cryptographic methods for authentication and securing data transfer.

Application services can make use of secure authentication methods, e.g. using public key cryptography and digital signatures (see Clause 10) to reduce the risks. Also, trusted third parties can be used, where such services are needed.

### 14.1.3 Protecting application services transactions

Control

Information involved in application service transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Implementation guidance

Information security considerations for application service transactions should include the following:

a) the use of electronic signatures by each of the parties involved in the transaction;

b) all aspects of the transaction, i.e. ensuring that:

   1) user's secret authentication information of all parties are valid and verified;

   2) the transaction remains confidential;

   3) privacy associated with all parties involved is retained;

c) communications path between all involved parties is encrypted;

d) protocols used to communicate between all involved parties are secured;

e) ensuring that the storage of the transaction details is located outside of any publicly accessible environment, e.g. on a storage platform existing on the organizational intranet, and not retained and exposed on a storage medium directly accessible from the Internet;

f) where a trusted authority is used (e.g. for the purposes of issuing and maintaining digital signatures or digital certificates) security is integrated and embedded throughout the entire end-to-end certificate/signature management process.

Other information

The extent of the controls adopted needs to be commensurate with the level of the risk associated with each form of application service transaction.

Transactions may need to comply with legal and regulatory requirements in the jurisdiction which the transaction is generated from, processed via, completed at or stored in.

宜通过文件化的协议来支持合作伙伴之间的应用服务安排，该协议使双方致力于商定的服务条款，包括授权细节（见上述 b））。

宜考虑受攻击后的恢复要求，包括保护所涉及应用服务的要求或确保所提供服务可用性的网络互连要求。

其他信息

通过公共网络访问的应用受到一系列的相关网络威胁，例如欺诈活动、合同争端或信息泄露给公众。因此，详细的风险评估和控制措施的正确选择是必不可少的。控制措施要求通常包括身份鉴别和数据安全传递的加密方法。

应用服务能利用安全鉴别方法（例如使用公开密钥系统和数字签名（见 10））以减少风险。另外，当需要这些服务时，可使用可信第三方。

### 14.1.3 保护应用服务交易

控制措施

宜保护涉及应用服务交易的信息，以防止不完整传送、错误路由、未授权消息变更、未授权泄露、未授权消息复制或重放。

实施指南

应用服务交易的信息安全考虑宜包括：

a) 交易中涉及的每一方的电子签名的使用；

b) 交易的所有方面，即确保：

1） 各方的用户秘密鉴别信息是有效的并经过验证的；

2） 交易是保密的；

3） 保留与涉及的各方相关的隐私；

c) 加密涉及的各方间的通信路径；

d) 在涉及的各方之间通信的协议是安全的；

e) 确保交易细节存储于任何公开可访问环境之外（例如，存储于组织内部互联网的存储平台），不留在或暴露于互联网可直接访问的存储介质上。

f) 当使用一个可信权威（例如为了颁布及维护数字签名和/或数字认证）时，安全可集成嵌入到整个端到端认证/签名管理过程中。

其他信息

采用控制措施的程度要对应于应用服务交易的每个形式相关的风险级别。

交易需要符合交易产生、处理、完成和/或存储的管辖区域的法律、法规要求。

## 14.2 Security in development and support processes

Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

### 14.2.1 Secure development policy

Control

Rules for the development of software and systems should be established and applied to developments within the organization.

Implementation guidance

Secure development is a requirement to build up a secure service, architecture, software and system. Within a secure development policy, the following aspects should be put under consideration:

a) security of the development environment;

b) guidance on the security in the software development lifecycle:

   1) security in the software development methodology;

   2) secure coding guidelines for each programming language used;

c) security requirements in the design phase;

d) security checkpoints within the project milestones;

e) secure repositories;

f) security in the version control;

g) required application security knowledge;

h) developers' capability of avoiding, finding and fixing vulnerabilities.

Secure programming techniques should be used both for new developments and in code re-use scenarios where the standards applied to development may not be known or were not consistent with current best practices. Secure coding standards should be considered and where relevant mandated for use. Developers should be trained in their use and testing and code review should verify their use.

If development is outsourced, the organization should obtain assurance that the external party complies with these rules for secure development (see 14.2.7).

Other information

Development may also take place inside applications, such as office applications, scripting, browsers and databases.

### 14.2.2 System change control procedures

Control

Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.

Implementation guidance

Formal change control procedures should be documented and enforced to ensure the integrity of system, applications and products, from the early design stages through all subsequent maintenance efforts.

## 14.2 开发和支持过程中的安全

| |
|---|
| 目标：宜确保进行信息安全设计，并确保其在信息系统开发生命周期中实施。 |

### 14.2.1 安全开发策略

控制措施

宜建立软件和系统开发规则，并应用于组织内的开发。

实施指南

安全开发是建立安全服务、安全架构、安全软件和系统的要求。基于一个安全开发策略，以下方面宜考虑：

a) 开发环境安全；

b) 软件开发生命周期中的安全指南；

1) 软件开发方法的安全；

2) 所使用每种程序语言的安全编码指南；

c) 设计阶段的安全要求；

d) 项目里程碑中的安全核查点；

e) 安全知识库；

f) 安全版本控制；

g) 所要求的应用安全知识；

h) 开发人员避免、发现和修复脆弱性的能力。

用于新开发和代码重用两种情况的安全编程技术，开发所应用的标准可能是未知的或者与当前最佳实践是不一致的。以考虑安全编码标准并且强制使用，宜对开发人员进行他们所使用、测试或代码评审的标准进行培训，并进行验证。

如果是外包开发，组织宜确保外部方遵从这些安全开发规则（见 14.2.7）。

其他信息

开发也可能发生在应用中，例如办公应用、脚本、浏览器和数据库等。

### 14.2.2 系统变更控制规程

控制措施

宜通过使用正式变更控制程序控制开发生命周期中的系统变更。

实施指南

宜将正式的变更控制规程文件化，并从早期设计阶段到所有后续的维护强制实施，以确

Introduction of new systems and major changes to existing systems should follow a formal process of documentation, specification, testing, quality control and managed implementation.

This process should include a risk assessment, analysis of the impacts of changes and specification of security controls needed. This process should also ensure that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work and that formal agreement and approval for any change is obtained.

Wherever practicable, application and operational change control procedures should be integrated (see 12.1.2). The change control procedures should include but not be limited to:

a) maintaining a record of agreed authorization levels;

b) ensuring changes are submitted by authorized users;

c) reviewing controls and integrity procedures to ensure that they will not be compromised by the changes;

d) identifying all software, information, database entities and hardware that require amendment;

e) identifying and checking security critical code to minimize the likelihood of known security weaknesses;

f) obtaining formal approval for detailed proposals before work commences;

g) ensuring authorized users accept changes prior to implementation;

h) ensuring that the system documentation set is updated on the completion of each change and that old documentation is archived or disposed of;

i) maintaining a version control for all software updates;

j) maintaining an audit trail of all change requests;

k) ensuring that operating documentation (see 12.1.1) and user procedures are changed as necessary to remain appropriate;

l) ensuring that the implementation of changes takes place at the right time and does not disturb the business processes involved.

Other information

Changing software can impact the operational environment and vice versa.

Good practice includes the testing of new software in an environment segregated from both the production and development environments (see 12.1.4). This provides a means of having control over new software and allowing additional protection of operational information that is used for testing purposes. This should include patches, service packs and other updates.

Where automatic updates are considered, the risk to the integrity and availability of the system should be weighed against the benefit of speedy deployment of updates. Automated updates should not be used on critical systems as some updates can cause critical applications to fail.

### 14.2.3 Technical review of applications after operating platform changes

Control

When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

Implementation guidance

保系统、应用和产品的完整性。引入新系统和对已有系统进行大的变更宜按照从文件、规范、测试、质量控制到实施管理这个正式的过程进行。

这个过程宜包括风险评估、变更影响分析和所需的安全控制措施规范。这一过程还宜确保不损害现有的安全和控制规程，确保支持程序员仅能访问系统中其工作那些必要的部分，确保任何变更要获得正式商定和批准。

只要可行，应用和运行变更控制规程宜集成起来（见 12.1.2）。该变更规程宜包括但不局限于：

a) 维护所商定授权级别的记录；

b) 确保由授权的用户提交变更；

c) 评审控制措施和完整性规程，以确保它们不因变更而损害；

d) 识别需要修正的所有软件、信息、数据库实体和硬件；

e) 识别和核查关键代码安全，以最小化出现已知安全弱点的可能性；

f) 在工作开始之前，获得对详细建议的正式批准；

g) 确保已授权的用户在实施之前接受变更；

h) 确保在每个变更完成之后更新系统文件设置，并将旧文件归档或丢弃；

i) 维护所有软件更新的版本控制；

j) 维护所有变更请求的审核踪迹；

k) 当必要时，确保对操作文件（见 12.1.1）和用户规程作合适的变更；

l) 确保变更的实施发生在正确的时刻，并且不干扰所涉及的业务过程。

其他信息

变更软件会影响运行环境，反之亦然。

良好的惯例包括在一个与生产与开发环境隔离（见 12.1.4）的环境中测试新软件。这提供对新软件进行控制和允许对被用于测试目的的运行信息给予附加保护的手段。这宜包括补丁、服务包和其他更新。

在考虑自动更新的情况，宜权衡系统的完整性及可用性风险与加速更新带来好处之间的关系。不宜在关键系统中使用自动更新，因为某些更新可能会导致关键应用程序的失败。

### 14.2.3 运行平台变更后应用的技术评审

控制措施

当运行平台发生变更时，宜对业务的关键应用进行评审和测试，以确保对组织的运行和安全没有负面影响。

实施指南

This process should cover:

a) review of application control and integrity procedures to ensure that they have not been compromised by the operating platform changes;

b) ensuring that notification of operating platform changes is provided in time to allow appropriate tests and reviews to take place before implementation;

c) ensuring that appropriate changes are made to the business continuity plans (see Clause 17).

Other information

Operating platforms include operating systems, databases and middleware platforms. The control should also be applied for changes of applications.

### 14.2.4 Restrictions on changes to software packages

Control

Modifications to software packages should be discouraged, limited to necessary changes and all changes should be strictly controlled.

Implementation guidance

As far as possible and practicable, vendor-supplied software packages should be used without modification. Where a software package needs to be modified the following points should be considered:

a) the risk of built-in controls and integrity processes being compromised;

b) whether the consent of the vendor should be obtained;

c) the possibility of obtaining the required changes from the vendor as standard program updates;

d) the impact if the organization becomes responsible for the future maintenance of the software as a result of changes;

e) compatibility with other software in use.

If changes are necessary the original software should be retained and the changes applied to a designated copy. A software update management process should be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software (see 12.6.1). All changes should be fully tested and documented, so that they can be reapplied, if necessary, to future software upgrades. If required, the modifications should be tested and validated by an independent evaluation body.

### 14.2.5 Secure system engineering principles

Control

Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.

Implementation guidance

Secure information system engineering procedures based on security engineering principles should be established, documented and applied to in-house information system engineering activities. Security should be designed into all architecture layers (business, data, applications and technology) balancing the need for information security with the need for accessibility. New technology should be analysed for security risks and the design should be reviewed against known attack patterns.

These principles and the established engineering procedures should be regularly reviewed to ensure that they are effectively contributing to enhanced standards of security within the engineering process. They

这一过程宜涵盖：

a) 评审应用控制和完整性规程，以确保它们不因操作系统变更而损害；

b) 确保及时提供运行平台变更的通知，以便于在实施之前进行合适的测试和评审；

c) 确保对业务连续性计划进行合适的变更（见第 17 章）。

其他信息

运行平台包括操作系统、数据库管理系统、中间件平台。控制措施也适用于应用的变更。

### 14.2.4 软件包变更的限制

控制措施

宜对软件包的修改进行劝阻，只限于必要的变更，且对所有的变更加以严格控制。

实施指南

如果可能且可行，宜使用厂商提供的软件包，而无需修改。在需要修改软件包时，宜考虑下列要点：

a) 内置控制措施和完整性过程被损害的风险；

b) 是否宜获得厂商的同意；

c) 当标准程序更新时，从厂商获得所需要变更的可能性；

d) 作为变更的结果，组织要负责进一步维护此软件的影响;

e) 在使用其他软件的兼容性。

如果变更是必要的，则原始软件宜保留，并将变更应用于已明显指定的拷贝。宜实施软件更新管理过程，以确保最新批准的补丁和应用更新已经安装在所有的授权软件中（见 12.6。1）。宜充分测试所有变更，并将其形成文件，若必要，可以使它们重新应用于进一步的软件升级。如果必要，所有的更新宜由独立的评估机构进行测试和确认。

### 14.2.5 安全系统工程原则

控制措施

宜建立、记录和维护安全系统工程原则，并应用到任何信息系统实施工作。

实施指南

基于安全工程原则的安全信息系统工程原则宜被建立、文件化、应用于内部信息系统工程活动。宜在所有结构层（业务、数据、应用和技术）进行安全设计，平衡所需辅助功能的信息安全要求。针对新技术，宜进行安全风险分析和方案评审，防止已知的安全攻击。

宜定期对上述原则和已建立的工程规程进行评审，以确保他们有效推动工程过程的增强安全标准。也确保他们能够保持与时俱进，能够对抗新的潜在的威胁以及适用于技术的发展

should also be regularly reviewed to ensure that they remain up-to-date in terms of combating any new potential threats and in remaining applicable to advances in the technologies and solutions being applied.

The established security engineering principles should be applied, where applicable, to outsourced information systems through the contracts and other binding agreements between the organization and the supplier to whom the organization outsources. The organization should confirm that the rigour of suppliers' security engineering principles is comparable with its own.

Other information

Application development procedures should apply secure engineering techniques in the development of applications that have input and output interfaces. Secure engineering techniques provide guidance on user authentication techniques, secure session control and data validation, sanitisation and elimination of debugging codes.

### 14.2.6 Secure development environment

Control

Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

Implementation guidance

A secure development environment includes people, processes and technology associated with system development and integration.

Organizations should assess risks associated with individual system development efforts and establish secure development environments for specific system development efforts, considering:

a) sensitivity of data to be processed, stored and transmitted by the system;

b) applicable external and internal requirements, e.g. from regulations or policies;

c) security controls already implemented by the organization that support system development;

d) trustworthiness of personnel working in the environment (see 7.1.1);

e) the degree of outsourcing associated with system development;

f) the need for segregation between different development environments;

g) control of access to the development environment;

h) monitoring of change to the environment and code stored therein;

i) backups are stored at secure offsite locations;

j) control over movement of data from and to the environment.

Once the level of protection is determined for a specific development environment, organizations should document corresponding processes in secure development procedures and provide these to all individuals who need them.

### 14.2.7 Outsourced development

Control

The organization should supervise and monitor the activity of outsourced system development.

Implementation guidance:

和所应用的方案。

若适用，安全工程原则宜应用于外包信息系统，该原则通过组织与组织外包供应商之间的合同及其他具有约束力的协议建立。组织宜确认供应商的安全工程原则严格程度与自身的相当。

其他信息

在有输入和输出界面的应用开发中，应用开发规程宜采用安全工程技术。安全工程技术提供了用户身份鉴别技术、安全会话控制措施、数据校验、调试代码的净化和清除等的指南。

### 14.2.6 安全开发环境

控制措施

组织宜建立并适当保护系统开发和集成工作的安全开发环境，覆盖整个系统开发生命周期。

实施指南

安全开发环境包括系统开发和集成相关的人、过程、技术。

组织宜针对每个系统的开发评估相关风险，并为特定系统开发建立安全开发环境，宜考虑：

a) 系统处理、存储和传输的敏感数据；
b) 适用的内部和外部要求，例如，来自规程或策略；
c) 组织总是实施支持系统开发的安全控制措施；
d) 员工工作在诚信的环境中；
e) 系统开发相关的外包程度；
f) 不同开发环境之间需要隔离；
g) 访问开发环境的控制措施；
h) 环境及其存储代码变更的监视；
i) 备份异地存储在安全位置；
j) 数据从一个环境转移到另一个环境的控制措施。

对于特定开发环境，一旦确定保护级别，组织宜在安全开发规程中记录相应的过程，并提供给需要的人。

### 14.2.7 外包开发

控制措施

组织宜管理和监视外包系统开发活动。

实施指南

Where system development is outsourced, the following points should be considered across the organization's entire external supply chain:

a) licensing arrangements, code ownership and intellectual property rights related to the outsourced content (see 18.1.2);

b) contractual requirements for secure design, coding and testing practices (see 14.2.1);

c) provision of the approved threat model to the external developer;

d) acceptance testing for the quality and accuracy of the deliverables;

e) provision of evidence that security thresholds were used to establish minimum acceptable levels of security and privacy quality;

f) provision of evidence that sufficient testing has been applied to guard against the absence of both intentional and unintentional malicious content upon delivery;

g) provision of evidence that sufficient testing has been applied to guard against the presence of known vulnerabilities;

h) escrow arrangements, e.g. if source code is no longer available;

i) contractual right to audit development processes and controls;

j) effective documentation of the build environment used to create deliverables;

k) the organization remains responsible for compliance with applicable laws and control efficiency verification.

Other information

Further information on supplier relationships can be found in ISO/IEC 27036.[21][22][23]

### 14.2.8 System security testing

Control

Testing of security functionality should be carried out during development.

Implementation guidance

New and updated systems require thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions. For in-house developments, such tests should initially be performed by the development team. Independent acceptance testing should then be undertaken (both for in-house and for outsourced developments) to ensure that the system works as expected and only as expected (see 14.1.1 and 14.1.9). The extent of testing should be in proportion to the importance and nature of the system.

### 14.2.9 System acceptance testing

Control

Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.

Implementation guidance

System acceptance testing should include testing of information security requirements (see 14.1.1 and 14.1.2) and adherence to secure system development practices (see 14.2.1). The testing should also be conducted on received components and integrated systems. Organizations can leverage automated tools,

在外包软件开发时，在组织的整个外部供应链中，宜考虑下列要点：

a） 有关外包内容的许可证安排、代码所有权和知识产权（见 18.1.2）；

b） 安全设计、编码和测试实践的合同要求（见 14.2.1）；

c） 为外部开发者提供被认可的威胁模型；

d） 交付物质量和准确性的验收测试；

e） 用于建立安全和隐私质量最小化可接受级别的安全阀值的证据的条款；

f） 已应用足够的测试来防止交付过程中有意或无意的恶意内容的证据的条款；

g） 已应用足够的测试来方针存在已知脆弱性的证据的条款；

h） 契约安排，例如，如果源代码不可用时；

i） 审核开发过程和控制措施的合同权利；

j） 用于创建可交付使用的建筑环境有效文档；

k） 组织保有遵从适用的法律和验证控制措施有效的职责。

其他信息

关于供应商关系的进一步信息参见 ISO/IEC27036。

### 14.2.8 系统安全测试

控制措施

在开发过程中，宜进行安全功能测试。

实施指南

新系统或更新的系统在开发过程中均需要全面的测试验证，包括准备详细的活动计划安排以及在一定条件下测试输入和期望的输出。作为内部开发，这样的测试首先宜由开发团队进行，然后进行独立的验收测试（包括内部开发和外包开发）以确保系统按预期希望工作（见 14.1.1 和 14.1.2）。测试的深度宜由系统的重要性和本质确定。

### 14.2.9 系统验收测试

控制措施

对于新建信息系统和新版本升级系统，宜建立验收测试方案和相关准则。

实施指南

系统验收测试宜包括信息安全要求测试（见 14.1.1 和 14.1.2）并遵循系统安全开发事件（见 14.2.1），宜进行单元测试和系统集成测试。组织可利用自动化工具，例如代码分析工

such as code analysis tools or vulnerability scanners, and should verify the remediation of security-related defects.

Testing should be performed in a realistic test environment to ensure that the system will not introduce vulnerabilities to the organization's environment and that the tests are reliable.

## 14.3 Test data

Objective: To ensure the protection of data used for testing.

### 14.3.1 Protection of test data

Control

Test data should be selected carefully, protected and controlled.

Implementation guidance

The use of operational data containing personally identifiable information or any other confidential information for testing purposes should be avoided. If personally identifiable information or otherwise confidential information is used for testing purposes, all sensitive details and content should be protected by removal or modification (see ISO/IEC 29101[26]).

The following guidelines should be applied to protect operational data, when used for testing purposes:

a) the access control procedures, which apply to operational application systems, should also apply to test application systems;

b) there should be separate authorization each time operational information is copied to a test environment;

c) operational information should be erased from a test environment immediately after the testing is complete;

d) the copying and use of operational information should be logged to provide an audit trail.

Other information

System and acceptance testing usually requires substantial volumes of test data that are as close as possible to operational data.

# 15 Supplier relationships

## 15.1 Information security in supplier relationships

Objective: To ensure protection of the organization's assets that is accessible by suppliers.

### 15.1.1 Information security policy for supplier relationships

Control

Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented.

Implementation guidance

The organization should identify and mandate information security controls to specifically address supplier access to the organization's information in a policy. These controls should address processes

作或脆弱性扫描器，同时宜验证安全相关缺陷的修复。

测试宜在现实测试环境中执行，以确保系统不会给组织环境引入脆弱性，并确保测试是可靠的。

### 14.3 测试数据

| 目标：确保保护测试数据。 |
| --- |

#### 14.3.1 系统测试数据的保护

控制措施

测试数据宜认真地加以选择、保护和控制。

实施指南

宜避免使用包含个人身份信息或其他机密信息的运行数据库用于测试。如果测试使用了个人身份信息或其他机密信息，那么在使用之前宜去除或修改所有的敏感细节和内容（见ISO/IEC29101）。

当用于测试时，宜使用下列指南保护运行数据：

a) 要用于运行应用系统的访问控制规程，还应用于测试应用系统；

b) 运行信息每次被拷贝到测试应用系统时要有独立的授权；

c) 在测试完成之后，要立即从测试应用系统清除运行信息；

d) 要记录运行信息的拷贝和使用日志以提供审核踪迹。

其他信息

系统和验收测试常常要求相当多的尽可能接近运行数据的测试数据。

## 15 供应商关系

### 15.1 供应商关系的信息安全

| 目标：确保保护可被供应商访问的组织资产。 |
| --- |

#### 15.1.1 供应商关系的信息安全策略

控制措施

为减缓供应商访问组织资产带来的风险，宜与供应商协商并记录相关信息安全要求。

实施指南

组织宜确定和授权特定说明的供应商，允许其访问组织策略中的信息安全控制措施信息。这些控制措施宜说明组织已实施的过程和规程，以及组织宜要求供应商实施这些过程和规程，包括：

and procedures to be implemented by the organization, as well as those processes and procedures that the organization should require the supplier to implement, including:

a) identifying and documenting the types of suppliers, e.g. IT services, logistics utilities, financial services, IT infrastructure components, whom the organization will allow to access its information;

b) a standardised process and lifecycle for managing supplier relationships;

c) defining the types of information access that different types of suppliers will be allowed, and monitoring and controlling the access;

d) minimum information security requirements for each type of information and type of access to serve as the basis for individual supplier agreements based on the organization's business needs and requirements and its risk profile;

e) processes and procedures for monitoring adherence to established information security requirements for each type of supplier and type of access, including third party review and product validation;

f) accuracy and completeness controls to ensure the integrity of the information or information processing provided by either party;

g) types of obligations applicable to suppliers to protect the organization's information;

h) handling incidents and contingencies associated with supplier access including responsibilities of both the organization and suppliers;

i) resilience and, if necessary, recovery and contingency arrangements to ensure the availability of the information or information processing provided by either party;

j) awareness training for the organization's personnel involved in acquisitions regarding applicable policies, processes and procedures;

k) awareness training for the organization's personnel interacting with supplier personnel regarding appropriate rules of engagement and behaviour based on the type of supplier and the level of supplier access to the organization's systems and information;

l) conditions under which information security requirements and controls will be documented in an agreement signed by both parties;

m) managing the necessary transitions of information, information processing facilities and anything else that needs to be moved, and ensuring that information security is maintained throughout the transition period.

Other information

Information can be put at risk by suppliers with inadequate information security management. Controls should be identified and applied to administer supplier access to information processing facilities. For example, if there is a special need for confidentiality of the information, non-disclosure agreements can be used. Another example is data protection risks when the supplier agreement involves transfer of, or access to, information across borders. The organization needs to be aware that the legal or contractual responsibility for protecting information remains with the organization.

### 15.1.2 Addressing security within supplier agreements

Control

All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

Implementation guidance

a) 确定和记录允许访问组织信息的供应商类型，例如 IT 服务、物流公用业、金融服务、IT 基础组件等；

b) 管理供应商关系的标准化过程和生命周期；

c) 定义允许不同类型供应商访问信息的类型，监视和控制访问；

d) 每种类型信息和访问的最小化安全要求作为单个供应商协议的基础，最小化信息安全要求基于组织的业务需求和要求及其风险轮廓确定；

e) 监视的过程和规程遵从为每种类型供应商及访问建立的信息安全要求，包括第三方评审和产品验证；

f) 准确性和完整性控制以确保信息或由任何一方所提供信息处理的完整性；

g) 为了保护组织信息，适用于供应商的业务类型；

h) 处理供应商访问相关的事件或突发事件，涉及组织和供应商的职责；

i) 如果必要，实施复原、恢复和应急计划确保信息或任何一方所提供信息处理的可用性；

j) 针对组织参与收购的人员开展意识培训，培训内容涉及收购相关的适当的策略、过程和规程；

k) 针对与供应商人员交互的组织人员开展意识培训，培训内容涉及基于供应商类型和供应商访问组织系统及信息级别的参与规则和行为；

l) 在一定条件下，将信息安全要求和控制措施记录在双方签订的协议中；

m) 管理信息、信息处理设施及其他还需删除的必要过渡，确保整个过渡期的信息安全。

其他信息

由于对供应商的信息安全管理不充分，可能使信息处于风险中。宜确定和应用控制措施，以管理供应商对信息处理设施的访问。例如，如果对信息的保密性有特殊的要求，就需要使用不泄漏协议。另一个例子是当供应商协议涉及信息跨国界传递或访问时的数据保护风险通。组织必要了解属于组织保护信息的法规和合同职责。

### 15.1.2 处理供应商协议中的安全问题

控制措施

宜与每个可能访问、处理、存储组织信息、与组织进行通信或为组织提供 IT 基础设施组件的供应商建立并协商所有相关的信息安全要求。

实施指南

Supplier agreements should be established and documented to ensure that there is no misunderstanding between the organization and the supplier regarding both parties' obligations to fulfil relevant information security requirements.

The following terms should be considered for inclusion in the agreements in order to satisfy the identified information security requirements:

a) description of the information to be provided or accessed and methods of providing or accessing the information;

b) classification of information according to the organization's classification scheme (see 8.2); if necessary also mapping between the organization's own classification scheme and the classification scheme of the supplier;

c) legal and regulatory requirements, including data protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met;

d) obligation of each contractual party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing;

e) rules of acceptable use of information, including unacceptable use if necessary;

f) either explicit list of supplier personnel authorized to access or receive the organization's information or procedures or conditions for authorization, and removal of the authorization, for access to or receipt of the organization's information by supplier personnel;

g) information security policies relevant to the specific contract;

h) incident management requirements and procedures (especially notification and collaboration during incident remediation);

i) training and awareness requirements for specific procedures and information security requirements, e.g. for incident response, authorization procedures;

j) relevant regulations for sub-contracting, including the controls that need to be implemented;

k) relevant agreement partners, including a contact person for information security issues;

l) screening requirements, if any, for supplier's personnel including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for doubt or concern;

m) right to audit the supplier processes and controls related to the agreement;

n) defect resolution and conflict resolution processes;

o) supplier's obligation to periodically deliver an independent report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report;

p) supplier's obligations to comply with the organization's security requirements.

Other information

The agreements can vary considerably for different organizations and among the different types of suppliers. Therefore, care should be taken to include all relevant information security risks and requirements. Supplier agreements may also involve other parties (e.g. sub-suppliers).

The procedures for continuing processing in the event that the supplier becomes unable to supply its products or services need to be considered in the agreement to avoid any delay in arranging replacement products or services.

宜建立供应商协议并文件化，以确保在组织和供应商之间关于双方要履行关于信息安全要求的相关义务不存在误解。

为满足识别的信息安全要求，宜考虑将下列条款包含在协议中：

a) 被提供和访问信息的描述以及提供和访问信息的方法；

b) 根据组织的分类方案进行信息分类（见 8.2），如果需要，则要将组织自身的分类方案和供应商的分类方案进行映射；

c) 包括数据保护、知识产权和版权的法律、法规要求，并描述如何确保这些要求得到满足；

d) 每个合同的合约方有义务执行一套已商定的控制措施，包括访问控制、性能评审、监视、报告和审核；

e) 信息可接受使用的规则，如果需要也包括不可接受的使用；

f) 授权访问或接收组织信息和规程的供应商人员列表及授权和撤销供应商人员访问或接收组织信息的条件；

g) 具体合同相关的信息安全策略；

h) 事件管理要求和规程（特别是事件修复期间的通告和合作）；

i) 具体规程和信息安全要求的培训和意识要求，例如事件响应、授权规程等；

j) 分包的相关规则，包括需要实施的控制措施；

k) 相关协议方，包括处理信息安全问题的联系人；

l) 如有，对供应商人员的审查要求，包括实施审查的职责、如果审查未完成或审查结果引起疑问或关注的通知规程；

m) 审核供应商协议相关过程和控制措施的权力；

n) 缺陷和冲突的解决过程；

o) 供应商有义务定期递交一份关于控制措施有效性的独立报告，并且同意及时纠正报告中提及的问题；

p) 供应商有义务遵从组织安全要求。

其他信息

协议会因不同的组织、供应商的不同类型发生很大变化。因此，宜注意要在协议中包括所有相关信息安全风险和要求。供应商协议也可涉及其他方（例如分包商）。

在协议中需要考虑当供应商不能提供其产品或服务时的连续处理规程，以避免在安排替代产品或服务时的任何延迟。

### 15.1.3 Information and communication technology supply chain

Control

Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain.

Implementation guidance

The following topics should be considered for inclusion in supplier agreements concerning supply chain security:

a) defining information security requirements to apply to information and communication technology product or service acquisition in addition to the general information security requirements for supplier relationships;

b) for information and communication technology services, requiring that suppliers propagate the organization's security requirements throughout the supply chain if suppliers subcontract for parts of information and communication technology service provided to the organization;

c) for information and communication technology products, requiring that suppliers propagate appropriate security practices throughout the supply chain if these products include components purchased from other suppliers;

d) implementing a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements;

e) implementing a process for identifying product or service components that are critical for maintaining functionality and therefore require increased attention and scrutiny when built outside of the organization especially if the top tier supplier outsources aspects of product or service components to other suppliers;

f) obtaining assurance that critical components and their origin can be traced throughout the supply chain;

g) obtaining assurance that the delivered information and communication technology products are functioning as expected without any unexpected or unwanted features;

h) defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers;

i) implementing specific processes for managing information and communication technology component lifecycle and availability and associated security risks. This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements.

Other information

The specific information and communication technology supply chain risk management practices are built on top of general information security, quality, project management and system engineering practices but do not replace them.

Organizations are advised to work with suppliers to understand the information and communication technology supply chain and any matters that have an important impact on the products and services being provided. Organizations can influence information and communication technology supply chain information security practices by making clear in agreements with their suppliers the matters that should be addressed by other suppliers in the information and communication technology supply chain.

Information and communication technology supply chain as addressed here includes cloud computing services.

### 15.1.3 信息和通信技术供应链

控制措施

供应商协议宜包括信息和通信技术服务以及产品供应链相关信息安全风险处理的要求。

实施指南

涉及供应链安全，宜考虑将下列事项包含在供应商协议中：

a) 除通用供应商关系信息安全要求之外，定义应用于信息和通信技术产品或服务获取的信息安全要求；

b) 对于信息和通信技术服务而言，如果供应商分包了部分提供给组织的信息和通信技术服务，则要求供应商在整个供应链中普及组织的安全要求；

c) 对于信息和通信技术产品而言，如果这些产品包括购自其他供应商的组件，则要求供应商在整个供应链中普及适当的安全实践；

d) 实施监视过程以及验证交付的信息和通信技术产品和服务符合规定安全要求的可接受的方法；

e) 为保持功能的关键产品或服务组件实施识别过程，当其在组织以外构建，特别是，如果顶层供应商将某些产品或服务组件外包给其他供应商时，这些产品或服务组件宜增加关注和审查度；

f) 获得在整个供应链中可跟踪关键组件及其来源的保障；

g) 获得已交付信息和通信技术产品按预期运行、无意外或不必要特性的保障；

h) 在组织和供应商之间，为供应链及其所有潜在问题和损害定义信息共享规则；

i) 为管理信息和通信技术组件的生命周期以及可用性和相关的安全风险实施专门的过程。这包括管理组件的下列风险：由于供应商不再经营导致组件不可用、由于技术进步导致供应商不再提供这些组件。

其他信息

专门的信息和通信技术供应链风险管理实践基于通用信息安全、质量、项目管理和系统工程实践之上，但不会代替他们。

建议组织与供应商一起理解信息和通信技术供应链以及对所提供的产品和服务有重要影响的所有事项。组织可通过在协议中与其供应商澄清宜由其他信息和通信技术供应链中的供应商处理的事项，来影响信息和通信技术供应链信息安全实践。

此处的信息和通信技术供应链包括云计算服务。

## 15.2 Supplier service delivery management

Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

### 15.2.1 Monitoring and review of supplier services

Control

Organizations should regularly monitor, review and audit supplier service delivery.

Implementation guidance

Monitoring and review of supplier services should ensure that the information security terms and conditions of the agreements are being adhered to and that information security incidents and problems are managed properly.

This should involve a service management relationship process between the organization and the supplier to:

a) monitor service performance levels to verify adherence to the agreements;

b) review service reports produced by the supplier and arrange regular progress meetings as required by the agreements;

c) conduct audits of suppliers, in conjunction with review of independent auditor's reports, if available, and follow-up on issues identified;

d) provide information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures;

e) review supplier audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;

f) resolve and manage any identified problems;

g) review information security aspects of the supplier's relationships with its own suppliers;

h) ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster (see Clause 17).

The responsibility for managing supplier relationships should be assigned to a designated individual or service management team. In addition, the organization should ensure that suppliers assign responsibilities for reviewing compliance and enforcing the requirements of the agreements. Sufficient technical skills and resources should be made available to monitor that the requirements of the agreement, in particular the information security requirements, are being met. Appropriate action should be taken when deficiencies in the service delivery are observed.

The organization should retain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by a supplier. The organization should retain visibility into security activities such as change management, identification of vulnerabilities and information security incident reporting and response through a defined reporting process.

### 15.2.2 Managing changes to supplier services

Control

## 15.2 供应商服务交付管理

| |
|---|
| 目标：保持符合供应商交付协议的信息安全和服务交付的商定水准。 |

### 15.2.1 供应商服务的监视和评审

控制措施

组织宜定期监视、评审和审核供应商服务交付。

实施指南

供应商服务的监视和评审宜确保坚持协议的信息安全条款和条件，并且信息安全事件和问题得到适当的管理。

这将涉及组织和供应商之间的服务管理关系过程，包括：

a) 监视服务执行级别以验证对协议的符合度；

b) 评审由供应商产生的服务报告，安排协议要求的定期进展会议；

c) 执行供应商审核和独立的审核员报告评审，如有，包括已识别问题的后续跟踪；

d) 当协议和所有支持性指南及规程需要时，提供关于信息安全事件的信息并实施评审；

e) 评审供应商的审核踪迹以及关于交付服务的信息安全事态、运行问题、失效、故障追踪和中断的记录；

f) 解决和管理所有已确定的问题；

g) 评审自身供应商关系的信息安全方面；

h) 确保供应商维护足够的服务能力以及可行的工作计划，该计划主要设计用来确保在遇到重大服务故障或灾难时（见 17）保持商定的服务连续性级别。

管理与供应商关系的职责宜分配给指定人员或服务管理组。另外，组织宜确保供应商分配了评审符合性和执行协议要求的职责。宜获得足够的技术技能和资源来监视满足协议的要求，特别是信息安全要求。当在服务交付中发现不足时，宜采取适当的措施。

组织宜对供应商访问、处理或管理的敏感或关键信息或信息处理设施的所有安全方面保持充分的、全面的控制和可见度。组织宜确保它们在安全活动中留有可见度，例如变更管理、脆弱性识别以及使用已定义报告过程的信息安全事件报告和响应。

### 15.2.2 供应商服务的变更管理

控制措施

Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

Implementation guidance

The following aspects should be taken into consideration:

a) changes to supplier agreements;

b) changes made by the organization to implement:

   1) enhancements to the current services offered;

   2) development of any new applications and systems;

   3) modifications or updates of the organization's policies and procedures;

   4) new or changed controls to resolve information security incidents and to improve security;.

c) changes in supplier services to implement:

   1) changes and enhancement to networks;

   2) use of new technologies;

   3) adoption of new products or newer versions/releases;

   4) new development tools and environments;

   5) changes to physical location of service facilities;

   6) change of suppliers;

   7) sub-contracting to another supplier.

# 16 Information security incident management

## 16.1 Management of information security incidents and improvements

| Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses. |
|---|

### 16.1.1 Responsibilities and procedures

Control

Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.

Implementation guidance

The following guidelines for management responsibilities and procedures with regard to information security incident management should be considered:

a) management responsibilities should be established to ensure that the following procedures are developed and communicated adequately within the organization:

   1) procedures for incident response planning and preparation;

   2) procedures for monitoring, detecting, analysing and reporting of information security events and incidents;

宜管理供应商服务提供的变更，包括保持和改进现有的信息安全策略、规程和控制措施，并考虑到业务信息、系统和涉及过程的关键程度及风险的再评估。

实施指南

宜考虑下列方面：

a) 供应商协议的变更；

b) 组织要实施的变更：

1） 对提供的现有服务的加强；

2） 所有新应用和系统的开发；

3） 组织策略和规程的更改或更新；

4） 解决信息安全事件和改进安全的新的或变更的控制措施。

c) 供应商服务实施的变更：

1） 对网络的变更和加强；

2） 新技术的使用；

3） 新产品或新版本的采用；

4） 新的开发工具和环境；

5） 服务设施物理位置的变更；

6） 供应商的变更；

7） 分包给另外的供应商。

## 16 信息安全事件管理

### 16.1 信息安全事件和改进的管理

| 目标：确保采用一致和有效的方法对信息安全事件进行管理，包括安全事件和弱点的传达。 |
| --- |

#### 16.1.1 职责和规程

控制措施

宜建立管理职责和规程，以确保快速、有效和有序地响应信息安全事件。

实施指南

信息安全事件管理的管理职责和规程宜考虑下列指南：

a） 宜建立管理职责确保以下规程在组织内充分开发和传达：

1） 事件响应计划和准备的规程；

2） 信息安全事件和事故监视、检测、分析和报告的规程；

3) procedures for logging incident management activities;

4) procedures for handling of forensic evidence;

5) procedures for assessment of and decision on information security events and assessment of information security weaknesses;

6) procedures for response including those for escalation, controlled recovery from an incident and communication to internal and external people or organizations;

b) procedures established should ensure that:

1) competent personnel handle the issues related to information security incidents within the organization;

2) a point of contact for security incidents' detection and reporting is implemented;

3) appropriate contacts with authorities, external interest groups or forums that handle the issues related to information security incidents are maintained;

c) reporting procedures should include:

1) preparing information security event reporting forms to support the reporting action and to help the person reporting to remember all necessary actions in case of an information security event;

2) the procedure to be undertaken in case of an information security event, e.g. noting all details immediately, such as type of non-compliance or breach, occurring malfunction, messages on the screen and immediately reporting to the point of contact and taking only coordinated actions;

3) reference to an established formal disciplinary process for dealing with employees who commit security breaches;

4) suitable feedback processes to ensure that those persons reporting information security events are notified of results after the issue has been dealt with and closed.

The objectives for information security incident management should be agreed with management, and it should be ensured that those responsible for information security incident management understand the organization's priorities for handling information security incidents.

Other information

Information security incidents might transcend organizational and national boundaries. To respond to such incidents there is an increasing need to coordinate response and share information about these incidents with external organizations as appropriate.

Detailed guidance on information security incident management is provided in ISO/IEC 27035.[20]

### 16.1.2 Reporting information security events

Control

Information security events should be reported through appropriate management channels as quickly as possible.

Implementation guidance

All employees and contractors should be made aware of their responsibility to report information security events as quickly as possible. They should also be aware of the procedure for reporting information security events and the point of contact to which the events should be reported.

Situations to be considered for information security event reporting include:

a) ineffective security control;

3） 记录事件管理活动的规程；

4） 法院依据的处理规程；

5） 已确定信息安全事件和信息安全弱点的评估规程；

b） 建立的规程宜确保：

1） 主管人员处理组织内信息安全事件的相关问题；

2） 建立安全事件检测和报告联络点；

3） 与处理信息安全事件相关问题的政府部门、外部利益团体或论坛等保护联系；

c） 报告规程宜包括：

1） 准备信息安全事态报告单，以支持报告行为和帮助报告人员记下信息安全事态中的所有必要的行为；

2） 信息安全事态发生后要采取的程序，即立即记录下所有的细节（如，不符合或违规的类型、出现的故障、屏幕上显示的消息、异常行为）；不要采取任何个人行动，但要立即向联系点报告并且只采取协调行动；

3） 引用一种已制定的正式纪律处理过程，来处理有安全违规行为的雇员；

4） 适当的反馈过程，以确保在信息安全事态处理完成后，能够将处理结果通知给事态报告人。

宜与管理者商定信息安全事件管理的目标，宜确保负责信息安全事件管理的人员理解组织处理信息安全事件的优先顺序。

其他信息

信息安全事件可能超越组织和国家的边界。为了响应这样的事件，适当时，与外部组织协同响应和共享这些事件的信息的需求日益递增。

### 16.1.2 报告信息安全事态

控制措施

信息安全事态宜尽可能快地通过适当的管理渠道进行报告。

实施指南

所有雇员和承包方人员都宜知道他们有责任尽可能快地报告任何信息安全事态。他们还宜知道报告信息安全事态的规程和联系点。

信息安全事态报告宜考虑的情况包括：

a） 安全控制措施失效；

b) breach of information integrity, confidentiality or availability expectations;

c) human errors;

d) non-compliances with policies or guidelines;

e) breaches of physical security arrangements;

f) uncontrolled system changes;

g) malfunctions of software or hardware;

h) access violations.

Other information

Malfunctions or other anomalous system behaviour may be an indicator of a security attack or actual security breach and should therefore always be reported as an information security event.

### 16.1.3 Reporting information security weaknesses

Control

Employees and contractors using the organization's information systems and services should be required to note and report any observed or suspected information security weaknesses in systems or services.

Implementation guidance

All employees and contractors should report these matters to the point of contact as quickly as possible in order to prevent information security incidents. The reporting mechanism should be as easy, accessible and available as possible.

Other information

Employees and contractors should be advised not to attempt to prove suspected security weaknesses. Testing weaknesses might be interpreted as a potential misuse of the system and could also cause damage to the information system or service and result in legal liability for the individual performing the testing.

### 16.1.4 Assessment of and decision on information security events

Control

Information security events should be assessed and it should be decided if they are to be classified as information security incidents.

Implementation guidance

The point of contact should assess each information security event using the agreed information security event and incident classification scale and decide whether the event should be classified as an information security incident. Classification and prioritization of incidents can help to identify the impact and extent of an incident.

In cases where the organization has an information security incident response team (ISIRT), the assessment and decision can be forwarded to the ISIRT for confirmation or reassessment.

Results of the assessment and decision should be recorded in detail for the purpose of future reference and verification.

### 16.1.5 Response to information security incidents

Control

b） 违反信息安全完整性、保密性和可用性期望；

c） 人员失误；

d） 不符合策略和指南；

e） 违反物理安全安排；

f） 未加控制的系统变更；

g） 软件或硬件故障；

h） 非法访问。

其他信息

故障或其他异常的系统行为可能是安全攻击和实际安全违规的显示，因此宜将其当作信息安全事态进行报告。

### 16.1.3 报告信息安全弱点

控制措施

宜要求使用组织信息系统和服务的所有雇员和承包方人员记录并报告他们观察到的或怀疑的任何系统或服务的安全弱点。

实施指南

为了预防信息安全事件，所有雇员和承包方人员宜尽可能快地将这些事情报告给他们的联络点。报告机制宜尽可能容易、可访问和可利用。

其他信息

宜建议雇员和承包方人员不要试图去证明被怀疑的安全弱点。测试弱点可能被看作是潜在的系统误用，还可能导致信息系统或服务的损害，并引起测试人员的法律责任。

### 16.1.4 评估和确定信息安全事态

控制措施

信息安全事态宜被评估，并且确定是否划分成信息安全事件。

实施指南

联络点宜利用被认可的信息安全事态和时间等级划分准则评估每一个信息安全事态，确定安全事态是否可以被划分为信息安全事件。事件的等级划分和特征有助于确定事件的影响和动机。

如果组织有信息安全事件响应小组（ISIRT），则信息安全事件响应小组可以提前评估和决策，以便于确认和再评估。

宜详细记录评估和决策的结果，以便将来参考和验证。

### 16.1.5 信息安全事件响应

控制措施

Information security incidents should be responded to in accordance with the documented procedures.

Implementation guidance

Information security incidents should be responded to by a nominated point of contact and other relevant persons of the organization or external parties (see 16.1.1).

The response should include the following:

a) collecting evidence as soon as possible after the occurrence;

b) conducting information security forensics analysis, as required (see 16.1.7);

c) escalation, as required;

d) ensuring that all involved response activities are properly logged for later analysis;

e) communicating the existence of the information security incident or any relevant details thereof to other internal and external people or organizations with a need-to-know;

f) dealing with information security weakness(es) found to cause or contribute to the incident;

g) once the incident has been successfully dealt with, formally closing and recording it.

Post-incident analysis should take place, as necessary, to identify the source of the incident.

Other information

The first goal of incident response is to resume 'normal security level' and then initiate the necessary recovery.

### 16.1.6 Learning from information security incidents

Control

Knowledge gained from analysing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.

Implementation guidance

There should be mechanisms in place to enable the types, volumes and costs of information security incidents to be quantified and monitored. The information gained from the evaluation of information security incidents should be used to identify recurring or high impact incidents.

Other information

The evaluation of information security incidents may indicate the need for enhanced or additional controls to limit the frequency, damage and cost of future occurrences, or to be taken into account in the security policy review process (see 5.1.2).

With due care of confidentiality aspects, anecdotes from actual information security incidents can be used in user awareness training (see 7.2.2) as examples of what could happen, how to respond to such incidents and how to avoid them in the future.

### 16.1.7 Collection of evidence

Control

The organization should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

Implementation guidance

宜具有与信息安全事件响应相一致的文件化规程。

实施指南

信息安全事件宜被指定的联络点及其他组织或外部团体的相关人员响应（见 16.1.1）。

响应应包括以下内容：

a) 尽可能地收集发生后的证据；

b) 若要求，开展信息安全法律证据分析（见 16.1.7）；

c) 若要求，上报；

d) 为了后期分析，确保所有的响应活动为正式记录；

e) 将存在的信息安全事件或任何相关的细节传达给其他内部和外部人员或者需要知道的组织；

f) 处理导致信息安全事件起因或有助于其发生的信息安全弱点；

g) 一旦时间成功处置，正式关闭并记录安全事件。

若必要，宜进行事后事件分析，以确定事件的起因。

其他信息

事件响应的首要目标是恢复到“正常安全水平”，然后启动必要的纠正措施。

### 16.1.6 对信息安全事件的总结

控制措施

获取信息安全事件分析和解决的知识宜被用户降低将来事件发生的可能性或影响。

实施指南

宜有一套机制量化和监视信息安全事件的类型、数量和代价。从信息安全事件评价中获取的信息宜用来识别再发生的事件或高影响的事件。

其他信息

对信息安全事件的评价可以指出需要增强的或另外的控制措施，以限制事件未来发生的频率、损害和费用，或者可以用在安全方针评审过程中（见 5.1.2）。

不过不涉及保密方面的问题，宜将真实的信息安全事件的场景作为可能发生信息安全事件的案例用于用户安全意识培训，包括如何对类似事件响应或避免类似安全事件将来发生。

### 16.1.7 证据的收集

控制措施

组织宜定义和应用识别、收集、获取和保存信息的程序，这些信息可以作为证据。

实施指南

Internal procedures should be developed and followed when dealing with evidence for the purposes of disciplinary and legal action.

In general, these procedures for evidence should provide processes of identification, collection, acquisition and preservation of evidence in accordance with different types of media, devices and status of devices, e.g. powered on or off. The procedures should take account of:

a) chain of custody;

b) safety of evidence;

c) safety of personnel;

d) roles and responsibilities of personnel involved;

e) competency of personnel;

f) documentation;

g) briefing.

Where available, certification or other relevant means of qualification of personnel and tools should be sought, so as to strengthen the value of the preserved evidence.

Forensic evidence may transcend organizational or jurisdictional boundaries. In such cases, it should be ensured that the organization is entitled to collect the required information as forensic evidence. The requirements of different jurisdictions should also be considered to maximize chances of admission across the relevant jurisdictions.

Other information

Identification is the process involving the search for, recognition and documentation of potential evidence. Collection is the process of gathering the physical items that can contain potential evidence. Acquisition is the process of creating a copy of data within a defined set. Preservation is the process to maintain and safeguard the integrity and original condition of the potential evidence.

When an information security event is first detected, it may not be obvious whether or not the event will result in court action. Therefore, the danger exists that necessary evidence is destroyed intentionally or accidentally before the seriousness of the incident is realized. It is advisable to involve a lawyer or the police early in any contemplated legal action and take advice on the evidence required.

ISO/IEC 27037[24] provides guidelines for identification, collection, acquisition and preservation of digital evidence.

# 17 Information security aspects of business continuity management

## 17.1 Information security continuity

| |
|---|
| Objective: Information security continuity should be embedded in the organization's business continuity management systems. |

### 17.1.1 Planning information security continuity

Control

The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

Implementation guidance

当为了进行纪律和法律相关的证据，宜制定和遵循内部规程。

总的来说，关于证据的规则宜提供识别、收集、获取、保存证据的过程，并且涉及不同类型的介质、设备和设备状态，例如开机或关机。这些过程宜考虑包括：

a） 监管链；

b） 证据的安全性；

c） 人员的安全性；

d） 涉及人员的角色和职责；

e） 人员的能力；

f） 记录；

g） 概要。

为了加强保存证据的价值，宜寻求可获得的人员和工具的资质证书或其他相关的资质证明。

证据可以超越组织和/或管辖区域的边界。在这样的情况下，宜确保组织有资格去收集要求的信息作证据。还宜考虑不同管辖区域的要求，以使证据跨越相关管辖区域被允许进入的机会最大化。

其他信息

识别是收集潜在证据文件和记录的过程。收集是获取可能包括潜在证据的物理事项的过程。采集是创建一个定义数据集副本的过程。保护是保持和维护潜在证据完整性和原始状态的过程。

当一个信息安全事态首次被检测到时，这个事态是否会导致法庭起诉可能不是显而易见的。因此，在认识到事件的严重性之前，存在必要的证据被故意或意外毁坏的危险。可取的做法是在任何预期的法律行为中及早聘请一位律师或警察，以获取所需证据的建议。

ISO/IEC 27037 为数字证据的识别、收集、获取和保存提供指南。

## 17 业务连续性管理的信息安全方面

### 17.1 信息安全连续性

| |
|---|
| 目标：组织的业务连续性管理体系中宜体现信息安全连续性。 |

#### 17.1.1 信息安全的连续性计划

控制措施

组织宜确定不利情况下（例如，一个危机或危难时）信息安全的要求和信息安全管理连续性。

实施指南

An organization should determine whether the continuity of information security is captured within the business continuity management process or within the disaster recovery management process. Information security requirements should be determined when planning for business continuity and disaster recovery.

In the absence of formal business continuity and disaster recovery planning, information security management should assume that information security requirements remain the same in adverse situations, compared to normal operational conditions. Alternatively, an organization could perform a business impact analysis for information security aspects to determine the information security requirements applicable to adverse situations.

Other information

In order to reduce the time and effort of an 'additional' business impact analysis for information security, it is recommended to capture information security aspects within the normal business continuity management or disaster recovery management business impact analysis. This implies that the information security continuity requirements are explicitly formulated in the business continuity management or disaster recovery management processes.

Information on business continuity management can be found in ISO/IEC 27031,[14] ISO 22313[9] and ISO 22301.[8]

### 17.1.2 Implementing information security continuity

Control

The organization should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

Implementation guidance

An organization should ensure that:

a) an adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience and competence;

b) incident response personnel with the necessary responsibility, authority and competence to manage an incident and maintain information security are nominated;

c) documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event and will maintain its information security to a predetermined level, based on management-approved information security continuity objectives (see 17.1.1).

According to the information security continuity requirements, the organization should establish, document, implement and maintain:

a) information security controls within business continuity or disaster recovery processes, procedures and supporting systems and tools;

b) processes, procedures and implementation changes to maintain existing information security controls during an adverse situation;

c) compensating controls for information security controls that cannot be maintained during an adverse situation.

Other information

Within the context of business continuity or disaster recovery, specific processes and procedures may have been defined. Information that is handled within these processes and procedures or within dedicated information systems to support them should be protected. Therefore an organization should

组织宜确定是否将信息安全连续性归为业务连续性管理过程或灾难恢复管理过程。当规划业务连续性和灾难恢复的时候，宜确定信息安全要求。

缺少正式的业务连续性计划和灾难恢复计划时，信息安全管理宜假定在不利条件下的信息安全要求与正常运行情况下相同。可替代的，组织可开展信息安全方面的一万五影响分析，以确定适用于不利条件的信息安全要求。

其他信息

为了减少对信息安全进行“附件”业务影响分析的时间和工作，建议将信息安全方面的业务影响分析捕获到正常的业务连续性管理和灾难恢复管理的业务影响分析中。表明宜在业务连续性管理或灾难恢复管理过程中明确制定信息安全连续性要求。

ISO/IEC 27031、 ISO/IEC 22313 和 ISO/IEC 22301 中均涉及业务连续性管理的相关信息。

### 17.1.2 实施信息安全连续性计划

控制措施

组织宜建立、文件化、实施和维护过程、规程和控制措施，确保在负面情况下要求的信息安全连续性级别。

实施指南

一个组织宜确保：

a）适当准备一个胜任的管理结构，使用具有必要权限、经验和能力的人员减轻或响应破坏性事态；

b）提名具有必要的职责、权限和能力的事件响应人员来处理事件、维护信息安全；

c）开发文件化的计划及响应和恢复规程，并获得批准。其详细说明组织如何基于已批准的信息安全连续性管理目标，处理破坏性事态并维护信息安全到预期的水平（见 17.1.1）。

根据信息安全连续性要求，组织宜建立、记录、实施和维护：

a）业务连续性或灾难恢复过程、规程、支持性系统和工具中的信息安全控制措施；

b）通过过程、规程和实施变更来维护不利条件下的现有信息安全控制措施；

c）对于在不利条件下不能维护的信息安全控制措施予以补偿。

其他信息

业务范围内的业务连续性和灾难恢复，具体的过程和规程可能已定义。宜保护这些过程和规程内处理的信息或支持他们所指定的信息系统。因此，组织宜邀请信息安全专家参与

involve information security specialists when establishing, implementing and maintaining business continuity or disaster recovery processes and procedures.

Information security controls that have been implemented should continue to operate during an adverse situation. If security controls are not able to continue to secure information, other controls should be established, implemented and maintained to maintain an acceptable level of information security.

### 17.1.3 Verify, review and evaluate information security continuity

Control

The organization should verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

"Implementation guidance"

Organizational, technical, procedural and process changes, whether in an operational or continuity context, can lead to changes in information security continuity requirements. In such cases, the continuity of processes, procedures and controls for information security should be reviewed against these changed requirements.

Organizations should verify their information security management continuity by:

a) exercising and testing the functionality of information security continuity processes, procedures and controls to ensure that they are consistent with the information security continuity objectives;

b) exercising and testing the knowledge and routine to operate information security continuity processes, procedures and controls to ensure that their performance is consistent with the information security continuity objectives;

c) reviewing the validity and effectiveness of information security continuity measures when information systems, information security processes, procedures and controls or business continuity management/disaster recovery management processes and solutions change.

Other information

The verification of information security continuity controls is different from general information security testing and verification and should be performed outside the testing of changes. If possible, it is preferable to integrate verification of information security continuity controls with the organization's business continuity or disaster recovery tests.

## 17.2 Redundancies

Objective: To ensure availability of information processing facilities.

### 17.2.1 Availability of information processing facilities

Control

Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

Implementation guidance

Organizations should identify business requirements for the availability of information systems. Where the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures should be considered.

Where applicable, redundant information systems should be tested to ensure the failover from one component to another component works as intended.

业务连续性或灾难恢复过程和程序的建立、实施和维护中。

在不利条件下，已实施的信息安全控制措施宜继续运行。如果安全控制措施不能继续保证信息安全，宜建立、实施和维护其他控制措施以保证达到到可接受的信息安全级别。

### 17.1.3 验证、评审和评价信息安全连续性计划

控制措施

组织宜定期验证已制定和实施信息安全业务连续性计划的控制措施，以确保在负面情况下控制措施的及时性和有效性。

实施指南

无论从运行还是连续性角度，组织、技术、规程和过程的变更均会导致信息安全连续性要求变更。在这种情况下，宜对这些已变更的要求进行评审，评审信息安全过程、规程和控制措施的连续性。

组织宜验证信息安全管理连续性，通过如下方面：

a) 演练和测试信息安全连续性过程、规程和控制措施的功能，确保与信息安全连续性目标一致；

b) 演练和测试信息安全连续性过程、规程及控制措施的知识和惯例，确保其与信息安全连续性管理目标一致；

c) 当信息系统、信息安全过程、规程及控制措施或业务连续性管理/灾难恢复管理过程及解决方案变更时，评审信息安全连续性措施的有效性和可用性。

## 17.2 冗余

目标：确保信息处理设施的有效性。

### 17.2.1 信息处理设施的可用性

控制措施

信息处理设备宜冗余部署，以满足高可用性需求。

实施指南

组织宜识别信息系统可用性的业务需求，如果现有系统框架不能保证可用性，宜考虑冗余组件或架构。

在适当的情况下，宜对冗余信息系统进行测试，以确保在故障发生时可以从一个组件顺利切换到另外一个组件。

Other information

The implementation of redundancies can introduce risks to the integrity or confidentiality of information and information systems, which need to be considered when designing information systems.

# 18 Compliance

## 18.1 Compliance with legal and contractual requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

### 18.1.1 Identification of applicable legislation and contractual requirements

Control

All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system and the organization.

Implementation guidance

The specific controls and individual responsibilities to meet these requirements should also be defined and documented.

Managers should identify all legislation applicable to their organization in order to meet the requirements for their type of business. If the organization conducts business in other countries, managers should consider compliance in all relevant countries.

### 18.1.2 Intellectual property rights

Control

Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

Implementation guidance

The following guidelines should be considered to protect any material that may be considered intellectual property:

a) publishing an intellectual property rights compliance policy which defines the legal use of software and information products;

b) acquiring software only through known and reputable sources, to ensure that copyright is not violated;

c) maintaining awareness of policies to protect intellectual property rights and giving notice of the intent to take disciplinary action against personnel breaching them;

d) maintaining appropriate asset registers and identifying all assets with requirements to protect intellectual property rights;

e) maintaining proof and evidence of ownership of licences, master disks, manuals, etc.;

f) implementing controls to ensure that any maximum number of users permitted within the licence is not exceeded;

g) carrying out reviews that only authorized software and licensed products are installed;

h) providing a policy for maintaining appropriate licence conditions;

其他信息

当设计信息系统的时候宜考虑，冗余部署可能引入的信息和信息系统完整性或保密性的风险。

## 18 符合性

### 18.1 符合法律和合同要求

| |
|---|
| 目标：避免违反任何法律、法令、法规或合同义务以及任何安全要求。 |

#### 18.1.1 可用法律及合同要求的识别

控制措施

对每一个信息系统和组织而言，所有相关的法律依据、法规和合同要求，以及为满足这些要求组织所采用的方法，宜加以明确地定义、形成文件并保持更新。

实施指南

为满足这些要求的特定控制措施和人员的职责宜加以定义并形成文件。

为了满足自身业务类型的要求，管理者应该明确所有的适用于组织立法。如果组织在其他国家开展业务，管理者应该考虑遵从所有相关国家的法律。

#### 18.1.2 知识产权（IPR）

控制措施

宜实施适当的规程，以确 保相关的知识产权和所有权的软件产品的使用，符合法律、法规和合同的要求。

实施指南

在保护被认为具有知识产权的材料时，宜考虑下列指南：

a) 发布一个知识产权符合性策略，该策略定义了软件和信息产品的合法使用；

b) 仅通过知名的和声誉好的渠道获得软件，以确保不侵犯版权；

c) 保持对保护知识产权的策略的了解，并通知对违规人员采取惩罚措施的意向；

d) 维护适当的资产登记簿，识别具有保护知识产权要求的所有资产；

e) 维护许可证、主盘、手册等所有权的证明和证据；

f) 实施控制措施，以确保不超过许可证所允许的最大用户数目；

g) 进行核查，确保仅安装已授权的软件和具有许可证的产品；

h) 提供维护适当的许可证条件的策略；

i) providing a policy for disposing of or transferring software to others;

j) complying with terms and conditions for software and information obtained from public networks;

k) not duplicating, converting to another format or extracting from commercial recordings (film, audio) other than permitted by copyright law;

l) not copying in full or in part, books, articles, reports or other documents, other than permitted by copyright law.

Other information

Intellectual property rights include software or document copyright, design rights, trademarks, patents and source code licences.

Proprietary software products are usually supplied under a licence agreement that specifies licence terms and conditions, for example, limiting the use of the products to specified machines or limiting copying to the creation of backup copies only. The importance and awareness of intellectual property rights should be communicated to staff for software developed by the organization.

Legislative, regulatory and contractual requirements may place restrictions on the copying of proprietary material. In particular, they may require that only material that is developed by the organization or that is licensed or provided by the developer to the organization, can be used. Copyright infringement can lead to legal action, which may involve fines and criminal proceedings.

### 18.1.3 Protection of records

Control

Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.

Implementation guidance

When deciding upon protection of specific organizational records, their corresponding classification based on the organization's classification scheme, should be considered. Records should be categorised into record types, e.g. accounting records, database records, transaction logs, audit logs and operational procedures, each with details of retention periods and type of allowable storage media, e.g. paper, microfiche, magnetic, optical. Any related cryptographic keys and programs associated with encrypted archives or digital signatures (see Clause 10), should also be stored to enable decryption of the records for the length of time the records are retained.

Consideration should be given to the possibility of deterioration of media used for storage of records. Storage and handling procedures should be implemented in accordance with manufacturer's recommendations.

Where electronic storage media are chosen, procedures to ensure the ability to access data (both media and format readability) throughout the retention period should be established to safeguard against loss due to future technology change.

Data storage systems should be chosen such that required data can be retrieved in an acceptable timeframe and format, depending on the requirements to be fulfilled.

The system of storage and handling should ensure identification of records and of their retention period as defined by national or regional legislation or regulations, if applicable. This system should permit appropriate destruction of records after that period if they are not needed by the organization.

To meet these record safeguarding objectives, the following steps should be taken within an organization:

a) guidelines should be issued on the retention, storage, handling and disposal of records and information;

i) 提供处理软件或转移软件给其他人的策略；

j) 符合从公共网络获得软件和信息的条款和条件；

k) 不对版权法不允许的商业录音带（胶片、音频）进行复制、格式转换或摘取内容；

l) 不对版权法不允许的书籍、文章、报告或其他文件中进行全部或部分地拷贝。

其他信息

知识产权包括软件或文件的版权、设计权、商标、专利权和源代码许可证。

通常具有所有权的软件产品的供应是根据许可协议进行的，该许可协议规定了许可条款和条件，例如，限制产品用于指定的机器或限制只能拷贝到创建的备份副本上。组织所开发的软件的知识产权意识和重要性宜向员工传达。

法律、法规和合同的要求可以对具有所有权的材料的拷贝进行限制。特别是，这些限制可能要求只能使用组织自己开发的资料，或者开发者许可组织使用或提供给组织的资料。版权侵害可能导致法律行为，这可能涉及罚款和刑事诉讼。

### 18.1.3 保护记录

控制措施

宜防止记录的遗失、毁坏、伪造、非授权访问和非授权删除，以满足法令、法规、合同和业务的要求。

实施指南

当确定保护组织的特定记录时，宜考虑基于组织的分类方法进行相应的分类。宜将记录分为记录类型，例如，帐号记录、数据库记录、事务日志、审计日志等，和运行规程，每个记录都带有详细的保存周期和可存储介质的类型，例如，纸质、缩微胶片、磁介质、光介质。还宜保存与已加密的归档文件或数字签名（见 10）相关的任何有关密钥材料，以使得记录在保存期内能够解密。

宜考虑存储记录的介质性能下降的可能性。宜按照制造商的建议实施存储和处理程规程。对于长期保存，宜考虑使用纸文件和微缩胶片。

若选择了电子存储介质，宜建立规程，以确保在整个保存周期内能够访问数据（介质和格式的可读性），以防护由于未来技术变化而造成的损失。

宜选择数据存储系统，使得所需要的数据能根据要满足的要求，在可接受的时间内、以可接受的格式检索出来。

存储和处理系统宜确保能按照国家或地区法律或法规的规定，清晰地标识出记录及其保存期限。该系统宜允许在保存期后恰当地销毁记录，如果组织不再需要这些记录的话。

为满足这些记录防护目标，宜在组织范围内采取下列步骤：

a) 要颁发关于保存、存储、处理和处置记录和信息的指南；

b) a retention schedule should be drawn up identifying records and the period of time for which they should be retained;

c) an inventory of sources of key information should be maintained.

Other information

Some records may need to be securely retained to meet statutory, regulatory or contractual requirements, as well as to support essential business activities. Examples include records that may be required as evidence that an organization operates within statutory or regulatory rules, to ensure defence against potential civil or criminal action or to confirm the financial status of an organization to shareholders, external parties and auditors. National law or regulation may set the time period and data content for information retention.

Further information about managing organizational records can be found in ISO 15489-1.[5]

### 18.1.4 Privacy and protection of personally identifiable information

Control

Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable.

Implementation guidance

An organization's data policy for privacy and protection of personally identifiable information should be developed and implemented. This policy should be communicated to all persons involved in the processing of personally identifiable information.

Compliance with this policy and all relevant legislation and regulations concerning the protection of the privacy of people and the protection of personally identifiable information requires appropriate management structure and control. Often this is best achieved by the appointment of a person responsible, such as a privacy officer, who should provide guidance to managers, users and service providers on their individual responsibilities and the specific procedures that should be followed. Responsibility for handling personally identifiable information and ensuring awareness of the privacy principles should be dealt with in accordance with relevant legislation and regulations. Appropriate technical and organizational measures to protect personally identifiable information should be implemented.

Other information

ISO/IEC 29100[25] provides a high-level framework for the protection of personally identifiable information within information and communication technology systems. A number of countries have introduced legislation placing controls on the collection, processing and transmission of personally identifiable information (generally information on living individuals who can be identified from that information). Depending on the respective national legislation, such controls may impose duties on those collecting, processing and disseminating personally identifiable information, and may also restrict the ability to transfer personally identifiable information to other countries.

### 18.1.5 Regulation of cryptographic controls

Control

Cryptographic controls should be used in compliance with all relevant agreements, legislation and regulations.

Implementation guidance

The following items should be considered for compliance with the relevant agreements, laws and regulations:

a) restrictions on import or export of computer hardware and software for performing cryptographic functions;

b) 要起草一个保存时间计划，以标识记录及其要被保存的时间周期；

c) 要维护关键信息源的清单。

其他信息

某些记录可能需要安全地保存，以满足法令、法规或合同的要求，以及支持必要的业务活动。举例来说，可以要求这些记录作为组织在法令或法规规则下运行的证据，以确保充分防御潜在的民事或刑事诉讼，股份持有者、外部方和审核员确认组织的财务状况。可以根据国家法律或规章来设置信息保存的时间和数据内容。

关于管理组织记录的更多信息可以参见 ISO 15489-1。

### 18.1.4 隐私和个人身份信息保护

控制措施

隐私和个人身份信息保护宜确保符合相关法律、法规的要求。

实施指南

宜制定和实施组织的隐私和个人身份信息保护策略策略。该策略宜通知到涉及个人身份信息处理的所有人员。

符合该策略和人们对隐私权及个人身份信息保护保护所相关的法律法规需要合适的管理结构和控制措施。通常，这一点最好通过任命一个负责人来实现，如隐私官，该隐私官宜向管理人员、用户和服务提供商提供他们各自的职责以及宜遵守的特定规程的指南。处理个人身份信息和确保了解隐私保护原则的职责宜根据相关法律法规来确定。宜实施适当的技术和组织措施以保护个人身份信息。

其他信息

ISO/IEC29100 提出了一个在信息和通信系统中保护个人身份信息的一个高层次的框架。许多国家已经具有控制个人身份信息（一般是指可以从该信息确定生命个体的信息）收集、处理和传输的法律。根据不同的国家法律，这种控制措施可以使那些收集、处理和传播个人身份信息的人承担责任，而且可以限制将该信息转移到其他国家的能力。

### 18.1.5 密码控制措施的规则

控制措施

使用密码控制措施宜遵从相关的协议、法律和法规。

实施指南

为符合相关的协议、法律和法规，宜考虑下面的事项：

a) 限制执行密码功能的计算机硬件和软件的入口和/或出口；

b) restrictions on import or export of computer hardware and software which is designed to have cryptographic functions added to it;

c) restrictions on the usage of encryption;

d) mandatory or discretionary methods of access by the countries' authorities to information encrypted by hardware or software to provide confidentiality of content.

Legal advice should be sought to ensure compliance with relevant legislation and regulations. Before encrypted information or cryptographic controls are moved across jurisdictional borders, legal advice should also be taken.

## 18.2 Information security reviews

| Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures. |
|---|

### 18.2.1 Independent review of information security

Control

The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur.

Implementation guidance

Management should initiate the independent review. Such an independent review is necessary to ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security. The review should include assessing opportunities for improvement and the need for changes to the approach to security, including the policy and control objectives.

Such a review should be carried out by individuals independent of the area under review, e.g. the internal audit function, an independent manager or an external party organization specializing in such reviews. Individuals carrying out these reviews should have the appropriate skills and experience.

The results of the independent review should be recorded and reported to the management who initiated the review. These records should be maintained.

If the independent review identifies that the organization's approach and implementation to managing information security is inadequate, e.g. documented objectives and requirements are not met or not compliant with the direction for information security stated in the information security policies (see 5.1.1), management should consider corrective actions.

Other information

ISO/IEC 27007[12], "Guidelines for information security management systems auditing" and ISO/IEC TR 27008[13], "Guidelines for auditors on information security controls" also provide guidance for carrying out the independent review.

### 18.2.2 Compliance with security policies and standards

Control

Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

Implementation guidance

b) 限制被设计用以增加密码功能的计算机硬件和软件的入口和/或出口；

c) 限制密码的使用；

d) 利用国家对硬件或软件加密的信息的授权的强制或任意的访问方法提供内容的保密性。

宜征求法律建议，以确保符合国家法律法规。在将加密信息或密码控制措施转移到所辖区域外之前，也宜获得法律建议。

### 18.2 信息安全评审

| 目标：确保信息安全实施及运行符合组织策略和程序。 |
| --- |

#### 18.2.1 独立的信息安全评审

控制措施

宜定期或发生较大变更时对组织的信息安全处置和实施方法（即控制目标、控制、策略、过程和信息安全程序）进行评审。

实施指南

管理人员宜开展独立评审，独立评审对于保证组织信息安全处理方法的持续性、适宜性、充分性和有效性是必要的。评审宜包括评价持续改进的可能性和变更安全方式的需求，包括策略和控制目标。

该评审宜由独立于所评审领域范围内的人员开展，如内部审核部门、独立的管理者或者专业的外部评审机构。从事评审活动的人员应具有一定的技能和经验。

独立评审的结果宜记录并报告给发起评审的管理者。评审记录宜保留。

如果独立评审确定组织处理信息安全的方法和实施是不充分的，例如文件化的目标和要求未实现或与信息安全政策规定的信息安全方向不一致（见 5.1.1），管理者宜考虑采取纠正措施。

其他信息

ISO/IEC27007“信息安全管理体系审核指南”和 ISO/IEC TR 27008“信息安全指南控制措施审核员指南”，也对开展独立评审提供了指导。

#### 18.2.2 符合安全策略和标准

控制措施

管理者宜定期对所辖职责范围内的信息安全过程和规程评审，以确保符合相应的安全政策、标准及其他安全要求。

实施指南

Managers should identify how to review that information security requirements defined in policies, standards and other applicable regulations are met. Automatic measurement and reporting tools should be considered for efficient regular review.

If any non-compliance is found as a result of the review, managers should:

a) identify the causes of the non-compliance;

b) evaluate the need for actions to achieve compliance;

c) implement appropriate corrective action;

d) review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses.

Results of reviews and corrective actions carried out by managers should be recorded and these records should be maintained. Managers should report the results to the persons carrying out independent reviews (see 18.2.1) when an independent review takes place in the area of their responsibility.

Other information

Operational monitoring of system use is covered in 12.4.

### 18.2.3 Technical compliance review

Control

Information systems should be regularly reviewed for compliance with the organization's information security policies and standards.

Implementation guidance

Technical compliance should be reviewed preferably with the assistance of automated tools, which generate technical reports for subsequent interpretation by a technical specialist. Alternatively, manual reviews (supported by appropriate software tools, if necessary) by an experienced system engineer could be performed.

If penetration tests or vulnerability assessments are used, caution should be exercised as such activities could lead to a compromise of the security of the system. Such tests should be planned, documented and repeatable.

Any technical compliance review should only be carried out by competent, authorized persons or under the supervision of such persons.

Other information

Technical compliance reviews involve the examination of operational systems to ensure that hardware and software controls have been correctly implemented. This type of compliance review requires specialist technical expertise.

Compliance reviews also cover, for example, penetration testing and vulnerability assessments, which might be carried out by independent experts specifically contracted for this purpose. This can be useful in detecting vulnerabilities in the system and for inspecting how effective the controls are in preventing unauthorized access due to these vulnerabilities.

Penetration testing and vulnerability assessments provide a snapshot of a system in a specific state at a specific time. The snapshot is limited to those portions of the system actually tested during the penetration attempt(s). Penetration testing and vulnerability assessments are not a substitute for risk assessment.

ISO/IEC TR 27008[13] provides specific guidance regarding technical compliance reviews.

管理者宜确定如何开展能够满足政策、标准和其他相应规程等需求的信息安全评审，定期评审宜考虑使用自动化测量和报告工具作为。

如果评审结果发现任何不符合，管理者宜：

a) 识别不符合的原因；

b) 评价确保合规采取措施的需要；

c) 实施适当的纠正措施；

d) 评审所采取的纠正措施，验证他的有效性，且识别任何缺陷或弱点。

评审结果和管理者采取的纠正措施宜被记录，且这些记录宜予以维护。当在管理者的职责范围内进行独立评审时，管理者宜将结果报告给执行独立评审的人员（见 18.2.1）。

其他信息

12.4 中包括了系统使用的运行监视。

### 18.2.3 技术符合性评审

控制措施

信息系统宜被定期评审是否符合组织的信息安全政策和标准。

实施指南

技术符合性评审宜通过自动化工具辅助下实施，以产生供技术专家进行后续解释的技术报告。可以选择由有经验的系统工程师手动地实施（如必要，由适当的软件工具支持）。

如果使用渗透测试或脆弱性评估，则宜格外小心，因为这些活动可能导致系统安全的损害。这样的测试宜预先计划，形成文件，且可重复执行。

任何技术符合性评审宜仅由有能力的、已授权的人员来完成，或在他们的监督下完成。

其他信息

技术符合性评审包括运行系统的试验，以确保硬件和软件控制措施被正确实施。这种类型的符合性核查需要专业技术专家。

符合性核查还包括，例如渗透测试和脆弱性评估，该项工作可以由针对此目的而专门签约的独立专家来完成。符合性核查有助于检测系统的脆弱性和核查为预防由于这些脆弱性引起的未授权访问而采取的控制措施的有效性。

渗透测试和脆弱性评估提供系统在特定时间特定状态的简单记录。这个简单记录只限制在渗透企图期间实际被测试系统的那些部分中。渗透测试和脆弱性评估不能代替风险评估。

ISO/IEC TR 27008 技术符合性评审特别指南。

# Bibliography


[1] ISO/IEC Directives, Part 2

[2] ISO/IEC 11770-1, *Information technology Security techniques — Key management — Part 1: Framework*

[3] ISO/IEC 11770-2, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*

[4] ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

[5] ISO 15489-1, *Information and documentation — Records management — Part 1: General*

[6] ISO/IEC 20000-1, *Information technology — Service management — Part 1: Service management system requirements*

[7] ISO/IEC 20000-2,[1)] *Information technology — Service management — Part 2: Guidance on the application of service management systems*

[8] ISO 22301, *Societal security — Business continuity management systems — Requirements*

[9] ISO 22313, *Societal security — Business continuity management systems — Guidance*

[10] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[11] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[12] ISO/IEC 27007, *Information technology — Security techniques — Guidelines for information security management systems auditing*

[13] ISO/IEC TR 27008, *Information technology — Security techniques — Guidelines for auditors on information security controls*

[14] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[15] ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

[16] ISO/IEC 27033-2, *Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security*

[17] ISO/IEC 27033-3, *Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues*

[18] ISO/IEC 27033-4, *Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways*

[19] ISO/IEC 27033-5, *Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Network (VPNs)*

[20] ISO/IEC 27035, *Information technology — Security techniques — Information security incident management*

[21] ISO/IEC 27036-1, *Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts*


1) ISO/IEC 20000-2:2005 has been cancelled and replaced by ISO/IEC 20000-2:2012, *Information technology — Service management — Part 2: Guidance on the application of service management systems.*

## 参考文献

[1] ISO/IEC 导则第2部分

[2] ISO/IEC 11770，信息技术—安全技术—密钥管理— 第1部分：框架

[3] ISO/IEC 11770，信息技术—安全技术—密钥管理— 第2部分：使用对称技术的机制

[4] ISO/IEC 11770，信息技术—安全技术—密钥管理— 第3部分：使用非对称技术的机制

[5] ISO 15489-1，信息和文件—记录管理—第1部分：概述

[6] ISO/IEC 20000-1:2012，信息技术—服务管理—第1部分：服务管理体系要求

[7] ISO/IEC 20000-2:2005，信息技术—服务管理—第1部分：最佳实践

[8] ISO/IEC 22301，社会安全—业务连续性管理体系—要求

[9] ISO/IEC 22313:2012，社会安全—业务连续性管理体系—指南

[10] ISO/IEC 27001，信息技术—安全技术—信息安全管理体系—要求

[11] ISO/IEC 27005，信息技术—安全技术—信息安全风险管理

[12] ISO/IEC 27007，信息技术—安全技术—信息安全管理体系审核指南

[13] ISO/IEC TR 27008，信息技术—安全技术—信息安全控制措施审核员指南

[14] ISO/IEC 27031，信息技术—安全技术—业务连续ICT就绪指南

[15] ISO/IEC 27033，信息技术—安全技术—网络安全—第1部分：概述和概念

[16] ISO/IEC 27033，信息技术—安全技术—网络安全—第2部分：网络安全设计和实施指南

[17] ISO/IEC 27033，信息技术—安全技术—网络安全—第3部分：网络相关场景—威胁、设计技术和控制问题

[18] ISO/IEC 27033，信息技术—安全技术—网络安全—第4部分：在网络间使用安全网关实施通信保护

[19]ISO/IEC 27033，信息技术—安全技术—网络安全—第5部分：使用VPN网络的安全通信

[20] ISO/IEC 27035，信息技术—安全技术—信息安全事件管理

[21] ISO/IEC 27036，信息技术—安全技术—供应商关系的信息安全—第1部分：概述和概念

[22] ISO/IEC 27036-2, *Information technology — Security techniques — Information security for supplier relationships — Part 2: Common requirements*

[23] ISO/IEC 27036-3, *Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for ICT supply chain security*

[24] ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*

[25] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

[26] ISO/IEC 29101, *Information technology — Security techniques — Privacy architecture framework*

[27] ISO 31000, *Risk management — Principles and guidelines*

[22] ISO/IEC 27036，信息技术—安全技术—供应商关系的信息安全—第2部分：通用要求

[23] ISO/IEC 27036，信息技术—安全技术—供应商关系的信息安全—第3部分：ICT供应链安全指南

[24] ISO/IEC 27037，信息技术—安全技术—电子证据识别、收集、获取和保存指南

[25] ISO/IEC 29100，信息技术—安全技术—隐私框架

[26] ISO/IEC 29101，信息技术—安全技术—隐私架构框架

[27] ISO 31000，风险管理— 原则和指南