信息安全技术—信息安全控制

Information security technology — Information security controls

(ISO/IEC 27002:2022, IDT)

翻译本

2022年12月

目录

前言

ISO（国际标准化组织）和 IEC（国际电工委员会）构成了全球标准化的专业体系。作为 ISO 或 IEC 成员的国家机构通过各自组织设立的技术委员会参与制定国际标准，以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开展合作。其他国际组织（政府和非政府）也与 ISO 和 IEC 保持联系，参与这项工作。

ISO/IEC 指令第 1 部分描述了制定本文件所用的程序以及用于进一步维护本文件的程序。特别应注意不同类型文件所需的不同批准标准。本文件是根据 ISO/IEC 指令第 2 部分的编辑规则起草的（请参阅 www.iso.org/directives 或 www.iec.ch/members_experts/refdocs）。

请注意，本文件的某些元素可能涉及专利权。ISO 和 IEC 不负责识别任何或所有此类专利权。在文件开发过程中识别的任何专利权的详细信息将在简介中和/或 ISO 收到的专利声明列表（请参阅 www.iso.org/patents）或 IEC 收到的专利声明列表（请参阅 patents.iec.ch）中列出。

本文件中使用的任何商品名称均为方便用户而提供的信息，并不构成认可。

有关标准的自愿性质、ISO 特定术语和与合格评定相关的表达的含义以及 ISO 在技术性贸易壁垒 (TBT) 中遵守世界贸易组织 (WTO) 原则的信息，请参阅 www.iso.org/iso/foreword.html。在 IEC 中，请参阅 www.iec.ch/understanding-standards。

本文件由 ISO/IEC JTC 1 信息技术联合技术委员会、SC 27 信息安全、网络安全和隐私保护小组委员会编写。

第三版取消并取代了第二版 (ISO/IEC 27002:2013)，后者已进行技术修订。它还纳入了技术勘误表 ISO/IEC 27002:2013/Cor. 1:2014 和
ISO/IEC 27002:2013/Cor. 2:2015。

主要变化如下：

— 标题已修改；

— 文档结构已更改，使用简单分类法和相关属性呈现控件；

— 合并了一些控件，删除了一些控件，并引入了几个新控件。完整的对应关系可在附件 B 中找到。

有关本文档的任何反馈或问题都应直接发送给用户的国家标准机构。这些机构的完整列表可在 www.iso.org/members.html 和www.iec.ch/national-committees 上找到。

引言

0.1 背景

本文件适用于所有类型和规模的组织。组织在实施基于ISO/IEC 27001信息安全管理体系的信息安全风险处置时，本文件可作为其确定和实施所需控制的参考；本文件还可作为组织在确定和实施普遍接受的信息安全控制时的指导文件。此外，本文件旨在用于制定行业和特定组织的信息安全管理指南，同时考虑其具体的信息安全风险环境。除本文件包含的控制外，可通过风险评估来确定特定于组织或环境所需要的控制。

所有类型和规模的组织（包括公共和私营部门、商业和非营利性组织）都会以多种形式创建、收集、处理、存储、传输和处置信息，包括电子的、物理的和口头的（如对话—会话和演示）。

信息的价值超出了字、数字和图像的本身：如知识、概念、观点和品牌都是无形信息。在互联的世界中，信息和相关资产都值得或需要保护，以防范各种风险源，无论该风险是源自自然界，还是意外或故意破坏。信息安全是通过实施一组适宜的控制来实现的，包括策略、规则、过程、规程、组织结构和软硬件功能。组织宜在必要时定义、实施、监视、评审和改进这些控制，以满足其特定的安全和业务目标。ISO/IEC 27001中规定的ISMS从整体、协调的视角审视组织的信息安全风险，在协调一致的管理体系总框架内确定和实施一套全面的信息安全控制。许多信息系统，包括其管理和运营，并没有按照ISO/IEC 27001所规定的ISMS和本文件来进行安全的设计。只通过技术措施所能实现的安全水平是有限的，宜通过适当的管理活动和组织过程给予支持。在进行风险处置时，需要仔细规划、注意细节，来确定宜实施哪些控制。成功的ISMS需要得到组织内所有人员的支持，还可能需要股东或供应商等其他利益相关方的参与，同时也需要业内专家的建议。

一个适宜、充分和有效的信息安全管理体系，为组织的管理层及其他利益相关方提供以下保证：它们的信息及其他相关资产处于合理的安全状态并免受威胁和损害，从而使组织能够实现既定的业务目标。

0.2 信息安全要求

组织确定其信息安全要求是必要的。信息安全要求有三个主要来源：

a) 考虑组织的整体业务战略与目标来对组织风险进行评估。这能通过特定于信息安全的风险评估来给予帮助或支持。这宜得出对必要控制的确定，以确保组织面临的残余风险符合其风险接受准则；

b) 组织及其利益相关方（贸易伙伴、服务提供者等）必须遵守的法律、法规、规章和合同要求及其社会文化环境；

c) 组织为支持其运行而为信息生存周期的所有步骤所建立的一整套原则、目标和业务要求。

0.3 控制

控制的定义是改变或维持风险的措施。本文件中的某些控制是修改风险，而其他控制则是维持风险。例如，信息安全方针只能维持风险，而遵守信息安全方针则能改变风险。此外，某些控制描述了不同风险环境下相同的通用措施。本文件提供了源于国际公认最佳实践的一系列组织、人员、物理和技术信息安全控制。

0.4 控制的确定

控制的确定取决于组织在风险评估后做出的决策，并有一个明确定义的范围。与已识别风险相关的决策宜基于风险接受准则、风险处置选项和组织所采用的风险管理方法。控制的确定还宜考虑所有相关的国家和国际法律法规。控制的确定还取决于不同控制的协同，以实现纵深防御。

组织可根据需要来设计控制，或从任何来源识别控制。在指定此类控制时，组织宜考虑相对于所实现的业务价值，实施和运行控制所需要的资源和投资。参见ISO/IEC TR 27016，了解有关ISMS投资的决策指南，以及这些决策在资源相互冲突的境下带来的经济后果。

在为实施控制而部署的资源与因缺乏这些控制而发生安全事件所导致的潜在业务影响之间宜取得平衡。风险评估的结果宜有助于指导和确定适当的管理措施、管理信息安全风险的优先顺序，以及实施为防范这些风险而确定的必要控制。

本文件中的某些控制可被视为信息安全管理的指导原则，适用于大多数组织。有关确定控制和其他风险处置选项的更多信息，可参见ISO/IEC 27005。

0.5 编制特定于组织的指南

本文件可被视为制定特定于组织的指南的出发点。本文件中并非所有的控制和指南都适用所有组织。组织还可能需要本文件中未包含的额外控制和指南，以满足其具体需求和解决已识别到的风险。在编制包含额外的指南或控制的文件时，对本文件中的条款交叉引用有助于为以后提供参考。

0.6 生存周期的考虑

信息具有从创建到销毁的生存周期。在其整个生存周期中，信息的价值和其面临的风险可能会变化（例如，未经授权披露或窃取公司财务账户在公布后并不重要，但完整性仍然至关重要），因此，在所有阶段信息安全都很重要。

与信息安全相关的信息系统和其他资产具有生存周期，包括构思、规范、设计、开发、测试、实施、使用、维护并最终退役和销毁。每个阶段均宜考虑信息安全。新的系统开发项目和对现有系统的变更，为改进安全控制提供了机会，同时考虑组织面临的风险和从安全事件中吸取的经验教训。

0.7 相关标准

本文件为普遍应用于各类组织的广泛的信息安全控制提供了指导，ISMS标准族中的其他文件还针对信息安全管理全过程的其他方面提供了补充建议或要求。

有关ISMS及ISMS标准族总体介绍参见ISO/IEC 27000。ISO/IEC 27000中提供了一个词汇表，定义了ISMS标准族中使用的大多数术语，并描述了该文件族中每项标准的范围和目的。

一些适用于特定行业的标准给出了针对特定领域的额外控制（例如，针对云服务的ISO/IEC 27017、针对隐私保护的ISO/IEC 27701、针对能源的ISO/IEC 27019、针对电信组织的ISO/IEC 27011和针对健康的ISO 27799）。这些标准收录在参考文献中，其中在第5章至第8章中引用了部分标准。

信息安全技术—— 信息安全控制

1 范围

本文件提供了一套通用信息安全控制参考集，包括实施指南。本文件适用于：

a) 组织基于 ISO/IEC 27001实施信息安全管理体系（ISMS）；
b) 组织基于国际公认最佳实践实施信息安全控制；
c) 组织编制其自身的信息安全管理指南。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1
访问控制 access control
确保对资产（3.1.2）的物理和逻辑访问是基于业务和信息安全要求进行授权和限制的手段。

3.1.2
资产 asset
对组织有价值的任何事物。
注： 在信息安全的语境下，可分为两类资产。
——主要资产：
- 信息；
- 业务过程（3.1.27）和活动。

——所有类型的支撑性资产（主要资产所依赖的资产），例如：
- 硬件；
- 软件；
- 网络；
- 人员（3.1.20）；
- 场所；
- 组织结构。

3.1.3
攻击 attack
未经授权企图销毁、更改、禁用、访问资产（3.1.2）的行为（无论成功或失败），或者企图泄露、窃取或未经授权使用资产的任何行为。

3.1.4
鉴别 authentication
确保实体所声称其特征是正确的一种措施。

3.1.5
真实性 authenticity
一个实体（3.1.11）是其所声称实体的性质。

3.1.6
保管链 chain of custody
可证明的对材料从一个时间点到另一个时间点上的持有、移动、处理和定位。
注： 材料包括ISO/IEC 27002语境下的信息及其他相关资产（3.1.2）。
[来源：ISO/IEC 27050-1:2019，3.1，有修改：添加注]

3.1.7
保密信息 confidential information
不向未经授权的个人、实体（3.1.11）或过程（3.1.27）提供或披露的信息。

3.1.8
控制 control
保持和/或改变风险的措施。
注1：控制包括但不限于保持和/或改变风险的任何过程（3.1.27）、方针（3.1.24）、设备、实践或其他条件和/或行动。注2：控制并非总能取得预期的改变效果。
[来源：ISO 31000:2018，3.8]

3.1.9
中断 disruption
在按照组织的目标进行产品和服务的预期交付时导致出现计划外的负面偏差的事件，无论是预期的还是未预期的。
[来源：ISO 22301:2019，3.10]

3.1.10
终端设备 endpoint device
联网的信息通信技术（ICT）硬件设备。
注： 终端设备包括台式电脑、笔记本电脑、智能手机、平板电脑、瘦客户端、打印机或其他包括智能仪表和物联网（IoT）设备的专用硬件等。

3.1.11
实体 entity
明显确实存在并与某一领域运行目的相关的事物。
注： 实体可能是物理的或逻辑的。
示例：个人、组织、设备、事物类组、电信服务用户、SIM 卡、护照、网卡、软件应用程序、服务或网站。
[来源：ISO/IEC 24760-1:2019, 3.1.1]

3.1.12
信息处理设施 information processing facility
任何信息处理系统、服务或基础设施，或者安置其的物理场所。
[来源：ISO/IEC 27000:2018，3.27]

3.1.13
信息安全违规 information security breach
信息安全性的受损，导致传输、存储或以其他方式处理的受保护信息遭到意外破坏、丢失、篡改、泄露或非授权访问等。

3.1.14
信息安全事态 information security event
表明一次可能的信息安全违规（3.1.13）或某些控制（3.1.8）失效的发生。
[来源：ISO/IEC 27035-1:2016，3.3]

3.1.15
信息安全事件 information security incident
与可能危害组织资产（3.1.2）或损害其运行相关的、单个或多个被识别的信息安全事态（3.1.14）。
[来源：ISO/IEC 27035-1:2016，3.4]

3.1.16
信息安全事件管理 information security incident management
采用一致和有效方法处理信息安全事件(3.1.15)的行为。
[来源：ISO/IEC 27035-1:2016，3.5]
3.1.17
信息系统 information system
应用程序、服务、信息技术资产或其他信息处理组件的组合。
[来源：ISO/IEC 27000:2018，3.35]

3.1.18
相关方 interested party
可能对一项决策或活动产生影响，或被其影响，或自认为受到其影响的个人或组织。
[来源：ISO/IEC 27000:2018，3.37]

3.1.19
抗抵赖性 non-repudiation
证明所声称事态或行动的发生及其起源实体（3.1.11）的能力。

3.1.20
工作人员 personnel
在组织指导下开展工作的人。
注：工作人员的概念包括组织的成员，诸如治理层、最高管理层、员工、临时工、合同工和志愿者。

3.1.21
个人可识别信息 personally identifiable information；PII
能建立信息和该信息有关的自然人的链接，或者能直接或间接链接到自然人的任何信息。
注：定义中的“自然人”是指PII主体（3.1.22）。确定PII主体是否可识别，宜考虑建立PII集与自然人联系的所有方式，这些方式可以被持有数据的隐私利益相关方或其他方合理利用。
[来源：ISO/IEC 29100:2011/Amd.1:2018，2.9]

3.1.22
PII 主体 PII principal
涉及个人可识别信息（PII）（3.1.21）的自然人。
注：根据管辖区域和特定的数据保护和隐私法规，也可使用“数据主体”代替术语“PII主体”。
[来源：ISO/IEC 29100:2011，2.11]

3.1.23
PII 处理者 PII processor
代表并根据PII（3.1.21）控制者指示处理个人可识别信息（PII）的隐私利益相关者。
[来源：ISO/IEC 29100:2011，2.12]

3.1.24
方针 policy
由其最高管理层正式表达的组织的意图和方向。
[来源：ISO/IEC 27000:2018，3.53]

3.1.25
隐私影响评估 privacy impact assessment；PIA
在组织更广泛的风险管理框架内，识别、分析、评价、咨询、沟通和策划处置与个人可识别信息（PII）（3.1.21）处理相关的潜在隐私影响的整体过程（3.1.27）。
[来源：ISO/IEC 29134:2017，3.7，有修改：删除注]

3.1.26
规程 procedure
执行某项活动或某个过程（3.1.27）的指定方法。
[来源：ISO 30000:2009，3.12]

3.1.27
过程 process
利用输入实现预期结果的相互关联或相互作用的一组活动。
[来源：ISO 9000:2015，3.4.1，有修改：删除注]

3.1.28
记录 record
组织或个人为履行法律义务或进行业务交易而创建、接收和保持的作为证据和资产（3.1.2）的信息。

注：本文件中，法律义务包括所有法律、法规、监管和合同要求。
[来源：ISO 15489-1:2016，3.14，有修改：增加注]

3.1.29
恢复点目标 recovery point objective；RPO
中断（3.1.9）发生后数据得以恢复的时间点。
[来源：ISO/IEC 27031:2011，3.12，有修改]

3.1.30
恢复时间目标 recovery time objective；RTO
中断（3.1.9）发生后，恢复最低限度的服务和/或产品以及支持系统、应用程序或功能的时间段。
[来源：ISO/IEC 27031:2011，3.13，有修改]

3.1.31
可靠性 reliability
与预期行为和结果一致的性质。

3.1.32
规则 rule
组织所接受的，表明其期望要做什么、允许什么或禁止什么的原则或指令。
注：可在特定主题策略（3.1.35）以及其他类型文档中正式表述规则。

3.1.33
敏感信息 sensitive information
一旦不可用、未经授权访问、篡改、泄露，可能对个人、组织、国家安全或公共安全带来潜在不利影响而需保护的信息。

3.1.34
威胁 threat
可能对系统或组织造成危害的不希望事件的潜在因素。
[来源：ISO/IEC 27000:2018，3.74]

3.1.35
特定主题策略 topic-specific policy
适当层级管理者正式提出的对某一特定主题的意图和指导。
注1：特定主题策略能正式表达规则（3.1.32）或组织标准。
注2：一些组织会为特定主题策略使用其他术语。
注3：本文件所提及的特定主题策略与信息安全有关。
示例：访问控制（3.1.1）的特定主题策略，清理桌面和屏幕的特定主题策略。

3.1.36
用户 user
有权访问组织信息系统（3.1.17）的相关方（3.1.18）。
示例：工作人员（3.1.20）、客户、供应商。

3.1.37
用户终端设备 user endpoint device
供用户用于访问信息处理服务的终端设备（3.1.10）。
注：用户终端设备可以指台式电脑、笔记本电脑、智能手机、平板电脑、瘦客户端等。

3.1.38
脆弱性 vulnerability
可能被一个或多个威胁（3.1.34）利用的资产（3.1.2）或控制（3.1.8）的弱点。
[来源：ISO/IEC 27000:2018，3.77]

3.2 缩略语

下列缩略语适用于本文件。

ABAC：基于属性的访问控制（attribute-based access control）
ACL：访问控制列表（access control list）
BIA：业务影响分析（business impact analysis）
BYOD：自携设备（bring your own device）
CAPTCHA：验证码（completely automated public turing test to tell computers and humans apart）
CPU：中央处理器（central processing unit）
DAC：自主访问控制（discretionary access control）
DNS：域名系统（domain name system）
GNSS：全球导航卫星系统（global navigation satellite system）
IAM：身份与访问管理（identity and access management）
ICT：信息通信技术（information and communication technology）
ID：标识符（identifier）
IDE：集成开发环境（integrated development environment）
IDS：入侵检测系统（intrusion detection system）
IoT：物联网（internet of things）
IP：互联网协议（internet protocol）
IPS：入侵防御系统（intrusion prevention system）
IT：信息技术（information technology）
ISMS：信息安全管理体系（information security management system）
MAC：强制访问控制（mandatory access control）
NTP：网络时间协议（network time protocol）
PIA：隐私影响评估（privacy impact assessment）
PII：个人可识别信息（personally identifiable information）
PIN：个人识别码（personal identification number）
PKI：公钥基础设施（public key infrastructure）
PTP：高精度时间同步协议（precision time protocol）
RBAC：基于角色的访问控制（role-based access control）
RPO：恢复点目标（recovery point objective）
RTO：恢复时间目标（recovery time objective）
SAST：静态应用安全测试（static application security testing）
SD：安全数字（secure digital）
SDN：软件定义网络（software-defined networking）
SD-WAN：软件定义广域网络（software-defined wide area networking）

SIEM：安全信息和事件管理（security information and event management）
SMS：短信服务（short message service）
SQL：结构化查询语言（structured query language）
SSO：单点登录（single sign on）
SWID：软件识别（software identification）
UEBA：用户和实体行为分析（user and entity behaviour analytics）
UPS：不间断电源（uninterruptible power supply）
URL：统一资源定位符（uniform resource locator）
USB：通用串行总线（universal serial bus）
VM：虚拟机（virtual machine）
VPN：虚拟专用网（virtual private network）
WLAN：无线局域网（wireless local area network）

4 文件结构

4.1 章条设置

本文件结构如下：

a) 组织控制（第 5 章）；
b) 人员控制（第 6 章）；
c) 物理控制（第 7 章）；
d) 技术控制（第 8 章）。

本文件含有2个资料性附录：

——附录 A 属性的使用；

——附录 B 本文件与 ISO/IEC 27002:2013的对应关系。

附录A解释了组织如何使用属性（见4.2）创建自己的视图，可以使用基于本文件所定义的控制属性或组织自行创建的控制属性。

附录B展示了本文件与ISO/IEC 27002:2013版本中各项控制的对应关系。

4.2 主题和属性

第5章至第8章中提供的控制分类统称为主题。控制类别为：

a) 人员，如果涉及到单独的个人；
b) 物理，如果涉及到物理对象；
c) 技术，如果涉及到技术；
d) 其他均归类为组织。

组织可使用属性来创建不同的视图，这些视图从主题的不同视角进行控制分类。属性可用于不同使用者在不同视图中进行控制的筛选、分类或展示。附录A解释了实现过程并提供了视图示例。

本文件给出了示例，将每一项控制关联到以下五种属性的相应属性值（前缀‘#’方便搜索）：

a) 控制类型
控制类型是从控制何时和如何改变信息安全事件发生风险的视角来看控制的一种属性。属性值包含预防（旨在防止信息安全事件发生的控制）、检测（作用于信息安全事件发生时的控制）和纠正（作用于信息安全事件发生后的控制）。

b) 信息安全属性
信息安全属性是从控制有助于保护哪些信息特征的视角来看控制的一种属性。属性值包含保密性、完整性和可用性。

c) 网络空间安全概念
网络空间安全概念是从控制与网络空间安全概念关联的视角来看控制的一种属性，ISO/IEC TS 27110描述的网络空间安全框架定义了网络空间安全概念。属性值包含识别、防护、发现、响应和恢复。

d) 运行能力
运行能力是从从业者信息安全能力的视角来看控制的一种属性。属性值包含治理、资产管理、信息保护、人力资源安全、物理安全、系统和网络安全、应用安全、安全配置、身份和访问管理、威胁和脆弱性管理、连续性、供应商关系安全、合规性、信息安全事件管理和信息安全保障。

e) 安全领域
安全领域是从四个信息安全领域的视角来看控制的一种属性。四个信息安全领域为：“治理和生态体系”，包括“信息系统安全治理和风险管理”和“生态系统网络空间安全管理”（包括内外部相关方）； “保护”，包括“IT安全架构”、“IT安全管理”、“身份和访问管理”、“IT安全维护”及“物理和环境安全”；“防御”，包括“检测”和“计算机安全事件管理”；“弹性”，包括“运行的连续性”和“危机管理”。属性值包含治理和生态体系、防护、防御和弹性。

本文件给出的属性是基于其在各类组织中应用的通用性考量而选择。组织可选择不考虑本文件所给出的一种或多种属性。组织也可创建自有属性（具有相应的属性值），形成组织自己的视图。A.2中包含了这种属性的示例。

4.3 控制的设计

每项控制的设计包含以下内容：
——控制名称：控制的简称；
——属性表：显示既定控制各项属性值的表格；
——控制：控制的说明；
——目的：为何实施控制；
——指南：如何实施控制；
——其他信息：解释性文本或对其他相关文件的参考引用。

对于某些控制的指南文本较长且涉及多个主题，使用子标题（即三级条）提高其可读性。此类子标题不一定在所有指南文本中使用。

5 组织控制

5.1 信息安全策略

5.1.1 属性表

信息安全策略的属性表见表1。

表1 信息安全策略属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#识别	#治理	#治理和生态体系 #弹性

5.1.2 控制

宜定义信息安全方针和特定主题策略，由管理层批准后发布，传达并让相关工作人员和相关方知悉，按计划的时间间隔以及在发生重大变更时对其进行评审。

5.1.3 目的

根据业务、法律、法规、规章和合同要求，确保信息安全的管理方向以及相应支持的持续适宜性、充分性、有效性。

5.1.4 指南

组织在最高层上宜定义“信息安全方针”，该方针由最高管理层批准，并规定了组织管理其信息安全的方法。

信息安全方针宜考虑以下方面产生的要求：

a) 业务战略和需求；
b) 法律、法规和合同；
c) 当前和预期的信息安全风险和威胁。

信息安全方针宜包括以下内容的陈述：

a) 信息安全的定义；
b) 信息安全目标或设定信息安全目标的框架；
c) 指导所有信息安全相关活动的原则；
d) 满足信息安全相关适用要求的承诺；
e) 持续改进信息安全管理体系的承诺；
f) 对既定角色分配的信息安全管理责任；
g) 处理豁免和例外的规程。

对信息安全方针的任何变更宜由最高管理层进行审批。

在较低层面，信息安全方针宜根据需要由特定主题策略予以支持，以进一步强制实

施信息安全控制。特定主题策略通常被构建为解决组织内某些目标群体的需求或涵盖某些安全领域。特定主题策略宜与组织的信息安全方针保持一致并与之互补。这样的主题包括但不限于：

a) 访问控制；
b) 物理和环境安全；
c) 资产管理；
d) 信息传输；
e) 用户终端设备的安全配置和处理；
f) 网络安全；
g) 信息安全事件管理；
h) 备份；
i) 密码技术和密钥管理；
j) 信息分级和处理；
k) 技术脆弱性管理；
l) 安全开发。

开发、评审和批准特定主题策略的责任宜根据相关工作人员的职权等级和技术能力进行分派。评审宜包括评估组织信息安全方针和特定主题策略的改进机会，并管理信息安全以应对下列变化：

a) 组织的业务战略；
b) 组织的技术环境；
c) 法律、法规、规章和合同；
d) 信息安全风险；
e) 当前和预期的信息安全威胁环境；
f) 从信息安全事态和事件中总结的经验教训。

信息安全方针和特定主题策略的评审宜考虑管理评审和审计的结果。某个策略发生变化时宜考虑其他相关策略的评审和更新以保持一致性。

信息安全方针和特定主题策略宜以意向读者适合的、可访问的和可理解的形式传达给相关工作人员及相关方。宜要求策略的接收者确认已理解并同意遵守适用的策略。组织可自行决定满足组织需求的这些策略文件的格式和名称。一些组织的信息安全方针和特定主题策略可列入单独的文件。组织可以将这些特定主题策略命名为标准、导则、策略或其他。

如果信息安全方针或任何特定主题策略在组织外进行分发，宜注意不要不当披露保密信息。

表2展示了信息安全方针与特定主题策略之间的差异。

表2 信息安全方针与特定主题策略之间的差异

	信息安全方针	**特定主题策略**
详略程度	一般的或高层级的	具体且详细的
文件化并被正式批准	最高管理层	适当级别的管理层

5.1.5 其他信息

各组织的特定主题策略可有所不同。

5.2 信息安全角色和责任

5.2.1 属性表

信息安全角色和责任的属性表见表3。

表3 信息安全角色和责任属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#识别	#治理	#治理和生态体系 #防护 #弹性

5.2.2 控制

信息安全角色和责任宜根据组织需求进行定义和分配。

5.2.3 目的

建立一个定义明确、获得批准和各方理解的架构以利于组织内信息安全的实现、运行和管理。

5.2.4 指南

信息安全角色和责任的分配宜根据信息安全方针和特定主题策略（见5.1）来完成。组织宜定义并管理下列责任：

a) 信息及其他相关资产的保护；
b) 落实具体信息安全过程；
c) 信息安全风险管理活动，尤其是对残余风险的接受（如风险责任人）；
d) 使用组织信息及其他相关资产的所有工作人员。

必要时，宜针对特定的地点和信息处理设施的责任补充更详细的指南。分配到信息安全责任的个人可以将安全任务委托给其他人员。然而，他们仍需负责，并确定任何被委托的任务是否已被正确地执行。

宜明确定义、记录并传达个人负责的每个安全区域。权限等级宜有明确定义并形成文件。承担特定信息安全角色的个人宜具备该角色所要求的知识和技能，同时宜支持他们跟进该角色以及角色需求的最新变化，以满足该角色的履责需要。

5.2.5 其他信息

许多组织会任命一名信息安全管理人员来全面负责信息安全的开发和实现，并为识别风险和缓解风险的控制提供支持。

然而，提供分配资源并实现这些控制的责任通常仍归于各个管理人员。一种通常的做法是为每一项资产指定一名责任人负责该资产的日常保护。

根据组织的规模和资源，可通过在原有角色基础上增加专门的角色或职责来涵盖信息安全工作。

5.3 职责分离

5.3.1 属性表

职责分离的属性表见表4。

表4 职责分离属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#治理 #身份和访问管理	#治理和生态体系

5.3.2 控制

宜分离相互冲突的职责和责任范围。

5.3.3 目的

降低欺诈、错误和绕过信息安全控制的风险。

5.3.4 指南

职责及其责任范围的分离旨在分离不同个体之间存在冲突的职责，以防止个人独立履行可能存在冲突的职责。

组织宜确定哪些职责及其责任范围需进行分离。可能需要进行职责分离的活动包括但不限于：

a) 变更的发起、审批和执行；
b) 访问权的请求、审批和授权；
c) 代码的设计、实现和审查；
d) 软件的开发和生产系统的管理；
e) 应用程序的使用和管理；
f) 数据库的使用和管理；
g) 信息安全控制的设计、审核和保证。

在设计职责分离控制时，宜考虑相互串通的可能性。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，例如对活动的监视、审核跟踪和管理监督等。

当使用基于角色的访问控制系统时，宜注意确保人员未被授予相互冲突的角色。存在大量角色时，组织宜考虑使用自动化工具来识别冲突并加快冲突的消除。宜仔细定义

和配置角色，确保在角色被删除或重新分配时最大程度减少访问问题。

5.3.5 其他信息

无其他信息。

5.4 管理责任

5.4.1 属性表

管理责任的属性表见表5。

表5 管理责任属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#识别	#治理	#治理和生态体系

5.4.2 控制

管理层宜要求所有工作人员根据组织已建立的信息安全方针、特定主题策略和规程，履行信息安全责任。

5.4.3 目的

确保管理层理解自己在信息安全中的角色并采取措施确保所有工作人员都清楚了解并履行自己的信息安全责任。

5.4.4 指南

管理层宜表现出对信息安全方针、特定主题策略、规程以及信息安全控制的支持。管理责任宜包括确保人员：

a) 在获得组织信息及其他相关资产的访问授权前，正确了解其信息安全角色和责任；
b) 获得相关的指南，其中明确指出该角色在组织内部的信息安全预期；
c) 被强制性要求执行组织的信息安全方针和特定主题策略；
d) 达到与其在组织内角色和责任相关的信息安全意识水平（见 6.3）；
e) 遵守任用、合同或协议中的条款和条件，包括组织的信息安全方针和适当的工作方法；
f) 通过持续的专业教育保持具备适当的信息安全技能和资质；
g) 在切实可行的情况下，可通过保密渠道报告违反信息安全方针、特定主题策略或信息安全规程的行为
（“检举”）。该渠道允许匿名报告，或者确保仅需要处理此类报告的人员可掌握报告人的身份信息；
h) 有足够的资源和充分的项目计划时间来实现组织的安全相关过程和控制。

5.4.5 其他信息

无其他信息。

5.5 与职能机构的联系

5.5.1 属性表

与职能机构的联系的属性表见表6。

表6 与职能机构的联系属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防 #纠正	#保密性 #完整性 #可用性	#识别 #防护 #响应 #恢复	#治理	#防御 #弹性

5.5.2 控制

组织宜建立并维护与相关职能机构的联系。

5.5.3 目的

确保组织就信息安全事宜与相关执法部门、监管机构和监督部门之间进行适当的信息交流。

5.5.4 指南

组织宜明确规定什么时候与哪个职能机构（例如执法部门、监管机构、监督部门）进行联系，以及如何及时报告已识别的信息安全事件。

与职能机构的联系还可用于促进了解这些机构当前和今后的预期（例如适用的信息安全法规）。

5.5.5 其他信息

遭受攻击的组织可请求职能机构对攻击源采取行动。

维护这样的联系，可能是支持信息安全事件管理的要求（见5.24~5.28），或者是应急计划和业务连续性过程的要求（见5.29、5.30）。与法规部门的联系还有助于对可能影响到组织的相关法律或法规变化进行预测，并预先做好准备。与其他职能机构的联系包括公共事业、紧急服务、电力供应、健康和安全部门，例如消防局

（与业务连续性有关）、电信提供者（与线路的布置和可用性有关）、供水部门（与设备的冷却设施有关）。

5.6 与特定相关方的联系

5.6.1 属性表

与特定相关方的联系的属性表见表7。

表7 与特定相关方的联系属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防 #纠正	#保密性 #完整性 #可用性	#防护 #响应 #恢复	#治理	#防御

5.6.2 控制

组织宜建立并维护与特定相关方或其他专业安全论坛和专业协会的联系。

5.6.3 目的

确保在信息安全方面进行适当的信息交流。

5.6.4 指南

宜成为特定相关方或论坛的成员，以实现下述目的：

a) 增进最佳实践的知识，掌握最新相关安全信息；
b) 确保了解最新的信息安全环境；
c) 获取与攻击和脆弱性有关的警报、公告和补丁的预警；
d) 获得专业的信息安全建议；
e) 共享和交换关于新的技术、产品、服务、威胁或脆弱性的信息；
f) 在处置信息安全事件时，提供适当的联络点（见 5.24~5.28）。

5.6.5 其他信息

无其他信息。

5.7 威胁情报

5.7.1 属性表

威胁情报的属性表见表8。

表8 威胁情报属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防 #检测 #纠正	#保密性 #完整性 #可用性	#识别 #发现 #响应	#威胁和脆弱性管理	#防御 #弹性

5.7.2 控制

宜收集并分析信息安全威胁相关的信息，以生成威胁情报。

5.7.3 目的

了解组织的威胁环境，以便采取适当的缓解措施。

5.7.4 指南

对已有或新出现的威胁进行信息收集和分析，以便：

a) 采取知情的行动，防止威胁对组织造成损害；
b) 减轻此类威胁的影响。

威胁情报可分为三个层级，宜全部考虑在内：

a) 战略级的威胁情报：关于不断变化的威胁形势的高层信息交换（例如攻击者类型或攻击类型）；
b) 战术级的威胁情报：关于攻击者所用方法、工具和所涉技术的信息；
c) 运营级的威胁情报：关于特定攻击的详细信息，包括技术指标。

威胁情报宜：

a) 具有相关性（即与组织的保护相关）；
b) 具有洞察力（即能够让组织准确而详细地理解威胁形势）；
c) 具有情境性，可提供态势感知（即根据事件的时间、发生的地点、既往经验和类似组织中的普遍性等来增加信息的上下联系）；
d) 具有可行动性（即组织可根据信息做出快速而有效的行动）。

威胁情报活动宜包括：

a) 建立威胁情报生成的目标；
b) 识别、审查并选择必要且适当的内外部信息源，以提供生成威胁情报所需的信息；
c) 从选定的来源中收集信息，可以是内部和外部的来源；
d) 对收集到的信息进行处理，为分析做好准备（例如对信息的翻译、格式化或证实）；
e) 分析信息以理解其与组织的关系及其对组织的意义；
f) 以可理解的方式与相关人员沟通和分享信息。

威胁情报宜予以分析并留待后续使用：

a) 通过实施过程将从威胁情报来源中收集到的信息纳入组织的信息安全风险管理过程；
b) 作为防火墙、入侵检测系统或反恶意软件解决方案等技术预防和检测控制的附加输入信息；
c) 作为信息安全测试过程和技术的输入信息。

组织宜与其他组织相互分享威胁情报，以改进总体的威胁情报。

5.7.5 其他信息

组织可利用威胁情报来预防、检测或响应威胁。组织可以生成威胁情报，但更常见的是接收并利用其他来源所生成的威胁情报。

威胁情报通常由独立提供者或顾问、政府机构或威胁情报协作团体提供。

控制（如5.25、8.7、8.16或8.23）的有效性取决于可用威胁情报的质量。

5.8 项目管理中的信息安全

5.8.1 属性表

项目管理中的信息安全的属性表见表9。

表9 项目管理中的信息安全属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#识别 #防护	#治理	#治理和生态体系 #防护

5.8.2 控制

宜将信息安全整合到项目管理中。

5.8.3 目的

确保与项目和交付成果相关的信息安全风险，在整个项目生存周期内通过项目管理得到有效解决。

5.8.4 指南

信息安全宜整合到项目管理中，以确保信息安全风险作为项目管理的一部分而得到解决。其适用于任意类型的项目，无论项目的复杂性、规模、持续时间、学科领域或应用范围（例如核心业务过程、ICT、设施管理或其他支持过程等方面的项目）。

使用的项目管理方法宜要求：

a) 在整个项目生存周期的早期阶段以及项目风险工作中定期评估并处置信息安全风险；
b) 在项目的早期阶段针对性提出信息安全要求，例如应用安全要求（见 8.26）、遵守知识产权的要求（见 5.32）等；
c) 在整个项目生存周期内，注意考虑并处置项目执行相关的信息安全风险，如内外部通信安全；
d) 评审信息安全风险处置进度，并对处置方法的有效性进行评估和测试。

宜在预定义阶段内由适当的人员或治理团体（如项目指导委员会）研究确定信息安全注意事项和相关活动的适当性，并负责跟进。

与项目相关的信息安全责任和权限宜有明确定义并分配给特定角色。

宜采用多种方法确定项目交付的产品或服务的信息安全要求，包括从信息安全方针、特定主题策略和法规中推导出合规性要求。更进一步的信息安全要求可以从威胁建模、事件回顾、脆弱性阈值的使用或应急计划等活动中推导出来，从而确保信息系统的体系结构和设计得到保护，免遭基于运行环境的已知威胁。

宜针对所有类型的项目，不仅是ICT开发项目，确定信息安全要求。确定这些要求时宜考虑：

a) 涉及哪些信息（信息确定）、相应的信息安全需求有哪些（分级，见 5.12），以及因缺乏充分的安全而可能造成的潜在负面业务影响有哪些；
b) 涉及的信息及其他相关资产必要的保护需求，尤其是保密性、完整性和可用性；
c) 实体身份声明中必要的置信度水平或保证水平，以此确定身份鉴别要求；
d) 为客户和其他潜在业务用户以及特权用户或技术用户，如相关项目成员、潜在运营人员或外部供应商提供访问资源调配和授权过程；
e) 告知用户其职责和责任；
f) 源于业务过程的要求，如交易登记和监控、抗抵赖性要求等；
g) 其他信息安全控制的强制要求（如日志和监控接口或数据泄露检测系统接口）；
h) 遵守组织经营所在地的法律、法规、监管和合同环境；
i) 第三方需具备必要的置信度水平或保证水平，以满足组织信息安全方针和特定主题策略，包括任何协议或合同中的相关安全条款。

5.8.5 其他信息

项目开发方法，如瀑布生存周期或敏捷生存周期，宜以结构化的方式支持信息安全，可根据项目的特点进行调整，以适应信息安全风险的严重性评估。尽早考虑产品或服务的信息安全要求（例如在规划和设计阶段），可为质量和信息安全提供更有效、更具成本效益的解决方案。ISO 21500和ISO 21502为项目管理的概念和过程提供了指导，这些概念和过程对项目的执行非常重要。

ISO/IEC 27005为使用风险管理过程以确定满足信息安全要求的控制提供了指南。

5.9 信息及其他相关资产的清单

5.9.1 属性表

信息及其他相关资产的清单的属性表见表10。

表10 信息及其他相关资产的清单属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#识别	#资产管理	#治理和生态体系 #防护

5.9.2 控制

宜编制和维护信息及其他相关资产（包括资产拥有者）的清单。

5.9.3 目的

识别组织的信息及其他相关资产，以保护其信息安全并分配适当的所有权。

5.9.4 指南

5.9.4.1 清单

组织宜识别信息及其他相关资产，并确定其在信息安全方面的重要性。适宜时，宜在专用清单或现有清单中维护这些记录。

信息及其他相关资产的清单宜准确、实时更新、具备一致性并与其他清单保持统一。为确保信息及其他相关资产的清单的准确性，宜：

a) 根据资产清单，定期审查已识别的信息及其他相关资产；
b) 在安装、变更或移除资产的过程中，自动强制更新清单。

适宜时，清单中宜包含资产的位置。

清单不一定是信息及其他相关资产的单一清单。考虑到清单宜由相关职能部门进行维护，可以将其视为一组动态清单，例如信息资产、硬件、软件、虚拟机（VMs）、设施、人员、胜任力、能力和记录等清单。

各资产宜根据其相关的信息分级（见5.12）进行分级。

信息及其他相关资产清单的粒度宜达到符合组织需要的水平。有时会因资产的性质而无法对信息生存周期中的特定资产实例形成书面文件。短期资产的举例：生存周期持续较短的VM实例。

5.9.4.2 所有权

对于已识别的信息及其他相关资产，宜将资产的所有权分配给个人或团体并确定分级（见5.12、5.13）。宜实施确保及时分配资产所有权的过程。资产被创建或转移到组织时，宜分配其所有权。当前资产拥有者离职或调整工作角色时，宜根据需要重新分配资产所有权。

5.9.4.3 资产拥有者的职责

资产拥有者宜负责在整个资产生存周期内对资产进行适当管理，包括：

a) 对信息及其他相关资产进行登记造册；
b) 对信息及其他相关资产进行适当的分级和保护；
c) 定期审查分级情况；
d) 将支持技术资产的组件，如数据库、存储、软件组件和子组件等列出并建立关联；

e) 确立信息及其他相关资产可接受使用的要求（见 5.10）；
f) 与分级相符的访问限制生效，并定期审查；
g) 信息及其他相关资产在被删除或销毁时，以安全的方式进行处理，并从清单中移除；
h) 拥有者参与到与其资产相关的风险识别和管理中；
i) 拥有者向承担管理其信息的角色和责任的人员提供支持。

5.9.5 其他信息

信息及其他相关资产的清单通常是确保信息得到有效保护的必备要件，也可用于其他目的，如健康与安全、保险或财务等原因。信息及其他相关资产的清单还可用于支持风险管理、审计活动、脆弱性管理、事件响应和恢复计划。

任务和责任可以被委派（例如委派保管人负责资产的日常看管），但委派任务的人员或团体仍保留责任。

对协同工作提供特定服务的信息及其他相关资产建立分组是很有用的。在此情况下，服务拥有者对服务的交付以及相关资产的运行负责。

有关信息技术（IT）资产管理的更多信息，参见ISO/IEC 19770-1。有关资产管理的更多信息，参见ISO 55001。

5.10 信息及其他相关资产的可接受使用

5.10.1 属性表

信息及其他相关资产的可接受使用的属性表见表11。

表11 信息及其他相关资产的可接受使用属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#资产管理 #信息保护	#治理和生态体系 #防护

5.10.2 控制

宜识别、文件化并实现信息及其他相关资产的可接受使用规则和处理规程。

5.10.3 目的

确保信息及其他相关资产得到适当的保护、使用和处理。

5.10.4 指南

使用或可以访问组织信息及其他相关资产的工作人员和外部组织用户，宜知晓组织保护和处理信息及其他相关资产的信息安全要求。他们宜对其用到的任何信息处理设施的使用负责。

组织宜就信息及其他相关资产的可接受使用制定特定主题策略，并将其传达给使用或处理信息及其他相关资产的任何人。可接受使用的特定主题策略宜为个人如何使用信息及其他相关资产提供清晰的指导。特定主题策略宜声明：

a) 从信息安全角度指出个人的期望行为和不可接受行为；
b) 信息及其他相关资产的允许使用和禁止使用；
c) 组织所开展的监视活动。

宜根据信息的分级（见5.12）和已确定风险，为信息生存周期制定可接受的使用规程。宜考虑以下事项：

a) 支持各级分级保护要求的访问限制；
b) 对信息及其他相关资产的授权用户记录进行维护；
c) 信息的临时或永久副本保护达到与原始信息保护一致的水平，；
d) 根据制造商规范（见 7.8），存储与信息相关的资产；
e) 清楚标记存储媒体的所有副本（电子或物理副本）以提醒授权的接收人注意（见 7.10）；
f) 信息及其他相关资产处置的授权，以及支持的信息删除方法（见 8.10）。

5.10.5 其他信息

可能会出现相关资产不直接属于组织的情况，例如公有云服务。对于此类第三方资产以及与此类外部资产相关组织的任何资产（如信息、软件）的使用，宜识别确定为适用和受控情形，例如，通过与云服务提供者的协议实现使用。使用协作性工作环境时也需谨慎小心。

5.11 资产归还

5.11.1 属性表

资产归还的属性表见表12。

表12 资产归还属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#资产管理	#防护

5.11.2 控制

适宜时，工作人员和其他相关方在任用、合同或协议变更及终止时，宜归还其拥有的所有组织资产。

5.11.3 目的

将资产归还作为变更或终止任用、合同或协议过程的一部分，以保护组织的资产。

5.11.4 指南

变更或终止过程宜正式化，包括归还由组织拥有或委托给组织的、所有先前发放的实物资产和电子资产。如工作人员或其他相关方购买了组织的设备或使用了自己的个人设备，则宜遵守相关规程，确保所有相关

信息被追踪并移交给组织，同时从设备中安全删除（见7.14）。

如工作人员或其他相关方掌握的知识对持续运营非常重要，则这些信息宜形成文件并移交给组织。

在终止通知期间及后期，组织宜防止收到终止合同通知的工作人员对相关信息（例如，知识产权）的未经授权拷贝。

组织宜明确识别并记录所有待归还的信息及其他相关资产，包括：

a) 用户终端设备；
b) 便携式存储设备；
c) 专用设备；
d) 信息系统、场所和物理档案室所使用的鉴别硬件（例如，机械钥匙、物理令牌和智能卡）；
e) 信息的物理副本。

5.11.5 其他信息

对组织未拥有的资产，其上信息的归还可能是困难的。在这种情况下，有必要采用其他信息安全控制来限制信息的使用，诸如访问权管理（见5.18）或采用密码技术（见8.24）。

5.12 信息分级

5.12.1 属性表

信息分级的属性表见表13。

表13 信息分级属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#识别	#信息保护	#防护 #防御

5.12.2 控制

宜根据组织基于保密性、完整性、可用性的信息安全需求以及相关方的要求，对信息进行分级。

5.12.3 目的

确保根据信息对组织的重要性来识别并理解信息的保护需求。

5.12.4 指南

组织宜建立针对信息分级的特定主题策略，并将其传达给所有相关方。组织宜在分级方案中考虑保密性、完整性和可用性要求。

信息的分级及相关保护控制宜考虑到共享或限制信息、保护信息完整性并确保可用性的业务需求，以及有关信息保密性、完整性或可用性的法律要求。非信息类资产也可进行分级，并与该资产存储、处理或保护的信息的分级保持一致。

信息拥有者宜对其分级负责。

分级方案宜包括分级规则以及随时间推移对分级进行评审的准则。宜根据信息在其生存周期中的价值、敏感性和重要性的变化，对分级结果进行更新。

该方案宜与访问控制（见5.1）的特定主题策略保持一致，并能够满足组织的特定业务需求。

可根据信息损害对组织的影响程度来确定分级。宜对方案中定义的每个级别进行命名，以便给出在该分级方案应用环境中的含义。

该方案宜在整个组织内保持一致，并包含在组织规程中，以便所有人以相同的方式对信息及适用的其他相关资产进行分级。通过这种方式，所有人对保护要求有相同的理解，并应用适当的保护。

组织内部使用的分级方案，即使各级别的名称相似，也可能与其他组织使用的方案不同。此外，即使不同组织的分级方案完全相同，在组织之间传递的信息在分级上可能会有所不同，这取决于其在每个组织中的应用环境。因此，与其他组织达成的、涵盖信息共享的协议，宜包括相应的规程以识别该信息的分级和解释其他组织的信息分级级别。可通过寻找相关处理和保护方法的等效性，确定不同方案之间的对应关系。

5.12.5 其他信息

分级为处理信息的人员提供了如何处理和保护信息的简明指示。将有相似保护需求的信息分组，并规定适用于每个组中所有信息的信息安全规程，有助于分级。这一方法减少了逐项的风险评估和定制化控制设计的需求。

在一段时间后，信息可能不再是敏感或关键的。例如，当信息公开后，不再有保密性要求，但仍需保护信息的完整性和可用性。宜考虑因分级过度可能导致实施不必要的控制，从而增加成本，或反之，分级不足可能导致没有足够的控制来保护信息免受损害。

例如，信息保密性分级方案可以基于以下四个级别：

a) 泄露不会造成损害；
b) 泄露会对声誉造成轻微损害或对运行造成轻微影响；
c) 泄露会对运行或业务目标造成重大的短期影响；
d) 泄露会对长期业务目标造成严重影响，或使组织的生存面临风险。

5.13 信息标记

5.13.1 属性表

信息标记的属性表见表14。

表14 信息标记属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#信息保护	#防御 #防护

5.13.2 控制

宜按照组织采用的信息分级方案，制定并实施适当的信息标记规程。

5.13.3 目的

促进信息分级的沟通，并支持信息处理和管理的自动化。

5.13.4 指南

信息标记的规程宜包括所有格式的信息及其他相关资产。标记宜反映5.12中所建立的分级方案。标记宜易于识别。该规程宜考虑信息的访问方式或根据存储媒体类型对资产的处理方式，对标记的位置和方式给出指导。该规程可规定：

a) 可以省略标记的情形（例如，标记非保密信息，以减少工作量）；
b) 如何对通过电子或物理方式或任何其他格式发送或存储的信息进行标记；
c) 如何处理标记无法使用的情形（例如，因技术限制）。

标记技术的示例包括：

a) 物理标记；
b) 页眉和页脚；
c) 元数据；
d) 水印；
e) 橡皮图章。

数字信息宜利用元数据以便识别、管理和控制信息，尤其是在保密性方面。元数据还宜能够高效、正确地搜索信息。元数据宜有助于系统根据相关分级标记进行交互和决策。

该规程宜根据本组织的信息模型和ICT架构来说明如何将元数据附加到信息中，宜使用什么标记以及宜如何对数据进行处理。

系统在处理信息时宜根据其信息安全属性添加相关的附加元数据。

工作人员和其他相关方宜了解标记规程。宜向所有工作人员提供必要的培训以确保信息的正确标记和相应的处理。

当系统包含有分级为敏感或关键的信息时，该系统的输出宜带有适当的分级标记。

5.13.5 其他信息

对分级信息标记是实现信息共享的一个关键要求。

其他可附加在信息上有用的元数据是信息由组织的哪个过程创建以及何时创建的。

信息及相关资产的标记有时有负面作用。分级的资产容易被识别，从而由恶意行为者进行潜在的滥用。

一些系统不在单个文件或数据库记录上标记分级而是以其包含或允许包含的任何信息的最高级别来对所有信息加以保护。这类系统通常会在导出信息时自行确定并标记信息。

5.14 信息传输

5.14.1 属性表

信息传输的属性表见表15。

表15 信息传输属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#资产管理 #信息保护	#防护

5.14.2 控制

宜为组织内部以及组织与其他各方之间所有类型的传输设施，制定信息传输规则、规程或协议。

5.14.3 目的

维护在组织内以及组织与外部相关方之间传输的信息的安全。

5.14.4 指南

5.14.4.1 总则

组织宜建立并向所有相关方传达信息传输的特定主题策略。信息传输的规则、规程和协议宜反映所涉信息的分级。在组织和第三方之间传输信息时，宜建立并维护传输

协议（包括接收方身份验证），以保护通过使用各种类型通信设施进行的信息传输（见5.10）。

信息传输可以通过电子传输、物理存储媒体传输和口头传递来实现。对于所有类型的信息传输，其规则、规程和协议宜包括：

a) 保护传输的信息免遭截获、未经授权访问、复制、修改、错误路由、破坏和拒绝服务的控制，包括与所涉及信息分级相称的访问控制水平以及敏感信息所需的任何特殊控制，诸如使用加密技术（见 8.24）；
b) 确保可追溯性和不可抵赖性的控制，包括在传输过程中维护信息保管链；
c) 确定与传输相关的适当联系人，包括信息拥有者、风险拥有者、安全管理者和信息保管者（如适用）；
d) 发生信息安全事件（诸如物理存储媒体或数据丢失）时的责任和义务；
e) 为敏感或关键信息使用商定的标记系统，确保标记的含义被快速理解，信息得到适当的保护（见 5.13）；
f) 传输服务的可靠性和可用性；
g) 信息传输设施可接受使用的特定主题策略或指南（见 5.10）；
h) 包括消息在内的所有业务记录的保存和处置指南；

注：业务记录的留存保存和处置方面可能有当地法律法规的要求。

i) 考虑与信息传输相关的其他法律法规和合同要求（见 5.31、5.32、5.33、5.34），例如电子签名要求。

5.14.4.2 电子传输

使用电子通信设施进行信息传输的规则、规程和协议也宜考虑以下事项：

a) 检测和防止可能通过使用电子通信传输的恶意软件（见 8.7）；
b) 保护以附件形式传输的敏感电子信息；
c) 防止在通信中将文件和消息发送到错误的地址或号码；
d) 在使用诸如即时通信、社交网络、文件共享或云存储等外部公共服务之前取得批准；
e) 通过可公开访问的网络传输信息时采用级别更高的身份验证；
f) 与电子通信设施相关的限制（例如，防止自动将电子邮件转发到外部邮件地址）；
g) 建议工作人员和其他相关方不要发送带有关键信息的短消息服务（SMS）或即时消息，因为这些信息可能会在公共场所中被未经授权的人员读取，或存储在未得到充分保护的设备当中；
h) 告知工作人员和其他相关方与使用传真机或传真服务有关的问题，即：
   1) 未经授权访问内置消息存储以检索消息；
   2) 故意或意外地对机器进行编程，以将消息发送到特定的号码。

5.14.4.3 物理存储媒体的传输

传输物理存储媒体（包括纸张）时，相关规则、规程和协议还宜包括：

a) 控制和通知传输、发送和接收的责任；
b) 确保正确的寻址和消息传输；
c) 按照制造商规范，保护物理媒体中存储的信息免受传输过程可能产生的任何物理损坏，例如对可能会降低存储媒体恢复有效性的环境因素加以避免，诸如暴

露在高温、潮湿或电磁场中，使用包装和传输的最低技术标准（例如，使用不透明信封）；

d) 经管理者同意的、已授权的可靠传输企业名单；
e) 快递员的识别标准；
f) 根据存储媒体中要传输的信息分级级别使用防伪或防篡改控制装置（例如，袋子、容器）；
g) 核实快递员身份的规程；
h) 经批准的、可提供各级别信息的运输或快递服务的第三方名单；
i) 保管日志记录以识别存储媒体的内容、应用的保护情况，并记录授权收件人的列表、转移到中转保管人的时间和目的地的收据。

5.14.4.4 口头传递

为保护信息的口头传递，宜提醒工作人员和其他相关方：

a) 保密对话不得在公共场所或不安全的沟通渠道中进行，因为保密对话的内容可能会被未经授权的人员窃听；
b) 不得在电话答录机或语音消息当中留下包含保密信息的消息记录，因为这些消息记录可能会被未经授权的人员重播、存储在公共系统中或因误拨而被错误存储；
c) 通过适当程度的屏蔽来阻止其听到会谈内容；
d) 确保实施适当的访问控制（例如，隔音、关门）；
e) 开始任何敏感的谈话前，宜给出免责声明，这样在场人员即可明确自己将听到的内容的等级和处理要求。

5.14.5 其他信息

无其他信息。

5.15 访问控制

5.15.1 属性表

访问控制的属性表见表16。

表16 访问控制属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#身份和访问管理	#防护

5.15.2 控制

宜基于业务和信息安全要求，建立和实施信息及其他相关资产的物理和逻辑访问控制规则。

5.15.3 目的

确保对信息及其他相关资产的授权访问，并阻止未经授权的访问。

5.15.4 指南

信息及其他相关资产拥有者宜就其资产，确定与访问控制相关的信息安全和业务要求。宜制定考虑了这些要求的访问控制特定主题策略,并将其传达给所有相关方。

这些要求和特定主题策略宜考虑以下内容：

a) 确定哪些实体需要对信息和其他相关资产进行哪种类型的访问；
b) 应用程序安全（见 8.26）；
c) 物理访问，需要有适当的物理入口控制来支持（见 7.2、7.3、7.4）；
d) 信息传播和授权（例如，需要了解原则）以及信息安全级别和信息分级（见 5.10、5.12、5.13）；
e) 对特权访问的限制（见 8.2）；
f) 职责分离（见 5.3）；
g) 有关限制获取数据或服务的相关法律、法规和合同义务（见 5.31、5.32、5.33、5.34、8.3）；
h) 访问控制功能的分离（例如，访问请求、访问授权、访问管理）；
i) 访问请求的正式授权（见 5.16 和 5.18）；
j) 访问权的管理（见 5.18）；
k) 日志记录（见第 8.15）。

宜通过定义适当的访问权和限制并将其映射到相关实体来实施访问控制规则（见 5.16）。实体可以代表一个个人用户，也可以代表一个技术或逻辑项（例如，机器、设备或服务）。为简化访问控制管理，可将特定角色分配给实体组。

在定义和实施访问控制规则时，宜考虑以下因素：

a) 访问权和信息分级之间的一致性；
b) 访问权与物理周边安全需求和要求之间的一致性；
c) 考虑到分布式环境中所有类型的可用连接，因此实体只能访问其授权使用的信息及其他相关资产，包括网络和网络服务；
d) 考虑如何反映与动态访问控制相关的元素或因素。

5.15.5 其他信息

在访问控制环境中，通常会使用一些首要原则。最常用的两项原则为：

a) “按需知晓”原则：只允许实体被授权访问执行其任务所需的信息（不同任务或角色意味着不同的“按需所知”，从而有不同的访问配置）；
b) “按需使用”原则：只有在明确需要的情况下，实体才能被分配信息技术基础设施的访问权限。在规定访问控制规则时，宜考虑以下事项：
a) 在“未经明确允许，则一律禁止”的前提下建立规则，而不能在“未经明确禁止，一律允许”的弱规则的基础上建立规则；
b) 信息处理设施自动发起的信息标记变更（见 5.13）和用户自主发起的信息标记变更；
c) 信息系统自动发起的和由管理员发起的用户许可变更；
d) 何时定义并定期审查批准。

访问控制规则宜通过形成文件的规程（见5.16、5.17、5.18、8.2、8.3、8.4、8.5、8.18）和已定义的责任（见5.2、5.17）来支持。

有几种实施访问控制的方法，诸如MAC（强制访问控制）、DAC（自主访问控制）、RBAC（基于角色的访问控制）和ABAC（基于属性的访问控制）。

访问控制规则还可以包含动态元素（例如，评估过去访问或特定环境值的函数）。访问控制规则可以在不同细粒度下实施，从覆盖整个网络或系统到特定的数据字段，还可以考虑诸如用户位置或用于接入的网络连接的类型等属性。这些原则以及如何定义细粒度访问控制可能会产生重大的成本影响。更强的规则和更细的粒度通常会导致更高的成本。宜使用业务需求和风险因素来定义应用哪些访问控制规则和需要达到何种粒度。

5.16 身份管理

5.16.1 属性表

身份管理的属性表见表17。

表17 身份管理属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#身份和访问管理	#防护

5.16.2 控制

宜管理身份的全生存周期。

5.16.3 目的

对访问信息及其他相关资产的个人和系统进行唯一标识，并为其适当地分配访问权。

5.16.4 指南

用于身份管理环境的过程宜确保：

a) 对于分配给个人的身份，特定身份仅与个人相关联，使其对使用该特定身份执行的行为负责；
b) 分配给多人的身份（例如共享身份），仅在出于业务或运行需要时，且需经专门批准的情况下才允许使用；
c) 分配给非人实体的身份，须经过适当的分离的批准并接受独立的持续监督；
d) 如果不再需要身份，宜及时禁用或删除身份，例如删除或不再使用其关联的实体，或者与身份相关的人员已离开组织或更改了角色；
e) 在特定域中，单个标识映射单个实体，（即，避免在同一应用环境中多个标识映射到同一实体（重复身份））；
f) 保存与用户身份和鉴别信息使用和管理相关的所有重大事态的记录。

组织宜有支持处理与用户身份相关信息变更的过程。这些过程可以包括重新验证与身份相关的受信任文档。当使用由第三方提供或发布的身份（例如，社交媒体凭据）时，组织宜确保第三方身份提供所需的信任级别，已知晓并充分处置了相关风险。这可能包括与第三方有关的控制（见5.19）以及与鉴别信息相关的控制（见 5.17）。

5.16.5 其他信息

提供或撤销对信息及其他相关资产的访问通常是一个多步骤过程：

a) 为建立身份确认业务需求；
b) 为实体分配逻辑标识之前验证其标识；
c) 建立身份；
d) 配置和激活身份，同时包括相关鉴别服务的配置和初始设置；
e) 根据适当的授权或权利决定，提供或撤销对身份的特定访问权（见 5.18）。

5.17 鉴别信息

5.17.1 属性表

鉴别信息的属性表见表18。

表18 鉴别信息属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#身份和访问管理	#防护

5.17.2 控制

宜通过管理过程控制鉴别信息的分配和管理，包括向工作人员提供鉴别信息的适当处理建议。

5.17.3 目的

确保适当的实体鉴别，并防止鉴别过程失败。

5.17.4 指南

5.17.4.1 鉴别信息的分配

分配和管理过程宜确保：

a) 在注册过程中自动生成的个人口令或个人识别码（PIN）是临时秘密鉴别信息，都要确保其唯一性且不可预测性，用户在首次使用后需要对其进行更改；
b) 建立相关规程，以便在提供新的、替换的或临时的鉴别信息之前验证用户身份；
c) 鉴别信息包括临时鉴别信息，以安全的方式（例如，通过经鉴别和保护的通道）传输给用户并避免使用不受保护的（明文）电子邮件消息；
d) 用户确认收到鉴别信息；
e) 系统或软件安装后，立即变更厂商预定义或提供的默认鉴别信息；
f) 与鉴别信息分配和管理有关的重大事态宜留存记录并确保其保密性，记录保存的方法需得到批准（例如，通过使用批准的口令保险库）。

5.17.4.2 用户责任

宜对访问或使用鉴别信息的任何人员提出建议以确保：

a) 诸如口令等秘密鉴别信息均予以保密。个人秘密鉴别信息不得与任何人共享。关联到多个用户或非个人实体的秘密鉴别信息，仅在特定环境中使用，且只能与授权人共享；
b) 在收到损害通知或任何其他受损迹象后，立即变更受影响或受损的鉴别信息；
c) 当使用口令作为鉴别信息时，宜根据最佳实践建议选择强口令，例如：
   1) 口令不得基于别人容易猜测或获得的与使用人相关的信息（例如，姓名、电话号码和出生日期等）；
   2) 口令不得基于字典单词或其组合；
   3) 使用易于记忆的口令短语，尽量包含字母和特殊字符；
   4) 口令有最小长度；
d) 不同的服务和系统不使用相同的口令；
e) 在任用条款和条件中包含需遵守这些规则的义务（见 6.2）。

5.17.4.3 口令管理系统

当口令用作鉴别信息时，口令管理系统宜：

a) 允许用户选择和更改自己的口令，并包括确认规程，以解决输入错误；
b) 根据良好实践建议[见“用户责任”中 c）]强制执行强口令；
c) 强制用户在首次登录时更改口令；
d) 如有必要，强制更改口令，例如：在安全事件发生后，在任用关系终止或变更时，当用户知道仍处于活动状态身份（例如，共享身份）的口令时；
e) 防止重复使用旧口令；
f) 防止使用被黑客入侵的系统中常用的口令和受损的用户名、口令组合；
g) 输入时不在屏幕上显示口令；
h) 以受保护的形式存储和传输口令。

宜根据批准的口令加密技术进行口令的加密和散列（见8.24）。

5.17.5 其他信息

口令或口令短语是一种常用的鉴别信息，也是验证用户身份的常用方法。其他类型的鉴别信息包括加密密钥、存储在产生鉴别信息的硬件令牌（例如，智能卡）上的数据和诸如虹膜扫描或指纹等生物特征数据，更多信息可在ISO/IEC 24760系列标准中找到。

要求频繁变更口令可能会遇到问题，因为用户可能会对频繁变更口令而恼怒、会忘记新口令、会在不安全的地方写下口令或者选择不安全的口令。提供单点登录（SSO）或其他鉴别管理工具（例如，口令保险库）可以减少用户需要保护的鉴别信息量，从而提高控制的有效性。然而这些工具也会增加鉴别信息泄露的概率。

有些应用程序要求用户口令由独立机构分配。在此情况下，“口令管理系统”的a）、c）和d）不适用。

5.18 访问权

5.18.1 属性表

访问权的属性表见表19。

表19 访问权属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#身份和访问管理	#防护

5.18.2 控制

宜根据组织访问控制的特定主题策略和规则来提供、评审、修改和删除信息及其他相关资产的访问权。

5.18.3 目的

确保根据业务要求定义和授权对信息及其他相关资产的访问。

5.18.4 指南

5.18.4.1 访问权的提供和撤销

分配或撤销实体鉴别身份的物理和逻辑访问权时，提供过程宜包括：

a) 从信息及其他相关资产拥有者获得使用信息及其他相关资产的授权（见 5.9），管理者也可以单独批准访问权；
b) 考虑有关访问控制方面的业务需求和组织的特定主题策略和规则；
c) 考虑职责分离，包括分离批准和实施访问权的角色以及分离冲突角色；
d) 确保在不需要访问信息及其他相关资产时删除访问权，尤其要确保及时删除组织离职用户的访问权；
e) 考虑给予有限时间内的临时访问权，并在到期日撤销这些权利，尤其是临时工作人员或工作人员申请的临时访问权；
f) 验证授予的访问级别是否符合访问控制的特定主题策略（见 5.15），是否符合其他信息安全要求，诸如职责分离（见 5.3）；
g) 确保只有在成功完成授权程序后才能激活访问权（例如，由服务提供者激活）；
h) 维护访问权限的集中记录,记录为用户标识(逻辑 ID 或物理 ID)分配的访问信息及其他相关资产的权限；
i) 修改已变更角色或工作的用户的访问权；
j) 可以通过移除、撤销或替换密钥、鉴别信息来实现移除或调整物理和逻辑访问权；
k) 维护用户逻辑和物理访问权的变更记录。

5.18.4.2 访问权的审查

定期审查物理和逻辑访问权，宜考虑以下事项：

a) 在同一组织内发生任何变更（例如，工作变更、升职、降职）或终止任用关系（见 6.1 至 6.5）后的用户的访问权；
b) 特许访问权的授权。

5.18.4.3 变更或终止任用关系前的考虑

变更或终止任用关系前，宜根据对诸如以下风险因素的评估，审查、调整或删除用户对信息及其他相关资产的访问权：

a) 终止或变更是否由用户或管理者发起以及终止的原因；
b) 用户的当前责任；
c) 当前可访问资产的价值。

5.18.5 其他信息

宜考虑根据业务需求建立用户访问角色，将多个访问权限汇总为典型的用户访问配置文件。访问请求和访问权审查在此类角色级别比在特定权限级别更容易管理。

宜考虑在工作人员合同和服务合同中加入条款，规定如果工作人员试图进行未经授权的访问，将受到制裁（见5.20、6.2、6.4、6.6）。

在管理者发起终止聘用关系时，心怀不满的工作人员或外部用户可能会故意破坏信息或破坏信息处理设施。在有人辞职或被解雇时，他们可能会试图收集信息以供自己将来使用。

克隆是组织向用户分配访问权的有效方式，但宜根据不同角色谨慎进行，而不是仅仅克隆具有所有相关访问权的身份。克隆具有导致对信息及其他相关资产的过度访问权的固有风险。

5.19 供应商关系中的信息安全

5.19.1 属性表

供应商关系中的信息安全的属性表见表20。

表20 供应商关系中的信息安全属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#识别	#供应商关系安全	#治理和生态体系 #防护

5.19.2 控制

宜定义并实施过程和规程，以管理与供应商产品或服务使用相关的信息安全风险。

5.19.3 目的

维护供应商关系中信息安全的商定级别。

5.19.4 指南

组织宜建立关于供应商关系的特定主题策略，并向所有相关方传达。

组织宜确定并实施相关过程和规程，以解决供应商提供产品和服务使用时的相关安

全风险。同时，也宜适用于组织使用云服务提供者提供的资源。这些过程和规程宜包括由组织实施的过程和规程，以及组织在开始使用、终止使用供应商产品或服务时要求供应商实施的过程和规程），例如：

a) 确定并记录可能影响组织信息保密性、完整性和可用性的供应商类型（例如，ICT 服务、物流、公用事业、金融服务、ICT 基础设施组件）；
b) 建立如何根据信息、产品和服务的敏感性评价和选择供应商的方法（例如，通过市场分析、客户推荐、文件审查、现场评估、认证）；
c) 评估和选择具有充分信息安全控制的供应商产品或服务，并对其进行评审；尤其是供应商实施的控制的准确性和完整性，确保供应商信息和信息处理的完整性，从而确保组织的信息安全；
d) 定义组织的信息、ICT 服务以及供应商可以访问、监视、控制或使用的物理基础设施；
e) 确定供应商提供的、可能会影响组织信息的保密性、完整性和可用性的 ICT 基础设施组件和服务的类型；
f) 评价和管理与如下方面相关的信息安全风险：
    1) 供应商使用组织信息及其他相关资产，包括潜在的恶意供应商人员带来的风险；
    2) 供应商提供的产品（包括产品中使用的软件组件和子组件）或服务存在故障或漏洞；
g) 监视每种类型的供应商和访问类型是否符合已建立的信息安全要求，包括第三方审查和产品验证；
h) 通过监视或其他方式发现供应商的不合规时，缓解供应商的不合规风险；
i) 处理与供应商产品和服务相关的事件和应急状况，包括组织和供应商的双方责任；
j) 弹性以及（如有必要）恢复和应急措施，以确保供应商信息和信息处理的可用性，从而保证组织信息的可用性；
k) 根据供应商类型及其对组织系统和信息的访问级别，为与供应商人员接洽的组织人员进行适当的约定规则、特定主题策略、过程和规程以及行为准则的意识培训；
l) 管理信息、其他相关资产以及任何需要变更的信息的必要传输，以确保信息在整个传送期间的安全；
m) 确保安全终止供应商关系的要求，包括：
    1) 取消访问权；
    2) 信息处理；
    3) 确定合同期间开发的知识产权归属；
    4) 供应商变更或内包时的信息可移植性；
    5) 记录管理；
    6) 归还资产；
    7) 安全处置信息及其他相关资产；
    8) 持续保密要求；
n) 供应商人员及设施的人身安全和物理安全水平。

宜考虑在供应商无法提供其产品或服务（例如，由于事件、供应商不再营业或由于技术进步不再提供某些组件）的情况下继续信息处理的规程，以避免安排更换产品或服务的任何延迟（例如，提前确定替代供应商或始终使用替代供应商）。）

5.19.5 其他信息

如果组织无法向供应商提出要求时，该组织宜：

a) 在决定选择供应商及其产品或服务时，考虑本控制中给出的指导；
b) 根据风险评估实施必要的补偿控制。

信息安全管理不力的供应商可使信息处于风险之中。宜确定并应用控制来管理供应商对信息及其他相关资产的访问。例如，对信息的保密性有特殊需求，则可使用不泄露协议或加密技术。另一个例子是当供应商协议涉及到跨国界的信息传输或访问时的个人数据保护风险，此时组织需要意识到其仍负有信息保护的法律或合同责任。

对供应商提供的ICT基础设施组件或服务控制不充分也可能造成风险。故障或易受攻击的组件或服务可能造成组织或其他实体的信息安全违规（例如，它们可能会对组织以外的实体造成恶意软件感染、攻击或其他伤害）。详见ISO/IEC 27036-2。

5.20 在供应商协议中强调信息安全

5.20.1 属性表

在供应商协议中强调信息安全的属性表见表21。

表21 在供应商协议中强调信息安全属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#识别	#供应商关系安全	#治理和生态体系 #防护

5.20.2 控制

宜根据供应商关系的类型建立相关的信息安全要求，并与每个供应商达成一致。

5.20.3 目的

维护供应商关系中信息安全的商定级别。

5.20.4 指南

宜建立供应商协议并形成文件，以确保组织和供应商双方明确履行相关信息安全要求的义务上不存在误解。为满足已识别的信息安全协议要求，可以在协议中考虑以下条款：

a) 对要提供或访问的信息的描述，以及提供或访问信息的方法；
b) 根据组织分级方案对信息进行分级（见 5.10、5.12、5.13）；
c) 在组织自身的分级方案和供应商的分级方案之间建立映射关系；
d) 法律法规和合同要求，包括数据保护、个人可识别信息（PII）、知识产权和版权的处理，以及对如何确保满足这些要求的描述；
e) 合同各方实施已商定控制的义务，包括访问控制、性能评审、监视、报告和审核以及供应商履行组织信息安全要求的义务；
f) 信息及其他相关资产的可接受使用规则，必要时，包括不可接受的使用；

g) 供应商人员使用组织信息及其他相关资产的授权和取消授权的规程或条件（例如，给出被授权使用组织信息及其他相关资产的供应商人员的明确名单）；
h) 关于供应商 ICT 基础设施的信息安全要求；特别是将每种类型的信息和访问类型的最低信息安全要求，作为基于组织业务需求和风险准则的单个供应商协议的基础；
i) 承包商未能满足要求的赔偿和补救；
j) 事件管理要求和规程（尤其是在事件补救过程中的通知和协作）；
k) 具体规程以及信息安全要求的培训和意识要求（例如，事件响应、授权规程）；
l) 关于分包的相关规定，包括需要实施的控制，诸如使用分包商的协议等（例如，供应商要求分包商履行与其相同的义务，维护分包商名单并在任何变更前进行通知）；
m) 相关联系人，包括信息安全问题联系人；
n) 在法律允许的情况下，对供应商人员的任何筛选要求，包括执行筛选的责任，以及当筛选未完成或者出现令人疑问或关注的结果时的通告规程；
o) 第三方证明与供应商过程相关的信息安全要求的证据和保障机制，以及关于控制有效性的独立报告；
p) 对与协议相关的供应商过程和控制进行审核的权利；
q) 供应商有义务定期递交控制有效性的独立报告，并同意及时纠正报告中提出的有关问题的协议；
r) 缺陷解决和争执解决过程；
s) 提供符合组织需求的备份（在周期、类型和存储位置方面）；
t) 确保备用设施（即灾难恢复场所）的可用性不会受到与主设施相同的威胁，并在主控制失效时考虑后备控制（备用控制）；
u) 具备变更管理过程，确保提前通知组织以及组织有不接受变更的可能；
v) 与信息分级相称的物理安全控制；
w) 在物理传输或逻辑传输期间，保护信息的信息传输控制；
x) 协议签订后的终止条款，包括记录管理、资产返还、信息及其他相关资产的安全处置以及任何持续的保密义务；
y) 对存储在供应商的组织信息，一旦不再需要则提供一种安全销毁的方法；
z) 在协议终止时，供应商确保向其他供应商或组织自身提供交割支持。

组织宜建立并维护与外部各方的协议登记册（例如，合同、谅解备忘录、信息共享协议），以跟踪其信息去向。组织还宜定期评审、验证和更新其与外部各方的协议，确保这些协议仍必要且符合相关信息安全条款的目的。

5.20.5 其他信息

不同组织和不同类型供应商的协议可能有很大差异。因此，宜注意包含所有相关的应对信息安全风险的要求。

有关供应商协议的详细信息，请参阅ISO/IEC 27036系列标准。有关云服务协议，请参阅ISO/IEC 19086系列标准。

5.21 管理信息通信技术供应链中的信息安全

5.21.1 属性表

管理信息通信技术供应链中的信息安全的属性表见表22。

表22 管理信息通信技术供应链中的信息安全属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#识别	#供应商关系安全	#治理和生态体系 #防护

5.21.2 控制

宜定义并实施过程和规程，以管理与ICT产品和服务供应链相关的信息安全风险。

5.21.3 目的

维护供应商关系中信息安全的商定级别。

5.21.4 指南

除对供应商关系的一般信息安全要求外，还宜考虑以下主题，以解决ICT供应链安全中的信息安全问题：

a) 确定适用于 ICT 产品或服务获取的信息安全要求；
b) 若供应商分包组织的部分 ICT 服务，则要求供应商在整个 ICT 供应链中宣贯组织的安全要求；
c) 若这些 ICT 产品包括从其他供应商或其他实体购买或获得的组件，则要求 ICT 产品供应商在整个供应链中宣贯适当的安全实践（例如，分包的软件开发商和硬件组件提供者）；
d) 要求 ICT 产品供应商提供描述产品使用软件组件的信息；
e) 要求 ICT 产品供应商提供信息，描述其产品实现的安全功能及其安全运行所需的配置；
f) 实施监视过程和可接受的方法，以确认交付的 ICT 产品和服务遵守了规定的安全要求。此类供应商审查方法的示例可包括渗透测试和对供应商信息安全活动的第三方证明或验证；
g) 实施一个过程来识别和记录对维护功能至关重要的产品或服务组件，并当这些产品或服务组件在组织外部构建时，尤其是如果总供应商将产品或服务组件的某些部分分包至其他供应商时，需要更多的关注和进一步跟进；
h) 获得关键组件及其来源在整个供应链可追溯的保障；
i) 获得对交付的ICT 产品按预期工作无任何意外或不需要功能的保障；
j) 实施过程以确保供应商提供的组件为正品，且未改变其规格。示例措施包括防篡改标记、加密哈希验证或数字签名。通过监视不合规格的性能指标，可判定篡改或假冒的组件。宜在系统开发生存周期的多个阶段（包括设计、开发、集成、运行和维护）实施篡改的预防和检测；
k) 获得 ICT 产品达到所需的安全水平的保障，例如，通过正式认证或评价；
l) 定义组织和供应商之间有关供应链和任何潜在问题及损害的信息共享规则；
m) 实施管理 ICT 组件生存周期、可用性和相关安全风险的具体过程，包括管理

因供应商不再经营导致组件不可用的风险或因技术进步供应商不再提供这些组件的风险。宜考虑确定替代供应商以及将软件和能力转移给替代供应商的过程。

5.21.5 其他信息

特定的ICT供应链风险管理实践是建立在一般的信息安全、质量、项目管理和系统工程实践之上，而不是取而代之。

建议组织与供应商合作，以知晓ICT供应链以及对所提供产品和服务有重要影响的任何事项。组织通过在与供应商的协议中明确在ICT供应链中宜由其他供应商解决的问题，可影响ICT供应链的信息安全实践。

ICT宜从信誉良好的来源获得。软件和硬件的可靠性属于质量控制问题。虽然组织通常不可能检查其厂商的质量控制体系，但可以根据厂商的声誉做出可靠的判断。

这里的ICT供应链包括云服务。ICT供应链示例如下：

a) 云服务供应，云服务提供者依赖软件开发商、电信服务提供者、硬件提供者；
b) 物联网，其中服务涉及设备制造商、云服务提供者（例如，物联网平台运营商）、移动和网络应用程序开发商、软件库厂商；
c) 托管服务，提供者依赖外部服务台，包括一线、二线和三线支持级别。更多详细信息，包括风险评估指南，参见ISO/IEC 27036-3。

软件标识（SWID）标记还可通过提供有关软件来源的信息，帮助在供应链中实现更好的信息安全。更多详情参见ISO/IEC 19770-2。

5.22 供应商服务的监视、评审和变更管理

5.22.1 属性表

供应商服务的监视、评审和变更管理的属性表见表23。

表23 供应商服务的监视、评审和变更管理属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#识别	#供应商关系安全 #信息安全保障	#治理和生态体系 #防护 #防御

5.22.2 控制

组织宜定期监视、评审、评价和管理供应商信息安全实践和服务交付的变更。

5.22.3 目的

维护供应商协议中规定的信息安全和服务交付的商定级别。

5.22.4 指南

供应商服务的监视、评审和变更管理宜确保遵守协议中的信息安全条款和条件，妥

善管理信息安全事件和问题，且供应商服务或业务状态的变更不会影响服务交付。

这宜包括管理组织和供应商之间关系的过程，以：

a) 监视服务性能水平以验证对协议的符合程度；
b) 监视供应商做出的变更包括：
   1) 对当前提供服务的加强；
   2) 任何新的应用程序和系统的开发；
   3) 供应商策略和规程的修正或更新；
   4) 新的或变更的控制以解决信息安全事件并提高信息安全。
c) 监视供应商服务的变更，包括：
   1) 网络的变更和强化；
   2) 新技术的应用；
   3) 新产品或更新版本/发行的采用；
   4) 新工具和环境的开发；
   5) 服务设施物理位置的变更；
   6) 分包商的变更；
   7) 分包给其他供应商。
d) 评审供应商提交的服务报告，并按照协议要求安排定期进度会议；
e) 对供应商和及其分包商进行审核，同时评审独立审计师的报告（如有），对所发现的问题进行追踪；
f) 提供有关信息安全事件的信息，并按照协议及任何支持指南和规程的要求评审该信息；
g) 评审供应商对与所提供服务相关的信息安全事态、操作问题、失效、故障和中断追溯的审计痕迹和记录；
h) 响应和管理任何已识别的信息安全事态或事件；
i) 识别并管理信息安全漏洞；
j) 评审供应商与其自身供应商关系上的信息安全方面；
k) 确保供应商保持足够的服务能力，并制定可行的计划，以确保在发生重大服务故障或灾难后保持商定的服务连续性级别（见 5.29、5.30、5.35、5.36、8.14）；
l) 确保供应商分配审查合规性和执行协议要求的责任；
m) 定期评估供应商是否维持足够的信息安全水平。

宜将管理供应商关系的责任分配给指定的个体或团队。宜提供足够的技术技能和资源，以监视协议的要求，尤其是信息安全要求是否得到满足。当发现服务交付中存在缺陷时，宜采取适当措施。

5.22.5 其他信息

详见ISO/IEC 27036-3。

5.23 云服务使用的信息安全

5.23.1 属性表

云服务使用的信息安全的属性表见表24。

表24 云服务使用的信息安全属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#供应商关系安全	#治理和生态体系 #防护

5.23.2 控制

宜根据组织的信息安全要求，建立云服务的获取、使用、管理和退出过程。

5.23.3 目的

确立并管理云服务使用的信息安全。

5.23.4 指南

组织宜建立云服务使用的特定主题策略，并向所有相关方传达。

组织宜明确并沟通将如何管理与云服务使用相关的信息安全风险，它可以是组织如何管理外部方提供服务的现有方法的一部分或扩展（见5.21和5.22）。

云服务的使用可能涉及云服务提供者和作为云服务客户的组织间的信息安全责任共担和协作。恰当地界定和落实云服务提供者和作为云服务客户的组织的责任是至关重要的。

组织宜定义：

a) 所有与云服务使用相关的信息安全要求；
b) 云服务选择准则和云服务使用范围；
c) 与云服务的使用和管理相关的角色和职责；
d) 哪些信息安全控制由云服务提供者管理，以及哪些信息安全控制由作为云服务客户的组织管理；
e) 如何获取和利用云服务提供者提供的信息安全能力；
f) 如何获得对云服务提供者实施的信息安全控制的保证；
g) 当一个组织使用多个云服务，尤其是来自不同云服务提供者的服务时，如何管理服务中的控制、接口和变更；
h) 处理与使用云服务使用有关的信息安全事件的规程；
i) 以监视、审查和评估云服务持续使用的方法管理信息安全风险；
j) 如何改变或停止使用云服务，包括云服务的退出策略。

云服务协议通常是预定义且不开放协商。对于所有云服务，组织宜与云服务提供者审查云服务协议。云服务协议宜满足组织的保密性、完整性、可用性和信息处理的要求，并具有适当的云服务级别目标和云服务质量目标。组织还宜进行相关风险评估，以识别与使用云服务相关的风险。与使用云服务相关的任何剩余风险都宜被明确识别，并被组织合适的管理者接受。

云服务提供者与作为云服务客户的组织间的协议，宜包括以下保护组织数据和服务

可用性的规定：

a) 按照行业公认的架构和基础设施标准提供解决方案；
b) 管理云服务的访问控制，以满足组织的要求；
c) 实施恶意软件监视和保护方案；
d) 在获批的地点（例如特定国家或地区）或特定管辖区内/受特定管辖区管辖的地方处理和存储组织的敏感信息；
e) 在云服务环境中发生信息安全事件时提供专门支持；
f) 确保在云服务分包给外部供应商（或禁止分包云服务）的情况下，满足组织的信息安全要求；
g) 支持组织收集数字证据，同时考虑不同司法管辖区的数字证据法律法规；
h) 当组织想要退出云服务时，在适当的时间范围内提供适当的支持和可用性的服务；
i) 作为云服务客户的组织基于其使用的云服务提供者的能力，提供所需的数据和配置信息备份，并安全地管理备份使其可用；
j) 作为云服务客户的组织，要求云服务提供者在服务提供期间或服务终止时，提供并退回自己的信息，如配置文件、源代码和数据等。

作为云服务客户的组织，宜考虑该协议是否要求云服务提供者在对服务交付方式作出任何具有实质性影响的变更之前，提前进行通知，包括：

a) 技术基础设施变更，影响或改变云服务产品（如重新定位、重新配置或硬件/软件变更）；
b) 在新的地理或法律管辖区处理或存储信息；
c) 使用对等云服务提供者或其他分包商（包括变更现有或使用新的相关方合作商）。

使用云服务的组织宜与其云服务提供者保持密切联系，联系人可为云服务的使用相互交换有关信息安全的信息，包括云服务提供者机制和作为云服务客户的组织机制，监视每个服务特征并报告协议中未能履行的承诺。

5.23.5 其他信息

此控制从云服务客户的角度考虑云安全。

有关云服务的更多信息，参见ISO/IEC 17788、ISO/IEC 17789和ISO/IEC 22123-1。有关支持退出策略的云可移植性的详细信息，参见ISO/IEC 19941。ISO/IEC 27017中描述了与信息安全和公有云服务相关的细节。有关充当PII处理器的公有云中PII保护的详细信息，参见ISO/IEC 27018。ISO/IEC 27036-4和云服务协议涵盖了云服务的供应商关系，其内容在ISO/IEC 19086系列中进行了处理，ISO/IEC 19086-4专门涵盖了安全和隐私。

5.24 信息安全事件管理规划和准备

5.24.1 属性表

信息安全事件管理规划和准备的属性表见表25。

表25 信息安全事件管理规划和准备属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#纠正	#保密性 #完整性 #可用性	#响应 #恢复	#治理 #信息安全事态管理	#防御

5.24.2 控制

组织宜通过定义、建立和传达信息安全事件管理过程、角色和责任，规划和准备管理信息安全事件。

5.24.3 目的

确保快速、有效、持续且有序的应对信息安全事件，包括信息安全事态的沟通。

5.24.4 指南

5.24.4.1 角色和职责

组织宜建立适当的信息安全事件管理过程。宜确定执行事件管理规程的角色和责任，并将其有效传达给内部和外部相关方。

宜考虑以下几点：

a) 建立报告信息安全事态的通用方法，包括联络点（见 6.8）；
b) 建立事件管理过程，为组织提供管理信息安全事件的能力，包括管理、记录、检测（发现）、鉴别分类、优先级划分、分析、沟通和协调相关方；
c) 建立事件响应过程，为组织提供评估、响应信息安全事件，并从信息安全事件中获取经验的能力；
d) 只允许有能力的人员在组织内处理与信息安全事件相关的问题。宜向此类人员提供规程文件和定期培训；
e) 建立事件响应人员所需培训、认证和持续专业发展的识别流程。

5.24.4.2 事件管理规程

宜与管理者就信息安全事件管理目标达成一致，并宜确保负责信息安全事件管理的人员了解组织处理信息安全事件的优先事项，包括基于潜在后果和严重程度的解决时间框架。宜实施事件管理规程，以实现这些目标和优先事项。

管理者宜确保根据不同场景为以下活动制定和实施信息安全事件管理计划，建立和实施信息安全事件管理规程：

a) 根据构成信息安全事件的标准评估信息安全事态；
b) 信息安全事态和事件的监测（见 8.15 和 8.16）、检测（见 8.16）、分级（见 5.25）、分析和报告（见 6.8）（通过人工或自动方式）；
c) 根据事件的类型和类别，管理信息安全事件，包括响应和升级（见 5.26），可能启动危机管理和连续性计划，从事件可控恢复以及与内部和外部相关方的沟通；

d) 与内部和外部相关方的协调，如政府机构、外部利益团体和论坛、供应商和客户（见 5.5 和 5.6）；
e) 记录事件管理活动；
f) 证据处理（见 5.28）；
g) 根本原因分析或事后经验总结的规程；
h) 确定经验教训，以及对事件管理规程或一般信息安全控制所需的任何改进。

5.24.4.3 报告规程

报告规程宜包括：

a) 发生信息安全事态时采取的行动（如立即记录发生的故障和屏幕上的信息等所有相关细节，立即向联络点报告并仅采取协调的行动）；
b) 使用事件表来支持人员在报告信息安全事件时所有必要的行动；
c) 以适当的反馈过程确保信息安全事态报告人员在问题被处理完毕后，尽可能地得到结果的通知；
d) 创建事件报告。

在实施事件管理规程时，宜考虑在规定的时间范围内向相关方报告事件的任何外部要求（如违反监管机构通知的要求）。

5.24.5 其他信息

信息安全事件可以跨越组织和国家边界。为了应对此类事件，协调应对措施并酌情与外部组织分享有关这些事件的信息是有益的。

ISO/IEC 27035系列标准中提供了有关信息安全事件管理的详细指南。

5.25 信息安全事态的评估和决策

5.25.1 属性表

信息安全事态的评估和决策的属性表见表26。

表26 信息安全事态的评估和决策属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#检测	#保密性 #完整性 #可用性	#发现 #响应	#信息安全事态管理	#防御

5.25.2 控制

组织宜评估信息安全事态，并决定是否将其归类为信息安全事件。

5.25.3 目的

确保信息安全事态的有效分类和优先级分级。

5.25.4 指南

宜商定信息安全事件的分类和优先级方案，以确定事件的后果和优先级。该方案宜包括将事态定性为信息安全事件的标准。联系人宜使用商定的方案评估每个信息安全事态。

负责协调和应对信息安全事件的人员宜对信息安全事态进行评估并做出决定。评估和决定的结果宜详细记录，以供将来参考和核实。

5.25.5 其他信息

ISO/IEC 27035系列标准为事件管理提供了进一步的指导。

5.26 信息安全事件的响应

5.26.1 属性表

信息安全事件的响应的属性表见表27。

表27 信息安全事件的响应属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#纠正	#保密性 #完整性 #可用性	#响应 #恢复	#信息安全事态管理	#防御

5.26.2 控制

宜按照文件化的规程响应信息安全事件。

5.26.3 目的

确保信息安全事件响应的效率和效果。

5.26.4 指南

组织宜建立信息安全事件响应规程，并将其传达给所有相关方。信息安全事件宜由具有所需能力的指定团体响应（见5.24）。 响应宜包括以下内容：

a) 如果事件的后果可能蔓延，则需要将受事件影响的系统纳入响应范围；
b) 事件发生后尽快收集证据（见 5.28）；
c) 按要求上报，包括危机管理活动，并调用业务连续性计划（见 5.29 和 5.30）；
d) 确保所有相关的响应活动都已正确记录，以备日后分析；
e) 按照知情需要原则，将信息安全事件的存在或任何相关细节告知所有相关的内部和外部相关方；
f) 与内部和外部各方协调，如政府机构、外部利益团体和论坛、供应商和客户，以提高响应效率，并帮助将对其他组织的影响降至最低；
g) 事件一旦处理完毕，正式将其关闭并记录；

h) 按要求进行信息安全取证分析（见 5.28）；
i) 进行事后分析，以确定根本原因。确保按照规定的规程进行记录和沟通（见 5.27）；
j) 识别和管理信息安全脆弱性和弱点，包括导致、促成或未能预防事件的控制的脆弱性和弱点。

5.26.5 其他信息

ISO/IEC 27035系列标准为事件管理提供了进一步的指导。

5.27 从信息安全事件中学习

5.27.1 属性表

从信息安全事件中学习的属性表见表28。

表28 从信息安全事件中学习属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#识别 #防护	#信息安全事态管理	#防御

5.27.2 控制

宜使用从信息安全事件中得到的知识来加强和改进信息安全控制。

5.27.3 目的

减少未来事件发生的可能性或影响。

5.27.4 指南

组织宜建立规程来量化和监控信息安全事件的类型、数量和成本。从信息安全事件评估中获得的信息宜用于：

a) 加强事件管理计划，包括事件场景和规程（见 5.24）；
b) 确定反复发生或后果严重事件及其原因，以更新组织的信息安全风险评估，并确定和实施必要的额外控制，以降低未来类似事件的发生的可能性或后果。实现这一目标的机制包括收集、量化和监控有关事件类型、数量和成本的信息；
c) 通过提供可能发生的事件、如何响应此类事件以及如何在未来避免类似安全事件的案例，增强用户意识和培训（见 6.3）。

5.27.5 其他信息

ISO/IEC 27035系列标准提供了进一步的指导。

5.28 证据收集

5.28.1 属性表

证据收集的属性表见表29。

表29 证据收集属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#纠正	#保密性 #完整性 #可用性	#发现 #响应	#信息安全事态管理	#防御

5.28.2 控制

组织宜建立并实施（implement）包括识别、收集、获取和保存信息安全事态相关证据的规程。

5.28.3 目的

确保对与信息安全事件相关的证据进行持续一致和有效的管理，以便纪律惩戒和法律处罚。

5.28.4 指南

为纪律惩戒和法律处罚的目的而处理信息安全事态的相关证据时，宜制定相应的内部规程并遵守。宜考虑不同司法管辖区的要求差异，以尽可能获得相应司法管辖区对证据的认可。

一般地，证据管理规程宜针对不同类型的存储媒体、设备和设备状态（即通电或断电）提供证据识别、收集、获取和保存的操作说明。证据尤其需要以一种适当的国家法院或其他纪律法庭能认可的方式收集。宜可以证明：

a) 记录完整，未被篡改；
b) 电子证据的副本与原件完全一致；
c) 收集证据的信息系统在记录证据时运行正常。

对证据收集人员和证据收集工具尽可能要求有资格证书或其他相关资格认证方式，以增强保存的证据的法律效力。

数字证据可能超出组织的或管辖的边界。在此情况下，宜确保组织有权收集作为数字证据所需的信息。

5.28.5 其他信息

当首次检测到信息安全事态时，其是否会导致法庭诉讼并不总是很明显。因此，在事件的严重性表现出来之前，存在故意或意外销毁必要证据的可能性。在任何预期的法律行动中尽早包含法律建议或执法行为，并就所需证据听取意见是明智的。

ISO/IEC 27037提供了识别、收集、获取和保存数字证据的定义和指南。 ISO/IEC 27050系列指导电子发现，包括将电子存储的信息作为证据进行的处理。

5.29 中断期间的信息安全

5.29.1 属性表

中断期间的信息安全的属性表见表30。

表30 中断期间的信息安全属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防 #纠正	#保密性 #完整性 #可用性	#防护 #响应	#连续性	#防护 #弹性

5.29.2 控制

组织宜制定在中断期间将信息安全维持在适当级别的计划。

5.29.3 目的

在中断期间保护信息及其他相关资产。

5.29.4 指南

组织宜确定在中断期间对信息安全控制的调整需求。信息安全需求宜包含在业务连续性管理过程中。

宜制定、实施、测试、审查和评估计划，以在破坏或故障后维护或恢复关键业务过程信息的安全性。信息安全宜在要求的时间内恢复到相应等级。

组织宜建立并维护：

a) 业务连续性和ICT连续性计划中的信息安全控制、支持系统和工具；
b) 中断期间维护现有信息安全控制的过程；
c) 对中断期间无法维持的信息安全控制的补偿性控制。

5.29.5 其他信息

在业务连续性和ICT连续性计划方面，与正常运行条件相比，可能有必要根据中断类型调整信息安全要求。作为在业务连续性管理中实施的业务影响分析和风险评估的一部分，除了维护可用性的需求外，还宜考虑和优先应对信息的保密性和完整性遭损的后果。

有关业务连续性管理系统的信息，参见ISO 22301和ISO 22313。有关业务影响分析（BIA）的进一步指导，参见ISO/TS 22317。

5.30 业务连续性的信息通信技术就绪

5.30.1 属性表

业务连续性的信息通信技术就绪的属性表见表31。

表31 业务连续性的信息通信技术就绪属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#纠正	#可用性	#响应	#连续性	#弹性

5.30.2 控制

宜根据业务连续性目标和ICT连续性要求，计划、实施、维护和测试ICT的就绪。

5.30.3 目的

确保组织的信息及其他相关资产在中断期间的可用性。

5.30.4 指南

业务连续性的信息通信技术就绪是业务连续性管理和信息安全管理的重要组成部分，以确保在中断期间继续完成组织的目标。

ICT连续性需求是业务影响分析（BIA）的结果。BIA过程宜使用影响类型和准则来评估交付产品和服务的业务活动中断带来的后续影响。影响的大小和持续时间用于确定宜分配给优先活动的恢复时间目标（RTO）。BIA随后宜确定支持优先活动所需的资源。还宜为这些资源指定RTO。这些资源的一个子集宜包括ICT服务。

涉及ICT服务的BIA可以扩展为确定ICT系统的性能与容量要求，以及在中断期间支持活动所需的信息恢复点目标（RPO）。

基于BIA的输出和涉及ICT服务的风险评估，组织宜识别和选择ICT连续性策略，仔细考虑中断前、中断期间和中断后的选项。业务连续性策略可以包括一个或多个解决方案。根据这些策略，宜制定计划，并实施和测试，以在关键过程中断或失效后的规定时间内达到ICT服务的可用性水平要求。

组织宜确保有：

a) 由具有必要的职责、权威性和能力的人员支持的合适的组织架构，为中断做准备，减轻和应对中断；
b) ICT连续性计划，包括详细说明组织计划如何管理 ICT 服务中断的响应和恢复规程：
   1) 通过演练和测试进行定期评估；
   2) 经管理者批准；
c) ICT 连续性计划包含以下ICT 连续性信息：
   1) 达到 BIA 中规定的业务连续性要求和目标的性能和容量规格；
   2) 每个优先的 ICT 服务的 RTO 和恢复这些组件的规程；
   3) 定义为信息的优先 ICT 资源的 RPO 和恢复信息的规程。

5.30.5 其他信息

考虑可用性时，ICT连续性管理是业务连续性要求的一个关键部分，以：

a) 无论何种原因导致的ICT服务中断都应得到响应，并从中恢复；
b) 确保优先活动的连续性得到所需ICT服务的支持；
c) 在ICT服务中断前，并检测到至少一个可能导致 ICT 服务中断的事件时，作出响应。ISO/IEC 27031提供了有关业务连续性ICT就绪的进一步指导。

有关业务连续性管理体系的更多指导，参见ISO 22301和ISO 22313。有关BIA的更多指导，参见ISO/TS 22317。

5.31 法律、法规、规章和合同要求

5.31.1 属性表

法律、法规、规章和合同要求的属性表见表32。

表32 法律、法规、规章和合同要求属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#识别	#合法合规	#治理和生态体系 #防护

5.31.2 控制

宜识别、文件化和保持更新与信息安全相关的法律、法规、规章和合同要求，以及组织满足这些要求的方法。

5.31.3 目的

确保遵守与信息安全相关的法律、法规、规章和合同要求。

5.31.4 指南

5.31.4.1 总则

在以下情况，宜考虑外部要求，包括法律、法规、规章或合同要求：

a) 制定信息安全策略和规程；
b) 设计、实施或变更信息安全控制；
c) 将信息和其他相关资产分类，作为为内部需求或供应商协议设置信息安全要求的过程的一部分；
d) 进行信息安全风险评估，确定信息安全风险应对活动；
e) 确定与信息安全相关的过程及相关的角色和职责；
f) 确定与组织相关的供应商合同要求以及产品和服务的供应范围。

5.31.4.2 法律和法规

组织宜：

a) 识别与组织信息安全相关的所有法律和法规，以明确其业务类型的要求；
b) 考虑所有相关国家的合规性，如果组织：
   - 在其他国家开展业务；
   - 使用产品和服务来自其法律法规可能影响组织的其他国家；
   - 传输信息跨过可能影响组织的法律法规管辖边界。
c) 定期审查已识别的法律和法规，以保持更新和识别新的法律；
d) 定义并文件化满足这些要求的具体过程和个人职责。

5.31.4.3 密码技术

密码技术是经常有特定法律要求的领域。宜考虑遵守与下列有关的协议、法律和法规：

a) 对用于执行密码功能的计算机硬件和软件的进口或出口限制；
b) 对设计为可增加密码功能的计算机硬件和软件的进口或出口限制；
c) 对密码技术使用的限制；
d) 各国管理部门规定的对加密信息的强制性或自主性的访问方法；
e) 数字签名、印章和证书的有效性。

建议为确保遵守相关法律法规时寻求法律咨询，尤其是加密信息或密码工具跨过司法管辖边界移动时。

5.31.4.4 合同

与信息安全相关的合同要求宜包括：

a) 与客户的合同；
b) 与供应商的合同（见 5.20）；
c) 保险合同。

5.31.5 其他信息

无其他信息。

5.32 知识产权

5.32.1 属性表

知识产权的属性表见表33。

表33 知识产权属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#识别	#合法合规	#治理和生态体系

5.32.2 控制

组织宜实现适当的规程来保护知识产权。

5.32.3 目的

确保遵守与知识产权和专利产品使用相关的法律、法规、规章和合同要求。

5.32.4 指南

宜考虑以下准则，以保护任何可被视为知识产权的材料：

a) 定义和传达关于保护知识产权的专题策略；
b) 发布知识产权合规规程以定义软件和信息产品的合规使用；
c) 仅通过已知和信誉良好的来源获取软件，以确保不侵犯版权；
d) 维护适当的资产登记簿，识别所有有知识产权保护要求的资产；
e) 保留许可证、手册等所有权的证明和证据；
f) 确保用户数或资源的最大数量[例如，中央处理器（CPU）数]不超过许可证许可数；
g) 进行审查，确保只安装授权软件和许可产品；
h) 提供维持适当许可条件的规程；
i) 提供处置软件或将软件转让给他方的规程；
j) 遵守从公共网络和外部来源获取的软件和信息的使用条款和条件；
k) 未经版权法或适用许可证允许，不得复制、转换为其他格式或从商业记录（视频、音频）中提取；
l) 未经版权法或适用许可证允许，不得复制全部或部分标准（如 ISO/IEC 国际标准）、书籍、文章、报告或其他文件。

5.32.5 其他信息

知识产权包括软件或文档版权、设计权、商标、专利和源代码许可。

专利软件产品通常根据许可协议提供，该协议规定了许可条款和条件，如，将产品的使用限制在指定的机器上，或将复制限制为仅创建备份副本。有关IT资产管理的详细信息，请参阅ISO/IEC 19770系列。

数据可以从外部来源获得。通常情况下，此类数据是根据数据共享协议或类似法律文书的条款获得的。此类数据共享协议宜明确允许对获取的数据进行何种处理。还建议明确说明数据来源。有关数据共享协议的详细信息，参见ISO/IEC 23751:2022。

法律、法规、规章和合同要求可能会对专利品的复制施加限制。特别地，可以要求只使用由组织开发的材料，或由开发人员许可或提供给组织的材料。侵犯版权可能引起法律诉讼，面临罚款和刑事处罚。

除了组织需要履行其对第三方知识产权的保护义务外，还宜管理个人和第三方未能保护组织自身知识产权的风险。

5.33 记录的保护

5.33.1 属性表

记录的保护的属性表见表34。

表34 记录的保护属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#识别 #防护	#合法合规 #资产管理 #信息保护	#防御

5.33.2 控制

宜保护记录不被丢失、破坏、篡改、未经授权的访问和未经授权的发布。

5.33.3 目的

确保遵守法律、法规、规章和合同要求，以及达到社区或社会对与记录保护和记录可用性相关的期望。

5.33.4 指南

当记录的业务环境和管理要求随时间变化时，组织宜采取以下步骤来保护记录的真实性、可靠性、完整性和可用性：

a) 发布记录的存储、保管链的处理和记录处置的指导，其中包括防止对记录的违规操作。这些指导宜与组织关于记录管理的特定主题策略和其他记录要求保持一致；
b) 制定一份保留期限表，定义记录及其保留期限。

存储和处理系统宜确保识别记录及其保留期，应考虑国家或地区法律或法规以及社区或社会期望（如适用）。如果组织不再需要这些记录，该系统宜允许在期限后恰当地销毁记录。

在决定保护组织的特定记录时，宜根据组织的分级方案考虑对其进行相应的信息安全分级。宜对记录进行分类（如会计记录、业务交易记录、人事记录、法律记录），每种记录都宜详细说明保留期和允许的存储媒体类型，可以是物理或电子的。

数据存储系统的选择，宜确保能根据所要满足的要求以可接受的时间和格式检索所需的记录。

如果选择了电子存储媒体，则宜制定规程，以确保在整个保留期内对记录（存储媒体和格式可读性）可访问，以防止未来技术变化造成的丢失。还宜保留与加密档案或数字签名相关的密钥和程序，以便在记录保留期间对记录进行解密（见8.24）。

存储和处理规程宜按照存储媒体制造商提供的建议实施。宜考虑用于存储记录的媒体老化的可能性。

5.33.5 其他信息

记录记载了单个事件或事务，或者能形成工作过程、活动或功能的聚合。这些记录都是商业活动和信息资产的证据。任何一组信息，无论其结构或形式如何，都可以作为

记录进行管理。这包括在业务过程中创建、采集和管理的文档形式的信息、数据集合或其他类型的数字或模拟信息。

在对记录的管理中，元数据是描述记录的应用环境、内容和结构，以及随时间变化的管理的数据。元数据是任何记录的必不可少的组成部分。

可能需要安全地保留一些记录，以满足法律、法规、规章或合同要求，并支持基本的业务活动。国家法律或法规规定信息保留的时间和数据内容。有关记录管理的更多信息，参见ISO 15489。

5.34 隐私和个人可识别信息保护

5.34.1 属性表

隐私和个人可识别信息保护的属性表见表35。

表35 隐私和个人可识别信息保护属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#识别 #防护	#信息保护 #合法合规	#防护

5.34.2 控制

组织宜根据适用的法律、法规和合同要求，识别并满足有关隐私保护和PII保护的要求。

5.34.3 目的

确保遵守与信息安全相关的PII保护方面的法律、法规、规章和合同要求。

5.34.4 指南

组织宜制定并向所有相关方传达关于隐私和PII保护的专题策略。

组织宜制定并实施隐私和个人识别信息保护的规程。这些规程宜传达给处理个人身份信息的所有相关方。遵守这些规程以及与隐私保护和PII保护有关的所有相关法律法规，需要设置适当的角色、责任和控制。通常，这最好通过任命一名负责人来实现，如隐私官员，该负责人宜就个人责任和宜遵循的具体规程向个人、服务提供者和其他相关方提供指导。

处理PII的责任宜考虑基于相关的法律法规。宜采取适当的技术和组织措施来保护PII。

5.34.5 其他信息

许多国家已出台法律，对PII的收集、处理、传输和删除进行控制。根据各自的国

家法律，此类控制能对收集、处理和扩散PII的行为施加责任，也能限制政府部门向其他国家传输PII。

ISO/IEC 29100为ICT系统内的PII保护提供了一个高等级框架。有关隐私信息管理体系的更多信息，参见 ISO/IEC 27701。有关PII处理的公有云隐私信息管理的具体信息，参见ISO/IEC 27018。

ISO/IEC 29134提供了隐私影响评估（PIA）指南，并举例说明了隐私影响评估报告的结构和内容。与ISO/IEC 27005相比，这主要关注PII处理，并与处理PII的组织相关。这有助于识别隐私风险和可能的缓解措施，以将这些风险降低到可接受的水平。

5.35 信息安全的独立评审

5.35.1 属性表

信息安全的独立评审的属性表见表36。

表36 信息安全的独立评审属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防 #纠正	#保密性 #完整性 #可用性	#识别 #防护	#信息安全保障	#治理和生态体系

5.35.2 控制

组织管理信息安全的方法及其实现，包括人员、过程和技术，宜在计划的时间间隔内或发生重大变化时进行独立评审。

5.35.3 目的

确保组织管理信息安全方法的持续适宜性、充分性和有效性。

5.35.4 指南

组织宜有进行独立评审的规程。

管理者宜计划并启动定期独立评审。评审宜包括对信息安全方法（包括信息安全策略、专题策略和其他控制）的改进可能性和变更必要性的评估。

此类评审宜由独立于被评审范围的个体（例如内部审计职能部门、独立管理人员或专门从事此类评审的外部组织）进行。进行这些评审的个体宜具备相应的能力。开展评审的人员不宜处于管理限制范围内，以确保评估的独立性。

独立评审的结果宜报告给发起评审的管理者，并在适当情况下报告给最高管理者。这些记录宜予以保存。如果独立评审发现组织管理信息安全的方法和实施不充分，例如，

记录在案的目标和要求未得到满足或其

不符合信息安全策略和专题策略（见5.1）中规定的信息安全方向，管理者宜采取纠正措施。除定期独立评审外，组织宜考虑在以下情况进行独立评审：

a) 影响组织的法律法规有变化；
b) 发生重大事件；
c) 组织开始新业务或改变当前业务；
d) 组织开始使用新产品或服务，或改变当前产品或服务的使用；
e) 该组织显著改变了信息安全的控制和规程。

5.35.5 其他信息

ISO/IEC 27007和ISO/IEC TS 27008为进行独立评审提供了指南。

5.36 符合信息安全的策略、规则和标准

5.36.1 属性表

符合信息安全的策略、规则和标准的属性表见表37。

表37 符合信息安全的策略、规则和标准属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#识别 #防护	#合法合规 #信息安全保障	#治理和生态体系

5.36.2 控制

宜定期评审组织的信息安全策略、专题策略、规则和标准的符合情况。

5.36.3 目的

确保信息安全的实施和运行与组织的信息安全策略、专题策略、规则和标准一致。

5.36.4 指南

管理人员、服务、产品或信息拥有者宜确定如何评审信息安全策略、专题策略、规则、标准和其他适用法规中定义的信息安全要求是否得到满足。宜考虑使用自动测量和报告工具进行有效的定期评审。

如果评审结果发现任何不合规情况，管理人员宜：

a) 确定不合规的原因；
b) 评估采取纠正措施以实现合规性的必要性；
c) 实施适当的纠正措施；
d) 评审采取的纠正措施以验证其有效性，并识别其任何缺陷或弱点。

宜记录并保留管理人员、服务、产品或信息拥有者进行的评审和纠正措施的结果。当在其职责范围内进行独立评审时，管理人员宜将这些结果记录报告给独立评审人员参

考（见5.35）。

宜根据风险情况及时完成纠正措施。如果在下一次计划的评审前没有完成，宜至少在该评审中说明进展情况。

5.36.5 其他信息

8.15、8.16和8.17中介绍了系统使用情况的运行监控。

5.37 文件化的操作规程

5.37.1 属性表

文件化的操作规程的属性表见表38。

表38 文件化的操作规程属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防 #纠正	#保密性 #完整性 #可用性	#防护 #恢复	#资产管理 #物理安全 #系统和网络安全 #应用安全 #安全配置 #身份和访问管理 #威胁和脆弱性管理 #连续性 #信息安全事态管理	#治理和生态体系 #防护 #防御

5.37.2 控制

信息处理设施的操作规程宜形成文件，并对有需要的工作人员可用。

5.37.3 目的

确保信息处理设施的正确和安全运行。

5.37.4 指南

宜为组织制定与信息安全相关的操作活动的规程文件，例如：

a) 活动需要许多人以相同的方式进行；
b) 该活动很少进行，下一次进行时，该规程可能已被遗忘；
c) 该活动是新的，如果没有正确执行，会带来风险；
d) 在将操作的工作移交给新工作人员之前。

操作规程宜规定：

a) 负责人；
b) 系统的安全安装和配置；
c) 对信息的处理和控制，包括自动和手动；
d) 备份（见 8.13）和快速恢复；

e) 调度要求，包括与其他系统的相互依赖性；
f) 处理作业执行过程中可能出现的错误或其他异常情况的操作说明，如对实用程序使用的限制（见 8.18）；
g) 支持和扩大的联系，包括在意外操作的事态中或有技术难题时的外部支持联系；
h) 存储媒体处理说明（见 7.10 和 7.14）；
i) 系统失效事态中使用的系统重启和恢复规程；
j) 审计迹和系统日志信息（见 8.15 和 8.17）以及视频监控系统（见 7.4）的管理；
k) 对容量、性能和安全性等进行监控的规程（见 8.6 和 8.16）；
l) 维护说明。

必要时，宜审查并更新操作规程文件。对操作规程文件的更改宜获得授权。在技术上可行的情况下，宜始终使用相同的规程、工具和实用程序对信息系统进行一致的管理。

5.37.5 其他信息

无其他信息。

6 人员控制

6.1 审查

6.1.1 属性表

审查的属性表见表39。

表39 审查属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#人力资源安全	#治理和生态体系

6.1.2 控制

在加入组织前，宜对所有拟录用工作人员的候选人进行背景审查，并在入职后持续进行，同时考虑适用的法律、法规和道德规范，与业务要求、访问信息的级别和感知到的风险相适宜。

6.1.3 目的

确保所有工作人员符合条件且适合其角色，并在其任用期间持续保持。

6.1.4 指南

宜对所有工作人员进行筛查，包括全职、兼职和临时员工。对于与服务供应商签订合同的工作人员，宜在组织与供应商之间的合同协议中明确筛查要求。

被考虑在组织内录用的所有候选人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。在某些司法管辖区，法律可能会要求该组织将筛查活动提前通知候选人。

验证宜考虑所有相关的隐私、PII保护以及与任用相关的法律等因素，且在许可时，宜包括以下内容：

a) 验证所需材料的可用性（例如，业务和个人方面的材料）；
b) 申请人履历的完整性和准确性验证；
c) 声称的学历和专业资格的证实；
d) 独立的身份验证（例如，护照或由相关权威机构签发的其他可接受文件）；
e) 更多细节的验证，例如，信用核查或犯罪记录核查（若候选人担任关键角色）。

当组织聘用个人担任特定信息安全角色时，组织宜确认该候选人：

a) 具有担任该安全角色的必要能力；
b) 能被信任担任该角色，特别是当该角色对组织是十分重要的。

当一项工作初次任命的或晋升的人员有权访问信息处理设施，特别是如果该设施处理的是保密信息（例如财务信息、个人信息或医疗健康信息）时，则组织也宜考虑进一步的、更详细的验证。

宜有规程确定验证评审的准则和限制，例如谁有资格筛查人员，以及如何、何时、为什么执行验证评审。在无法及时完成验证的情况下，宜实施暂缓控制直到验证完成，例如：

a) 延迟到岗；
b) 延迟分配公司资产；
c) 到岗时减少访问权限；
d) 终止任用关系。

根据工作人员角色的重要性，宜定期重复审查，以确认人员的持续适用性。

6.1.5 其他信息

无其他信息。

6.2 任用条款和条件

6.2.1 属性表

任用条款和条件的属性表见表40。

表40 任用条款和条件属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#人力资源安全	#治理和生态体系

6.2.2 控制

宜在任用合同协议中规定工作人员和组织对信息安全的责任。

6.2.3 目的

确保工作人员理解其承担角色的信息安全责任。

6.2.4 指南

工作人员的合同义务宜考虑组织的信息安全方针和相关特定主题策略。此外，可以澄清和说明以下几点：

a) 所有访问保密信息的工作人员宜在获取信息和其他相关资产之前宜签署保密或不泄露协议（见 6.6）；
b) 法律责任和权利，例如版权、数据保护相关法律法规（见 5.32 和 5.34）；
c) 信息分级的责任，以及对工作人员处理的组织信息及其它相关资产、信息处理设施和信息服务进行管理的责任（见 5.9 至 5.13）；
d) 处理来自利益相关方信息的责任；
e) 工作人员无视组织安全要求时所采取的措施（见 6.4）。在任用之前，宜和候选人交流信息安全角色和责任相关信息。

组织宜确保工作人员同意与信息安全相关的条款和条件。这些条款和条件宜与他们对信息系统和服务相关组织资产进行访问的类型和范围相适宜。当法律法规、规章制度、信息安全方针或特定主题策略发生变更时，宜重新评审与信息安全相关的条款和条件。

适用时，任用条款和条件中的责任宜在任用结束后延续一段规定的时间（见6.5）

6.2.5 其他信息

行为准则能用于陈述工作人员在保密性、PII保护、道德规范、组织信息和其他相关资产的适当使用等方面的信息安全责任，以及组织所期望的良好实践。

与供应商人员有关的外部方可能被要求代表签约个人签署合同协议。

对于不是法人实体和没有员工的组织，可根据该控制的指导，考虑同等的合同协议、条款和条件。

6.3 信息安全意识、教育和培训

6.3.1 属性表

信息安全意识、教育和培训的属性表见表41。

表41 信息安全意识、教育和培训属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#人力资源安全	#治理和生态体系

6.3.2 控制

组织的工作人员和相关方，宜按其工作职能，接受适当的信息安全意识、教育和培训，及定期更新的组织信息安全方针、特定主题策略和规程。

6.3.3 目的

确保工作人员和相关方意识到并履行其信息安全责任。

6.3.4 指南

6.3.4.1 总则

信息安全意识、教育和培训方案宜按照组织的信息安全方针、特定主题策略和信息安全相关规程建立，考虑组织要保护的信息以及为保护这些信息所实施的信息安全控制。

信息安全意识、教育和培训宜定期进行。初始的意识、教育和培训不仅适用于新员工，也适用于那些调配到对信息安全要求完全不同的新岗位或角色的工作人员。

在意识、教育或培训活动结束时，宜评估工作人员的理解情况，以检验知识的传授以及意识、教育和培训方案的有效性。

6.3.4.2 意识

信息安全意识方案宜旨在使工作人员意识到他们的信息安全责任以及履行责任的方式。

宜考虑组织中的工作人员角色，包括内部和外部人员（例如外部顾问、供应商人员）的期望来规划意识方案。宜持续的，最好定期的安排意识方案中的活动，以便活动可以重复并覆盖新员工。意识方案宜汲取信息安全事件的经验教训。

意识方案宜通过适当的现场或虚拟渠道开展一系列意识提升活动，如竞赛、宣传手册、海报、新闻简讯、网站、资讯会议、简报、电子学习模块和电子邮件。

信息安全意识宜包括以下方面的概况：

a) 管理层对整个组织的信息安全承诺；
b) 熟悉并遵从适用的信息安全规则和义务的需要，如信息安全方针和特定主题策略、标准、法律法规、规章制度、合同和协议；
c) 对个人作为和不作为的问责制度，以及确保或保护组织和相关方的信息的安全的一般责任；

d) 基本的信息安全规程[如报告信息安全事态（6.8）]和基线控制[如口令安全（5.17）]；信息安全问题的更多信息和建议的联络点和资源，包括进一步的信息安全意识材料。

6.3.4.3 教育和培训

组织宜为因角色需要特定技能和专业知识的技术团队确定、准备和实施适当的培训计划。技术团队宜具备配置和维护设备、系统、应用程序和服务所需安全级别的技能。如果缺少技能，组织宜采取行动并获得这些技能。

教育和培训方案宜考虑不同的形式（如讲座或自学，由专家或顾问指导（在职培训），轮换员工跟进不同的活动，招聘有经验的员工和聘请顾问）。教育培训可使用不同的授课方式，包括课堂教学、远程学习、网络教学、自学及其他。技术人员宜通过订阅时事通讯和杂志，或参加旨在提高技术和专业水平的会议和活动，使其知识保持最新。

6.3.5 其他信息

当编制意识方案时，重要的是，不仅要关注“做什么”和“怎么做”，还要关注“为什么”。工作人员要理解信息安全的目标以及他们自己行为对组织的潜在影响，包括正面的和负面的，这些也很重要。

信息安全意识、教育和培训可以是其他活动的一部分，或与之协同开展，例如通用信息管理、ICT、安全、隐私或安全培训等活动。

6.4 违规处理过程

6.4.1 属性表

违规处理过程的属性表见表42。

表42 违规处理过程属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防 #纠正	#保密性 #完整性 #可用性	#防护 #响应	#人力资源安全	#治理和生态体系

6.4.2 控制

宜有正式的、且已被传达的违规处理过程，以对违反信息安全方针的工作人员和其他相关方采取措施。

6.4.3 目的

确保工作人员和其他相关方了解违反信息安全方针的后果，威慑并妥善处理违规的工作人员和其他相关方。

6.4.4 指南

在没有验证信息安全违规已经发生之前，不能开始该违规处理过程（见5.28）。正式的违规处理过程宜提供分级响应，并考虑如下因素：

a) 违规的性质（何人、何事、何时、如何发生）、严重程度及其后果；
b) 故意（恶意）违规还是无意（意外）违规；
c) 首次违规还是多次违规；
d) 违规者是否接受过适当的培训。

响应宜考虑相关法律、法规、监管合同和业务要求以及其他要求的因素。违规处理过程宜作为一种威慑，防止工作人员和其他相关方违反信息安全方针及信息安全的特定主题策略和规程。故意违反信息安全方针可能需要立即采取措施。

6.4.5 其他信息

在可能的情况下，宜根据适用的要求保护受到违规处理的个人的身份信息。

当个人在信息安全方面表现出色时可给予奖励，从而提升信息安全并鼓励良好行为。

6.5 任用终止或变更后的责任

6.5.1 属性表

任用终止或变更后的责任的属性表见表43。

表43 任用终止或变更后的责任属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#人力资源安全 #资产管理	#治理和生态体系

6.5.2 控制

宜确定任用终止或变更后仍有效的信息安全责任及其义务，传达至相关工作人员和其他相关方并执行。

6.5.3 目的

在任用或合同变更或终止过程中保护组织的利益。

6.5.4 指南

在任用终止或变更的管理过程中宜定义哪些信息安全责任和义务在终止或变更后仍然有效。这可能包括信息、知识产权和获得的其他知识以及任何其他保密协议规定的责任（见6.6）。在任用或合同终止后仍然有效的责任和义务宜包含在个人的任用条款和条件（见6.2）、合同或协议中。在个人任用关系结束后，持续一段时间的其他合同或协议也可能包含信息安全责任。

终止当前责任或任用并开始新的责任或任用时，宜管理对责任或任用的变更。

任何离职或变更工作角色的员工所承担的信息安全角色和责任都宜被确定并转移给另一位员工。

宜建立一个过程，将变更和操作规程传达给相关人员、其他相关方和相关联系人（例如客户和供应商）。当工作人员、合同或与组织有关的工作发生终止时，或组织内的工作发生变更时，任用终止或变更程序也宜适用于外部人员（例如供应商）。

6.5.5 其他信息

在许多组织中，人力资源职能部门通常负责整个终止过程，并与过渡人员的主管人员一起管理相关程序的信息安全方面。对于通过外部方（如通过供应商）提供的人员，该终止过程由外部方根据组织与外部方之间的合同进行。

6.6 保密或不泄露协议

6.6.1 属性表

保密或不泄露协议的属性表见表44。

表44 保密或不泄露协议属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性	#防护	#人力资源安全 #信息保护 #供应商关系安全	#治理和生态体系

6.6.2 控制

宜识别、文件化、定期评审反映组织信息保护需求的保密或不泄露协议，并与工作人员和其他相关方签署。

6.6.3 目的

维护工作人员或外部相关方可获取信息的保密性。

6.6.4 指南

保密或不泄露协议宜使用法律强制条款来保护保密信息。保密或不泄露协议适用于相关方和组织的工作人员。根据组织的信息安全要求，协议中的条款宜通过考虑被处理信息的类型、级别、用途和其他方的访问权限来确定。为确定保密或不泄露协议的要求，宜考虑以下因素：

a) 要保护的信息（例如保密信息）的界定；
b) 协议的期望持续时间，包括可能需要无限期维护保密性或直到信息公开的情况；
c) 协议终止时所需的措施；
d) 签署者的责任和措施，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，及其与保密信息的保护关系；

f) 保密信息的许可使用，及签署者使用该信息的权利；
g) 在高度敏感的情况下，对涉及保密信息的活动的审核和监视的权利；
h) 未授权披露或保密信息泄露的通知和报告过程；
i) 协议终止时，信息归还或销毁的条款；
j) 不遵守协议时采取的预期措施。

组织宜考虑遵守所适用管辖范围的保密和不泄露协议（见5.31、5.32、5.33、5.34）。宜定期评审保密和不泄露协议的要求，当发生影响这些要求的变更时，也宜进行评审。

6.6.5 其他信息

保密和不泄露协议保护组织的信息，并告知签署者以授权、负责的方式来保护、使用和披露信息的责任。

6.7 远程工作

6.7.1 属性表

远程工作的属性表见表45。

表45 远程工作属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#资产管理 #信息保护 #物理安全 #系统和网络安全	#防护

6.7.2 控制

宜在工作人员远程工作时实施安全措施，以保护在组织场所外所访问的、处理的或存储的信息。

6.7.3 目的

确保工作人员远程工作时的信息安全。

6.7.4 指南

远程工作是指组织工作人员在组织办公场所以外的地点工作，通过ICT设备硬拷贝或电子方式访问信息。远程工作环境包括“远程办公”“灵活工作场所”“虚拟工作环境”和“远程维护”。

注：由于不同司法管辖区的立法和法规不同，本指南中的所有建议可能无法全部适用。

允许远程工作活动的组织宜发布针对远程工作的特定主题策略，以定义相关工作条件和限制。当认为适用时，宜考虑下列事项：

a) 远程工作地点现有或建议的物理安全，可考虑地理位置和本地环境的物理安全，包括人员所在的不同司法管辖区；
b) 远程物理环境的规则和安全机制，例如可上锁的文件柜、地点之间的安全运输和远程访问规则、桌面清理、信息和其他相关资产的打印和处理以及信息安全事态的报告（见 6.8）；
c) 预期的远程工作物理环境；
d) 通信安全要求，考虑远程访问组织系统的需要、通信链路上被访问和传输的信息敏感性以及系统和应用程序的敏感性；
e) 远程访问的使用，例如支持在私有设备上处理和存储信息的虚拟桌面访问；
f) 远程工作场所的其他人员（如家人和朋友）未经授权访问信息或资源的威胁；
g) 在公共场所其他人员未经授权访问信息或资源的威胁；
h) 家庭网络和公共网络的使用，以及对无线网络服务配置的要求或限制；
i) 采取安全措施，如防火墙和防范恶意软件；
j) 远程部署和初始化系统的安全机制；
k) 考虑到允许远程访问组织网络的单因子鉴别机制的漏洞，用于鉴别和启用访问权限的安全机制。

考虑的指南和措施宜包括：

a) 当不允许使用不受组织控制的私有设备时，对远程工作活动提供合适的设备和存储设施；
b) 确定允许的工作、可持有信息的级别以及远程工作人员有权访问的内部系统和服务；
c) 为远程工作人员和提供支持的人员提供培训。宜包括如何在远程工作时以安全的方式开展业务；
d) 提供适合的通信设备，包括安全远程访问的方法，例如对设备屏幕锁定和无操作定时器的要求；启用设备位置跟踪；安装远程擦除功能；
e) 物理安全；
f) 关于家人和访客获取设备和信息的规则和指南；
g) 硬件和软件的支持和维护的提供；
h) 保险的提供；
i) 用于备份和业务连续性的规程；
j) 审核和安全监视；
k) 当远程工作活动终止时，撤销授权和访问权，并归还设备。

6.7.5 其他信息

无其他信息。

6.8 信息安全事态的报告

6.8.1 属性表

信息安全事态的报告属性表见表46。

表46 信息安全事态的报告属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#检测	#保密性 #完整性 #可用性	#发现	#信息安全事态管理	#防御

6.8.2 控制

组织宜提供机制，使工作人员通过适当渠道及时报告观察到的或可疑的信息安全事态。

6.8.3 目的

支持及时、一致和有效地报告工作人员识别出的信息安全事态。

6.8.4 指南

所有工作人员和用户宜意识到他们有责任尽可能快地报告信息安全事态，以防止或尽量减少信息安全事件的影响。他们还宜知道报告信息安全事态的规程和联络点。报告机制宜尽可能简单、方便和可用。信息安全事态包括事件、违规和脆弱性。

信息安全事态报告需要考虑的情况包括：

a) 无效的信息安全控制；
b) 未达到信息保密性、完整性或可用性的预期；
c) 人为差错；
d) 不符合信息安全方针、特定主题策略或适用标准；
e) 物理安全措施的受损；
f) 未经过变更管理流程的系统变更；
g) 软件或硬件的故障，或其他异常系统行为；
h) 非法访问；
i) 脆弱性；
j) 疑似恶意软件感染。

宜建议工作人员和用户不要试图证明可疑的信息安全脆弱性。测试脆弱性可能被解释为对系统的潜在误用，还可能导致对信息系统或服务的损害，并可能破坏或掩盖数字证据。最终，这可能导致执行测试的个人承担法律责任。

6.8.5 其他信息

更多信息参见ISO/IEC 27035系列。

7 物理控制

7.1 物理安全边界

7.1.1 属性表

物理安全边界的属性表见表47。

表47 物理安全边界属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#物理安全	#防护

7.1.2 控制

宜定义并使用安全边界来保护包含信息及其他相关资产的区域。

7.1.3 目的

防止对组织信息及其他相关资产进行未经授权的物理访问、损坏和干扰。

7.1.4 指南

适宜时，对于物理安全边界宜考虑并实施以下指南：

a) 根据与边界内资产相关的信息安全要求，定义安全边界以及每个边界的设置场所和强度；

b) 放置信息处理设施的建筑物或场所具有良好的物理边界（即：在容易发生入侵的边界或区域内不宜有间隙）。场所的外部屋顶、墙壁、天花板和地板宜采用坚固的结构，所有通往外部的门宜通过控制装置（例如：门闩、警报器、锁）进行适当的保护，以防止未经授权的访问。在无人看管时宜锁好门和窗；宜考虑对窗户进行外部保护，尤其是靠近地面楼层的窗户；还宜考虑对通风口的保护；

c) 宜根据适用的标准，给安全边界里的所有防火门和墙体安装报警器，并进行监视和测试，以建立所需的防御水平。它们宜以故障安全[注1]的方式运行。

7.1.5 其他信息

可以通过在组织场所和信息处理设施周围设置一个或多个物理屏障来实现物理保护。

安全的区域可以是一个可上锁的办公室或多个被连续的内部物理安全屏障包围的房间。在安全边界内具有不同安全要求的区域之间，可能需要额外的屏障和边界来控制物理访问。组织宜考虑在威胁增加的情况下可以加强的物理安全措施。

注[1]：故障安全：<计算机安全>在发生故障时避免受损，参见 ISO/IEC 2382:2015 信息技术-词汇。

7.2 物理入口

7.2.1 属性表

物理入口的属性表见表48。

表48 物理入口属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#物理安全 #身份和访问管理	#防护

7.2.2 控制

安全区域宜由适当的入口控制和访问点保护。

7.2.3 目的

确保只有获得授权后才能对组织的信息及其他相关资产进行物理访问。

7.2.4 指南

7.2.4.1 总则

宜控制诸如交接区等访问点以及未授权的人员可以进入的其他地点，并在可能的情况下让其与信息处理设施隔离，以避免未经授权的访问。

宜考虑以下指南：

a) 仅允许获得授权的人员进入组织的场所和建筑物。物理区域访问权的管理过程宜包括对授权的批准、定期评审、更新和撤销（见 5.18）；

b) 安全地维护和监视所有访问的纸质登记册或用于审核的电子踪迹，并保护所有日志（见 5.33）和敏感的鉴别信息；

c) 建立和实施过程和技术机制，以管理对组织处理或存储信息的区域的访问。鉴别机制包括使用门禁卡、生物特征鉴别或双因素身份鉴别，例如：门禁卡和秘密的 PIN。进入敏感区域时，宜考虑使用双重安全门；

d) 设置有人员监视的接待区，或通过其他方式来控制对组织场所或建筑物的物理访问；

e) 进出组织场所时，查验人员或相关方的个人物品；

f) 注：关于是否允许查验个人物品，当地的法律法规可能会有相应的规定。

g) 要求所有人员和相关方佩戴某种形式的可见身份标识，并在遇到没有人员陪同的访客和未佩戴可见身份标识的人时立即通知安保人员。宜考虑使用易于区分的标识，以便更好地识别长期雇员、供应商和访客；

h) 允许供应商人员只有在有需要时才可以有限制地访问安全区域或信息处理设施。这种访问宜得到授权并宜对它进行监控；

i) 当建筑物内有多个不同组织持有的资产时，特别关注该建筑物的物理访问安全；

j) 对物理安全措施进行设计，使得当发生物理访问事故的可能性增加时，它们能得到加强；

k) 保护其他入口（例如：紧急出口），防止未经授权的访问；

l) 建立密钥管理过程，以确保对物理密钥或鉴别信息（例如：锁具的密码，办公室、房间和钥匙柜等设施的组合锁）的管理，并确保具有日志或年度密钥审核以及对物理密钥或鉴别信息的访问是受控的。有关鉴别信息的进一步指南见5.17。

7.2.4.2 访客

宜考虑以下指南：

a) 通过适当的方式验证访客的身份；

b) 记录访客进入和离开组织场所的日期和时间；

c) 仅允许访客出于特定的、经授权的目的才可以访问组织，并向其提供有关该区域安全要求和应急规程的说明；

d) 监督所有访客，除非获得明确的例外许可。

7.2.4.3 交接区和来料

宜考虑以下指南：

a) 仅限已识别和授权的人员可以从建筑物外部进入交接区；

b) 交接区的设计能让交接人员在不发生未经授权访问建筑物的其他部分的情况下完成物资装卸；

c) 当通往限制区域的门打开时，交接区的外门得到安全保护；

d) 运入的物资在运离交接区之前，查验是否有爆炸物、化学品或其他危险品；

e) 运入的物资在进入组织的场所时，根据资产管理规程（见 5.9 和 7.10）进行登记；

f) 在可能的情况下，对进出的物资进行物理隔离；

g) 检查运入的物资在途中是否发生了篡改。如果发现有，宜立即向安保人员报告。

7.2.5 其他信息

无其他信息。

7.3 办公室、房间和设施的安全保护

7.3.1 属性表

办公室、房间和设施的安全保护的属性表见表49。

表49 办公室、房间和设施的安全保护属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#物理安全 #资产管理	#防护

7.3.2 控制

宜对办公室、房间和设施的物理安全进行设计，并予以实施。

7.3.3 目的

防止对组织在办公室、房间和设施中的信息及其他相关资产进行未经授权的物理访问、损坏和干扰。

7.3.4 指南

为保护办公室、房间和设施的安全，宜考虑以下指南：

a) 关键设施的安置要避免公众可访问的地方；
b) 适用时，确保建筑物不引人注目，并尽可能少地表明其用途，建筑物内外没有可识别出是否存在信息处理活动的明显标志；
c) 对设施进行配置，以防止从外部可以看到或听到保密信息或活动。适宜时，宜考虑使用电磁屏蔽；
d) 使得可识别出保密信息处理设施所在位置的通讯录、内部电话簿和在线可访问地图不会让任何未授权的人员轻易获得。

7.3.5 其他信息

无其他信息。

7.4 物理安全监视

7.4.1 属性表

物理安全监视的属性表见表50。

表50 物理安全监视属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防 #检测	#保密性 #完整性 #可用性	#防护 #发现	#物理安全	#防护 #防御

7.4.2 控制

宜持续监视场所，以防止发生未经授权的物理访问。

7.4.3 目的

发现并阻止未经授权的物理访问。

7.4.4 指南

物理场所宜由监视系统进行监视，监视系统可以包括警卫、入侵者警报、闭路电视等视频监视系统以及内部管理或由监视服务提供者管理的物理安全信息管理软件。

宜通过以下方式持续监视对装有关键系统的建筑物的访问，以发现未经授权的访问或可疑行为：

a) 安装闭路电视等视频监视系统，以查看和记录访问组织场所内外敏感区域的情况；
b) 根据相关适用标准安装并定期测试用于触发入侵者警报的触点、声音或运动探测器，例如：

1) 在任何可能发生触点闭合或断开的地方（例如：门、窗和下方物体）安装触点探测器，当触点发生闭合或断开时，触发警报，用作紧急警报；
2) 基于红外技术的运动探测器，当物体通过其视野时触发警报；
3) 安装对玻璃破碎声音敏感的传感器，可用于触发警报，提醒安保人员；

c) 使用这些警报覆盖所有外门和可接近的窗户。空置区宜始终配有警报；还宜为其他区域（例如：计算机室或通信室）配置警报。

监视系统的设计宜保密，因为泄露可能会导致容易发生未被发现的非法入侵。

宜保护监视系统免受未经授权的访问，以防止未授权的人员访问监视信息（例如：视频录像）或系统被远程禁用。

警报系统控制面板宜放置在警报覆盖的区域；对于安全警报，其控制面板宜放置在报警人员可以方便出入的位置。控制面板和探测器宜具有防篡改机制。宜定期测试系统，以确保其按预期工作，尤其是在其组件是由电池供电的情况下。

使用任何监视和记录机制时，宜考虑当地法律法规，包括数据保护和PII保护的法律，尤其是有关人员监视和录像保存期的要求。

7.4.5 其他信息

无其他信息。

7.5 物理和环境威胁防范

7.5.1 属性表

物理和环境威胁防范的属性表见表51。

表51 物理和环境威胁防范属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#物理安全	#防护

7.5.2 控制

宜对物理和环境威胁的防范进行设计并予以实施，例如：自然灾害和其它对基础设施有意或无意的物理威胁。

7.5.3 目的

防止或减少由物理和环境威胁引起的事态的后果。

7.5.4 指南

宜在物理现场开始关键作业之前以及定期地进行风险评估，以识别物理威胁和环境威胁的潜在后果。宜实施必要的防护措施，并监视威胁的变化。宜就如何管理因火灾、洪水、地震、爆炸、内乱、有毒废物、环境排放和其他形式的自然灾害或人为灾害等物理和环境威胁所产生的风险征求专业人士的意见。

物理场所的位置和建造宜考虑：

a) 当地的地形，例如：适当的海拔、水体和构造断层线；
b) 城市威胁，例如：那些能吸引政治动荡、犯罪活动或恐怖袭击的、知名度高的地方；

根据风险评估结果，宜识别相关的物理和环境威胁，并在以下作为示例的情形中考虑适当的控制：

a) 火灾：安装和配置能够在早期发现火灾的系统，以发送警报或触发灭火系统，防止火灾损坏存储媒体和相关信息处理系统。灭火时宜使用最适合周围环境的物质（例如：密闭空间中的气体）；
b) 水灾：在包含存储媒体或信息处理系统的区域的地板下安装能够早期发现水灾的系统。水泵或具有同等功能的设备宜随时可用，以防发生水灾；
c) 电涌：采用能够保护服务器和客户端信息系统免受电涌或类似事件影响的系统，以尽量减少此类事态的后果；
d) 爆炸物和武器：随机抽查进入敏感信息处理设施的人员、车辆或货物，检查是否携带有爆炸物或武器。

7.4.6 其他信息

保险箱或其他形式的安全存储设施可以保护存储在其中的信息免受火灾、地震、洪水或爆炸等灾害的影响。组织在设计用于保护其环境并减少城市威胁的控制时，可以在环境设计中考虑犯罪预防的概念。例如：雕像或水景既可以作为一种景观，也可以作为一个物理屏障，可以代替使用保护柱。

7.6 在安全区域工作

7.6.1 属性表

在安全区域工作的属性表见表52。

表52 在安全区域工作属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#物理安全	#防护

7.6.2 控制

宜设计并实现在安全区域工作的安全措施。

7.6.3 目的

保护安全区域内的信息及其他相关资产免受在这些区域工作的人员的损坏和未经授权的干扰。

7.6.4 指南

在安全区域工作的安全措施宜适用于所有人员，并涵盖在安全区域内进行的所有活

动。宜考虑以下指南：

a) 基于“须知”的原则来确定员工只须知晓的安全区域及其内部活动；
b) 出于安全原因和为了减少发生恶意活动的可能性，避免在安全区域进行无人监督的工作；
c) 对空置的安全区域进行物理上锁并定期检查；
d) 未经授权，不允许使用拍照、视频录制、音频录制或其他记录设备，例如：用户终端设备中的相机；
e) 适当地控制安全区域内用户终端设备的携带和使用；
f) 以易于看到或获取的方式张贴应急规程。

7.6.5 其他信息

无其他信息。

7.7 清理桌面和屏幕

7.7.1 属性表

清理桌面和屏幕的属性表见表53。

表53 清理桌面和屏幕属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性	#防护	#物理安全	#防护

7.7.2 控制

宜定义并适当地执行纸质和可移动存储媒体的桌面清理规则和信息处理设施的屏幕清理规则。

7.7.3 目的

减少在正常工作时间内外，办公桌、屏幕和其他可访问地点上的信息发现未经授权的访问、丢失和损坏的风险。

7.7.4 指南

组织宜制定清理桌面和屏幕的的特定主题策略，并将其传达给所有相关方。宜考虑以下指南：

a) 当敏感或关键的商业信息（例如：纸质或电子存储媒体上的信息）不需要使用时，尤其是办公室没人时，把这些信息锁起来，最好是放在保险箱、储藏柜或其他形式的安全家具中；
b) 在不使用或无人看管时，通过钥匙锁或其他安全手段保护用户终端设备；
c) 在无人看管时，让用户终端设备退出登录或使用由用户鉴别机制控制的屏幕和键盘锁定机制进行保护。所有计算机和系统都宜配置超时或自动退出登录功能；
d) 让发起者立即取走打印机或多功能设备的输出。使用具有鉴别功能的打印机，这样发起者将是唯一能得到打印输出的人，而且只有当其站在打印机旁边时才能取走它；
e) 安全地存放包含敏感信息的文件和可移动存储媒体，并在不再需要时，使用安

全处置机制将其丢弃；

f) 建立和传达屏幕弹窗配置的规则和指南（例如：如有可能，在演示、屏幕共享或公共场所时，关闭新邮件和新消息弹窗）；

g) 当不再需要时，清除白板和其他类型显示设备上的敏感或关键信息。

组织在腾空设施时宜有适当的规程，包括在离开前进行最后的清理，以确保没有留下组织的资产（例如：文件落在抽屉或家具后面）。

7.7.5 其他信息

无其他信息。

7.8 设备安置和保护

7.8.1 属性表

设备安置和保护的属性表见表54。

表54 设备安置和保护属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#物理安全 #资产管理	#防护

7.8.2 控制

宜安全地安置并保护设备。

7.8.3 目的

减少来自物理和环境威胁、未经授权的访问和损坏的风险。

7.8.4 指南

为保护设备，宜考虑以下指南：

a) 设备的安置要尽量减少对工作区域的不必访问和避免对工作区域进行未经授权的访问；

b) 谨慎地安置处理敏感数据的信息处理设施，以减少在其使用过程中，信息被未授权的人员查看到的风险；

c) 采取控制，将潜在的物理和环境威胁的风险降至最低。例如：盗窃、火灾、爆炸物、烟雾、水（或供水故障）、灰尘、振动、化学效应、电源干扰、通信干扰、电磁辐射和蓄意破坏行为；

d) 制定在信息处理设施附近的饮食和吸烟指南；

e) 监视对信息处理设施的运行可能有不利影响的环境条件，例如：温度和湿度；

f) 对所有建筑物进行防雷保护，并对所有进场电力和通信线路安装防雷过滤器；

g) 考虑对工业环境中的设备使用特殊保护方法，例如：键盘膜；

h) 保护处理保密信息的设备，以最大限度地降低电磁辐射导致的信息泄漏风险；

i) 将组织管理的信息处理设施与非组织管理的信息处理设施进行物理隔离。

7.8.5 其他信息

无其他信息。

7.9 组织场所外的资产安全

7.9.1 属性表

组织场所外的资产安全的属性表见表55。

表55 组织场所外的资产安全属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#物理安全 #资产管理	#防护

7.9.2 控制

宜保护组织场所外的资产。

7.9.3 目的

防止组织场所外设备的丢失、损坏、失窃或危及其安全以及组织运行的中断。

7.9.4 指南

在组织场所外使用的、存储或处理信息的任何设备（例如：移动设备）需要得到保护，包括组织拥有的设备和私人拥有并代表组织使用的设备[自携设备（BYOD）]。这些设备的使用宜由管理人员授权。

对于在组织场所外的、存储和处理信息的设备的保护，宜考虑以下指南：

a) 不得将带到组织场所外的设备和存储媒体留在公共和不安全的地方且无人看管；
b) 始终遵守制造商关于保护设备的说明，例如：防止暴露于强电磁场、水、高温、潮湿、灰尘；
c) 当组织场所外的设备在不同的个人或相关方之间转移时，维护一份明确了该设备保管链的日志，其中至少包括对设备负责的人员的姓名和组织名称。宜在转移前安全删除不需要随资产转移的信息；
d) 在必要和切实可行的情况下，要求获得将设备和媒体带离组织场所的授权，并保留此类带离的记录，以维护用于审核的电子踪迹（见 5.14）；
e) 乘坐公共交通时，不查看设备（例如：手机或笔记本电脑）上的信息，并防范与背后窥视相关的风险；
f) 实施位置跟踪和设备远程擦除功能。

永久安装在组织场所之外的设备[例如：天线和自动柜员机（ATM）]可能会面临更高的被损坏、盗窃或窃听风险。这些风险在不同地点之间可能存在很大差异，在确定最合适的措施时宜对此予以考虑。当在组织场所外安置设备时，宜考虑以下指南：

a) 物理安全监视（见 7.4）；
b) 防范物理和环境威胁（见 7.5）；

c) 物理访问和防篡改控制；
d) 逻辑访问控制。

7.9.5 其他信息

有关保护信息存储和处理设备以及用户终端设备的其他方面的更多信息，参见8.1和6.7。

7.10 存储媒体

7.10.1 属性表

存储媒体的属性表见表56。

表56 存储媒体属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#物理安全 #资产管理	#防护

7.10.2 控制

存储媒体宜在其获取、使用、运输和处置的整个生存周期内，按照组织的分级方案和处理要求进行管理。

7.10.3 目的

确保只有在获得授权后才能披露、修改、删除或销毁存储媒体上的信息。

7.10.4 指南

7.10.4.1 可移动存储媒体

宜考虑以下可移动存储媒体的管理指南：

a) 制定关于可移动存储媒体管理的特定主题策略，并向任何使用或处理可移动存储媒体的人员传达该特定主题策略；
b) 在必要和可行的情况下，要求获得从组织带离存储媒体的授权，并保存此类带离的记录，以维护用于审核的电子踪迹；
c) 根据信息分级将所有存储媒体存放在安全的环境中，并根据制造商的规范保护其免受环境威胁（例如：高温、潮湿、湿热、电场或老化）；
d) 如果信息的保密性或完整性是重要考虑因素，则使用密码技术保护可移动存储媒体中的信息；
e) 为了在仍然需要存储的信息时降低存储媒体退化的风险，在信息无法被读取之前将其传输到新的存储媒体中；
f) 在不同的存储媒体上存储有价值信息的多个副本，以进一步减少偶发的信息损坏或丢失的风险；
g) 考虑对可移动存储媒体进行注册登记，以限制信息丢失的可能性；
h) 仅在因为组织需要使用时，才启用可移动存储媒体端口（例如：SD 卡插槽和

USB 端口）；

i) 在需要使用可移动存储媒体的时，监视信息向此类存储媒体的传输；

j) 在物理传输过程中，信息可能容易受到未经授权的访问、误用或损坏，例如：通过邮政服务或快递邮寄存储媒体时。

在此控制中，媒体包括纸质文件。传输物理存储媒体时，宜应用5.14中的安全措施。

7.10.4.2 安全重复使用或处置

宜制定存储媒体的安全重复使用或处置规程，从而使得保密信息被泄露给未授权的人员的风险减小到最小。安全重复使用或处置包含保密信息的存储媒体的规程宜与该信息的敏感性相适宜。宜考虑以下事项：

a) 如果包含保密信息的存储媒体需要在组织内重复使用，则在重复使用前安全地删除数据或格式化存储媒体（见 8.10）；

b) 当不再需要时，安全地处置包含保密信息的存储媒体（例如：通过销毁、粉碎或安全地删除内容）；

c) 有适当的规程来识别可能需要安全处置的物品；

d) 许多组织提供回收和处置存储媒体的服务。宜注意选择合适的、具有充分控制和经验的外部供应商；

e) 记录敏感物品的处置情况，以维护审核踪迹；

f) 当待处置的存储媒体出现积压时，要考虑聚合效应，这会导致大量非敏感信息变得敏感。

宜对包含敏感数据的受损设备进行风险评估，以确定是否宜物理销毁这些物品，而不是将其送去维修或丢弃（见7.14）。

7.10.5 其他信息

当存储媒体上的保密信息未加密时，宜考虑对存储媒体进行额外的物理保护。

7.11 支持性设施

7.11.1 属性表

支持性设施的属性表见表57。

表57 支持性设施属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防 #检测	#完整性 #可用性	#防护 #发现	#物理安全	#防护

7.11.2 控制

宜保护信息处理设施使其免于由支持性设施的故障而引起的电源故障和其他中断。

7.11.3 目的

防止信息及其他相关资产的丢失、损坏或泄露，或由于支持性设施的故障和破坏而导致组织运行的中断。

7.11.4 指南

组织依靠设施（如电力、电信、供水、燃气、排污、通风和空调）来支持其信息处理设施。因此，组织宜：

a) 确保用于支持设施的设备按照相关制造商的规范进行了配置、操作和维护；
b) 确保定期评估设施的性能，以满足业务增长并保持与其他支持性设施的兼容；
c) 确保定期检查和测试用于支持性设施的设备，以确保其运行正常；
d) 如需要，发出警报以检测设施故障；
e) 如需要，确保设施使用多种物理途径进行多路供给；
f) 如果联网，要确保用于支持性设施的设备与信息处理设施在不同网段；
g) 确保用于支持性设施的设备仅在需要时以安全的方式连接到互联网。

宜提供应急照明和应急通信。关闭电源、供水、供气或其他设施的应急开关和阀门宜位于紧急出口或设备室附近。宜详细记录应急联系方式，确保在中断时对相关人员可用。

7.11.5 其他信息

网络连接的额外冗余可以通过来自多个设施供应商的多条路由获得。

7.12 布缆安全

7.12.1 属性表

布缆安全的属性表见表58。

表58 布缆安全属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #可用性	#防护	#物理安全	#防护

7.12.2 控制

宜保护传输电力、数据或支持信息服务的电缆免受窃听、干扰或损坏。

7.12.3 目的

防止信息及其他相关资产的丢失、损坏、失窃或泄露以及与电力和通信布缆相关的组织运行中断。

7.12.4 指南

宜考虑以下布缆安全指南：

a) 进入信息处理设施的电力和通信线路尽可能位于地下，或受到足够的替代保护，如地板电缆保护槽和电缆保护钢管；如果电缆位于地下，则保护电缆免受意外切割（如使用铠装导管或接线保护盒）；
b) 将电力电缆与通信电缆隔离以防止干扰；
c) 对于敏感的或关键的系统，需要考虑更进一步的控制，包括：

1) 在检查点和终接点处安装铠装导管、给储藏间或储藏盒上锁和放置报警器；
2) 使用电磁屏蔽装置保护电缆；
3) 定期进行技术扫描和物理检查，以检测连接到电缆上的未授权设备；
4) 控制对配线架和电缆室的访问（如使用机械钥匙或插销）；
5) 使用光纤电缆；

d) 在电缆的每一端贴上标记，提供足够的来源和目的地详细信息，以便对电缆进行物理识别和检查。宜就如何管理布缆事件或故障引起的风险寻求专家建议。

7.12.5 其他信息

有时，对于占用同一办公场所的多个组织来说，电缆和通信缆线是组织间的共享资源。

7.13 设备维护

7.13.1 属性表

设备维护的属性表见表59。

表59 设备维护属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#物理安全 #资产管理	#防护 #弹性

7.13.2 控制

设备宜予以正确的维护，以确保信息的可用性、完整性和保密性。

7.13.3 目的

防止因缺乏维护而导致信息及其他相关资产的丢失、损坏、失窃或泄露，以及组织运行的中断。

7.13.4 指南

宜考虑以下设备维护指南：

a) 按照供应商建议的服务频率和规范维护设备；
b) 组织要实施和监视维护程序；
c) 仅授权维修人员才可以对设备进行维修和保养；
d) 宜保存所有可疑的或实际的故障记录，以及所有预防性和纠正性维护记录；
e) 当设备按计划进行维护时，实现适当的控制，考虑维护是由现场人员还是组织外部人员执行；使维护人员遵守适当的保密协议；
f) 在现场进行维护时监督维护人员；
g) 授权和控制远程维护访问；
h) 如果保存了信息的设备被带离现场进行维护，则对场外资产采取安全措施（见7.9）；
i) 遵守保险规定的所有维护要求；

j) 维护后的设备在重新使用前，实施检查，以确保设备未被篡改且功能正常；
k) 如果确定设备要被处置，则采取设备的安全处置或重复使用的措施（见7.14）。

7.13.5 其他信息

设备包括信息处理设施、不间断电源（UPS）和电池、发电机、交流发电机和转换器、物理入侵检测系统和报警器、烟雾探测器、灭火器、空调和电梯的技术部件。

7.14 设备的安全处置或重复使用

7.14.1 属性表

设备的安全处置或重复使用的属性表见表60。

表60 设备的安全处置或重复使用属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性	#防护	#物理安全 #资产管理	#防护

7.14.2 控制

宜对包含存储媒体的设备的所有部分进行核查，以确保在处置或重复使用之前，任何敏感数据和注册软件已被删除或安全的重写。

7.14.3 目的

防止信息从待处置或重复使用的设备中泄露。

7.14.4 指南

在设备处置或重复使用前，宜验证其是否包含存储媒体。

包含保密或版权保护信息的存储媒体宜进行物理销毁，或者宜使用技术手段将信息销毁、删除或覆盖，确保原始信息不可检索，而不能采用一般的删除功能。有关存储媒体安全处置的详细指南，参见7.10；有关信息删除的详细指南，参见8.10。

标识组织或表明分级、拥有者、系统或网络的标记宜在处置前移除，包括转售或捐赠给慈善机构。

组织宜考虑在租赁结束或搬出场地外时取消安全控制，如访问控制或监视设备。这取决于以下因素：

a) 将设施恢复原状的租赁协议；
b) 最大限度地降低将系统上的敏感信息留给下一个租户的风险（例如用户访问列表、视频或图像文件）；
c) 在下一个场所重复使用控制的能力。

7.14.5 其他信息

包含存储媒体的受损设备可能需要进行风险评估，以确定这些物品是否宜被物理销毁，而不是送去维修或丢弃。设备的草率处置或重复使用可能导致信息泄露。

除了安全删除磁盘外，全磁盘加密还可以降低设备处置或重新部署时泄露保密信息的风险，前提是：

a) 加密过程足够强大并覆盖整个磁盘（包括剩余空间、交换分区（swap）文件）；
b) 密钥的长度足以抵御暴力破解；
c) 密钥自身的保密性能够得到保障（如从不存储在同一磁盘上）。有关密码的更多建议见8.24。

根据存储媒体所用技术及其所存信息的分级级别，存储媒体安全重写的技术会有所不同。宜评审重写工具以确保其适用于存储媒体所用的技术。

有关存储媒体净化方法的详细信息见ISO/IEC 27040。

8 技术控制

8.1 用户终端设备

8.1.1 属性表

用户终端设备的属性表见表61。

表61 用户终端设备属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#资产管理 #信息保护	#防护

8.1.2 控制

宜保护通过用户终端设备进行存储、处理或访问的信息。

8.1.3 目的

保护信息免受使用用户终端设备带来的风险。

8.1.4 指南

8.1.4.1 总则

组织宜建立用户终端设备安全配置和操作的特定主题策略。特定主题策略宜传达给所有相关人员，并考虑以下事项：

a) 用户终端设备可以操作、处理、存储或支持的信息类型和分级级别；
b) 用户终端设备的注册；
c) 物理保护要求；
d) 软件安装限制（例如由系统管理员远程控制）；
e) 用户终端设备软件（包括软件版本）和应用更新（例如主动自动更新）的要求；
f) 与信息服务、公共网络或任何其他办公场所外网络连接的规则（例如要求使用个人防火墙）；
g) 访问控制；

h) 存储设备加密；
i) 防止恶意软件；
j) 对远程进行禁用、删除或锁定；
k) 备份；
l) web 服务和 web 应用的使用；
m) 最终用户行为分析（见 8.16）；
n) 可移动设备的使用，包括可移动存储设备和禁用物理端口（例如 USB 端口）的可能性；
o) 如果用户终端设备支持，使用分区功能，可以安全地将组织的信息和其他相关资产（如软件）与设备上的其他信息和其他相关资产分开。

宜考虑某些信息是否非常敏感，只能通过用户终端设备访问，而不能存储在设备上。在此情况下，设备可能需要额外的技术保护措施。如确保禁用在脱机工作状态下下载文件，并禁用安全数字（SD）卡等本地存储。

宜尽可能通过配置管理（见8.9）或自动化工具来实施有关此控制的建议。

8.1.4.2 用户责任

宜让所有用户了解用户终端设备保护的安全要求和程序，以及实施此类安全措施时所承担的责任。用户宜注意：

a) 注销活动会话并在不再需要时终止服务；
b) 在不使用时，通过物理控制（如钥匙锁或特殊锁）和逻辑控制（如口令访问）保护用户终端设备不被未授权使用；不要让承载重要、敏感或关键业务信息的设备无人值守；
c) 在公共场所、开放式办公室、会议场所和其他未受保护的区域谨慎使用设备（例如避免阅读涉密信息，当有人可以从身后看到时，使用防窥屏膜）；
d) 物理保护用户终端设备免受盗窃（例如在汽车和其他形式的交通工具、酒店房间、会议中心和会议室）。对于用户终端设备被盗或丢失的情况，宜建立一个与组织的法律、法规、监管、合同（包括保险）和其他安全要求相符的具体规程。

8.1.4.3 使用个人设备

如果组织允许使用个人设备（携带自己的设备办公），除本控制中给出的指南外，还宜考虑以下事项：

a) 分离设备的个人和工作使用，包括使用软件支持此类分离，并保护私人设备上的业务数据；
b) 只有在用户确认知晓其职责（物理保护、软件更新等）后才能访问业务信息，放弃业务数据的所有权，允许组织在设备被盗或丢失或不再授权使用服务时远程擦除数据。在此情况下，宜考虑 PII 的法律法规；
c) 制定特定主题策略和规程，以防止与私有设备上开发的知识产权相关的争议；
d) 访问私人拥有的设备（以验证机器的安全性或在调查期间），该访问可能会被法律所禁止；
e) 软件许可协议，组织可能会对个人或外部用户拥有的用户终端设备上的客户端软件的许可负责。

8.1.4.4 无线连接

组织宜建立以下规程：

a) 设备上无线网络连接的配置（例如禁用易受攻击的协议）；
b) 根据特定主题策略（如因为需要备份或软件更新），使用具有适当带宽的无线或有线连接。

8.1.4.5 其他信息

用户终端设备上的信息保护控制取决于用户终端设备是否仅在组织的安全场所和网络连接内使用，或者是否暴露于组织外部的更多物理和网络的相关威胁。

用户终端设备的无线网络连接与其他类型的网络连接类似，但在识别控制时宜考虑到重要的差异。具体而言，因网络带宽有限或者因为在计划备份时用户终端设备未连接，用户终端设备上的信息进行备份有时可能出现存储失败。

某些USB端口，如USB-C，因为此类端口有着其他用途（如电源传输和显示输出），所以禁用这些USB端口不太现实。

8.2 特许访问权

8.2.1 属性表

特许访问权的属性表见表62。

表62 特许访问权属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#身份和访问管理	#防护

8.2.2 控制

宜限制和管理特许访问权的分配和使用。

8.2.3 目的

为确保仅授权的用户、软件组件和服务具有特许访问权。

8.2.4 指南

特许访问权的分配宜根据访问控制（见5.15）的相关特定主题策略，通过授权过程进行控制。宜考虑下列步骤：

a) 识别每个系统或过程（例如操作系统、数据库管理系统和应用程序）需要的特许访问权用户；
b) 根据访问控制（见 5.15）的特定主题策略，按需并在“一事一议”的基础上向用户分配特许访问权（例如：仅限于具有必要能力开展需要特许访问活动的个人，并基于其职能角色的最低要求）；
c) 维护授权过程（例如：确定谁可以批准特许访问权，或在授权过程完成之前不授予特许访问权）和所有分配特权的记录；

d) 定义和实施特权访问权到期的要求；
e) 采取措施确保用户知道自己的特许访问权限以及自己何时会处于特许访问模式。可能的措施包括使用特定的用户身份、用户界面设置甚至特定的设备；
f) 特许访问权的身份验证要求可能高于正常访问权的要求。在使用特权访问权限进行工作之前，可能需要重新认证或加强认证；
g) 定期和在组织变更后，评审使用特许访问权工作的用户，以验证其职责、角色、责任和能力是否仍符合使用特许访问权的条件（见 5.18）；
h) 根据系统的配置能力，建立特定规则以避免使用通用管理用户 ID（如“root”）。管理和保护此类身份的认证信息（见 5.17）；
i) 仅在实施批准的变更或活动（例如维护活动或某些关键变更）所需的时间窗口内授予临时特许访问，而不是永久授予特许访问权。这通常被称为碎玻璃规程，通常通过权限访问管理技术实现自动化；
j) 记录对系统的所有特许访问，以便进行审计；
k) 不向多个人共享或链接具有特许访问权限的身份，为每个允许分配特定特许访问权限的人分配单独的身份。可以对身份进行分组（如通过定义管理员组），以简化特许访问权限的管理；
l) 仅将具有特许访问权限的身份用于执行管理任务，而不用于日常的一般任务[即检查电子邮件、访问网络（用户宜具有单独的正常网络身份以进行这些活动）]。

8.2.5 其他信息

特许访问权限是提供给身份、角色或过程的访问权限，允许执行一般用户或过程无法执行的活动。系统管理员角色通常需要特许访问权限。

不当使用系统管理员权限（信息系统的任何功能或设施，使用户可以无视系统或应用程序控制）是导致系统故障或违规的主要因素。

有关访问管理以及信息和通信技术资源访问安全管理的更多信息，参见ISO/IEC 29146。

8.3 信息访问限制

8.3.1 属性表

信息访问限制的属性表见表63。

表63 信息访问限制属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#身份和访问管理	#防护

8.3.2 控制

宜按照已建立的访问控制的特定主题策略，限制对信息及其他相关资产的访问。

8.3.3 目的

确保仅授权的访问，并防止未授权访问信息及其他相关资产。

8.3.4 指南

宜根据既定的专题策略限制对信息和其他相关资产的访问。为支持访问限制要求，宜考虑以下事项：

a) 不允许未知用户身份或匿名访问敏感信息。仅允许对不包含任何敏感信息的存储位置进行公开或匿名访问；
b) 提供配置方法，以控制对系统、应用程序和服务中信息的访问；
c) 控制特定用户可访问的数据；
d) 控制哪些身份或身份组具有哪些访问权限，如读、写、删除和执行；
e) 为隔离敏感应用程序、应用程序数据或系统提供物理或逻辑访问控制。

此外，组织在出现下列情形时宜考虑保护敏感信息的动态访问管理技术和过程：

a) 需要对谁可以在什么时期以什么方式访问此类信息进行精确控制；
b) 希望与组织外的人共享此类信息，并保持对谁可以访问这些信息的控制；
c) 希望实时动态管理此类信息的使用和分发；
d) 希望保护此类信息免受未授权的更改、复制和分发（包括打印）；
e) 希望监控信息的使用；
f) 希望记录此类信息发生的任何更改，以防将来需要进行调查。

动态访问管理技术宜在信息的整个生存周期（即创建、处理、存储、传输和处置）内保护信息，包括：

a) 基于特定用例建立动态访问管理规则，考虑：
   1) 基于身份、设备、位置或应用程序授予访问许可；
   2) 利用分级方案，以确定需要使用动态访问管理技术保护哪些信息。
b) 建立运行、监控和报告过程，并支持技术基础设施。

动态访问管理系统宜通过以下方式保护信息：

a) 需要身份验证、适当的凭证或证书才能访问信息；
b) 限制访问，例如在指定的时间范围内（如在给定日期之后或直到特定日期）；
c) 使用加密来保护信息；
d) 定义信息的打印权限；
e) 记录谁访问了信息以及如何使用信息；
f) 如果检测到盗用信息的尝试，则会发出警报。

8.2.6 其他信息

动态访问管理技术和其他动态信息保护技术可以支持对信息的保护，即便在无法实施传统访问控制的数据起源组织之外共享数据。该技术可以应用于包含信息的文档、电子邮件或其他文件，以限制谁可以访问内容以及以何种方式访问内容。该部分可以达到颗粒级别，并且可以适应整个信息生存周期。

动态访问管理技术不会取代传统的访问管理[如使用访问控制列表（ACL）]，但可以为约束、实时评估、即时数据缩减和其他对最敏感信息有用的增强添加更多因素。该技术提供了一种在组织环境之外控制访问的方法。动态访问管理技术可以支持事件响应，因为权限可以随时修改或撤销。

ISO/IEC 29146中提供了访问管理框架的其他信息。

8.4 源代码的访问

8.4.1 属性表

源代码的访问的属性表见表64。

表64 源代码的访问属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#身份和访问管理 #应用安全 #安全配置	#防护

8.4.2 控制

宜适当对源代码、开发工具和软件库的读写访问进行管理。

8.4.3 目的

防止引入未授权的功能，避免无意或恶意的变更，并维护有价值知识产权的保密性。

8.4.4 指南

宜严格控制对源代码和相关事项（如设计、规范、验证计划和批准计划）以及开发工具（如编译器、构建器、集成工具、测试平台和环境）的访问。

对于源代码，这可以通过控制此类代码的中央存储来实现，最好是在源代码管理系统中。

对源代码的读写权限可因人员的角色而异。例如，可以在组织内部广泛提供对源代码的阅读权限，但对源代码的编写权限仅提供给特权人员或指定拥有者。当组织内的多个开发人员使用代码组件时，宜实施对集中代码数据库的阅读权限设置。此外，如果在组织内部使用开源代码或第三方代码组件，则可以广泛提供对此类外部代码数据库的读取权限。但编写权限仍然宜受到限制。

宜考虑采用以下指南来控制对源程序库的访问权限，以减少计算机程序损坏的可能性：

a) 按照既定规程管理对程序源代码和源程序库的访问权限；
b) 根据业务需要授予对源代码的读写访问权，并根据既定规程设法解决更改或误用的风险；
c) 根据变更控制规程（见 8.32）更新源代码和相关事项，并对源代码的访问权予以授予，且仅在收到适当授权后执行；
d) 不允许开发人员直接访问源代码存储库，而是通过开发人员工具来控制源代码活动和获取源代码授权；
e) 在一个安全的环境中保存程序列表，在这个环境中，读写权限宜得到适当的管理和分配；
f) 维护所有访问和源代码更改的审核日志。

如果计划发布程序源代码，则宜考虑额外的控制，以确保其完整性（如数字签名）。

8.4.5 其他信息

如果未正确控制对源代码的访问，则未授权的人员可能会篡改源代码或检索到开发环境中的某些数据（例如生产数据、配置详细信息的副本）。

8.5 安全鉴别

8.5.1 属性表

安全鉴别的属性表见表65。

表65 安全鉴别属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#身份和访问管理	#防护

8.5.2 控制

宜根据信息访问限制和访问控制的特定主题策略实现安全的鉴别技术和规程。

8.5.3 目的

在授予对系统、应用程序和服务的访问权限时，确保用户或实体得到安全的鉴别。

8.5.4 指南

宜选择适当的鉴别技术来证实用户、软件、消息和其他实体的身份。

鉴别的强度宜适合访问信息的分级。如果需要强鉴别和身份验证，宜使用替代口令的鉴别方法，如数字证书、智能卡、令牌或生物识别手段等。

鉴别信息宜附带访问关键信息系统的附加身份验证因素（也称为多因素身份验证）。结合使用多种鉴别因素，例如你知道什么、你拥有什么和你是什么，可以减少发生未经授权的访问的可能性。多因素鉴别可以与其他技术相结合，根据预定义的规则和模式，在特定情况下要求额外的验证因素，例如从不寻常的位置、不常用的设备或在特殊的时间进行访问。

如果生物特征鉴别信息被泄露，则宜使其失效。根据使用条件（例如潮湿或老化），生物特征鉴别可能不可用。为应对这些问题，生物特征鉴别宜至少伴随一种替代鉴别技术。

登录系统或应用程序的规程宜设计为将未经授权的访问的风险降至最低。登录规程和技术的实施宜考虑以下因素：

a) 在成功完成登录过程之前不显示敏感系统或应用程序信息，以避免向未授权的用户提供任何不必要的帮助；
b) 显示一般通知，警告系统、应用程序或服务只能由授权用户访问；
c) 在登录过程中不向未授权用户提供协助信息（例如，如果出现错误情况，系统

不指示数据的哪部分是正确的或不正确的）；

d) 仅在完成所有输入数据后验证登录信息；

e) 防止对用户名和口令的暴力登录尝试（例如，验证码（CAPTCHA）在预定义的失败尝试次数后要求重置口令，或在最大错误次数后拦截用户）；

f) 记录失败和成功的尝试；

g) 如果检测到可能试图或成功违反登录控制的行为，则将触发安全事态（例如，当达到一定数量的错误口令尝试时，向用户和组织的系统管理员发送警报）；

h) 成功登录后，在单独的通道上显示或发送以下信息：

1) 上次成功登录的日期和时间；

2) 自上次成功登录后，任何未成功登录尝试的详细信息；

i) 输入口令时不以明文显示口令；在某些情况下，可能不需要启用该功能，以方便用户登录（例如，出于可访问性原因或避免由于重复错误而拦截用户）；

j) 不通过网络传输明文口令，以避免被网络“嗅探器”程序捕获；

k) 在规定的非活动期后终止非活动会话，特别是在高风险位置，如组织安全管理之外的公共或外部区域或用户终端设备上；

l) 限制连接持续时间，为高风险应用程序提供额外的安全性，并减少未经授权的访问的机会窗口。

8.5.5 其他信息

有关实体鉴别保证的更多信息，参见ISO/IEC 29115。

8.6 容量管理

8.6.1 属性表

容量管理的属性表见表66。

表66 容量管理属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防 #检测	#完整性 #可用性	#识别 #防护 #发现	#连续性	#治理和生态体系 #防护

8.6.2 控制

宜根据当前和预期的容量需求，监视和调整资源的使用。

8.6.3 目的

确保信息处理设施、人力资源、办公室和其他设施所需的容量。

8.6.4 指南

宜识别信息处理设施、人力资源、办公室和其他设施的容量需求，同时考虑相关系统和过程的业务关键性。宜进行系统调整和监视，以确保并在必要时提高系统的可用性和效率。

组织宜对系统和服务进行压力测试，以确认有足够的系统容量来满足峰值性能要求。宜部署发现类控制，以便适时指出问题。

对未来容量需求的预测宜考虑到新的业务和系统需求以及本组织信息处理能力的当前和预测趋势。

宜特别注意采购周期长或成本高的任何资源。因此，管理者、服务或产品所有者宜监视关键系统资源的利用情况。

管理者宜使用容量信息来识别和避免可能对系统安全或服务构成威胁的潜在资源限制和对关键人员的依赖，并计划适当的行动。

通过增加容量或减少需求能实现足够容量的供给。宜考虑以下事项以增加容量：

a) 招聘新的工作人员；
b) 获得新的设施或空间；
c) 获得更强大的处理系统、内存和存储；
d) 利用云计算，它具有直接解决容量问题的固有特性。云计算具有弹性和可扩展性，能按需快速扩展和减少特定应用程序和服务的可用资源。

宜考虑以下事项以减少对组织资源的需求：

a) 删除过时数据（磁盘空间）；
b) 处置已达到保留期限的硬拷贝记录（释放搁架）；
c) 应用程序、系统、数据库或环境的停用；
d) 优化批处理过程和时间表；
e) 优化应用程序代码或数据库查询；
f) 拒绝或限制资源消耗服务的带宽，如果这些服务不是关键的（例如视频流）。对于关键任务系统，宜考虑一份记录在案的容量管理计划。

8.6.5 其他信息

有关云计算的弹性和可扩展性的更多详细信息，见ISO/IEC TS 23167。

8.7 恶意软件防范

8.7.1 属性表

恶意软件防范的属性表见表67。

表67 恶意软件防范属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防 #检测 #纠正	#保密性 #完整性 #可用性	#防护 #发现	#系统和网络安全 #信息保护	#防护 #防御

8.7.2 控制

宜实施恶意软件防范，并通过适当的用户意识教育予以支持。

8.7.3 目的

确保信息及其他相关资产免受恶意软件攻击。

8.7.4 指南

恶意软件防范宜基于恶意软件检测和修复软件、信息安全意识、适当的系统访问和变更管理控制。仅使用恶意软件检测和修复软件通常是不够的。宜考虑以下指南：

a) 实施防止或检测未经授权软件使用的规则和控制［例如，应用程序许可列表（即使用提供许可应用程序的列表）］（见 8.19 和 8.32）；
b) 实施防止或发现使用已知或可疑恶意网站的控制（例如，阻止列表）；
c) 减少恶意软件可利用的脆弱性［例如，通过技术脆弱性管理（见 8.8 和 8.19）］；
d) 定期自动验证系统的软件和数据内容，尤其是支持关键业务过程的系统；调查是否存在任何未经批准的文件或未经授权的修改；
e) 针对源自或通过外部网络或从任何其他媒体上获取文件和软件的相关风险建立保护措施；
f) 安装并定期更新恶意软件检测和修复软件，以扫描计算机和电子存储媒体。进行定期扫描，包括：
   1) 在使用前，扫描通过网络或任何形式的电子存储媒体接收的任何数据以发现恶意软件；
   2) 在使用前，扫描电子邮件和即时消息附件以及下载以发现恶意软件。在不同地点（例如，电子邮件服务器、台式计算机）和接入组织网络时进行扫描；
   3) 在访问前，扫描网页以发现恶意软件。
g) 基于风险评估结果确定恶意软件检测和修复工具的安置和配置，并考虑：
   1) 在最有效的地方进行纵深防御。例如，在网络网关（诸如电子邮件、文件传输和 web 的各种应用协议中）以及用户终端设备和服务器中检测恶意软件；
   2) 攻击者的规避技术（例如，使用加密文件）来传输恶意软件或使用加密协议传输恶意软件。
h) 在维护和应急期间，注意防止可能绕过对恶意软件的正常控制而引入恶意软件；
i) 实施一个过程，以授权临时或永久禁用防范恶意软件的部分或所有措施，包括例外批准权限、记录的批准理由和评审日期。当恶意软件防范导致正常操作中断时，这可能是必要的；
j) 为从恶意软件攻击中恢复，准备适当的业务连续性计划，包括所有必要的数据和软件备份（包括在线和离线备份）以及恢复措施（见 8.13）；
k) 隔离可能发生灾难性后果的环境；
l) 明确在系统上防范恶意软件的规程和责任，包括对其使用以及报告恶意软件攻击并从中恢复的培训；
m) 向所有用户提供意识教育或培训（见 6.3），使其了解如何识别和可能减少接收、发送或安装被恶意软件感染的电子邮件、文件或程序［在 n)和 o)中收集的信息能用于确保意识教育和培训保持最新］；

n) 实施定期收集新恶意软件信息的规程，诸如订阅邮件列表或查看相关网站；

o) 验证与恶意软件相关的信息，诸如警告公告，是否来自合格和信誉良好的来源（例如，可靠的互联网网站或恶意软件检测供应商），并且是否准确和有用的。

8.7.5 其他信息

在某些系统（例如，某些工业控制系统）上安装防范恶意软件的软件并不总是可能的。某些形式的恶意软件感染计算机操作系统和计算机固件，使得常见的恶意软件控制不能将系统清理干净，这就有必要对操作系统软件，有时还包括对计算机固件进行完全重新镜像，以恢复到安全状态。

8.8 技术脆弱性管理

8.8.1 属性表

技术脆弱性管理的属性表见表68。

表68 技术脆弱性管理属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#识别 #防护	#威胁和脆弱性管理	#治理和生态体系 #防护 #防御

8.8.2 控制

宜获取有关使用中的信息系统的技术脆弱性的信息，评价组织暴露于此类脆弱性的风险，并采取适当措施。

8.8.3 目的

防止利用技术脆弱性。

8.8.4 指南

8.8.4.1 识别技术脆弱性

组织宜拥有准确的资产清单（见5.9至5.14），作为有效技术脆弱性管理的先决条件；清单宜包括软件供应商、软件名称、版本号、当前部署状态（例如，在哪些系统上安装了哪些软件）以及组织内负责软件的人员。

为了识别技术脆弱性，组织宜考虑：

a) 明确并确立与技术脆弱性管理相关的角色和责任，包括脆弱性监视、脆弱性风险评估、更新、资产跟踪和所需的任何协调责任；

b) 对于软件和其他技术（基于资产清单，见 5.9），识别将用于识别相关技术脆弱性并保持对其感知的信息资源。根据资产清单的变化或发现其他新的或有用的资源时，更新信息资源清单；

c) 要求信息系统供应商（包括其组件）确保脆弱性报告、处理和披露，包括适用合同中的要求（见 5.20）；

d) 使用适用于所用技术的脆弱性扫描工具来识别脆弱性，并验证脆弱性修补是否成功；

e) 由能够胜任且被授权人员进行有计划、有记录和可重复的渗透测试或脆弱性评估，以支持脆弱性识别。因为此类活动可能导致系统安全受损，需谨慎行事；

f) 跟踪第三方库和源代码的使用情况以发现脆弱性。这宜包括在安全编码中（见8.28）。

组织宜制定规程和发展能力，以：

a) 检测其产品和服务中是否存在脆弱性，包括这些产品和服务中使用的任何外部组件；

b) 从内部或外部来源接收脆弱性报告。

组织宜提供一个公共联络点，作为脆弱性披露专题策略的一部分，以便研究人员和其他人能够报告问题。组织宜建立脆弱性报告规程、在线报告表格，并利用适当的威胁情报或信息共享论坛。组织还宜考虑提供缺陷奖励计划来激励组织识别脆弱性，以便适当地补救脆弱性。组织还宜与主管行业机构或其他利益相关方共享信息。

8.8.4.2 评价技术脆弱性

为评价已识别的技术脆弱性，宜考虑以下指南：

a) 分析和验证报告，以确定需要什么样的应对和补救活动；

b) 一旦确定了潜在的技术脆弱性，就要确定相关风险和要采取的行动。此类行动可能涉及更新易受攻击的系统或应用其他控制。

8.8.4.3 采取适当的措施解决技术脆弱性

宜实施软件更新管理过程，以确保为所有授权软件安装最新的批准补丁和应用程序更新。如果需要变更，宜保留原始软件，并将变更应用于指定副本。所有变更都宜经过充分测试和记录，以便在必要时重新应用于未来的软件升级。如果需要，这些修改宜由独立评估机构进行测试和验证。

宜考虑以下指南来解决技术脆弱性：

a) 对潜在技术脆弱性的识别采取适当和及时的行动；明确对潜在相关技术脆弱性通知做出反应的时间表；

b) 依据需要解决技术脆弱性的紧迫程度，根据与变更管理相关的控制（见 8.32）或通过遵循信息安全事件响应规程（见 5.26）采取行动；

c) 仅使用合法来源（可能是组织内部的或外部的）的更新；

d) 在安装更新之前对其进行测试和评价，以确保其有效且不会产生无法容忍的副作用［即，如果更新可用，评估与安装更新相关的风险（宜将脆弱性带来的风险与安装更新的风险进行比较）］；

e) 首先应对高风险系统；

f) 开发补救措施（通常是软件更新或补丁）；

g) 测试以确认补救或缓解措施是否有效；

h) 提供验证补救措施真实性的机制；

i) 如果没有可用的更新或无法安装更新，考虑其他控制，诸如：

1) 采用软件供应商或其他相关来源建议的任何变通方法；

2) 关闭与脆弱性相关的服务或功能；
3) 在网络边界调整或添加访问控制（例如，防火墙）（见 8.20 至 8.22）；
4) 通过部署合适的流量过滤器（有时称为虚拟补丁），保护易受攻击的系统、设备或应用程序免受攻击；
5) 增加监视以发现实际攻击；
6) 提高对脆弱性的认识。

对于获得的软件，如果供应商定期发布其软件的安全更新信息，并提供自动安装此类更新的设施，则组织宜决定是否使用自动更新。

8.8.4.4 其他考虑

宜对技术脆弱性管理中采取的所有步骤保留审核日志。

宜定期监视和评价技术脆弱性管理过程，以确保其有效性和效率。

有效的技术脆弱性管理过程宜与事件管理活动保持一致，以便向事件响应功能传递有关脆弱性的数据，并提供在事件发生时要执行的技术规程。

当组织使用第三方云服务提供者提供的云服务时，云服务提供者宜确保对其资源的技术脆弱性管理。云服务提供者的技术脆弱性管理责任宜是云服务协议的一部分，其中宜包括报告云服务提供者进行与技术脆弱性相关行动的过程（见5.23）。对于某些云服务，云服务提供者和云服务客户分别负有责任。例如，云服务客户负责对其用于云服务的自有资产进行脆弱性管理。

8.8.5 其他信息

技术脆弱性管理可被视为变更管理的子功能，因此可利用变更管理过程和规程（见8.32）。

更新可能无法充分解决问题，并产生负面副作用。此外，在某些情况下，一旦应用了更新，就很难卸载更新。

如果无法对更新进行充分测试（例如，由于成本或缺乏资源），可考虑延迟更新，以根据其他用户的经验评价相关风险。使用ISO/IEC 27031可能是有益的。

在产生软件补丁或更新的地方，组织可考虑提供自动更新过程，将这些更新安装在受影响的系统或产品上，而无需客户或用户的干预。如果提供了自动更新过程，则可允许客户或用户选择关闭自动更新或控制更新安装时间的选项。

当供应商提供了自动更新过程，并且可在不需要干预的情况下将更新安装到受影响的系统或产品上时，组织来决定是否应用自动过程。不选择自动更新的一个原因是保留对何时执行更新的控制。例如，在业务操作完成之前，不能更新用于该操作的软件。

脆弱性扫描的一个弱点是，它可能没有充分考虑到纵深防御：总是按顺序调用的两种对策可能有被另一种策略屏蔽的脆弱性。复合对策不易受攻击，而脆弱性扫描器可能报告这两个组件都易受攻击。因此，组织宜注意评审脆弱性报告并采取行动。

许多组织不仅在组织内部，而且还向诸如客户、合作伙伴或其他用户的利益相关方提供软件、系统、产品和服务。这些软件、系统、产品和服务可能存在影响用户安全

的信息安全脆弱性。

组织可向用户发布补救措施和披露脆弱性信息（通常通过公共咨询），并为软件脆弱性数据库服务提供适当的信息。

有关使用云计算时技术脆弱性管理的更多信息，见ISO/IEC 19086系列和ISO/IEC 27017。

ISO/IEC 29147提供了有关接收脆弱性报告和发布脆弱性建议的详细信息。ISO/IEC 30111提供了有关处理和解决报告的脆弱性的详细信息。

8.9 配置管理

8.9.1 属性表

配置管理的属性表见表69。

表69 配置管理属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#安全配置	#防护

8.9.2 控制

宜建立、记录、实施、监视和评审硬件、软件、服务和网络的配置，包括安全配置。

8.9.3 目的

确保硬件、软件、服务和网络在要求的安全设置下正常运行，并且配置不会因未经授权或不正确的变更而改变。

8.9.4 指南

8.9.4.1 总则

组织宜明确并实施过程和工具，以在硬件、软件、服务（例如，云服务）和网络、新安装的系统以及操作系统的整个生存周期内强制执行已定义的配置（包括安全配置）。

角色、职责和规程宜配备到位，以确保对所有配置变更进行恰当的控制。

8.9.4.2 标准模板

宜定义硬件、软件、服务和网络安全配置的标准模板：

a) 使用公开可用的指南（例如，来自供应商和独立安全组织的预定义模板）；
b) 考虑所需的保护级别，以确定足够的安全级别；
c) 支持组织的信息安全方针、特定主题策略、标准和其他安全要求；
d) 考虑安全配置在组织环境中的可行性和适用性。

宜定期评审模板，并在需要解决新的威胁或脆弱性时，或在引入新的软件或硬件版本时更新模板。在为硬件、软件、服务和网络的安全配置建立标准模板时，宜考虑以下

事项：

a) 最小化具有特权或管理员级别访问权限的身份的数量；
b) 禁用不必要、未使用或不安全的身份；
c) 禁用或限制不必要的功能和服务；
d) 限制对强大实用程序和主机参数设置的访问；
e) 同步时钟；
f) 安装后立即更改厂商默认的鉴别信息（诸如默认口令），并查看其他重要的默认安全相关参数；
g) 调用超时功能，以此在预定的不活动期后自动注销计算设备；
h) 验证是否满足许可证要求（见 5.32）。

8.9.4.3 管理配置

宜记录硬件、软件、服务和网络的既定配置，并维持所有配置变更的日志。这些记录宜安全保存。这可通过多种方式实现，诸如配置数据库或配置模板。

配置变更宜遵循变更管理过程（见8.32）。配置记录可包含相关信息：

a) 资产的最新拥有者或联系信息；
b) 上次配置变更的日期；
c) 配置模板的版本；
d) 与其他资产配置的关系。

8.9.4.4 监控配置

宜使用一套全面的系统管理工具（例如，维护工具、远程支持、企业管理工具、备份和恢复软件）对配置进行监控，并宜定期评审，以验证配置设置、评估口令强度和评估执行的活动。可将实际配置与定义的目标模板进行比较。宜通过自动执行定义的目标配置或手动分析偏差并采取纠正措施来解决所有偏差。

8.9.4.5 其他信息

系统文档通常记录硬件和软件配置的详细信息。系统强化是配置管理的典型部分。

配置管理可与资产管理过程和相关工具集成。

自动化通常更有效地管理安全配置（例如，采用基础设施即代码）。配置模板和目标可能是保密信息，因此宜防止未经授权的访问。

8.10 信息删除

8.10.1 属性表

信息删除的属性表见表70。

表70 信息删除属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性	#防护	#信息保护 #合法合规	#防护

8.10.2 控制

当不再需要时，宜删除存储在信息系统、设备或任何其他存储媒体中的信息。

8.10.3 目的

防止敏感信息不必要的暴露，并遵守法律、法规、规章和合同等有关信息删除的要求。

8.10.4 指南

8.10.4.1 总则

敏感信息的保存时间不宜超过其所需的时间，以降低不当披露的风险。删除有关系统、应用程序和服务的信息时，宜考虑以下事项：

a) 根据业务需求并考虑相关法律、法规和规章，选择删除方法（例如，电子盖写或加密擦除）；
b) 记录删除结果作为证据；
c) 当使用信息删除服务供应商时，从其获取信息删除证据。

如果第三方代表组织存储其信息，该组织宜考虑将信息删除的要求纳入第三方协议，以便在此类服务存续期间和终止时强制执行。

8.10.4.2 删除方法

根据本组织关于数据保留的特定主题策略，并考虑到相关法律、法规和规章，当不再需要时，宜通过以下方式删除敏感信息：

a) 将系统配置为在不再需要时安全地销毁信息（例如，在数据保留的特定主题策略或主题访问请求所规定的期限之后）；
b) 删除任何位置的过时版本、副本和临时文件；
c) 使用经批准的安全删除软件永久删除信息，以帮助确保无法使用专业恢复或取证工具恢复信息；
d) 使用经批准、认证的安全处置服务提供者；
e) 使用适合于被处置存储媒体类型的处置机制（例如，对硬盘驱动器和其他磁性存储媒体进行消磁）。

在使用云服务的情况下，组织宜验证云服务提供者提供的删除方法是否可接受，如果可接收，组织宜使用该方法，或要求云服务提供者删除信息。在可用且适用的情况下，宜根据特定主题策略自动执行这些删除过程。根据被删除信息的敏感性，日志能跟踪或验证这些删除过程是否已发生。

为了避免在将设备送回供应商时无意中暴露敏感信息，宜在设备离开组织场所之前移除辅助存储器（例如，硬盘驱动器）和内存，以保护敏感信息。

考虑到某些设备（例如，智能手机）的安全删除只能通过销毁或使用这些设备中嵌入的功能（例如，“恢复出厂设置”）来实现，组织宜根据此类设备处理的信息分级选择适当的方法。

7.14中描述的控制应用于物理销毁存储设备，同时删除其包含的信息。在分析可能

的信息泄漏事件的原因时，信息删除的正式记录非常有用。

8.10.5 其他信息

有关云服务中用户数据删除的信息，见ISO/IEC 27017。有关删除PII的信息，见ISO/IEC 27555。

8.11 数据脱敏

8.11.1 属性表

数据脱敏的属性表见表71。

表71 数据脱敏属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性	#防护	#信息保护	#防护

8.11.2 控制

宜根据组织关于访问控制的特定主题策略和其他相关的特定主题策略以及业务要求使用数据脱敏，并考虑到适用的法律法规。

8.11.3 目的

限制敏感数据（包括PII）的暴露，并遵守法律、法规、规章和合同要求。

8.11.4 指南

如果需要保护敏感数据（例如，PII），组织宜考虑使用诸如数据掩蔽、假名化或匿名化的技术来隐藏此类数据。

假名化或匿名化技术能隐藏PII，掩蔽PII主体或其他敏感信息的真实身份，并断开PII与PII主体身份或与其他敏感信息之间的链接。

当使用假名化或匿名化技术时，宜验证数据是否已进行了充分的假名化或匿名化。数据匿名化宜考虑敏感信息的所有元素是有效的。作为例子，如果考虑不当，即便能直接识别此人的数据是匿名的，也能通过更多数据来间接识别此人。

数据脱敏的其他技术包括：

a) 加密（要求授权用户拥有密钥）；
b) 清空或删除字符（防止未经授权的用户看到完整的消息）；
c) 不同的数字和日期；
d) 替换（将一个值替换为另一个值以隐藏敏感数据）；
e) 用散列替换值。

在实施数据脱敏技术时，宜考虑以下几点：

a) 不允许所有用户访问所有数据，因此设计查询和掩码，以便仅向用户显示所需的最小数据；
b) 在有些情况下，对于一组数据中的某些记录，用户不宜看到某些数据；在此情况下，设计和实施数据混淆处理机制（例如，如果患者不希望医院工作人员

能够看到他们的所有记录，即使在紧急情况下，那么呈现给医院工作人员的是部分混淆数据，并且只有在数据包含用于适当治疗的有用信息的情况下，具有特定角色的工作人员才能访问数据）；

c) 当数据被混淆时，PII 主体可要求用户不知道数据是否被混淆（混淆了混淆过程，在医疗设施中可能使用，例如，患者不想让工作人员知道诸如怀孕或血液检查结果等敏感信息被混淆）；

d) 任何法律、法规或规章要求（例如，要求在处理或存储期间掩藏支付卡信息）。

在使用数据掩蔽、假名化或匿名化时，宜考虑以下事项：

a) 根据所处理数据的使用情况确定数据掩蔽、假名化或匿名化的程度强弱；

b) 对所处理数据的访问控制；

c) 对所处理数据使用方法的协议或限制；

d) 禁止将所处理数据与其他信息进行核对，以识别 PII 主体；

e) 跟踪所处理数据的提供和接收。

8.11.5 其他信息

匿名化不可逆转地改变了PII，以至于无法再直接或间接地识别PII主体。

假名化将标识信息替换为别名。对用于执行假名化的算法（有时称为“附加信息”）的了解允许至少以某种形式识别PII主体。因此，此类“附加信息”宜单独保存并加以保护。

虽然假名化因此比匿名化弱，但假名化数据集在统计研究中可能更有用。

数据脱敏是一组隐藏、替换或混淆敏感数据项的技术。数据脱敏可以是静态的（当数据项在原始数据库中被掩蔽时）、动态的（使用自动化和规则来实时保护数据）或即时的（数据在应用程序内存中被掩蔽）。

散列函数能被用来匿名化PII。为防止枚举攻击，此类函数宜始终与加盐函数结合使用。

资源标识符及其属性［例如，文件名、统一资源定位符（URL）］中的PII宜避免或适当匿名。ISO/IEC 27018中给出了有关公有云中PII保护的其他控制。

ISO/IEC 20889中提供了有关去识别技术的其他信息。

8.12 数据防泄露

8.12.1 属性表

数据防泄露的属性表见表72。

表72 数据防泄露属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防 #检测	#保密性	#防护 #发现	#信息保护	#防护 #防御

8.12.2 控制

数据防泄露措施宜用于处理、存储或传输敏感信息的系统、网络和任何其他设备。

8.12.3 目的

检测（detect）并防止个人或系统未经授权披露和提取信息。

8.12.4 指南

组织宜考虑以下事项以减少数据泄露的风险：

a) 识别并对信息进行分级以防止泄露（例如，个人信息、定价模型和产品设计）；
b) 监视数据泄露的渠道（例如，电子邮件、文件传输、移动设备和便携式存储设备）；
c) 采取措施防止信息泄露（例如，隔离包含敏感信息的电子邮件）。数据防泄露工具宜用于：
d) 识别并监视处于未经授权披露风险中的敏感信息（例如，用户系统上非结构化数据中的敏感信息）；
e) 检测敏感信息的泄露（例如，信息上传到不受信任的第三方云服务或通过电子邮件发送时）；
f) 阻止暴露敏感信息的用户行为或网络传输（例如，防止将数据库条目复制到电子表格中）。

组织宜确定是否有必要限制用户复制、粘贴或将数据上传到组织外的服务、设备和存储媒体的能力。如果存在这种情况，组织宜实施技术措施允许用户查看和操作远程保存的数据，例如采用数据防泄露工具或对现有工具进行配置，但需防止在组织控制之外进行复制和粘贴。如果需要导出数据，宜由数据拥有者批准，并要求用户对其行为负责。

宜通过使用条款和条件、培训及审计等方式解决屏幕截图或拍照问题。

在备份数据的位置，宜确保使用加密、访问控制和对保存备份的存储媒体进行物理保护等措施来保护敏感信息。数据防泄露还宜考虑用于防止对手的情报活动获取保密或秘密信息（地缘政治、人力、金融、商业、科学或任何其他信息），这些信息可能利于间谍活动或对社会至关重要。无论作为独立措施还是对对手情报活动的回应，数据防泄露措施宜着眼于混淆对手的决策，如将真实信息替换为虚假信息。此类措施例如逆向社会工程或使用蜜罐吸引攻击者。

8.12.5 其他信息

数据防泄露工具旨在识别数据、监视数据的使用和移动，并采取措施防止数据泄露（例如，提醒用户注意其危险行为，并阻止数据向便携式存储设备的传输）。

数据防泄露本质上会涉及监视人员的通信和在线活动，并扩展到外部方的消息，如果可能引发法律问题，宜在部署数据防泄露工具之前予以考虑。与隐私、数据保护、任用、数据截获和电信相关的很多法律法规，适用于与数据防泄露相关的监视和数据处理。

一些标准安全控制能支持数据防泄露，例如访问控制和安全文件管理（见5.12和5.15）的特定主题策略。

8.13 信息备份

8.13.1 属性表

信息备份的属性表见表73。

表73 信息备份属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#纠正	#完整性 #可用性	#恢复	#连续性	#防护

8.13.2 控制

信息、软件和系统的备份副本宜按照商定的备份特定主题策略进行维护和定期测试。

8.13.3 目的

能够恢复丢失的数据或系统。

8.13.4 指南

宜建立针对备份的特定主题策略来满足组织的数据保存和信息安全要求。

宜提供充足的备份设施，以确保所有必要的信息和软件在存储媒体发生事件、失效或丢失后能够恢复。宜针对组织如何备份信息、软件和系统制定并实施计划，以满足备份的特定主题策略。

设计备份计划时宜考虑以下事项：

a) 建立备份副本的准确完整的记录，以及文件化的恢复规程；
b) 在备份的程度（例如，完全备份或差异备份）和频率中反映组织的业务要求（例如，恢复点目标，见 5.30）、涉及信息的安全要求和信息对组织持续运行的关键程度；
c) 将备份存储在安全可靠的远程地点，与主站点相隔足够距离，以避免主站点发生灾难时受到损坏；
d) 给予备份信息一个与主站点应用标准相一致的适当的物理和环境保护级别（见 7 和 8.1）；
e) 定期测试备份媒体，以确保必要时，可在紧急情况下使用这些备份媒体。在测试系统上测试恢复备份数据的能力，而不是覆盖原始存储媒体，以防备份或恢复过程中出现故障，导致无法挽回的数据损坏或丢失；
f) 根据已识别的风险（例如，在保密性较为重要的情况下）通过加密手段保护备份；
g) 注意确保在进行备份之前可检测到意外的数据丢失。

操作规程宜监视备份的执行情况，解决执行计划备份失败的情况，以便根据备份的特定主题策略确保备份的完整性。

宜定期测试单个系统和服务的备份措施以确保其满足事件响应及业务连续性计划（见5.30）的目标。上述测试宜与恢复规程测试相结合，并根据业务连续性计划所需的恢复时间进行检查。对于关键系统和服务，备份措施宜覆盖在发生灾难时恢复完整系统必需的所有系统信息、应用程序和数据。

当组织使用云服务时，宜获取在云服务环境中组织信息、应用程序和系统的备份副本。当使用云服务所提供的信息备份服务时，组织宜确定是否以及如何满足备份要求。

宜确定基本业务信息的保存周期，并考虑保存归档文件副本的任何要求。当信息保存周期届满后，组织宜考虑将备份存储媒体中的信息删除（见8.10），法律和法规的要求也宜考虑在内。

8.13.5 其他信息

有关存储安全（包括保存方面的考虑事项）的更多信息，见ISO/IEC 27040。

8.14 信息处理设施的冗余

8.14.1 属性表

信息处理设施的冗余的属性表见表74。

表74 信息处理设施的冗余属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#可用性	#防护	#连续性 #资产管理	#防护 #弹性

8.14.2 控制

信息处理设施宜具有足够的冗余以满足可用性要求。

8.14.3 目的

确保信息处理设施的持续运行。

8.14.4 指南

组织宜识别业务服务和信息系统的可用性要求。组织宜设计并实施具有适当冗余的系统架构，以满足这些要求。

可通过复制部分或全部信息处理设施（例如，备用组件或全部双份）而达到冗余目的。组织宜计划并实施激活冗余组件和处理设施的规程。规程宜确定冗余组件和处理活动是否始终处于激活状态，或在紧急情况下可自动或手动激活。宜确保冗余组件和冗余信息处理设施与主组件和主信息处理设施保持相同的安全级别。

宜有机制对信息处理设施的故障进行告警，使组织能够执行计划的规程，并允许在信息处理设施维修或更换时持续可用。

当实现冗余系统时，组织宜考虑以下事项：

a) 与两个或多个网络和关键信息处理设施供应商（例如，互联网服务提供者）签订合同；
b) 使用冗余的网络；
c) 使用两个地理上分离且具备镜像系统的数据中心；
d) 使用物理冗余的供电设施或供电来源；
e) 使用软件组件的多个并行实例，并在实例之间（同一数据中心或不同数据中心的实例之间）进行自动负载均衡；
f) 具有系统的复制组件（例如，CPU、硬盘、内存）或网络的复制组件（例如，防火墙、路由器、交换机）。适用时，宜在生产模式测试冗余信息系统，以确保

从一个组件到另一个组件的故障切换按预期执行。

8.14.5 其他信息

在要求短时间内恢复的情况下，冗余与业务连续性的信息通信技术就绪（见5.30）之间有着密切的关系，许多冗余措施可以作为ICT连续性战略和解决方案的一部分。

实施冗余可能给信息和信息系统的完整性（例如，将数据拷贝到复制组件的过程可能会导致错误）或保密性（例如，复制组件的薄弱安全控制可能导致保密性受损）造成风险，在设计信息系统时宜予以考虑。

信息处理设施的冗余通常不会解决由于应用程序内部故障导致的应用程序不可用问题。

通过使用公有云计算，信息处理设施的多个实时版本可能存在于多个分离的物理位置，相互之间具备自动故障切换和负载均衡。

ISO/IEC TS 23167讨论了在云服务环境中提供冗余和自动故障切换的一些技术及措施。

8.15 日志

8.15.1 属性表

日志的属性表见表75。

表75 日志属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#检测	#保密性 #完整性 #可用性	#识别	#信息安全事态管理	#防护 #防御

8.15.2 控制

宜生成、存储、保护和分析用于记录活动、异常、故障及其他相关事态的日志。

8.15.3 目的

记录事态，生成证据，确保日志信息的完整性，防止未经授权的访问，识别可能导致信息安全事件的信息安全事态，并支持调查。

8.15.4 指南

8.15.4.1 总则

组织宜确定创建日志的目的、收集和记录的数据以及保护、处理日志数据时对日志的任何特定要求。这些宜在日志的特定主题策略中文件化。

适用时，事态日志宜包括每个事态的以下事项：

a) 用户 ID；
b) 系统活动；

c) 相关事态的日期、时间和细节，例如登录和退出；
d) 设备标识、系统标识和位置；
e) 网络地址和协议。

记录日志时宜考虑下列事态：

a) 成功的和被拒绝的对系统的访问尝试；
b) 成功的和被拒绝的对数据以及其他资源的访问尝试；
c) 系统配置的变更；
d) 特权的使用；
e) 实用程序和应用程序的使用；
f) 被访问的文件和访问类型，包括重要数据文件的删除；
g) 由访问控制系统发出的警报；
h) 安全系统的激活和停用，例如防病毒系统和入侵检测系统；
i) 标识的创建、修改或删除；
j) 用户在应用程序中执行的事务。在某些情况下，应用程序是由第三方提供或运行的服务或产品。

重要的是，所有系统均具备同步的时间源（见8.17），这样可使系统之间日志相互关联，以便对事件进行分析、告警和调查。

8.15.4.2 日志的保护

用户，包括拥有特许访问权的用户，不宜拥有删除或停用其自身活动日志的权限。他们可能会操纵其直接控制的信息处理设施上的日志。因此，有必要保护和评审这些日志，以维护对特权用户的问责。

宜实施控制以防止日志信息的未经授权变更和日志设施的运行问题，包括：

a) 对已记录的消息类型的更改；
b) 日志文件被编辑或删除；
c) 存放日志文件的存储媒体空间不足时，导致无法记录事态或过去记录的事态被覆盖。

为了保护日志，宜考虑使用以下技术：密码散列、在追加型和只读文件中进行记录、和在公开透明文件中进行记录。

一些审计日志可能由于数据保存要求或证据收集和保留要求（见5.28）进行归档。

若组织需要向厂商发送系统或应用程序日志以协助调试或排除错误，在发送厂商前，宜尽可能使用数据脱敏技术（见8.11）对日志进行去标识化处理，包括用户名、互联网协议地址（IP）、主机名或组织名等信息。

事态日志可能包含敏感数据和个人可识别信息。宜采取适当的隐私保护措施（见5.34）。

8.15.4.3 日志分析

日志分析宜覆盖对信息安全事态的分析和解释，以帮助识别异常活动或异常行为，从而反映出受损的迹象。对信息安全事态的分析宜考虑以下事项：

a) 执行分析的专家所需的技能；
b) 确定日志分析规程；
c) 每个安全相关事态所要求的属性；
d) 通过使用预先确定的规则[例如，安全信息和事件管理（SIEM）或防火墙规则以及入侵检测系统（IDS）或恶意软件签名等]所识别的例外情况；
e) 相较于异常活动和行为的已知行为模式和标准网络流量[用户和实体行为分析（UEBA）]；
f) 趋势或模式分析的结果（例如，使用数据分析、大数据技术和专业分析工具等产生的结果）；
g) 可用的威胁情报。

日志分析宜得到特定监视活动的支持，以帮助识别和分析异常行为，包括：

a) 评审成功的和失败的对受保护资源[例如，域名系统（DNS）服务器、门户网站和文件共享等]的访问尝试；
b) 检查 DNS 日志，以识别与恶意服务器的出站网络连接，例如与僵尸网络命令和控制服务器相关的连接；
c) 检查服务提供者的使用情况报告（例如，费用清单或服务报告），以确定系统和网络内的异常活动（例如，通过评审活动模式）；
d) 包括物理监视（诸如出入口）的事态日志，以确保更准确的异常发现和事件分析；
e) 关联日志以实现有效且高度准确的分析。

宜识别可疑和实际的信息安全事件（例如，恶意软件感染或防火墙探测），并开展进一步调查（例如，作为信息安全事件管理过程的一部分，见5.25）。

8.15.5 其他信息

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，宜考虑使用适合的实用程序或审计工具执行文件查询。

事态日志为自动监视系统（见8.16）奠定基础，能够对系统安全产生综合报告和告警。

SIEM工具或等效服务可用于存储、关联、规范化和分析日志信息，并生成告警。SIEM要仔细配置，以优化其效益。考虑的配置包括标识和选择适当的日志源、规则的调整及测试以及用例的开发。

使用公开透明文件记录日志，如证书透明系统。这样的文件可以提供额外的检测机制，有助于防止日志被篡改。

在云环境中，可以在云服务客户和云服务提供者之间共享日志管理职责。根据使用的云服务的类型，职责有所不同。更多指南可在ISO/IEC 27017中找到。

8.16 监视活动

8.16.1 属性表

监视活动的属性表见表76。

表76 监视活动属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#检测 #纠正	#保密性 #完整性 #可用性	#发现 #响应	#信息安全事态管理	#防御

8.16.2 控制

宜监视网络、系统和应用程序，以发现异常行为，并采取适当措施评价潜在的信息安全事件。

8.16.3 目的

发现（detect）异常行为和潜在的信息安全事件。

8.16.4 指南

监视范围和级别宜根据业务及信息安全要求，并考虑相关法律法规予以确定。宜根据业务及信息安全要求，并考虑相关法律法规，确定监视范围和级别。监视记录宜在规定的保存周期内进行维护。

宜考虑将以下事项纳入监视系统：

a) 网络、系统和应用程序的出入流量；
b) 系统、服务器、网络设备、监视系统、关键应用程序等的访问；
c) 关键或管理级系统和网络配置文件；
d) 来自安全工具的日志，如反病毒、IDS、入侵防御系统（IPS）、web 过滤器、防火墙、数据防泄露系统等；
e) 与系统和网络活动相关的事态日志；
f) 检查正在执行的代码是否被授权在系统中运行，并且未被篡改（例如通过重新编译添加不必要代码）；
g) 资源（例如，CPU、硬盘、内存、带宽）的使用及其性能。

组织宜建立正常行为的基线，并根据该基线监视异常情况。建立基线时，宜考虑以下事项：

a) 评审系统在平常和高峰期的使用情况；
b) 每个用户或用户组的正常访问时间、访问位置、访问频率。

监视系统宜根据既定基线进行配置，以识别异常行为，例如：

a) 过程或应用程序的意外终止；
b) 通常与恶意软件有关的活动或者源于已知恶意 IP 地址或网络域（例如，与僵尸网络命令和控制服务器有关）的流量；
c) 已知攻击特征（例如，拒绝服务和缓冲区溢出）；
d) 异常的系统行为（例如，击键记录、过程注入和标准协议的使用偏差等）；

e) 瓶颈和过载（例如，网络排队、延迟级别和网络抖动）；
f) 系统或信息未经授权的访问（实际或尝试）；
g) 业务应用程序、系统和网络的未经授权扫描；
h) 对受保护资源（例如，DNS 服务器、门户网站和文件系统）成功和失败的访问尝试；
i) 与预期行为相关的异常用户和系统行为。

宜使用监视工具进行持续监视。宜根据组织需要和能力，实时或定期进行监视。监视工具宜包括处理大量数据、适应不断变化的威胁形势及允许实时通知的能力。这些工具还宜能够识别特定的签名和数据、网络或应用程序行为模式。

宜将自动化监视软件配置为根据预定义阈值生成告警（例如，通过管理控制台、电子邮件或即时通信系统）。告警系统宜根据组织的基线进行调整和训练，以尽量减少误报。宜有专人对告警作出响应，并接受适当培训，以准确解释潜在事件。宜配备冗余系统和过程来接收和响应告警通知。

宜将异常事态传达给相关方，以改进以下活动：审计、安全评价、脆弱性扫描和监视（见5.25）。宜制定规程，来及时响应监视系统的正指标，以尽量减少不良事态（见5.26）对信息安全的影响。还宜建立识别和处理误报的规程，包括调整监视软件以减少未来误报的数量。

8.16.5 其他信息

可以通过下列方式加强安全监视：

a) 利用威胁情报系统（见 5.7）；
b) 利用机器学习和人工智能的能力；
c) 使用黑名单或白名单；
d) 执行系列技术安全评估（例如，脆弱性评估、渗透测试、网络攻击模拟和网络响应演习），并利用这些评估的结果帮助确定基线或可接受的行为；
e) 使用性能监视系统帮助确定和发现（detect）异常行为；
f) 将日志与监视系统结合使用。

通常使用诸如入侵检测系统等专业软件执行监视活动。这些活动可配置为正常、可接受、预期的系统和网络活动的基线。

监视异常通信有助于识别僵尸网络（即僵尸网络拥有者恶意控制下的一组设备，通常用于向其他组织的其他计算机上发动分布式拒绝服务攻击）。如果计算机由外部设备控制，则受感染的设备与控制器之间存在通信。因此，组织宜使用技术手段监视异常通信，并采取必要的措施。

8.17 时钟同步

8.17.1 属性表

时钟同步的属性表见表77。

表77 时钟同步属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#检测	#完整性	#防护 #发现	#信息安全事态管理	#防护 #防御

8.17.2 控制

组织使用的信息处理系统的时钟宜与批准的时间源同步。

8.17.3 目的

能够关联和分析安全相关事态及其他记录数据，并支持对信息安全事件的调查。

8.17.4 指南

宜文件化并实施内外部的时间显示、可靠同步和准确性要求。这些要求可来自于法律法规、合同、标准和内部监视的需求。宜定义组织内使用的标准参照时间，并考虑用于所有系统，包括建筑物管理系统、出入系统和其他可用于协助调查的系统。

宜使用与国家原子钟或全球导航卫星系统（GNSS）等广播的无线电时间相关联的时钟，作为日志系统的参考时钟；采用一致、可靠的日期和时间源，以确保准确的时间戳。宜使用诸如网络时间协议（NTP）或精确时间协议（PTP）等协议来保持所有联网系统与基准时钟同步。

组织可以同时使用两个外部时间源，以提高外部时钟的可靠性，并适当管理所有差异。

当使用多个云服务或同时使用云服务和本地服务时，时钟同步可能会很困难。在此情况下，宜监视每项服务的时钟，并记录差异，以减轻差异带来的风险。

8.17.5 其他信息

正确设置计算机时钟对确保事态日志的准确性至关重要，事态日志可被要求用于调查或作为法律、违规案例的证据。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。

8.18 特权实用程序的使用

8.18.1 属性表

特权实用程序的使用的属性表见表78。

表78 特权实用程序的使用属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#系统和网络安全 #安全配置 #应用安全	#防护

8.18.2 控制

对于可能超越系统和应用控制的实用程序的使用宜予以限制并严格控制。

8.18.3 目的

对于可能超越系统和应用程序控制的实用程序的使用宜予以限制并严格控制。

8.18.4 指南

使用可能超越系统和应用程序控制的实用程序，宜考虑以下指南：

a) 将使用实用程序的用户限制到可信的、已授权的最小实际用户数（见 8.2）；
b) 对实用程序使用标识、鉴别和授权规程，包括使用实用程序人员的唯一身份标识；
c) 对实用程序的授权级别进行定义并文件化；
d) 对实用程序的临时使用进行授权；
e) 当要求职责分离时，禁止访问系统中应用程序的用户使用实用程序；
f) 移除或禁用所有不必要的实用程序；
g) 至少将实用程序与应用程序软件进行逻辑隔离。可行时，将此类工具软件的网络通信与应用流量分离；
h) 限制实用程序的可用性（例如，在授权变更的期间内）；
i) 记录实用程序的所有使用。

8.18.5 其他信息

大多数信息系统都有一个或多个实用程序，可以覆盖系统和应用程序控制，例如，诊断、修补、防病毒、磁盘碎片整理、调试器、备份和网络工具。

8.19 运行系统软件的安装

8.19.1 属性表

运行系统软件的安装的属性表见表79。

表79 运行系统软件的安装属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#安全配置 #应用安全	#防护

8.19.2 控制

宜实施规程和措施以安全地管理运行系统上的软件安装。

8.19.3 目的

确保运行系统的完整性，防止技术脆弱性被利用。

8.19.4 指南

宜考虑下列指南，以安全地管理运行系统上软件的变更和安装：

a) 经过培训的管理员在适当管理授权（见 8.5）下，方可执行运行软件更新；
b) 确保在运行系统上仅可安装经批准的可执行代码，不安装开发代码或编译器；
c) 全面、成功的测试（见 8.29 和 8.31）之后方可安装和更新软件；
d) 更新所有相应的程序源库；
e) 使用配置控制系统来保持对所有运行软件及系统文件的控制；
f) 在实施变更之前定义回滚策略；
g) 维护运行软件所有更新的审计日志；
h) 如软件需要读取或处理归档数据，则归档旧版本的软件，同时归档所有必需的信息和参数、规程、配置细节和支持性软件，以作为应急措施。

升级到新版本的任何决策宜考虑变更的业务要求和发布版本的安全性（例如，采用新信息安全功能或影响当前版本信息安全漏洞的数量和严重程度）。当软件补丁有助于消除或降低信息安全脆弱性（见8.8和8.19）时宜应用软件补丁。

计算机软件可能依赖外部提供的软件和软件包（例如，使用托管在外部站点上模块的软件程序），宜对其进行监视和控制以避免未授权变更，因为他们可能会引入信息安全脆弱性。

在运行系统中所使用的由厂商提供的软件宜在供应商支持的级别上予以维护。随着时间的推移，软件厂商将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。运行系统中使用的开源软件宜保持在软件的最新适当版本。随着时间的推移，开源代码也可能停止维护，但仍然可以在开源软件存储库中找到。组织也宜考虑在运行系统中依赖停止维护的开源软件的风险。

当供应商参与安装或更新软件时，宜仅在必要且获得适当授权的情况下，方可授予供应商物理或逻辑访问权。宜监视供应商的活动（见5.22）。

组织宜定义并执行严格的规则，规定用户可以安装哪些类型的软件。

运行系统上的软件安装宜采用最小特权原则。组织宜确定允许哪些类型的软件安装（例如，现有软件的更新和安全补丁）以及禁止哪些类型的软件安装（例如，仅供个人使用的软件和来源于未知或可疑的且具有潜在恶意的软件）。宜根据相关用户的角色授予这些权限。

8.19.5 其他信息

无其他信息。

8.20 网络安全

8.20.1 属性表

网络安全的属性表见表80。

表80 网络安全属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防 #检测	#保密性 #完整性 #可用性	#防护 #发现	#系统和网络安全	#防护

8.20.2 控制

宜保护、管理和控制网络和网络设备以保护系统和应用程序中的信息。

8.20.3 目的

保护网络中的信息及其支持性的信息处理设施，免受经由网络造成的损害。

8.20.4 指南

宜实施控制，以确保网络中信息的安全，并保护所连接的网络服务，以防止未经授权的访问。尤其是，宜考虑以下事项：

a) 网络可支持的信息类型和分级级别；
b) 建立网络设备的管理职责及规程；
c) 维护文件以保持最新，包括网络拓扑图和设备（例如，路由器、交换机）的配置文件；
d) 适宜时，分离网络运行与 ICT 系统运行责任（见 5.3）；
e) 建立控制，以保护通过公共网络、第三方网络或无线网络传输的数据的保密性和完整性，并保护连接的系统和应用程序（见 5.22、8.24、5.14 和 6.6）。还可能需要额外的控制来保持网络服务和连接到网络的计算机的可用性；
f) 适当开展日志和监视，以记录、检测可能影响或与信息安全相关的行为（见 8.16 和 8.15）；
g) 密切协调网络管理活动，以优化对组织的服务，并确保控制在整个信息处理基础设施中得到一致应用；
h) 鉴别网络上的系统；
i) 限制和过滤系统与网络的连接（例如，使用防火墙）；
j) 检测、限制和鉴别设备和装置与网络的连接；
k) 加固网络设备；
l) 隔离网络管理通道与其他网络流量；
m) 如果网络受到攻击，则临时隔离关键子网（例如，使用网闸）；
n) 禁用易受攻击的网络协议。

组织宜确保对虚拟化网络的使用应用适当的安全控制。虚拟化网络还包括软件定义网络（SDN、SD-WAN）。从安全角度考虑，采用虚拟化网络是可取的，因为它允许逻辑隔离物理网络通信，尤其对于使用分布式计算实现的系统和应用程序。

8.20.5 其他信息

有关网络安全的更多信息见ISO/IEC 27033系列标准。有关虚拟化网络的更多信息见ISO/IEC TS 23167。

8.21 网络服务的安全

8.21.1 属性表

网络服务的安全的属性表见表81。

表81 网络服务的安全属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#系统和网络安全	#防护

8.21.2 控制

宜识别、实施和监视网络服务的安全机制、服务级别和服务要求。

8.21.3 目的

确保使用网络服务的安全。

8.21.4 指南

宜（由内部或外部网络服务提供者）识别并实施特定服务所需的安全措施，如安全功能、服务级别和服务要求。组织宜确保网络服务提供者实施这些措施。

宜确定并定期监测网络服务提供者以安全方式管理约定服务的能力。审计权限宜由组织和供应商共同约定。组织还宜考虑由服务提供者提供第三方认证以证明其保持了适当的安全措施。

宜制定和实现网络和网络服务的使用规则，包括：

a) 允许访问的网络和网络服务；
b) 访问各种网络服务的身份鉴别要求；
c) 决定允许访问网络和网络服务的授权规程。
d) 网络管理、技术控制和规程，以保护对网络连接和网络服务的访问；
e) 用于访问网络和网络服务的方法[例如，使用虚拟专用网络（VPN）或无线网络]；
f) 用户访问时的时间、位置和其他属性；
g) 监测网络服务的使用。

宜考虑网络服务的以下安全特性：

a) 用于网络服务安全的技术，诸如身份鉴别、加密和网络连接控制；
b) 按照安全和网络连接规则，与网络服务安全连接所需的技术指标；
c) 允许用户按照性能、可用性和保密性要求选择使用的缓存（例如，在内容交付网络中）及其指标；
d) 必要情况下，限制访问网络服务或应用程序的网络服务使用规程。

8.21.5 其他信息

网络服务包括提供网络连接、提供专用网络服务和管理网络安全管理解决方案（例如，防火墙和入侵检测系统）。这些服务的范围可以包括从简单的非托管带宽到复杂的

增值服务。

有关访问管理框架的更多指南，请参见ISO/IEC 29146。

8.22 网络隔离

8.22.1 属性表

网络隔离的属性表见表82。

表82 网络隔离属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#系统和网络安全	#防护

8.22.2 控制

宜在组织的网络中隔离信息服务组、用户组和信息系统组。

8.22.3 目的

划分网络安全边界，并根据业务需求控制边界之间的流量。

8.22.4 指南

组织宜考虑通过将大型网络划分为独立的网络域并将他们与公共网络（即互联网）分开，来管理大型网络的安全。域的选择可以基于信任程度、关键性和敏感性（例如，公共访问域、桌面域、服务器域、低风险和高风险系统）以及组织单位（例如，人力资源、财务、营销）或某些组合（例如，连接到多个组织单位的服务器域）来选择域。可以使用物理或逻辑上不同的网络来进行隔离。

每个域的周界都宜清楚定义。如果允许在网络域之间进行访问，则宜使用网关（例如，防火墙、过滤路由器）在周界处进行控制。网络域的划分和网关允许访问的准则，宜基于对每个域安全要求的评估。评估宜按照访问控制的特定主题策略（见5.15）、访问要求、所处理信息的价值和分级，并考虑采用适当网关技术的相对成本和性能影响。

由于网络周界定义不清，无线网络需要特殊处理。无线网络隔离宜考虑无线电覆盖调整。对于敏感环境，宜考虑将所有无线接入视为外部连接，并在授予内部系统访问权限之前，将该接入与内部网络隔离，直到按照网络控制规则（见8.20）通过网关。如果工作人员仅使用符合组织特定策略的受控用户终端设备，则宜将访客的无线接入网络与工作人员的无线接入网络分开。访客的WLAN宜至少与工作人员的WLAN具有相同的限制，以劝阻工作人员使用访客的WLAN。

8.22.5 其他信息

由于业务关系的形成需要信息处理和网络设施的互连或共享，网络往往超越组织边界。这种扩展会增加对组织使用网络的信息系统进行未经授权的访问的风险，因此，

其中一些信息系统由于其敏感性或关键性需要其他网络用户的保护。

8.23 网页过滤

8.23.1 属性表

网页过滤的属性表见表83。

表83 网页过滤属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#系统和网络安全	#防护

8.23.2 控制

宜管理对外部网站的访问，以减少对恶意内容的暴露。

8.23.3 目的

保护系统不受恶意软件的危害，并防止访问未授权的网页资源。

8.23.4 指南

组织宜降低工作人员访问包含非法信息或包含病毒或钓鱼内容的网站的风险。可采用阻止相关网站IP地址或域的技术。一些浏览器和反恶意软件会自动地或进行人工配置后执行此操作。

组织宜为工作人员确定应当或不应当访问的网站类型，宜考虑阻止对以下类型网站的访问：

a) 具有信息上传功能的网站，除非有合理的业务原因；
b) 已知或可疑的恶意网站（例如，传播恶意软件或网络钓鱼内容的网站）；
c) 命令和控制服务器；
d) 从威胁情报中获取的恶意网站（见 5.7）；
e) 分享非法内容的网站。

在部署此控制之前，组织宜建立安全适当使用在线资源的规则，包括对不良或不适宜的网站以及基于web的应用程序的任何限制。这些规则宜保持更新。

宜向工作人员提供有关安全适当使用在线资源（包括访问网页）的培训。培训宜包括组织的规则、提出安全问题的联系人以及出于合理业务需要访问受限网页资源的例外过程。还宜培训工作人员，确保在浏览器上报网站不安全但允许用户继续使用的报告的情况下，他们不会拒绝浏览器建议。

8.23.5 其他信息

网页过滤可以包含一系列技术，包括签名、启发式、可接受网站或域列表、被禁止网站或域列表以及为防止恶意软件和其他恶意活动攻击组织的网络和系统的定制配置。

8.24 密码技术的使用

8.24.1 属性表

密码技术的使用的属性表见表84。

表84 密码技术的使用属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#安全配置	#防护

8.24.2 控制

宜定义并实现有效使用密码技术的规则，包括密钥管理。

8.24.3 目的

根据业务和信息安全要求，并考虑密码技术相关的法律、法规、规章和合同要求，确保适当有效地使用密码技术，以保护信息的保密性、真实性或完整性。

8.24.4 指南

8.24.4.1 总则

使用密码技术时宜考虑以下几点：

a) 组织定义的密码特定策略，包括信息保护的一般原则。有必要制定关于使用密码技术的特定策略，使得密码技术使用的效益最大化，风险最小化，并避免不恰当或不正确的使用密码技术；

b) 确定所需的保护级别和信息分级，以确定所需密码算法的类型、强度和质量；

c) 使用密码技术，保护用户在移动终端设备、存储媒体上保存的信息，以及通过网络传输到此类设备或存储媒体的信息。；

d) 密钥管理方法，包括密钥生成和保护的方法以及在密钥丢失、泄露或损坏的情况下恢复加密信息的方法；

e) 角色和责任：

1) 有效使用密码技术的实施规则；

2) 密钥管理，包括密钥生成（见 8.24）；

f) 拟采用的标准以及组织批准或要求使用的密码算法、密码强度、密码解决方案和使用惯例；

g) 使用加密信息对内容检查等控制的影响（例如，恶意软件检测或内容过滤）。

在实施组织有效使用密码技术的规则时，宜考虑适用于世界不同地区使用密码技术的法规和国家限制以及加密信息的跨境流动问题（见5.31）。

与加密服务外部供应商（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责任、服务可靠性和服务提供响应时间（见5.22）。

8.24.4.2 密钥管理

适当的密钥管理需要生成、存储、归档、检索、分发、停用和销毁加密密钥的安全过程。密钥管理系统宜基于一套约定的标准、规程和安全方法：

a) 为不同的密码系统和不同的应用程序生成密钥；
b) 签发和获取公钥证书；
c) 向目标实体分发密钥，包括如何在收到密钥时激活密钥；
d) 存储密钥，包括授权用户获取密钥的方式；
e) 更改或更新密钥，包括何时及如何更改密钥的规则；
f) 处理泄露的密钥；
g) 撤销密钥，包括如何撤销或停用密钥[例如，当密钥被泄露或用户离开组织时（在此情况下，密钥也宜归档）]；
h) 恢复丢失或损坏的密钥；
i) 备份或归档密钥；
j) 销毁密钥；
k) 密钥管理相关的日志记录和审计；
l) 按照组织的密钥管理规则，设置密钥的激活和停用日期，使密钥只能在一段时间内使用；
m) 处理获取加密密钥的法律请求（如在法庭案件中，加密信息可能需要以未加密的形式提供，作为证据）。宜保护所有加密密钥，以防修改和丢失。此外，秘密和私钥需要防止未授权的使用和泄露。用于生成、存储和归档密钥的设备宜受到物理保护。

除了完整性之外，对于许多密钥使用情景，还宜考虑公钥的真实性。

8.24.5 其他信息

公钥的真实性通常通过使用证书颁发机构和公钥证书的公钥管理过程来解决，但对少量密钥，也可通过应用手动流程等技术手段来来解决。

密码技术可用于实现不同的信息安全目标，例如：

a) 保密性：使用信息加密来保护存储或传输的敏感或关键信息；
b) 完整性或真实性：使用数字签名或消息验证码来验证存储或传输的敏感或关键信息的真实性或完整性。使用算法进行文件完整性检查；
c) 抗抵赖性：使用加密技术提供事件或行为发生或不发生的证据；
d) 身份鉴别：使用密码技术对请求访问或与系统用户、实体和资源进行交易的用户和其他系统实体进行身份证明。

ISO/IEC 11770系列提供了有关密钥管理的更多信息。

8.25 安全开发生存周期

8.25.1 属性表

安全开发生存周期的属性表见表85。

表85 安全开发生存周期属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#应用安全 #系统和网络安全	#防护

8.25.2 控制

宜建立并应用软件和系统安全开发规则。

8.25.3 目的

确保在软件和系统的安全开发生存周期内设计和实现信息安全。

8.25.4 指南

安全开发是建立安全的服务、体系结构、软件和系统的要求。为此，宜考虑以下方面：

a) 开发、测试和生产环境的分离（见 8.31）；

b) 软件开发生存周期中的安全指南：
   1) 软件开发方法中的安全性（见 8.28 和 8.27）；
   2) 使用的每种编程语言的安全编码指南（见 8.28）；

c) 规范和设计阶段的安全要求（见 5.8）；

d) 项目中的安全检查点（见 5.8）；

e) 系统和安全测试，如回归测试、代码扫描和渗透测试（见 8.29）；

f) 源代码和配置的安全存储库（见 8.4 和 8.9）；

g) 版本控制中的安全性（见 8.32）；

h) 所需的应用安全知识和培训（见 8.28）；

i) 开发人员预防、发现和修复漏洞的能力（见 8.28）；

j) 许可要求和替代方案，以确保经济高效的解决方案，同时避免未来的许可问题（见 5.32）。如果开发外包，组织宜确保供应商遵守组织的安全开发规则（见8.30）。

8.25.5 其他信息

开发也可以在应用程序内部进行，例如office应用程序、脚本、浏览器和数据库。

8.26 应用程序安全要求

8.26.1 属性表

应用程序安全要求的属性表见表86。

表86 应用程序安全要求属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#应用安全 #系统和网络安全	#防护 #防御

8.26.2 控制

在开发或获取应用程序时，宜识别、规定和批准信息安全要求。

8.26.3 目的

确保在开发或获取应用程序时，识别并满足所有信息安全要求。

8.26.4 指南

8.26.4.1 总则

宜确定并指定应用程序安全要求。这些要求通常通过风险评估来决定。这些要求宜在信息安全专家的支持下制定。

根据应用程序的用途，应用程序安全要求可以涵盖广泛的主题。应用程序安全要求宜包括（如适用）：

a) 对实体身份的信任程度[例如，通过身份鉴别（见 5.17、8.2 和 8.5）]；
b) 确定应用程序要处理的信息类型和分级；
c) 需要分离对应用程序中数据和功能的访问和访问级别；
d) 针对恶意攻击或无意中断的恢复能力[例如，防止缓冲区溢出或结构化查询语言（SQL）注入]；
e) 交易产生、处理、完成或存储所在司法管辖区（转化为国标时 需调整此类说法）的法律、法规和监管要求；
f) 所有相关方的隐私需求；
g) 任何保密信息的保护要求；
h) 在处理、传输和静止时对数据的保护；
i) 需要对所有相关方之间的通信进行安全加密；
j) 输入控制，包括完整性检查和输入验证；
k) 自动化控制（例如，批准限制或双重批准）；
l) 输出控制，同时考虑谁可以对输出进行访问，和输出访问的授权；
m) 围绕“自由文本”字段内容的限制，因为这些限制可能导致保密数据（例如，个人数据）的非受控存储；
n) 源自业务过程的需求，例如，事务日志和监测、抗抵赖性需求；
o) 其他安全控制的强制要求（例如，与日志记录和监测或数据泄漏检测系统的接口）；
p) 错误消息处理。

8.26.4.2 交易服务

此外，对于在组织和合作伙伴之间提供交易服务的应用程序，在确定信息安全要求时宜考虑以下事项：

a) 各方对对方声称的身份的可信程度；

b) 信息交换或信息处理完整性所需的可信级别以及不完整性的识别机制（例如循环冗余校验、哈希、数字签名）；
c) 批准、发布或签署关键交易文件相关的授权过程；
d) 保密性、完整性、关键文件的发送和接收证明以及抗抵赖性（例如与招标和合同过程相关的合同）；
e) 任何交易的保密性和完整性（例如订单、送货地址详细信息和收据确认）；
f) 对交易保密时限的要求；
g) 保险和其他合同要求。

8.26.4.3 电子订购和支付应用

此外，对于涉及电子订购和支付的应用，宜考虑以下事项：

a) 维护订单信息的保密性和完整性的要求；
b) 适用于验证客户提供的支付信息的可验证程度；
c) 避免交易信息丢失或不必要的重复；
d) 在任何可公开访问的环境之外存储交易的详细信息（例如，在组织内部网络的存储平台上，不是保留和公开在可直接通过互联网访问的电子存储媒体上）；
e) 如果使用受信任的机构（例如，为了发布和维护数字签名或数字证书），安全性将被集成并嵌入到整个端到端证书或签名管理过程中。

考虑到法律要求（参见5.31至5.36，尤其是关于密码相关法律，参见5.31），可以通过应用密码技术（参见8.24）来解决上述几个问题。

8.26.5 其他信息

通过网络访问的应用程序会受到一系列与网络相关的威胁，例如欺诈活动、合同纠纷或向公众披露信息；不完整的传输、错误的路由、未授权的消息更改、复制或重播。因此，详细的风险评估和仔细决定控制是必不可少的。所需的控制通常包括用于身份鉴别和保护数据传输的加密方法。

有关应用程序安全性的更多信息，请参阅ISO/IEC 27034系列。

8.27 安全体系架构和工程原则

8.27.1 属性表

安全体系架构和工程原则的属性表见表87。

表87 安全体系架构和工程原则属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#应用安全 #系统和网络安全	#防护

8.27.2 控制

宜建立、维护工程安全体系的原则并进行文档化，将其应用于所有信息系统开发活动。

8.27.3 目的

确保信息系统在开发生存周期内安全地设计、实现和运行。

8.27.4 指南

宜建立、安全工程原则并进行文档化，将其应用于信息系统工程活动。安全性的设计宜进入到所有体系架构层（业务、数据、应用程序和技术）。宜分析新技术的安全风险，并根据已知的攻击模式审查设计。

安全工程原则为用户身份鉴别技术、安全会话控制以及数据验证和清理提供指导。安全系统工程原则宜包括以下分析：

a) 保护信息和系统免受已识别威胁所需的全方位安全控制；
b) 安全控制防止、检测或响应安全事态的能力；
c) 特定业务过程所需的特定安全控制（例如，敏感信息加密、完整性检查和数字签名信息）；
d) 在何处以及如何实施安全控制（例如，集成安全架构和技术基础设施）；
e) 单个安全控制（手动和自动）如何协同工作以产生一套完整的控制。

安全工程原则宜考虑：

a) 需要与安全架构集成；
b) 技术安全基础设施[例如，公钥基础设施（PKI）、身份和访问管理（IAM）、数据泄漏预防和动态访问管理]；
c) 组织开发和支持所选技术的能力；
d) 满足安全要求的成本、时间和复杂性；
e) 目前的良好实践。

安全体系工程宜涉及：

a) 安全架构原则的使用，如“设计安全”、“纵深防御”、“默认安全”、“默认拒绝”、“安全故障”、 “不信任外部应用程序输入”、“部署安全”、“假定违约”、“最小特权”，“可用性和可管理性”和“功能最少”；
b) 面向安全的设计评审，以帮助识别信息安全漏洞，确保安全控制得到确定，并满足安全要求；
c) 不完全符合要求（如由于压倒一切的安全要求）的安全控制的文件得到正式确认；
d) 系统加固。

组织宜考虑“零信任”原则，如：

a) 假设该组织的信息系统已经遭到破坏，因此不单单依赖网络周界安全；
b) 采用“从不信任，总是验证”的方法访问信息系统；
c) 确保对信息系统的请求进行端到端加密；
d) 验证向信息系统发出的每个请求时，宜将请求视同为开放外部网络发来的请求，即便这些请求来自组织内部（即不自动信任其周界内或周界外的任何东西）；
e) 使用“最小权限”和动态访问控制技术（见 5.15、5.18 和 8.2）。这包括基于应用语境信息（如认证信息（见 5.17）、用户身份（见 5.16）、与用户终端设备有关的数据和数据分级（见 5.12））对信息或系统的请求进行鉴别和

授权；

f) 始终基于包括身份鉴别信息（参见 5.17）和用户身份（参见 5.16）、与用户终端设备有关的数据和数据分级（参见 5.12）在内的信息，对请求者进行身份鉴别，并始终验证对信息系统的授权请求，例如强制实施强身份鉴别（如多因素，参见 8.5）。

在适用的情况下，宜通过组织与组织外包供应商之间的合同和其他有约束力的协议，将既定的安全工程原则应用于信息系统的外包开发。组织宜确保供应商的安全工程实践符合组织的需求。

宜定期审查安全工程原则和已建立的工程规程，以确保其能有效地强化工程过程中的安全标准。宜确保安全工程原则在应对任何新的潜在威胁方面与时俱进，同时与应用技术和解决方案的先进性保持同步。

8.27.5 其他信息

安全工程原则可应用于一系列技术的设计或配置，例如：

——容错和其他弹性技术；

——隔离（例如通过虚拟化或容器化）；

——防篡改。

安全虚拟化技术可用于防止在同一物理设备上运行的应用程序之间的干扰。如果应用程序的虚拟实例受到攻击者的攻击，则只有该实例受到影响。该攻击对任何其他应用程序或数据都没有影响。

防篡改技术可用于检测信息容器的篡改，无论信息容器是物理形式（如防盗报警器）还是逻辑形式（如数据文件）。这种技术的特点是可以产生试图篡改容器的记录。此外，这种安全控制还可以通过销毁数据来防止成功提取数据（如可以删除设备内存）。

8.28 安全编码

8.28.1 属性表

安全编码的属性表见表88。

表88 安全编码属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#应用安全 #系统和网络安全	#防护

8.28.2 控制

软件开发中宜应用安全编码原则。

8.28.3 目的

确保安全的编写软件，以减少软件中潜在的信息安全脆弱性。

8.28.4.1 总则

宜在组织层面建立过程，以对安全编码进行良好的治理。宜建立并应用最低层级的安全基线。此外，这些过程和治理宜扩展以覆盖来自第三方的或者开源软件的软件组件。

组织宜监视已存在的软件威胁以及有关软件脆弱性的最新建议和信息，通过持续改进和学习来指导组织的安全编码原则。这有助于确保实施有效的安全编码实践，以应对快速变化的威胁。

8.28.4.2 规划和编码前

安全编码原则宜用于新开发和重用场景中。这些原则宜应用于组织内部自研及组织对它方提供产品及服务的开发活动。编码前的计划和前置条件宜包括：

a) 特定于组织的期望和已批准用于内部自研和外包代码开发的安全编码原则；
b) 导致信息安全脆弱性的常见和以往编码实操与缺陷；
c) 配置开发工具如集成开发环境（IDE），以帮助创建安全的代码；
d) 如适用，遵循开发工具供应商及执行环境供应商发布的指南；
e) 维护和使用更新的开发工具（如编译器）；
f) 编写安全的代码的开发人员的资格；
g) 安全设计和架构，包括威胁建模；
h) 安全编码标准，并在相关情况下强制使用这些标准；
i) 使用受控环境进行开发。

8.28.4.3 编码期间

编码期间的注意事项宜包括：

a) 针对所使用编程语言和技术的安全编码实践；
b) 使用安全编程技术，例如结对编程、重构、同行评审、安全迭代和测试驱动开发；
c) 使用结构化编程技术；
d) 文档化代码并消除那些可能导致信息安全脆弱性被利用的编程缺陷；
e) 禁止使用不安全的设计技术（如使用硬编码口令、未经批准的代码示例和免鉴别可访问的 web 服务）。

测试宜在开发期间和开发后进行（见8.29）。静态应用程序安全测试（SAST）过程可识别软件中的安全脆弱性。

在软件投入运行之前，宜评估以下内容：

a) 攻击面和最小特权原则；
b) 对最常见的编程错误进行分析，并对这些已得到缓解的错误进行文档记录。

8.28.4.4 评审和维护

代码进入运行状态后：

a) 宜对更新进行安全地打包和部署；
b) 宜处理报告的信息安全脆弱性（见 8.8）；
c) 宜记录错误和可疑攻击，并定期评审日志，以便在必要时对代码进行调整；
d) 宜保护源代码免受未经授权的访问和篡改（如通过使用可提供诸如访问控制及版本控制的配置管理工具）。

如果使用外部工具和库，组织宜考虑：

a) 确保对外部库进行管理（如通过维护所用库及其版本的清单），并随发布周期定期更新；
b) 选择、授权和重用经过充分审查的组件，尤其是鉴别和密码组件；
c) 外来组件的许可、安全和历史记录；
d) 确保软件可维护、已追踪，并且源于被证实、有信誉的来源方；
e) 开发资源和制品的长期可用性。

当软件包需要修改时，宜考虑以下几点：

a) 内置控制和完整性过程受到损害的风险；
b) 是否获得厂商的同意；
c) 从厂商处获得标准程序更新所需变更的可能性；
d) 因组织对软件进行变更，可能造成本组织未来将要负责该软件的维护所带来的影响；
e) 与其他在用软件的兼容性。

8.28.5 其他信息

一个指导原则是确保在必要时调用安全相关代码，并防篡改。使用编译后的二进制代码安装的程序也具备这些属性，但只适用于该应用内的数据。对于解释性语言，只有当代码在使用它的用户和进程无法访问的服务器上执行时，并且其数据保存在受到类似机制保护的数据库中，本概念才适用。例如解释的代码可能在云服务上运行，而对代码本身的访问需要管理员权限。这种管理员访问宜受到安全机制如即时管理原则和强鉴别的保护。如果应用程序拥有者可以通过直接远程访问服务器来访问脚本，那么原则上攻击者也可以。在此情况下，宜配置Web服务器以阻止进行目录浏览。

应用程序代码的设计最好是假设代码总是会受到错误或恶意行为的攻击。此外，关键应用程序可设计为能够容忍内部故障。例如在数据用于安全或财务等关键应用程序之前，可检查复杂算法的输出以确保其位于安全范围内。执行边界检查的代码很简单，因此更容易证明正确性。

某些web应用程序易受到设计和编码不当引入的各种脆弱性的影响，例如数据库注入和跨站点脚本攻击。在这些攻击中，请求可能被篡改以滥用WEB服务器的功能。

有关ICT安全评估的更多信息，见ISO/IEC 15408系列标准。

8.29 开发和验收中的安全测试

8.29.1 属性表

开发和验收中的安全测试的属性表见表89。

表89 开发和验收中的安全测试属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#识别	#应用安全 #信息安全保障 #系统和网络安全	#防护

8.29.2 控制

宜在开发生存周期中定义和实施安全测试过程。

8.29.3 目的

确认将应用程序或代码部署到生产环境时是否满足信息安全要求。

8.29.4 指南

新的信息系统、升级及新版本宜在开发过程中进行彻底的测试和验证。安全测试宜作为系统或组件测试的组成部分。

安全测试宜针对一组功能性或非功能性需求进行，安全测试宜包括如下测试：

a) 安全功能[例如用户身份鉴别（见 8.5）、访问限制（见 8.3）和密码的使用（见 8.24）]；
b) 安全编码（见 8.28）；
c) 安全配置（见 8.9、8.20 和 8.22），包括操作系统、防火墙和其他安全组件的安全配置。

宜使用一组准则确定测试计划。测试的范围宜与系统的重要性、性质以及所引入变更可能造成的影响相称。测试计划宜包括：

a) 活动和测试的详细时间表；
b) 各种条件下的输入和预期输出；
c) 评估结果的准则；
d) 必要时采取进一步行动的决策。

组织可借助自动工具如代码分析工具或脆弱性扫描器进行测试，并宜验证安全相关缺陷是否修复。

对于内部开发，此类测试最初宜由开发团队执行。然后宜进行独立验收测试，以确保系统按预期工作，且仅按预期工作（见5.8）。宜考虑以下几点：

a) 将执行代码审查活动作为与测试发现安全缺陷相关的要素之一，包括非预期的输入和条件；
b) 执行脆弱性扫描，以识别不安全的配置和系统脆弱性；
c) 执行渗透测试，以识别不安全的代码和设计。

宜遵循采购流程进行外包开发和组件采购。与供应商签订的合同宜确定已识别的安全要求（见5.20）。宜在获取产品和服务之前根据这些准则对其进行评价。

宜在与目标生产环境尽可能匹配的测试环境中进行测试，以确保系统不会将脆弱性引入到组织环境，并确保测试是可靠的（见8.31）。

8.29.5 其他信息

可建立多个测试环境，以开展不同类型的测试（例如功能测试和性能测试）。这些不同的环境可以是虚拟的，其通过单独的配置来模拟各种操作环境。

还需要考虑对测试环境、工具和技术的测试与监视，以确保有效的测试。同样的考虑也适用于对部署在开发、测试和生产环境中的监视系统的监视，需要根据系统和数据的敏感性进行判断，以确定多少层的元测试是有用的。

8.30 外包开发

8.30.1 属性表

外包开发的属性表见表90。

表90 外包开发属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防 #检测	#保密性 #完整性 #可用性	#识别 #防护 #发现	#系统和网络安全 #应用安全 #供应商关系安全	#治理和生态体系 #防护

组织宜指导、监视和评审系统开发外包相关的活动。

8.30.3 目的

确保组织要求的信息安全措施在系统开发外包中得以实现。

8.30.4 指南

当系统开发外包时，组织宜沟通需求和期望并就此达成一致，同时持续监视和评审外包工作的交付是否满足这些期望。宜在整个组织的外部供应链中考虑如下几点：

a) 与外包内容相关的许可协议、代码所有权和知识产权（见 5.32）；
b) 安全设计、编码和测试活动的合同要求（见 8.25 至 8.29）；
c) 提供威胁模型以供外部开发人员考虑；
d) 交付件质量和准确性的验收测试（见 8.29）；
e) 提供证据如保证报告，证明已建立最低可接受级别的安全和隐私能力；
f) 提供证据，证明已应用足够的测试，以防止交付时存在恶意内容（包括有意的和无意的）；
g) 提供证据，证明已应用充分的测试，以防止已知脆弱性的存在；
h) 软件源代码的托管协议（如当供应商倒闭）；
i) 对开发过程和控制进行审核的合同权利；
j) 开发环境的安全要求（见 8.31）；
k) 考虑适用的法律（例如个人数据保护相关法律）。

8.30.5 其他信息

有关供应商关系的更多信息，见ISO/IEC 27036系列标准。

8.31 开发、测试和生产环境的隔离

8.31.1 属性表

开发、测试和生产环境的隔离的属性表见表91。

表91 开发、测试和生产环境的隔离属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#应用安全 #系统和网络安全	#防护

8.31.2 控制

宜隔离并保护开发、测试和生产环境。

8.31.3 目的

保护生产环境和数据免受开发和测试活动的影响。

8.31.4 指南

为防止产生生产问题，宜识别和实施生产、测试和开发环境的隔离。宜考虑如下条款：

a) 充分隔离开发和生产系统，并在不同区域（如在单独的虚拟或物理环境中）对其进行操作；
b) 定义、记录和实施从开发状态到生产状态的软件部署规则和授权；
c) 在应用于生产系统之前，在测试或暂存环境中对生产系统和应用程序的变更进行测试（见 8.29）；
d) 不在生产环境中进行测试（除在已经确定和批准的情况外）；
e) 非必要时，编译器、编辑器和其他开发工具或实用程序不可通过生产系统访问；
f) 在菜单中显示适当的环境标识标签，以降低出错的风险；
g) 不将敏感信息拷贝到开发和测试系统环境中（除在为开发和测试系统提供了等效的控制以外）。

开发和测试环境宜始终受到保护，并考虑：

a) 修补和更新所有开发、集成和测试工具（包括构建器、集成器、编译器、配置系统和软件库）；
b) 系统和软件的安全配置；
c) 对环境的访问控制；
d) 监视环境的变化和存储在其中的代码；
e) 安全的监视环境；
f) 对环境进行备份。

未经事先评审和批准，个人不得对开发和生产环境进行变更。这可通过诸如隔离访问权或通过监视规则来实现。特殊情况下，宜实施诸如详细的日志记录和实时监视等附加措施，以便检测和处理未授权的变更。

8.31.5 其他信息

如果没有恰当的措施和规程，有权访问生产系统的开发人员和测试人员可能会带来重大风险（如对文件或系统环境不必要的修改、系统故障、在生产系统中运行未经授权和测试的代码、泄露机密数据、数据完整性和可用性问题）。需要维护一个已知且稳定的环境，在其中执行有意义的测试，并防止开发人员不当的访问生产环境。

措施和规程包括精心设计的角色与实施职责分离要求相结合、适当的监视过程。

开发和测试人员也会威胁到生产信息的保密性。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或信息的变更。因此，为了减少意外变更或未经授权访问生产软件和业务数据的风险，隔离开发、测试和运行环境是有必要的（测试数据的保护见8.33）。

在某些情况下，开发、测试和生产环境之间可能无法隔离，测试可在开发环境中进行，也可以通过对实时用户或服务器（如少量试点用户）的受控部署来进行。在某些情况下，产品测试可通过在组织内部现场使用产品来进行。此外，为了减少实时部署的停机时间，可以支持两个相同的生产环境（不论何时其中只有一个是处于活动状态）。

需在开发和测试环境（8.33）中使用生产数据支持相关过程。

在进行最终用户培训时，组织也可以考虑本节中提供的培训环境指南。

8.32 变更管理

8.32.1 属性表

变更管理的属性表见表92。

表92 变更管理属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#应用安全 #系统和网络安全	#防护

8.32.2 控制

信息处理设施和信息系统的变更宜遵从变更管理规程。

8.32.3 目的

执行变更时保护信息安全。

8.32.4 指南

引入新系统和对已有系统进行大的变更宜按照商定的规则，并从文件、规范、测试、质量控制到管理实施这个正式的过程进行。宜明确管理责任和规程，以确保所有变更得到完善的控制。

宜将变更控制规程文件化，并强制实施，以确保从早期设计到后续维护中整个系统开发生存周期内，信息处理设施和信息系统中信息的保密性、完整性和可用性。

当可行时，宜整合ICT基础设施和软件的变更控制规程。变更控制规程宜包括：

a) 考虑所有依赖关系，规划和评估变更的潜在影响；
b) 变更授权；
c) 向相关方传达变更；
d) 变更测试和验收（见 8.29）；
e) 变更实施，包括部署计划；
f) 紧急情况和应急考虑，包括回退规程；
g) 维护包含上述内容的变更记录；
h) 确保操作文件（见 5.37）和用户规程根据需要进行变更，以保持适宜性；
i) 确保 ICT 连续性计划以及响应和恢复规程（见 5.30）根据需要进行变更，以保持适宜性。

8.32.5 其他信息

对信息处理设施和信息系统的变更缺乏控制是系统故障或安全失效的常见原因。对生产环境的变更，特别是当软件从开发环境向运行环境转移时，可能影响应用程序的完整性和可用性。

变更软件会影响生产环境，反之亦然。

良好的实践包括在一个与生产和开发环境隔离（见12.1.4）的环境中测试ICT组件（见8.31）。能够提供一种方法，可用于控制新软件，以及对用于测试目的的运行信息进行额外保护。这其中宜包括补丁、服务包和其他更新。

生产环境包括操作系统、数据库和中间件平台。本控制宜适用于应用程序和基础设施的变更。

8.33 测试信息

8.33.1 属性表

测试信息的属性表见表93。

表93 测试信息属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性	#防护	#信息保护	#防护

8.33.2 控制

宜适当的选择、保护和管理测试信息。

8.33.3 目的

确保测试的相关性，并保护用于测试的运行信息。

8.33.4 指南

宜选择测试信息，以确保测试结果的可靠性和相关运行信息的保密性。不宜将敏感信息（包括个人可识别信息）复制到开发和测试环境中（见8.31）。

无论测试环境是内部还是在云服务上构建，当用于测试时，宜应用下列指南保护运行信息的副本：

a) 对测试环境采取与运行环境相同的访问控制规程；
b) 每次将运行信息拷贝到测试环境时有单独的授权；
c) 记录运行信息的复制和使用，以提供审核追踪；
d) 如果用于测试，通过移除或屏蔽（见 8.11）保护敏感信息；
e) 测试完成后立即从测试环境中正确地删除（见 8.10）运行信息，以防止未授权使用测试信息。测试信息宜安全存储（以防止篡改，否则可能产生无效结果），且仅用于测试目的。

8.33.5 其他信息

系统和验收测试可能需要大量尽可能接近运行信息的测试信息。

8.34 在审计测试中保护信息系统

8.34.1 属性表

在审计测试中保护信息系统的属性表见表94。

表94 在审计测试中保护信息系统属性表

控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
#预防	#保密性 #完整性 #可用性	#防护	#系统和网络安全 #信息保护	#治理和生态体系 #防护

8.34.2 控制

宜规划涉及运行系统评估的审计测试和其他保障活动，并在测试人员和适合的管理人员之间达成一致。

8.34.3 目的

尽可能减少审计和其他保障活动对运行的系统和业务过程的影响。

8.34.4 指南

宜遵守如下指南：

a) 就访问系统和数据的审计请求与适合的管理人员达成一致；
b) 商定和控制技术审计测试的范围；
c) 将审计测试限制为对软件和数据的只读访问。如果只读访问无法获得必要的信息，则由具有必要访问权限且有经验的管理员代表审计员执行测试；
d) 如果授予访问权限，需在此之前确定并验证用于访问系统的设备（如笔记本电脑或平板电脑）的安全要求（如防病毒和补丁）；
e) 除只读之外，宜仅允许对系统文件的隔离副本进行其它类型的访问，当审计完成时，宜删除这些副本或者审计存档要求保留这些文件时，对副本给予适当的保护；
f) 识别和商定特殊或额外的处理请求，如运行审计工具；

g) 在工作时间以外进行可能影响系统可用性的审计测试；
h) 监控和记录所有出于审计和测试目的的访问。

8.34.5 其他信息

审计测试和其他保障活动也可能发生在开发和测试系统上开展，此类测试可能影响代码的完整性或导致此类环境中敏感信息的泄露。

附 录 A

（资料性）属性的使用

A.1 概述

本附录以表格的形式展示了一种使用属性来创建控制的不同视图的方法。五个属性的例子是（见 4.2）：

a) 控制类型（#预防，#检测，#纠正）；
b) 信息安全属性（#保密性、#完整性、#可用性）；
c) 网络空间安全概念（#识别、#防护、#发现、#响应、#恢复）；
d) 运行能力（#治理、#资产管理、#信息保护、#人力资源安全、#物理安全、#系统和网络安全、 #应用安全、#安全配置、#身份和访问管理、#威胁和脆弱性管理、#连续性、#供应商关系安全、 #合法合规、#信息安全事态管理、#信息安全保障）；
e) 安全领域（#治理和生态体系、#防护、#防御、#弹性）。表A.1包含本文件中所有控制及其给定属性值的矩阵。

可使用简单电子表格或数据库等工具对矩阵进行筛选或排序，该工具可包括更多信息，如控制文本、指南、特定组织指南或属性（见A.2）。

表A.1 控制及其属性值矩阵

控制标识符	控制名称	控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
5.1	信息安全策略	#预防	#保密性 #完整性 #可用性	#识别	#治理	#治理和生态体系 #弹性
5.2	信息安全角色和责任	#预防	#保密性 #完整性 #可用性	#识别	#治理	#治理和生态体系 #防护 #弹性
5.3	职责分离	#预防	#保密性 #完整性 #可用性	#防护	#治理 #身份和访问管理	#治理和生态体系
5.4	管理责任	#预防	#保密性 #完整性 #可用性	#识别	#治理	#治理和生态体系
5.5	与职能机构的联系	#预防 #纠正	#保密性 #完整性 #可用性	#识别 #防护 #响应 #恢复	#治理	#防御 #弹性
5.6	与特定相关方的联系	#预防 #纠正	#保密性 #完整性 #可用性	#防护 #响应 #恢复	#治理	#防御

控制标识符	控制名称	控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
5.7	威胁情报	#预防 #检测 #纠正	#保密性 #完整性 #可用性	#识别 #发现 #响应	#威胁和脆弱性管理	#防御 #弹性
5.8	项目管理中的信息安全	#预防	#保密性 #完整性 #可用性	#识别 #防护	#治理	#治理和生态体系 #防护
5.9	信息及其他相关资产的清单	#预防	#保密性 #完整性 #可用性	#识别	#资产管理	#治理和生态体系 #防护
5.10	信息及其他相关资产的可接受使用	#预防	#保密性 #完整性 #可用性	#防护	#资产管理 #信息保护	#治理和生态体系 #防护
5.11	资产归还	#预防	#保密性 #完整性 #可用性	#防护	#资产管理	#防护
5.12	信息分级	#预防	#保密性 #完整性 #可用性	#防护	#信息保护	#防护 #防御
5.13	信息标记	#预防	#保密性 #完整性 #可用性	#防护	#信息保护	#防御 #防护
5.14	信息传输	#预防	#保密性 #完整性 #可用性	#防护	#资产管理 #信息保护	#防护
5.15	访问控制	#预防	#保密性 #完整性 #可用性	#防护	#身份和访问管理	#防护
5.16	身份管理	#预防	#保密性 #完整性 #可用性	#防护	#身份和访问管理	#防护
5.17	鉴别信息	#预防	#保密性 #完整性 #可用性	#防护	#身份和访问管理	#防护
5.18	访问权	#预防	#保密性 #完整性 #可用性	#防护	#身份和访问管理	#防护
5.19	供应商关系中的信息安全	#预防	#保密性 #完整性 #可用性	#防护	#供应商关系安全	#治理和生态体系 #防护

控制标识符	控制名称	控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
5.20	在供应商协议中强调信息安全	#预防	#保密性 #完整性 #可用性	#识别	#供应商关系安全	#治理和生态体系 #防护
5.21	管理信息通信技术供应链中的信息安全	#预防	#保密性 #完整性 #可用性	#识别	#供应商关系安全	#治理和生态体系 #防护
5.22	供应商服务的监视、评审和变更管理	#预防	#保密性 #完整性 #可用性	#识别	#供应商关系安全 #信息安全保障	#治理和生态体系 #防护 #防御
5.23	云服务使用的信息安全	#预防	#保密性 #完整性 #可用性	#防护	#供应商关系安全	#治理和生态体系 #防护
5.24	信息安全事件管理规划和准备	#纠正	#保密性 #完整性 #可用性	#响应 #恢复	#治理 #信息安全事态管理	#防御
5.25	信息安全事态的评估和决策	#检测	#保密性 #完整性 #可用性	#发现#响应	#信息安全事态管理	#防御
5.26	信息安全事件的响应	#纠正	#保密性 #完整性 #可用性	#响应 #恢复	#信息安全事态管理	#防御
5.27	从信息安全事件中学习	#预防	#保密性 #完整性 #可用性	#识别 #防护	#信息安全事态管理	#防御
5.28	证据收集	#纠正	#保密性 #完整性 #可用性	#发现 #响应	#信息安全事态管理	#防御
5.29	中断期间的信息安全	#预防 #纠正	#保密性 #完整性 #可用性	#防护 #响应	#连续性	#防护 #弹性
5.30	业务连续性的信息通信技术就绪	#纠正	#可用性	#响应	#连续性	#弹性
5.31	法律、法规、规章和合同要求	#预防	#保密性 #完整性 #可用性	#识别	#合法合规	#治理和生态体系 #防护

控制标识符	控制名称	控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
5.32	知识产权	#预防	#保密性 #完整性 #可用性	#识别	#合法合规	#治理和生态体系
5.33	记录的保护	#预防	#保密性 #完整性 #可用性	#识别 #防护	#合法合规 #资产管理 #信息保护	#防御
5.34	隐私和个人可识别信息保护	#预防	#保密性 #完整性 #可用性	#识别 #防护	#信息保护 #合法合规	#防护
5.35	信息安全的独立评审	#预防 #纠正	#保密性 #完整性 #可用性	#识别 #防护	#信息安全保障	#治理和生态体系
5.36	符合信息安全的策略、规则和标准	#预防	#保密性 #完整性 #可用性	#识别 #防护	#合法合规 #信息安全保障	#治理和生态体系
5.37	文件化的操作规程	#预防 #纠正	#保密性 #完整性 #可用性	#防护 #恢复	#资产管理 #物理安全 #系统和网络安全 #应用安全 #安全配置 #身份和访问管理 #威胁和脆弱性管理 #连续性 #信息安全事态管理	#治理和生态体系 #防护 #防御
6.1	审查	#预防	#保密性 #完整性 #可用性	#防护	#人力资源安全	#治理和生态体系
6.2	任用条款和条件	#预防	#保密性 #完整性 #可用性	#防护	#人力资源安全	#治理和生态体系
6.3	信息安全意识、教育和培训	#预防	#保密性 #完整性 #可用性	#防护	#人力资源安全	#治理和生态体系
6.4	违规处理过程	#预防 #纠正	#保密性 #完整性 #可用性	#防护 #响应	#人力资源安全	#治理和生态体系

控制标识符	控制名称	控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
6.5	任用终止或变更后的责任	#预防	#保密性 #完整性 #可用性	#防护	#人力资源安全 #资产管理	#治理和生态体系
6.6	保密或不泄露协议	#预防	#保密性	#防护	#人力资源安全 #信息保护 #供应商关系安全	#治理和生态体系
6.7	远程工作	#预防	#保密性 #完整性 #可用性	#防护	#资产管理 #信息保护 #物理安全 #系统和网络安全	#防护
6.8	信息安全事态的报告	#检测	#保密性 #完整性 #可用性	#发现	#信息安全事态管理	#防御
7.1	物理安全边界	#预防	#保密性 #完整性 #可用性	#防护	#物理安全	#防护
7.2	物理入口	#预防	#保密性 #完整性 #可用性	#防护	#物理安全 #身份和访问管理	#防护
7.3	办公室、房间和设施的安全保护	#预防	#保密性 #完整性 #可用性	#防护	#物理安全 #资产管理	#防护
7.4	物理安全监视	#预防 #检测	#保密性 #完整性 #可用性	#防护 #发现	#物理安全	#防护 #防御
7.5	物理和环境威胁防范	#预防	#保密性 #完整性 #可用性	#防护	#物理安全	#防护
7.6	在安全区域工作	#预防	#保密性 #完整性 #可用性	#防护	#物理安全	#防护
7.7	清理桌面和屏幕	#预防	#保密性	#防护	#物理安全	#防护

控制标识符	控制名称	控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
7.8	设备安置和保护	#预防	#保密性 #完整性 #可用性	#防护	#物理安全 #资产管理	#防护
7.9	组织场所外的资产安全	#预防	#保密性 #完整性 #可用性	#防护	#物理安全 #资产管理	#防护
7.10	存储媒体	#预防	#保密性 #完整性 #可用性	#防护	#物理安全 #资产管理	#防护
7.11	支持性设施	#预防 #检测	#完整性 #可用性	#防护 #发现	#物理安全	#防护
7.12	布缆安全	#预防	#保密性 #可用性	#防护	#物理安全	#防护
7.13	设备维护	#预防	#保密性 #完整性 #可用性	#防护	#物理安全 #资产管理	#防护 #弹性
7.14	设备的安全处置或重复使用	#预防	#保密性	#防护	#物理安全 #资产管理	#防护
8.1	用户终端设备	#预防	#保密性 #完整性 #可用性	#防护	#资产管理 #信息保护	#防护
8.2	特许访问权	#预防	#保密性 #完整性 #可用性	#防护	#身份和访问管理	#防护
8.3	信息访问限制	#预防	#保密性 #完整性 #可用性	#防护	#身份和访问管理	#防护
8.4	源代码的访问	#预防	#保密性 #完整性 #可用性	#防护	#身份和访问管理 #应用安全 #安全配置	#防护
8.5	安全鉴别	#预防	#保密性 #完整性 #可用性	#防护	#身份和访问管理	#防护

控制标识符	控制名称	控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
8.6	容量管理	#预防 #检测	#完整性 #可用性	#识别 #防护 #发现	#连续性	#治理和生态体系 #防护
8.7	恶意软件防范	#预防 #检测 #纠正	#保密性 #完整性 #可用性	#防护 #发现	#系统和网络安全 #信息保护	#防护 #防御
8.8	技术脆弱性管理	#预防	#保密性 #完整性 #可用性	#识别 #防护	#威胁和脆弱性管理	#治理和生态体系 #防护 #防御
.9	配置管理	#预防	#保密性 #完整性 #可用性	#防护	#安全配置	#防护
8.10	信息删除	#预防	#保密性	#防护	#信息保护 #合法合规	#防护
8.11	数据脱敏	#预防	#保密性	#防护	#信息保护	#防护
8.12	数据防泄露	#预防 #检测	#保密性	#防护 #发现	#信息保护	#防护 #防御
8.13	信息备份	#纠正	#完整性 #可用性	#恢复	#连续性	#防护
8.14	信息处理设施的冗余	#预防	#可用性	#防护	#连续性 #资产管理	#防护 #弹性
8.15	日志	#检测	#保密性 #完整性 #可用性	#识别	#信息安全事态管理	#防护 #防御
8.16	监视活动	#检测 #纠正	#保密性 #完整性 #可用性	#发现 #响应	#信息安全事态管理	#防御
8.17	时钟同步	#检测	#完整性	#防护 #发现	#信息安全事态管理	#防护 #防御

控制标识符	控制名称	控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
8.18	特权实用程序的使用	#预防	#保密性 #完整性 #可用性	#防护	#系统和网络安全 #安全配置 #应用安全	#防护
8.19	运行系统软件的安装	#预防	#保密性 #完整性 #可用性	#防护	#安全配置 #应用安全	#防护
8.20	网络安全	#预防 #检测	#保密性 #完整性 #可用性	#防护 #发现	#系统和网络安全	#防护
8.21	网络服务的安全	#预防	#保密性 #完整性 #可用性	#防护	#系统和网络安全	#防护
8.22	网络隔离	#预防	#保密性 #完整性 #可用性	#防护	#系统和网络安全	#防护
8.23	网页过滤	#预防	#保密性 #完整性 #可用性	#防护	#系统和网络安全	#防护
8.24	密码技术的使用	#预防	#保密性 #完整性 #可用性	#防护	#安全配置	#防护
8.25	安全开发生存周期	#预防	#保密性 #完整性 #可用性	#防护	#应用安全 #系统和网络安全	#防护
8.26	应用程序安全要求	#预防	#保密性 #完整性 #可用性	#防护	#应用安全 #系统和网络安全	#防护 #防御
8.27	安全体系架构和工程原则	#预防	#保密性 #完整性 #可用性	#防护	#应用安全 #系统和网络安全	#防护
8.28	安全编码	#预防	#保密性 #完整性 #可用性	#防护	#应用安全 #系统和网络安全	#防护 #防御
8.29	开发和验收中的安全测试	#预防	#保密性 #完整性 #可用性	#识别	#应用安全 #信息安全保障 #系统和网络安全	#防护

控制标识符	控制名称	控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
8.30	外包开发	#预防 #检测	#保密性 #完整性 #可用性	#识别 #防护 #发现	#系统和网络安全 #应用安全 #供应商关系安全	#治理和生态体系 #防护
8.31	开发、测试和生产环境的隔离	#预防	#保密性 #完整性 #可用性	#防护	#应用安全 #系统和网络安全	#防护
8.32	变更管理	#预防	#保密性 #完整性 #可用性	#防护	#应用安全 #系统和网络安全	#防护
8.33	测试信息	#预防	#保密性 #完整性	#防护	#信息保护	#防护
8.34	在审计测试中保护信息系统	#预防	#保密性 #完整性 #可用性	#防护	#系统和网络安全 #信息保护	#治理和生态体系 #防护

表A.2提供了一个通过筛选特定属性值为#纠正性来创建视图的示例。

表A.2 #纠正控制视图

控制标识符	控制名称	控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
5.5	与职能机构的联系	#预防 #纠正	#保密性 #完整性 #可用性	#识别 #防护 #响应 #恢复	#治理	#防御 #弹性
5.6	与特定相关方的联系	#预防 #纠正	#保密性 #完整性 #可用性	#防护 #响应 #恢复	#治理	#防御
5.7	威胁情报	#预防 #检测 #纠正	#保密性 #完整性 #可用性	#识别 #发现 #响应	#威胁和脆弱性管理	#防御 #弹性
5.24	信息安全事件管理规划和准备	#纠正	#保密性 #完整性 #可用性	#响应 #恢复	#治理 #信息安全事态管理	#防御
5.26	信息安全事件的响应	#纠正	#保密性 #完整性 #可用性	#响应 #恢复	#信息安全事态管理	#防御

控制标识符	控制名称	控制类型	信息安全属性	网络空间安全概念	运行能力	安全领域
5.28	证据收集	#纠正	#保密性 #完整性 #可用性	#发现 #响应	#信息安全事态管理	#防御
5.29	中断期间的信息安全	#预防 #纠正	#保密性 #完整性 #可用性	#防护 #响应	#连续性	#防护 #弹性
5.30	业务连续性的信息通信技术就绪	#纠正	#可用性	#响应	#连续性	#弹性
5.35	信息安全的独立评审	#预防 #纠正	#保密性 #完整性 #可用性	#识别 #防护	#信息安全保障	#治理和生态体系
5.37	文件化的操作规程	#预防 #纠正	#保密性 #完整性 #可用性	#防护 #恢复	#资产管理 #物理安全 #系统和网络安全 #应用安全 #安全配置 #身份和访问管理 #威胁和脆弱性管理 #连续性 #信息安全事态管理	#治理和生态体系 #防护 #防御
6.4	违规处理过程	#预防 #纠正	#保密性 #完整性 #可用性	#防护 #响应	#人力资源安全	#治理和生态体系
8.7	恶意软件防范	#预防 #检测 #纠正	#保密性 #完整性 #可用性	#防护 #发现	#系统和网络安全 #信息保护	#防护 #防御
8.13	信息备份	#纠正	#完整性 #可用性	#恢复	#连续性	#防护
8.16	监视活动	#检测 #纠正	#保密性 #完整性 #可用性	#发现 #响应	#信息安全事态管理	#防御

A.2 组织视图

属性主要用于创建不同的控制视图，组织可忽视本文件中所提议的示例，创建组织自用的属性并赋以不同的值，以满足组织的特定需求。此外，分配给每个属性的值可能在组织之间有所不同，因为组织可能对控制或与属性关联的值（当这些值在组织环境下有特定含义时）的用法或适用范围有不同的看法。第一步是理解为什么组织愿意拥有特定属性。例如，如果一个组织基于安全事态已经制定了风险处理计划[见ISO/IEC 27001—2016，6.1.3 e）]，就愿意将风险场景属性与本文件中的每项控制关联起来。

这种属性的好处是加快了与风险处理相关的ISO/IEC 27001要求的实现过程，即将通过风险处理过程确定的控制（称为“必要”控制）与ISO/IEC 27001—2016中的控制进行比较，本文件中的附录A可确保未忽略任何必要的控制。

一旦知道了目的和好处，下一步就是确定属性值。例如，组织可能会识别9个事态：

a) 移动设备丢失或被盗；
b) 组织场所的丢失或盗窃；
c) 不可抗力、故意破坏和恐怖主义；
d) 软件、硬件、电源、互联网和通信故障；
e) 欺诈；
f) 黑客；
g) 泄露；
h) 违反法律；
i) 社会工程。

因此，第二步可以通过为每个事态分配标识符来完成，例如e1、e2、…、e9。

第三步是将控制标识符和控制名称从此文档复制到电子表格或数据库中，并将属性值与每个控件关联，每个控件可以具有多个属性值。最后一步是对电子表格进行排序或查询数据库以提取所需的信息。

其他关于组织属性以及可能的值的示例包括：

a) 成熟度（来自 ISO/IEC 33000 系列或其他成熟度模型的值）；
b) 实施状态（待办、正在进行、部分实施、完全实施）；
c) 优先级（1、2、3 等）；
d) 涉及的组织领域（安全、ICT、人力资源、高层管理等）；
e) 事态；
f) 涉及的资产；
g) 构建和运行，以区分在服务生存周期不同阶段使用的控件；
h) 组织与之合作的或可以从中过渡的其他框架。

B B

附 录 B

（资料性）

本文件与 ISO/IEC 27002:2013 的对应关系

本附录的目的是为目前正在使用上个版本并希望过渡到此版本的组织，提供与ISO/IEC 27002:2013的兼容性过渡。

表B.1提供了第5章至第8章中规定的控制与ISO/IEC 27002:2013中控制的对应关系。

表B.1 本文件中的控制与 ISO/IEC 27002:2013 中控制之间的对应关系

ISO/IEC 27002:2022 控制标识符	ISO/IEC 27002:2013 控制标识符	控制名称
5.1	05.1.1, 05.1.2	信息安全策略
5.2	06.1.1	信息安全角色和责任
5.3	06.1.2	职责分离
5.4	07.2.1	管理责任
5.5	06.1.3	与职能机构的联系
5.6	06.1.4	与特定相关方的联系
5.7	新增	威胁情报
5.8	06.1.5, 14.1.1	项目管理中的信息安全
5.9	08.1.1, 08.1.2	信息及其他相关资产的清单
5.10	08.1.3, 08.2.3	信息及其他相关资产的可接受使用
5.11	08.1.4	资产归还
5.12	08.2.1	信息分级
5.13	08.2.2	信息标记
5.14	13.2.1, 13.2.2, 13.2.3	信息传输
5.15	09.1.1, 09.1.2	访问控制
5.16	09.2.1	身份管理
5.17	09.2.4, 09.3.1, 09.4.3	鉴别信息
5.18	09.2.2, 09.2.5, 09.2.6	访问权
5.19	15.1.1	供应商关系中的信息安全
5.20	15.1.2	在供应商协议中强调信息安全
5.21	15.1.3	管理信息通信技术供应链中的信息安全
5.22	15.2.1, 15.2.2	供应商服务的监视、评审和变更管理

ISO/IEC 27002:2022 控制标识符	ISO/IEC 27002:2013 控制标识符	控制名称
5.23	新增	云服务使用的信息安全
5.24	16.1.1	信息安全事件管理规划和准备
5.25	16.1.4	信息安全事态的评估和决策
5.26	16.1.5	信息安全事件的响应
5.27	16.1.6	从信息安全事件中学习
5.28	16.1.7	证据收集
5.29	17.1.1, 17.1.2, 17.1.3	中断期间的信息安全
5.30	新增	业务连续性的信息通信技术就绪
5.31	18.1.1, 18.1.5	法律、法规、规章和合同要求
5.32	18.1.2	知识产权
5.33	18.1.3	记录的保护
5.34	18.1.4	隐私和个人可识别信息保护
5.35	18.2.1	信息安全的独立评审
5.36	18.2.2, 18.2.3	符合信息安全的策略、规则和标准
5.37	12.1.1	文件化的操作规程
6.1	07.1.1	审查
6.2	07.1.2	任用条款和条件
6.3	07.2.2	信息安全意识、教育和培训
6.4	07.2.3	违规处理过程
6.5	07.3.1	任用终止或变更后的责任
6.6	13.2.4	保密或不泄露协议
6.7	06.2.2	远程工作
6.8	16.1.2, 16.1.3	信息安全事态的报告
7.1	11.1.1	物理安全边界
7.2	11.1.2, 11.1.6	物理入口
7.3	11.1.3	办公室、房间和设施的安全保护
7.4	新增	物理安全监视
7.5	11.1.4	物理和环境威胁防范

ISO/IEC 27002:2022 控制标识符	ISO/IEC 27002:2013 控制标识符	控制名称
7.6	11.1.5	在安全区域工作
7.7	11.2.9	清理桌面和屏幕
7.8	11.2.1	设备安置和保护
7.9	11.2.6	组织场所外的资产安全
7.10	08.3.1, 08.3.2, 08.3.3, 11.2.5	存储媒体
7.11	11.2.2	支持性设施
7.12	11.2.3	布缆安全
7.13	11.2.4	设备维护
7.14	11.2.7	设备的安全处置或重复使用
8.1	06.2.1, 11.2.8	用户终端设备
8.2	09.2.3	特许访问权
8.3	09.4.1	信息访问限制
8.4	09.4.5	源代码的访问
8.5	09.4.2	安全鉴别
8.6	12.1.3	容量管理
8.7	12.2.1	恶意软件防范
8.8	12.6.1, 18.2.3	技术脆弱性管理
8.9	新增	配置管理
8.10	新增	信息删除
8.11	新增	数据脱敏
8.12	新增	数据防泄露
8.13	12.3.1	信息备份
8.14	17.2.1	信息处理设施的冗余
8.15	12.4.1, 12.4.2, 12.4.3	日志
8.16	新增	监视活动
8.17	12.4.4	时钟同步
8.18	09.4.4	特权实用程序的使用

ISO/IEC 27002:2022 控制标识符	ISO/IEC 27002:2013 控制标识符	控制名称
8.19	12.5.1, 12.6.2	运行系统软件的安装
8.20	13.1.1	网络安全
8.21	13.1.2	网络服务的安全
8.22	13.1.3	网络隔离
8.23	新增	网页过滤
8.24	10.1.1, 10.1.2	密码技术的使用
8.25	14.2.1	安全开发生存周期
8.26	14.1.2, 14.1.3	应用程序安全要求
8.27	14.2.5	安全体系架构和工程原则
8.28	新增	安全编码
8.29	14.2.8, 14.2.9	开发和验收中的安全测试
8.30	14.2.7	外包开发
8.31	12.1.4, 14.2.6	开发、测试和生产环境的隔离
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	变更管理
8.33	14.3.1	测试信息
8.34	12.7.1	在审计测试中保护信息系统

表B.2提供了ISO/IEC 27002:2013中规定的控制与本文件中的控制之间的对应关系。

表B.2 ISO/IEC 27002:2013 中的控制与本文件中的控制之间的对应关系

ISO/IEC 27002:2013 控制标识符	ISO/IEC 27002:2022 控制标识符	控制名称
5		信息安全策略
5.1		信息安全管理指导
5.1.1	5.1	信息安全策略
5.1.2	5.1	信息安全策略的评审
6		信息安全组织
6.1		内部组织
6.1.1	5.2	信息安全的角色和责任
6.1.2	5.3	职责分离

ISO/IEC 27002:2013 控制标识符	ISO/IEC 27002:2022 控制标识符	控制名称
6.1.3	5.5	与职能机构的联系
6.1.4	5.6	与特定相关方的联系
6.1.5	5.8	项目管理中的信息安全
6.2		移动设备和远程工作
6.2.1	8.1	移动设备策略
6.2.2	6.7	远程工作
7		人力资源安全
7.1		任用前
7.1.1	6.1	审查
7.1.2	6.2	任用条款及条件
7.2		任用中
7.2.1	5.4	管理责任
7.2.2	6.3	信息安全意识、教育和培训
7.2.3	6.4	违规处理过程
7.3		任用的终止和变更
7.3.1	6.5	任用终止或变更的责任
8		资产管理
8.1		有关资产的责任
8.1.1	5.9	资产清单
8.1.2	5.9	资产的所属关系
8.1.3	5.10	资产的可接受使用
8.1.4	5.11	资产归还
8.2		信息分级
8.2.1	5.12	信息的分级
8.2.2	5.13	信息的标记
8.2.3	5.10	资产的处理
8.3		媒体处理
8.3.1	7.10	移动媒体的管理
8.3.2	7.10	媒体的处置
8.3.3	7.10	物理媒体的转移
9		访问控制
9.1		访问控制的业务要求
9.1.1	5.15	访问控制策略
9.1.2	5.15	网络和网络服务的访问
9.2		用户访问管理
9.2.1	5.16	用户注册和注销
9.2.2	5.18	用户访问供给

ISO/IEC 27002:2013 控制标识符	ISO/IEC 27002:2022 控制标识符	控制名称
9.2.3	8.2	特许访问权管理
9.2.4	5.17	用户的秘密鉴别信息管理
9.2.5	5.18	用户访问权的评审
9.2.6	5.18	访问权的移除或调整
9.3		用户责任
9.3.1	5.17	秘密鉴别信息的使用
9.4		系统和应用访问控制
9.4.1	8.3	信息访问限制
9.4.2	8.5	安全登录规程
9.4.3	5.17	口令管理系统
9.4.4	8.18	特权实用规程的使用
9.4.5	8.4	程序源代码的访问控制
10		密码
10.1		密码控制
10.1.1	8.24	密码控制的使用策略
10.1.2	8.24	密钥管理
11		物理和环境安全
11.1		安全区域
11.1.1	7.1	物理安全边界
11.1.2	7.2	物理入口控制
11.1.3	7.3	办公室、房间和设施的安全保护
11.1.4	7.5	外部和环境威胁的安全防护
11.1.5	7.6	在安全区域工作
11.1.6	7.2	交接区
11.2		设备
11.2.1	7.8	设备安置和保护
11.2.2	7.11	支持性设施
11.2.3	7.12	布缆安全
11.2.4	7.13	设备维护
11.2.5	7.10	资产的移动
11.2.6	7.9	组织场所外的设备与资产安全
11.2.7	7.14	设备的安全处置或重复使用
11.2.8	8.1	无人值守的用户设备
11.2.9	7.7	清理桌面和屏幕策略
12		运行安全
12.1		运行规程和责任
12.1.1	5.37	文件化的操作规程

ISO/IEC 27002:2013 控制标识符	ISO/IEC 27002:2022 控制标识符	控制名称
12.1.2	8.32	变更管理;
12.1.3	8.6	容量管理
12.1.4	8.31	开发、测试和运行环境的隔离
12.2		恶意软件防范
12.2.1	8.7	恶意软件的控制
12.3		备份;
12.3.1	8.13	信息备份
12.4		日志和监视
12.4.1	8.15	事态日志
12.4.2	8.15	日志信息的保护
12.4.3	8.15	管理员和操作员日志
12.4.4	8.17	时钟同步
12.5		运行软件控制
12.5.1	8.19	运行系统软件的安装
12.6		技术方面的脆弱性管理
12.6.1	8.8	技术方面的脆弱性管理
12.6.2	8.19	软件安装限制
12.7		信息系统审计的考虑
12.7.1	8.34	信息系统审计控制
13		通信安全
13.1		网络安全管理
13.1.1	8.20	网络控制
13.1.2	8.21	网络服务的安全
13.1.3	8.22	网络中的隔离
13.2		信息传输
13.2.1	5.14	信息传输策略和规程
13.2.2	5.14	信息传输协议
13.2.3	5.14	电子传输
13.2.4	6.6	保密或不泄露协议
14		系统获取、开发和维护
14.1		信息系统的安全要求
14.1.1	5.8	信息安全要求分析和说明
14.1.2	8.26	公共网络上应用服务的安全保护
14.1.3	8.26	应用服务事务的保护
14.2		开发和支持过程中的安全
14.2.1	8.25	安全的开发策略
14.2.2	8.32	系统变更控制规程

ISO/IEC 27002:2013 控制标识符	ISO/IEC 27002:2022 控制标识符	控制名称
14.2.3	8.32	运行平台变更后对应用的技术评审
14.2.4	8.32	软件包变更的限制
14.2.5	8.27	安全的系统工程原则
14.2.6	8.31	安全的开发环境
14.2.7	8.30	外包开发
14.2.8	8.29	系统安全测试
14.2.9	8.29	系统验收测试
14.3		测试数据
14.3.1	8.33	测试数据的保护
15		供应商关系
15.1		供应商关系中的信息安全
15.1.1	5.19	供应商关系的信息安全策略
15.1.2	5.20	在供应商协议中强调安全
15.1.3	5.21	信息与通信技术供应链
15.2		供应商服务交付管理
15.2.1	5.22	供应商服务的监视和审查
15.2.2	5.22	供应商服务的变更管理
16		信息安全事件管理
16.1		信息安全事件和改进的管理
16.1.1	5.24	责任和规程
16.1.2	6.8	信息安全事态的报告
16.1.3	6.8	报告信息安全脆弱性
16.1.4	5.25	信息安全事态的评估和决策
16.1.5	5.26	信息安全事件的响应
16.1.6	5.27	从信息安全事件中学习
16.1.7	5.28	证据收集
17		业务连续性管理的信息安全方面
17.1		信息安全的连续性
17.1.1	5.29	规划信息安全连续性
17.1.2	5.29	实现信息安全连续性
17.1.3	5.29	验证、评审和评价信息安全连续性
17.2		冗余
17.2.1	8.14	信息处理设施的可用性
18		符合性
18.1		符合法律和合同要求
18.1.1	5.31	适用的法律和合同要求的识别
18.1.2	5.32	知识产权

ISO/IEC 27002:2013 控制标识符	ISO/IEC 27002:2022 控制标识符	控制名称
18.1.3	5.33	记录的保护
18.1.4	5.34	隐私和个人可识别信息保护
18.1.5	5.31	密码控制规则
18.2		信息安全评审
18.2.1	5.35	信息安全的独立评审
18.2.2	5.36	符合安全策略和标准
18.2.3	5.36, 8.8	技术符合性评审

参 考 文 献

[1] ISO 9000 质量管理体系 基础和术语

[2] ISO 55001 资产管理 管理体系 要求

[3] ISO/IEC 11770（所有部分） 信息技术 安全技术 密钥管理

[4] ISO/IEC 15408（所有部分） 信息技术 安全技术 信息技术安全评估准则

[5] ISO 15489（所有部分） 信息与文献 文件（档案）管理

[6] ISO/IEC 17788 信息技术 云计算 概览与词汇

[7] ISO/IEC 17789 信息技术 云计算 参考架构

[8] ISO/IEC 19086（所有部分） 信息技术 云计算 服务水平协议（SLA）框架

[9] ISO/IEC 19770（所有部分） 信息技术 IT 资产管理

[10] ISO/IEC 19941 信息技术 云计算 互操作性和可移植性

[11] ISO/IEC 20889 隐私增强数据去识别术语和技术分类

[12] ISO 21500 项目、项目群和项目组合管理 背景和概念

[13] ISO 21502 项目、项目群和项目组合管理 项目管理指南

[14] ISO 22301 安全与弹性 业务连续性管理体系 要求

[15] ISO 22313 安全与弹性 业务连续性管理体系 ISO 22301 的使用指南

[16] ISO/TS 22317 公共安全 业务连续性管理体系 业务影响分析指南（BIA）

[17] ISO 22396 安全与弹性 社区弹性 组织间信息交换指南

[18] ISO/IEC TS 23167 信息技术 云计算 常用技术和工艺

[19] ISO/IEC 23751:2022 信息技术 云计算和分布式平台 数据共享协议（DSA）框架

[20] ISO/IEC 24760（所有部分） IT 安全和隐私 身份管理框架

[21] ISO/IEC 27001:2013 信息技术 安全技术 信息安全管理体系 要求

[22] ISO/IEC 27005 信息技术 安全技术 信息安全风险管理

[23] ISO/IEC 27007 信息技术、网络安全和隐私保护 信息安全管理体系审核指南

[24] ISO/IEC TS 27008 信息技术 安全技术 信息安全控制评估指南

[25] ISO/IEC 27011 信息技术 安全技术 基于 ISO/IEC 27002 的电信组织信息安全控制实践指南

[26] ISO/IEC TR 27016 信息技术 安全技术 信息安全管理 组织经济学

[27] ISO/IEC 27017 信息技术 安全技术 基于 ISO/IEC 27002 的云服务信息安全控制实践指南

[28] ISO/IEC 27018 信息技术 安全技术 个人可识别信息（PII）处理者在公有云中保护 PII的实践指南

[29] ISO/IEC 27019 信息技术 安全技术 能源公用事业行业的信息安全控制

[30] ISO/IEC 27031 信息技术 安全技术 ICT 业务连续性准备指南

[31] ISO/IEC 27033（所有部分） 信息技术 安全技术 网络安全

[32] ISO/IEC 27034（所有部分） 信息技术 应用安全

[33] ISO/IEC 27035（所有部分） 信息技术 安全技术 信息安全事件管理

[34] ISO/IEC27036（所有部分） 信息技术 安全技术 供应商关系的信息安全

[35] ISO/IEC27037 信息技术 安全技术 数字证据的识别、收集、采集和保存指南

[36] ISO/IEC 27040 信息技术 安全技术 存储安全

[37] ISO/IEC27050（所有部分） 信息技术 电子发现

[38] ISO/IECTS 27110 信息技术、网络安全和隐私保护 网络安全框架开发指南

[39] SO/IEC 27701 安全技术 ISO/IEC 27001 与 ISO/IEC 27002 在隐私信息管理的扩展 要求与指南

[40] ISO 27799 健康信息学 使用 ISO/IEC 27002 的健康信息安全管理

[41] ISO/IEC 29100 信息技术 安全技术 隐私保护框架

[42] ISO/IEC 29115 信息技术 安全技术 实体身份验证保证框架

[43] ISO/IEC 29134 信息技术 安全技术 隐私影响评估指南

[44] ISO/IEC 29146 信息技术 安全技术 访问管理框架

[45] ISO/IEC 29147 信息技术 安全技术 漏洞披露

[46] ISO 30000 船舶与海上技术 拆船管理体系 拆船厂安全与环境无害化管理体系规范

[47] ISO/IEC 30111 信息技术 安全技术 漏洞处理过程

[48] ISO 31000:2018 风险管理 指南

[49] IEC 31010 风险管理 风险评估技术

[50] ISO/IEC 22123（所有部分） 信息技术 云计算

[51] ISO/IEC 27555 信息安全、网络安全和隐私保护 个人可识别信息删除指南