信息技术 安全技术

信息安全控制实用规则

Information technology-Security techniques

-Code of practice for information security controls

（ISO/IEC 27002：2013）

目　　录

前言

ISO 和 IEC 形成全球标准专业系统。通过技术委员会建立的参与开发国际标准的 ISO 或 IEC 的成员国，由各自的组织处理特定的技术活动的领域。ISO 和 IEC 技术委员会协调共同感兴趣的领域。与 ISO 和 IEC 联络的其它国际组织、政府和非政府的组织也参与了这个工作。在信息技术领域，ISO 的 IEC 已经建立了一个联合技术委员会，ISO/IEC JTC 1。

国际标准被起草与 ISO/IEC 导则，Part 2 给出的规则一致。

ISO/IEC 27002 已拟定联合技术委员会 ISO/IEC JTC 1，信息技术，小组委员会 SC 27， IT 安全技术。

注意，本文档可能是专利权主体的某些元素的可能性是存在的。 ISO 将不负责识别任何或所有这样的专利权问题。

本第二版抵消并替代了第一版(ISO/IEC 27002:2005)，已在技术和结构上进行了修订。

文件说明

本标准是笔者利用业余时间自行翻译。因笔者水平有限，错误和疏漏之处再所难免。欢迎各位批评指正。

特别声明：

a) 若因阅读和使用本翻译标准给读者造成的任何损失，本人一概不承担任何责任；
b) 本翻译标准著作权归本人所有，仅供阅读学习之用，未经许可，不得用于任何商业目的。

笔者联系方式：
邮箱：lzh900@163.com
ＱＱ：605577186

李振华
QMS/ISMS/SMS/ITSS/COBIT/CISP/R&S/SercityCCIE
2014 年 7 月于北京

0 引言

0.1 背景和语境

设计本国际标准作为组织基于 ISO/IEC 27001 的信息安全管理体系（ISMS）实施过程中选择控制措施的参考，或作为组织实施通常被公认的信息安全控制措施的参考。本标准也适用于发展工业和组织具体的信息安全管理指导方针，考虑到他们具体的信息安全风险的环境。

各种类型和规模（包括公有和私营行业、商业和非盈利）的组织发多种形式收集、处理、存储和传输信息，包括电子、物理和口头的（如，交谈和报告）。

信息的价值超越了文字、数字和图像：知识、观念、思想和品牌是无形的信息形式的例子。在一个相互联系的世界，包含在他们的操作、处理和保护中的信息和相关的过程、系统、网络和人员，是象其它重要业务资产一样的资产，对组织的业务是有价值的，因此，应得到或需要保护防止各种危险。

资产容易遭受故意或无意的威胁，在相关的过程、系统、网络和人员有自身的脆弱性的时候。业务过程和系统的变化，或其它外部的变化（如，新的法律和法规），可能产生新的信息安全风险。因而，考虑到威胁利用脆弱性损害组织，已经呈现的信息安全风险的多种方法。有效的由保护组织防止威胁和脆弱性信息安全降低这些风险，进而降低对它的资产的影响。

实施一组适当的控制措施实现信息安全，包括策略、过程、程序、组织结构和软硬件功能。如果需要，这些控制措施需要建立、实施、监视、评审和改进，以确保满足组织的特定的安全和业务目标。ISMS（如 ISO / IEC 27001 规定的） 从全面协调组织信息安全风险的视角，在相干管理体系的整体框架下，有序实施一套全面的信息安全控制措施。

许多信息系统没有设计成 ISO/IEC 27001 和这个标准中理解的安全。通过技术手段实现的安全性是有限的，应支持适当的管理和程序。在要求的地方，控制措施的识别要仔细的规划并关注细节。成功的 ISMS 得到组织中所有雇员的支持。它也可能要求利益干系人、供应商和其它外部团体的参与。来自外部团体专家的建议也是需要的。

在更一般的意义上说，有效的信息安全向管理者和其它利益干系人保证，组织的资产是相当的安全，被保护防止损坏，因而，担当一个业务的使能者。

0.2 信息安全要求

组织识别它的安全要求是基本的。有三个安全要求的主要来源：

a) 对组织的风险评估，考虑组织整体业务战略和目标。通过风险评估，对资产的威胁被识别，脆弱性发生的可能性被评价，潜在的影响被估计；

b) 组织的法律、法规、监管和合同要求，交易伙伴、承包人和服务提供商必须满足，和他们的社会文化环境；

c) 组织的信息操作、处理、存储、传达和存档的原则、目标和业务要求被开发并支

持它的运行。

实放控制措施中的资源使用需要来平衡，防止可能缺乏这些控制措施的安全问题而导致业务损害。风险评估的结果帮助指导和确定适当的管理活动和管理信息安全风险的优先级，并实施被选择的控制措施以保护防止这些风险。

ISO/IEC 27005 提供了信息安全风险管理指南，包括风险评估、风险处置、风险接受、风险传达、风险监视和风险评审。

0.3 选择控制措施

从本标准或其他控制措施集选择控制措施，或设计新的控制措施，来满足特定的需要是适当的。

控制措施的选择依赖于组织基于风险接受准则、风险处置选择和应用于组织的一般风险管理方法来决定，并也应遵从所有相关的国家、国际法律和法规。控制措施选择也依赖于控制措施交互的提供深度防护的方法。

本标准中的某些控制措施可被当作信息安全管理的指导原则，并且可用于大多数组织。下面的实施指南提供更详细的控制措施的解释。更多的关于选择控制措施和其他风险处理选择可以在 ISO/IEC 27005 中找到。

0.4 开发你自己的指南

本国际标准可认为是组织开发其详细指南的起点。对一个组织来说，本实用规则中的控制措施和指南并非全部适用，此外，没有包括在本标准中的另外的控制措施被要求。

为便于审核员和业务伙伴进行符合性检查，当开发包含另外的指南或控制措施的文件时，对本标准中条款的相互参考可能是有用的。

0.5 生命周期考虑

信息有一个自然的生命周期，从建立、开始、存储、处理、使用和传输，到最终的毁灭或衰落。资产的价值和风险在他们的生命周期（如，公司财务收号的非授权泄漏或被盗，远不及他们被正式地公布重要）是可以变化的，但信息安全仍然重要对所有阶段的某些程度。

信息系统有生命周期，他们被构想、详述、开发、测试、实施、使用、维护和到期退役从服务和解决。信息安全应考虑每一个阶段。新系统开发和变更到现有系统，组织更新和提升安全控制，考虑当前实际的的和规划的信息安全风险事件。

0.6 相关标准

本标准提供一个很宽范围的通常被普遍应用于许多不同组织的信息安全控制措施，ISO/IEC 27000 标准簇在管理信息安全全过程的其它方面提供了更完整的建议或要求

参考 ISO/IEC 27000 为一般的介绍于 ISMS 和标准簇。ISO/IEC 27000 提供一个词汇表，正式地定义使用在整个 ISO/IEC 27000 标准簇中的大部分术语，描述了每个家族成员的和目标。

信息技术　安全技术 信息安全控制实用规则

1　范围

本国际标准给出了组织信息安全标准和信息安全管理实践指南，包括考虑组织的信息安全风险环境的控制措施的选择、实施和管理。

本国际标准被设计由组织使用致力于：

a）实现基于ISO/IEC 27001信息安全管理体系过程中选择控制措施；

b）实现普遍接受的信息安全控制；

c）开发他们自己的信息安全管理指南。

2　引用标准

下列文档，全部或部分，是本标准参考的标准，并在它的应用上是不可缺少的。有日期的参考，仅这个版本被引用适合。没标注日期的参考，参考文档（包括任何的修订）的最近版本被应用。

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

3　术语和定义

ISO/IEC 27000给出的术语和定义适用于本文档的目的。

4　本标准的结构

本标准包括 11 个安全控制措施的章节（共含有 39 个主要安全类别）和 1 个介绍风险评估和本标准的结构

本标准包含14个安全控制条款，共包含35个主要的安全类别和114条控制措施。

4.1　条款

每个条款定义安全控制措施包含一个或多个主要的安全类别。

本标准中条款的顺序不意味着他们的重要性。依赖于环境、来自任何或所有条款安全控制措施可能是重要的，因而，每个组织应用本标准应识别出适合的控制措施，这些是如何的重要以及他们应用到单独的业务过程。此外，本标准所列出的不是优先顺序。

4.2　控制措施类别

每一个主要的安全控制措施类别包含：

a）　一个控制目标，声明要实现什么；

b）　一个或多个控制措施，可能被应用来实现这个控制目标。

控制措施描述被结构化如下：

控制措施

定义满足控制目标的特定的控制措施的陈述。

实施指南

提供更多的细节信息来支持控制措施的实施和满足控制目标。这个指南可能不完全适合或满足所有的情况，可能不能达到组织具体的控制措施要求。

其它信息

提供更进一步可能需要考虑的信息，如，法律考虑和其它标准的参考。如果没有其它信息被提供的话，这个部分不显示。

5 信息安全方针

5.1 信息安全管理方向

目标：为信息安全提供管理指导和支持并确保与业务需求和相关法律和法规相一致。

5.1.1 信息安全方针（原条款不变）

控制措施

一组信息安全方针应被定义，并由管理者批准、发布、传达给所有员工和外部团体。

实施指南

在最高级，组织应定义一个由管理者批准的“信息安全方针”，阐述组织管理信息安全目标的方法。

信息安全方针应定位于下面建立的要求：

a) 业务战略；

b) 法规、法律和合同；

信息安全方针应包含的声明：

a) 指导所有相关信息安全活动的信息安全、目标和原则的定义；

b) 为信息安全管理定义的角色的一般和具体的责任分配；

c) 处理偏差和异常处理。

在较低级，信息安全方针应以具体主题的策略来支持，更进一步的授权信息安全控制措施的实施，且是典型的结构来处理组织某个目标组的需要或覆盖某个主题。

这样的策略主题案例包括：

a) 访问控制（见 9）；

b) 信息分类（和处理）（见 8.2）；

c) 物理和环境安全（见 11）；

d) 面向最终用户的主题如下：

1) 资产的可接受使用（见 8.1.3）；

2) 清空桌面和清除屏幕（见 11.2.9）；

3) 信息转移（见 13.2.1）；

4) 移动设备和远程工作（见 6.2）；

5) 软件安全和使用的限制（见 12.6.2）；

e) 备份（见 12.3）；

f) 信息转移（见 13.2）；

g) 恶意软件的防护（见 12.2）；

h) 技术脆弱性管理（见 12.6.1）；

i) 密码学控制（见 10）；

j) 通讯安全（见 13）；

k) 个人可识别信息的隐私和保护（见 18.1.4）；

l) 供应商关系（见 15）；

这些策略应与雇员和相关外部团体以一种相关联的、易接受的和易理解的方式进行沟通，如，一个“信息安全意识、教育和培训程序（见 7.2.2）”的文本。

其它信息

需要各种贯穿组织内部的信息安全策略。内部策略对大型或更的组织尤其的有用，这些定义和批准的控制措施的预期水平与那些实施的控制措施进行分离，或一个策略应用于组织内许多不同的人或功能。信息安全策略可以以一个单独的“信息安全策略“文件发布，或作为一组单独的相关文件。

如果任何信息安全策略分配到组织外部，应注意不要泄漏保密信息。

一些组织对这些策略文件使用其它的术语，如，“标准”、“指导”或“规则”。

5.1.2 信息安全方针的评审（原条款不变）

控制措施

应按计划的时间间隔或当重大变化发生时进行信息安全方针评审，以确保它持续的适宜性、充分性和有效性。

实施指南

每个方针应有一个由管理者批准的所有人，他负有对方针进行开发、评审和评价的职责。评审应包括评估组织方针改进的机会，和管理信息安全响应组织环境、业务状况、法律条件或技术环境变化的方法。

信息安全方针的评审应考虑管理评审的结果。

应获得管理对一个修订方针的批准。

6 信息安全组织

6.1 内部组织

目标：建立一个管理框架，发起和控制组织内信息安全的实施和运行。

6.1.1 信息安全角色和职责（原 6.1.3）

控制措施

所有的信息安全职责应被定义和分配。

实施指南

信息安全职责的分配应和信息安全方针（见 5.1.1）相一致。各个资产的保护和执行特定安全过程的职责应被清晰的识别。信息安全风险管理活动的职责，特别是残余风险的接受被定义。这些职责应在必要时加以补充，为特定场所和信息处理设施提供更详细的指南。资产保护和执行特定安全过程的局部职责应予以清晰地定义。

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

个人负责的领域要予以清晰地规定；特别是，应进行下列工作：

a) 资产和信息安全过程应予以识别并清晰地定义；
b) 应分配每一资产或安全过程的实体职责，并且该职责的细节应形成文件（见 8.1.2）；
c) 授权级别应清晰地予以定义，并形成文件；
d) 被指定为在信息安全领域能履行职责的个人，应在这个领域有能力并给出最新发展的机会；
e) 供应商关系信息安全方面的协调和监管应被确定并形成文档。

其它信息

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

然而，资源和实施控制措施的职责归于个别的管理人员。一种通常的做法是对每一资产指定一名所有人，他也就对该信息资产的日常保护负责。

6.1.2 职责分离（原 10.1.3）

控制措施

冲突的职责和权限应被分开，减少对组织资产未经授权或无意的修改或误用。

实施指南

应注意，在无授权或未被监测时，应使个人不能访问、修改或使用资产。事件的启动要与其授权分离。勾结的可能性应在设计控制措施时予以考虑。

小型组织可能感到难以实现这种责任分割，但就可能性和可行性来说，该原则是适用的。如果难以分割，应考虑其他控制措施，例如对活动的监视、审计跟踪和管理监督应被考虑。

其它信息

职责分离是减小无意或有意滥用组织资产的一个方法。

6.1.3 与监管机构的联系（原 6.1.6）

控制措施

应与监管机构保持适当的联系。

实施指南

组织应有程序指明什么时候应当与哪个部门（例如，执法部门、监管团体、监管机构）联系，以及如何确认信息安全事件及时的报告（如，怀疑可能触犯了法律时）。

其它信息

来自互联网攻击下的组织，可能需要授权采取行动来抵制攻击源。

保持这样的联系可能是支持信息安全事件管理（第 16）或业务连续性和应急计划过程（第 17）的要求。与监管团体的联系有助于预先知道组织必须遵循的法律法规方面预期的变化，并为这些变化做好准备。与其他监管部门的联系包括公共事业、应急服务、电力供应、健康和安全等。如，消防部门（业务连续性连接有关）、电信提供商（与路由连接性和可用性有关）、供水部门（与设备的冷却设施有关）。

6.1.4 与特定利益集团的联系（原 6.1.7）

控制措施

与特殊权益团体、其他专业安全论坛和行业协会保持适当联系。

实施指南

应考虑成为特定利益集团或论坛的成员，以便：

a) 增进对最佳实践和最新相关安全信息的了解；
b) 确保当前的信息安全环境的了解是最近的和完整的；
c) 尽早收到关于攻击和脆弱性的预警、建议和补丁；
d) 获得信息安全专家的建议；
e) 分享和交换关于新的技术、产品、威胁或脆弱性的信息；
f) 提供处理信息安全事件时适当的联络点（见 16）。

其它信息

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

6.1.5 项目管理中的信息安全（新增）

控制措施

信息安全应融入项目管理中，与项目类型无关。

实施指南

信息安全应被集成到组织的项目管理方法中，以确保信息安全风险被识别并以项目的一部分被处理。这个一般应用到任何项目中，不管项目的性质，如，核心业务过程的项目、IT、设备管理和其它的支持过程。使用的项目管理方法应要求：

a) 信息安全目标包含在项目目标中；
b) 一个信息安全风险评估被执行在项目的早期阶段，以识别必要的控制措施；
c) 信息安全是应用项目方法所有阶段的一部分。

信息安全影响在所有项目中应被处理并定期评审。信息安全的职责应被定义并分配给

项目管理方法中定义的特定的角色。

6.2 移动设备和远程工作

目标：确保远程工作和移动设备使用的安全。

6.2.1 移动设备策略（原 11.7.1）

控制措施

一个策略和配套的安全措施应被采用，以管理使用移动设备带来的风险。

实施指南

当使用移动设备时，应特别小心以确保业务信息不被破坏。移动设备策略应考虑到在不受保护的环境下使用移动设备工作的风险。

移动设备策略应考虑：

a) 移动设备的注册；
b) 物理保护的要求；
c) 软件安装的限制；
d) 移动设备软件版本和应用补丁的要求；
e) 连接到信息服务的限制；
f) 访问控制；
g) 密码技术；
h) 恶意软件保护；
i) 远程禁用、删除或锁定；
j) 备份；
k) Web 服务和 web 应用的使用。

在公共场所、会议室和其它未受保护的区域使用移动设备时应特别小心。应保护在这些场所的设备避免未授权访问或泄露这些设施所存储和处理的信息，如，使用密码技术（见 10）和强制使用秘密身份认证信息（见 9.2.4）。

移动设备也应物理保护，避免被盗，尤其当离开（如，在汽车和其它运输形式、宾馆、会议中心和会议室）的时候。一个明确的程序应被建立，考虑法律、保险和组织的其它安全要求，在移动设备被盗或丢失的情况下。设备携带重要的、敏感的或关键的业务信息，不应离开无人看管，如果可能，应物理上锁带离或特殊锁应被使用来保护这个设备。

对于使用移动计算设施的人员应安排培训，以提高他们对这种工作方式导致的附加风险的意识，并且应实施控制措施。

移动设备策略允许拥有移动设备的个人使用的地方，这个策略和相关安全测量也应考虑：

a) 设备个人和业务使用分离，包括使用软件来支持分离和保护个人设备上的业务数

据；

b) 提供对业务信息的访问，仅当用户签署一个终端用户协议了解他们的职责之后（物理保护、软件更新等），宣布放弃业务数据的所有权、在设备被盗或丢失的情况下允许由组织远程擦去数据，或当不再被授权使用这个设备的时候。这个策略需要考虑隐私法。

其它信息

移动设备无线网络连接类似于其他类型的网络连接，但在确定控制措施时，应考虑两者的重要区别。典型的区别有：

a) 一些无线安全协议是不成熟的，并有已知的弱点；

b) 存储在移动设备上信息可能不能备份，因为受限的网络带宽和/或因为移动设备在规定的备份时间不能进行连接。

移动设备通常共享普通的功能，如网络、互联网访问、e-mail 和文件处理，固定的使用设备。移动设备信息安全控制措施通常由采用那些固定使用设备和那些在组织附属建筑外的使用的威胁增加的设备。

6.2.2 远程工作（原 11.7.2）

控制措施

应实施策略和配套的安全措施来保护信息被访问、被处理或被存储在远程工作站点。

实施指南

组织允许远程工作活动应发布一个策略，定义使用远程工作的条件和限制。被视为合适的和由法律允许的地方，应考虑下面的问题：

a) 远程工作场地的现有物理安全，要考虑到建筑物和本地环境的物理安全；

b) 推荐的物理的远程工作环境；

c) 通信安全要求，要考虑远程访问组织内部系统的需要、被访问的并且在通信链路上传递的信息的敏感性，以及内部系统的敏感性；

d) 预防私有设备上处理和存储信息的虚拟桌面访问的规定

e) 未授权访问信息或由其它人使用住宿的资源的威胁，如，家人和朋友；

f) 家庭网络的使用和无线网络服务配置的要求或限制；

g) 针对私有设备开发的预防知识产权争论的策略和程序；

h) 法律禁止的对私有设备的访问（检查机器安全或在调查期间）；

i) 使组织对雇员或外部团体用户私人拥有的工作站上的客户端软件负有责任的软件许可协议；

j) 恶意软件保护和防火墙要求。

要考虑的指南和安排应包括：

a) 当不允许使用不在组织控制下的私有设备时，对远程工作活动提供合适的设备和存储设施；

b) 确定允许的工作、工作小时数、可以保持的信息分类和授权远程工作者访问的内部系统和服务；

c) 提供适合的通信设备，包括使远程访问安全的方法；

d) 物理安全；

e) 有关家人和来宾访问设备和信息的规则和指南；

f) 硬件和软件支持和维护的规定；

g) 保险的规定；

h) 用于备份和业务连续性的程序；

i) 审计和安全监视；

j) 当远程工作活动终止时，撤销授权和访问权，并返回设备。

其它信息

远程工作指的是各种形式的办公室外面，包括非传统的工作环境， 如那些被称为“远程办公”，“灵活的工作场所”，“远程工作”和“虚拟网络” 环境。

7 人力资源安全

7.1 任用前

目标：确保雇员和承包人理解其职责、考虑其承担的角色是适合的。

7.1.1 筛查（原 8.1.2）

控制措施

所有雇用的候选人背景调查应被执行依据相关法律、法规、道德规范，并应符合业务需求、使用的信息分类及意识到的风险。

实施指南

验证应考虑所有相关的隐私、个人可识别信息的保护和任用相关的法律，并应包括以下内容（允许时）：

a) 令人满意的性格借鉴的可用性（如，一个企事业和一个个人）；

b) 申请人履历的核查（针对完备性和准确性）；

c) 声称的学业和专业资质的确认；

d) 独立的身份证明（护照或类似文件）；

e) 更多详细的检查，例如信用复查或犯罪记录检查。

当一个人个被聘用为一个特殊的信息安全角色的时候，组织应确定候选人：

a) 有必要的能力来扮演这个安全角色；

b) 能被信任担当这个角色，尤其是如果这个角色对组织是重要的。

一个工作的地方，或者是最初任命的，或者是升职的，涉及到这个人对信息处理设施进行访问，和，特别是，如果这些设施正在处理保密信息，例如，财务信息或高度保密的

信息，那么，组织还要考虑进一步的、更详细的核实。

程序应定义验证检查的准则和限制，如，谁有资格审查人员，以及如何、何时、为什么执行验证检查。

对于承包人也应确保一个筛选过程。在这些情况下，组织与承包人之间的合同，应明确提出责任：有组织的筛选；如果未完成审查或结果引起怀疑或关注时，需要遵循的通知程序。

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

7.1.2 任用条款和条件（原 8.1.3）

控制措施

与员工和承包人达成一致的合同，应规定他们的和组织的信息安全责任。

实施指南

员工或承包人的合同责任，还应反应组织的信息安全方针，除澄清和声明以下内容：

a) 所有访问保密信息的雇员、承包人要在给予访问信息处理设施权之前签署保密或不泄露协议（见 13.2.4）；
b) 雇员、承包人的法律义务和权利，例如关于版权法、数据保护法（见 18.1.2 和 18.1.4）；
c) 由雇员或承包人处理的与信息、信息处理设施和信息服务相关的信息的分类和组织资产的管理的职责（见 8）；
d) 由雇员或承包人处理接收到的其他公司或外部团体的信息的职责；
e) 如果雇员或承包人漠视组织的安全要求所采取的措施（见 7.2.3）。

信息安全角色和责任应传达给工作候选人，在雇用前处理。

组织应确保雇员或承包人同意适用于他们将访问的与信息系统和服务有关的组织资产的性质和程度的信息安全条款和条件。

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

其它信息

一个行为细则被使用来规定雇员的或承包人的关于保密性、数据保护、道德规范、组织设备和设施的适当使用以及组织期望的最佳实践的信息安全责任。与承包人合伙的一个外部团体，可能被要求考虑签订商定的个别利益的协议。

7.2 任用中

目标：确保员工和承包人意识到并履行信息安全职责。

7.2.1 管理者职责（原 8.2.1）

控制措施

管理者应要求所有员工和承包人运用信息安全与组织已建立的策略和程序相一致。

实施指南

管理者职责应包括确保雇员和承包人：

a) 在被准许访问保密信息或信息系统前，应适当的向他们介绍他们的信息安全角色和责任；

b) 获得声明他们在组织中角色的信息安全期望的指南；

c) 被激励来履行组织的信息安全策略；

d) 对于他们在组织内相关的角色和职责的信息安全的意识达到一定级别（见 7.2.2）；

e) 遵守任用的条款和条件，包括组织的信息安全方针和适当的工作方法；

f) 持续拥有适当的技能和资格以及规定的基本的教育；

g) 提供一个匿名举报的通道，来报告信息安全方针或程序的违反情况（“揭发”）。

管理者应说明对信息安全方针、程序和控制措施的支持，并担当一个角色模范。

其它信息

如果雇员和承包人没有意识到他们的安全职责，他们会对组织造成相当大的破坏。激励全体员工可能更可靠的和产生尽量少的信息安全事件。

管理不善会使员工低估信息安全对组织产生的负面影响。例如，缺乏有效的管理可能导致安全被忽视或组织资产的潜在误用。

7.2.2 信息安全意识、教育和培训（原 8.2.2）

控制措施

组织内所有员工、相关方、承包人应接受适当的意识教育和培训，并定期更新与他们工作职责相关的组织策略及程序。

实施指南

信息安全意识程序应致力于使员工、相关方、 承包人意识到他们的信息安全责任和通过哪些这些责任被解除。

信息安全意识程序应被建立，与组织的信息安全方针和相关程序保持一致，考虑到组织被保护的信息和已执行了保护信息的控制措施。意识程序包括了很多意识提升的活动，如，竞赛（如，一个信息安全日）和发布小册子或简报。

意识程序应被规划，考虑到员工在组织中的角色、场所、组织对承包人的意识期望。意识程序的活动应随时间的推移、定期地规划，以至于活动被重复并训练新员工和承包人。意识程序也应被定期地更新，按时与组织策略和程序保持一致，并应建立在信息安全事件的经验教训中。

意识培训应被执行作为组织信息安全意识程序的要求。意识培训可以使用不同的交付介质，包括基于课堂的、远程学习、基于 web 的、自学和其它。

信息安全教育和培训也应包含如下方面：

a) 规定管理者贯穿组织的信息安全担负的责任；

b) 需要友好的并遵从适当的信息安全规则和责任，如同被定义的策略、标准、法律、法规、合同和协议；

c) 任何人自己的作为和不作为的个人责任，和对安全或保护属于组织和外部团体的信息的一般责任；

d) 基本的信息安全责任（如，信息安全事件报告）和基准的控制措施（如，口令安全、恶意代码控制和清空桌面）；

e) 额外的信息安全事件的信息和建议所需要的联络点和资源，对信息安全事件的忠告，包括进一步的信息安全教育和培训材料。

信息安全教育和培训应定期地举办。最初的教育和培训适用于那些调到新的本质上不同的信息安全要求的位置或角色，不仅仅是新的开始者，而且应在角色有效之前举行。

组织应开发教育和培训程序，为了实施有效地教育和培训。这个程序应与组织的信息安全方针和相关程序保持一致，考虑组织被保护的信息和对信息保护实施的控制措施。这个程序应考虑教育和培训的不同形式，如演讲和自学。

其它信息

当构成一个意识程序的时候，不仅致力于“做什么”和“怎么做”，而且也包含“为什么做”是重要的。员工理解信息安全目标和他们自己的行为对组织的潜在的、积极的和消极的影响是重要的。

意识、教育和培训可以是分开的，或与其它的培训活动协作实施，如，IT 或一般的培训。意识、教育和培训活动应是合适的并与个人的角色、职责和技能相关联。

员工理解的评估可以在意识、教育和培训课程结束时实施，测试知识的转移。

7.2.3 纪律处理（原 8.2.3）

控制措施

对于信息安全违规的雇员，应采取一个正式的与清晰的违纪处理。

实施指南

纪律处理之前应有一个信息安全违规发生的验证过程（见 16.1.7）。

正式的纪律处理过程应确保公正和公平的处理被怀疑违反信息安全的雇员。正式的纪律处理应提供一个分等级的响应，要考虑诸如违规的性质、重要性及对业务的影响等因素，是否是第一次或重复违反，是否对违反者进行过适当的培训，相关法律、业务合同和其他因素也是需要考虑的。

纪律处理也应用来作为一个威慑，防止员工违反组织的信息安全方针和程序以及任何其它的信息安全破坏。故意破坏可要求立即行动。

其它信息

纪律处理也可成为一个动机或激励，如果确定与有关信息安全一致的异常行为要积极的制裁。

7.3 任用的终止或变化

目标：保证组织利益作为变更或终止作用过程的一部分。

7.3.1 任用终止或变化的责任（原 8.3.1）

控制措施

在任用终止或变更后信息安全责任和义务依然有效应被定义和传达给雇员或承包人，并被执行。

实施指南

终止职责的传达应包括继续存在信息安全要求和法律责任，适当时，还包括任何保密协议规定的职责（见 13.2.4），并且在雇员或承包人的任用结束后持续一段时间仍然有效的任用条款和条件（见 7.1.2）。

雇用终止后责任和义务仍然有效应被包含在雇员或承包人雇用条款和条件中（见 7.1.2）。

职责或任用的变更应被管理，作为当前职责或雇用的终止与新的职责或雇用开始相结合。

其它信息

人力资源的功能通常是全部的终止过程，并与管理相关程序信息安全方面的人员离职的监督管理员一起工作。在承包人通过外部团体提供的情况下，终止过程由外部团体来保证，并在组织与外部团体之间协商一致的处理过程。

有必要通知雇员、顾客、承包人关于组织人员的变化和运营上的安排。

8 资产管理

8.1 对资产负责

目标：识别组织资产并定义适当的保护职责。

8.1.1 资产清单（原 7.1.1）

控制措施

与信息和信息处理设施相关的资产应被识别，并编制和维护这些资产一个清单。

实施指南

一个组织应识别信息生命周期的相关资产，并记录他们的重要性。信息的生命周期应包括建立、处理、存储、传输、删除和毁灭。记录应保持适当的专有性或现有清单。

资产清单应是准确的、最新的、与其他的的清单一致并结合的。

每一个识别的资产，应分配资产的所有者（见 8.1.2），并应标识其分类（见 8.2）。

其它信息

资产清单可帮助确保有效的资产保护，也可以是其他目的需要，例如健康与安全、保

险或财务（资产管理）等原因。

ISO/IEC 27005 提供了资产的举例，当识别资产的时候，组织可能需要来考虑。编制资产清单的过程是风险管理的一个重要的先决条件（见 ISO/IEC 27000 和 ISO/IEC 27005）。

8.1.2 资产的权属（原 7.1.2）

控制措施

处于清单中的资产应被认领。

实施指南

个人以及被批准管理资产生命周期责任的其他实体有资格被分配作为资产所有人。

确保及时分配资产权属的过程通常被执行。当资产被建立或当资产被转移到组织的时间应被分配权属。资产所有人应对贯穿整个资产生命周期的资产的适当管理负责。

资产所有人应：

a) 确保资产被编制清单；

b) 确保资产被适当的分类，并被保护；

c) 定义并定期评审重要资产的访问限制和分类，考虑适当的访问控制策略；

d) 确保当资产被删除或破坏时适当的操作。

其它信息

确定所有人可以是一个个人或一个被批准控制资产整个生命周期的管理责任实体。确定所有人对资产的任何财产权不是必需的。

日常任务可以委派，例如委派给一个管理人员每天照看资产，但所有人仍保留职责。

在复杂的信息系统中，委派一组一起来提供特定服务的资产可能是有用的。在这种情况下，这个服务的所有人负责服务的交付，包括它的资产操作。

8.1.3 资产的可接受使用（原 7.1.3）

控制措施

与信息处理设施有关的信息和资产的可接受使用规则应被确定、形成文件并加以实施。

实施指南

雇员、外部团体用户使用和访问组织资产应了解与信息处理设施和资源相关的资产的信息安全要求，他们应对任何信息处理设施的使用负责，且任何这些使用在他们的职责内实施。

8.1.4 资产归还（原 8.3.2）

控制措施

所有雇员、外部团体用户在他们的雇用、合同或协议终止的时候，应归还他们拥有的所有资产。

实施指南

终止过程应被正式化，包括归还自身拥有的或委托给组织的所有先前发放的物理和电

子资产。

雇员或外部团体用户购买了组织的设备或使用他们自己的设备时，应遵循程序确保所有相关的信息已转移给组织，并且已从设备中安全的删除（见 11.2.7）。

雇员或外部团体用户了解进行的操作的重要性时，此信息应形成文件并传达给组织。

在通知终止时间期间，组织应控制由终止雇员和承包人对相关信息的非授权复制（如，知识产权）。

8.2 信息分类

目标：依照信息对组织的重要性，确保信息获得一个合适的保护级别。

8.2.1 信息的类别（原 7.2.1）

控制措施

信息应被分类，根据法律要求、价值、危险度和敏感性，对未经授权的泄漏或修改。

实施指南

信息的分类及相关保护控制措施应考虑信息共享或限制的业务需求和法律要求。不同于信息的资产也能被分类，并与被存储、由资产的其它处理或保护的信息分类一致。

信息资产的所有人应为他们的分类负责。

分类方案应包括分类的约定和一段时间后分类评审的标准。方案中应通过分析保密性、完整性、可用性及信息考虑的其它要求来确定保护级别。方案应与访问控制策略（见 9.1.1）结合考虑。

每个级别应给出一个容易理解分类方案应用上下文的名称。

方案应被考虑贯穿整个组织，因此每个人以相同的方法归类信息和相关资产，有一个保护要求和运用适当保护的共同的理解。

分类应包括在组织的过程中，并且是一致的和连贯的贯穿组织。分类的结果应表明依赖于它们对组织的敏感性和危险度的资产价值，如，依据保密性、完整性和可用性。分类的结果应依据它们生命周期中价值、敏感性和危险度的变化而更新。

其它信息

分类提供人们如何处理和保护它们的简明提示。建立类似保护需求的信息组和特有的信息安全程序，有助于应用到每个组中的所有信息。这种方法降低了逐项风险评估和控制措施的定制设计的需求。

在一段时间后，信息通常不再是敏感的或危险的，例如，当该信息已经公开时。这些方面应予以考虑，因为分类越高致使实施不必要的控制措施，从而导致附加成本或相反的在分类下可能会危及业务目标的实现。

下面是一个信息保密性分类方案的例子，可以基于四个级别：

a) 泄漏没有造成损害；

b) 泄漏造成轻微的麻烦或轻微的操作不便；

c) 泄漏造成一个显著的短期的经营或战术目标的影响；

d) 泄漏造成一个严重的长期的战备目标或组织生于生存风险的影响。

8.2.2 信息的标记（原 7.2.2）

控制措施

一套适当的信息标记程序应被开发和实施，根据组织所采用的信息分类方案。

实施指南

信息标记的程序需要涵盖信息和它相关的物理和电子格式的资产。该标记要根据 8.2.1 中建立的方案反映出分类规划。标记应容易识别。这个程序应给出在哪里和标记如何被帖上的指导，并考虑信息如何被访问或资产如何依赖于介质类型来处理。这个程序可以定义标记被忽略的地方的情况，如，非保密信息的标记可减少工作量。雇员和承包人应理解标记程序。

系统的输出包含被分类为敏感或危险的信息应携带一个适当的分类标记。

其它信息

被分类信息的标记是信息共享的一个关键要求。物理标记和元数据是一种常用的标记形式。

信息的标记和它相关的资产有时可能有负面影响。被分类的资产是容易来识别和被内部或外部的攻击者窃取。

8.2.3 资产的处理（原 7.2.2）

控制措施

处理资产的程序应被开发并实施，根据组织采用的信息分类方案。

实施指南

操作、处理、存储和传输与分类（见 8.2.1）一致的信息程序应被制定。

下列条款应被考虑：

a) 每个分类的级别支持保护要求的访问限制；

b) 资产已被授权的接受者的正式的记录的维护；

c) 临时或永久信息拷贝的保护与源信息的保护在一个级别上；

d) IT 资产依据厂商说明书的贮储；

e) 被授权接受者关注的所有介质的插贝的清晰标记。

在组织内被使用的分类方案不等于由其它组织使用的方案，即使级别的名称类似；另外，在组织之间移动的信息依赖于每个组织的背景可能改变其分类，即使他们的分类方案是相同的。

与包括信息共享的其它组织的协议，应包括识别信息分类和来自其它组织对信息标记解释的程序。

8.3 介质处理

目标：防止存储在介质上的信息被未经授权的泄漏、修改、删除或破坏。

8.3.1 可移动介质的管理（原 10.7.1）

控制措施

根据组织采用的分类方案对可移动介质的管理的程序应被执行。

实施指南

下列对于可移动介质的管理指南应加以考虑：

a） 对从组织取走的任何可重用的介质中的内容，如果不再需要，应是不可恢复的；

b） 如果需要并可行，对于从组织取走的介质应要求授权，取走的记录应加以保持，以保持审核踪迹；

c） 所有介质应被保存在符合厂商说明的保险、安全的环境中；

d） 如果数据保密性和完整性是重要的考虑因素，加密技术应被使用来保护在移动介质上的数据；

e） 为减轻介质降低而仍然需要的数据的风险，应在不可用之前将数据转移到新的介质上；

f） 有价值数据的多个插贝应在单独的介质上，以降低同时发生数据损害或丢失的风险；

g） 可移动介质的登记应被考虑，以减少数据丢失的机会；

h） 可移动驱动仅应被激活，如果是业务原因需要这样做；

i） 有一个需要使用可移动介质，将信息传输到这样介质的地方，应被监视。

程序和授权级别应被形成文件。

8.3.2 介质处置（原 10.7.2）

控制措施

不再需要的介质，应使用正式的程序安全地处置。

实施指南

应建立安全处置介质的正式程序，以最小化保密性信息泄漏给未授权人员的风险。包含保密性信息介质的安全处置程序应与信息的敏感性相一致。下列控制应予以考虑：

a) 包含有保密性信息的介质应被安全地存储和处置，如，利用焚化或切碎的方法，或者删除，由组织内其它应用使用的数据；

b) 程序应有适当的识别可能需要安全处置的条目；

c) 将所介质项收集起来并安全的处置可能是容易的，而不是试图分离出敏感项；

d) 许多组织提供收集和处置介质的服务；应仔细的选择一个合适的有足够控制能力和经验的外部团体；

e) 敏感条目的处置应被记录，以便保持审核踪迹。

当处置堆积的介质时，应考虑聚焦效应，它可能使大量不敏感信息变成敏感信息。

其它信息

被损坏的设备包含敏感数据可能需要一个风险评估，以确定这些项是否应物理破坏，而不是送出修理或丢弃（见 11.2.7）。

8.3.3 物理介质转移（原 10.8.3）

控制措施

在运输期间，包含信息的介质应加以保护，防止未经授权的访问、滥用或损坏。

实施指南

应考虑下列指南以保护运输中的包含信息的介质：

a) 应使用可靠的运输或通讯员；
b) 授权的通讯员列表应经管理者同意；
c) 验证通讯员身份的程序应被开发；
d) 包装应足以保护内容免遭在运输期间可能出现的任何物理损坏，并且符合厂商的说明，如，保护防止可能减少介质恢复效力的任何环境因素，如，暴露于过热、潮湿或电磁区域；
e) 日志应被保持，识别介质的内容，保护应用及记录转移到经过的管理人并到最终目的接收的时间。

其它信息

信息在物理运输期间易受未授权访问、不当使用或破坏，如，通过邮政服务或通讯员送介质。在这个控制措施下，介质包括纸质文档。

当介质上的保密信息不被加密的时候，额外的介质物理保护应被考虑。

9 访问控制

9.1 访问控制的业务要求

目标：限制访问信息和信息处理设施。

9.1.1 访问控制策略（原 11.1.1）

控制措施

访问控制策略应被建立、形成文件，并基于业务和信息安全要求进行评审。

实施指南

资产所有者应为接近他们资产的特定用户角色确定适当的访问控制规则、访问权利和限制，细致慎密的控制措施与信息安全风险相关联映射。

逻辑的和物理的（也见第 11 章）访问控制措施应在一起考虑。用户和服务提供商应被给出一个通过访问控制满足业务要求的清晰说明。

策略应考虑到下列内容：

a）业务应用的安全要求；

b）信息传播和授权的策略，例如，需知（原则）、信息安全级别和信息分类（见 8.2）；

c）系统和网络的访问权利和信息分类策略之间的一致性；

d）关于限制访问数据或服务的相关法律和合同义务（见 18.1）；

e）在识别出各种可用连接类型的分布式和网络环境中的访问权的管理；

f）访问控制角色的分离，例如访问请求、访问授权、访问管理；

g）访问请求正式授权的要求（见 9.2.1 和 9.2.2）；

h）访问权利定期评审的要求（见 9.2.5）；

i）访问权的撤消（见 9.2.6）；

j）涉及用户身份和秘密认证信息使用和管理的所有重大事态的记录存档；

k）特权访问的角色（见 9.2.3）。

其它信息

在规定访问控制规则时，应认真考虑下列内容：

a）建立基于“未经明确允许，一律禁止”前提下的规则，而不是软弱的“未经明确禁止，一律允许”；

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

c）信息系统自动启动的用户许可和管理员启动的用户许的变更；

d）在发布之前，需要专门批准和无须批准的规则。

访问控制规则应有正式的程序支持（见 9.2、9.3、9.4）并定义职责（见 6.1.1、9.3）。

基于访问控制的角色是一个被许多组织将访问权利和业务角色联系在一起的成功使用的方法。

指导访问控制策略的常用的两个原则是：

a) 需知：你只准许访问你执行任务需要的信息（不同的任务/角色意味着不同的需知和今后不同的访问文本属性）；

b) 需用：你只准许访问你执行任务/工作/角色需要的信息处理设施（IT 设备、应用程序、程序、房间）。

9.1.2 网络和网络服务的访问（原 11.4.1）

控制措施

用户应仅被提供已专门授权使用的网络和网络服务。

实施指南

应制定关于网络和网络服务的使用策略。这一策略应包括：

a）允许被访问的网络和网络服务；

b）确定允许谁访问哪些网络和网络服务的授权程序；

c）保护访问网络连接和网络服务的管理控制措施和程序；

d）访问网络和网络服务使用的方法（如，VPN 和无线网络的使用）；

e）访问各种网络服务的用户身份认证要求；

f） 网络服务使用的监视。

网络服务的使用策略应与组织的访问控制策略相一致（见 9.1.1）。

其它信息

未授权和不安全连接到的网络服务可能影响整个组织。这个控制措施对于到敏感或关键业务应用或到高风险场所用户的网络连接是非常的重要，如，组织信息安全管理和控制以外的公共区域或外部区域。

9.2 用户访问管理

目标：确保授权用户访问系统和服务，并防止未授权的访问。

9.2.1 用户注册和注销（原 11.2.1）

控制措施

正式的用户注册和注销过程应被执行，以确保访问权利的分配。

实施指南

管理用户 ID 的过程应包括：

a）使用唯一用户 ID，使得用户与其行为连接起来，并保留其行为的责任；仅当他们的业务或操作原因必需的地方并应经过批准和形成文件后共享 ID 才被允许使用；

b）离开组织的用户的用户 ID 要立即取消或删除；

c）定期地识别、删除或取消多余的用户 ID;

d）确保多余的用户 ID 不会发给其他用户。

其它信息

提供或撤消对信息或信息处理设施的访问通常有两个步骤：

a) 分配、启动或撤消用户 ID；

b) 提供、或撤消这些用户 ID 的访问权利（见 9.2.2）。

9.2.2 用户访问规定（新增）

控制措施

用户 ID 分配或撤消访问权利被准的规定过程应包括：

a) 获得信息系统或服务所有者对信息系统或服务使用的授权（见 8.1.2），访问权利也可以由管理者适当的独立批准；

b) 验证准许访问的级别适于访问策略（见 9.1）且与其它要求（如，职责分离）相一致（见 6.1.2）；

c) 确保访问权利在授权程序完成之前未被激活（如，服务提供商）；

d) 维护一个对访问信息系统或服务的用户 ID 访问权利被准许的核心记录；

e) 对改变了角色或工作的用户访问权利进行改变，或离开组织的用户访问权利进行阻止，并立即删除；

f) 与信息系统或服务（见 9.2.5）的所有者定期评审访问权利。

其它信息

应给出建立基于业务要求的用户访问角色的考虑，总结访问权利到典型用户访问文本属性。基本角色的级别的访问请求和评审比基本特定权利的级别（见 9.2.4）易于管理。

应给出包括个人合同和服务合同的特定的处罚条款，如果个人或承包人试图未授权访问（见 7.1.2，7.1.3，13.2.4，15.1.2）。

9.2.3 特权访问权利的管理（原 11.2.2）

控制措施

特权访问权利的分配和使用应被限制和控制。

实施指南

特权访问权利的分配应被控制，通过一个与相关的访问控制策略（见 9.1.1）一致的正式的授权过程。应考虑下列步骤：

a）特权访问权利与每个系统或过程相关联，如，操作系统、数据库管理系统或每个应用，并且他们需要分配的用户应被识别；

b）特权访问权利应被分配给需用基础上和事态中事态基础上的用户，并与访问控制策略（见 9.1.1）相一致，如，他们的功能角色的最低要求；

c）授权过程和所有特权分配的记录应被维护。特权访问权利应不被准许直到授权过程完成；

d）特权访问权利终止的要求应被定义；

e）特权访问权利应被分配一个不同于正规业务活动使用的用户 ID。正规的业务活动应不能由特权 ID 执行；

f）特权访问权利用户的技能应被定期地评审，为了验证他们是否与他们的职责相一致；

g）特定的程序应被建立和维护，为了避免一般管理用户 ID 被非授权使用，根据系统的配置能力；

h）当共享一般管理用户 ID 的时候，秘密认证信息的保密性应被维护（如，变更口令频率和当特权用户级别或变更工作时，尽早改变口令，在特权用户中用适当的机制传达他们）。

其它信息

系统管理特权的不恰当使用(使用户无视系统或应用控制措施的信息系统的任何特性或设施）可能是导致系统故障或中断的主要促成因素。

9.2.4 用户密码认证信息的管理（原 11.2.3）

控制措施

秘密认证信息的分配应使用正式的管理过程来控制。

实施指南

此过程应包括下列要求：

a）应要求用户签署一份声明，以保证个人秘密认证信息保密性和保持组（如，共享）秘密认证信息仅在该组成员范围内使用；签署的声明可包括在任用条款和条件中（见 7.1.2）；

b）当需要用户维护自己的秘密认证信息的时候，应在初始时提供给他们一个安全的临时秘密认证信息，并在第一次使用时强制其改变；

c）程序应被建立，在提供一个新的、代替的或临时秘密认证信息之前，验证用户身份；

d）临时秘密认证信息应以秘密方式给到用户；外部方的用户或无保护（明文）的电子邮件消息应被避免；

e）临时秘密认证信息对个人应是唯一的，且不可猜测的；

f） 用户应告知已收到秘密认证信息；

g）厂商缺省的秘密认证信息应被改变后才进行系统或软件的安装。

其它信息

口令是通常被使用的秘密认证信息类型，且是验证用户身份的一种通常的方法。秘密认证信息的其它类型是加密密钥和存储在硬件令牌（如 smart cards）上产生身份认证代码的数据。

9.2.5 用户访问权利的评审（原 11.2.4）

控制措施

资产所有者应当定期审查用户的访问权利。

实施指南

访问权利的评审应考虑如下：

a) 用户访问权利应在规定的时间间隔或任何变更之后被评审；如，升职、降级或雇用终止（见 7）；

b) 用户访问权利应在组织内换岗时被评审并重新分配；

c) 特权访问权利的授权应在更频繁的时间间隔内被评审；

d) 特权分配应定期被检查，以确保不能获得未授权的特殊权限；

e) 特权帐号的变更应在定期评审时被记录。

其它信息

这个控制措施补偿了在 9.2.1、9.2.2 和 9.2.6 控制措施执行的可能的弱点。

9.2.6 访问权利的删除或调整（原 8.3.3）

控制措施

当任用、合同或协议终止时或调整变更时，应删除或调整所有雇员和外部团体用户对信息和信息处理设施的访问权利。

实施指南

一旦终止，个人对信息和与信息处理设施关联的资产或服务的访问权利应被终止或暂停。这将决定是否必须删除访问权利。任用的变化应体现在新的雇用不被批准的所有访问权利的删除。访问权利应被删除或调整包括物理和逻辑访问。删除或调整能被完成由密钥、身体认证卡、信息处理设施或订阅的删除、撤回或复位。标识雇员或承包人访问权利的任何文档应被体现在访问权利的删除或调整上。如果一个离开的雇员或外部团体用户已知用户 ID 的口令保留在活动状态，则应在任用、合同或协议终止或变化时改变密码。

信息和信息处理设施相关的资产的访问权利在雇用终止或变化之前应被减小或删除，依赖于对风险因素的评价，如：

a) 是否由雇员、外部团体用户或管理者发起的终止或变更，以及终止的原因；

b) 雇员、外部团体用户或任何其他用户的现有职责；

c) 当前可访问资产的价值。

其它信息

在某些情况下，访问权利的分配基于对多人可用而不是只是雇员、外部团体用户的离开，如，组 ID。在这种情况下，来自任何组访问列表中个人离开应被删除，并通知所有其它雇员和外部团体用户涉及不应再与离开的个人共享这些信息。

在管理者发起终止的情况中，不满的雇员或外部团体用户可能故意破坏信息或破坏信息处理设施。在个人辞职或被免职的情况下，他们可能冒险收集信息以便将来使用。

9.3 用户职责

目标：使用户对保护他们的身份认证信息负起责任

9.3.1 秘密认证信息的使用（原 11.3.1）

控制措施

用户应被要求遵循组织使用秘密认证信息的实践。

实施指南

所有用户应被告知：

a）保持秘密身份认证信息的保密性，确保不被泄漏给任何其它团体，包括权威人士；

b）避免保留秘密身份认证信息的记录（如，在纸上、软件文件中或手持设备中），除非可以对其进行安全地存储及存储方法得到批准（如，密码保管室）；

c）每当有任何迹象表明受到损害时就变更秘密身份认证信息；

d）当口令作为秘密身份认证信息使用的时候，选择足够的最小长度的优质口令：

1）易于记忆；

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

3）不容易遭受字典攻击（如，不是由字典中的词所组成的）；

4）避免连续相同的，全数字的或全字母的字符；

5）如果是临时的，第一次使用要变更。

e）不共享个人用户的秘密身份认证信息；

f）确保适当的口令保护，当在自动开始工作程序中并被存储的口令被使用作为秘密身份认证信息的时候；

g）在业务目的和非业务目的中不使用相同的秘密身份认证信息。

其它信息

单点登录（SSO）或其它秘密身份认证信息管理工具的规定，减小了用户被要求保护的秘密身份认证信息的数量，因而能增加这个控制措施的有效性。无论如何，这些工具也能增加泄漏秘密身份认证信息的影响。

9.4 系统和应用的访问控制

目标：防止对系统和应用的的未授权访问。

9.4.1 信息访问限制（原 11.6.1）

控制措施

信息和应用系统功能的访问应依据访问控制策略来限制。

实施指南

对访问的限制应基于单个业务应用要求并与被定义的访问控制策略一致。

为支持访问限制要求，应考虑应用以下指南：

a）提供菜单来控制访问到的应用系统功能；

b）由特别用户访问的数据的控制；

c）用户访问权利的控制，如，读、写、删除和执行；

d）其他应用的访问权利的控制；

e）包含在输出中信息的限制；

f）提供物理或逻辑访问控制，为敏感应用、应用数据或系统的隔离。

9.4.2 安全登录程序（原 11.5.1）

控制措施

如果访问控制策略需要，应通过安全登录程序控制对操作系统和应用的访问。

实施指南

适当的身份认证技术应被选择，来支持用户身份的要求。

强壮的认证和身份验证被要求的地方，可供选择用口令作为认证方法，如，加密方法、智能卡、令牌或造物方法等应被使用。

登录到系统或应用的程序应被设计，以最小化非授权访问的机会。登录程序因此应公开最小的系统或应用的信息，以避免给非授权用户提供一个任何不必要的帮助。好的登录程序应：

a）不显示系统或应用标识符，直到登录过程已成功完成为止；

b）显示只有已授权的用户才能访问计算机的一般性的告警通知；

c）在登录过程中，不提供对未授权用户有帮助的消息；

d）仅在所有输入数据完成时才验证登录信息。如果出现差错情况，系统不应提示数据部分是正确的或不正确的；

e）保护防止强力登录尝试；

f）记录不成功的尝试和成功的尝试；

g）升级一个安全事态，如果一个潜在的企图或登录控制成功的突破被检测；

h）成功登录完成时显示下列信息：

1）成功登录前的日期和时间；

2）从最后成功登录以来，任何不成功登录企图的细节；

i）不显示被输入的口令；

j）不通过网络以明文传输口令；

k）在被定义不活跃时期后终止不活跃的会话，尤其在高风险场所，如公共区域或组织的安全管理的外部区域或移动设备；

l）限制连接次数以为高风险应用提供附加安全，并减少非授权访问机会的窗口。

其它信息

口令是提供识别和认证的一个通用的方法，基于只有用户知道的秘密。用加密方法和认证协议同样能够实现。用户认证的强度应适合于被访问信息的分类。

如果口令通过网络在登录会话期间以明文传输，它们可能被网络“嗅探器”程序捕获。

9.4.3 口令管理系统（原 11.5.3）

控制措施

口令管理系统应是交互式的，并确保口令质量。

实施指南

一个口令管理系统应：

a）强制使用个人用户 ID 和口令，以保持责任性；

b）允许用户选择和变更他们自己的口令，并且包括一个允许输入出错的确认程序；

c）强制选择优质口令；

d）第一次登录时强制用户变更他们的口令；

e）强制定期改变口令，并作为必需的；

f）维护以前使用口令的记录，并防止重复使用；

g）在输入口令时，不在屏幕上显示；

h）口令文件和应用系统数据分开存储；

i）以保护的形式存储和传输口令。

其它信息

某些应用要求用户口令由独立的权威来分配；这种情况下，以上指导 b）、d）和 e）

不会采用。大多数情况下，口令由用户选择和维护。

9.4.4 特权实用程序的使用（原 11.5.4）

控制措施

实用程序的使用，可能推翻系统和应用程序控制，应被限制并严格控制。

实施指南

可能推翻系统和应用控制的实用程序的使用，就考虑下列指南：

a）对实用工具使用标识、认证和授权程序；

b）实用程序和应用软件分开；

c）实用程序的使用限制到可信、已授权的最小实际用户数（也见 9.2.3）；

d）实用程序使用的特别授权；

e）限制实用程序的可用性，如，在授权变更期间；

f） 记录实用程序的所有使用；

g）对实用程序的授权级别进行定义并形成文件；

h）删除或禁用所有不必要的实用程序；

i） 要求责任分割地方，访问系统中应用程序的用户不能使用实用程序。

其它信息

大多数计算机安装有一个或多个可能推翻系统和应用控制的实用程序。

9.4.5 程序源码的访问控制（原 12.4.3）

控制措施

对程序源代码的访问应被限制。

实施指南

对程序源代码和相关事项（诸如设计、说明书、验证计划和确认计划）的访问应被严格控制，以防引入非授权功能和避免无意识的变更，同时也维护有价值的知识产权的机密性。对于程序源代码，可以通过这种代码的中央存储控制来获得，更好的在程序源库中。为了控制对程序源码库的访问以减少潜在的计算机程序的破坏，应考虑下列指南：

a) 若有可能，程序源库不应保留在运行系统中；

b) 程序源代码和源程序库应根据制定的程序进行管理；

c) 支持人员不应有无限制访问程序源库；

d) 程序库源的更新和有关事项，向程序员发布程序源仅应在适当的授权被接收之后进行；

e) 程序列表应保存在安全的环境中；

f) 所有访问到程序源库的审计日志应被维护；

g) 程序源库的维护和拷贝应受服从严格的变更控制程序（见 14.2.2）。

如果程序源代码被有意公布，应考虑另外的控制措施以帮助保证它的完整性（如，数字签名）。

10 密码学

10.1 密码控制

目标：确保适当有效的密码学的使用以保护信息的机密性、真实性和/或完整性。

10.1.1 密码控制使用政策（原 12.3.1）

控制措施

应开发和实施用于保护信息的密码控制的使用策略。

实施指南

制定密码策略时，应考虑下列内容：

a) 组织间对于密码控制的使用的管理方法，包括业务信息保护下的一般原则；
b) 基于风险评估，应确定需要的保护级别，并考虑需要的加密算法的类型、强度和质量；
c) 使用加密保护通过移动电话、可移动介质设备或者通过通信线路传输的信息；
d) 密钥管理方法，包括应对加密密钥的保护方法和在密钥丢失、损坏或毁坏后加密信息的恢复方法；
e) 角色和职责，如，谁负责：
   1）策略的实施；
   2）密钥管理，包括密钥生成（参见 10.1.2）；
f) 为在整个组织内有效实施而采用的标准（哪种解决方案用于哪些业务过程）；
g) 使用加密信息对控制措施的影响依赖于内容检查（例如病毒检测）。

当实施组织的密码策略时，应考虑世界不同地区应用密码技术的规定和国家限制，和加密信息跨越国界时的问题（见 18.1.5）。

可以使用密码控制措施实现不同的安全目标，如：

a) 保密性：使用信息加密以保护存储或传输中的敏感或关键信息；
b) 完整性/真实性：使用数字签名和消息鉴别码以验证存储和传输中的敏感或关键信息的真实性和完整性；
c) 不可否认性：使用密码技术获得一个事件或行为发生或未发生的证据；
d) 身份认证：使用密码技术以验证用户和要求访问到或与系统用户、实体和资源交易的其它系统实体。

其它信息

有关一个密码解决方案是否合适的决策，应被看作一般的风险评估过程和选择控制措施的一部分。该评估可以用来判定一个密码控制措施是否合适，应运用什么类型的控制措施以及应用于什么目的和业务过程。

使用密码控制措施的策略对于使利益最大化，使利用密码技术的风险最小化，以及避

免不合适或不正确的使用。

而言，十分必要。在使用数字签名时，应考虑任何相关的法律，特别是规定什么条件下数字签名被合法绑定的法律（参见 15.1）。

应征求专家建议以选择合适的加密控制措施，以满足信息安全方针目标。

10.1.2 密钥管理（原 12.3.2）

控制措施

应开发和实施加密密钥的使用、保护和有效期的策略，贯穿他们的整个生命周期。

实施指南

策略应包括贯穿整个生命周期的加密密钥的管理要求，包括产生、存储、存档、恢复、分发和销毁密钥。

加密算法、密钥长度和实际用法应依据最佳实践来选择，适当的密钥管理要求保护过程为产生、存储、存档、恢复、分发和销毁加密密钥。

所有加密密钥应被保护防止修改和丢失。另外，秘密的和私有的密钥需要保护防止非授权使用和公开。用来生成、存储和归档密钥的设备应进行物理保护。

密钥管理系统应基于已商定的标准、程序和安全方法，以便：

a) 生成用于不同加密系统和不同应用的密钥；
b) 生成和获得公开密钥证书；
c) 分发密钥给预期实体，包括在收到密钥时应如何激活；
d) 存储密钥，包括已授权用户如何访问密钥；
e) 变更或更新密钥，包括应何时变更密钥和如何变更密钥的规则；
f) 处理已损害的密钥；
g) 撤销密钥，包括应如何撤消或解除密钥，例如，当密钥已损害时或当用户离开组织时（在这种情况下，密钥也要归档）；
h) 恢复已丢失或损坏的密钥；
i) 备份或归档密钥；
j) 销毁密钥；
k) 记录和审计与密钥管理相关的活动。

为了减少可能的不正确的使用，应规定密钥的激活日期和解除激活日期，以使它们只能用于与密钥管理策略关联的有限的时间段。

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

与外部加密服务提供者（例如与认证机构）签订的服务级协议或合同的内容，应涵盖服务责任、服务可靠性和服务规定的响应次数等（见 15.2）。

其它信息

加密密钥的管理对有效使用密码技术来说是必需的。ISO/IEC 11770 提供了更多密钥管理的信息。

加密技术还可以用来保护加密密钥。可能必须考虑处理访问加密密钥的法律要求，例如，加密的信息可能需要以未加密的形式提供，以作为法庭案例的证据。

11 物理和环境安全

11.1 安全区域

目标：防止对组织的信息和信息处理设施的未授权物理访问、损坏和干扰。

11.1.1 物理安全边界（原 9.1.1）

控制措施

安全边界应被定义，来保护包含敏感信息、关键信息和信息处理设施的区域。

实施指南

对于物理安全边界，若合适，下列指南应予以考虑和实施：

a) 安全边界应被定义，各个边界的设置地点和强度取决于边界内资产的安全要求和风险评估的结果；

b) 包含信息处理设施的建筑物或场地的边界应在物理上是安全的（即，在边界或区域内不应存在可能易于闯入的任何缺口）；场所的外部屋顶、墙和地板应是坚固结构，所有外部的门要使用控制机制来适当保护，以防止未授权进入，（如，门闩、报警器、锁）；无人看管的门和窗户应上锁，还要考虑窗户的外部保护，尤其是地面一层的窗户；

c) 对场所或建筑物的物理访问应安置有人接待区或其他控制方法来控制；进入场所或建筑物应仅限于已授权人员；

d) 如果可行，应建立物理屏障以防止未授权进入和环境污染；

e) 安全边界的所有防火门应可发出报警、被监视并被检验，和墙一起按照合适的地方、国家和国际标准建立所需的抗力级别；他们应以一种安全的方式按照当地防火规范来运行。

f) 应按照地方、国家和国际标准建立适当的入侵检测系统，并定期检测以覆盖所有的对外的门和易接近的窗；要一直警惕空闲区域；其他区域要提供掩护方法，例如计算机室或通信室；

g) 组织管理的信息处理设施应在物理上与外部团体管理的设施分开。

其它信息

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

一个安全区域可以是一个可上锁的办公室，或是被连续的内部物理安全屏障包围的几

个房间。在安全边界内具有不同安全要求的区域之间需要控制物理访问附加屏障和边界。特别注意物理访问安全应给出多组织对建筑物资产的所有权的情况。

物理控制的应用，尤其安全区域，应适应于组织的技术、经济环境和风险评估的规定。

11.1.2 物理入口控制（原 9.1.2）

控制措施

安全区域应由适合的入口控制所保护，以确保只有授权的人员才允许访问。

实施指南

下列指南应予以考虑：

a) 记录访问者进入和离开的日期和时间，所有的访问者要予以监督，除非他们的访问事前已经经过批准；只能允许他们访问特定的、已授权的目标，并要向他们宣布关于该区域的安全要求和应急程序的说明。访问者的身份应由合适的方法进行验证。

b) 访问处理或储存保密信息的区域要受到限制，并且仅限于已执行了合适的访问控制措施后的授权人员，如，执行了一个双因素身份认证机制，一个访问卡和 PIN 密码。

c) 所有访问的物理记录簿或电子审计追踪应被安全的维护和监视；

d) 所有雇员、承包方人员和外部团体人员应被要求穿着一些可视标识的衣物，如果遇到无人陪同的访问者和未佩带可视标识的任何人应立即通知安全人员。

e) 外部团体支持服务人员只有在需要时才能有限制的访问安全区域或秘密信息处理设施；这种访问应被授权并受监视；

f) 对安全区域的访问权要定期地予以评审和更新，并在需要时废除（见 9.2.5 和 9.2.6）。

11.1.3 办公室、房间和设施的安全保护（原 9.1.3）

控制措施

办公室、房间和设施的物理安全应被设计并实施。

实施指南

应考虑下列指南以保护办公室、房间和设施：

a) 关键设施应坐落在可避免公众进行访问的场地；

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

c) 设施应被配置，以预防保密信息或活动被从外面看到或听到。电磁屏蔽也被考虑作为适当的选择；

d) 标识保密信息处理设施的位置的目录和内部电话簿不要轻易被非授权人员得到。

11.1.4 外部和环境威胁的安全防护（原 9.1.4）

控制措施

应设计并采取物理安全措施来防范自然灾害、恶意攻击或事故。

实施指南

如何避免火灾、洪水、地震、爆炸、市民动荡和其它自然或人为灾难的专家建议应被获得。

11.1.5 在安全区域工作（原 9.1.5）

控制措施

在安全区域工作的程序应被设计和运用。

实施指南

下列指南应予以考虑：

a） 只有必须知道的基础上，员工才应知道安全区域的存在或其中的活动；

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

c） 未使用的安全区域在物理上要上锁并周期地予以检查；

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

在安全区域工作的安排包括对工作在安全区域内的雇员、外部团体用户的控制，并涵盖他们在安全区域发生的所有活动的控制。

11.1.6 交接区（原 9.1.6）

控制措施

诸如交接区和未经授权人员可能进行房屋的其它点的访问点应被控制，如果可能，隔离信息处理设施，以避免未授权访问。

实施指南

下列指南应予以考虑：

a） 由建筑物外进入交接区的访问应局限于已标识的和已授权的人员；

b） 交接区应设计，以至于物品能被装卸而无需交付人员访问建筑物的其他部分；

c） 当内部的门打开时，交接区的外部门应得到安全保护；

d） 在进来的物资从交接区运到使用地点之前，应被检查并检验爆炸物、化学药品或其它的危险材料；

e） 进来的物资应按照资产管理程序（见 8）在场所的入口处进行登记；

f） 如果可能，进入和外出的货物应在物理上予以隔离；

g） 进料应被检查途中被篡改的证据。如果这些篡改被发现应立即报告给安全人员。

11.2 设备

目标：防止资产的丢失、损坏、失窃或损害和组织的支行的中断。

11.2.1 设备安放和保护（原 9.2.1）

控制措施

应妥善安放或保护设备，以减少来自环境威胁、危害以及未授权访问的机会。

实施指南

下列指南应予以考虑以保护设备：

a) 设备应被安放，以尽量减少不必要的在工作区域的访问；

b) 处理敏感数据的信息处理设施应被仔细地放到适当的位置，以减少非授权人员在使用期间窥视到信息的风险；

c) 存储设施应被保护，避免非授权访问；

d) 要求专门保护的部件要被保护，以降低所要求的一般保护等级；

e) 控制措施应被采用，以减小潜在的物理和环境威胁的风险，如，偷窃、火灾、爆炸、烟雾、水（或供水故障）、尘埃、振动、化学影响、电源干扰、通信干扰、电磁辐射和故意破坏；

f) 应建立在信息处理设施附近进食、喝饮料和抽烟的指南；

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

h) 防雷保护应被应用于所有建筑，防雷保护过滤器应被安装在所有进入的电源和通信线路；

i) 对于工业环境中的设备，要考虑使用专门的保护方法，例如键盘保护膜；

j) 处理保密信息的设备应被保护，以减少由于电磁辐射而导致信息泄露的风险；

11.2.2 配套设施（原 9.2.2）

控制措施

应保护设备使其免于由配套设施的失效而引起的电源故障和其他中断。

实施指南

配套设施（如电力、通讯、供水、气体、排污、通风和空调）应：

a) 符合设备制造商的规格说明和本地法律要求；

b) 定期评价满足业务增长的容量和其它配套设施的相互影响；

c) 定期的检查和测试以确保它们的正常功能；

d) 如果需要，检测到的故障被告警；

e) 如果需要，注入多条物理布线。

紧急照明和通讯设施应被提供。切断电源、水、气体或其它的设施的紧急转换开关，应被安放在紧急出口附近或设备间。

其它信息

网络连接的附加冗余应由多个提供商的多路由的方式获得。

11.2.3 布缆安全（原 9.2.3）

控制措施

传输数据或支持信息服务的电力及通信布缆应被保护，免遭拦截、干扰或破坏。

实施指南

布缆安全的下列指南应予以考虑：

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

b) 为了防止干扰，电源电缆要与通信电缆分开；

c) 对于敏感的或关键的系统，更进一步的控制考虑应包括：

1）在检查点和终结点安装导管和上锁的房间或盒子；

2）使用电磁防辐射装置保护电缆；

3）对于电缆连接的未授权装置要主动实施技术清除和物理检查；

4）控制对配线盘和电缆室的访问；

11.2.4 设备维护（原 9.2.4）

控制措施

设备应予以正确地维护，以确保其持续的可用性和完整性。

实施指南

设备维护的下列指南应予以考虑：

a) 要按照供应商推荐的服务时间间隔和规范对设备进行维护；

b) 只有已授权的维护人员才可对设备进行修理和服务；

c) 要保存所有可疑的或实际的故障以及所有预防和纠正维护的记录；

d) 当对设备安排维护时，应实施适当的控制措施，要考虑维护是由场所内部人员执行还是由外部人员执行；当需要时，保密信息需要从设备中删除或者维护人员应该是足够可靠的；

e) 应遵守由保险策略所施加的所有要求；

f) 对设备维护之后，将设备放回运行环境之前，它应被检查，确保设备没被损坏并没有故障。

11.2.5 资产的移动（原 9.2.7）

控制措施

设备、信息或软件在授权之前不应带出组织场所。

实施指南

下列指南应予以考虑：

a) 雇员和外部团体用户在授权之后，允许将资产带离场所，并应被标识；

b) 应设置设备移动的时间限制，并在返还时执行符合性检查；

c) 若需要并合适，要对设备作出移出记录和返回记录；

d) 处理和使用资产的任何人的身份、角色和隶属关系应被文档化，且这个文档与设备、信息或软件一直归还。

其它信息

现场检查、保证检测未授权资产的移动，也能被执行来检测非授权记录装置、武器等等，防止他们进入和出去办公场所。这样的现场检查应按照相关法律法规执行。应让每个人都知道将进行现场检查，并且只能在法律法规要求的适当授权下执行证实。

11.2.6 场外设备和资产安全（原 9.2.5）

控制措施

应对组织场所的设备采取安全措施，要考虑工作在组织场所以外的不同风险。

实施指南

组织场所外的任何信息存储和处理设备的使用，应由管理者授权。这个应用于组织拥有的设备和被使用于组织支持的私人拥有的设备。

离开办公场所的设备的保护应考虑下列指南：

a）离开建筑物的设备和介质在公共场所不应无人看管。

b）制造商的设备保护说明要始终加以遵守，例如，防止暴露于强电磁场内；

c）离开场所边界的控制措施应被确定，如家庭工作、遥控工作、临时场所，通过实施风险评估和适当的控制措施，如，封闭文档柜、清理桌面策略、计算机访问控制和与办公室安全通讯（见 ISO/IEC 27033）；

d）当离开场所的设备被转移到不同的个人或外部团体时，应维护定义一个设备的监管链且至少包括那些负责设备的组织和人名的日志。

安全风险在不同场所可能有显著不同，例如，损坏、盗窃和截取，要考虑确定最合适的控制措施。

其它信息

用于家庭工作或从正常工作地点运走的信息存储和处理设备包括所有形式的个人计算机、备忘记事簿、移动电话、智能卡、纸张及其他形式的设备。

关于保护移动设备的其他方面的更多信息在 6.2 中可以找到。

可以适当的避免风险，由阻止某个雇员离开办公场所或限制他们使用便携式 IT 设备；

11.2.7 设备的安全处置和再利用（原 9.2.6）

控制措施

包含储存介质设备的所有部件应被检查，以确保在处置或再利用之前，任何敏感信息和许可软件已被删除或安全重写。

实施指南

设备应被检查以确保在处置或重利用之前，是否或没有存储介质被包含。

包含保密或版权信息的存储介质应被物理破坏或信息应采用使原始信息不可获取的技术来破坏、删除或重写，而不是使用标准删除或格式化功能。

其它信息

包含敏感信息的已损坏的设备可能需要实施风险评估，以确定这些部件是否要进行销

毁、而不是送去修理或丢弃。信息可能被损害通过粗心地处置或再利用设备。

除磁盘安全擦除之外，全部磁盘加密以减小保密信息的泄漏风险，当设备被处置或再利用时，假如：

a) 加密过程足够强壮并包括整个磁盘（包括不活跃的空间、替代文件等）；

b) 加密密钥足够长以抵抗强力破解；

c) 加密密钥自己保持秘密（如，从不存储在相同的磁盘）。

更多的密码学建议（见 10）。

安全重写存储介质的技术随存储介质技术不同而不同。重写工具应被检查确保它们是存储介质适合的技术。

11.2.8 无人值守的用户设备（原 11.3.2）

控制措施

用户应确保无人值守的用户设备有适当的保护。

实施指南

所有用户应了解保护无人值守的设备的安全要求和程序，以及他们对实现这种保护所负有的职责。建议用户应：

a）结束时终止活动的会话，除非采用一种合适的锁定机制保证其安全，如，有口令保护的屏幕保护程序；

b）当不再需要时，应从应用或网络服务注销；

c）当不使用设备时，用带钥匙的锁或与之效果等同的控制措施来保护计算机或移动设备免遭未授权使用，例如，口令访问。

11.2.9 清除桌面和清除屏幕策略（原 11.3.3）

控制措施

应采用清除桌面上纸张、可移动存储介质策略和清除信息处理设施屏幕策略。

实施指南

清除桌面和清除屏幕策略应考虑信息分类（见 8.2）、法律和合同要求（见 18.1）、相应风险和组织的文化方面。下列指南应予以考虑：

a）当不需要时，特别是当空出办公室时，应将敏感或关键业务信息（如在纸质或电子存储介质上的）锁起来（理想情况下，在保险柜或保险箱或其他形式的安全设备中）；

b） 当无人值守时，计算机和终端应注销、或使用屏幕和由口令、令牌或类似于用户身份认证合机制控制的键盘机制保护；当不使用时，应使用带钥匙的锁、口令或其他控制措施进行保护；

c）应防止复印机或其他复制技术（例如扫描仪、数字照相机）的未授权使用；

d） 包含敏感或机密信息的介质应立即从打印机中清除。

其它信息

清除桌面/清除屏幕策略降低了正常工作时间之中和之外对信息的未授权访问、丢失、破坏的风险。保险箱或其他形式的安全存储设施也可保护存储于其中的信息免受灾难（例如火灾、地震、洪水或爆炸）的影响。

要考虑使用带 PIN 码功能的打印机，使得原始操作人员仅当站在打印机旁边的时候是，才能获得打印的输出。

12 操作安全

12.1 操作程序和职责

目标：确保正确、安全的信息处理设施运行。

12.1.1 文件化的操作程序（原 10.1.1）

控制措施

运行程序应形成文件、并对所有需要的用户。

实施指南

应为与信息处理和通信设施相关的操作活动准备形成文件的程序，例如计算机启动和关机程序、备份、设备维护、介质处理、计算机机房、邮件处置管理和安全设备等。

运行程序应详述操作指南，包括：

a） 系统的安装和配置；

b） 自动和手动加工和处理信息；

c） 备份（见 12.3）；

d） 规划要求，包括与其他系统的相互关系、最早工作开始时间和最后工作完成时间；

e） 在工作执行期间处理错误或其它的异常条件的操作指南，包括对系统工具的使用限制（见 9.4.4）；

f） 支持和升级联系，包括出现非预期操作或技术难题时的外部支持联系；

g） 特定输出及介质处理的指作指南，诸如特殊文具的使用或保密输出的管理，包括任务失败时输出的安全处置程序（见 8.3 和 11.2.7）；

h） 系统失败事件使用的系统重启和恢复程序；

i） 审计跟踪和系统日志信息的管理（见 12.4）；

j） 监视程序。

操作程序和系统活动的文档化程序应作为正式的文件处理，其变更由管理者授权。技术上可行时，信息系统应使用相同的程序、工具和工具软件进行一贯的管理。

12.1.2 变更管理（原 10.1.2）

控制措施

对影响信息安全的组织、业务流程、信息处理设施和系统的变更应加以控制。

实施指南

特别的，下列条款应予以考虑。

a）重大变更的识别和记录；

b）变更的策划和测试；

c）对这种变更的潜在影响的评估，包括信息安全影响；

d）对建议变更的正式批准程序；

e）验证信息安全要求已被满足；

f）向所有有关人员传达变更细节；

g）回退程序，包括从不成功变更和未预料事件中中止和恢复的程序与职责；

h）紧急变更处理的规定使需要恢复事件的变更能快速且在受控下完成。

正式的管理职责和程序应是适当的，以确保所有的变更的的控制。当发生变更时，包含所有相关信息的审计日志要予以保留。

其它信息

对信息处理设施和系统的变更缺乏控制是系统或安全故障的常见原因。对运行环境的变更，特别是当系统从开发阶段向运行阶段转移时，可能影响应用程序的可靠性。（见14.2.2）。

12.1.3 容量管理（原 10.3.1）

控制措施

资源的使用应加以监视、调整，并应作出对于未来容量要求的预测，以确保拥有所需的系统性能。

实施指南

关注有关系统的业务临界状态，应识别容量要求。应使用系统调整和监视确保必需提高的系统可用性和效率。应有检测控制措施以及时地指示问题。未来容量要求的预测应考虑新业务和系统的要求以及组织信息处理容量的当前和预期的趋势。

需要特别关注长订货交货周期或高成本相关的所有资源；因此管理者应监视关键系统资源的使用。他们应识别出使用的趋势，特别是有关业务应用或信息系统管理工具。

管理者应使用这些信息来识别和避免潜在的瓶颈及对关键员工的依赖，他们可能引起对系统安全或服务的威胁，并策划适当的行动。

提供足够的容量可以由增加容量或降低需求来获得。管理容量需求的例子包括：

a) 废弃数据的删除（磁盘空间）；

b) 应用、系统、数据库或环境的退役；

c) 优化批处理和进度；

d) 优化应用逻辑或数据库队列；

e) 拒绝或限制渴求资源的带宽，如果这些不是关键业务（如，视频流）。

应考虑关键任务系统的文档化的容量管理计划。

其它信息

这个控制措施也处理人力资源、办公室和设备的容量，

12.1.4 开发、测试和运行环境分离（原 10.1.4）

控制措施

开发、测试和运行环境应被分离，以减少未授权访问或对运行环境变更的风险。

实施指南

为防止操作的问题，运行、测试和开发环境之间的的分离级别应被识别并实施是必须的。

下列条款应加以考虑：

a) 软件从开发转移到运行状态的规则应被定义并形成文件；
b) 开发和运行应运行在不同的系统或计算机处理器上，且在不同的域或目录内；
c) 运行系统和应用的变更应在应用到运行系统之前，在测试或升级环境中进行测试；
d) 除特殊例外情况，测试不应在运行系统上完成；
e) 编译器、编辑器、其他开发工具或系统工具如果没有要求，不应从运行系统中访问到；
f) 用户应在运行和测试系统中使用不同的用户档案文件，菜单要显示合适的标识消息以减少出错的风险；
g) 敏感数据不应拷贝到测试系统环境中，除非为测试环境提供等效的控制措施（见 14.3）。

其它信息

开发和测试活动可能引起严重的问题，例如，文件或系统环境的不需要的修改或者系统故障。有必要保持一种已知的和稳定的环境，来执行有意义的测试并防止不适当的开发者访问到运行环境。

若开发和测试人员访问运行系统及其信息，那么他们可能会引入未授权和未测试的代码或改变运行数据。在某些系统中，这种能力可能被误用于实施欺诈，或引入未测试的或恶意代码，从而导致严重的运行问题。

开发者和测试者还造成对运行信息保密性的威胁。如果开发和测试活动共享相同的计算环境，那么可能引起非故意的软件和信息的变更。因此，为了减少意外变更或未授权访问运行软件和业务数据的风险，分离开发、测试和运行环境是有必要的（见 14.3 的测试数据保护）。

12.2 恶意软件防护

目标：确保信息和信息处理设施不受恶意软件侵害。

12.2.1 控制恶意软件（原 10.4.1）

控制措施

与适当的用户意识相结合，实施检测、预防和恢复控制措施来防范恶意软件。

实施指南

防范恶意代码要基于恶意代码监测、修复软件、信息安全意识、适当的系统访问和变更管理控制。下列指南要加以考虑：

a）建立禁止使用未授权软件的正式策略（见 12.6.2 和 14.2）；

b）实施控制措施预防和检测未授权软件的使用（如，应用程序白名单）；

c）实施控制措施预防和检测已知或可疑恶意代码网络的使用（如，黑名单）；

d）建立防范风险的正式策略，该风险与来自或经由外部网络或在其他介质上获得的文件和软件相关，此策略指示应采取什么保护措施；

e）减少可能被恶意代码利用的脆弱性，如，通过技术脆弱性管理（见 12.6）；

f）对支持关键业务过程的系统中的软件和数据内容进行定期评审。应正式审查存在的任何未批准的文件或未授权的修改；

g）安装和定期更新恶意代码检测和修复软件来扫描计算机和介质，以作为预防控制或作为例行程序的基础；执行的扫描应包括：

1）恶意代码使用前，扫描从网络上接收到的任何文件或通过任何存储介质的格式；

2）恶意代码使用前，扫描电子邮件附件和下载内容；该扫描应被执行在不同地方，如，在电子邮件服务器、台式计算机和进入组织的网络时；

3）针对恶意代码，扫描 web 页面；

h）　定义程序和职责，以处理在系统上防护恶意代码、对他们使用的培训、恶意代码攻击报告和恢复；

i）制定适当的从恶意代码攻击中恢复的业务连续性计划，包括所有必要数据和软件备份以及恢复安排（见 12.3）；

j）实施程序定期收集信息，如，订阅邮件列表或检查提供新恶意代码信息的 web 站点；

k）实施检验与恶意代码相关信息的程序，并确保警告公告是准确和翔实的；管理者应确保使用合格的来源，如，声誉好的期刊、可靠的 Internet 网站或防范恶意代码软件的供应商，被用来区分虚假的和真实的；要让所有用户了解欺骗问题，以及在收到它们时要做什么。

l）孤立的环境，可能导致灾难性的影响。

其它信息

在信息处理环境中使用来自不同供应商和技术的防范恶意代码的两个或多个软件产品，能改进恶意代码防护的有效性。

应注意防止在实施维护和紧急程序期间引入恶意代码，这将避开正常的恶意代码防护的控制措施。

某种情况下，恶意代码防护可能导致运行中的干扰。

恶意代码检测和修复软件的使用独立的作为一个恶意代码控制措施，通常是不胜任的，一般需要伴有预防恶意代码介绍的运行程序。

12.3 备份

目标：防止数据丢失。

12.3.1 信息备份（原 10.5.1）

控制措施

根据既定的备份策略备份信息、软件和系统映象的拷贝，并定期测试。

实施指南

应建立备份策略来定义组织对信息、软件和系统备份的要求。

备份策略应定义保留和保护要求。

应提供足够的备份设施，以确保所有基本信息和软件能在灾难或介质失效后进行恢复。

当设计备份计划时，下列条款应加以考虑：

a） 精确的和完整的备份拷贝的记录和文档化恢复程序应被产生；

b） 备份的程度（如，全备份或差异备份）和频率应考虑组织的业务要求、涉及信息的安全要求和组织连续运行信息的临界状态；

c） 备份应被存储在远端场所，这个场所应保持足够的距离以避免因主场所发生灾难而对备份造成的任何损害；

d） 应给予备份信息一个与主办公场所应用标准相一致的适当的物理和环境保护等级（见 11）；

e） 必要时，定期地测试备份介质，确保当需要应急使用时可以依靠这些备份介质；这应与恢复程序结合并检查对恢复所需要的时间。测试恢复备份数据的能力应被执行，映射到专用的测试介质，不是重写原始介质，避免备份或恢复过程失败而导致不可修复的数据损坏或丢失；

f） 在保密性十分重要的情况下，备份应通过加密方法进行保护。

运行程序应监视备份的执行和预定备份的故障处理，以确保备份根据备份策略来完成。

各个系统和服务的备份安排应定期测试，以确保他们满足业务连续性计划的要求。对于关键系统和服务，备份安排覆盖在发生灾难时恢复整个系统所必需的所有系统信息、应用和数据。

基本业务信息的保存期应被确定，考虑对永久保存的存档拷贝的任何要求。

12.4 日志和监控

目标：记录事态并生成证据。

12.4.1 **事态日志（原 10.10.1）**

控制措施

事态日志记录用户活动、例外、故障和信息安全事态，应被产生、保持和定期评审。

实施指南

当相关联的时候，事态日志应包括：

a） 用户 ID；

b） 系统活动；

c） 日期、时间和关键事态的细节，例如注册和注销；

d） 若有可能，设备身份或位置，以及系统标识；

e） 成功的和被拒绝的对系统尝试访问的记录；

f） 成功的和被拒绝的对数据以及其他资源尝试访问的记录；

g） 系统配置的变化；

h） 特权的使用；

i） 系统工具和应用程序的使用；

j） 访问的文件和访问类型；

k） 网络地址和协议；

l） 访问控制系统引发的报报警；

m） 防护系统的激活和停用，如，防病毒系统和入侵检测系统；

n） 用户在应用上执行的交易记录。

事态日志安置基本的自动监视系统，在系统安全上能产生统一的报告和告警。

其它信息

事态日志可以包含敏感数据和个人可识别的信息。应采取适当的隐私保护措施（见 18.1.4）。

可能时，系统管理员不允许删除或停用他们自己活动日志。

12.4.2 **日志信息的保护（原 10.10.3）**

控制措施

日志设施和日志信息应加以保护，以防止篡改和未授权的访问。

实施指南

应实施控制措施以防止日志信息被未授权更改和与日志设施有关的操作问题，包括：

a) 更改已记录的消息类型；

b) 日志文件被编辑或删除；

c) 超越日志文件介质的存储容量，导致不能记录事态的故障或过去记录事态被覆盖。

一些审计日志可能需要被存档，以作为记录保留策略的一部分，或由于收集和保留证据的要求（也见 16.1.7）。

其它信息

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。为帮助识别出对安全监视目的有重要意义的事态，应考虑将相应的消息类型自动地拷贝到第二份日志，或使用适合的系统工具或审计工具，执行文件查询及合理化。

需要保护系统日志，因为如果其中的数据被修改或删除，它们的存在可能产生安全的虚假感觉。实时拷贝系统日志到系统管理员或操作员控制外的系统，可以用来保护日志。

12.4.3 管理员和操作员日志（原 10.10.4）

控制措施

系统管理员和系统操作员活动应被记录、日志被保护并定期检查。

实施指南

特权用户帐号持有者在他们的直接控制下也许能够操纵信息处理设施上的日志，因此，保护和审查维护日志对特权用户赋予责任是必要的。

其它信息

对在系统和网络管理员控制之外进行管理的入侵检测系统可以用来监视系统和网络管理活动的符合性。

12.4.4 时钟同步（原 10.10.6）

控制措施

一个组织或安全域内的所有相关信息处理系统的时钟应使用一个单一的时钟源进行同步。

实施指南

时间的表现、同步和精确性的外部和内部的要求应被文件规定。这些要求可能是法律的、监管的、合同要求的、标准符合性的或内部监视要求的。组织内使用的标准参考时间应被定义。

组织从外部源获得参考时间的方法和如何可靠地同步内部时钟应被记录在案并被实施。

其它信息

正确设置计算机时钟对确保审计记录的准确性是重要的，审计日志可用于调查或作为法律、法规案例的证据。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。链接到国家原子钟无线电广播时间的时钟可被使用作为日志系统的主时钟。网络时间协议可被使用，保持所有的服务器与主时钟同步。

12.5 运行软件的控制

目标：保证操作系统的完整性

12.5.1 操作系统上软件的安装（新增）

控制措施

控制在操作系统上软件安装的程序应被落实。

实施指南

在操作系统上软件的变更控制应考虑下列指南：

a) 运行软件、应用和程序库的更新仅应由经过训练的管理员在适当的管理授权下来执行（见 9.4.5）；

b) 操作系统仅保留被批准的执行代码，没有开发代码和编译程序；

c) 应用和操作系统软件仅应被执行在广泛的和成功的测试之后；这个测试应涵盖可用性、安全性、对其它系统的影响和用户友好性，并应在独立的系统上执行（见 12.1.4）；它应被确保所有的对应的源代码库已被更新；

d) 配置控制系统应被使用以保持所有执行软件和系统文档的控制；

e) 变更实施前应安置一个回退策略；

f) 对运行程序库的所有更新的审计日志应被维护；

g) 应用软件的先前版本应被保留作为应变措施；

h) 软件的老版本应被存档，与所有要求的信息、参数、程序、配置细节和支持软件作为长久数据以存档的方式被保留。

操作系统中使用的由厂商提供的软件应以供应商的水平来维护，随着时间的推移，软件厂商将停止老版本软件的支持。组织应用考虑信赖于不被支持的软件的风险。

任何对新版本的升级决定，应考虑版本变更和安全的业务要求，如，新的信息安全功能、数量的引入和影响这个版本的信息安全问题的严重性。软件补丁应被应用，当他们可以帮助来消除或降低信息安全弱点的时候（见 12.6 ）.

物理或逻辑访问应仅被给到需要时的供应商的支持目的，并得到管理批准。供应商的活动应被监视（见 15.2.1）。

信赖于外部提供的软件和模块的计算机软件，应被监视和控制，以避免可能引入安全弱点的非授权变更。

12.6 技术脆弱性管理

目标：防止技术脆弱性的利用。

12.6.1 技术脆弱性的管理（条款不变）

控制措施

应及时获得信息系统技术脆弱性的信息，评价对这些脆弱性组织的暴露程度，并采取适当的措施来处理相关的风险。

实施指南

当前并完整的资产清单（见 8）是进行有效的技术脆弱性管理的前提。支持技术脆弱性管理所需的特定信息包括软件厂商、版本号、当前部署的状态（如，在什么系统上安装什么软件），以及组织内负责软件的人员。

应采取适当的和及时的行动以响应对潜在技术脆弱性的识别。为建立有效的技术脆弱性管理过程应遵循下面的指南：

a) 组织应定义并建立与技术脆弱性管理相关的角色和职责，包括脆弱性监视、脆弱性风险评估、补丁、资产追踪，和任意需要的协调职任；

b) 识别有关技术脆弱性和维护脆弱性意识的软件和其它技术的信息资源应被识别，对于软件和其他技术（基于资产清单，见 8.1.1）；这些信息资源应根据清单的变更或当发现其它新的或有用的资源时进行更新；

c) 应制定时间表对潜在的有关技术脆弱性的通知做出反映；

d) 一旦潜在的技术脆弱性被确定，组织应识别相关的风险并采取措施；这些措施可能包括对脆弱系统的补丁，或者应用其它控制措施；

e) 依据技术脆弱性需要解决的紧急程度，应根据变更管理相关的控制措施（见 12.1.2），或者遵照信息安全事态响应程序（见 16.1.5）采取措施；

f) 如果有来自合法源的可用的补丁，则应评估与安装该补丁相关的风险（由脆弱性引起的风险与安装补丁带来的风险应进行比较）；

g) 在安装补丁之前，应进行测试和评估，以确保它们是有效的，且不会导致不能容忍的负面影响；如果没有可用的补丁，应考虑其它控制措施，如：

   1）关闭与脆弱性有关的服务和能力；

   2）选配或增加访问控制措施，如，在网络边界上添加防火墙（见 13.1）；

   3）增加监视以检测真实的攻击；

   4）提高脆弱性意识；

h) 应保持所有执行程序的审计日志；

i) 应定期对技术脆弱性管理过程进行监视和评价，以确保其有效性和效率；

j) 处于高风险中的系统应首先处理；

k) 有效的技术脆弱性管理过程应与事件管理活动结合考虑，脆弱性数据传达给事件响应功能，事件发生时提供技术脆弱性程序来执行；

l) 定义一个程序来处理，脆弱性已被识别，但没有合适的对策的情形。在这种情形中，组织应评估与已知脆弱性相关的风险，并规定合适的检测和纠正行动。

其它信息

技术脆弱性管理可以作为变更管理的一个子功能被评审，并可利用变更管理过程和程序（见 12.1.2 和 14.2.2）。

厂商往往尽早发布补丁要承受重大的压力。因此，补丁可能不足以解决该问题，并且可能存在负作用。而且，在某些情况下，一旦补丁被应用后，很难被卸载。

如果不能对补丁进行充分的测试，如，由于成本或资源缺乏，那么可以根据其它用户的报告经验，考虑推迟打补丁，评价相关的风险。

12.6.2 软件安装限制（原 12.4.1）

控制措施

应建立和执行规则来控制由用户安装软件。

实施指南

组织应定义和执行严格的策略，用户可以安装的软件类型。

最小特权原则应被应用。如果准许某个特权，用户可以有能力来安全软件。组织应识别被允许安装软件的类型（如，对现有软件的更新和安全补丁），和禁止安装的软件（如，仅由个人使用的软件和出身于未知和怀疑带潜在恶意代码的软件）。用户所涉及的角色的特权应被准许。

其它信息

在计算机设备上不受控的软件安装可能导致引入脆弱性、产生信息泄漏、丢失完整性或其它信息安全事件，或违反知识产权。

12.7 信息系统审计的考虑

目标：将运行系统上审计活动的影响最小化。

12.7.1 信息系统审计控制（原 15.3.1）

控制措施

涉及对运行系统验证的审计要求和活动，应谨慎地加以规划并取得批准，以便最小化业务过程的中断。

实施指南

应遵守下列指南：

a) 应与合适的管理者商定对系统和数据访问的审计要求；
b) 技术审计测试的范围应商定并被控制；
c) 审计测试应限于对软件和数据的只读访问；
d) 非只读的访问应只允许隔离的系统文件的拷贝，当审核完成时，应被删除，或者在审计文件要求下，具有保留这些文件的义务，则要给予适当的保护；
e) 特定的或附加的过程要求应被识别和同意；
f) 可能影响系统可用性的审计测试应在非业务时间段来完成；
g) 所有访问应被监视和记录，以产生参考踪迹。

13 通信安全

13.1 网络安全管理

目标：确保网络中信息和支持它的信息处理设施的保护。

13.1.1 网络控制（原 10.6.1）

控制措施

应管理和控制网络，以保护系统和应用程序中的信息。

实施指南

控制措施应被实施，以确保网络上的信息安全、防止未授权访问所连接的服务。特别是，下列条款应予以考虑：

a）应建立网络设备管理职责和程序；

b）若合适，网络的操作职责要与计算机操作分开（见 6.1.2）；

c）具体的控制措施应被建立，以保护通过公网或无线网的数据的保密性和完整性，且保护被连接的系统和应用程序（见 10 和 13.2）。具体的控制措施也被要求，以维护网络服务和计算机连接的可用性；

d） 应使用适当的日志和监视控制措施，以使可能被影响的活动或相关的信息安全能被记录和检查；

e）管理活动应紧密地协调对组织服务的优化和确保控制措施被一贯地应用于信息处理基础设施；

f）网络上的系统应被身份认证；

g） 系统连接到网络应受限制。

其它信息

关于网络安全的另外信息可以在ISO/IEC 27033找到。

13.1.2 网络服务的安全（原 10.6.2）

控制措施

所有网络服务的安全机制、服务水平和管理要求，应予以明确并列入网络服务协议中，无论这些服务是否由公司内部提供还是外包。

实施指南

网络服务提供商以安全方式管理商定服务的能力应予以确定并定期监视，还应商定审核的权利。

应识别特殊服务的安全约定，例如安全特性、服务级别和管理要求。组织应确保网络服务提供商实施了这些措施。

其它信息

网络服务包括连接的提供、私有网络服务、增值网络和使用的网络安全解决方案，例如防火墙和入侵检测系统。这些服务既包括的范围从简单的未受控的带宽到复杂的增值产品。

网络服务的安全特性可以是：

a) 为网络服务应用的安全技术，例如身份认证、加密和网络连接控制；

b) 依据安全和网络连接规划，与网络服务安全连接的技术参数被要求；

c) 若需要，使用网络服务程序来限制对网络服务或应用的访问。

13.1.3 网络隔离（原 11.4.5）

控制措施

应在网络中隔离信息服务分类、用户及信息系统。

实施指南

大型网络安全管理的一种方法是将他们分成独立的网络域，这些域可以基于信任级别来选择（例如，公共访问域、桌面域、服务器域），基于组织单元（例如，人力资源、财务、市场）或一些组合（例如，与多个组织单元连接的服务器域）。分离可以被完成使用不同的物理网络或不再的逻辑网络（例如，虚拟私有网络）。

每个域的边界应被恰当的定义。网络域之间的访问应被允许，但应在边界使用网关来控制（例如，防火墙，过滤路由器）。分离网络成域和通过网关允许访问的标准，应基于每个域的安全要求的评估。这个评估应依赖于访问控制策略（见 9.1.1）、访问要求、重要性、信息处理分类、考虑相对成本和结合合适的网关技术的性能影响。

由于无线网网络边界定义不明确，要求特殊处理。由于敏感环境，考虑外部连接的所有无线访问与内部网络隔离，直到对内部系统访问的外部连接被准许通过与网络控制策略（见 13.1.1）相一致的网关。

适当的实施身份认证、加密和现代的用户级别网络访问控制技术，基本无线网的标准可以有能力直接连接到组织的内网。

其它信息

正在日益扩充的网络超出组织的边界，形成的业务伙伴可能需要互联或共享信息处理和网络设施。这样的扩充可能增加对使用此网络的组织的信息系统进行未授权访问的风险，其中的某些系统由于其敏感性或关键性可能需要防范其他的网络用户。

13.2 信息传输

目标：维护组织与任何外部实体的信息传输安全。

13.2.1 信息传输策略和程序（原 10.8.1）

控制措施

应有正式的传输策略、程序和控制措施，以保证所有类型的通信设施间的信息传输安全。

实施指南

使用通信设施进行信息交换的程序和控制措施应考虑下列条款：

a) 设计用来防止交换信息遭受截取、复制、修改、错误路由和破坏的程序；
b) 检测和防止可能通过使用电子通信传输的恶意代码的程序；
c) 保护以附件形式传输的敏感电子信息的程序；
d) 电子通信设施可接受使用的概要策略或指南（见 8.1.3）；
e) 员工、外部团体和任何其他用户的不危害组织的职责，例如诽谤、扰乱、扮演、

连锁信件转发、未授权购买等；

f) 密码技术的使用，例如保护信息的保密性、完整性和真实性（见 10）；

g) 所有业务通信（包括消息）的保持和处理指南，要与相关国家和地方法律法规一致；

h) 与通信设施转发相关的控制措施和限制，例如将电子邮件自动转发到外部邮件地址；

i) 提醒工作人员来采取相应的预防措施不泄露秘密信息；

j) 不遗弃应答机上包含秘密信息的消息，由于这些消息可能被授权个人复制、存储在公共系统或作为一个不正当行为的结果被不正确的存储；

k) 通告员工关于使用传真机或服务的问题，也就是：

1）非授权访问内置存储消息到恢复消息；

2）故意或意外的机器编程来发送消息到具体的号码；

3）由于误拨号或使用错误存储的号码将文档和消息发送给错误的电话号码；

另外，应提醒工作人员，不要在公共场所或不安全的通讯通道或开放办公室和会场进行保密会谈。

信息交换服务应符合所有相关的法律要求（见 18.1）。

其它信息

可能通过使用很多不同类型的通信设施进行信息交换，包括电子邮件、语音、传真和视频。

可能通过很多不同类型的介质进行软件交换，包括从互联网下载和从出售现货供应产品的厂商处获得。

应考虑与电子数据交换、电子商务、电子通信和控制要求相关的业务、法律和安全影响。

13.2.2 信息传输协议（原 10.8.2）

控制措施

协议应处理组织与外部方传输商业信息的安全传输。

实施指南

信息交换协议应包含如下条款：

a) 控制和通知传输、分派和接收的管理职责；

b) 确保可追溯性和不可抵赖性的程序；

c) 打包和传输的最低技术标准；

d) 有条件转让契约；

e) 信使标识标准；

f) 信息安全事件结果的责任和义务，例如数据丢失；

g) 商定的敏感或关键信息的标签系统的使用，确保标记的含义能直接理解，信息受

到适当的保护（见 8.2）；

h) 记录和阅读信息和软件的技术标准；

i) 为保护敏感项，可以要求任何专门的控制措施，例如密码学（见 10）；

j) 在信息传输期间维护一个监管链；

k) 访问控制的可接受级别。

应建立和保持策略、程序和标准，以保护传输中的信息和物理介质（见 8.3.3），并在交换协议中引用。

任何协议的安全内容应反映涉及的业务信息的敏感性。

其它信息

协议可以是电子的或手写的，可能采取正式合同的形式。对秘密信息而言，这样的信息交换使用的特定机制对于所有组织和各种协议应是一致的。

13.2.3 电子消息（原 10.8.3）

控制措施

涉及电子消息的信息应适当保护。

实施指南

电子消息的信息安全考虑应包括以下方面：

a) 对应于组织采用的分类设计，防止消息遭受未授权访问、修改或拒绝服务攻击；

b) 确保正确的处理和消息传输；

c) 服务的可靠性和可用性；

d) 法律方面的考虑，例如电子签名的要求；

e) 在使用外部公开服务（例如即时消息、交际网络或文件共享）前获得批准；

f) 更强壮的身份认证级别用于控制来自公共可访问网络的访问。

其它信息

很多种电子消息（例如电子邮件、电子数据交换（EDI）、交际网络）在业务通信中充当一个角色。

13.2.4 保密或不泄露协议（原 6.1.5）

控制措施

应确定组织信息保护需要的保密性或不泄露协议的要求，定期审查并记录。

实施指南

保密或不泄露协议应使用法律强行的期限来解决保护机密信息的要求。保密或不泄露协议应用到外部各方或组织的雇员。其它方类型、和它的允许访问或秘密信息的处理要素考虑应被选择或增加。为识别保密或不泄露协议的要求，需考虑下列因素：

a) 定义要保护的信息（如机密信息）；

b) 协议的期望持续时间，包括保密性需要不定期维护的情形；

c) 协议终止时要求的活动；

d) 为避免未授权信息泄露的签署者的职责和行为；

e) 信息所有者、商业秘密和知识产权，以及他们如何与机密信息保护相关联；

f) 机密信息的允许使用，及签署者使用信息的权力；

g) 对涉及机密信息的活动的审计和监视权力；

h) 未授权泄露或机密信息破坏的通知和报告过程；

i) 关于协议终止时信息归档或销毁的条款；

j) 违反协议后期望采取的措施。

基于一个组织的安全要求，在保密性或不泄露协议中可能需要其他因素。

保密性和不泄露协议应针对它适用的管辖范围(也见 18.1)遵循所有适用的法律法规。

保密性和不泄露协议的要求应进行周期性评审，当发生影响这些要求的变更时，也要进行评审。

其它信息

保密性和不泄密协议保护组织信息，并告知签署者他们的职责，以授权、负责的方式保护、使用和公开信息。

对于一个组织来说，可能需要在不同环境中使用保密性或不泄密协议的不同格式。

14 信息系统获取、开发和维护

14.1 信息系统的安全要求

目标：确保安全是信息系统生命周期的的一个有机组成部分，包括对向公共网络提供服务的信息系统要求。

14.1.1 信息安全需求分析和说明（原 12.1.1）

控制措施

在新的信息系统或增强已有信息系统的业务要求陈述中，应规定对安全控制措施的要求。

实施指南

信息安全要求应被识别，使用诸如从策略和规则、威胁模型、事件评审或脆弱性阈值的使用中导出合规性要求。识别的结果应文件化并由所有的利益相关者评审。

信息安全要求和控制措施应反映出（参见 8.2）所涉及的信息的业务价值和由于缺乏足够安全导致潜在的负面业务影响。

信息安全要求识别和管理和与过程的关联应被集成在信息系统项目的早期阶段。信息安全要求考虑越早，如在设计阶段能使解决方案更有效且成本更节约。

信息安全要求也应考虑：

a) 为了得到用户身份认证需求，要求信任级别接近用户的身份要求；

b) 访问配置和授权过程，为业务用户、特权用户或技术用户；

c) 告诉用户和操作员他们的义务和责任；

d) 所涉及资产的保护需求被要求，尤其是关于可用性、保密性和完整性；

e) 来自业务过程的要求，诸如交易记录、监视和不可抵赖的要求；

f) 由其它安全控制措施强制的要求，如，日志、监视或数据泄漏监测系统。

通过公共网络提供服务或执行交易的应用，14.1.2 和 14.1.3 专用控制措施应被考虑。

如果产品被获得，一个正式的测试和获取过程应被遵循。与供应商签订的合同应体现已识别的安全要求。被提议的产品的安全功能不满足指定的要求，在购买这个产品之前应重新考虑风险和相关的控制措施。

与最终软件/系统服务栈相关联产品的安全配置指南的可用性应被评估和实现。

接受产品的标准应被定义，如已识别的安全要求的功能条款、给定的保证应被满足。产品应被评估依赖于获得之前的标准。附加的功能应被评审以确保不产生不可接受的额外风险。

其它信息

ISO/IEC 27005 和 ISO 31000 提供了使用风险管理过程确定控制措施满足信息安全要求的指南。

14.1.2 保护公共网络上的应用服务（新增）

控制措施

公网上应用服务中传输的信息应被保护，以免遭受欺诈、合同纠纷、未经授权的披露和修改。

公网上应用服务的信息安全应考虑如下：

a) 每个团体的信任级别要求每一个其它的身份要求，如，通过身份认证；

b) 与可能批准的内容、关键问题或标记交易文档相关联的授权过程；

c) 确保通讯的伙伴充分了解他们规定的授权或服务使用；

d) 确定并满足保密性、完整性、发送和接收关键文档和合同的不可抵赖性，如与投标和合同关联的过程；

e) 关键文档的完整性信任级别被要求；

f) 任何机密信息的保护要求；

g) 任何订单交易、支付信息、交付地址细节和接收确认的机密性和完整性；

h) 由客户提供的验证支付信息适当的验证程度；

i) 选择最合适的支付结算方式以防止欺诈；

j) 维持订单信息的机密性和完整性的保护级别被要求；

k) 避免交易信息的丢失或复制；

l) 与任何不诚实交易相关联的倾向；

m) 保险要求。

上述考虑的大部分能由密码学控制措施的应用来处理（详见 10），考虑与法律要求的

合规性（详见 18，尤其是密码学法律的 18.1.5）。

在合作伙伴之间的应用服务安排应由文档化的协议来提供，保证合作伙伴之间同意服务的条款，包括上面（见 b））的授权细节。

反攻击的弹性要求应被考虑，包括保护涉及的应用服务器或确保网络互联的可用性被要求来交付服务。

其它信息

通过公网可得到的应用受到一系列网络的威胁，如欺诈活动、合同纠纷或信息泄漏给大众。因此，详尽的风险评估和合理的控制措施选择是必不可少的。控制措施被要求通常包括认证和数据安全传输的加密算法。

应用服务能利用安全认证算法，如使用公钥加密和数字签名（详见 10）来降低风险。而且，可信任的第三方能被使用，这样的服务被需要。

14.1.3 保护应用服务交易（新增）

控制措施

应用服务传输中所涉及到的信息应加以保护，以防止不完整的传输、路由错误、未经授权的消息改变、未授权披露、未经授权的消息复制或重放。

实施指南

应用服务传输中信息安全考虑应包括如下：

a) 包含在交易中的每一个合作伙伴的电子签名的使用；
b) 交易的所有方面，如，确保：
   1) 所有合作伙伴的用户的安全认证信息是有效的且是被验证的；
   2) 交易保持机密性；
   3) 涉及的所有合作伙伴的关联的隐私被保留；
c) 所有涉及的合作伙伴之间的通讯路径是加密的；
d) 所有涉及的合作伙伴的通讯协议是加密的；
e) 确保交易细节的存储安置在任何公共可访问的外面，如存储平台安置在组织的内联网，且不保留和裸露互联网可访问的存储介质上；
f) 可依赖的授权被使用（如，为发布、维护数据签名或数字证书的目的）安全被集成且被嵌入贯穿整个端到端证书/签名管理过程。

其它信息

被采用的控制措施的程度需要与每个应用服务交易的格式关联的风险级别相当。

交易可能需要遵从交易产生、处理、完成或存储的管辖范围内的法律法规。

14.2 开发和支过持程中的安全

目标：确保在整个信息系统开发生命周期中的信息安全设计与实施。

14.2.1 安全开发策略（新增）

控制措施

应制定及应用关于软件和系统的开发规则。

实施指南

安全开发是对建立安全服务、架构、软件和系统的要求。在安全开发策略中，应考虑如下方面：

a) 开发环境的安全；

b) 软件开发生命周期中安全指导：

1) 软件开发方法的安全；

2) 每个被使用的程序设计语言的安全代码指南；

c) 设计阶段的安全要求；

d) 项目里程碑中的安全检查点；

e) 安全资源库；

f) 版本控制的安全；

g) 必需的应用安全知识；

h) 开发者避免、查找和解决脆弱性的能力。

当应用到开发中的标准还不为人所知或与当前最佳实践不一致的情况下，安全程序设计技术应被使用在新的开发和代码再利用场景中。安全代码标准应被考虑并被强制性使用。开发者应接受培训对它们的使用，测试和代码审查应被验证它们的使用。

如果开发被外包，组织应确保外包方遵从这些安全开发的规则（见 14.2.7）。

其它信息

开发也可能发生在应用中，如办公应用、脚本、浏览器和数据库。

14.2.2 系统变更控制程序（原 12.5.1）

控制措施

在开发生命周期中系统的变更应由正式的变更控制程序来控制。

实施指南

应将正式的变更控制程序文档化，并强制实施以确保系统、应用和产品的完整性，从早期的开发阶段直到后期的维护工作。

新系统的引入和原有系统的主要变更应按照从文档、规范、测试、质量控制到实施管理这样正式的过程进行。

这个过程应包括风险评估、变更影响分析、所需的安全控制措施规范。这一过程还应确保不损坏现有的安全和控制程序，确保支持程序员仅能访问系统中其工作所需的那些部分，确保任何变更要获得正式协商和批准。

只要可行，应用和运行变更控制程序应集成起来（见 12.1.2）。该变更程序应包括并不限于：

a) 维护所商定授权级别的记录；

b) 确保由授权的用户提交变更；

c) 评审控制措施和完整性程序，以确保它们不因变更而损坏；

d) 识别需要修正的所有软件、信息、数据库实体和硬件；

e) 在工作开始之前，获得对详细建议的正式批准；

f) 确保已授权的用户在实施之前接受变更；

g) 确保在每个变更完成之后更新系统文档设置，并将旧文档归档或丢弃；

h) 维护所有软件更新的版本控制；

i) 维护所有变更请求的审计踪迹；

j) 当需要时，确保对操作文档（见 12.1.1）和用户程序作合适的变更；

k) 确保变更的实施发生在正确的时刻，并且不干扰所涉及的业务过程。

其它信息

变更软件会影响运行环境。

良好的惯例包括在一个与生产与开发完全隔离的环境中测试新软件（见 12.1.4）。这提供对新软件进行控制和允许对被用于测试目的的运行信息给予附加保护的手段。这应包括补丁、服务包和其它更新。

自动更新应被考虑，依赖于更新快速部署的好处来权衡系统完整性和可用性的风险。不应在关键系统中使用自动更新，因为某些更新可能会导致关键应用的失败。

14.2.3 操作平台变更后对应用的技术评审（原 12.5.2）

控制措施

当操作平台发生变更时，应对业务的关键应用进行评审和测试，以确保对组织的运行或安全没有负面影响。

实施指南

这一过程应涵盖：

a) 评审应用控制和完整性程序，以确保它们不因操作平台变更而损坏；

b) 确保及时提供操作平台变更的通知，以便于在实施之前进行合适的测试和评审；

c) 确保对业务连续性计划进行合适的变更（见第 17 章）。

其它信息

操作平台包括操作系统、数据库和中间件平台。这些控制措施也应被申请应用的变更。

14.2.4 对软件包变更的限制（原 12.5.3）

控制措施

应软件包的修改应被劝阻，必要的变更应被限制，且对所有的变更加以严格控制。

实施指南

如果可能且可行，应使用厂商提供的软件包，而无需修改。在必须修改软件包时，应考虑下列各点：

a) 内置控制措施和完整性过程被损坏的风险；

b) 是否应获得厂商的同意；

c) 当标准程序更新时，从厂商获得所需要变更的可能性；

d) 作为变更的结果，组织要负责进一步维护此软件的影响；

e) 与使用中的其它软件的兼容性。

如果变更是必要的，则原始软件应保留，并将变更应用于已明显确定的拷贝。应实施软件更新管理过程，以确保最新批准的补丁和应用更新已经安装在所有的授权软件中（见12.6.1）。应全部测试所有变更，并将其形成文档，以使它们可以重新应用于必要的进一步的软件升级。如果需要，所有的更新应由独立的评估机构进行测试和验证。

14.2.5 安全系统工程原则（新增）

控制措施

安全系统工程原则应被建立、形成文件、维护并应用到任何信息系统实施工作。

实施指南

基于安全工程原则的安全信息系统工程程序应被建立、形成文件并被应用到组织内部的信息系统工程活动。安全应在所有的体系结构层进行设计（业务层、数据层、应用层和技术层）以平衡信息安全需求与可达性的需求。新技术应被分析安全风险并且设计应被评审依赖于大家熟知的攻击模式。

这些原则和建立的工程程序应被不断地评审以确保它们在工程过程中是在有效地控制来增加安全标准。它们也应该被不断地评审以确保保持在最新时期与任何新的潜在的威胁进行抗衡，并保持适用于技术的发展和实用的解决方案。

已建立的安全工程原则应被应用于适用的信息系统外包，通过合同和其它约束的协议在组织和组织外包的供应商之间。组织应确认供应商的安全工程原则与组织所拥有的安全工程原则的严格程序是可比较的。

其它信息

应用开发程序应应用安全工程技术在有输入和输出接口应用的开发中。安全工程技术在用户身份认证技术、安全会话控制和数据有效性、免疫系统和高度代码的排除提供指导。

14.2.6 安全的开发环境（新增）

控制措施

组织应建立并适当保护安全开发环境和涵盖整个系统开发周期的集成工作。

实施指南

安全开发环境包括与系统开发和集成相关的人、过程和技术。

组织应评估与单个系统开发工作相关的风险并为具体的系统开发工作建立安全开发环境，应考虑：

a）由系统处理、存储和传输的数据的敏感性；

b）来自条例或策略的适用的外部和内部要求；

c）组织已经执行的支持系统开发的安全控制措施；

d）在环境中个人工作的信用；

e）与系统开发相关的外包程度；

f）不同开发环境之间的隔离需求；

g）对开发环境的访问控制措施；

h）对环境和代码存储点变更的监视；

i）备份和存储在现场外的安全位置；

j）数据进入或流出环境的移动控制措施。

具体的开发环境保护级别一旦被确定，组织应记录安全开发程序中对应的过程并提供给需要他们的所有个体。

14.2.7 外包开发（原 12.5.5）

控制措施

组织应监督并监视外包系统开发的活动。

实施指南

系统开发被外包的地方，应考虑下列要点，并贯穿组织整个外部供应链：

a）涉及外包内容的许可约定、代码所有权和知识产权（见 18.1.2）；

b）为安全设计、代码和测试实践的合同的要求（见 14.2.1）；

c）对外部开发者威胁模型被批准的条款；

d）交付物的质量和准确性的验收测试；

e）安全阈值的证据的条款被用于建立安全和加密质量的最低可接受级别；

f）充足的测试的证据条款被应用以避免在交付时存在有意的和无意的恶意内容；

g）充足的测试的证据条款被应用以避免出现众所周知的脆弱性；

h）如果源代码不再可用，履约保证约定等等；

i）合同权利来审计开发过程和控制程序；

j）建设环境的有效证据被使用来创建可交付物；

k）组织保持对可用法律的遵从和控制措施有效性的验证。

其它信息

供应商关系更进一步的信息可以在 ISO/IEC 27036 中找到。

14.2.8 系统安全测试（新增）

控制措施

安全功能测试应在开发的过程中执行。

实施指南

新的和更新的系统在开发过程期间要求全面的测试和验证，包括：在条件范围内活动、

测试输入和预期输出详细规划的准备。内部开发，测试应由开发团队执行初始化。单独的验收测试然后被保证（内部和外部开发）以确保系统工作实现预期且唯一实现预期（见14.1.1 和 14.1.9）。测试的程度对系统的重要性和类型应是相称的。

14.2.9 系统验收测试（原 10.3.2）

控制措施

在建立新系统、升级系统和更新版本时，必须建立验收测试程序和相关标准。

实施指南

系统验收测试应包括：信息安全要求的测试（见 14.1.1 和 14.1.2）和并遵守安全系统开发惯例（见 14.2.1）。这些测试也应对接收组件和集成系统进行控制。组织可以利用自动化工具，如代码分析工具或脆弱性扫描工具，并且应验证相关安全影响的纠正。

测试应被执行在一个真实的测试环境，以确保系统不会引入脆弱性到组织的环境，且这个测试是可信赖的。

14.3 测试数据

目标：确保测试数据的保护。

14.3.1 测试数据的保护（原 12.4.2）

控制措施

测试数据应被仔细筛选、保护和控制。

实施指南

应避免使用包含个人可辩认的信息或其它秘密信息用于测试目的。如果测试使用了个人可辩认或其他秘密信息，所有敏感细节和内容应被去除或修改以得到保护（见 ISO/IEC29101）。

当用于测试时，应使用下列指南保护运行数据：

a) 应用于运行应用系统的访问控制程序，也应该应用于测试应用系统；
b) 运行信息每次被拷贝到测试环境时应有独立的授权；
c) 在测试完成之后，应立即从测试应用系统清除运行信息；
d) 应记录运行信息的拷贝和使用日志以提供审核踪迹。

其它信息

系统和验收测试常常要求相当多的尽可能接近运行数据的测试数据量。

15 供应商关系

15.1 供应商关系中的信息安全

目标：确保保护供应商可访问的组织资产。

15.1.1 供应商关系的信息安全策略（原 6.2.1）

控制措施

为降低与供应商访问组织资产关联的风险所涉及的信息安全要求应与供应商协商一致并被记录。

实施指南

组织应识别和批准信息安全控制，该控制在一个策略中明确地提出供应商访问组织的信息。这些控制应提出组织执行的过程或规程，也提出组织应要求供应商执行的那些过程或规程，包括：

a) 识别和记录供应商的类型，例如：组织允许其访问信息的 IT 服务、物流工具、财务服务、IT 基础架构组件等；
b) 管理供应商关系的一个标准化的过程和生命周期；
c) 定义不同类型的供应商允许访问的信息类型，并监视和控制这些访问；
d) 每种信息类型和访问类型的最小信息安全要求，作为单个供应商协议的基础，并基于组织的业务需要、要求和它的风险属性；
e) 监视已建立的每个供应商类型和访问类型的信息安全要求的过程和规程的遵守情况，包括第三方评审和产品确认；
f) 准确和完整的控制以确保任一方提供的信息或信息处理的完整性；
g) 义务类型适用于供应商保护组织的信息；
h) 处理与供应商访问相关联的突发事件和意外事故，包括组织和供应商的共同责任；
i) 如有必要的话，弹性、恢复和应急安排来确保由任一方提供的信息或信息处理的可用性；
j) 组织人员意识培养由有关适当的策略、过程或规程来获得；
k) 组织人员的意识培养与供应商人员基于供应商的类型和供应商访问组织系统和信息的级别相关的适当的约定和行为规则相互配合；
l) 信息安全要求和控制下的条件被记录在由双方签署的协议中；
m) 管理必要的信息转换、信息处理设备和任何其它的必须的移动，并确保在转换的整个周期被信息安全被维护；

其它信息

安全管理不充分，可能使信息由于外部方介入而处于风险中。应确定和应用控制措施，以管理供应商对信息处理设施的访问。例如，如果对信息的保密性有特殊的要求，就需要使用不泄漏协议。另一个例子是数据保护风险，当供应商协议涉及转让、访问、信息跨越边界时。组织应意识到，保护属于组织信息的法律或合同责任。

15.1.2 供应商协议中提出的安全（原 6.2.3）

控制措施

应建立与信息安全相关的要求，并与供应商协商一致，包括访问、处理、存储、沟通

或为组织的信息提供 IT 基础架构组件。

实施指南

供应商协议应被建立并记录，确保组织和供应商之间关于双方的义务和责任满足相关的信息安全要求不存在误解。

为满足识别的信息安全要求，下列条款应被考虑包含在协议中：

a) 被提供或被访问的信息的描述，提供或访问信息的方法；
b) 来自组织分类表（见 8.2）的信息分类；如果需要将组织拥有的分类表和供应商的分类表进行映射；
c) 法律和法规要求，包括数据保护、知识产权和著作权、和如何确保他们被满足的描述；
d) 每个合同当事人的责任和义务被执行一个协商一致的控制集，包括：访问控制、履行回顾、监视、报告和审计；
e) 信息使用的可接受规则，如果需要包括不接受的使用；
f) 或者明确的列出被授权访问或获得组织信息的供应商人员，或者明确授权的程序或条件，并且明确由供应商访问或受理组织信息的授权删除；
g) 特定合约的信息安全策略；
h) 事件管理必备的条件和程序（尤其是事件纠正期间的通告和协作）；
i) 为特定的过程和信息安全要求必需的培训和意识教育，例如：事件响应、授权程序；
j) 子合约的相关规则，包括被执行的必需的控制；
k) 合作伙伴的相关协议，包括信息安全问题的联系人；
l) 检查要求，如果真的发生检查不完整或给定不确定或有顾虑原因的结果，供应商人员包括控制检查和通告过程的责任；
m) 恰当的审计供应商人员和控制相关的协议；
n) 缺陷解决和冲突解决的过程；
o) 供应商有义务定期地提交控制有效性的独立报告，在报告中体现相关问题协商一致的纠正时间；
p) 供应商有义务遵从组织的安全要求。

其它信息

协议会随不同的组织和不同类型的供应商型存在很大的差异。因此，应注意要在协议中包括的所有信息安全风险和要求。供应商协议也包含其它方（如，子供应商）。

在协议中，需要考虑当供应商不能提供处理事件的产品或服务时的连续处理程序，以避免在安排替代产品或服务时的任何延迟。

15.1.3 ICT 供应链（新增）

控制措施

与供应商的协议应包括与信息、通信技术服务和产品供应链相关的信息安全风险解决的要求。

实施指南

有关供应链安全，下列条款应被考虑包含在供应商协议中：

a) 除了供应商关系基本的信息安全要求外，适用于信息和通讯技术产品或服务获取的信息安全要求应被定义；

b) 对于信息和通讯技术服务，如果供应商分包部分信息和通讯技术服务，要求供应商传播组织的安全要求到整个供应链；

c) 对于信息和通讯技术产品，如果这些产品包含向其它供应商购买组件，要求供应商传播适当的安全惯例到整个供应链；

d) 实施一种监视过程和适当的方法，来验证所交付的信息和通讯技术产品和服务遵循规定的安全要求；

e) 实施一个过程，来识别产品或服务组件处于维持功能的临界状态，因此，要求提高注意和监督，尤其是组织外购时，顶层供应商向其它供应商外购产品或服务组件时；

f) 确保危险的组件和他们的源头能被跟踪贯穿整个供应链；

g) 确保交付的信息和通讯技术产品期望的功能被保证，没有任何的意外或有缺点的特性；

h) 在组织和供应商内定义一个规则，共享有关供应链和任何潜在的问题和妥协；

i) 实施特定的过程，管理信息和通讯技术组件生命周期和可用性并与安全风险关联。包括：管理由于供应商不再经营或由于技术发展不再提供这些组件而造成的组件不再可用的风险。

其它信息

具体的信息和通信技术供应链风险管理实践建立在一般的信息安全、质量、项目管理和系统工程基础之上，但不能代替他们的做法。

组织应与供应商一起来了解信息和通信技术供应链，提供的信息和通讯技术产品或服务产生重大影响的任何事情。组织可以影响信息和通信技术供应链信息安全的做法，在与他们的供应商协议中，明确在信息和通信技术供应链中应该由其它供应商处理的事项。

信息和通信技术供应链同样被应用解决云计算服务。

15.2 供应商服务交付管理

目标：维持与供应商协议中商定的信息安全和服务交付的水平。

15.2.1 监测和评审供应商服务（原 10.2.2）

控制措施

组织应定期监测、评审和审计供应商服务交付。

实施指南

供应商服务的监测和评审应确保协商一致的信息安全条款和条件被遵循，信息安全事件和问题被适当的管理。

在组织和供应商之间应包括一个服务管理关系过程：

a) 监视服务执行级别以检查对协议的符合度；
b) 评审由供应商产生的服务报告，安排由协议要求的定期的进展会议；
c) 与独立审计员报告的评审配合实施对供应商的审计，如果可行，把识别出的问题进一步的采取行动；
d) 提供信息安全事件的信息，并在任何支持指南和程序中评审这个信息作为协议的要求；
e) 评审供应商有关服务交付中对信息安全事态、操作问题、故障、原因追查和中断的记录和审计跟踪；
f) 解决和管理任何已识别的问题；
g) 评审供应商与它拥有的供应商关系的情况；
h) 确保供应商维持足够的服务能力与可行的计划一起被设计，来确保主要的服务失败或灾难发生时协商一致的服务连续性水平被维持（见 17）。

管理与供应商关系的职责应分配给指定人员或服务管理组。另外，组织应确保供应商分配了检查符合性和执行协议要求的职责。应获得足够的技术技能和资源来监视满足协议的要求，特别是信息安全要求。当在服务交付中发现不足时，应采取适当的措施。

组织应对供应商访问、处理或管理的敏感或关键信息或信息处理设施的所有安全方面保持充分的、全面的控制和可见度。组织应确保他们对安全活动留有可见度，例如，通过一个被定义的报告过程，管理变更、识别脆弱性和报告/响应信息安全事件。

15.2.2 供应商服务变更管理（原 10.2.3）

控制措施

应管理供应商提供的变更，包括维护、改进现有的信息安全策略、程序和控制，应将商业信息的关键性、系统、流程和风险的重新评估考虑在内。

实施指南

应考虑下列方面：

a) 供应商协议的变更；
b) 组织要实施的变更：
   1）对提供的现有服务的加强；
   2）任何新应用和系统的开发；
   3）组织方针策略和程序的更改或更新；
   4）解决信息安全事件、改进安全的新的或的控制措施。

c) 供应商服务实施的变更：

1）对网络的变更和加强；

2）新技术的使用；

3）新产品或新版本的采用；

4）新的开发工具和环境；

5）服务设施的物理位置的变更；

6）供应商的变更；

7）外包给其它的供应商。

16 信息安全事件管理

16.1 信息安全事件管理和持续改进

目标：确保一致和有效的方法来管理信息安全事件，包括安全事态和弱点的报告。

16.1.1 职责和程序（原 13.2.1）

控制措施

应建立管理职责和程序，以确保快速、有效和有序地响应信息安全事件。

实施指南

信息安全事件管理职责和程序应考虑下列指南：

a）应建立管理职责，以确保下列的程序被开发并在组织内传达：

1）事件响应计划和预案程序；

2）信息事态和事件监视、检测、分析和报告程序；

3）事件管理活动日志程序；

4）司法证据处理程序；

5）信息安全事态的判断和信息安全弱点评估程序；

6）事件升级和控制恢复、内外部人员或组织报告程序；

b）程序被建立应确保：

1）主管人员处理组织内信息安全事件的相关问题；

2）应落实安全事件监测和报告的唯一联系点；

3）处理信息安全事件应与权威机构、外部利益团体和论坛保持适当的联系；

c）报告程序应包括：

1）准备信息安全事态报告的形式来支持报告活动，并帮助人们记住信息安全事态报告所必需的活动；

2）程序是保证一个信息安全事态发生的情况下的，例如，注意所有直接地细节，如不遵守或违反、发生故障的类型、屏幕上的消息和立即报告给唯一联系点以及协调活动；

3）引用一个建立正式的纪律处理过程来处理干了安全破坏的员工；

4）适当的反馈流程，以确保报告安全事件的那些人被通知问题处理后的结果并关闭问题。

应与管理者商定信息安全事件管理的目标，应确保负责信息安全事件管理的人员理解组织处理信息安全事件的优先顺序。

其它信息

信息安全事件可能超越组织边界和国家边界。为了对这样的事故做出响应，与适当的外部组织协同响应和共享这些事件的信息的需求日益增大。

ISO/IEC 27035.[20]提供了信息安全事件管理的详细指南。

16.1.2 报告信息安全事态（原 13.1.1）

控制措施

信息安全事态应尽可能快地通过适当的管理渠道进行报告。

实施指南

所有雇员、承包方人员和第三方人员都应知道他们有责任尽可能快地报告信息安全事态。他们还应知道报告信息安全事态的程序和联系点。报

被认为要报告的信息安全事态的情况包括：

a）无效的安全控制；

b）违背信息完整性、机密性和可用性的预期；

c）人为错误；

d）不遵守策略或指导方针；

e）违反物理安全布置；

f） 系统变更不被控制；

g）软件或硬件故障；

h）非法访问。

其它信息

故障或其它异常的系统行为可能是安全攻击和实际安全违规的指示，因此应将其当作信息安全事态进行报告。

16.1.3 报告信息安全弱点（原 13.1.2）

控制措施

应要求使用组织信息系统和服务的所有员工和承包方记录并报告他们观察到的或可疑的系统或服务的安全弱点。

实施指南

为了预防信息安全事件，所有员工和承包方应尽可能快地将这些事情报告给联系点。报告机制应尽可能容易、可理解和可用。

其它信息

应通知员工和承包方不要试图去证明被怀疑的安全弱点。测试弱点可能被看作是潜在的系统误用，还可能导致信息系统或服务的损害，或引起测试人员的法律责任。

16.1.4 信息安全事态的评估和决策（新增）

控制措施

信息安全事态应当被评估与决策，如果他们被归类为信息安全事件。

实施指南

联系点应使用经协商一致的信息安全事态和事件分类表并决定事态是否归类到信息安全事件。类别和优先级可以帮助来识别事件的影响和程度。

示例，如果组织有一个信息安全事件响应小组，这些评估和决策应转给信息安全事件响应小组来确认或重估。

评估和决策的结果应被详细记录，以便将来参考和验证。

16.1.5 信息安全事故的响应（新增）

控制措施

信息安全事件应依照程序文件响应。

实施指南

信息安全事件应被指定的联系点和组织的其他相关人员或外部各方作出响应（见16.1.1）。

响应应包括如下内容：

a) 事件发生后尽早收集证据；
b) 安排信息安全司法分析，作为必选项（见 16.1.7）；
c) 升级，作为必选项；
d) 确保所有牵涉的响应活动适当的记录以供日后分析；
e) 传达信息安全事件或任何相关的细节的现状给需要了解的内部和外部人员或组织；
f) 处理信息安全弱点找到原因或为事件做贡献；
g) 一旦事件被成功处理，正式地关闭并记录它。

应进行事件后的分析，如有必要，确定事件原因。

其它信息

事件响应的首要目的是恢复到‘正常安全水平’然后开始必要的恢复。

16.1.6 回顾信息安全事件（原 13.2.2）

控制措施

从分析和解决信息安全事件中获取知识，以减少未来事件的可能性或影响。

实施指南

应有适当的机制，使信息安全事件的类型、数量和成本能被量化和监视。从信息安全事件评价中获取的信息被用来识别重复发生或高影响的事件。

其它信息

信息安全事件的评估可能表明增强或追加控制措施，以限制事件将来再发生的频率、损伤和成本，或可用在安全策略审查过程中（见 5.1.2）。

在保密性方面应有的关注，来自实际的信息安全事件的轶事可以用于用户意识培训（见 7.2.2），作为可能发生的案例，如何响应此类事件的发生，以及将来如何避免他们。

16.1.7 收集证据（原 13.2.3）

控制措施

组织应制定和应用程序，用于鉴定、收集、获得和保存那些可作为证据的信息。

实施指南

为了处理应对惩罚和诉讼活动的证据时，应制定和遵循内部程序。

一般来说，这些证据程序应被提供证据的标识、收集、获取和保留的过程，并与不同类型的介质、设备和设备的状态协调一致，例如：开机或关机。该程序应考虑：

a）保管链；

b）证据的安全；

c）人员的安全；

d）参与人员的任务和职责；

e）人员的能力；

f）记录；

g）简要情况。

人员资格和工具的可用性、验证和其他相关的方法应被寻找，以增强证据保存的价值。

证据可以超越组织边界和/或管辖权边界。在这样的情况下，应确保授权某组织去收集需要的信息作证据。还应考虑不同管辖权的要求，以使证据能在相关管辖区域内获得最大的可用机会。

其它信息

识别过程涉及潜在证据的搜索、识别和记录。收集过程可以包含潜在证据的自然规律的推断过程。获取过程是创建一个定义集的数据拷贝。保存过程是保持和维护潜在证据的完整性和原始状态的过程。

当一个信息安全事件首次被检测到，这个事件是否会导致法律行为可能不是显而易见的。因此，在认识到事件的严重性之前，可能存在重要的证据被故意或意外毁坏的危险。明智的做法是在任何预期的法律行为中及早聘请一位律师或警察，以获取所需证据的建议。

ISO / IEC 27037 [24]提供了识别、收集、获取和保存数字证据的指南。

17 信息安全方面的业务连续性管理

17.1 信息安全连续性

目标：信息安全连续性应嵌入组织的业务连续性管理体系中（BCM）。

17.1.1 规划信息安全连续性（原 14.1.1）

控制措施

组织应确定其在不利情况下的信息安全和信息安全管理连续性要求，如危机或灾难。

实施指南

组织应确定在业务连续性管理过程或灾难恢复管理过程中捕获信息安全连续性。在规划业务连续性和灾难恢复的时候应确定信息安全要求。

缺乏正式的业务连续性和灾难恢复规划时，信息安全管理应承担的信息安全需求在不得的情况下保持不变，相比正常操作条件。另外，组织可以为信息安全方面执行业务影响分析，确定信息安全的要求应用于不利的情况。

其它信息

为了减少对信息安全业务影响分析的额外的时间和努力，推荐在正常业务连续性管理和灾难恢复管理业务影响分析中捕获信息安全方面的业务影响分析。这意味着信息安全连续性要求被明确规划在业务连续性管理和灾难恢复管理过程中。

业务连续性管理的信息可详见 ISO/IEC 27031,[14] ISO 22313[9] and ISO 22301.[8]

17.1.2 实施信息安全的连续性（新增）

控制措施

组织应建立、记录、实施和维护流程、程序、控制措施，以保证在不利情况下信息安全连续性要求的等级。

实施指南

组织应确保：

a) 适当的管理结构应准备就绪，为减轻和应对破坏性事件，使用有相应权力、经验和技能的应急响应人员；
b) 应指定有必需的责任、权限和能力来管理事件和维护信息安全的应急响应人员；
c) 形成文件的计划、响应和恢复程序被开发和批准，详细说明组织如何管理破坏性事件，并保持信息安全达到基于管理层批准的信息安全连续性目标（见 17.1.1）的预定水平。

根据信息安全连续性要求，组织应建立、形成文件、实施和保持：

a) 业务连续性和灾难恢复中信息安全控制措施流程、程序和支持系统和工具；
b) 在不利情况下，流程、程序和实施改变到现有信息安全控制措施；
c) 在不利情况下，信息安全控制措施不能被保持要有补救控制措施。

其它信息

在业务连续性和灾难恢复的背景下，特定的流程和程序可能被定义。这些流程或程序处理的信息或支持他们的专用信息系统的信息应被保护。因此，组织在建立、实施和保持

业务连续性或灾难恢复的流程和程序时应包含信息安全专家。

在不利情况下，已实施的信息安全控制措施应继续运行。如果安全控制措施不能继续保护信息，其它的控制措施应被建立、实施和维护来保持信息安全的可接受水平。

17.1.3 验证、评审和评估信息安全的连续性（原 14.1.5）

控制措施

组织应定期验证其建立和实施的信息安全连续性控制措施，以确保他们在不利的情况下是有效和生效的。

实施指南

无论是在运行的或连续性的背景下，组织、技术、程序和流程的变化，可以导致信息安全连续性要求的变化。在这种情况下，信息安全流程、程序和控制措施的连续性应紧跟着这些要求的变化进行检查。

组织应验证他们的信息安全管理连续性：

a) 训练和测试信息安全连续性流程、程序和控制措施的功能，保证与信息安全连续性目标相一致；

b) 训练和测试信息安全连续性流程、程序和控制措施的知识和日常操作，保证全心他们的性能五信息安全连续性目标相一致；

c) 当信息系统、信息安全流程、程序和控制措施或业务连续性管理/灾难恢复管理过程和解决方案豪华时，应检查信息安全连续性测量的有效性和效率。

其它信息

信息安全的连续性控制验证不同于一般的信息安全测试和验证，应被执行在更改测试之外。如果可能的话，最好是将信息安全的连续性控制措施验证与组织业务连续性和灾难恢复测试进行整合。

17.2 冗余（新增）

目标：确保信息处理设施的可用性。

17.2.1 信息处理设施的可用性（新增）

控制措施

信息处理设施应当实现足够的冗余，以满足可用性需求。

实施指南

组织应确定信息系统可用性的业务需求。用现有的系统架构无法保证可用性的地方，应考虑冗余部件或结构。

在适用的情况下，冗余信息系统应进行测试以确保故障转移从一个组件到另一个组件工作的打算。

其它信息

冗余的实施可能引起信息和信息系统完整性和机密性的风险，当设计信息系统的时候应予以考虑。

18 符合性

18.1 符合法律和合同要求

目标：避免违反相关信息安全的法律、法规、规章、合同义务以及任何安全要求。

18.1.1 识别使用的法律和合同的要求（原 15.1.1）

控制措施

对每一个信息系统和组织而言，所有相关的法令、法规和合同要求，以及为满足这些要求组织所采用的方法，应加以明确地定义、形成文件并保持更新。

实施指南

为满足这些要求的特定控制措施和人员的职责应同样加以定义并形成文件。

管理者应识别所有为满足他们业务需要的可用的法律法规。如果组织在其它国家开展业务，管理者应考虑所有有关国家的符合性。

18.1.2 知识产权（IPR）（原 15.1.2）

控制措施

应实施适当的程序，以确保在使用具有知识产权的材料和具有所有权的软件产品时，符合法律、法规和合同的要求。

实施指南

在保护被认为具有知识产权的材料时，应考虑下面的指南：

a) 发布一个知识产权符合性策略，该策略定义了软件和信息产品的合法使用；
b) 仅通过知名的和声誉好的渠道获得软件，以确保不侵犯版权；
c) 保持对保护知识产权的策略的意识，并通知对违规人员采取惩罚措施的意向；
d) 维护适当的资产登记簿，识别具有保护知识产权要求的所有资产；
e) 维护许可证、主盘、手册等所有权的证明和证据；
f) 实施控制措施，以确保不超过所允许的最大用户数目；
g) 进行检查，确保仅安装已授权的软件和具有许可证的产品；
h) 提供维护适当的许可证条件的策略；
i) 提供处理软件或转移软件给其他人的策略；
j) 符合从公共网络获得软件和信息的条款和条件；
k) 不对版权法不允许的商业录音带进行复制、格式转换或摘取内容；
l) 不对版权法不允许的书籍、文章、报告和其它文件中进行全部或部分地拷贝。

其它信息

知识产权包括软件或文档的版权、设计权、商标、专利权和源代码许可证。

通常具有所有权的软件产品的供应是根据许可协议进行的，该许可协议规定了许可条款和条件，例如，限制产品用于指定的机器或限制只能拷贝到创建的备份副本上。组织所开发的软件的知识产权的重要性和意识需要跟员工阐述清楚。

法律、法规和合同的要求可以对具有所有权的材料的拷贝进行限制。特别是，这些限制可能要求只能使用组织自己开发的资料，或者开发者许可组织使用或提供给组织的资料。版权侵害可能导致法律行为，这可能涉及罚款和刑事诉讼。

18.1.3 记录的保护（原 15.1.3）

控制措施

按照法律、法规、合同和业务需求保护记录，以免遭受损失、破坏、篡改、未经授权的访问和未授权的发布。

实施指南

当决定保护特定的时候，应考虑基于组织分类规划进行适当的分类。例如，帐号记录、数据库记录、事务日志、审计日志和运行程序，每个程序都带有详细的保存周期和存储介质的类型，例如，纸质、缩微胶片、磁介质、光介质。还应保存与已加密的归档文件或数字签名（见 10）相关的任何有关密码密钥材料，以使得记录在保存期限满后能够脱密。

应考虑存储记录的介质性能下降的可能性。应按照制造商的建议实施存储和处理程序。

若选择了电子存储介质，应建立程序，以确保在整个保存周期内能够访问数据（介质和格式的可读性），以防范由于未来技术变化而造成的损失。

应选择数据存储系统，使得所需要的数据能根据要满足的要求，在可接受的时间内、以可接受的格式检索出来。

存储和处理系统应确保能按照国家或地区法律或法规的规定，清晰地标识出记录及其保存期限。该系统应允许在保存期后恰当地销毁记录，如果组织不需要这些记录的话。

为满足记录防护目标，应在组织范围内采取下列步骤：

a) 应颁发关于保存、存储、处理和处置记录和信息的指南；
b) 应起草一个保存时间计划，以标识记录及其应被保存的时间周期；
c) 应维护关键信息源的清单；

其它信息

某些记录可能需要安全地保存，以满足法令、法规或合同的要求，支持必要的业务活动。举例来说，可以要求这些记录作为组织在法令或法规规则下运行的证据，以确保充分防御潜在的民事或刑事诉讼，或者和股份持有者、外部方和审核员确认组织的财务状况。可以根据国家法律或规章来设置信息保存的时间和数据内容。

关于管理组织记录的更多信息可以参见 ISO 15489-1.[5]。

18.1.4 隐私和个人可识别信息的保护（原 15.1.4）

控制措施

应依照相关的法律、法规和合同条款的要求，确保隐私和个人可识别信息的保护。

实施指南

应制定和实施组织的隐私和个人可识别信息保护的数据策略。该策略应通知到涉及私人可识别信息处理的所有人员。

符合该策略和所有相关的数据保护法律法规需要合适的管理结构和控制。通常，这一点最好通过任命一个负责人来实现，如隐私官员，该官员应向管理人员、用户和服务提供商提供他们各自的职责以及应遵守的特定程序的指南。处理个人可识别信息和确保隐私意识保护原则的职责应根据相关法律法规来确定。应实施适当的技术和组织措施以保护个人可识别信息。

其它信息

ISO/IEC 29100[25] 提供一个在信息和通信技术保护系统中个人可识别信息保护的高层次的框架。一些国家已经立法将个人可识别信息的控制着眼于收集、处理和传输过程中（一般居住的人可以从这个信息中识别出来）。根据各自国家的法律，这样的控制可以对那些收集、处理和传播的个人可识别信息的人承担责任，也可以限制个人信息转移到其他国家的能力。

18.1.5 密码控制措施的监管（原 15.1.6）

控制措施

使用密码控制措施应遵从相关的协议、法律和法规。

实施指南

为符合相关的协议、法律和法规，应考虑下面的事项：

a) 限制执行密码功能的计算机硬件和软件的出入口；
b) 限制被设计用以增加密码功能的计算机硬件和软件的出入口；
c) 限制密码的使用；
d) 利用国家对硬件或软件加密的信息的授权的强制或任意的访问方法提供内容的保密性。

应征求法律建议，以确保符合国家法律法规。在将加密信息或密码控制措施转移越过司法边界之前，也应获得法律建议。

18.2 信息安全审查

目标：确保信息安全依照组织的策略和程序运行和实施。

18.2.1 信息安全的独立审查（原 6.1.8）

控制措施

组织管理信息安全的方法及实施（例如信息安全的控制目标、控制措施、策略、过程和规程）应按照计划的时间间隔或发生重大变更时进行独立评审。

实施指南

独立评审应由管理者启动。对于确保一个组织管理信息安全方法的持续的适宜性、充分性和有效性，这种独立评审是必须的。评审应包括评估安全方法改进的机会和变更的需要，包括策略和控制目标。

这样的评审应由独立于被评审范围的人员执行，例如内部审核部门、独立的管理人员或专门进行这种评审的第三方组织。从事这些评审的人员应具备适当的技能和经验。

独立评审的结果应被记录并报告给启动评审的管理者。这些记录应加以保持。

如果独立评审识别出组织管理信息安全的方法和实施不充分，例如：文档化的目标和要求不满足或不符合信息安全方针文件（见 5.1.1）中声明的信息安全的方向，管理者应考虑纠正措施。

其它信息

ISO/IEC 27007[12], “信息安全管理体系审核指南”和 ISO/IEC TR 27008[13], “信息安全控制措施审核员指南” 也提供了独立评审的指导。

18.2.2 符合安全策略和标准（原 15.2.1）

控制措施

管理者应定期审查其职责范围内的信息安全处理和规程被正确的执行，以确保符合安全策略、标准和其他安全要求。

实施指南

管理者应确定如何来检查在策略、标准和其它合适规程中定义的信息安全要求被满足。自动测量和报告工具应被考虑为有效的定期检查。

如果检查结果发现任何不符合，管理者应：

a) 确定不符合的原因；

b) 评价达到符合所采取措施的必要性；

c) 实施适当的纠正措施；

d) 检查所采取的纠正措施来验证它的有效性，并确定缺陷或弱点。

评审结果和管理者采取的纠正措施应被记录，且这些记录应予以维护。当在管理者的职责范围内进行独立评审时，管理者应将结果报告给执行独立评审的人员（见 18.2.1）。

其它信息

12.4中包括了系统使用的运行监视。

18.2.3 技术符合性检查（原 15.2.2）

控制措施

应定期检查信息系统与组织安全策略和标准的符合性。

实施指南

技术符合性检查应优选自动化工具的支持，生成由技术专家后续解释的技术报告。另外，手动检查（如果需要的话，通过适当的软件工具的支持）由有经验的系统工程师执行。

如果使用渗透测试或脆弱性评估，则应格外小心，因为这些活动可能导致系统安全的

损害。这样的测试应预先计划、形成文件和可重复的。

任何技术符合性检查应仅由有能力的、已授权的人员或在他们的监督下完成。

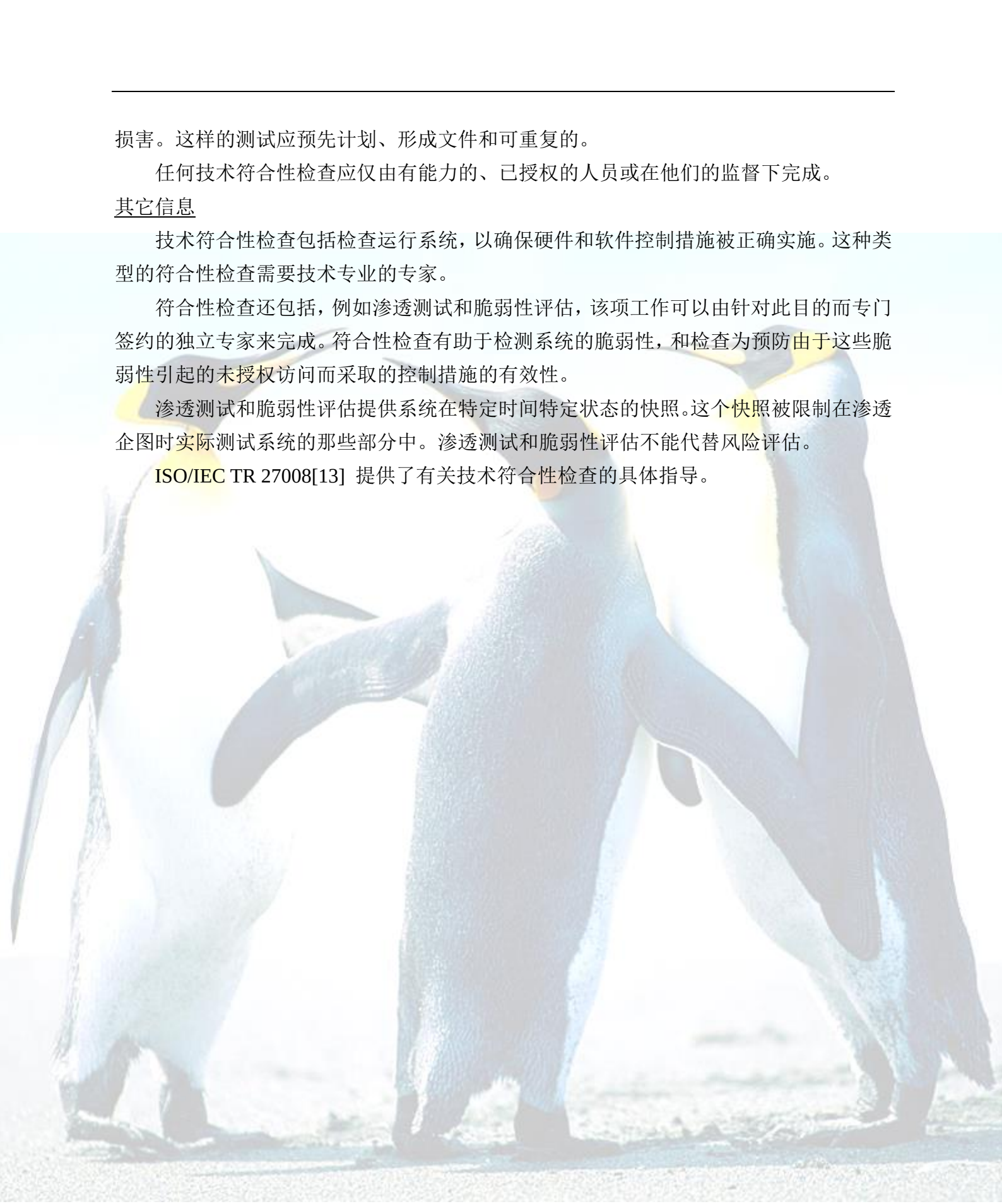
其它信息

技术符合性检查包括检查运行系统，以确保硬件和软件控制措施被正确实施。这种类型的符合性检查需要技术专业的专家。

符合性检查还包括，例如渗透测试和脆弱性评估，该项工作可以由针对此目的而专门签约的独立专家来完成。符合性检查有助于检测系统的脆弱性，和检查为预防由于这些脆弱性引起的未授权访问而采取的控制措施的有效性。

渗透测试和脆弱性评估提供系统在特定时间特定状态的快照。这个快照被限制在渗透企图时实际测试系统的那些部分中。渗透测试和脆弱性评估不能代替风险评估。

ISO/IEC TR 27008[13] 提供了有关技术符合性检查的具体指导。



Bibliography

[1] ISO/IEC Directives, Part 2

[2] ISO/IEC 11770-1, *Information technology Security techniques — Key management — Part 1: Framework*

[3] ISO/IEC 11770-2, *Information technology — Security techniques — Key management — Part 2:Mechanisms using symmetric techniques*

[4] ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3:Mechanisms using asymmetric techniques*

[5] ISO 15489-1, *Information and documentation — Records management — Part 1: General*

[6] ISO/IEC 20000-1, *Information technology — Service management — Part 1: Service management system requirements*

[7] ISO/IEC 20000-2,1)*Information technology — Service management — Part 2: Guidance on the application of service management systems*

[8] ISO 22301, *Societal security — Business continuity management systems — equirements*

[9] ISO 22313, *Societal security — Business continuity management systems — Guidance*

[10] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[11] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[12] ISO/IEC 27007, *Information technology — Security techniques — Guidelines for information security management systems auditing*

[13] ISO/IEC TR 27008, *Information technology — Security techniques — Guidelines for auditors on information security controls*

[14] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[15] ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

[16] ISO/IEC 27033-2, *Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security*

[17] ISO/IEC 27033-3, *Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues*

[18] ISO/IEC 27033-4, *Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways*

[19] ISO/IEC 27033-5, *Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Network (VPNs)*

[20] ISO/IEC 27035, *Information technology — Security techniques — Information security incident management*

[21] ISO/IEC 27036-1, *Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts*

1) ISO/IEC 20000-2:2005 has been cancelled and replaced by ISO/IEC 20000-2:2012, *Information technology — Service management — Part 2: Guidance on the application of service management systems*.

[22] ISO/IEC 27036-2, *Information technology — Security techniques — Information security for supplier relationships — Part 2: Common requirements*

[23] ISO/IEC 27036-3, *Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for ICT supply chain security*

[24] ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*

[25] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

[26] ISO/IEC 29101, *Information technology — Security techniques — Privacy architecture framework*

[27] ISO 31000, *Risk management — Principles and guidelines*