ICS 35.040
L 80

中华人民共和国国家标准

GB/T 22081—2016/ISO/IEC 27002:2013
代替 GB/T 22081—2008

信息技术　安全技术
信息安全控制实践指南

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

(ISO/IEC 27002:2013,IDT)

2016-08-29 发布　　2017-03-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 22081—2008《信息技术　安全技术　信息安全管理实用规则》。

本标准与 GB/T 22081—2008 相比，主要技术变化如下：

——结构变化见附录 NA；

——术语变化见附录 NB。

本标准使用翻译法等同采用 ISO/IEC 27002:2013《信息技术　安全技术　信息安全控制实践指南》及其相应的技术勘误(ISO/IEC 27002:2013/COR 1:2014)。

与本标准中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/T 29246—2012　信息技术　安全技术　信息安全管理体系　概述和词汇(ISO/IEC 27000:2009,IDT)。

本标准做了下列编辑性修改：

——增加了资料性附录 NA；

——增加了资料性附录 NB。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：中国电子技术标准化研究院、中电长城网际系统应用有限公司、中国信息安全认证中心、山东省标准化研究院、广州赛宝认证中心服务有限公司、北京江南天安科技有限公司、上海三零卫士信息安全有限公司、中国合格评定国家认可中心、北京时代新威信息技术有限公司、黑龙江电子信息产品监督检验院、浙江远望电子有限公司、杭州在信科技有限公司。

本标准主要起草人：许玉娜、上官晓丽、闵京华、尤其、公伟、卢列文、倪文静、王连强、陈冠直、于惊涛、付志高、赵英庆、卢普明、王曙光、虞仲华、韩硕祥、魏军、程瑜琦、孔祥林、邬敏华、李华、李阳。

本标准所代替标准的历次版本发布情况为：

——GB/T 22081—2008。

引　言

0.1　背景和环境

本标准可作为组织基于 GB/T 22080[10] 实现信息安全管理体系(ISMS)过程中选择控制时的参考，或作为组织在实现通用信息安全控制时的指南。在考虑具体信息安全风险环境后，本标准也可用于制定特定行业和特定组织的信息安全管理指南。

所有类型和规模的组织(包括公共和私营部门、商业组织、非盈利性组织)都会收集、处理、存储和传输包括电子、物理和语音(如会谈和演讲)等多种形式的信息。

信息的价值超越文字、数字和图像的本身，例如：知识、概念、观点和品牌都是无形信息。在互联世界中对于组织业务而言，信息和相关过程、系统、网络及其操作、处理与保护活动中所涉及的人员都是资产，与其他重要的业务资产一样，对组织的业务至关重要，因此值得或需要保护以防范各种危害。

资产易遭受故意和意外的威胁；且相关的过程、系统、网络和人员均有其固有脆弱性。业务过程和系统的变更或其他外部变更(如新的法律法规)可能产生新的信息安全风险。因此，考虑到威胁利用脆弱性损害组织的途径多种多样，信息安全风险始终存在。有效的信息安全通过防范威胁和脆弱性使组织得到保护来减少风险，从而降低对其资产的影响。

信息安全可通过实现一组合适的控制来达到，包括策略、过程、规程、组织结构和软硬件功能。必要时，需要建立、实现、监视、评审和改进这些控制，以确保其满足组织特定的安全和业务目标。GB/T 22080[10] 规定的 ISMS 采用整体的、协调的观点看待组织的信息安全风险，以便在一致的管理体系总体框架下实现一套全面的信息安全控制。

从 GB/T 22080[10] 和本标准来看，许多信息系统的设计未达到是安全的。通过技术手段可获得的安全是有限的，宜通过适当的管理和规程给予支持。确定哪些控制应该存在，这需要仔细规划并注意细节。一个成功的信息安全管理体系需要得到组织内的所有员工的支持，股东、供应商或其他外部各方的参与，也需要外部各方的专家建议。

在更一般的意义上，有效的信息安全也向管理者及其他相关方保证组织资产处于合理的安全，并受到保护不被损害，因此其角色等同于业务推动者。

0.2　信息安全要求

组织识别其安全要求是必要的。安全要求的 3 个主要来源是：

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

b)　组织及其贸易伙伴、合同方和服务提供商必须满足的法律、法规、规章制度和合同要求，以及他们的社会文化环境；

c)　组织为支持其运行，针对信息的操作、处理、存储、通信和归档而建立的原则、目标和业务要求。

实现控制所使用的资源，必须权衡缺少这些控制而导致的安全问题以及可能导致的业务危害。风险评估的结果将有助于指导和确定合适的管理措施、信息安全风险管理的优先级以及为防范这些风险所选择控制实现的优先级。

ISO/IEC 27005[11] 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、风险沟通、风险监视和风险评审各方面的建议。

0.3 控制的选择

控制可以选自本标准或其他控制集，或适当时针对特定的需求设计新的控制。

控制的选择取决于组织决策，该决策基于风险接受准则、风险处置选项、组织采用的通用风险管理方法；控制的选择也必须遵守所有相关的国家法律法规。同时控制的选择也取决于控制交互方式以提供纵深防御。

本标准中的某些控制可被当作信息安全管理的指导原则，并且可用于大多数组织。在每个控制之下，详细地给出了其实现指南。有关选择控制的更详细信息以及其他的风险的处置选项，可参见ISO/IEC 27005[11]。

0.4 编制组织自己的指南

本标准可作为组织制定其特定指南的起点。对一个组织来说，本标准中的控制和指南并非全部适用。另外，可能还需要增加一些不包含在本标准中的控制和指南。当制定包含一些增加的控制和指南的组织文件时，给出一些对本标准可用条款的交叉应用，这可能是有用的，以支持审核员和和业务伙伴的符合性检查。

0.5 生命周期的考虑

信息有其固有的生命周期，即从其创建和产生，经过存储、处理、使用和传输到其最终销毁或消失。在其生命周期中，信息资产的价值和所面临的风险可能会变化(如在公司账目正式公布后，对它的窃取和未授权泄露所产生的危害将极大的降低)，但在所有阶段，信息安全仍存在一定程度的重要性。

信息系统的生命周期包括构思、规约、设计、开发、测试、实现、使用、维护，并最终退役和销毁。在每一阶段均应考虑到信息安全。在每一阶段上均应考虑信息安全。开发新的系统或对现有系统的改变，为组织升级和改进安全控制提供了机会，同时应考虑实际的安全事件以及当前和预测的信息安全风险。

0.6 相关标准

本标准就一个广泛的、可通用于不同组织的信息安全控制集，提供了相应的指南；而信息安全管理体系标准族中的其他标准就信息安全管理全过程的其他方面提供了补充建议或要求。

信息安全管理体系标准的总体介绍参见ISO/IEC 27000。ISO/IEC 27000中提供的词汇表确定了信息安全管理体系标准中使用的绝大部分术语，并描述了每个标准的范围和目标。

信息技术　安全技术
信息安全控制实践指南

1　范围

本标准为组织的信息安全标准和信息安全管理实践提供了指南，包括考虑了组织信息安全风险环境的控制的选择、实现和管理。

本标准被设计用于组织：

a）　选择控制，即基于GB/T 22080[10]，在实现一个信息安全管理体系的过程中选择控制；

b）　实现通用的、可接受的信息安全控制；

c）　制定组织自己的信息安全管理指南。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

ISO/IEC 27000　信息技术　安全技术　信息安全管理体系　概述和词汇(Information technology—Security techniques—Information security management systems—Overview and vocabulary)。

3　术语和定义

ISO/IEC 27000界定的术语和定义适用于本文件。

4　标准结构

本标准包括14个安全控制的章节，共含有35个主要安全类别以及114项控制。

4.1　章节

定义安全控制的每个章节，包含一个或多个主要安全类别。

本标准中各章节的顺序不表示其重要性。根据不同的环境，任何或所有章节中的安全控制都可能是重要的，因此应用本标准的每一个组织，宜识别可应用的控制，这些控制多么重要，以及它们如何应用到各个业务过程。另外，本标准的列表没有优先顺序。

4.2　控制类别

每一个主要安全控制类别包括：

a）　一个控制目标，声明要实现什么；

b）　一个或多个控制，可被用于实现该控制目标。

控制的描述结构如下：

控制

为满足控制目标，给出定义特定控制的陈述。

实现指南

为支持该控制的实现并满足控制目标，提供更详细的信息。该指南可能不能完全适用或不足以在所有情况下适用，也可能不能满足组织的特定控制要求。

其他信息

提供需要考虑的进一步的信息，例如法律方面的考虑和对其他标准的参考。如无其他信息，本项将不给出。

5 信息安全策略

5.1 信息安全管理指导

目标：依据业务要求和相关法律法规，为信息安全提供管理指导和支持。

5.1.1 信息安全策略

控制

信息安全策略集宜被定义，由管理者批准，并发布、传达给所有员工和外部相关方。

实现指南

在最高层上，组织宜定义一个“信息安全方针”，该方针宜获得管理层批准，并建立组织管理其信息安全目标的方法。

信息安全方针宜关注下列方面产生的要求：

a) 业务战略；

b) 法律、法规和合同；

c) 当前和预期的信息安全威胁环境。

该信息安全方针宜包括涉及以下内容的陈述：

a) 信息安全、目标和原则的定义，以指导所有信息安全有关的活动；

b) 把信息安全管理方面的一般和特定责任的分配给已定义的角色；

c) 处理偏差和意外的过程。

在较低层面，该信息安全策略宜由特定主题的策略予以支持，这些策略进一步强制性地规定了信息安全控制的实现，并通常是结构化的，以强调组织内某些目标群体需求或涵盖某些主题。

例如，这样的策略主题包括：

a) 访问控制(见第 9 章)；

b) 信息分级(和处理)(见 8.2)；

c) 物理和环境安全(见第 11 章)；

d) 面向终端用户的策略，如：

   1) 资产的可接受使用(见 8.1.3)；

   2) 桌面和屏幕的清理(见 11.2.9)；

   3) 信息传输(见 13.2.1)；

   4) 移动设备和远程工作(见 6.2)；

   5) 软件安装及其使用限制(见 12.6.2)；

e) 备份(见 12.3)；

f) 信息传输(见 13.2)；

g) 恶意软件防范(见 12.2)；

h) 技术脆弱性管理(见 12.6.1)；

i) 密码控制(见第 10 章);

j) 通信安全(见第 13 章);

k) 隐私及其个人可识别信息的保护(见 18.1.4);

l) 供应商关系(见第 15 章)。

这些策略宜采用预期读者适合的、可访问和可理解的形式传达给员工和外部相关方,例如,在“信息安全意识、教育和培训”(见 7.2.2)环境下。

其他信息

内部信息安全策略的需求因组织而异。内部策略对于大型和复杂的组织而言尤其有用,当这些组织中确定和批准控制预期水平的人员与实现控制的人员是分离的,或者当内部策略应用在组织不同的人员或职能时,也是非常有用的。信息安全策略可以以单一“信息安全策略”文件的形式发布,或作为各不相同但相互关联的一套文件的形式发布。

如果信息安全策略在组织外进行分发,宜注意不要泄露保密信息。

一些组织使用其他术语用于这些策略文件,例如“标准”“导则”或“规则”。

5.1.2 信息安全策略的评审

控制

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

实现指南

每个策略宜有专人负责,他对策略的制定、评审和评价具有被批准的管理责任。评审宜包括评估组织策略和信息安全管理方法的改进机会,以适应组织环境、业务状况、法律法规或技术环境发生的变化。

信息安全策略评审宜考虑管理评审的结果。

宜获得管理层对修订的策略的批准。

6 信息安全组织

6.1 内部组织

目标:建立一个管理框架,以启动和控制组织内信息安全的实现和运行。

6.1.1 信息安全的角色和责任

控制

所有的信息安全责任宜予以定义和分配。

实现指南

信息安全责任的分配宜与信息安全策略(见 5.1.1)相一致。各个资产的保护责任和执行特定安全过程的责任宜被清晰地标识。宜定义信息安全风险管理活动的责任,特别是接受残余风险的责任。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。宜定义本地资产保护和执行特定安全过程的责任。

被分配了信息安全责任的个体可以将安全任务委托给其他人员。尽管如此,他们仍然负有责任,并且他们宜确定任何被委托的任务是否已被正确地执行。

宜指明个体负责的领域。特别是,宜进行下列工作:

a) 识别和定义资产和信息安全过程;

b) 指定每一资产或安全过程的责任实体,并且该责任的细节要形成文件(见 8.1.2);

c) 定义授权级别并形成文件；

d) 被任命的个体宜具备信息安全领域的能力且被给予机会以跟进相关发展，使其能够履行信息安全领域责任；

e) 宜对供应商关系中信息安全方面的监督和协调予以识别，并形成文件。

其他信息

在许多组织中，将任命一名信息安全管理人员全面负责安全的开发实现，并支持控制的识别。

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

6.1.2 职责分离

控制

宜分离冲突的职责及其责任范围，以减少未授权或无意的修改或者不当使用组织资产的机会。

实现指南

宜注意，任何人都不能在非授权或不被监视的情况下访问、修改和使用资产。宜把一活动的启动与其授权相分离。在设计该控制时，宜考虑勾结的可能性。

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、审核踪迹和管理监督等。

其他信息

职责分离是一种降低意外或蓄意滥用组织资产的风险的方法。

6.1.3 与职能机构的联系

控制

宜维护与相关职能机构的适当联系。

实现指南

组织宜有规程指明什么时候与哪个职能机构(例如，执法部门、法规部门、监管部门)进行联系，以及如何及时报告已识别的信息安全事件(例如，已识别的信息安全事件可能很触犯了法律)。

其他信息

受到来自互联网的攻击组织可能需要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(第16章)或业务连续和应急计划过程(第17章)的要求。与法规部门的联系还有助于预先知道组织必须实现的法律法规方面预期的变化，并进行预先准备。与其他部门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(关系到业务连续性)、电信提供商(关系到路由和可用性)、供水部门(关系到设备的冷却设施)。

6.1.4 与特定相关方的联系

控制

宜维护与特定相关方、其他专业安全论坛和专业协会的适当联系。

实现指南

宜考虑把特定的相关方或论坛中的成员关系作为一种手段，来：

a) 增进最佳实践的知识，掌握最新相关安全信息；

b) 确保了解的信息安全环境是最新的和全面的；

c) 获取以前的有关攻击和脆弱性的预警、公告和补丁；

d) 获得信息安全专家的建议；

e) 共享和交换关于新的技术、产品、威胁或脆弱性的信息；

f) 当处置信息安全事件时，提供适当的联络点(第16章)。

其他信息

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

6.1.5 项目管理中的信息安全

控制

宜关注项目管理中的信息安全问题，无论何种类型的项目。

实现指南

宜把信息安全整合到组织的项目管理方法中，作为项目的一部份，以确保识别并强调了信息安全风险。这通常可应用于所有项目，无论其特征是什么，例如核心业务过程、IT、设施管理和其他支持过程等方面的项目。使用的项目管理方法宜要求：

a) 信息安全目标被纳入项目目标；

b) 为识别必要的控制，在项目的早期阶段宜进行信息安全风险评估；

c) 信息安全作为所采用的项目管理方法各个阶段的一部分。

在所有项目中宜解决和定期评审信息安全问题。宜定义信息安全责任，并分配给在项目管理方法中定义的特定角色。

6.2 移动设备和远程工作

目标：确保移动设备远程工作及其使用的安全。

6.2.1 移动设备策略

控制

宜采用相应的策略及其支持性的安全措施以管理由于使用移动设备所带来的风险。

实现指南

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

移动设备策略宜考虑：

a) 移动设备的注册；

b) 物理保护的要求；

c) 软件安装的限制；

d) 移动设备软件版本和应用补丁的要求；

e) 连接到信息服务的限制；

f) 访问控制；

g) 密码技术；

h) 恶意软件防范；

i) 远程禁用、删除或锁定；

j) 备份；

k) Web服务和Web应用程序的使用。

当在公共场所、会议室和其他不受保护的区域使用移动计算设备时，宜加以小心。为避免未授权访问或泄露这些设备所存储和处理的信息，宜有适当的保护，例如使用密码技术(见第10章)和强制使用秘密鉴别信息(见9.2.4)。

还宜对移动设备进行物理保护，以防被偷窃，例如，特别是遗留在汽车和其他形式的运输工具上、旅

馆房间、会议中心和会议室。宜为移动设备的被窃或丢失等情况建立一个符合法律、保险和组织的其他安全要求的特定规程。携带重要、敏感或关键业务信息的设备不宜无人值守，若有可能，宜以物理的方式锁起来，或使用专用锁来保护设备。

宜安排使用移动设备的人员进行培训，以提高他们对这种工作方式导致的附加风险和所实现的控制的了解。

当移动设备策略允许使用私人移动设备时，策略和相关的安全措施宜考虑：

a) 分离设备的私人和业务使用，包括使用软件来支持这种分离并保护在私人设备上的业务数据；
b) 仅在以下情况提供对业务信息的访问：用户签订最终用户协议知晓其职责（物理保护、软件升级等）；放弃业务数据的所有权；允许组织远程擦除数据在设备被盗或丢失时、或不再授权使用该服务时。本策略需要考虑隐私方面的法律法规。

其他信息

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

a) 一些无线安全协议是不成熟的，并有已知的弱点；
b) 因为受限的网络带宽或因为移动设备在规定的备份时间未能连接网络，在移动设备上存储的信息可能不能备份。

移动设备通常与固定使用设备享用相同的功能，如联网、互联网接入、电子邮件和文件处理。移动设备上的信息安全控制通常包含固定使用设备上采用的措施和为解决在组织场地之外使用带来的威胁而采用的措施。

6.2.2 远程工作

控制

宜实现相应的策略及其支持性的安全措施，以保护在远程工作地点上所访问的、处理的或存储的信息。

实现指南

允许远程工作活动的组织宜发布策略，以定义使用远程工作的条件和限制。当认为适用且法律允许时，宜考虑下列事项：

a) 远程工作场地的现有物理安全，要考虑到建筑物和本地环境的物理安全；
b) 推荐的物理的远程工作环境；
c) 通信安全要求，要考虑远程访问组织内部系统的需要、被访问的并在通信链路上传递的信息的敏感性以及内部系统的敏感性；
d) 提供虚拟桌面访问以防止在私人设备上处理和存储信息；
e) 住处的其他人员（例如，家人和朋友）未授权访问信息或资源的威胁；
f) 家庭网络的使用和无线网络服务配置的要求或限制；
g) 针对私有设备开发的预防知识产权争论的策略和规程；
h) 对私人设备的访问（以验证机器安全或开展调查）可能是被法律禁止的；
i) 使组织对员工或外部相关方人员等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) 恶意软件防范和防火墙要求。

考虑的指南和安排宜包括：

a) 当不允许使用不在组织控制下的私人设备时，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、可以保持的信息分级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) 提供硬件和软件支持和维护;
g) 提供保险;
h) 用于备份和业务连续性的规程;
i) 审核和安全监视;
j) 当远程工作活动终止时,撤销授权和访问权,并返回设备。

其他信息

远程工作指的是办公室以外的所有形式的工作,包括非传统工作环境比如那些被称为“远程办公”“弹性工作场所”“远地工作”和“虚拟工作”环境。

7 人力资源安全

7.1 任用前

目标:确保员工和合同方理解其责任,并适合其角色。

7.1.1 审查

控制

宜按照相关法律法规和道德规范,对所有任用候选者的背景进行验证核查,并与业务要求、访问信息的等级和察觉的风险相适宜。

实现指南

验证宜考虑所有相关的隐私、个人身份信息的保护以及与任用相关的法律,且允许时,宜包括以下内容:

a) 有效的可接受的推荐材料(例如,企业出具和个人出具的文字材料);
b) 申请人履历的验证(针对该履历的完备性和准确性);
c) 声称的学历、专业资质的证实;
d) 独立的个人身份验证(护照或类似文件);
e) 更多细节的验证,例如信用核查或犯罪记录核查。

当组织聘用人员担任一个特定的信息安全角色时,组织宜确认该候选人,是否:

a) 具有执行该安全角色所必须的能力;
b) 可被信任担任该角色,特别是当该角色对组织是十分重要的。

当为一项工作所初始任命的或晋升的人员有权访问信息处理设施,特别是如果该设施正在处理保密信息,例如,财务信息或高度保密的信息,该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,例如谁有资格审查人员,以及如何、何时、为什么执行验证评审。

宜确保对合同方人员审查的过程。在这种情况下,组织和合同方的协议宜规定执行审查的责任,以及当审查未完成或审查结果引起怀疑或关注时,需遵守的通告规程。

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

7.1.2 任用条款及条件

控制

宜在员工和合同方的合同协议中声明他们和组织对信息安全的责任。

实现指南

员工或合同方的合同义务宜反映组织的信息安全策略，并澄清和声明：

a) 所有访问保密信息的员工和合同方人员宜在给予访问信息处理设施权限之前签署保密或不泄露协议(见 13.2.4)；

b) 员工、合同方的法律责任和权利，例如关于版权法、数据保护法(见 18.1.2 和 18.1.4)；

c) 信息分级的责任，以及对与由员工或合同方处理的信息、信息处理设施和信息服务有关的其他资产进行管理的责任(见第 8 章)；

d) 雇员或合同方处理来自其他公司或外部方的信息的责任；

e) 雇员或合同方漠视组织的安全要求所要采取的措施(见 7.2.3)。

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。

组织宜确保员工和合同方同意与信息安全相关的条款和条件，这些条款和条件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。

若适用，包含于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 7.3)。

其他信息

一个行为准则可用来陈述员工或合同方有关保密性、数据保护、道德规范、组织设备和设施的适当使用等方面的责任，以及组织所期望的良好实践。在合同协议中，与合同方有关的外部方能被要求作为合同方的代表。

7.2 任用中

目标：确保员工和合同方意识到并履行其信息安全责任。

7.2.1 管理责任

控制

管理层宜要求所有员工和合同方按照组织已建立的策略和规程应用信息安全。

实现指南

管理责任宜包括确保员工和合同方：

a) 在被允许访问保密信息或信息系统前了解其信息安全角色和责任；

b) 获取了声明其组织角色的信息安全期望的指南；

c) 受到激励以实现组织的信息安全策略；

d) 对于他们在组织内的角色和责任相关的信息安全意识达到一定程度(见 7.2.2)；

e) 遵守任用的条款和条件，包括组织的信息安全策略和适当的工作方法；

f) 保持适当的技能和资质，并定期接受教育；

g) 提供违反信息安全策略或规程的匿名报告通道(“举报”)。

管理层宜展示出对信息安全策略、规程和控制的支持，并以身作则。

其他信息

如果不使员工和合同方了解他们的信息安全责任，他们就可能组织造成相当大的破坏。得到激励的人员可能是更可靠的并能减少信息安全事件的发生。

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

7.2.2 信息安全意识、教育和培训

控制

组织所有员工和相关的合同方，宜按其工作职能，接受适当的意识教育和培训，及组织策略及规程

的定期更新的信息。

实现指南

信息安全意识培训方案旨在使员工,适当时,包括合同方,了解他们的信息安全责任以及免责的方法。

信息安全意识方案宜按照组织的信息安全策略和相关规程建立,考虑组织要保护的信息以及为保护这些信息所实现的控制。意识方案宜包括一些意识提升活动,像组织宣传活动(例如"信息安全日")、发行宣传册或制作简报等。

宜考虑组织中的员工角色,相关时还需考虑组织对合同方意识的期望来规划意识方案。宜随时间安排,最好定期安排意识方案中的活动,以便活动可以重复并覆盖新的员工和合同方。意识方案宜根据组织的策略和规程定期更新,并宜汲取信息安全事件的经验教训。

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

信息安全教育和培训宜覆盖一般方面,例如:

a) 在整个组织范围内说明管理层对信息安全的承诺;
b) 熟悉并遵从适用的信息安全规则和义务的要求,正如策略、标准、法律、法规、合同和协议中所定义的;
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外部方的信息的安全的一般责任;
d) 基本的信息安全规程(例如信息安全事件报告)和基线控制(例如口令安全、恶意软件控制和清空桌面);
e) 可得到关于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教育和培训材料。

信息安全教育和培训宜定期进行。初始的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员工,且宜在其开展工作前进行培训。

为有效进行教育和培训,组织宜制定信息安全意识培训方案。该方案宜与组织的信息安全策略和相关规程保持一致,并考虑组织要予保护的信息以及为保护这些信息已实现的控制。该方案宜考虑教育和培训的不同形式,例如讲座或自学。

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"。员工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,也很重要。

意识、教育和培训可以是其他培训活动的一部分,或与之协同开展,例如通用信息技术或通用安全培训。意识、教育和培训活动宜适于并与个人的角色、责任和技能相关。

在意识、教育和培训课程结束时,可评估员工的理解情况,以测试知识传递效果。

7.2.3 违规处理过程

控制

宜有正式的、且已被传达的违规处理过程以对信息安全违规的员工采取措施。

实现指南

在没有验证信息安全违规已经发生之前(见 16.1.7),不能开始该违规处理过程。

正式的违规处理过程宜确保对被怀疑信息安全违规的员工,给予了正确和公平的对待。无论违规是第一次或是已发生过,无论违规者是否经过适当地培训,正式的违规处理过程宜规定一个处理程度的响应,要考虑例如违规的性质、重要性及对于业务的影响等因素,相关法律、业务合同和其他因素等。

违规处理过程也可用于对员工的一种威慑,防止他们违反组织的信息安全策略和规程及其他信息安全违规。故意的违规可能需要立刻采取相应的措施。

其他信息

如果对值得注意的信息安全行为定义了一些主动地惩罚，那么违规处理过程还可能成为一种动力或激励。

7.3 任用的终止和变更

目标：在任用变更或终止过程中保护组织的利益。

7.3.1 任用终止或变更的责任

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职责，传达至员工或合同方并执行。

实现指南

责任终止的传达宜包括正在进行的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责任(见 13.2.4)，并且在员工、合同方雇佣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)。

责任及其职责在任用终止后仍然有效的内容宜包含在员工、合同方的合同条款及条件中(见 7.1.2)。

当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。

其他信息

人力资源的职能通常是与管理相关规程的安全方面的监督管理员一起负责总体的任用终止处理。在外部方提供合同方的情况下，责任终止的处理可能由该外部方根据组织与外部方的协议处理。

有必要通知员工、顾客、合同方关于组织人员的变更和运营上的安排。

8 资产管理

8.1 有关资产的责任

目标：识别组织资产并定义适当的保护责任。

8.1.1 资产清单

控制

宜识别信息，以及与信息和信息处理设施相关的其他资产，并编制和维护这些资产的清单。

实现指南

组织宜识别与信息生命周期相关的资产并将资产的重要性形成文件。信息生命周期宜包括创建、处理、存储、传输、删除和销毁。适当时，宜将专有的或现有的资产清单形成文件并维护。

资产清单宜准确，实时更新并与其他清单一致。

宜为每项已识别的资产指定所属关系(见 8.1.2)并分级(见 8.2)。

其他信息

资产清单有助于确保形成有效的资产保护，还可以基于诸如健康与安全、保险或财务(资产管理)等原因，要求该清单具有其他意图。

ISO/IEC 27005[11]提供了识别资产时组织可能需要考虑的资产示例。编制资产清单的过程是风险管理的重要前提条件(见 ISO/IEC 27000，ISO/IEC 27005[11])。

8.1.2 资产的所属关系

控制

宜维护资产清单中资产的所属关系。

实现指南

对资产生命周期具有被认可的管理责任的个人和其他实体有资格被指定为资产拥有者。

确保及时分配资产所属关系的过程要经常被实现。资产在创立或转移到组织时宜分配其所有权。资产被创建或转移到组织时,宜指定拥有者。资产拥有者宜对资产的整个生命周期负有适当的管理责任。

资产拥有者宜:

a) 确保资产登记造册;

b) 确保对资产进行了适当的分级和保护;

c) 考虑适用的可用的访问控制策略,定义并定期评审对重要资产的访问限制和分级;

d) 确保资产在删除或销毁时进行了合适的处置。

其他信息

已识别的拥有者可以是一个人或一个实体,其对控制资产的整个生命周期负有管理责任。已识别的拥有者没有必要拥有资产产权。

例行任务可以被委派,例如委派给一个管理员日常看管资产,但该拥有者仍然要承担责任。

在复杂的信息系统中,可以用资产分组来协同工作以提供特定服务。在此情况下,服务拥有者要为服务交付负责,包括其资产的运行。

8.1.3 资产的可接受使用

控制

宜识别可接受的信息使用规则,以及与信息和信息处理设施有关的资产的可接受的使用规则,形成文件并加以实现。

实现指南

使用或拥有组织资产访问权的员工和外部方用户,宜知晓组织信息的信息安全要求,以及组织与信息、信息处理和资源相关的其他资产的信息安全要求。他们宜对其使用任何信息处理资源以及在其责任下进行的任何使用负责。

8.1.4 资产归还

控制

所有员工和外部用户在任用、合同或协议终止时,宜归还其占用的所有组织资产。

实现指南

终止过程宜被正式化,包括归还所有先前发出的组织拥有的或被委托的物理的和电子的资产。

当员工或外部方用户购买了组织的设备或使用他们自己人员设备时,宜遵循该规程确保所有相关的信息已移交给组织,并且这些信息已从那些设备中安全地删除(见 11.2.7)。

当员工或外部方用户拥有的知识对正在进行的操作非常重要时,那么这样的信息宜形成文件并移交给组织。

在终止通知期间,组织宜控制被终止合作的员工和合同方对相关信息(如知识产权)的未授权拷贝。

8.2 信息分级

目标:确保信息依据其对组织的重要程度受到适当水平的保护。

8.2.1 信息的分级

控制

信息宜按照法律要求、价值、重要性及其对未授权泄露或修改的敏感性进行分级。

实现指南

信息的分级及相关保护控制宜考虑到共享或限制信息的业务需求和法律要求。非信息类的资产的分级也可与该资产存储、处理或保护的信息分级保持一致。

信息资产的拥有者宜对其分级负责。

分级方案宜包含当时的分级规则和当时的分级评审准则。宜通过分析考虑到的信息的保密性、完整性和可用性以及其他任何要求,以评估方案的保护级别。该方案宜与访问控制策略一致(见 9.1.1)。

宜命名每个不同的级别,以便给出在该分级方案应用语境中的含义。

方案宜在整个组织中保持一致,以便每个人以同样的方式对信息和相关资产进行分级,对保护要求有相同的理解,并应用适当的保护。

组织的过程宜包含分级,并在组织中保持一致和协调。分级的结果宜体现资产的价值,该价值取决于资产对组织的敏感性和重要性,例如,依据保密性、完整性和可用性。分级结果宜根据资产在其生命周期中的价值、敏感性和重要性的变化进行更新。

其他信息

分级为处理信息的人员提供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。这一途径减少了逐项的风险评估和客户化控制设计的需求。

在一段时间后,信息可能不再是敏感的或关键的,例如,当该信息已经公开时。这些方面宜予以考虑,因为过多的分级致使实现不必要的控制,从而导致附加成本,相反,若缺乏有效的分级,就可能损害业务目标的实现。

以下给出了一个四级信息保密性分级方案示例:

a) 泄露不造成损害;

b) 泄露造成轻微的困境或操作不便;

c) 泄露对于运行和战术目标造成重大的短期影响;

d) 泄露对长期战略目标造成了严重影响,或对组织的生存造成风险。

8.2.2 信息的标记

控制

宜按照组织采用的信息分级方案,制定并实现一组适当的信息标记规程。

实现指南

信息标记的规程需要涵盖物理和电子格式的信息及其相关资产。该标记宜反映 8.2.1 中所建立的分级方案。标记宜易于识别。该规程宜考虑信息被访问的方式或资产根据其介质类型被处理的方式,对标记的位置和方式给出指导。该规程可规定省略标记的情形,例如省略非保密信息的标记,以减少工作量。宜使员工和合同方了解标记规程。

包含分级为敏感或关键信息的系统输出宜带有合适的分级标记。

其他信息

分级信息的标记是实现信息共享的一个关键要求。物理标签和元数据标签是常见的标记形式。

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,从而被内部人员或外部攻击者窃取。

8.2.3 资产的处理

控制

宜按照组织采用的信息分级方案,制定并实现资产处理规程。

实现指南

宜建立信息操作、处理、存储和传输的规程，并与其分级（见 8.2.1）保持一致。

宜考虑以下：

a） 支持每个级别的保护要求的访问限制；

b） 对资产授权接受者的正式记录的维护；

c） 对信息的临时或永久拷贝的保护，与原始信息的保护级别一致；

d） 符合制造商说明书的 IT 资产存储；

e） 清晰地标记介质的所有拷贝，以便引起已授权接受者的关注。

不同组织的分级方案可能不尽相同，即使其分级名称相似。另外，在组织间传递的信息的分级根据其在不同组织的情境可能发生变化，即使分级方案完全相同。

包含信息共享的与其他组织的协议宜包含识别信息分级的规程和诠释其他组织信息分级标记的规程。

8.3 介质处理

目标：防止存储在介质中的信息遭受未授权的泄露、修改、移除或破坏。

8.3.1 移动介质的管理

控制

宜按照组织采用的分级方案，实现移动介质管理规程。

实现指南

对于可移动介质的管理，宜考虑下列指南：

a） 如果组织不再需要可重用的介质，该介质离开组织时，宜使其内容不可恢复；

b） 在必要并可行时，对从组织取走介质宜要求得到授权，并保存取走的记录，以维护审核踪迹；

c） 要将所有介质存储在符合制造商说明书的安全、保密的环境中；

d） 若数据的保密性和完整性是重要的考虑因素，宜使用密码技术保护可移动介质中的数据；

e） 当数据仍然需要时，为降低其存储介质老化的风险，宜在数据变成不可读前，将其转移至新的介质中；

f） 有价值数据的多个拷贝宜分开存储在不同的介质中，以进一步减少数据同时损坏或丢失的风险；

g） 宜考虑可移动介质的登记，以减少数据丢失的机会；

h） 只有在业务需求时，才宜使用可移动介质驱动器；

i） 在需要使用移动介质时，宜监视对这样介质的信息传输。

规程和授权级别宜形成文件。

8.3.2 介质的处置

控制

宜使用正式的规程安全地处置不再需要的介质。

实现指南

宜建立介质安全处置的正式规程，以最小化把保密信息泄露给未授权人员的风险。包含保密信息的介质的安全处置规程宜与信息的敏感性相一致。宜考虑下列条款：

a） 包含有保密信息的介质宜被安全地存储和处置，例如，利用焚化或粉碎的方法，或者将数据擦除供组织内其他应用使用；

b） 宜有规程识别可能需要安全处置的项目；

c) 将所有介质部件收集起来并进行安全处置,可能比试图分离出敏感部件更容易;

d) 许多组织提供介质收集和处置服务;宜注意选择具有足够控制和经验的合适的外部方;

e) 处置敏感项宜做记录,以便维护审核踪迹。

当大量处置介质时,宜考虑可导致大量不敏感信息成为敏感信息的集聚效应。

其他信息

可能需要对包含敏感数据的已损坏设备进行风险评估以确定其部件是否宜进行物理销毁,而不是被送修或废弃(见 11.2.7)。

8.3.3 物理介质的转移

控制

包含信息的介质在运送中宜受到保护,以防止未授权访问、不当使用或毁坏。

实现指南

为保护包含信息的介质在传输中的安全,宜考虑下列指南:

a) 要使用可靠的运输或送信人;

b) 授权的送信人列表要经管理层批准;

c) 要制定验证送信人身份的规程;

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

e) 宜保持其中标识了介质的内容、所应用的保护,并记录了移交给运输方的时间和接受地点的日志。

其他信息

信息在物理传输期间易受未授权访问、不当使用或破坏,例如在通过邮政服务或送信人传送时。在本控制中,介质包括纸质文件。

当介质中的保密信息未加密时,宜考虑额外的物理防护。

9 访问控制

9.1 访问控制的业务要求

目标:限制对信息和信息处理设施的访问。

9.1.1 访问控制策略

控制

宜基于业务和信息安全要求,建立访问控制策略,形成文件并进行评审。

实现指南

资产拥有者宜就其资产,为特定用户角色确定适当的访问控制规则、访问权及限制,其详细程度和控制的严格程度宜反映相关的信息安全风险。

访问控制包括逻辑的和物理的(见第 11 章),且宜一并考虑。宜为用户和服务提供商提供一份清晰的说明书,其中陈述了有该访问控制所要满足的业务要求。

该策略宜考虑到下列内容:

a) 业务应用的安全要求;

b) 信息传播和授权的策略,例如,“按需所知”原则和信息安全级别以及信息分级的需要(见 8.2);

c) 系统和网络的访问权和信息分级策略之间的一致性;

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) 在了解各种可用的连接类型的分布式和网络化环境中,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) 访问请求的正式授权要求(见 9.2.1、9.2.2);
h) 有关访问权定期评审的要求(见 9.2.5);
i) 访问权的取消(见 9.2.6);
j) 涉及用户身份、秘密鉴别信息的使用和管理有关的所有重大事态的记录的归档;
k) 具有特许访问权的角色(见 9.2.3)。

其他信息

在规定访问控制规则时,宜认真考虑下列内容:

a) 在"未经明确允许,则一律禁止"的前提下建立规则,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) 信息处理设施自动启动的信息标记变更和用户自主启动的信息标记变更(见 8.2.2);
c) 信息系统自动启动的用户许可变更和由管理员启动的用户许可变更;
d) 要求在颁发之前得到批准的规则,以及不要求在颁发之前得到批准的规则。

访问控制规则宜通过正式的规程(见 9.2、9.3、9.4)和已定义的责任(见 6.1.1、9.3)来支持。

基于角色的访问控制是一种被许多组织成功使用的来关联业务角色和访问权的方法。

指导访问控制策略制定的两个常用原则是:

a) "按需所知"原则:只允许访问执行任务所需的信息(不同任务/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:只允许访问执行任务/工作/角色所需要的信息处理设施(IT 设备、应用程序、规程、场所)。

9.1.2 网络和网络服务的访问

控制

宜仅向用户提供他们已获专门授权使用的网络和网络服务的访问。

实现指南

宜制定一个有关网络和网络服务使用的策略。该策略宜包括:

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规程;
c) 保护访问网络连接和网络服务的管理控制和规程;
d) 访问网络和网络服务使用的手段(如使用 VPN 和无线网络);
e) 访问各种网络服务的用户鉴别要求;
f) 监视网络服务的使用。

有关网络服务使用策略宜与组织访问控制策略相一致(见 9.1.1)。

其他信息

对网络服务的未授权和不安全连接可影响整个组织。对于与敏感或关键业务应用的网络连接,或对于处于高风险区域(例如,公共区域或超出组织信息安全管理和控制的外部区域)中用户的连接而言,这一控制特别重要。

9.2 用户访问管理

目标:确保授权用户对系统和服务的访问,并防止未授权的访问。

9.2.1 用户注册和注销

控制

宜实现正式的用户注册及注销过程，以便可分配访问权。

实现指南

用户 ID 的管理过程宜包括：

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

b) 立即禁用或删除离开该用户的 ID(见 9.2.6)；

c) 定期识别并删除或禁用冗余的用户 ID；

d) 确保冗余的用户 ID 不会发给其他用户。

其他信息

提供或撤销对信息或信息处理设备的访问，通常采用以下两步规程：

a) 分配和启用或撤销用户 ID；

b) 对这样的用户 ID 提供或撤销访问权(见 9.2.2)。

9.2.2 用户访问供给

控制

宜对所有系统和服务的所有类型用户，实现一个正式的用户访问供给过程以分配或撤销访问权。

实现指南

用于对用户 ID 访问权进行分配或撤销的供给过程宜包括：

a) 针对信息系统或服务的使用，从系统或服务的拥有者那里获得授权(见 8.1.2)；从管理层那里就访问权获得单独批准可能也是合适的；

b) 验证所授予的访问程度是否与访问策略(见 9.1)相适宜，是否与职责分离之类的其他要求相一致(见 6.1.2)；

c) 确保授权规程完成之前，访问权未被激活(例如，没有被服务提供商所激活)；

d) 维护一份集中式的访问权记录，记载所授予的用户 ID 要访问的信息系统或服务；

e) 调整已变更角色和工作的用户的访问权，并立即删除或阻断已离开组织的用户的访问权；

f) 定期与信息系统或服务的责任主体评审访问权(见 9.2.5)。

其他信息

宜考虑基于业务要求建立用户访问角色，以此把一些访问权概括到一些典型的用户访问轮廓中。在角色层面上比在特殊权限层面上，更容易对访问请求和评审(见 9.2.4)进行管理。

宜考虑在人员合同和服务合同中包括员工或合同方试图进行未授权访问的处罚条款(见 7.1.2、7.2.3、13.2.4 和 15.1.2)。

9.2.3 特许访问权管理

控制

宜限制并控制特许访问权的分配和使用。

实现指南

特许访问权的分配宜按照相关访问控制策略(见 9.1.1)，通过正式的授权过程加以控制。宜考虑下列步骤：

a) 识别与每个系统或过程(如操作系统、数据库管理系统、每个应用程序)相关的特许访问权，以及需要将其分配的用户；

b) 特许访问权宜按照访问控制策略(见 9.1.1)在“按需使用”和“一事一议”的基础上分配给用户,也就是基于职能角色的最低要求;
c) 宜维护授权过程和所有特权的分配记录。在该授权过程没有完成之前,特许访问权不宜进行分配;
d) 宜定义特许访问权到期的要求;
e) 特许访问权宜赋予一个用户 ID——该用户 ID 不同于常规业务活动所使用的那些 ID,常规业务活动不应根据这一所授的 ID 予以执行;
f) 宜定期评审具有特许访问权的用户的能力,以验证其是否符合其工作职责;
g) 为了避免一般管理用户 ID 的未授权使用,宜根据系统配置能力,建立并维护一些特定的规程;
h) 对于一般管理用户 ID,当共享时,宜维护秘密鉴别信息的保密性(例如,频繁变更口令;当一个特定用户离开或变更工作时尽可能快地变更口令;特定用户之间要使用合适的机制进行沟通)。

其他信息

系统管理权(能使用户超越系统或应用控制的信息系统的任何特性或能力)的不恰当使用是一种导致系统故障或违规的主要影响因素。

9.2.4 用户的秘密鉴别信息管理

控制

宜通过正式的管理过程控制秘密鉴别信息的分配。

实现指南

此过程宜包括下列要求:

a) 要求用户签署一份声明,以保持个人秘密鉴别信息的保密性,并保持组秘密鉴别信息(当共享时)仅在该组成员范围内使用;签署的声明可包括在任用条款和条件中(见 7.1.2);
b) 若需要用户维护自己秘密鉴别信息,要在初始时提供给他们一个安全的临时秘密鉴别信息,并首次使用时强制改变;
c) 宜建立一些规程,以在提供一个新的、代替的或临时的秘密鉴别信息之前,验证用户身份;
d) 宜以安全的方式将临时秘密鉴别信息提供给用户;宜避免使用外部方或未受保护的(明文)电子邮件;
e) 临时秘密鉴别信息宜对个人而言是唯一的、不可猜测的;
f) 用户宜认可接受秘密鉴别信息;
g) 在系统或软件安装后,宜改变提供商的默认秘密鉴别信息。

其他信息

口令是一种秘密鉴别信息的常用类型和验证用户身份的常用手段。其他秘密鉴别信息的类型如密钥以及存储在硬件令牌(如智能卡)的生成鉴别码的其他数据。

9.2.5 用户访问权的评审

控制

资产拥有者宜定期对用户的访问权进行评审。

实现指南

访问权的评审宜考虑下列指南:

a) 宜定期和在任何变更之后如升职、降职或任用终止(见第 7 章)后对用户的访问权进行评审;
b) 当在同一个组织中变更角色时,宜评审和重新分配用户的访问权;
c) 对于特许访问权的授权宜以更频繁的时间间隔进行评审;

d) 宜定期核查特许访问权的分配，以确保不能获得未授权的特殊权限；

e) 具有特许访问权的账户的变更宜在定期评审时记入日志。

其他信息

本控制可弥补执行 9.2.1、9.2.2 和 9.2.6 中控制时可能存在的弱点。

9.2.6 访问权的移除或调整

控制

所有员工和外部用户对信息和信息处理设施的访问权在任用、合同或协议终止时，宜予以移除，或在变更时予以调整。

实现指南

任用终止时，宜移除或暂停个人对与信息处理设施和服务有关的信息和资产的访问权。这将决定移除访问权是否是必要的。任用的变更宜体现在不适用于新岗位的访问权的移除上。宜移除或改变的访问权包括物理和逻辑访问。移除或调整可通过移除、撤销或更换密钥、身份识别卡、信息处理设施或订阅的权限实现。任何标识雇员和合同方人员访问权的文件宜反映访问权的移除和调整。如果一个已离开的员工或外部用户知道仍然“存活”的用户 ID 的密码，则宜在任用、合同或协议终止或变更后改变这些口令。

对信息资产和信息处理设施的访问权在任用终止或变更前是否减少或移除，取决于对风险因素的评价，例如：

a) 终止或变更是由员工、外部用户还是由管理者提出，以及终止的原因；

b) 员工、外部用户或任何其他用户的当前责任；

c) 当前可访问资产的价值。

其他信息

在某些情况下，访问权的分配可基于是否可用于多人，例如组 ID，而不是基于离开的员工或外部用户。在这种情况下，离开的人员宜从组访问列表中中移除，并宜做安排，以建议所有相关的其他员工和外部用户不宜再与已离开的人员共享信息。

在由管理者提出任用终止的情况下，不满的员工或外部用户可能故意破坏信息或破坏信息处理设施。在员工辞职或被解雇的情况下，他们可能被诱引，收集将来可用的信息。

9.3 用户责任

目标：让用户承担保护其鉴别信息的责任。

9.3.1 秘密鉴别信息的使用

控制

宜要求用户遵循组织在使用秘密鉴别信息时的惯例。

实现指南

宜建议所有用户：

a) 保持秘密鉴别信息的保密性，确保其不被泄露至任何其他方，包括职能机构的人员。

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

c) 一旦有迹象表明秘密鉴别信息可能受到损害时，就对其进行变更。

d) 当使用口令作为秘密鉴别信息时，宜选择具有最小长度的优质口令，这些口令：

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，例如，名字、电话号码和生日等；

3) 不容易遭受字典攻击(即,不是由字典中的词所组成的);
4) 避免使用连续相同的,全数字的或全字母的字符;
5) 如果是临时的口令,在第一次登录时要修改。

e) 个人用户的秘密鉴别信息不要共享。
f) 当口令作为秘密鉴别信息在自动登录规程中使用和存储时,确保其得到适当保护。
g) 业务用途和非业务用途使用不同的秘密鉴别信息。

其他信息

提供单点登录(SSO)或其他秘密鉴别信息管理工具,可减少要求用户保护的秘密鉴别信息的数量,从而能提高本控制的有效性。但是,这些工具也加大了秘密鉴别信息泄露的影响。

9.4 系统和应用访问控制

目标:防止对系统和应用的未授权访问。

9.4.1 信息访问限制

控制

宜按照访问控制策略限制对信息和应用系统功能的访问。

实现指南

对访问的限制宜基于各个业务应用要求,并符合已制定的组织访问控制策略。

为支持访问限制要求,宜考虑应用以下指南:

a) 提供控制访问应用系统功能的选择菜单;
b) 控制特定用户可访问的数据;
c) 控制用户的访问权,如,读、写、删除和执行;
d) 控制其他应用的访问权;
e) 限制输出中包含的信息;
f) 提供物理或逻辑访问控制以隔离敏感应用程序、应用数据或系统。

9.4.2 安全登录规程

控制

当访问控制策略要求时,宜通过安全登录规程控制对系统和应用的访问。

实现指南

宜选择适当的身份鉴别技术以证实用户声称的身份。

在需要强认证和身份验证时,宜使用如密码手段、智能卡、令牌或生物特征识别方法等替代口令的鉴别方法。

登录系统或应用的规程宜设计成可使未授权访问的机会最小化。因此,登录规程宜公开最少的、与系统或应用有关的信息,以避免给未授权用户提供任何不必要的帮助。良好的登录规程宜:

a) 不显示系统或应用标识符,直到登录过程已成功完成为止;
b) 显示一般性的警示通告,只有已授权的用户才能访问计算机;
c) 在登录规程执行期间,不提供对未授权用户有帮助作用的帮助消息;
d) 仅在所有输入数据完成时才验证登录信息。如果出现一个差错条件,系统不宜指出数据的哪一部分是正确的或不正确的;
e) 防止暴力破解登录尝试;
f) 记录不成功的尝试和成功的尝试;
g) 当检测到一个潜在的或已经成功的登录控制违规时,则产生一个安全事态;

h) 在成功登录完成时，显示下列信息：
   1) 之前成功登录的日期和时间；
   2) 上次成功登录后的任何不成功登录尝试的细节；
i) 不显示正在输入的口令；
j) 不在网络上以明文传输口令；
k) 在设定的不活动的时间段后，终止不活动会话，尤其在高风险区域，例如公共区域、组织安全管理外的区域或移动设备区域；
l) 限制连接次数，为高风险的应用程序提供额外的保护并减少未授权访问的机会。

其他信息

口令是一种通用的提供标识和鉴别的方式，这种方式是建立在只有用户知悉的秘密的基础上。使用密码手段和鉴别协议也可以获得同样的效果。用户鉴别的强度宜和所访问信息的保密级别相适应。

如果在登录会话期间，口令在网络上以明文传输，那么它们可能会被网络“嗅探器”程序捕获。

9.4.3 口令管理系统

控制

口令管理系统宜是交互式的，并宜确保优质的口令。

实现指南

一个口令管理系统宜：

a) 强制使用个人用户 ID 和口令，以维护可核查性；
b) 允许用户选择和变更他们自己的口令，并且包括一个确认规程，以便允许输入出错的情况；
c) 强制选择优质口令；
d) 在第一次登录时强制用户变更口令；
e) 强制定期和根据需要变更口令；
f) 维护以前使用过的口令的记录，并防止重复使用；
g) 输入口令时，不在屏幕上显示；
h) 分开存储口令文件和应用系统数据；
i) 以受保护的方式，存储和传输口令。

其他信息

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

9.4.4 特权实用程序的使用

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。

实现指南

使用可能超越系统和应用的控制的实用程序，宜考虑下列指南：

a) 对实用程序使用标识、鉴别和授权规程；
b) 将实用程序与应用软件分开；
c) 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 9.2.3)；
d) 对实用程序的临时使用进行授权；
e) 限制实用程序的可用性，例如，在授权变更的期间内；
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) 移除或禁用所有不必要的实用程序；

i) 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。

其他信息

大多数计算机安装有一个或多个可能超越系统和应用控制的实用程序。

9.4.5 程序源代码的访问控制

控制

宜限制对程序源代码的访问。

实现指南

对程序源代码和相关内容（例如设计、说明书、验证计划和确认计划）的访问宜严格控制，以防引入非授权功能，避免无意的变更，并维护有价值的知识产权的保密性。对于程序源代码的保存，可以通过这种代码的受控的集中存储来实现，更好的是放在源程序库中。为了控制对源程序库的访问以减少潜在的计算机程序的破坏，宜考虑下列指南：

a) 若有可能，在运行系统中不宜保留源程序库；

b) 程序源代码和源程序库宜根据制定的规程进行管理；

c) 宜限制支持人员访问源程序库；

d) 更新源程序库和有关内容，向程序员发布程序源码宜在获得适当的授权之后进行；

e) 程序列表宜保存在安全的环境中；

f) 宜维护对源程序库所有访问的审计日志；

g) 维护和拷贝源程序库宜受严格变更控制规程的制约（见 14.2.2）。

如需发布源代码，宜考虑采取保护其完整性的额外的控制（如数字签名）。

10 密码

10.1 密码控制

目标：确保适当和有效地使用密码技术以保护信息的保密性、真实性和（或）完整性。

10.1.1 密码控制的使用策略

控制

宜开发和实现用于保护信息的密码控制使用策略。

实现指南

制定密码策略时，宜考虑下列内容：

a) 组织内使用密码控制的管理方法，包括保护业务信息的一般原则；

b) 基于风险评估，来识别需要的保护级别，同时考虑需要的加密算法的类型、强度和质量；

c) 对通过移动介质、可拆卸的介质设备或通信线路来传输的信息使用加密保护；

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

e) 角色和责任，例如，谁负责：

   1) 策略的实现；

   2) 密钥管理，包括密钥生成（见 10.1.2）；

f) 为在整个组织内有效实现而采用的标准（针对那些业务过程，使用哪些解决方案）；

g) 使用加密后的信息对依赖于内容检查的控制（例如恶意软件检测）的影响。

当实现组织的密码策略时，宜考虑我国应用密码技术的规定和限制，以及加密信息跨越国界时的问

题(见 18.1.5)。

密码控制可用于达到不同的安全目标,例如:

a) 保密性:使用信息加密以保护存储或传输中的敏感或关键信息;
b) 完整性/真实性:使用数字签名或消息鉴别码以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) 抗抵赖性:使用密码技术以提供一个事态或行为发生或未发生的证据;
d) 可鉴别性:使用密码技术以鉴别对系统的用户、实体和资源进行请求访问或交互的用户和其他系统实体。

其他信息

关于密码解决方案是否合适的决策,宜作为风险评估和控制选择的一部分。该评估能被用于决定密码控制是否适宜,采用何种控制、及用于何种目的和业务过程。

密码控制的使用策略对于密码技术使用的成效最大化、风险最小化,以及避免不合适或不正确的使用,是十分必要的。

在选择适宜的密码控制时宜征求专家建议以满足信息安全策略目标。

10.1.2 密钥管理

控制

宜制定和实现贯穿其全生命周期的密钥使用、保护和生存期策略。

实现指南

策略宜包括密钥在其全生命周期中的管理要求,包括密钥生成、存储、归档、恢复、分发、废止和销毁。

宜根据最佳实践选择密码算法、密钥长度和使用惯例。适合的密钥管理要求具有密钥生成、存储、归档、恢复、分发、废止和损坏的安全过程。

宜保护所有的密钥免遭修改和丢失。另外,私密密钥和私钥需要防范非授权的泄露和使用。用来生成、存储和归档密钥的设备宜进行物理保护。

密钥管理系统宜基于已商定的标准、规程和安全方法,以便:

a) 生成用于不同密码系统和不同应用的密钥;
b) 发布和获得公钥证书;
c) 分发密钥给预期实体,包括在收到密钥时要如何激活;
d) 存储密钥,包括已授权用户如何访问密钥;
e) 变更或更新密钥,包括要何时变更密钥和如何变更密钥的规则;
f) 处理泄露的密钥;
g) 撤销密钥,包括要如何撤消或吊销密钥,例如,当密钥泄露或当用户离开组织时(在这种情况下,密钥也要归档);
h) 恢复已丢失或损坏的密钥;
i) 备份或归档密钥;
j) 销毁密钥;
k) 记录和审核与密钥管理相关的活动。

为了减少密钥不恰当使用的可能性,宜规定密钥的激活日期和吊销日期,以使它们只能用于由相关的密钥管理策略确定的时间周期。

除了安全地管理私密密钥和私钥外,还宜考虑公钥的真实性。公钥真实性的鉴别过程可以由认证机构正式颁发的公钥证书来完成,该认证机构宜是一个具有合适的控制和规程以提供所需的信任度的公认组织。

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

其他信息

密钥管理对于有效使用密码技术来说是必需的。ISO/IEC 11770[2][3][4] 提供了更多密钥管理的信息。

密码技术还可以用来保护密钥。需要考虑制定规程来处理对密钥访问的法律要求,例如,加密的信息可能需要以未加密的形式提供,以作为法庭证据。

11 物理和环境安全

11.1 安全区域

目标:防止对组织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

控制

宜定义和使用安全边界来保护包含敏感或关键信息和信息处理设施的区域。

实现指南

对于物理安全边界,若适合,宜考虑和实现下列指南:

a) 宜确定安全边界,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宜在物理上是安全的(即,在边界或区域内不宜存在可能易于闯入的任何缺口);场所的房顶、墙和地板宜是坚固建筑,所有通往外部的门宜使用控制机制(例如,门闩、报警器、锁等)来适当保护,以防止未授权进入;无人看管的门和窗户要上锁,还要考虑窗户的外部保护,尤其是地面一层的窗户;

c) 宜设立人工接待区域或采用其他手段,控制实际进入场所或建筑物;宜限制只有授权的人员才能进入场所或建筑物;

d) 适用时,宜建立物理屏障以防止未授权进入和环境污染;

e) 宜根据相关标准,在安全边界的所有防火门及其墙体上,安装报警装置,并进行监事和测试,以建立所需的防卫水平;它们宜按我国消防规范安全运行;

f) 宜按照我国标准,对所有的外部门窗安装适当的安防监测系统,并进行定期测试;宜一直警惕空闲区域;其他区域宜提供掩护方法,例如计算机室或通信室;

g) 组织管理的信息处理设施宜在物理上与外部方管理的设施分开。

其他信息

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

一个安全区域可以是一个可上锁的办公室,或是被连续的内部物理安全屏障包围的几个房间。在安全边界内具有不同安全要求的区域之间宜需要额外的屏障和边界以控制物理访问。宜特别注意容纳多个组织资产的建筑的物理访问安全。

风险评估确定的物理控制的应用,特别是针对安全区域,宜与组织的技术和经济环境相适应。

11.1.2 物理入口控制

控制

安全区域宜由适合的入口控制所保护,以确保只有授权的人员才允许访问。

实现指南

宜考虑下列指南：

a) 记录访问者进入和离开的日期和时间，所有的访问者宜予以监督，除非他们的访问事前已经经过批准；只允许他们访问特定的、已授权的目的，并宜向他们宣布关于该区域的安全要求和应急规程的说明。来访者的身份宜通过适当的方式进行身份验证。

b) 宜通过实现适当的访问控制，来实现仅限于已授权人员才可访问处理或储存保密信息的区域，例如，可采用如门禁卡和秘密个人识别码的双因素鉴别机制。

c) 宜安全地维护和监视所有访问的纸质登记册或者电子审核踪迹。

d) 所有员工、合同方人员和外部人员以及所有访问者宜佩带某种形式的可视标识，如果遇到无人护送的访问者和未佩带可视标识的任何人宜立即通知保安人员。

e) 限制外部支持服务人员，仅当需要时才能访问安全区域或保密信息处理设施；这种访问宜被授权并受监视。

f) 对安全区域的访问权宜定期地予以评审和更新，并在必要时废除（见 9.2.5、9.2.6）。

11.1.3 办公室、房间和设施的安全保护

控制

宜为办公室、房间和设施设计并采取物理安全措施。

实现指南

保护办公室、房间和设施的安全，宜考虑下列指南：

a) 关键设施的安置宜避免公众访问的场地。

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

c) 宜配置设施以防保密信息或活动被外部可视或可听。适当时，也宜考虑电磁屏蔽。

d) 标识保密信息处理设施位置的目录和内部电话簿不要轻易被未授权的任何人得到。

11.1.4 外部和环境威胁的安全防护

控制

宜设计和应用物理保护以防自然灾害、恶意攻击和意外。

实现指南

在如何避免火灾、洪水、地震、爆炸、社会动荡和其他形式的自然灾难或人为灾难的破坏方面，宜征求专家建议。

11.1.5 在安全区域工作

控制

宜设计和应用安全区域工作规程。

实现指南

宜考虑下列指南：

a) 基于“须知”原则，员工宜仅知晓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，均宜避免在安全区域内进行不受监督的工作；

c) 未使用的安全区域宜上锁并定期予以评审；

d) 未经授权，不宜允许携带摄影、视频、音频或其他记录设备，例如移动设备中的照相机。

安全区域的工作安排包括对在安全区域工作的员工和外部用户的控制，控制要覆盖发生在安全区域内的所有活动。

11.1.6 交接区

控制

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

实现指南

宜考虑下列指南:

a) 由建筑物外进入交接区的访问宜限于已标识的和已授权的人员;
b) 交接区宜设计为在交接人员无需访问建筑物的其他部分就能装卸物资;
c) 当内部门打开时,交接区外部门宜得到安全保护;
d) 运进的物资在搬离交接区之前,宜进行检查和检验是否存在爆炸物、化学品或者其他危险物质;
e) 运进的物资宜按照资产管理规程(见第 8 章)在场所入口处进行登记;
f) 如可能,运进和运出的货物宜在物理上予以隔离;
g) 宜检查运进的物资是否存在途中篡改,如有,宜立即向相关安全人员报告。

11.2 设备

目标:防止资产的丢失、损坏、失窃或危及资产安全以及组织活动的中断。

11.2.1 设备安置和保护

控制

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

实现指南

为保护设备,宜考虑下列指南:

a) 设备宜进行适当安置,以尽量减少不必要的对工作区域的访问;
b) 宜谨慎放置处理敏感数据的信息处理设施,以减少其在使用期间信息被未授权人员窥视的风险;
c) 宜保护存储设施以防止未授权访问;
d) 宜保证那些需要特别保护的部件是安全的,以降低所要求的总体保护等级;
e) 宜采取控制以最小化潜在的物理和环境威胁的风险,例如偷窃、火灾、爆炸、烟雾、水(或供水故障)、尘埃、振动、化学影响、电源干扰、通信干扰、电磁辐射和故意破坏;
f) 宜建立在信息处理设施附近饮食和吸烟的规定;
g) 宜监视可能对信息处理设施运行状态产生负面影响的环境条件(例如温度和湿度);
h) 所有建筑物都宜采用避雷保护,所有接入的电源和通信线路都宜装配雷电保护过滤器;
i) 对于工业环境中的设备,宜考虑使用专门的保护方法,例如键盘保护膜;
j) 宜保护处理保密信息的设备,以最小化因辐射而导致信息泄露的风险。

11.2.2 支持性设施

控制

宜保护设备使其免于由支持性设施的失效而引起的电源故障和其他中断。

实现指南

支持性设施(如电力、电信、供水、燃气、排污、通风和空调)宜:

a) 符合设备制造商规范及本地相关法律要求;

b) 定期评估其能力以满足业务增长的需要并保持与其他支持设施的交互；

c) 定期检查和测试确保其功能正常；

d) 如需要，报警以检测故障；

e) 如需要，使用多种物理途径进行多路供给。

宜提供应急照明和应急通信。关闭电源、供水、供气和其他设施的应急开关和阀门宜位于应急出口或设备室附近。

其他信息

有关网络连接的附加冗余，可通过多重路由的手段，从多个设施供应商那里获得。

11.2.3 布缆安全

控制

宜保证传输数据或支持信息服务的电源布缆和通信布缆免受窃听、干扰或损坏。

实现指南

对于布缆安全，宜考虑下列指南：

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

b) 为了防止干扰，电源电缆宜与通信电缆分开；

c) 对于敏感的或关键的系统，宜考虑更进一步的控制：

1) 在检查点和终接点处安装铠装电缆管道和上锁的房间或盒子；

2) 使用电磁屏蔽装置保护电缆；

3) 对于电缆连接的未授权装置宜主动实现技术清除和物理检查；

4) 控制对配线盘和电缆室的访问。

11.2.4 设备维护

控制

设备宜予以正确地维护，以确保其持续的可用性和完整性。

实现指南

对于设备维护，宜考虑下列指南：

a) 宜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) 宜保存所有可疑的或实际的故障的记录，以及所有预防性和纠正性维护记录；

d) 当对设备安排维护时，宜实现适当的控制，并考虑到是现场维护还是送出维护；当必要时，保密信息宜从设备中删除或者维护人员宜是足够可靠的；

e) 宜遵守保险策略中规定的所有维护要求；

f) 维护后的设备在重新使用前，宜实施检查以确保设备未被篡改，也没有功能失常。

11.2.5 资产的移动

控制

设备、信息或软件在授权之前不宜带出组织场所。

实现指南

宜考虑下列指南：

a) 宜对授权允许将资产带出办公场所的员工和外部用户进行标识；

b) 宜设置资产带出的时间限制，并在返还时进行符合性验证；

c) 若必要并适合，宜对资产的和返还进行记录；

d) 任何处理或使用资产的人员的身份、角色和隶属关系宜形成文件，并随设备、信息或软件一同返回。

其他信息

用于检测未授权资产移动的抽查也可用作检测未授权的记录装置、武器等，以防止其进出办公场所。该抽查宜按照相关法律法规执行。抽查活动宜让每个个体都知晓，并且验证活动只能在法律法规要求的适当授权范围内予以执行。

11.2.6 组织场所外的设备与资产安全

控制

宜对组织场所外的资产采取安全措施，要考虑工作在组织场所外的不同风险。

实现指南

在组织场所外使用信息存储和处理设备宜得到管理者的授权。这适用于组织拥有的设备和为了组织利益使用的私人设备。

对于离开场所的设备的保护，宜考虑下列指南：

a) 离开场所的设备和介质在公共场所不宜无人看管；

b) 宜始终遵守制造商的设备保护说明，例如，防止暴露于强电磁场内；

c) 组织场所外工作位置如家庭工作、远程办公和临时工作地点的控制宜根据风险评估确定，当适合时，宜应用合适的控制，例如，可上锁的存档柜、清理桌面策略、对计算机的访问控制以及与办公室的安全通信(参见 ISO/IEC 27033[15][16][17][18][19])；

d) 当组织场所外的设备在不同个体或外部方之间传递时，宜维护设备的一系列保管记录，该记录宜至少包括设备负责人的姓名和所属组织。

诸如损坏、被盗和窃听等风险在一些场所之间可能不同，宜在确定最合适的控制予以考虑。

其他信息

用于家庭工作或从常规工作地点带走的信息存储和处理设备包括所有形式的个人计算机、管理设备、移动电话、智能卡、纸张或其他形式的设备。

有关保护移动设备其他方面的更多信息可见 6.2。

为避免风险，不鼓励相关员工在组织场所外工作或限制其使用便携式的 IT 设备可能是恰当的。

11.2.7 设备的安全处置或再利用

控制

包含储存介质的设备的所有部分宜进行核查，以确保在处置或再利用之前，任何敏感信息和注册软件已被删除或安全的重写。

实现指南

在设备处置或再利用前，宜验证其是否包含存储介质。

包含保密或版权信息的存储介质宜进行物理销毁，或者采用使原始信息不可获取的技术进行破坏、删除或写覆盖，而不能采用一般的删除或格式化功能。

其他信息

包含存储介质且已损坏的设备可能需要进行风险评估，以确定这些设备是否要物理销毁、而不是送去修理或丢弃。设备的草率处置或再利用可能导致信息泄露。

当设备予以处置或重新调配时，除了安全的磁盘擦除，全盘加密可以减少保密信息泄露的风险，如果：

a) 加密过程足够强壮并覆盖整个磁盘(包括剩余空间、交换文件等)；

b) 加密密钥足够长能抵御暴力破解攻击；

c) 加密密钥自身的机密性能够得到保障(如用于加密磁盘的密钥从不存储在被加密保护的磁盘中)。

关于加密的更多建议见第10章。

安全重写存储介质的技术根据存储介质不同而不同。宜评审重写工具以确保其适用于存储介质。

11.2.8 无人值守的用户设备

控制

用户宜确保无人值守的用户设备有适当的保护。

实现指南

所有用户宜了解保护无人值守的设备的安全要求和规程,以及他们对实现这种保护所负有的责任。建议用户宜:

a) 结束时终止活动的会话,除非采用一种合适的锁定机制保证其安全,例如,口令保护的屏幕保全机制;
b) 不再需要时退出应用程序或网络服务;
c) 当不在使用时,通过使用带钥匙的锁或等效的控制(如口令访问)等,避免未授权使用计算机或移动设备。

11.2.9 清理桌面和屏幕策略

控制

宜针对纸质和可移动存储介质,采取清理桌面策略;宜针对信息处理设施,采用清理屏幕策略。

实现指南

清理桌面和清理屏幕策略宜考虑信息分级(见8.2)、法律和合同要求(见18.1)、相应的风险和组织的文化方面。宜考虑下列指南:

a) 当不需要诸如纸质上的或电子存储介质上的敏感或关键业务信息时,特别是办公室无人时,宜将其锁起来(理想情况下,在保险柜或保险箱或者其他形式的安全设备中);
b) 当无人值守时,计算机和终端宜退出登录,或使用由口令、令牌或类似的用户鉴别机制控制的屏幕和键盘锁定机制进行保护;当不使用时,宜使用带钥匙的锁、口令或其他控制进行保护;
c) 宜防止复印机或其他复制技术(例如扫描仪、数字照相机)的未授权使用;
d) 包含敏感或涉密信息的介质宜立即从打印机中取走。

其他信息

清理桌面/清理屏幕策略降低了正常工作期间和工作之外未授权访问、丢失、破坏信息的风险。保险箱或其他形式的安全存储设施还可保护存储于其中的信息免受如火灾、地震、洪水或爆炸等灾难的影响。

宜考虑使用带有个人识别码(PIN)功能的打印机,使得发起打印的人员是能得到其打印输出的唯一人员以及在打印机附近的唯一人员。

12 运行安全

12.1 运行规程和责任

目标:确保正确、安全的运行信息处理设施。

12.1.1 文件化的操作规程

控制

操作规程宜形成文件,并对所需用户可用。

实现指南

与信息处理和通信设施相关的操作活动宜制定相应的文件化规程，例如计算机启动和关机规程、备份、设备维护、介质处理、计算机机房、邮件处置管理和安全等规程。

操作规程宜规定操作说明书，包括：

a) 系统安装和配置；
b) 自动和手动的信息处理及处置；
c) 备份(见 12.3)；
d) 时间安排要求，包括与其他系统的相互关系、最早工作开始时间和最后工作完成期限；
e) 对在工作执行期间可能出现的处理差错或其他异常情况的指导，包括对使用系统实用工具的限制(见 9.4.4)；
f) 当出现不期望操作或技术困难时，支持和升级的联系人，包括外部支持性联络；
g) 特定输出及介质处理的指导，例如使用特殊信纸或管理保密输出，包括任务失败时输出的安全处置规程(见 8.3 和 11.2.7)；
h) 系统失效时使用的系统重启和恢复规程；
i) 审计踪迹和系统日志信息的管理(见 12.4)；
j) 监视规程。

宜将操作规程和系统活动的文件化规程看作正式的文件，其变更由管理者授权。技术上可行时，信息系统宜使用相同的规程、工具和实用程序进行一致的管理。

12.1.2 变更管理

控制

宜控制影响信息安全的变更，包括组织、业务过程、信息处理设施和系统变更。

实现指南

特别是，宜考虑下列条款：

a) 重大变更的标识和记录；
b) 变更的策划和测试；
c) 对这种变更的潜在影响的评估，包括信息安全影响；
d) 对建议变更的正式批准规程；
e) 验证信息安全要求已得到满足；
f) 向所有有关人员传达变更细节；
g) 回退规程，包括从不成功变更和未预料事态中退出和恢复的规程与责任；
h) 提供紧急变更流程，以便为解决一个事件所需要的变更能够快速且受控地实现(见 16.1)。

正式的管理者责任和规程宜到位，以确保所有变更得到满意的控制。当发生变更时，包含所有相关信息的审计日志宜予以保留。

其他信息

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

12.1.3 容量管理

控制

宜对资源的使用进行监视，调整和预测未来的容量需求，以确保所需的系统性能。

实现指南

宜考虑相关系统业务关键性，来识别容量需求。宜使用系统调整和监视以确保并必要时改进系统

的可用性和效率。宜有检测控制以及时地指出问题。对未来容量需求的预测宜考虑新的业务、系统要求以及当前的组织信息处理能力和预计的发展趋势。

需要特别关注与订货交货周期长或成本高相关的所有资源;因此管理者宜监视关键系统资源的使用情况。管理者宜识别出使用的趋势,特别是与业务应用或信息系统管理工具相关的使用。

管理者宜使用该信息来识别和避免可能威胁到系统安全或服务的潜在的瓶颈及对关键员工的依赖,并策划适当的措施。

提供足够的容量能通过增加容量或者减少需求达到。管理容量需求的例子包括:

a) 删除废弃数据(磁盘空间);

b) 释放应用、系统、数据库或环境资源;

c) 优化批处理进程和进度表;

d) 优化应用逻辑或数据库查询;

e) 拒绝或限制非关键业务的资源高消耗服务的带宽(如视频流)。

宜为关键业务系统考虑文件化的容量管理计划。

其他信息

本控制还关注人力资源以及办公室和设施等。

12.1.4 开发、测试和运行环境的分离

控制

宜分离开发、测试和运行环境,以降低对运行环境未授权访问或变更的风险。

实现指南

宜识别和实现运行、测试和开发环境的分离级别,运行、测试和开发环境分离对防止运行问题发生是必须的。

宜考虑下列条款:

a) 宜定义软件从开发状态到运行状态的传送规则并形成文件;

b) 开发和运行软件宜在不同的系统或计算机处理器上以及在不同的域或目录内运行;

c) 在应用到运行系统之前,操作系统和应用程序的变更宜在测试或临时环境中进行测试;

d) 除在特殊情况下,测试不宜在运行系统上进行;

e) 非必要时,编译器、编辑器和其他开发工具或系统实用工具不宜从运行系统上被访问到;

f) 用户宜在运行和测试系统中使用不同的用户配置文件,菜单宜显示合适的标识消息以减少出错的风险;

g) 敏感数据不宜拷贝到测试系统环境中,除非为测试系统提供了相同的控制(见 14.3)。

其他信息

开发和测试活动可能引起严重的问题,例如,文件或系统环境的不期望修改或者系统故障。有必要维护一种已知的和稳定的环境以执行有意义的测试并防止对运行环境的不当的开发者访问。

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

开发和测试人员也会威胁到运行信息的保密性。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、测试和运行设施是有必要的(测试数据的保护见 14.3)。

12.2 恶意软件防范

目标:确保信息和信息处理设施防范恶意软件。

12.2.1 恶意软件的控制

控制

宜实现检测、预防和恢复控制以防范恶意软件，并结合适当的用户意识教育。

实现指南

防范恶意软件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。宜考虑下列指南：

a) 建立禁止使用未授权软件的正式策略(见 12.6.2、14.2)；
b) 实现控制(如应用程序白名单)，以防止或发现未授权软件的使用；
c) 实现控制(如黑名单)，以防止或发现已知或可疑的恶意网站的访问；
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，该策略宜说明需采取的保护措施；
e) 减少可能被恶意软件利用的脆弱性，如通过技术脆弱性管理(见 12.6)；
f) 定期评审支持关键业务过程的系统软件和数据内容；宜正式调查存在的任何未批准的文件或未授权的修改；
g) 作为一项预防控制，或例行程序，宜安装和定期更新恶意软件检测和修复软件扫描计算机和介质；执行的扫描宜包括：
   1) 在使用通过网络或任何形式的存储介质得到的文件前，要扫描恶意软件；
   2) 在使用电子邮件附件和下载前，要扫描恶意软件；该扫描宜在不同的位置进行实施，例如：在电子邮件服务器上、在台式机上以及在接入组织网络时；
   3) 扫描网页的恶意软件；
h) 就系统上恶意软件的防护，定义规程和责任，并就恶意软件攻击，培训它们的使用、报告和恢复；
i) 为从恶意软件攻击中恢复，宜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以及恢复安排(见 12.3)；
j) 实现定期收集信息的规程，例如订阅邮件列表或验证提供新恶意软件的 web 站点；
k) 实现规程以验证与恶意软件相关的信息，并确保报警公告是准确的和有价值的；管理者宜确保可靠的来源(例如，声誉好的期刊、可信的互联网站或防范恶意软件的软件供应商)被用于区分虚假的和真实的恶意软件；所有用户宜了解欺骗问题，以及收到后如何处理；
l) 隔离可能导致灾难性影响的环境。

其他信息

使用两个或多个来自不同供应商的用于防范信息处理环境中恶意软件的软件产品，能改进恶意软件防护的有效性。

宜注意防止在维护和紧急规程期间引入恶意软件，它们可能绕过正常的恶意软件防护的控制。

在某些条件下，恶意软件防护可能干扰运行。

单独使用恶意软件检测及修复软件作为恶意软件控制通常不充分，通常需要结合防止恶意软件引进的操作规程。

12.3 备份

目标：防止数据丢失

12.3.1 信息备份

控制

宜按照既定的备份策略，对信息、软件和系统镜像进行备份，并定期测试。

实现指南

宜建立备份策略以确定组织信息、软件和系统的备份要求。

备份策略宜确定保留和保护要求。

宜提供足够的备份设备以确保所有必要的信息和软件能在灾难或介质故障后恢复。

设计备份计划时，宜考虑下列条款：

a) 宜建立备份拷贝的准确完整的记录，以及文件化的恢复规程；

b) 备份的程度(例如完全备份或差异备份)和频率宜反映组织的业务要求、涉及信息的安全要求和信息对组织持续运行的关键度；

c) 备份宜存储在一个远程地点，有足够距离，以避免主办公场所灾难时受到损坏；

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

e) 宜定期测试备份介质以确保当必要的应急使用时可以依靠这些备份介质；这宜与恢复规程的测试相结合，并检查是否符合所需的恢复时间。宜使用专用的测试介质进行备份数据恢复能力的测试，而不是覆盖原始介质，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) 在保密性十分重要的情况下，备份宜通过加密手段进行保护。

操作规程宜监视备份的执行情况，解决执行计划备份的故障，以确保根据备份策略实施备份的完整性。

宜定期测试单个系统和服务的备份安排以确保其满足业务连续性计划的要求。对于关键系统和服务，备份安排宜包括在发生灾难时恢复完整系统必需的所有系统信息、应用和数据。

宜确定必要业务信息的保存周期，考虑到永久保存归档文件副本的任何要求。

12.4 日志和监视

目标：记录事态并生成证据。

12.4.1 事态日志

控制

宜产生、保持并定期评审记录用户活动、异常、错误和信息安全事态的事态日志。

实现指南

事态日志宜包括相关的：

a) 用户ID；

b) 系统活动；

c) 关键事态的日期、时间和细节，例如登录和退出；

d) 设备标识或位置(如可能)，以及系统标识；

e) 成功的和被拒绝的对系统访问尝试的记录；

f) 成功的和被拒绝的对数据以及其他资源访问尝试的记录；

g) 系统配置的变更；

h) 特定权限的使用；

i) 系统工具和应用程序的使用；

j) 被访问的文件和访问类型；

k) 网络地址和协议；

l) 由访问控制系统发出的告警；

m) 防护系统的激活和停用，例如防病毒系统和入侵检测系统；

n) 用户在应用程序中事务记录。

事态日志是自动监视系统的基础,能够对系统安全产生综合报告和警报。

其他信息

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 18.1.4)。

可能时,系统管理员宜不具有删除或停用其自身活动日志(见 12.4.3)的权限。

12.4.2 日志信息的保护

控制

记录日志的设施和日志信息宜加以保护,以防止篡改和未授权的访问。

实现指南

宜实现控制以防止日志信息的未授权更改和日志设施的运行问题,包括:

a) 已记录的消息类型的更改;

b) 日志文件被编辑或被删除;

c) 超过日志文件存储介质的容量,导致不能记录事态或过去记录事态被写覆盖。

一些审计日志可能被要求存档,以作为记录保存策略的一部分或由于收集和保留证据的需要(见 16.1.7)。

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实用工具或审计工具执行文件查询及规范化。

需要保护系统日志,因为如果其中的数据被修改或删除,可能导致一个错误的安全判断。系统管理员或操作员控制之外的系统日志的实时复制可被用于保护日志。

12.4.3 管理员和操作员日志

控制

系统管理员和系统操作员活动宜记入日志,并对日志进行保护和定期评审。

实现指南

特权用户的账户持有人可能能够在其直接控制下操作信息处理设施上的日志,因此有必要保护和评审日志以维护特权用户的可核查性。

其他信息

系统和网络管理员控制之外的入侵检测系统可被用于监视系统和网络管理活动的符合性。

12.4.4 时钟同步

控制

一个组织或安全域内的所有相关信息处理设施的时钟,宜与单一一个基准的时间源同步。

实现指南

宜对内部和外部的时间显示、同步和准确性的要求形成文件。该要求可以是法律、法规、合同要求、符合的标准或内部监控的要求。宜定义组织内使用的标准的基准时间。

组织从外部源获得基准时间的途径以及如何同步内部时钟宜形成相应的文件并实现。

其他信息

正确设置计算机时钟对确保审计记录的准确性是重要的,审计日志可用于调查或作为法律、纪律处理的证据。不准确的审计日志可能妨碍调查,并损害这种证据的可信性。可使用链接到源于国家原子钟的无线电广播时间,作为日志生成系统的主时钟。可使用网络时间协议来保持所有服务器与主时钟

完全同步。

12.5 运行软件控制

目标:确保运行系统的完整性

12.5.1 运行系统软件的安装

控制

宜实现运行系统软件安装控制规程。

实现指南

控制运行系统上软件的变更,宜考虑下列指南:

a) 宜仅由受过培训的管理员,根据合适的管理授权(见 9.4.5),进行运行软件、应用和程序库的更新;
b) 运行系统宜仅具有经过批准的可执行代码,而不能具有开发代码和编译程序;
c) 应用和操作系统软件宜仅在全面的、成功的测试后予以实现;这种测试宜包括实用性、安全性、对其他系统的影响和用户友好性的测试,且测试宜在独立的系统上完成(见 12.1.4);宜确保所有对应的程序源码库已经更新;
d) 宜使用配置控制系统对所有已开发的软件和系统文件进行控制;
e) 在变更实现之前宜有回退的策略;
f) 宜维护对运行程序库的所有更新的审计日志;
g) 宜保留应用软件的先前版本作为应急措施;
h) 软件的旧版本,连同所有需要的信息和参数、规程、配置细节以及支持软件宜被归档,并与归档的数据具有相同的保留期。

在运行系统中所使用的由厂商供应的软件宜在供应商支持的级别上加以维护。一段时间后,软件供应商停止支持旧版本的软件。组织宜考虑依赖于这种不再支持的软件的风险。

升级到新版的任何决策宜考虑变更的业务要求和新版的安全,即引入的新安全功能或影响该版本安全问题的数量和严重程度。当软件补丁有助于消除或减少安全弱点(见 12.6)时,宜使用软件补丁。

必要时在管理者批准的情况下,仅为了支持目的,才授予供应商物理或逻辑访问权。宜监视供应商的活动(见 15.2.1)。

计算机软件可能依靠外部提供的软件和模块,宜对这些产品进行监视和控制,以避免可能引入安全弱点的非授权的变更。

12.6 技术方面的脆弱性管理

目标:防止对技术方面的脆弱性的利用。

12.6.1 技术方面脆弱性的管理

控制

宜及时获取在用的信息系统的技术方面的脆弱性信息,评价组织对这些脆弱性的暴露状况并采取适当的措施来应对相关风险。

实现指南

当前的、完整的资产清单(见第 8 章)是进行有效技术方面的脆弱性管理的先决条件。支持技术方面的脆弱性管理所需的特定信息包括软件供应商、版本号、部署的当前状态(例如,在什么系统上安装什么软件),以及组织内负责软件的人员。

宜采取适当的、及时的措施以响应潜在的技术方面脆弱性。建立有效的技术方面的脆弱性管理过程宜遵循下列指南：

a) 组织宜定义和建立与技术方面的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、打补丁、资产追踪和任何要求的协调职责；

b) 用于识别相关的技术方面的脆弱性和维护有关这些脆弱性的认识的信息资源，宜被识别用于软件和其他技术（基于资产清单，见 8.1.1）；这些信息资源宜根据清单的变更而更新，或当发现其他新的或有用的资源时，也宜更新；

c) 宜制定时间表对潜在的相关技术方面的脆弱性的通知做出反映；

d) 一旦潜在的技术方面的脆弱性被确定，组织宜识别相关的风险并采取措施；这些措施可能包括对脆弱的系统打补丁或应用其他控制；

e) 按照技术方面的脆弱性需要解决的紧急程度，宜根据变更管理相关的控制（见 12.1.2），或者遵照信息安全事件响应规程（见 16.1.5）采取措施；

f) 如果有可用的补丁，则宜评估与安装该补丁相关的风险（脆弱性引起的风险宜与安装补丁带来的风险进行比较）；

g) 在安装补丁之前，宜进行测试与评价，以确保它们是有效的，且不会导致不能容忍的负面影响；如果没有可用的补丁，宜考虑其他控制，例如：

   1) 关闭与脆弱性有关的服务和功能；

   2) 调整或增加访问控制，例如在网络边界上添加防火墙（见 13.1）；

   3) 增加监视以检测或预防实际的攻击；

   4) 提高脆弱性意识；

h) 宜保持所有执行规程的审计日志；

i) 宜定期对技术方面的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) 宜首先解决处于高风险的系统；

k) 有效的技术方面的脆弱性管理过程宜与事件管理活动保持一致，以传递脆弱性数据至事件响应活动并在事件发生时提供可执行的技术规程；

l) 确定脆弱性被识别但没有合适对策时的规程。在该情况下，组织宜评价与已知脆弱性相关的风险，并确定适当的检测和纠正活动。

其他信息

技术方面的脆弱性管理可被看作是变更管理的一个子功能，因此可以利用变更管理的过程和规程（见 12.1.2 和 14.2.2）。

供应商往往是在很大的压力下发布补丁。因此，补丁可能不足以解决该问题，并且可能存在负作用。而且，在某些情况下，一旦补丁被安装后，很难被卸载。

如果不能对补丁进行充分的测试，如由于成本或资源缺乏，那么可以考虑推迟打补丁，以便基于其他用户报告的经验来评价相关的风险。可参考使用 ISO/IEC 27031[14]。

12.6.2 软件安装限制

控制

宜建立并实现控制用户安装软件的规则。

实现指南

组织宜确定并严格实现用户能安装的软件类别的策略。

宜使用最小授权原则。如获得了某些特权，用户就可能具有安装软件的能力。组织宜确定允许安装的软件类型（如现有软件的升级和安全补丁）和禁止安装的软件类型（如仅为个人使用的软件，与未知的或可疑的潜在的恶意软件相关的软件）。宜针对用户所涉及的角色授予这些特权。

其他信息

在计算机设备上不受控制的安装软件可能导致脆弱性，进而导致信息泄露、完整性损失、其他信息安全事件，或违反知识产权。

12.7 信息系统审计的考虑

目标：使审计活动对运行系统的影响最小化。

12.7.1 信息系统审计控制

控制

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

实现指南

宜遵守下列指南：

a) 访问系统和数据的审计要求宜与相关的管理达成一致；
b) 宜商定和控制技术审计测试范围；
c) 审计测试宜限于对软件和数据的只读访问；
d) 除只读之外的访问宜仅允许对系统文件的被隔离的副本进行操作，当审计完成时，宜擦除这些拷贝，或者当审计存档要求下有保留这些文件的时，给予适当的保护；
e) 特殊或额外的处理宜得到确定和商定；
f) 可能影响系统可用性的审计测试宜在业务时间外进行；
g) 宜监视和记录所有访问，以产生参考踪迹。

13 通信安全

13.1 网络安全管理

目标：确保网络中的信息及其支持性的信息处理设施得到保护。

13.1.1 网络控制

控制

宜管理和控制网络以保护系统和应用中的信息。

实现指南

宜实现控制，以确保网络中信息的安全，确保所连接的网络服务得到保护，免遭未授权访问。特别的，宜考虑下列条款：

a) 宜建立网络设备管理的责任和规程；
b) 在合适的地方，网络的运行责任宜与计算机运行责任予以分离(见 6.1.2)；
c) 宜建立专门的控制，以保护在公用网络上或无线网络上流经数据的保密性和完整性，并且保护已连接的系统及应用(见第 10 章和 13.2)；为维护所连接的网络服务和计算机的可用性，还可以需要专门的控制；
d) 宜应用合适的日志生成和监视，以便能记录和检测到一些可能影响信息安全或与信息安全相关的活动；
e) 为优化对组织的服务和确保在信息处理基础设施中诸多控制的一致应用，宜紧密协调相应的管理活动；

f) 宜鉴别网络上的系统；

g) 宜限制与网络的系统连接。

其他信息

有关网络安全的更多信息参见 ISO/IEC 27033[15][16][17][18][19]。

13.1.2 网络服务的安全

控制

所有网络服务的安全机制、服务级别和管理要求宜予以确定并包括在网络服务协议中，无论这些服务是由内部提供的还是外包的。

实现指南

网络服务提供商以安全方式管理商定服务的能力，宜予以确定并定期监视，还宜商定审计的权利。

宜识别特殊服务必要的安全安排，例如安全特征、服务水平和管理要求。组织宜确保网络服务提供商实现了这些措施。

其他信息

网络服务包括接入服务、私有网络服务、增值网络和受控的网络安全解决方案，例如防火墙和入侵检测系统。这些服务既包括简单的未受控的带宽也包括复杂的增值的提供。

网络服务的安全特征可以是：

a) 为网络服务应用的安全技术，例如鉴别、加密和网络连接控制；

b) 按照安全和网络连接规则，网络服务的安全连接需要的技术参数；

c) 若必要，使用网络服务规程，以限制对网络服务或应用的访问。

13.1.3 网络中的隔离

控制

宜在网络中隔离信息服务、用户及信息系统。

实现指南

管理大型网络安全的一种方法是将该网络分成独立的网络域。域的选择可以基于信任级别（如公共访问域、桌面域、服务器域）、所属的组织单元（如人力资源、财务、市场）或某些组合（如连接到多个组织单元的服务器域）。域之间的隔离可以使用不同的物理网络或者使用不同的逻辑网络（如虚拟专用网络）。

宜明确界定每个域的边界。网络域之间允许访问，但宜在边界处使用网关（如防火墙、过滤路由器）进行控制。划分网络域以及允许穿过网关访问的准则宜基于对每个域安全要求的评估。该评估宜与访问控制策略（见 9.1.1）、访问要求、被处理信息的价值和分级相一致，并考虑到相对成本和采用合适的网关技术对性能的影响。

由于无线网络的边界难以确定，因此需要专门处理。对敏感环境而言，宜考虑把所有无线访问视为外部连接，并将该访问从内部网络隔离，直到该访问在授权访问内部系统之前根据网络控制策略（见 13.1.1）通过了网关为止。

当恰当地实现时，现代的、基于标准的无线网络的鉴别、加密和用户分级网络访问控制技术可能对直连组织内网是足够的。

其他信息

因为形成的业务伙伴关系可能需要信息处理和网络设施的互连或共享，网络通常超出了组织边界。这样的扩展会增加对使用网络的组织信息系统未授权访问的风险，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网络用户。

13.2 信息传输

目标：维护在组织内及与外部实体间传输信息的安全。

13.2.1 信息传输策略和规程

控制

宜有正式的传输策略、规程和控制，以保护通过使用各种类型通信设施进行的信息传输。

实现指南

使用通信设施进行信息传输的规程和控制宜考虑下列条款：

a) 设计用来防止传输信息遭受截取、复制、修改、错误寻址和破坏的规程；
b) 检测和防止可能通过使用电子通信传输的恶意软件的规程(见 12.2.1)；
c) 保护以附件形式传输的敏感电子信息的规程；
d) 通信设施可接受使用的策略或指南的概述(见 8.1.3)；
e) 员工、合同方人员和任何其他用户不危害组织的责任，例如诽谤、扰乱、冒名、连锁信转发、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(见第 10 章)；
g) 所有业务通信(包括消息)的保留和处理指南，要与国家和地方法律法规一致；
h) 与使用通信设施相关的控制和限制，例如将电子邮件自动转发到外部邮件地址；
i) 建议员工采取适当的预防措施以防泄露保密信息；
j) 不将包含保密信息的消息留在应答机上，因为可能被未授权个人重放，也不能留在公用系统或者由于误拨号而被不正确地存储；
k) 建议员工有关传真机的使用或服务问题，即：
   1) 未授权访问内置消息存储器，以检索消息；
   2) 有意的或无意的对机器编程，将消息发送给特定的电话号码；
   3) 由于误拨号或使用错误存储的号码将文件和消息发送给错误的电话号码。

另外，宜提醒员工，不要在公共场所、通过不安全的通信方式、开放的办公室和会场进行保密会谈。

信息传输服务宜符合所有相关的法律要求(见 18.1)。

其他信息

可通过使用多种不同类型的通信设施进行信息传输，例如电子邮件、声音、传真和视频。

可通过多种不同类型的介质进行软件传输，包括从互联网下载和从出售现货的供应商处获得。

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

13.2.2 信息传输协议

控制

协议宜解决组织与外部方之间业务信息的安全传输。

实现指南

信息传输协议宜包括：

a) 对传输、分发、接收进行控制和通知的管理责任；
b) 确保可追溯性和不可抵赖性的规程；
c) 打包和传输的最低技术标准；
d) 托管协议；
e) 信使标识标准；
f) 信息安全事态发生时的责任和义务，例如数据丢失；

g) 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 8.2）；

h) 用于记录和读取信息和软件的技术标准；

i) 为保护敏感项[例如密码（见第 10 章）]，可以要求任何专门的控制；

j) 维护信息在传输过程中的监管链；

k) 访问控制的可接受级别。

为保护传输中的信息和物理介质（见 8.3.3），宜建立和维护策略、规程和标准，并宜在传输协议中予以引用。

任何协议的信息安全内容宜反映所涉及业务信息的敏感度。

其他信息

协议可以是电子的或手写的，并可采取正式合同或任用条款的形式。对保密信息而言，信息传输使用的特定机制对于所有组织和各种协议宜是一致的。

13.2.3 电子消息发送

控制

宜适当保护包含在电子消息发送中的信息。

实现指南

电子消息发送的信息安全考虑宜包括以下方面：

a) 保护消息免遭未授权访问、修改，或与组织所采用的分级模式相称的拒绝服务；

b) 确保正确的寻址和消息传输；

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) 在使用外部公共服务（例如即时消息或文件共享）前获得批准；

f) 强鉴别级别，控制来自公共可访问网络的访问。

其他信息

存在多种类型的电子消息发送，例如电子邮件、电子数据交换以及社交网络，在业务通信中扮演了一个角色。

13.2.4 保密或不泄露协议

控制

宜识别、定期评审和文件化反映组织信息保护需要的保密性或不泄露协议的要求。

实现指南

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外部方或组织的员工。宜基于其他方的类型及其被允许访问或处理的保密信息，来选择或添加要素。为识别保密性或不泄露协议的要求，宜考虑下列因素：

a) 要保护的信息（例如保密信息）的定义；

b) 协议的期望持续时间，包括不确定地需要维护保密性的情况；

c) 协议终止时所需的措施；

d) 签署者的责任和行为，以避免未授权信息泄露；

e) 信息、商业秘密和知识产权的所有权，及其如何与保密信息的保护相关；

f) 保密信息的许可使用，及签署者使用信息的权力；

g) 对涉及保密信息的活动的审核和监视的权力；

h) 未授权泄露或保密信息破坏的通知和报告过程；

i) 协议终止时,要返还或销毁的信息项;

j) 违反协议时期望采取的措施。

基于一个组织的信息安全要求,在保密性或不泄露协议中可能需要其他因素。

保密性和不泄露协议宜针对其适用的管辖范围遵循所有适用的法律法规(见 18.1)。

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

其他信息

保密性和不泄密协议保护组织信息,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。

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形式。

14 系统获取、开发和维护

14.1 信息系统的安全要求

目标:确保信息安全是信息系统整个生命周期中的一个有机组成部分。这也包括提供公共网络服务的信息系统的要求。

14.1.1 信息安全要求分析和说明

控制

新建信息系统或增强现有信息系统的要求中宜包括信息安全相关要求。

实现指南

宜使用不同的方法来识别信息安全要求,例如,来自政策法规的符合性要求、威胁建模、事件评审或脆弱性阈值的使用。识别结果宜形成文件并被所有利益相关方评审。

信息安全要求和控制宜反映出所涉及信息的业务价值(见 8.2),和可能由于缺乏足够的安全导致的潜在的负面的业务影响。

宜在信息系统项目初期阶段识别和管理信息安全要求和相关的过程。尽早考虑信息安全要求(如在设计阶段)可形成更高效和具有成本效益的解决方案。

信息安全要求宜考虑:

a) 针对用户声称身份所要求的信任度,得出用户鉴别要求;

b) 对业务用户、特权人员或技术人员的访问配置和授权过程;

c) 告知用户和操作人员的职责和责任;

d) 所涉及资产的保护需求,尤其是有关可用性、保密性和完整性;

e) 来自业务过程的要求,例如,事务日志、监视和抗抵赖要求;

f) 其他安全控制规定的要求,例如,对记录和监视系统或数据泄露检测系统的接口。

对于在公共网络上提供服务或实现交易的应用而言,宜考虑 14.1.2 和 14.1.3 中给出的控制。

如需某种产品,则宜遵循一个正式的测试和获取过程。与供货商签订的合同宜确定已识别的安全要求。如果推荐的产品的安全功能不能满足规定的安全要求,那么在购买产品之前宜重新考虑引入的风险和相关控制。

宜评价和实现可用的产品安全配置指南及其系统的最终软件/服务栈。

宜规定产品接收准则(如产品的功能性方面),这可为满足已识别的安全要求提供保证。宜在获取产品之前根据这些准则评价产品。宜评审附加功能以确保其不会引入不可接受的附加风险。

其他信息

ISO/IEC 27005[11]和 ISO 31000[27]提供了使用风险管理过程识别满足信息安全要求的控制的

指南。

14.1.2 公共网络上应用服务的安全保护

控制

宜保护在公共网络上的应用服务中的信息以防止欺诈行为、合同纠纷以及未经授权的泄露和修改。

实现指南

公共网络上应用服务的安全宜考虑：

a) 每一方要求其他方所声称身份的信心程度，例如通过鉴别；

b) 与可批准、发布或签署关键交易文件内容的人员相关联的授权过程；

c) 确保在与合作伙伴的沟通中，完整地告知了他们有关服务供给或使用的授权；

d) 确定并满足关键文件的保密性、完整性、分发和接受证明的要求以及合同的抗抵赖要求，例如所关联的投标和签署合同的过程；

e) 关键文件完整性所要求的可信等级；

f) 任何保密信息的保护要求；

g) 任何订单交易、支付信息、交付地址细节和接收确认的保密性和完整性；

h) 适用于验证顾客提供的支付信息的验证程度；

i) 为防止欺诈，选择最适合的支付结算方式；

j) 为维护订单信息的保密性和完整性所需的保护级别；

k) 避免交易信息的丢失或复制；

l) 与任何欺诈交易相关的义务；

m) 保险要求。

上述考虑可以通过应用密码控制来实现(见第 10 章)，还要考虑符合法律要求(见第 18 章，特别是 18.1.5 密码法规)。

合作伙伴间的应用服务协议宜形成文件，该协议列出了双方达成一致的服务条款，包括上述授权[见 b)]的细节。

宜考虑受攻击后快速恢复的要求，可包括为了交付服务，保护所涉及到的应用服务器的要求或确保所需的网络连接的可用性的要求。

其他信息

通过公共网络可访问的应用程序易遭受许多网络相关的威胁，如欺诈活动、合同争端和向公众泄露信息。因此详细的风险评估和适当的控制选择不可或缺。所要求的控制通常包括有关鉴别和使数据传输安全的密码学方法。

可以使应用服务使用安全的鉴别方法，如使用公钥密码技术和数字签名(见第 10 章)以减少风险。另外，当需要这些服务时，可使用可信第三方。

14.1.3 应用服务事务的保护

控制

宜保护应用服务事务中的信息，以防止不完整的传输、错误路由、未授权的消息变更、未授权的泄露、未授权的消息复制或重放。

实现指南

应用服务事务的信息安全宜考虑：

a) 事务中涉及的每一方的电子签名的使用；

b) 事务的所有方面，即确保：

1) 各方的用户秘密鉴别信息是有效的并经过验证的；

2） 事务保持保密性；
3） 保持各方相关联的隐私；
c） 加密涉及的各方间的通信路径；
d） 在涉及的各方之间通信的协议是安全的；
e） 确保事务细节存储于任何公开可访问环境之外，如存储于组织内部互联网的存储平台，不留在或暴露于互联网可直接访问的存储介质上；
f） 当使用一个可信机构（例如为了颁布及维护数字签名或数字认证）时，安全可被集成嵌入到整个端到端认证/签名管理过程中。

其他信息

采用控制的程度要对应每种形式应用服务事务相关的风险级别。

事务需要符合事务产生、处理、完成或存储的管辖区域的法律、规则和规章。

14.2 开发和支持过程中的安全

目标：确保信息安全在信息系统开发生命周期中得到设计和实现。

14.2.1 安全的开发策略

控制

针对组织内的开发，宜建立软件和系统开发规则并应用。

实现指南

安全开发是建立安全服务、架构、软件和系统的要求。宜在安全开发策略中考虑：

a） 开发环境的安全；
b） 软件开发生命周期中的安全指南：
1） 软件开发方法的安全；
2） 每种使用的编程语言的安全编码指南；
c） 设计阶段的安全要求；
d） 项目里程碑内的安全检查点；
e） 安全库；
f） 版本控制的安全；
g） 所需的应用安全知识；
h） 开发人员避免、发现和修复脆弱性的能力。

当开发所用的标准可能未知或与当前的最佳实践不一致时，新开发和代码复用时均宜使用安全的编程技术。宜考虑安全的编码标准，并在适当时强制使用。宜培训开发人员使用安全的编码标准，测试和代码评审宜验证其使用。

如开发外包时，组织宜获得外包方遵守安全开发规则的保障（见 14.2.7）。

其他信息

也可能针对内部应用实现开发，如办公软件、脚本、浏览器和数据库。

14.2.2 系统变更控制规程

控制

宜使用正式的变更控制规程来控制开发生命周期内的系统变更。

实现指南

宜将正式的变更控制规程文件化，并强制实施，以确保从最初设计至后续维护中系统、应用和产品的整体性。引入新系统和对已有系统进行大的变更宜按照从文件、规范、测试、质量控制到管理实现这

个正式的过程进行。

这个过程宜包括风险评估、变更影响分析和所需安全控制的规范。这一过程还宜确保不损害现有的安全和控制规程,确保支持程序员仅能访问系统中其工作那些必要的部分,确保任何变更要获得正式商定和批准。

只要可行,应用和运行变更控制规程宜集成起来(见 12.1.2)。该变更控制规程宜包括但不限于:

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) 评审控制和完整性规程,以确保它们不因变更而受到损害;

d) 识别需要修正的所有软件、信息、数据库实体和硬件;

e) 识别和检查安全关键代码以最小化已知安全弱点发生的可能性;

f) 在工作开始之前,获得对详细建议的正式批准;

g) 确保已授权的用户在实现之前接受变更;

h) 确保在每个变更完成之后更新系统文件设置,并将旧文件归档或丢弃;

i) 维护所有软件更新的版本控制;

j) 维护所有变更请求的审计踪迹;

k) 确保变更了操作文件(见 12.1.1)和用户规程,作为必要的合适保存;

l) 确保在正确的时间上进行了变更,并且不干扰所涉及的业务过程。

其他信息

变更软件会影响运行环境,反之亦然。

良好的做法包括在一个与生产和开发环境隔离(见 12.1.4)的环境中测试新软件。它提供了一种方法,可用于控制新软件,以及对被用于测试目的的运行信息进行额外保护。这宜包括补丁、服务填充和其他更新。

当考虑自动更新时,宜对系统完整性和可用性面临的风险与更新的快速部署的益处之间进行权衡。由于某些更新可导致关键应用失败,不宜在关键系统中使用自动更新。

14.2.3 运行平台变更后对应用的技术评审

控制

当运行平台发生变更时,宜对业务的关键应用进行评审和测试,以确保对组织的运行和安全没有负面影响。

实现指南

这一过程宜包括:

a) 评审应用控制和完整性规程,以确保它们不因运行平台变更而受到损害;

b) 确保及时提供运行平台变更的通知,以便于在实现前进行适当的测试和评审;

c) 确保对业务连续性计划进行适当的变更(见第 17 章)。

其他信息

运行平台包括操作系统、数据库和中间件平台。本控制也适用应用程序的变更。

14.2.4 软件包变更的限制

控制

宜不鼓励对软件包进行修改,仅限于必要的变更,且对所有变更加以严格控制。

实现指南

如果可能且可行,宜使用厂商提供的软件包,而无需修改。在需要修改软件包时,宜考虑下列要点:

a) 内置控制和完整性过程被损害的风险;

b) 是否宜获得厂商的同意；

c) 当标准程序更新时，从厂商获得所需变更的可能性；

d) 作为变更的结果，组织需负责进一步维护此软件带来的影响；

e) 与其他在用软件的兼容性。

如果变更是必要的，宜保留原始软件，并将变更应用于指定的副本。宜实现软件更新管理过程，以确保最新批准的补丁和应用更新已经安装在所有的授权软件中(见 12.6.1)。宜充分测试所有变更并形成文件，以便必要时可以将其重新应用于将来的软件升级。如果必要，所有的修改宜由独立的评估机构进行测试和验证。

14.2.5 系统安全工程原则

控制

宜建立、文件化和维护系统安全工程原则，并应用到任何信息系统实现工作中。

实现指南

宜建立基于安全工程原则的安全信息系统工程规程，形成文件并应用于内部信息系统的工程活动。安全宜审计到所有架构层(业务、数据、应用和技术)之中，以平衡信息安全需求和访问需求。宜针对安全风险，分析新技术，并针对已知的攻击模式，评审相应的设计。

宜定期评审这些原则和已建立的工程规程，以确保其有效地用于工程过程中的安全增强标准。还宜定期评审以确保其在对抗任何潜在的新威胁方面保持最新，并保持其对技术和解决方案发展的适用性。

适用时，宜通过组织与外包供应商间的合同以及其他绑定的协议，把已建立的安全工程原则应用到外包的信息系统。组织宜证实供应商的安全工程原则的严谨性与其自身的原则是可比的。

其他信息

应用开发规程宜适用于具有输入输出接口的应用开发中的安全工程技术。安全工程技术提供了用户鉴别技术、安全会话控制和数据确认、调试代码的净化和消除方面的指南。

14.2.6 安全的开发环境

控制

组织宜针对覆盖系统开发全生命周期的系统开发和集成活动，建立安全开发环境，并予以适当保护。

实现指南

安全的开发环境包括与系统开发和集成相关的人员、过程和技术。

组织宜评估与单个系统开发工作相关的风险，并为特定系统的开发工作建立安全的开发环境，考虑：

a) 系统所处理、存储和传输的数据的敏感性；

b) 适用的外部和内部要求，如法律法规或策略的要求；

c) 组织已实现的支持系统开发的安全控制；

d) 工作环境中人员的可信度(见 7.1.1)；

e) 系统开发的外包程度；

f) 分离不同开发环境的需求；

g) 访问开发环境的控制；

h) 监视环境及其所存储代码的变更；

i) 在安全的异地存储备份；

j) 控制数据移入移出环境的活动。

一旦特定开发环境的保护级别被确定,组织宜将相应的过程形成安全开发规程文件并提供给有需要的人员。

14.2.7 外包开发

控制

组织宜督导和监视外包系统开发活动。

实现指南

系统开发外包时,宜考虑组织所有外部供应链的以下方面:

a) 与外包内容相关的许可证、代码所有权和知识产权(见 18.1.2);
b) 安全设计、编码和测试的合同要求(见 14.2.1);
c) 向外部开发者提供已批准的威胁模型;
d) 交付件质量和准确性的验收测试;
e) 提供用以建立安全和隐私保护能力的最低可接受级别的安全阈值的证据;
f) 提供充分测试的证据,用以防范交付时包含有意和无意的恶意内容;
g) 提供充分测试的证据,用以防范已知的脆弱性;
h) 托管安排,如,当源代码不可用时;
i) 对开发过程和控制进行审计的合同权利;
j) 生成交付件的编译环境有效的文件化;
k) 组织保有遵守相关法律法规和验证控制有效性的责任。

其他信息

有关供应商关系的更多信息参见 ISO/IEC 27036[21][22][23]。

14.2.8 系统安全测试

控制

宜在开发过程中进行安全功能测试。

实现指南

新系统和升级的系统要求在开发过程中进行全面的测试和验证,包括准备详细的活动安排、各种条件范围下的测试输入和预期输出。对于内部开发,宜由开发团队进行最初测试。然后,宜进行独立地验收测试(包括内部和外包开发),以确保系统工作按预期且仅按预期(见 14.1.1 和 14.1.9)进行工作。测试范围宜与系统性质和重要性成正比。

14.2.9 系统验收测试

控制

宜建立对新的信息系统、升级及新版本的验收测试方案和相关准则。

实现指南

系统验收测试宜包括信息安全要求测试(见 14.1.1 和 14.1.2)和是否遵循安全系统开发实践测试(见 14.2.1)。该测试还宜在接收组件和集成系统上进行。组织可借助自动工具如代码分析工具或漏洞扫描器,并宜验证与安全有关的缺陷的修复。

宜在真实的测试环境中进行测试以确保系统不会将脆弱性引入组织环境,并确保测试是可靠的。

14.3 测试数据

目标:确保用于测试的数据得到保护。

14.3.1 测试数据的保护

控制

测试数据宜认真地加以选择、保护和控制。

实现指南

宜避免在测试中使用包含个人可识别信息或任何其他保密信息的运行数据。如果个人可识别信息或其他保密信息被用于测试意图，那么宜通过删除或修改来保护所有的敏感细节和内容（见ISO/IEC 29101[26]）。

当用于测试意图时，宜使用下列指南保护运行数据：

a) 用于运行应用系统的访问控制规程，也宜用于测试应用系统；

b) 运行信息每次被拷贝到测试环境时宜有单独的授权；

c) 测试完成后，宜立即从测试环境中清除运行信息；

d) 宜记录运行信息的拷贝和使用以提供审计踪迹。

其他信息

系统和验收测试通常要求大量的尽可能接近运行数据的测试数据。

15 供应商关系

15.1 供应商关系中的信息安全

目标：确保供应商可访问的组织资产得到保护。

15.1.1 供应商关系的信息安全策略

控制

为降低供应商访问组织资产的相关风险，宜与供应商就信息安全要求达成一致，并形成文件。

实现指南

组织宜有策略来识别和落实信息安全控制，以专门解决供应商访问组织信息的问题。

这些控制强调组织要实现的以及组织要求供应商要实现的过程和规程，包括：

a) 识别并记录组织允许访问其信息的供应商类型，如IT服务、物流、金融服务、IT基础设施组件；

b) 用于管理供应商关系的标准化过程和生命周期；

c) 确定不同类型供应商被允许的信息访问类型，并对信息访问进行监视和控制；

d) 将各类信息和各类访问的最低信息安全要求作为单个供应商协议的基础，该协议基于组织的业务需求和要求及其风险状况；

e) 对各类供应商和各类访问遵守所建立的信息安全要求进行监视的过程和规程，包括第三方评审和产品确认；

f) 准确和完备的控制，以确保任何一方所提供的信息或信息处理的完整性；

g) 可用于供应商保护组织信息的义务类型；

h) 处理与供应商访问相关的事件和应急状况，包括组织和供应商的双方责任；

i) 恢复力，必要时，恢复和应急安排以确保任何一方提供的信息或信息处理的可用性；

j) 对参与采购的组织人员进行适用的策略、过程和规程的意识培训；

k) 对与供应商人员接洽的组织人员进行适当的约定和行为准则的意识培训，该准则基于供应商类型及其对组织系统和信息的访问级别；

l) 在双方签字的协议中记录信息安全要求和控制的条件；
m) 管理信息、信息处理设施和任何需要移动的其他设施的必要切换变迁，并确保维护整个变迁过程中的信息安全。

其他信息

信息安全管理不充分的供应商可使信息处于风险中。宜识别并应用控制来管理供应商对信息处理设施的访问。例如，如对信息的保密性有特殊需求，则可以使用非披露协议。另一个例子是当供应商协议涉及到跨国界的信息传送或访问时的数据保护风险，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。

15.1.2 在供应商协议中强调安全

控制

宜与每个可能访问、处理、存储、传递组织信息或为组织信息提供 IT 基础设施组件的供应商建立所有相关的信息安全要求，并达成一致。

实现指南

宜建立供应商协议并形成文件，以确保组织和供应商双方在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要求，宜在协议中考虑：

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(见 8.2)进行信息分级，必要时，在组织的分级方案和供应商的分级方案之间建立映射关系；
c) 法律法规要求，包括数据保护、知识产权和版权，以及对如何确保满足这些要求的描述；
d) 合同各方实现已商定控制的义务(包括访问控制、性能评审、监视、报告和审计等)；
e) 信息的可接受使用规则，必要时，包括不可接受的使用；
f) 对于供应商人员访问或接收组织信息，或者给出被授权访问或接收组织信息的供应商人员的明确名单，或者给出授权和取消授权的规程或条件；
g) 与具体合同相关的信息安全策略；
h) 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)；
i) 具体规程以及信息安全要求的培训和学习要求，如事件响应、授权规程；
j) 分包的相关规定，包括需要实现的控制；
k) 相关的协议合作伙伴，包括信息安全问题的联络人；
l) 如果有，提出对供应商人员的筛选要求，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；
m) 对与协议相关的供应商过程和控制进行审核的权利；
n) 缺陷解决和争执解决的过程；
o) 供应商定期递交控制有效性的独立报告和及时纠正报告中提出的有关问题的协议的义务；
p) 供应商遵守组织安全要求的义务。

其他信息

不同组织和不同类型供应商的协议可能有很大不同。因此，宜注意包含所有相关的信息安全风险和要求。供应商协议也可能涉及其他方(如分包商)。

在协议中需要考虑当供应商不能提供产品或服务时的连续处理规程，以避免拖延安排替代产品或服务。

15.1.3 信息与通信技术供应链

控制

供应商协议宜包括信息与通信技术服务以及产品供应链相关的信息安全风险处理要求。

实现指南

就涉及供应链安全的供应商协议的内容，宜考虑以下主题：

a) 除了对供应商关系的一般信息安全要求外，确定适用于信息与通信技术产品或服务获取的信息安全要求；
b) 对于信息与通信技术服务，若供应商分包部分的组织信息与通信技术服务，则要求供应商在整个供应链中传播组织的安全要求；
c) 对于信息与通信技术产品，若这些产品包括从其他供应商购买的组件，则要求供应商在整个供应链中传播适当的安全实践；
d) 实现监视过程和可接受的方法，以确认信息与通信技术产品和服务遵守了所声明的安全要求；
e) 实现一个过程来标识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，需要更多的关注和审查；
f) 获得关键组件及其来源在供应链中可追溯的保障；
g) 获得对交付的信息与通信技术产品按预期工作无任何意外的或不需要的功能的保障；
h) 确定与供应链及在组织和供应商中任何潜在的问题和妥协有关的信息共享规则；
i) 实现管理信息与通信技术组件生命周期、可用性和相关安全风险的具体过程，包括管理因供应商不在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。

其他信息

特定的信息与通信技术供应链风险管理实践是建立一般的信息安全、质量、项目管理和系统工程实践之上，而不是替代它们。

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

这里的信息与通信技术供应链包括云计算服务。

15.2 供应商服务交付管理

目标：维护与供应商协议一致的信息安全和服务交付的商定级别。

15.2.1 供应商服务的监视和审查

控制

组织宜定期监视、评审和审核供应商服务交付。

实现指南

宜监视和评审供应商服务，以确保协议中的信息安全条款和条件被遵守，并且信息安全事件和问题得到妥善管理。

宜在组织和供应商间涉及服务管理关系过程以：

a) 监视服务性能水平以验证对协议的符合程度；
b) 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；
c) 结合对独立审核员报告的评审（如果可用）和对所发现问题的追踪，审核供应商；
d) 提供关于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；
e) 评审供应商审核踪迹和与交付服务相关的信息安全事态、运行问题、失效、故障追踪和中断的记录；
f) 解决并管理任何被识别出的问题；
g) 评审供应商与其自身供应商关系上的信息安全方面；

h) 确保在主要服务出现故障或遭受灾难后,供应商维护了足够的服务能力及可行计划,以确保维护商定的服务连续性水平(见第 17 章)。

宜将管理供应商关系的责任分配给指定的个体或服务管理团队。另外,组织宜确保供应商为符合性评审和协议要求的强制执行分配了责任。宜有足够的技术能力和资源可用,以监视协议要求尤其是信息安全要求一直得到满足。当发现服务交付中的不足时,宜采取合适的措施。

组织宜对供应商访问、处理或管理的敏感或关键信息或信息处理设施的所有安全方面保持充分的、全面的控制和可见性。组织宜保持安全活动的可见性,诸如管理变更、脆弱性识别、按照规定的报告过程进行的信息安全事件报告和响应等。

15.2.2 供应商服务的变更管理

控制

宜管理供应商所提供服务的变更,包括维护和改进现有的信息安全策略、规程和控制,管理宜考虑变更涉及到的业务信息、系统和过程的关键程度及风险的再评估。

实现指南

宜考虑以下方面:

a) 供应商协议的变更;
b) 组织做出的变更以实现:
   1) 对当前提供服务的加强;
   2) 任何新应用程序和系统的开发;
   3) 组织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安全性;
c) 供应商服务做出的变更以实现:
   1) 网络的变更和强化;
   2) 新技术的应用;
   3) 新产品或新版本/发布的采用;
   4) 新工具和环境的开发;
   5) 服务设施物理位置的变更;
   6) 供应商的变更;
   7) 分包给其他供应商。

16 信息安全事件管理

16.1 信息安全事件的管理和改进

目标:确保采用一致和有效的方法对信息安全事件进行管理,包括对安全事态和弱点的沟通。

16.1.1 责任和规程

控制

宜建立管理责任和规程,以确保快速、有效和有序地响应信息安全事件。

实现指南

信息安全事件管理责任和规程宜考虑下列指南:

a) 宜建立管理责任以确保以下规程被制定并在组织内得到充分的交流:
   1) 规划和准备事件响应的规程;

2） 监视、发现、分析和报告信息安全事态和事件的规程；
3） 记录事件管理活动的规程；
4） 处理司法证据的规程；
5） 评估和决断信息安全事态以及评估信息安全弱点的规程；
6） 包括升级、事件的受控恢复、与内外部人员或组织沟通在内的响应的规程；

b） 所建立的规程宜确保：
1） 胜任的人员处理组织内的信息安全事件相关问题；
2） 建立安全事件发现和报告的联络点；
3） 维护与处理信息安全事件相关问题的部门、外部相关团体或论坛之间适当的联系；

c） 报告规程宜包含：
1） 准备信息安全事态报告表格，以便在信息安全事态发生时支持报告行动和帮助人员在报告时记住所有必要的行动；
2） 在信息安全事态发生时所采取的规程，例如立刻注意到所有细节（诸如不合规或违规的类型、发生的故障、屏幕上的消息），并立刻向联络点报告和仅采取协调行动；
3） 参考已建立的正式纪律处罚过程来处理安全违规的员工；
4） 适宜的反馈过程，以确保信息安全事态报告人员在问题被处理并关闭后得到结果的通知。

信息安全事件管理的目标宜与管理层商定，并宜确保信息安全事件管理责任人理解组织在处理信息安全事件上的优先级。

其他信息

信息安全事件可能超越组织和国家的边界。为了响应这类事件，与外部组织适时地协同响应和共享有关事件的信息的需要日益增加。

信息安全事件管理的详细指南见 ISO/IEC 27035[20]。

16.1.2 报告信息安全事态

控制

宜通过适当的管理渠道尽快地报告信息安全事态。

实现指南

所有员工和合同方人员都宜知道他们有责任尽可能快地报告信息安全事态。他们还宜知道报告信息安全事态的规程和联络点。

可进行信息安全事态报告的情况如下：

a） 无效的安全控制；
b） 违背信息完整性、保密性或可用性的预期；
c） 人为差错；
d） 不符合策略或指南；
e） 物理安全安排的违规；
f） 不受控的系统变更；
g） 软件或硬件的故障；
h） 非法访问。

其他信息

故障或其他异常的系统行为可能是安全攻击和实际安全违规的迹象，因此宜始终将其当作信息安全事态进行报告。

16.1.3 报告信息安全弱点

控制

宜要求使用组织信息系统和服务的员工和合同方注意并报告任何观察到的或可疑的系统或服务中

的信息安全弱点。

实现指南

为了防止信息安全事件，所有员工和合同方宜尽可能快地将这些问题向联络点报告。报告机制宜尽可能地简单、方便和可用。

其他信息

宜建议员工和合同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滥用，还可能引起对信息系统或服务的损害，并导致执行测试的人员在法律上的责任。

16.1.4 信息安全事态的评估和决策

控制

宜评估信息安全事态并决定其是否属于信息安全事件。

实现指南

联络点宜使用商定的信息安全事态和事件分级尺度评估每个信息安全事态，并决定该事态是否该归于信息安全事件。事件的分级和优先级有助于标识事件的影响和程度。

当组织中有信息安全事件响应团队(ISIRT)时，评估和决策可交至 ISIRT 进行确认和再评估。

宜详细记录评估和决策的结果，供日后参考和验证。

16.1.5 信息安全事件的响应

控制

宜按照文件化的规程响应信息安全事件。

实现指南

宜通过任命的联络点、组织内或外部方的相关人员对信息安全事件予以响应(见 16.1.1)。

响应宜包括：

a) 事件发生后尽快收集证据；

b) 按要求进行信息安全取证分析(见 16.1.7)；

c) 按要求升级；

d) 确保所有涉及的响应活动被适当记录，便于日后分析；

e) 本着按需知晓原则，与其他内部和外部人员或组织交流存在的信息安全事件及任何相关细节；

f) 处理发现的导致或促使事件发生的信息安全弱点；

g) 一旦事件被成功处理，正式将其关闭并记录。

必要时，宜进行事后事件分析以识别事件来源。

其他信息

事件响应的首要目的是重新回到“正常的安全水平”，然后启动必要的恢复。

16.1.6 从信息安全事件中学习

控制

宜利用在分析和解决信息安全事件中得到的知识来减少未来事件发生的可能性和影响。

实现指南

宜有能够量化和监视信息安全事件的类型、规模和代价的机制。宜利用从信息安全事件评价中获得的信息来识别易复发的或高影响的事件。

其他信息

信息安全事件的评价可能表明，需要强化或附加的控制来降低未来事件发生的频率、损害和代价，或在安全策略评审过程中加以考虑(见 5.1.2)。

在确保保密性的前提下，来自实际信息安全事件的案例可被用于意识培训（见 7.2.2），作为例子说明发生了什么、如何响应以及未来如何避免。

16.1.7 证据的收集

控制

组织宜确定和应用规程来识别、收集、获取和保存可用作证据的信息。

实现指南

宜制定内部规程，并在处理用于纪律和法律目的的证据时遵守。

一般来说，这些规程宜根据不同类型的介质、设备及设备状态（如开机或关机）提供证据识别、收集、获取和保存的过程。这些规程宜考虑：

a） 监管链；

b） 证据的安全；

c） 人员的安全；

d） 所涉及人员的角色和责任；

e） 人员的能力；

f） 文件化；

g） 简报。

可用时，宜寻求对人员和工具资格的认证或其他相关手段，以增强所保存证据的价值。

法律证据可能超越组织或司法管辖的边界。在这种情况下，宜确保组织有资格去收集作为法律证据所要求的信息。还宜考虑不同司法管辖区的要求，以使跨越相关司法管辖区的准入机会最大化。

其他信息

识别是包括搜索、辨认和记录潜在证据的过程。收集是聚集可能包含潜在证据的物证的过程。获取是在已定义的集合中创建数据拷贝的过程。保存是维护和保护潜在证据的完整性和原始状态的过程。

当一个信息安全事态被首次发现时，这个事态是否会导致法庭诉讼可能不是显而易见的。因此，在认识到事件的严重性之前，必要的证据被故意或意外毁坏的危险是存在的。如果预计要采取任何法律行动，最好及早请律师或警察介入，并接受关于所需证据的建议。

ISO/IEC 27037[24]提供数字证据的识别、收集、获取和保存的指南。

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

目标：宜将信息安全连续性纳入组织业务连续性管理之中。

17.1.1 规划信息安全连续性

控制

组织宜确定在不利情况（如危机或灾难）下，对信息安全及信息安全管理连续性的要求。

实现指南

组织宜确定在业务连续性管理过程或灾难恢复管理过程中是否包含了信息安全连续性。宜在计划业务连续性和灾难恢复时确定信息安全要求。

若没有正式的业务连续性和灾难恢复计划，信息安全管理宜假设与正常运行条件相比，不利情况下的信息安全要求仍保持不变。或者，组织能实施信息安全方面的业务影响分析以确定信息安全要求适

用于不利情况。

其他信息

为减少“额外的”信息安全方面的业务影响分析花费的时间和精力，建议从常规业务连续性管理或灾难恢复管理的业务影响分析中获取信息安全方面的信息。这可表明信息安全连续性要求在业务连续性管理或灾难恢复管理过程中已被明确制定。

业务连续性管理的更多信息参见 ISO/IEC 27031[14]、ISO 22313[9]和 ISO 22301[8]。

17.1.2 实现信息安全连续性

控制

组织宜建立、文件化、实现并维护过程、规程和控制，以确保在不利情况下信息安全连续性达到要求的级别。

实现指南

组织宜确保：

a) 具有一个适当的管理架构通过具有必要权限、经验和能力的人员来准备、减轻和响应中断事态；

b) 指派事件响应人员，其具有管理事件和维护信息安全的必要责任、授权和能力；

c) 基于受到管理层批准的信息安全连续性目标(见 17.1.1)，制定和批准文件化计划、响应和恢复规程，详细描述组织将如何管理中断事态，以及如何维护其信息安全达到一个预定的水平。

根据信息安全连续性要求，组织宜建立、记录、实现和维护：

a) 在业务连续性或灾难恢复过程、规程、支持系统和工具中的信息安全控制；

b) 在不利情况下维护现有信息安全控制的过程、规程和实现变更；

c) 在不利情况下不能维护的信息安全控制的补偿控制。

其他信息

针对业务连续性或灾难恢复，可能已确定了专用的过程和规程。宜保护在这些过程和规程中或其支持性信息系统中处理的信息。因此组织在建立、实现和维护业务连续性或灾难恢复过程和规程时，宜需要信息安全专家。

在不利情况下，已实现的信息安全控制宜继续运行。若安全控制不能继续保护信息，宜建立、实现和维护其他控制来保持信息安全在可接受水平。

17.1.3 验证、评审和评价信息安全连续性

控制

组织宜定期验证已建立和实现的信息安全连续性控制，以确保这些控制在不利情况下是正当和有效的。

实现指南

无论是在运行还是连续性情况下，组织的、技术的、规程的和过程变更都可导致信息安全连续性要求的变化。在这些情况下，宜针对这些变化评审信息安全连续性的过程、规程和控制。

组织宜通过以下方面验证其信息安全管理的连续性：

a) 演练和测试信息安全连续性过程、规程和控制的功能以确保其符合信息安全连续性目标；

b) 演练和测试信息安全连续性过程、规程和控制的常识和常规操作以确保其性能符合信息安全连续性目标；

c) 当信息系统、信息安全过程、规程和控制或业务连续性管理/灾难恢复管理过程和解决方案变更时，评审信息安全连续性措施的正确性和有效性。

其他信息

信息安全连续性控制的验证与一般信息安全测试和验证不同，宜在变更测试之外进行。如可能，信息安全连续性控制的验证宜与组织业务连续性或灾难恢复测试整合。

17.2 冗余

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

控制

信息处理设施宜具有足够的冗余以满足可用性要求。

实现指南

组织宜识别信息系统可用性的业务要求。当使用现有系统架构不能保证可用性时，宜考虑冗余组件或架构。

如可能，宜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。

其他信息

实现冗余可能给信息和信息系统的完整性或保密性带来风险，在设计信息系统时宜加以考虑。

18 符合性

18.1 符合法律和合同要求

目标：避免违反与信息安全有关的法律、法规、规章或合同义务以及任何安全要求。

18.1.1 适用的法律和合同要求的识别

控制

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

实现指南

为满足这些要求的特定控制和人员的责任宜同样加以定义并形成文件。

为满足其业务类型的要求，管理人员宜识别所有适用于其组织的法律。如果组织在其他国家开展业务，管理人员宜考虑符合性问题。

18.1.2 知识产权

控制

宜实现适当的规程，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。

实现指南

在保护被认为具有知识产权的材料时，宜考虑下列指南：

a) 发布一个知识产权符合性策略，该策略定义了软件和信息产品的合法使用；

b) 仅通过知名的和声誉好的渠道获得软件，以确保不侵犯版权；

c) 保持对保护知识产权的策略的了解，并通知对违规人员采取惩罚措施的意向；

d) 维护适当的资产登记簿，识别具有保护知识产权要求的所有资产；

e) 维护许可证、原版盘、手册等所有权的证明和证据；

f) 实现控制，以确保不超过所允许的最大用户数目；

g) 进行评审，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(胶片、音频)进行复制、格式转换或摘取内容；

l) 不对版权法不允许的书籍、文章、报告或其他文件中进行全部或部分地拷贝。

其他信息

知识产权包括软件或文件的版权、设计权、商标、专利权和源代码许可证。

通常具有所有权的软件产品的供应是根据许可协议进行的，该许可协议规定了许可条款和条件，例如，限制产品用于指定的机器或限制只能拷贝到创建的备份副本上。组织所开发的软件的知识产权重要性及其保护意识传达给员工。

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，这可能涉及罚款和犯罪诉讼。

18.1.3 记录的保护

控制

宜根据法律、法规、规章、合同和业务要求，对记录进行保护以防其丢失、毁坏、伪造、未授权访问和未授权发布。

实现指南

当决定保护特定的组织记录后，宜基于该组织分级方案考虑其相应级别。宜将记录按类型分类，例如，账号记录、数据库记录、事务日志、审计日志和运行规程，每个记录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。还宜保存与已加密的归档文件或数字签名(见第10章)相关的任何有关密钥材料，以使得记录在保存期内能够解密。

宜考虑存储记录的介质性能下降的可能性。宜按照制造商的建议实现存储和处理规程。

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

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

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

为满足这些记录防护目标，宜在组织范围内采取下列步骤：

a) 宜颁发关于保存、存储、处理和处置记录和信息的指南；

b) 宜起草一个保存时间计划，以标识记录及其要被保存的时间周期；

c) 宜维护关键信息来源的清单。

其他信息

某些记录可能需要安全地保存，以满足法令、法规或合同的要求，以及支持必要的业务活动。举例来说，可以要求这些记录作为组织在法令或法规规则下运行的证据，以确保充分防御潜在的民事或刑事诉讼，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保护

控制

宜依照相关的法律、法规和合同条款的要求，以确保隐私和个人可识别信息得到保护。

实现指南

针对隐私和个人可识别信息保护，宜制定和实现组织的数据策略。该策略宜通知到涉及个人可识别信息处理的所有人员。

符合该策略和所有相关的涉及个人隐私保护和个人可识别信息保护的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，如数据保护官员，该数据保护官员宜向管理人员、用户和服务提供商提供他们各自的职责以及宜遵守的特定规程的指南。处理个人可识别信息和确保了解数据保护原则的责任宜根据相关法律法规来确定。宜实现适当的技术和组织措施以保护个人可识别信息。

其他信息

ISO/IEC 29100[25]在信息和通信技术系统内提供了个人可识别信息保护的高层框架。许多国家已经发布控制个人可识别信息(一般是指可以从该信息确定生命个体的信息)收集、处理和传输的法律。根据各国法律，这种控制可以使那些收集、处理和传播个人可识别信息的人承担职责，而且可以限制将个人可识别信息转移到其他国家的能力。

18.1.5 密码控制规则

控制

密码控制的使用宜遵从所有相关的协议、法律和法规。

实现指南

为符合相关的协议、法律和法规，宜考虑以下事项：

a) 限制执行密码功能的计算机硬件和软件的入口或出口；

b) 限制被设计用以增加密码功能的计算机硬件和软件的入口或出口；

c) 限制加密技术的使用；

d) 国家主管部门对加密信息的强制或自主访问方法，该信息通过硬件或软件加密来提供其内容保密性。

宜征求法律建议，以确保符合国家法律法规。在将加密信息或密码控制跨越司法管辖边界转移之前，也宜获得法律建议。

18.2 信息安全评审

目标：确保依据组织策略和规程来实现和运行信息安全。

18.2.1 信息安全的独立评审

控制

宜按计划的时间间隔或在重大变化发生时，对组织的信息安全管理方法及其实现(如信息安全的控制目标、控制、策略、过程和规程)进行独立评审。

实现指南

管理者宜启动独立评审。对于确保一个组织管理信息安全的方法持续适宜、充分有效，这种独立评审是必要的。评审宜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。

这样的评审宜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宜具备适当的技能和经验。

独立评审的结果宜被记录并报告给启动评审的管理者。这些记录宜加以维护。

如果独立评审识别出组织管理信息安全的方法和实现不充分，例如，不符合信息安全策略文件（见5.1.1）中声明的信息安全的方向，管理者宜考虑纠正措施。

其他信息

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

18.2.2 符合安全策略和标准

控制

管理者宜定期评审其责任范围内的信息处理和规程与适当的安全策略、标准和任何其他安全要求的符合性。

实现指南

管理人员宜识别如何评审策略、标准和其他适用的法律法规规定的信息安全要求得到满足。为了高效的定期评审，宜考虑采用自动测量和报告工具。

如果评审结果发现任何不符合，管理人员宜：

a) 识别不符合的原因；

b) 评价达到符合性的措施需要；

c) 实现适当的纠正措施；

d) 评审所采取的纠正措施，验证其有效性，明确其缺陷或弱点。

宜记录并维护管理人员进行评审和采取纠正措施的结果。当在管理人员的责任范围内进行独立评审时，管理人员宜将结果报告给执行独立评审的人员（见18.2.1）。

其他信息

系统使用的运行监视见12.4。

18.2.3 技术符合性评审

控制

宜定期评审信息系统与组织的信息安全策略和标准的符合性。

实现指南

技术符合性宜更适合在自动化工具辅助下实现评审，来产生供技术专家进行后续解释的技术报告。或者，由有经验的系统工程师进行人工评审（必要时，在适当的软件工具支持下）。

如果使用渗透测试或脆弱性评估，则宜格外小心，因为这些活动可能导致系统安全的损害。这样的测试宜预先计划，形成文件，且可重复执行。

任何技术符合性评审宜仅由有能力的、已授权的人员来完成，或在他们的监督下完成。

其他信息

技术符合性评审包括运行系统的检查，以确保硬件和软件控制被正确实现。这种类型的符合性评审需要专业技术知识。

符合性评审还包括，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。符合性评审有助于发现系统的脆弱性，并有助于检查控制是否能有效预防由于这些脆弱性导致的未授权访问。

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。该快照仅限于渗透攻击期间实际被测试的系统部分。渗透测试和脆弱性评估不能代替风险评估。

ISO/IEC TR 27008[13]提供了技术符合性评审的专门指南。

附 录 NA
（资料性附录）
GB/T 22081—2016 与 GB/T 22081—2008 对比

表 NA.1 GB/T 22081—2016 与 GB/T 22081—2008 对比表

GB/T 22081—2016	GB/T 22081—2008
5 信息安全策略	
5.1 信息安全管理指导	
5.1.1 信息安全策略	5.1.1 信息安全方针文件
5.1.2 信息安全策略的评审	5.1.2 信息安全方针的评审
6 信息安全组织	
6.1 内部组织	
6.1.1 信息安全的角色和责任	6.1.3 信息安全职责的分配 8.1.1 角色和职责
6.1.2 职责分离	10.1.3 责任分割
6.1.3 与职能机构的联系	6.1.6 与政府部门的联系
6.1.4 与特定相关方的联系	6.1.7 与特定利益集团的联系
6.1.5 项目管理中的信息安全	新的控制
6.2 移动设备和远程工作	
6.2.1 移动设备策略	11.7.1 移动计算和通信
6.2.2 远程工作	11.7.2 远程工作
7 人力资源安全	
7.1 任用前	
7.1.1 审查	8.1.2 审查
7.1.2 任用条款及条件	8.1.3 任用条款和条件
7.2 任用中	
7.2.1 管理责任	6.1.1 信息安全的管理承诺 8.2.1 管理职责
7.2.2 信息安全意识、教育和培训	8.2.2 信息安全意识、教育和培训
7.2.3 违规处理过程	8.2.3 纪律处理过程
7.3 任用的终止和变更	
7.3.1 任用终止或变更的责任	8.3.1 终止职责
8 资产管理	
8.1 有关资产的责任	
8.1.1 资产清单	7.1.1 资产清单
8.1.2 资产的所属关系	7.1.2 资产责任人

表 NA.1（续）

GB/T 22081—2016	GB/T 22081—2008
8.1.3 资产的可接受使用	7.1.3 资产的可接受使用
8.1.4 资产归还	8.3.2 资产的归还
8.2 信息分级	
8.2.1 信息的分级	7.2.1 分类指南
8.2.2 信息的标记	7.2.2 信息的标记和处理
8.2.3 资产的处理	7.2.2 信息的标记和处理 10.7.3 信息处理规程
8.3 介质处理	10.7 介质处置
8.3.1 移动介质的管理	10.7.1 可移动介质的管理
8.3.2 介质的处置	10.7.2 介质的处置
8.3.3 物理介质的转移	10.8.3 运输中的物理介质
9 访问控制	
9.1 访问控制的业务要求	
9.1.1 访问控制策略	11.1.1 访问控制策略
9.1.2 网络和网络服务的访问	11.4.1 使用网络服务的策略
9.2 用户访问管理	
9.2.1 用户注册和注销	11.2.1 用户注册
9.2.2 用户访问供给	11.2.1 用户注册 11.2.2 特殊权限管理
9.2.3 特定访问权管理	11.2.2 特殊权限管理
9.2.4 用户的秘密鉴别信息管理	11.2.3 用户口令管理 11.5.2 用户标识和鉴别
9.2.5 用户访问权的评审	11.2.4 用户访问权的复查
9.2.6 访问权的移除或调整	8.3.3 撤销访问权
9.3 用户责任	
9.3.1 秘密鉴别信息的使用	11.3.1 口令使用
9.4 系统和应用访问控制	
9.4.1 信息访问限制	11.6.1 信息访问限制 11.6.2 敏感系统隔离
9.4.2 安全登录规程	11.5.1 安全登录规程 11.5.5 会话超时 11.5.6 联机时间的限定
9.4.3 口令管理系统	11.2.3 用户口令管理 11.5.4 系统实用工具的使用

表 NA.1（续）

GB/T 22081—2016	GB/T 22081—2008
9.4.4 特权实用程序的使用	11.5.4 系统实用工具的使用
9.4.5 程序源代码的访问控制	12.4.3 对程序源代码的访问控制
10 密码	
10.1 密码控制	
10.1.1 密码控制的使用策略	12.3.1 使用密码控制的策略
10.1.2 密钥管理	12.3.2 密钥管理
11 物理和环境安全	
11.1 安全区域	
11.1.1 物理安全边界	9.1.1 物理安全周边
11.1.2 物理入口控制	9.1.2 物理入口控制
11.1.3 办公室、房间和设施的安全保护	9.1.3 办公室、房间和设施的安全保护
11.1.4 外部和环境威胁的安全防护	9.1.4 外部和环境威胁的安全防护
11.1.5 在安全区域工作	9.1.5 在安全区域工作
11.1.6 交接区	9.1.6 公共访问、交接区安全
11.2 设备	
11.2.1 设备安置和保护	9.2.1 设备安置和保护
11.2.2 支持性设施	9.2.2 支持性设施
11.2.3 布缆安全	9.2.3 布缆安全
11.2.4 设备维护	9.2.4 设备维护
11.2.5 资产的移动	9.2.7 资产的移动
11.2.6 组织场所外的设备与资产安全	9.2.5 组织场所外的设备安全
11.2.7 设备的安全处置或再利用	9.2.6 设备的安全处置或再利用
11.2.8 无人值守的用户设备	11.3.2 无人值守的用户设备
11.2.9 清理桌面和屏幕策略	11.3.3 清空桌面和屏幕策略
12 运行安全	
12.1 运行规程和责任	
12.1.1 文件化的操作规程	10.1.1 文件化的操作规程
12.1.2 变更管理	10.1.2 变更管理
12.1.3 容量管理	10.3.1 容量管理
12.1.4 开发、测试和运行环境的分离	10.1.4 开发、测试和运行设施分离
12.2 恶意软件防范	
12.2.1 恶意软件的控制	10.4.1 控制恶意代码 10.4.2 控制移动代码
12.3 备份	

表 NA.1（续）

GB/T 22081—2016	GB/T 22081—2008
12.3.1 信息备份	10.5.1 信息备份
12.4 日志和监视	10.10 监视
12.4.1 事态日志	10.10.1 审计记录
12.4.2 日志信息的保护	10.10.3 日志信息的保护
12.4.3 管理员和操作员日志	10.10.4 管理员和操作员日志
12.4.4 时钟同步	10.10.6 时钟同步
12.5 运行软件控制	
12.5.1 运行系统软件的安装	12.4.1 运行软件的控制
12.6 技术方面的脆弱性管理	
12.6.1 技术方面脆弱性的管理	12.6.1 技术脆弱性的控制
12.6.2 软件安装限制	新的控制
12.7 信息系统审计的考虑	
12.7.1 信息系统审计控制	15.3.1 信息系统审计控制措施
13 通信安全	
13.1 网络安全管理	
13.1.1 网络控制	10.6.1 网络控制 11.4.3 网络上的设备标识
13.1.2 网络服务的安全	10.6.2 网络服务安全
13.1.3 网络中的隔离	11.4.5 网络隔离
13.2 信息传输	
13.2.1 信息传输策略和规程	10.8.1 信息交换策略和规程
13.2.2 信息传输协议	10.8.2 交换协议
13.2.3 电子消息发送	10.8.4 电子消息发送
13.2.4 保密或不泄露协议	6.1.5 保密性协议
14 系统获取、开发和维护	
14.1 信息系统的安全要求	
14.1.1 信息安全要求分析和说明	12.1.1 安全要求分析和说明
14.1.2 公共网络上应用服务的安全保护	10.9.1 电子商务
14.1.3 应用服务事务的保护	10.9.2 在线交易
14.2 开发和支持过程中的安全	
14.2.1 安全的开发策略	新的控制
14.2.2 系统变更控制规程	12.5.1 变更控制规程
14.2.3 运行平台变更后对应用的技术评审	12.5.2 操作系统变更后应用的技术评审
14.2.4 软件包变更的限制	12.5.3 软件包变更的限制

表 NA.1（续）

GB/T 22081—2016	GB/T 22081—2008
14.2.5 系统安全工程原则	新的控制
14.2.6 安全的开发环境	新的控制
14.2.7 外包开发	12.5.5 外包软件开发
14.2.8 系统安全测试	新的控制
14.2.9 系统验收测试	10.3.2 系统验收
测试数据	
14.3.1 测试数据的保护	12.4.2 系统测试数据的保护
15 供应商关系	
15.1 供应商关系中的信息安全	
15.1.1 供应商关系的信息安全策略	新的控制
15.1.2 在供应商协议中强调安全	6.2.3 处理第三方协议中的安全问题
15.1.3 信息与通信技术供应链	新的控制
15.2 供应商服务交付管理	
15.2.1 供应商服务的监视和审查	10.2.1 服务交付 10.2.2 第三方服务的监视和评审
15.2.2 供应商服务的变更管理	10.2.3 第三方服务的变更管理
16 信息安全事件管理	
16.1 信息安全事件的管理和改进	
16.1.1 责任和规程	13.2.1 职责和规程
16.1.2 报告信息安全事态	13.1.1 报告信息安全事态
16.1.3 报告信息安全弱点	13.1.2 报告安全弱点
16.1.4 信息安全事态的评估和决策	新的控制
16.1.5 信息安全事件的响应	新的控制
16.1.6 从信息安全事件中学习	13.2.2 对信息安全事件的总结
16.1.7 证据的收集	13.2.3 证据的收集
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 规划信息安全连续性	14.1.1 在业务连续性管理过程中包含信息安全 14.1.3 制定和实施包含信息安全的连续性计划
17.1.2 实现信息安全连续性	14.1.3 制定和实施包含信息安全的连续性计划
17.1.3 验证、评审和评价信息安全连续性	14.1.5 测试、维护和再评估业务连续性计划
17.2 冗余	
17.2.1 信息处理设施的可用性	新的控制
18 符合性	
18.1 符合法律和合同要求	

表 NA.1（续）

GB/T 22081—2016	GB/T 22081—2008
18.1.1　适用的法律和合同要求的识别	15.1.1　可用法律的识别
18.1.2　知识产权	15.1.2　知识产权(IPR)
18.1.3　记录的保护	15.1.3　保护组织的记录
18.1.4　隐私和个人可识别信息保护	15.1.4　数据保护和个人信息的隐私
18.1.5　密码控制规则	15.1.6　密码控制措施的规则
18.2　信息安全评审	
18.2.1　信息安全的独立评审	6.1.8　信息安全的独立评审
18.2.2　符合安全策略和标准	15.2.1　符合安全策略和标准
18.2.3　技术符合性评审	15.2.2　技术符合性核查

附 录 NB
（资料性附录）
GB/T 22081—2016 与 GB/T 22081—2008 主要关键词变化

Control “控制措施”改为“控制”。
Implement “实施”改为“实现”。
Maintain “保持”改为“维护”。
asset owner“资产责任人”改为“资产拥有者”。

参 考 文 献

[1] ISO/IEC 导则 第二部分

[2] ISO/IEC 11770-1 信息技术 安全技术 密钥管理 第1部分:框架

[3] ISO/IEC 11770-2 信息技术 安全技术 密钥管理 第2部分:使用对称技术的机制

[4] ISO/IEC 11770-3 信息技术 安全技术 密钥管理 第3部分:使用非对称技术的机制

[5] ISO 15489-1 信息和文献 记录管理 第1部分:总则

[6] ISO/IEC 20000-1 信息技术 服务管理 第1部分:服务管理系统要求

[7] ISO/IEC 20000-2[1)] 信息技术 服务管理 第2部分:服务管理系统的应用指南

[8] ISO 22301 公共安全 业务连续性管理体系 要求

[9] ISO 22313 公共安全 业务连续性管理体系 指南

[10] GB/T 22080 信息技术 安全技术 信息安全管理体系 要求

[11] ISO/IEC 27005 信息技术 安全技术 信息安全风险管理

[12] ISO/IEC 27007 信息技术 安全技术 信息安全管理体系审核指南

[13] ISO/IEC TR 27008 信息技术 安全技术 信息安全控制审核员指南

[14] ISO/IEC 27031 信息技术 安全技术 信息和通信技术业务连续性准备指南

[15] ISO/IEC 27033-1 信息技术 安全技术 网络安全 第1部分:概述和概念

[16] ISO/IEC 27033-2 信息技术 安全技术 网络安全 第2部分:网络安全设计和实现指南

[17] ISO/IEC 27033-3 信息技术 安全技术 网络安全 第3部分:网络场景参考—威胁、设计技术和控制问题

[18] ISO/IEC 27033-4 信息技术 安全技术 网络安全 第4部分:使用安全网关的网间通信安全保护

[19] ISO/IEC 27033-5 信息技术 安全技术 网络安全 第5部分:使用虚拟专用网的跨网通信安全保护

[20] ISO/IEC 27035 信息技术 安全技术 信息安全事件管理

[21] ISO/IEC 27036-1 信息技术 安全技术 供应商关系的信息安全 第1部分:概述和概念

[22] ISO/IEC 27036-2 信息技术 安全技术 供应商关系的信息安全 第2部分:通用要求

[23] ISO/IEC 27036-3 信息技术 安全技术 供应商关系的信息安全 第3部分:ICT供应链安全指南

[24] ISO/IEC 27037 信息技术 安全技术 数字证据的识别、收集、采集和保存

[25] ISO/IEC 29100 信息技术 安全技术 隐私保护框架

[26] ISO/IEC 29101 信息技术 安全技术 隐私保护架构框架

[27] ISO 31000 风险管理 原则和指南

中 华 人 民 共 和 国
国 家 标 准
信息技术 安全技术
信息安全控制实践指南
GB/T 22081—2016/ISO/IEC 27002:2013
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 4.75 字数 139 千字
2016 年 10 月第一版 2016 年 10 月第一次印刷
*
书号:155066·1-55200 定价 63.00 元

GB/T 22081-2016