Information Technology-
Security Techniques-
Code of practice for information security management

信息技术
安全技术
信息安全管理实施指南

目录

Ⅰ版本说明

版本	日期	作者	备注
V1.0	2005/11	刘青	

II 文件说明

本套中文版文件是笔者利用业余时间自行翻译的。因笔者水平有限，其中错误和遗漏之处再说难免。欢迎各位安全界同仁批评指正。

但是需要特别声明的是，若因阅读、使用本文而给读者造成的任何形式的损失，本人不承担任何责任。

本文中文版文件的著作权归本人所有。本文仅供网上阅读学习之用，亦可通过电子文件复制的方式进行传播。未经授权，不得用于任何商业目的。

笔者联系方式：

邮箱：liuq1217@163.com

MSN：liuq1217@msn.com

手机：138 1116 0364

刘青

BS7799LA

2005 年 12 月草于北京

III 前言

ISO（国际标准组织）和IEC（国际电工委员会）形成了世界范围内标准化的专门体系。ISO 或IEC的成员国家通过技术委员会参与国际标准的研究制定，这些技术委员会是由相关组织建立的用来管理某一特定领域的技术活动。ISO 和IEC 技术委员会在共同感兴趣的领域中合作，其他与ISO 和IEC 有联络关系的政府和非政府的国际组织也参与其工作。

国际标准遵照ISO/IEC 导则第2 部分给出的规则起草。

在信息技术领域，ISO 和IEC 建立了一个联合技术委员会：ISO/IEC JTC1。国际标准ISO/IEC 17799是由联合技术委员会ISO/IEC JTC 1 信息技术子委员会SC27 第一工作组：需求、安全服务和指南工作组负责筹备制定的。

需要引起注意的是ISO/IEC 17799 的一些部分可能具有专利权的问题。ISO 不承担辨别任何或所有这种专利权的责任

0 简介

0.1 什么是信息安全？

信息是一种资产，就象其它重要的业务资产一样，对于组织的业务是不可或缺的，因此需要妥善保护。这种保护在当今互连日益紧密的业务环境中尤为重要。正是因为互连的增加，将信息暴露给数量更多、范围更广的威胁和脆弱点（参见 OECD 信息系统和网络安全指南）。

信息可以以多种方式存在，可以打印或书写在纸张上，以电子文档形式存储，通过邮寄或电子方式传播，以胶片形式显示或在交谈中表达出来。无论采取何种方式或手段进行共享或存储，都应加以妥善保护。

信息安全就是要保护信息免受威胁的影响，从而确保业务的连续性，缩减业务风险，最大化投资收益并充分把握业务机会。

应通过实施一整套适当的控制措施来实现信息安全。控制措施包括策略、过程、程序、组织结构和软硬件功能。需建立、实施、监视、评审，适当时改进这些控制措施，从而确保实现组织特定的安全和业务目标。这一过程应与组织的其他业务管理过程共同实施。

0.2 为什么需要信息安全

信息和支持性过程、系统和网络都是重要的业务资产。规定、实现、保持和改进信息安全对于保持竞争优势、现金流、盈利能力、法律符合性及商业形象都是至关重要的。

组织及其信息系统和网络也要面临来自多个方面的威胁，包括计算机辅助欺诈、间谍、心怀不满的员工、故意破坏、火灾或水灾。危害的来源也是多种多样，如恶意代码、计算机黑客和拒绝服务攻击（DOS）等也变得更加普遍、大胆和复杂。

信息安全对于公共或私人业务以及关键的基础设施都是很重要的。无论在那一方面，如电子政务或电子商务，信息安全都将有助于避免或降低有关的风险。公共网络与专用网络的互连以及信息资源的共享，都增加了实现访问控制的难度。分布式计算的趋势也降低了集中管理的有效性。

很多信息系统在设计时，没有考虑到安全问题。通过技术手段获得的安全保障是十分有限的，必须辅之以相应的管理和程序。确定需要使用什么控制措施需要周密计划，并对细节问题加以注意。作为信息安全管理的最基本要求，组织的全体员工都应参与到信息安全管理中来。信息安全管理可能还需要股东、供应商、第三方、顾客或其他外部机构的参与，也需要组织外部专家的建议。

0.3 如何确定安全要求

组织应确定其安全要求。安全要求有三个主要来源：

1. 第一个来源是组织风险评估的结果。进行风险评估时，应考虑组织的整体业务战略及业务目标。通过风险评估，识别对资产的威胁，评价脆弱点及发生的可能性，并评估其影响。
2. 第二个来源是组织、其商业伙伴、合同商和服务提供商必须满足的法律、法规、规章和合同要求以及社会文化环境；
3. 第三个来源是组织为支持其业务运作而为信息处理规定的一套专门的原则、目标和业务要求。

0.4 评估安全风险

应通过系统的安全风险评估来识别安全要求。应将实施控制措施的支出与安全失效所可能导致的业务影响权衡考虑。

风险评估的结果将为信息安全风险管理和实施选择的控制措施来防范风险，提供指导并确定适当的管理措施和优先级。

应定期重复进行风险评估，以阐述任何可能影响风险评估结果的变更。

关于安全风险评估的更多信息，参见 4.1“评估安全风险”。

0.5 选择控制措施

一旦确定了安全要求和风险并做出风险处置的决策，则应选择并实施适当的控制措施以确保将风险降低到可接受的程度。可以从本标准或其它标准选择控制措施，适当时，也可设计新的控制措施以满足特定要求。应在组织确定的风险接受准则、风险处置选项以及组织应用的整体风险管理方法的基础上，选择安全控制措施并遵守所有相关的国家或国际法律法规。

本标准中的一些控制措施可以作为信息安全管理的指导性原则，并适用于大多数组织。将在 0.6“信息安全起点”条款中予以详细阐述。

关于选择控制措施和其他风险处置选项的更多信息，参见 4.2“处置安全风险”条款。

0.6 信息安全起点

许多控制措施都为实施信息安全提供了一个良好的起点。这些控制措施或者是基于基本的法律法规要求，或者是信息安全的通用惯例。

从法律法规的角度来看，对组织至关重要的控制措施包括：

a) 数据保护和个人信息隐私（参见 15.1.4）；
b) 组织记录的保护（参见 15.1.3）；
c) 知识产权（参见 15.1.2）。

信息安全的通用惯例包括：

a) 信息安全策略文档（参见 5.1.1）；

b) 信息安全责任的分配（参见 6.1.3）；

c) 信息安全意识、教育与培训（参见 8.2.2）；

d) 应用程序的正确处理（参见 12.2）；

e) 脆弱点管理（参见 12.6）；

f) 业务连续性管理（参见 14）；

g) 信息安全事故管理及改进（参见 13.2）。

这些控制措施适用于大多数组织，并可在大多数环境中使用。

需要注意的是，尽管本标准中的控制多时都很重要并且要予以考虑，但是控制措施是否适当，还是取决于组织所面临的特定风险。因此，尽管上述方法是一个良好的起点，但是不能取代根据风险评估结果选择的控制措施。

0.7 关键成功因素

经验表明，下列因素对于组织成功地实施信息安全通常是非常关键的：

a) 反映业务目标的信息安全策略、目标和活动；

b) 与组织文化保持一致的实施、保持、监视和改进信息安全的方法或框架；

c) 来自管理层的实际支持和承诺；

d) 对信息安全要求、风险评估和风险管理有着良好的理解；

e) 向所有的管理者、雇员和他方宣传安全，以提高安全意识；

f) 向所有的管理者、雇员和他方发布关于信息安全策略和标准的指南；

g) 为信息安全管理活动提供资金支持；

h) 提供适当的意识、教育和培训；

i) 建立有效的信息安全事故管理过程；

j) 实施测量系统，用于用于评价信息安全管理和反馈的改进建议。

0.8 开发组织自己的指导方针

本实施指南可作为制定组织特定指导方针的起点。本实施指南中的所有控制措施或指南并非全都适用。此外，可能还需要本指南未能涵盖的控制措施或指南。当开发出包含其他指南和控制措施的文档后，与本标准条款的相互引用将有助于审核员和业务伙伴进行符合性检查。

1. 范围

本标准给在组织内引进、实施、维护和改进信息安全管理提供指导和通用准则。本标准中列举的控制目标为信息安全管理通用目标提供通用指南。

控制的目的额此国际通行标准的控制措施是为了满足风险评估的需要。这些国际标准将作为实践指导服务于组织安全标准的建立，并作用于安全的实践管理，最终帮助建立组织相互交易的信心。

2. 术语与定义

注：

新版 ISO17799 共采用术语 17 个，其中采用 ISO/IEC 13335-1:2004 4 个，ISO/IEC TR 18044 2 个，ISO Guide 73：2002 6 个，ISO Guide 2：1996 1 个，其余 4 个为本标准所规定。

本标准采用以下术语和定义：

2.1 资产

任何对于组织具有价值的事物

[ISO/IEC 13335-1:2004]

2.2 控制措施

管理风险的方法，包括方针（策略）、程序、指南、惯例或组织架构，这些方法可以是行政的、技术的、管理的或法律的。

2.3 指南

阐明为实现方针中设立的目标应该做什么和怎么做的描述

[ISO/IEC 13335-1:2004]

2.4 信息处理设施

任何信息处理系统、服务或基础设施，或放置他们的物理场所。

2.5 信息安全

保护信息的保密性、完整性、可用性及其他属性，如：真实性、可核查性、可靠性、防抵赖性。

2.6 信息安全事件 information security event

信息安全事件是指系统、服务或网络的一种可识别的状态的发生，它可能是对信息安全策略的违反或防护措施的失效，或是和安全关联的一个先前未知的状态。
[ISO/IEC TR 18044]

2.7 信息安全事故 information security incident

一个信息安全事故由单个的或一系列的有害或意外信息安全事件组成，它们具有损害业务运作和威胁信息安全的极大的可能性。
[ISO/IEC TR 18044]

2.8 方针

管理层正式发布的总体意图与方向。

2.9 风险

事件发生的可能性和后果的结合。
[ISO Guide 73：2002]

2.10 风险分析

系统地使用信息以识别来源和估计风险。
[ISO Guide 73：2002]

2.11 风险评估

风险分析和风险评价的全过程
[ISO Guide 73：2002]

2.12 风险评价

将估计的风险与既定的风险准则进行比较以确定重要风险的过程。
[ISO Guide 73：2002]

2.13 风险管理

指导和控制一个组织的风险的协调的活动。
[ISO Guide 73：2002]
注：典型风险管理包括风险评估、风险处置、风险接受和风险沟通。

2.14 风险处置

选择和实施措施以改变风险的过程。
[ISO Guide 73：2002]

2.15 第三方

当考虑一个问题时，被认为是独立于涉及方的人员或实体。
[ISO Guide 2：1996]

2.16 威胁

非预期事件地潜在原因，这些事件可能对系统或组织造成损害。

[ISO/IEC 13335-1:2004]

2.17 脆弱性

可能被一个或多个威胁利用的一个或一组资产的弱点。

[ISO/IEC 13335-1:2004]

注：笔者认为该定义存在缺陷，敬请诸位读者自行确定

3 本标准的架构

本标准包括 11 个安全控制条款，39 个主要安全类和一个风险评估和处置的介绍性条款。

3.1 条款

每个条款都包括许多主要的安全类。这 11 个条款是（小括号中的数字表示该条款中包括的主要的安全类数量）：

a) 信息安全方针（1）
b) 组织信息安全（2）
c) 资产管理（2）
d) 人力资源安全（3）
e) 物理和环境安全（2）
f) 通信和操作管理（10）
g) 访问控制（7）
h) 信息系统的获取、开发和维护（6）
i) 信息安全事故管理（2）
j) 业务连续性管理（1）
k) 符合性（3）

注：条款不以其重要程度为排名的先后顺序。根据环境的需要，所有的条款可能都是重要的，所以每个组织在使用本标准时都需要识别出适用的条款、其重要度以及他们在单个业务过程中的应用。同样，此标准中的所有列表都无先后之分，除非特别声明。

3.2 主要安全类

每个安全类包括：

a) 一个控制目标，陈述要实现什么；
b) 一个或多个控制措施，可用于实现控制目标。

控制措施的描述分为以下结构：

控制措施

规定特定的控制措施以满足控制目标。

实施指南

提供更为详细的信息以支持控制措施的实施从而满足控制目标。部分指南可能并不适用于所有的情况，因此可以考虑其他适宜的控制措施。

其他信息

提供可能需要考虑的其他信息，如法律和参考其他的标准。

4 风险评估和处置

4.1 评估安全风险

风险评估应当根据风险接受准则以及与组织有关的目标来识别、量化和排列风险的优先顺序。风险评估的结果应指导和确定适当的管理措施、信息安全风险的优先顺序及实施以及挂选择的可以防范这些风险的控制措施。可能需要重复地进行风险评估并选择控制措施，从而可以涵盖组织的不同部分或单个信息系统。

风险评估应包括评价风险程度的系统化的方法（风险分析）以及将估计的风险与风险准则进行比较从而确定风险重要程度的过程（风险评价）。

应定期进行风险评估，以阐述安全要求和风险情况的变化，如在资产、威胁、脆弱点、影响、风险评价等方面的变化。当发生重要变化时，应重新进行风险评估。应采用系统化的方式进行风险评估，从而可以产生可比较的和可复制的结果。

应清晰规定信息安全风险评估的范围，从而确保信息安全风险评估的有效性，适当时应包括在其他区域进行的风险评估的关系。

风险评估的范围可以是整个组织、组织的一部分、单独的信息系统、特定的系统组件或服务。风险评估方法的示例在 ISO/IEC TR 13335-3 中描述。

注：根据 ISO13335-1:2004 标准中的内容，新版的 ISO13335 共包含 2 个部分。该处所说的 ISO/IEC TR 13335-3 为旧版的标准，敬请注意。

4.2 安全风险的处置

进行风险处置之前，组织应确定风险是否可接受的准则。风险可能是被接受的，如低风险或风险的处置对于组织来说不是成本有效的。应记录这些决定。

对于风险评估确定的每一个风险都应考虑风险的处置决定。处置风险的可选方案包括：

a) 采用适宜的控制措施削减风险；
b) 客观地并有意识地接受风险，确保其满足组织的策略和风险接受标准；
c) 不采纳可能导致风险的措施从而避免风险；
d) 将风险转嫁给其他方，如保险公司或供应商。

风险处置决定应当采用适当的风险控制措施，应选择并实施这些控制措施以满足风险评估所确定的要求。控制措施应确保可以将风险削减倒可接受的程度。选择控制措施应考虑以下方面的内容：

a) 本国或国际法律法规的要求和限制；

b) 组织目标；
c) 运营的要求和限制；
d) 应削减与风险有关的实施和运行成本，并与组织的要求和限制条件保持一致；
e) 需权衡控制措施实施及运营的投资和安全失效可能导致的损害。

可以从本标准或其他标准中选择控制措施，也可以设计新的控制措施来满足组织的特定需要。需要注意的是，部分控制措施可能并不适用于每一个信息系统或环境，也可能并不适用于每一个组织。例如，10.1.3 条款描述了如何进行职责分离从而防止欺诈或错误。该条款可能就不适用于小型组织，因此需要考虑其他的方法来实现这一控制目标。再如，10.10 条款描述了如何监视系统的使用以及如何收集证据。这一控制可能，如事件日值可能与适用的法律法规相冲突，如顾客或工作场所的隐私保护方面的法律法规。

应在系统或项目要求规范和设计阶段考虑信息安全控制措施。如果未能这么做，将可能导致额外的成本掷出，并可能削减解决措施的有效性，在最糟糕的情况下，可能无法实现充分的安全。

应该认识到任何一种控制模式都不达到完全的安全。因此应实施另外的管理措施从而来监视、评价并改进安全控制措施的效率和有效性，已支持组织业务目标的实现。

5. 安全方针

5.1 信息安全方针

目标：为信息安全提供管理指导和支持，并与业务要求和相关的法律法规保持一致。

管理者应根据业务目标制定清晰的方针方向，并通过在整个组织中颁发和维护信息安全方针来表明对信息安全的支持和承诺。

5.1.1 信息安全策略文档

控制：

信息安全方针文档应经过管理层的批准，并传达给所有雇员和外部相关方。

实施指南：

信息安全方针应阐述管理层的承诺，并规定组织管理信息安全的方法。该策略文档应包括以下方面的陈述：

a) 信息安全的定义、其整体目标和范围以及安全作为保障信息安全共享机制的重要性（参看简介）；
b) 陈述信息安全的管理意图、支持性目标和准则，并与业务战略和目标保持一致；
c) 设立控制目标和控制措施的框架，包括风险评估和风险管理的架构；
d) 对安全方针、准则、标准的简介，也包括对机构有特别重要性的法律的要求，例如：
   1) 要符合法律及合同要求；
   2) 安全教育、培训、意识的要求；
   3) 业务连续性管理；
   4) 违反安全方针的后果。
e) 信息安全管理的一般的和特定的责任的定义，包括报告安全事件；
f) 支持该方针的文档的参考说明，如更详尽的安全策略，特定信息系统的程序，用户应该遵守的或安全规则。

应以预期的读者适合的、可访问的和可理解的形式将信息安全方针传递给整个组织的用户。

其他信息

信息安全方针可能是总体方针文件的一部分。如果信息安全方针在组织外进行分发，应注意不要泄露敏感信息。更多内容参考 ISO/IEC 13335-1：2004。

5.1.2 信息安全方针评审

控制：

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，以确保它的持续适宜性、充分性和有效性。

实施指南：

信息安全方针应有专人负责，他具有安全方针制定、评审和评估的管理职责。评审应包括评估组织信息安全方针的改进的机会和适应组织环境、业务状况、法律条件或技术环境变化的信息安全管理方法。

信息安全方针评审应考虑管理评审的结果。要定义管理评审程序，包括时间表或评审周期。

管理评审的输入应包括以下信息：

a) 相关方的反馈；
b) 独立评审的结果（见6.1.8）；
c) 预防和纠正措施的状态（见6.1.8 和15.2.1）；
d) 以往管理评审的结果；
e) 执行情况和信息安全方针符合性；
f) 可能影响组织管理信息安全方法的变化，包括组织环境、业务状况、资源可用性、合同、法律法规的条件或技术环境的变化。
g) 关于威胁和脆弱点的趋势；
h) 已报告的信息安全事故（见13.1）；
i) 相关专家的建议（见6.1.6）。

管理评审的输出应包括与以下方面有关的任何决定和措施；

a) 组织管理信息安全的方法和它的执行过程的改进；
b) 控制目标和控制措施的改进
c) 资源和/或职责分配的改进。

管理评审的记录应被维护。

应获得管理者对方针修订的批准。

6 组织信息安全

6.1 内部组织

目标：管理组织内部的安全

应建立管理框架，以启动和控制组织范围内的信息安全的实施。
管理者应批准整个组织内的信息安全方针、分配安全角色并协调和评审安全的实施。
若需要，要在组织范围内建立信息安全专家建议的资料源，并在整个组织内均可获得该资料。
要发展与外部安全专家或组织（包括相关权威人士）的联系，以便跟上行业发展趋势、跟踪标准和评估方法，并且当处理信息安全事故时，提供合适的联络地点。应鼓励信息安全的多学科交叉途径。

6.1.1 信息安全管理承诺

控制：

管理者应通过清晰的方向、说明性承诺、明确的信息安全职责分配和确认，来积极的支持组织内的安全。

实施指南

管理者应：

a) 确保信息安全目标得以识别，满足组织需求，并已被整合到相关过程中；
b) 制定、评审、批准信息安全方针；
c) 评审信息安全方针实施的有效性；
d) 为安全举措提供清晰的方向和可视化的管理者支持；
e) 为信息安全提供所需的资源；
f) 批准整个组织内信息安全特定角色和职责的分配；
g) 启动计划和程序来保持信息安全意识；
h) 确保整个组织内的信息安全控制的实施相互协调；（见6.1.2）。

管理者应识别寻求内外部专家的信息安全建议的需要，并在整个组织内评审和协调建议结果。

根据组织的规模不同，这些职责可以由一个专门的管理协调小组或由一个已存在的机构（例如董事会）承担。

其他信息：

更多内容可参考 ISO/IEC TR 13335-1：2004。

6.1.2 信息安全协调

控制：

信息安全活动应由来自组织不同部门并具备相关角色和工作职责的代表进行协调。

实施指南：

典型的，信息安全协调应包含管理人员、用户、行政人员、应用设计人员、审核员和安全专员，以及各领域专家技术的协调和协作，这些领域包括保险、法律问题、人力资源、IT或风险管理等。这些活动应：

a) 确保安全活动的实施与信息安全方针相一致；
b) 确定如何处理不符合；
c) 核准信息安全相关的方法和过程，例如风险评估、信息分类；
d) 识别重大的威胁变化和信息系统内暴露于威胁下的信息和信息处理过程；
e) 评估信息安全控制实施的充分性性和协调性；
f) 有效地促进整个组织内的信息安全教育、培训和意识；
g) 评价在信息安全事故的监视和评审中获得的信息，推荐适当的措施响应识别的信息安全事故。

如果组织没有使用一个独立的跨部门的小组，例如因为这样的小组对组织规模来说是不适当的，那么上面描述的措施应由其它的合适的管理机构或单独管理人员实施。

6.1.3 信息安全职责分配

控制：

所有的信息安全职责应予以清晰地定义。

实施指南：

信息安全职责的分配应和信息安全方针（见第 4 章）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。这些职责应在必要时加以补充，来为特定地点和信息处理设施提供更详细的指南。资产保护和执行特定安全过程（诸如业务连续性规划）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是否已被正确地执行。

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) 与每个特殊系统相关的资产和安全过程应予以标识并清晰地定义；
b) 应分配每一资产或安全过程的实体职责，并且应形成该职责细节的文件；
c) 授权级别应清晰地予以定义，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和实施，并支持控制措施的识别。

然而，提供控制资源并实施这些控制的职责通常归于各个管理者。一种通常的做法是对每一资产指定一名拥有者，他也就对该信息资产的日常保护负责。

6.1.4 信息处理设施的授权问题

控制：

应规定并实施新信息处理设施的管理授权过程。

实施指南：

授权过程应考虑下列指南：

a) 新设施要有相应用户管理者的授权，以授权设施的用途和使用；还要获得负责维护本地系统安全环境的管理者授权，以确保所有相关安全策略和要求得到满足；
b) 若需要，硬件和软件应进行检验，以确保它们与其他系统部件兼容；
c) 使用个人或私有信息处理设施（例如膝上电脑、家用电脑或手上装置）处理业务信息，可能引起新的脆弱点，因此应识别和实施必要的控制。

6.1.5 保密协议

控制：

应识别并定期评审反映组织信息保护需要的保密或非扩散协议的需求。

实施指南：

保密或不泄露协议应使用合法可实施条款来解决保护机密信息的要求。要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，包括不确定的需要维持保密性的情形；
c) 协议终止时所需的措施；
d) 为避免未授权信息泄露的签署者的职责和行为 （即“需要知道的”）
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) 机密信息的许可使用，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需求，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 15.1.1）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，当发生影响这些需求的变更时，也要进行评

其他信息：

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

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。

6.1.6 与政府机构的联系

控制：

应保持与相关政府机构的适当联系。

实施指南：

组织应建立程序，规定何时应当与哪个机构（例如，执法部门、消防局、监管部门）联系，如果怀疑已识别的信息安全事故可能触犯了法律，如何及时报告。

由于互联网而遭受攻击的组织可能需要外部第三方（例如互联网服务提供商或电信运营商）采取措施以抵制攻击源。

其他信息：

保持这样的联系可能是支持信息安全事故管理（第 13.2 节）或业务连续性和偶然性规划过程（第 14 章）的一个要求。与法规部门的联系也是有用的，以预测和准备即将到来的组织必须遵循的法律法规方面的变化。与其他部门的联系包括公共部门、紧急服务和健康安全部门，例如消防局（与 14 章的业务连续性有关）、电信提供商（与路由和可用性有关）、用水供应者（与设备的冷却设施有关）。

6.1.7 与特殊利益团体的联系

控制：

应保持与特殊利益团体或其他专家安全论坛和行业协会的适当联系。

实施指南：

获得特殊利益团体或论坛的成员资格，应考虑将其作为一种方式来：

a) 增进关于相关安全信息的最佳实践和最新状态的知识；
b) 确保对于信息安全环境的理解是最新的和完整的；
c) 尽早接受到关于攻击和脆弱点的警告、建议和补丁；
d) 获得得到信息安全专家建议的途径；
e) 分享和交换关于新的技术、产品、威胁或脆弱点的信息；

f） 提供处理信息安全事故时的适应的联络地点（见13.2.1）。

其他信息：

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

6.1.8 信息安全的独立评审

控制：

应按计划的时间间隔或当发生重大的信息安全变化时，对组织的信息安全管理方法及其实施情况（如，信息安全控制目标、控制措施、策略、过程和程序）进行独立评审。

实施指南：

独立评审应由管理者发起。这种独立评审对确保组织管理信息安全方法的持续适宜性、充分性和有效性是必须的。评审应包括评价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区域的个人执行，例如内部审核部门、独立的管理者或专门做这种评审的第三方组织。从事这些评审的个人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或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，管理者应考虑纠正措施。

其他信息：

管理者应定期评审（15.2.1）的区域也要独立评审。评审方法包括访谈管理者、检查记录或安全策略文件的评审。ISO 19011：2002，质量和/或环境管理体系审核指南，也提供实施独立评审的有帮助的指导信息，包括评审方案的建立和实施。15.3 详细说明了与运行的信息系统独立评审相关的控制和系统审核工具的使用。

6.2 外部组织

目标：保持被外部组织访问、处理、沟通或管理的组织信息及信息处理设备的安全。

组织的信息处理设施和信息资产的安全不应由于引入外部各方的产品或服务而降低。

任何外部各方对组织信息处理设施的访问、对信息资产的处理和通讯都应予以控制。

若有与外部各方一起工作的业务需要，它可能要求访问组织的信息和信息处理设施、从外部各方获得一个产品和服务或提供给外部各方一个产品和服务，就要进行风险评估，以确定安全蕴涵和控制要求。在与外部各方签订的合同中要商定和定义控制措施。

6.2.1 识别与外部组织相关的风险

控制：

应识别来自涉及外部组织的业务过程的信息和信息处理设施的风险，并在允许访问前实施适当的控制。

实施指南：

当需要允许外部组织访问组织的信息处理设施或信息时，应实施风险评估（见第 4 章）以识别特定控制的需求。关于外部组织访问的风险的识别应考虑以下问题：

a) 外部组织需要访问的信息处理设施；
b) 外部组织对信息和信息处理设施的访问类型，例如：
   1) 物理访问，例如进入办公室，计算机机房，档案室；
   2) 逻辑访问，例如访问组织的数据库，信息系统；
   3) 组织和外部组织网络的网络连接，例如永久性连接、远程访问；
   4) 现场访问还是非现场访问；
c) 所涉及信息的价值和敏感性，及对业务运行的危险程度；
d) 保护不打算被外部组织访问到的信息所需要的控制；
e) 处理组织信息所涉及的外部组织的人员；
f) 组织或授权访问的人员如何被识别、进行授权验证，多长时间需要重新确认；
g) 外部组织在贮存、处理、传送、共享和交换信息过程中所使用的不同的方法和控制；
h) 当需要时外部组织无法获得访问，外部组织进入或接收到不正确的信息或误导信息的影响；
i) 处理信息安全事故和潜在破坏的惯例和程序，当发生信息安全事故时外部组织继续访问的期限和条件；
j) 应考虑与外部组织有关的法律法规要求和其他合同责任；
k) 其他利益相关人的利益如何被安排所影响。

除非已实施适当的控制，可行时，签订合同规定外部组织连接或访问以及合作安排的期限和条件，才可允许外部组织访问组织信息。一般而言，与外部组织合作导致的安全要求或内部控制通过与外部组织的协议反映出来（见 6.2.2 和 6.2.3）。

应确保外部组织意识到他们的责任，并且接受在访问、处理、通讯或管理组织的信息和信息处理设施所涉及的职责和责任。

其他信息：

没有充分的安全管理，信息可能由于外部组织而处于风险中。应识别和应用控制，以管理外部组织访问信息处理设施。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。

如果使用高级别外包，或涉及到几个外部组织时，组织会面临与内部处理、管理和通信相关的风险。

控制 6.2.2 和 6.2.3 涵盖了对不同外部各方的安排，例如，包括：

a) 服务提供商（例如互联网服务提供商）、网络提供商、电话服务、维护和支持服务；
b) 受管理的安全服务；
c) 顾客；
d) 设施和运行的外包，例如，IT 系统、数据收集服务、中心呼叫业务；
e) 管理和业务顾问和审核员；
f) 开发者和提供商，例如软件产品和IT 系统的开发者和提供商；
g) 清洁、供应和其他外包支持服务；
h) 临时人员、实习学生安排和其他短期临时安排。

这些协议能帮助减少与外部组织相关的风险。

6.2.2 当与顾客接触时，强调安全

控制：

应在允许顾客访问组织的信息或资产前强调所有的安全要求。

实施指南：

想要在允许顾客访问组织任何资产（依据访问的类型和范围，并不需要应用所有的条款）前解决安全问题应考虑下列条款：

a) 资产保护，包括：
   - 保护组织资产（包括信息和软件）的程序，以及对已知脆弱点的管理；
   - 确定资产是否受到损害（例如丢失数据或修改数据）的程序；
   - 完整性；
   - 对拷贝和泄露信息的限制；
b) 要提供的产品或服务的描述；
c) 顾客访问的不同原因、需求和利益；
d) 访问控制策略，包括：
   - 允许的访问方法，唯一标识的控制和使用，例如用户ID 和口令；
   - 顾客访问和权限的授权过程；
   - 没有明确授权的访问均被禁止的声明；
   - 撤消访问权力或中断系统间连接的过程；
e) 信息错误（例如个人信息的错误）、信息安全事故和安全违规的报告、修改和调查的安排；
f) 要提供确保每项服务可用的描述；
g) 服务的目标级别和服务的不可接受级别；
h) 监视和撤销与组织资产有关的任何活动的权利；
i) 组织和顾客各自的义务；
j) 关于法律事件和如何确保满足法律要求（例如，数据保护法律）的责任。如

果该协议涉及与其他国家的消费者的合作，特别要考虑到不同国家的法律体系（也见15.1）；

k) 知识产权（IPRs）和版权转让（见15.1.2）以及任何协作性工作的保护（见6.1.5）。

其他信息：

与顾客访问组织资产有关的安全需求，可能随所访问的信息处理设施和信息的不同而发生变化。这些安全需求能够通过用户协议（包括所有已识别的风险和安全需求（见 6.2.1））得以解决。

与外部各方的协议也可能涉及其他机构。允许外部各方访问的协议应包括允许指派其他有资格的机构访问，并规定他们访问和涉及的条件。

6.2.3 在第三方协议中强调安全

控制：

与第三方签订的协议中应覆盖所有相关的安全要求。这些协议可能涉及对组织的喜讯你或信息处理设施的访问、处理、沟通或管理，或增加信息处理设施的产品和服务。

实施指南：

协议应确保在组织和第三方之间不存在误解。关于第三方的保证，组织应满足自己的需要。

为满足识别的安全需求（见 6.2.1），下列条款应考虑包含在协议之内：

a) 信息安全策略；
b) 确保资产得到保护的控制措施，包括：
   - 保护组织资产（包括信息、软件和硬件）的程序；
   - 所有需要的物理保护控制和机制；
   - 确保防止恶意软件（见10.4.1）的控制；
   - 确定资产是否受到损害（例如信息、软件和硬件的丢失或修改）的程序；
   - 确保在协议截止时或在合同执行期间双方同意的某一时间段对信息和资产的归档或销毁的控制；
   - 保密性、完整性、可用性和任何其他相关的资产属性（见2.1.5）；
   - 对拷贝和泄露信息，以及保密性协议的使用的限制（见6.1.5）；
c) 对用户和管理者在方法、程序和安全方面的培训；
d) 确保用户意识到信息安全职责和问题；
e) 若合适，人员转职的规定；
f) 关于硬件和软件安装和维护的职责；
g) 一种清晰的报告结构和商定的报告格式；
h) 一种清晰规定的变更管理过程；
i) 访问控制策略，包括：
   - 第三方访问的必要性的不同原因、需求和利益；

- 允许的访问方法，唯一标识符（诸如用户ID 和口令）的控制和使用；
- 用户访问和特权的认证过程；
- 维护被授权使用正在提供的服务的个人清单的需求以及他们与这种使用相关的权利和特权是哪些；
- 没有明确授权的所有访问都要禁止的声明；
- 撤消访问权力或中断系统间连接的过程；

j) 报告、通知和调查信息安全事故和安全违规以及违背协议所声明的要求的安排；

k) 提供的每项产品和服务的描述，根据安全分类（见7.2.1）提供可获得信息的描述；

l) 服务的目标级别和服务的不可接受级别；

m) 可验证的性能要求的定义、监督和报告；

n) 监视和撤销与组织资产有关的任何活动的权利；

o) 审核协议规定的职责，授权第三方进行这些审核，以及列举审核员的法定权限的权利；

p) 建立逐级解决问题的过程；

q) 服务持续的要求，包括根据一个组织的业务优先级对可用性和可靠性的测量；

r) 协议双方的相关义务；

s) 关于法律事件和如何确保满足法律要求（例如，数据保护法律）的责任。如果该协议涉及与其他国家的组织的合作，特别要考虑到不同国家的法律体系（也见15.1）；

t) 知识产权（IPRs）和版权转让（见15.1.2）以及任何协作性工作的保护（见6.1.5）；

u) 包括具有转包商的第三方，这些转包商需要实施的安全控制；

v) 协议中重新协商/终止的条件：

- 应提供意外处理计划以处理任一方机构在协议到期之前终止合作关系的情况；
- 如果组织的安全需求发生变化，协议的重新协商；
- 资产列表、许可证、协议或与他们相关的权利的目前的文件。

其他信息：

协议会随组织和第三方机构类型的不同发生很大的变化。因此，应注意要在协议中包括所有识别的风险和安全需求（见 6.2.1）。需要时，在安全管理计划中扩展所需的控制和程序。

如果外包信息安全管理，协议应指出第三方将如何保证维持风险评估中定义的适当的安全，安全如何适于识别和处理风险的变化。

外包和其他形式的第三方服务提供之间的区别包括责任问题、策划过渡期和在此期间的潜在的运行破坏、紧急处理计划的安排和预期的详细的评审、安全事故信息的收集和管理。因此，组织计划和管理到外包安排的过渡期，提供适当的过程管理变化和协议的重新协商/终止是十分重要的。

需要考虑当第三方不能提供它的服务时的持续处理程序，以避免在安排替代服务时的任何延迟。

与第三方的协议也可能涉及到其他方。允许第三方访问的协议应包括允许指派其他有资格方的访问，并规定他们访问和涉及的条件。

一般而言，协议主要由组织制定。在一些环境下，也可能有例外，协议由第三方制定并强加于一个组织。组织需要确保它本身的安全不会没有必要的被第三方在强制协议中规定的要求所影响。

7 资产管理

7.1 资产责任

目标：实现并保持组织资产的适当保护

所有资产应是可核查的，并且有指定的责任人。

对于所有资产要标识出责任人，并且要赋予维护相应控制的职责。特定控制的实施可以由责任人适当的委派别人承担，但责任人仍有对资产提供适当保护的责任。

7.1.1 资产清单

控制：

应清楚识别所有的资产，编制并保持所有重要资产清单

实施指南：

一个组织应识别所有资产并将资产的重要性形成文件。资产清单应包括所有为从灾难中恢复而需要的信息，包括资产类型、格式、位置、备份信息、许可信息和业务价值。一个清单不应复制其他不必要的清单，但它应确保内容是相关联的。

另外，应商定每一资产的所有权（见 7.1.2）和信息分类（见 7.2），并形成文件。基于资产的重要性、业务价值和安全分类，应识别与资产重要性对应的保护级别（更多关于如何评价资产的重要性的内容可参考 ISO/IEC TR 13335-3）。

其他信息：

与信息系统相关的资产有很多类型，包括：

a) 信息资产：数据库和数据文件、合同和协议、系统文件、研究信息、用户手册、培训材料、操作或支持程序、业务连续性计划、后备运行安排、审计记录、归档的信息；
b) 软件资产：应用软件、系统软件、开发工具和实用程序；
c) 物理资产：计算机设备、通信设备、可移动介质和其他设备；
d) 服务：计算和通信服务、通用公用事业，例如，供暖，照明，能源，空调；
e) 人员，他们的资格、技能和经验；
f) 无形资产，如组织的声誉和形象。

资产清单可帮助确保有效的资产保护，其他业务目的也可能需要资产清单，例如健康与安全、保险或财务（资产管理）原因。编制一份资产清单的过程是风险管理的一个重要的先决条件（见第 4 章）。

7.1.2 资产所有者关系

控制：

与信息处理设施有关的所有信息和资产应由组织指定的部门或人员承担责任 2。

实施指南：

资产所有者应负责：

a) 确保与信息处理设施相关的信息和资产进行了适当的分类；
b) 确定并周期性评审访问限制和分类，要考虑到可应用的访问控制策略。

所有权可以分配给：

a) 业务过程；
b) 已定义的活动集
c) 应用；
d) 已定义的数据集。

其他信息：

日常任务可以委派给其他人，例如委派给一个管理人每天照看资产，但责任人仍保留职责。

在复杂的信息系统中，委派一组资产可能是比较有用的，它们一块工作来提供服务功能。在这种情况下，服务责任人负责服务的提供，包括资产本身的功能。

7.1.3 资产的可接受使用

控制：

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

实施指南：

所有员工、合同方和第三方用户应遵循信息处理设施相关信息和资产的可接受的使用规则，包括：

a) 电子邮件和互联网使用（见10.8）规则；
b) 移动设备，尤其是在组织外部使用设备（见11.7;1）的使用指南；

具体规则或指南应由相关管理者提供。使用或拥有访问组织资产权利的员工、合同方和第三方用户应意识到他们使用信息处理设施相关的信息和资产以及资源时的限制条件。他们应对信息处理资源的使用及在他们职责下进行的使用负责。

2术语“所有者”是为控制生产、开发、保持、使用和保护资产而确定的赞同管理职责的个人或实体。术语“所有者”不指对资产有实际所有权的人员。

7.2 信息分类

目标：确保信息可以得到适当程度的保护

应对信息进行分类，以在处理信息时指明保护的需求、优先级和期望程度。

信息具有可变的敏感性和重要性。某些项可能要求附加等级的保护或特别的处理。信息分类机制用来定义一组合适的保护等级和传递特别处理措施的需求。

7.2.1 分类指南

控制：

应按照信息的价值、法律要求及对组织的敏感程度和关键程度进行分类。

实施指南：

信息的分类及相关保护控制要考虑到共享或限制信息的业务需求以及与这种需求相关的业务影响。

分类指南应包括根据预先确定的访问控制策略（见 11.1.1）进行初始分类和一段时间后进行重新分类的惯例。

确定资产的类别、对其周期性评审、确保其跟上时代并处于适当的级别，这些都应是资产所有者（见 7.1.2）的职责。分类要考虑 10.7.2 提及的集合效果。

对于分类种类的数目和从其使用中获得的好处要予以考虑。过度复杂的方案可能对使用来说不方便和不经济，或许是不实际的。在解释其他组织文件上的分类标记应小心，因为其他组织可能对于相同或类似命名的标记有不同的定义。

其他信息：

保护级别可通过分析被考虑信息的机密性、完整性、可用性及其他需求进行评估。

在某一段时间之后，信息通常不再是敏感的或重要的，例如，当该信息已经公开时。上述各方面应予以考虑，因为过多的分类致使实施不必要的控制措施，从而导致附加费用。

当指派分类级别的同时考虑具有类似安全需求的文件可简化分类的任务。

一般地说，给予信息的分类是确定该信息如何予以处理和保护的简便方法。

7.2.2 信息标识与处置

控制：

应制定并实施一套与组织所采用的分类方案一致的信息标识和处置的程序。

实施指南：

信息标识程序需要涵盖物理和电子格式的信息资产。

系统的输出包含的分类为敏感的或重要的信息应在该输出中携带合适的分类标识。该标识要根据 7.2.1 中所建立的规则反映出分类。待考虑的项目包括打印报告、屏幕显示、记录介质（例如磁带、磁盘、CD）、电子报文和文件传送。

对每种分类级别，要定义包括安全处理、储存、传输、删除、销毁的处理程序。还要包括任何安全相关事件的监督和记录以及保管链的程序。

涉及信息共享的与其他组织的协议应包括识别信息分类和解释其他组织分类标识的程序。

其他信息：

分类信息的标记和安全处理是信息共享安排的一个关键要求。物理标记是常用的标记形式。然而，某些信息资产（诸如电子形式的文件等）不能做物理标记，而需要使用电子标记手段。例如，通知标记可在屏幕上显示出来。当标记不适用时，可能要应用信息分类指定的其他方式，例如通过程序或元数据。

8 人力资源安全

8.1 雇佣[3]前

目标：确保员工、合同方和第三方用户了解他们的责任并适合于他们所考虑的角色，减少盗窃、滥用或设施误用的风险。

安全职责应于雇用前在适当的岗位描述、雇用条款和条件中指出。

应充分筛选所有应聘者、合同方和第三方用户，特别是对敏感岗位的成员。

员工、合同方和信息处理设施的第三方用户要签署关于他们的安全角色和职责的协议。

8.1.1 角色和职责

控制：

应根据组织的信息安全方针，规定员工、合同方和第三方用户的安全角色和职责并形成文件。

实施指南：

安全角色和职责应包括以下要求：

a) 按照组织的信息安全方针（见5.1）实施和运作；
b) 保护资产免受未授权访问、泄露、修改、销毁或干扰；
c) 执行特定的安全过程或活动；
d) 确保职责分配给可采取措施的个人；
e) 报告安全事件或潜在事件或对组织的其他安全风险。

安全角色和职责应被定义并在雇前阶段清晰的传达给岗位候选者。

其他信息：

岗位描述能被用来将安全角色和职责形成文件。还应清晰的定义并传达没有在组织雇用过程（例如通过第三方组织雇用）中雇用的个人的安全角色和职责。

---

3 解释：这里的“雇用”意指以下不同的情形：人员雇用（暂时的或长期的）、工作角色的指定、工作角色的变化、合同的分配及所有这些活动的终止。

8.1.2 选拔

控制：

应根据相关的法律、法规和道德，对所有的求职者、合同方和第三方用户进行背景验证检查，该检查应与业务要求、接触信息的类别及已知风险相适宜

实施指南：

验证检查应考虑所有相关的隐私、个人数据保护和/或与雇用相关的法律，并应包括以下内容（允许时）：

a) 获得令人满意的品质资料（如，一项业务和一个个人）；
b) 申请人履历的核查（针对完整性和准确性）；
c) 声称的学术、专业资质的证实；
d) 独立的身份核查（身份证或护照或相似的文件）；
e) 更多细节的检查，例如信用卡检查或犯罪记录检查。

当一个职务（原先任命的或提升的）涉及到对信息处理设施进行访问的人时，特别是，如果这些设施正在处理敏感信息，例如，财务信息或高度保密的信息，那么，该组织还要考虑进一步的、更详细的检查。

程序应确定验证检查的准则和限制，例如谁有资格筛选人员、如何、何时、为什么执行验证检查。

对于合同方和第三方用户也要执行筛选过程。若合同方是通过代理提供的，那么，与代理的合同要清晰地规定代理对筛选的职责，以及如果未完成筛选或结果引起怀疑或关注时，这些代理需要遵守的通知程序。同样，与第三方（也见6.2.3）的协议应清晰的指定筛选的所有职责和通知程序。

关于所有被考虑在组织内录用的候选者的信息应按照在相关权限中存在的合适的法律来收集和处理。依据适用的法律，应将筛选活动提前通知候选者。

8.1.3 雇佣条款和条件

控制：

作为合同责任的一部分，员工、合同方和第三方用户应统一并签署他们的雇佣合同的条款和条件。这些条款和条件应规定他们和组织对于信息安全的责任。

实施指南：

雇用的条款和条件除澄清和声明以下内容外，还应涉及组织的安全策略：

a） 所有访问敏感信息的雇员、合同方和第三方用户要在能访问信息处理设施前签署

保密或不泄密协议；

b) 雇员、合同方和其他用户的法律职责和权利，例如关于版权法、数据保护法（也见15.1.1 和15.1.2）；

c) 与雇员、合同方或第三方用户操作的信息系统和服务有关的信息分类和组织资产管理的职责（也见7.2.1 和10.7.3）；

d) 雇员、合同方或第三方用户操作来自其他公司或外部团体的信息的责认；

e) 组织处理人员信息的职责，包括由于组织雇用或在组织雇用过程中产生的信息（也见15.1.4）；

f) 扩充到组织办公地点之外和正常工作时间之外的职责，例如在家中工作的情形（也见9.2.5 和11.7.1）；

g) 如果雇员、合同方或第三方用户漠视安全要求所要采取的行动（也见8.2.3）。

h) 组织应确保雇员、合同方和第三方用户同意关于信息安全的条款和条件，那些适于他们对信息系统和服务有关的组织资产的访问性质和程度。

i) 若合适，包含于雇用条款和条件中的职责应在雇用结束后持续一段规定的时间（也见8.3）。

其他信息：

一个行为规范可用于覆盖雇员、合同方或第三方用户关于机密性、数据保护、道德规范、组织设备和设施适当使用及组织期望的规范实践的职责。合同方或第三方用户可能与一个外部组织有关，此外部组织可能需要使用契约来代表已签约的个体。

8.2 雇佣中

目标：确保所有的员工、合同方和第三方用户了解信息安全威胁和相关事宜、他们的责任和义务，并在他们的日常工作中支持组织的信息安全方针，减少人为错误的风险。

应确定管理职责来确保安全应用于组织内个人的整个雇用期。

为尽可能减小安全风险，应对所有雇员、合同方和第三方用户提供安全程序和信息处理设施的正确使用方面的适当程度的意识、教育和培训。还应建立一个正式的处理安全违规的纪律处理。

8.2.1 管理职责

控制：

管理者应要求所有的员工、合同方和第三方用户按照组织已建立的方针和程序实施安全

实施指南：

管理职责应包括确保员工、合同方和第三方用户：

a) 在被授权访问敏感信息或信息系统前知道其信息安全角色和职责；

b) 从组织获得声明他们角色的安全期望的指南；

c） 被激励以实现组织的安全方针；
d） 对于他们在组织内的角色和职责的相关安全问题的意识程度达到一定级别；
e） 遵守雇用的条款和条件，包括组织的信息安全方针和工作的合适方法；
f） 持续拥有适当的技能和资质。

其他信息：

如果雇员、合同方和第三方用户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。被激励的人员更可靠并能减少信息安全事故的发生。

缺乏有效的管理会致使员工感觉被低估，并由此导致对组织的负面安全影响。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。

8.2.2 信息安全意识、教育和培训

控制：

组织的所有员工，适当时，包括合同方和第三方用户，应受到与其工作职能相关的适当的意识培训和组织方针及程序的定期更新培训。

实施指南：

意识培训应从一个正式的介绍过程开始，这个过程用来在被允许访问信息或服务前介绍组织的安全方针和期望。

正在进行的培训应包括安全要求、法律职责和业务控制，还有信息处理设施正确使用的培训，例如注销程序、软件包的使用和纪律处理（见8.2.3）的信息。

其他信息：

安全意识、教育和培训活动应是适当的并关联于员工的角色、职责和技能，并应包括关于已知威胁的信息，向谁咨询进一步的安全建议和合适的报告信息安全事故（也见13.1）的渠道。

加强意识的培训旨在使个人认识到信息安全问题及信息安全事故，并按照他们岗位角色的需要对其响应。

8.2.3 惩戒过程

控制：

应建立一个正式的员工违反安全的惩戒过程。

实施指南：

惩戒过程之前应有一个安全违规的验证过程（也见 13.2.3 的证据收集）。

正式的惩戒过程应确保正确和公平的对待被怀疑安全违规的雇员。无论违规是第一次或是已发生过，无论违规者是否经过适当的培训，正式的惩戒过程应规定一个分级的响应，要考虑诸如违规的性质、重要性及对于业务的影响等因素，相关法律、业务合同和其他因素也是需要考虑的。对于严重的明知故犯的情况，应立即免职、删除访问权限和特权，如果需要，直接护送出现场。

其他信息：

惩戒过程也可用于对雇员、合同方和第三方用户的一种威慑，防止他们违反组织的安全方针和程序，以及其他安全违规。

8.3 雇佣的终止或变更

目标：确保员工、合同方和第三方用户离开组织或雇佣变更时以一种有序的方式进行

应有合适的职责确保管理雇员、合同方和第三方用户从组织的退出，并确保他们归还所有设备及删除他们的所有访问权力。

组织内职责和工作的变化管理应符合本章内容，与职责或工作的终止管理相似，任何新的雇用应遵循8.1 节内容进行管理。

8.3.1 终止职责

控制：

应清晰规定和分配进行雇佣中止或变更的责任

实施指南：

终止职责的传达应包括正在进行的安全需求和法律职责，适当时，还包括机密性协议规定的职责（见6.1.5）和在雇员、合同方或第三方用户的雇用结束后持续一段时间仍然有效的雇用条款和条件（见8.1.3）。

规定职责和义务在雇用终止后仍然有效的内容应包含在雇员、合同方或第三方用户的合同中。

职责和工作的变化管理应与职责或工作的终止管理相似，任何新的雇用管理遵循8.1 节内容。

其他信息：

人力资源的职能通常是与管理相关程序的安全方面的监督经理一块负责总体的工作终止处理。在合同方的例子中，终止职责的处理可能由代表合同方的代理完成，其他情况下的用户可能由他们的组织来处理。

有必要通知员工、顾客、合同方或第三方用户组织人员的变化和运营上的安排。

8.3.2 归还资产

控制：

当雇佣、合同或协议终止时，员工、合同方和第三方用户应归还所使用的组织资产。

实施指南：

终止过程应被正式化以包括所有先前发放的软件、公司文件和设备的归还。其他组织资产，例如移动计算设备、信用卡、访问卡、软件、手册和存储于电子介质中的信息也需要归还。

当雇员、合同方或第三方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（也见 10.7.1）。

当一个雇员、合同方或第三方用户拥有的知识对正在进行的操作具有重要意义时，此信息应形成文件并传达给组织。

8.3.3 撤销访问权限

控制：

当雇佣、合同或协议终止时，应撤销所有员工、合同方和第三方用户对信息和信息处理设施的访问权限，或根据变化调整。

实施指南：

工作终止时，个人对与信息系统和服务有关的资产的访问权力应被重新考虑。这将决定是否必须删除访问权力。工作的变化应反映在不适用于新的工作的权力的删除上。应删除或改变的访问权力包括物理和逻辑访问、密钥、ID 卡、信息处理设备（也见 11.2.4）、签名，要从标识其作为组织的现有用户的文件中删除。如果一个已离开的雇员、合同方或第三方用户知道仍保持活动状态的帐户的密码，则应在工作、合同或协议终止或变化后改变密码。

对信息资产和信息处理设施的访问权力在工作终止或变化前是否减少或删除，依赖于对风险因素的评价，例如：

a) 终止或变化是由员工、合同方或第三方用户发起还是由管理者发起，终止的原因；
b) 员工、合同方或任何其他用户的现有职责；
c) 当前可访问资产的价值。

其他信息：

在某些情况下，访问权力的分配基于对于多人可用而不是基于离开的雇员、合同方或第三方用户，例如群 ID。在这种情况下，离开的个人应从群访问列表中删除，还应建议所有相关的其他雇员、合同方和第三方用户不应再与已离开的员工共享信息。

在管理者发起终止的情况中，不满的雇员、合同方或第三方用户可能故意破坏信息或破坏信息处理设施。在员工辞职的情况下，他们可能为将来的使用而收集必要的信息。

9 物理和环境安全

9.1 安全区域

目标：防止对组织办公场所和信息的非授权物理访问、破坏和干扰

关键或敏感的信息处理设施要放置在安全区域内，并受到一种已定义的安全边界的保护，包括适当的安全屏障和入口控制。这些设施要在物理上避免未授权访问、损坏和干扰。

所提供的保护要与所标识的风险相匹配。

9.1.1 物理安全边界

控制：

组织应使用安全边界（障碍物，如钱、控制进入大门的卡或人工接待台）来保护包含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) 安全边界应清晰地予以定义，各个边界的设置地点和强度取决于边界内资产的安全需求和风险评估的结果；
b) 包含有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）；场地的外墙应是坚固结构，所有外部门
c) 要使用控制机制来适当保护，以防止未授权进入，例如，门闩、报警器、锁等；无人值守的门和窗户应上锁，还要考虑窗户的外部保护，尤其是一层的窗户；
d) 有人管理的接待区域或其他控制对场地和建筑物的物理访问的手段要到位；进入场地或建筑物应仅限于已授权人员；
e) 如果需要，应建立物理屏障以防止未授权进入和环境污染；
f) 安全边界的所有防火门应可发出报警信号、被监视并经过检验，它和墙一起按照合适的地方、国内和国际标准建立所需的抵抗程度；他们应用故障保护方式按照局部放火规则来运行。
g) 应按照地方、国内和国际标准建立适当的入侵检测体系，并定期检测以覆盖所有的外部门窗；要一直对空闲区域发出警报；其他区域要提供掩护方法，例如计算机室或通信室；
h) 组织管理的信息处理设施应在物理上与第三方管理的设施分开。

其他信息：

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

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需求的区域之间需要控制物理访问的附加屏障和边界。

具有多个组织的建筑物应有特殊的需求，他们需要专门的物理访问安全的考虑。

9.1.2 物理进入控制

控制：

应通过适当的进入控制对安全区域进行保护，以确保只有经过授权的人员才可以访问

实施指南：

应考虑以下指南：

a) 记录访问者进入和离开的日期和时间，所有的访问者要予以监督，除非他们的访问事前已经经过批准；只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。
b) 访问处理敏感信息或储存敏感信息的区域要受到控制，并且仅限于已授权的人员；认证控制（例如，访问控制卡加个人识别号）应用于授权和确认所有访问；所有访问的审计踪迹要安全地加以维护。
c) 所有员工、合同方和第三方用户以及所有访问者要佩带某种形式的可视标识，应立即识别出无人护送的访问者和未佩带可视标识的任何人。
d) 第三方支持服务人员只有在需要时才能有限制的访问安全区域或敏感信息处理设施；这种访问应被授权并受监视；
e) 对安全区域的访问权力要定期地予以评审和更新，需要时废除（见8.3.3）。

9.1.3 办公室、房间和设施的安全

控制：

应设计并实施保护办公室、房间和设施的物理安全

实施指南：

应考虑下列指南以保护办公室、房间和设施：

a) 相关的健康和安全法规、标准要考虑在内；
b) 关键设施应坐落在可避免公众进行访问的场地；
c) 适用时，建筑物要不引人注目，并且在建筑物内侧或外侧用不明显的标记给出其用途的最少指示，以标识信息处理活动的存在；
d) 标识敏感信息处理设施位置的目录和内部电话簿不要轻易被公众得到。

9.1.4 防范外部或环境威胁

控制：

应设计并实施针对火灾、水灾、地震、爆炸、骚乱和其他形式的自然或人为灾难的物理保护措施。

实施指南：

要考虑任何邻近地点所带来的安全威胁，例如，邻近建筑物的火灾、屋顶漏水或地下室地板渗水或者街上爆炸。

要避免火灾、洪水、地震、爆炸、社会动荡和其他形式的自然或人为制造的灾难的破坏，需考虑以下因素：

a) 危险或易燃材料应在离安全区域安全距离以外的地方存放。大批供应品（例如文具）不应存放于安全区域内；
b) 恢复设备和备份介质的存放地点应与主场地有一段安全的距离，以避免影响主场地的灾难产生的破坏；
c) 应提供适当的灭火设备，并应放在合适的地点。

9.1.5 在安全区域工作

控制：

应设计并实施在安全区域工作的物理保护和指南。

实施指南：

应考虑以下方面的指南：

a) 只在有必要知道的基础上，人员才应知道安全区域的存在或其中的活动；
b) 由于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、合同方和第三方用户的控制，以及对其他发生在安全区域的第三方活动的控制。

9.1.6 公共访问和装卸区域

控制：

访问区域如装卸区域及其他未经授权人员可能进入办公场所的地点应加以控制，如果可

能的话，与信息处理设施加以隔离以防止非授权的访问。

实施指南：

应考虑以下方面的指南：

a）由建筑物外进入装卸区域的访问应局限于已标识的和已授权的人员；
b）装卸区域应设计成在无需交货人员获得对本建筑物其他部分的访问权的情况下就能卸下物资；
c）当内部的门打开时，装卸区域的外部的门应关闭；
d）在进来的物资从装卸区域运到使用地点之前，要检查是否存在潜在威胁（见9.2.1d））。
e）如果合适（也见7.1.1），进来的物资应按照资产管理程序在场地的入口处进行登记。
f）如果可能，进入和外出的货物应在物理上予以隔离。

9.2 设备安全

目标：防止资产的丢失、损坏或被盗，以及对组织业务活动的干扰

应保护设备免受物理的和环境的威胁。

对设备的保护（包括离开组织使用和财产移动）是减少未授权访问信息的风险和防止丢失或损坏所必需的。这样做还要考虑设备安置和处置。可能需要专门的控制用来防止物理威胁以及保护支持性设施，诸如电源供应和布缆基础设施。

9.2.1 设备选址与保护

控制：

应对设备进行选址安置或保护，以减少来自环境的威胁或危害，并减少未授权访问的机会

实施指南：

为保护设备，应考虑以下方面的指南：

a) 设备应进行安置，以尽量减少不必要的对工作区域的访问；
b) 应把处理敏感数据的信息处理设施放在适当的限制观测的位置，以减少在其使用期间信息被窥视的风险，还应保护储存设施以防止未授权访问；
c) 要求专门保护的部件要予以隔离，以降低所要求的总体保护等级；
d) 应采取控制以减小潜在的物理威胁的风险，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；
e) 应建立在信息处理设施附近进食、喝饮料和抽烟的指南；
f) 对于可能对信息处理设施运行状态产生负面影响的环境条件（例如温度和湿度）

要予以监视；

g） 所有建筑物都应采用避雷保护，所有进入的电源和通信线路都应装配雷电保护过滤器；

h） 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；

i） 应保护处理敏感信息的设备，以减少由于辐射而导致信息泄露的风险；

9.2.2 支持性设施

控制：

应保护设备免受电力中断或其他因为支持性设施失效所导致的中断

实施指南：

应有足够的支持性设施（例如电、供水、排污、加热/通风和空调）来支持系统。支持性设施应定期检查并适当的测试以确保他们的功能，减少由于他们的故障或失效带来的风险。应按照设备制造商的说明提供合适的供电。

对支持关键业务操作的设备，推荐使用支持有序关机或持续运行的不间断电源（UPS）。电源偶然事故计划要包括 UPS 故障时要采取的措施。如果电源故障延长，而处理要继续进行，则要考虑备份发电机。要提供足够的燃料供给，以确保在延长的时间内发电机可以进行工作。UPS 设备和发电机要定期地检查，以确保它们拥有足够容量，并按照制造商的建议予以测试。另外，如果办公地点很大，一个单独变电站无法承担，则考虑使用多来源电源。

另外，应急电源开关应位于设备房间应急出口附近，以便紧急情况时快速切断电源。万一主电源出现故障时要提供应急照明。

要有稳定足够的供水以支持空调、加湿设备和灭火系统（当使用时），还应有警报来指示水压的降低，这可能破坏设备或阻止有效的灭火。

连接到公共提供商的电信设备应至少有两条不同线路以防止在一条连接路径发生故障时语音服务失效。要有足够的语音服务以满足地方法规对于应急通信的要求。

其他信息：

实现持续供电的选项包括多路供电，以避免供电的单一故障点。

9.2.3 电缆安全

控制：

应保护承载数据或支持信息服务的电力和通讯电缆免遭中断或破坏

实施指南：

电缆安全应考虑以下指南：

a） 进入信息处理设施的电源和电信线路宜在地下，或者若可能提供足够的可替换保

护；

b） 网络布缆要免受未授权窃听或损坏，例如，利用电缆管道或使路由避开公众区域；

c） 为了防止干扰，电源电缆要与通信电缆分开；

d） 使用清晰的可识别电缆和设备记号，以最小化处理失误，例如，对错误网络电缆的意外配线；

e） 使用文件化配线列表减少失误的可能性；

f） 对于敏感的或关键的系统，更进一步的控制考虑应包括：

1） 在检查点和终接点处安装铠装电缆管道和上锁的房间或盒子；

2） 使用可替换的路由选择和/或传输介质，以提供适当的安全；

3） 使用布光缆；

4） 使用电磁防辐射装置保护电缆；

5） 技术清除、物理检查与电缆连接的未授权装置；

6） 控制对配线仪表板和电缆室的访问；

9.2.4 设备维护

控制：

应正确维护设备，以确保其持续的可用性和完整性

实施指南：

设备维护应考虑以下指南：

a） 要按照供应商推荐的服务时间间隔和规范对设备进行维护；

b） 只有已授权的维护人员才可对设备进行修理和服务；

c） 要保存所有可疑的或实际的故障和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，要考虑维护是由现场人员执行还是由外部人员执行；当需要时，敏感信息需要从设备中删除或者维护人员是足够清楚的；

e） 要遵守由保险策略所施加的所有要求。

9.2.5 场外设备安全

控制：

应对场外设备进行安全防护，考虑在组织边界之外工作的不同风险

实施指南：

无论所有权，在组织办公地点外使用任何信息处理设备都要通过管理者授权。

场外设备的保护要考虑下列指南：

a） 离开建筑物的设备和介质在公共场所不要无人值守。在旅行时便携式计算机要作为手提行李携带，若可能宜伪装起来；

b） 制造商保护设备用的说明书要始终加以遵守，例如，防止暴露于强电磁场内；

c） 家庭工作控制应根据风险评估确定，当适合时，要施加合适的控制，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（也见 ISO/IEC 18028 网络安全）；

d） 足够的安全保障掩蔽物宜到位，以保护设备离开场地。

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

其他信息：

用于家庭工作或从正常工作地点运走的信息贮存和处理设备包括所有形式的个人计算机、组织者、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参见 11.7.1 到。

9.2.6 设备的安全处置或重用

控制：

应检查包所有含存储介质的设备，以确保在销毁前所有敏感数据或授权软件已经被移除或安全重写。

实施指南：

包含敏感信息的设备在物理上应予以销毁或者采用使原始信息不可获取的技术将其安全地重写而不是使用标准删除功能。

其他信息：

包含敏感信息的被销毁的设备需要风险评估，以确定这些部件是否要进行销毁、修理或丢弃。

信息可能通过对设备的草率处置或重用而被泄漏（也见 10.7.2）。

9.2.7 资产转移

控制：

未经授权，不得将设备、信息或软件带离工作场所

实施指南：

下列指南应予以考虑：

a) 在未经授权的情况下，不应让设备、信息或软件离开办公场地；
b) 应识别有权允许资产移动，离开办公场地的雇员、合同方和第三方用户；
c) 应设置设备移动的时间限制，并在返还时执行一致性检查；

d) 若需要并合适，要对设备作出移出记录，当返回时，要作出送回记录。

其他信息：

为了检测未授权的资产移动，要进行抽查，以检测未授权的记录装置、武器等等，并防止他们进入办公场地。这样的抽查应按照相关规章制度执行。要让每个人都知道将进行抽查，只能在法律法规要求的适当认可下执行检查。

10 通信和操作管理

10.1 操作程序和职责

目标：确保信息处理设施的正确和安全操作

应建立所有信息处理设施的管理和操作职责和程序。这包括制订合适的操作程序。

当合适时，应实施责任分离，以减少疏忽或故意误用系统的风险。

10.1.1 文件化的操作程序

控制：

应编制并保持文件化的操作程序，并确保所有需要的用户可以获得

实施指南：

与信息处理和通信设施相关的系统活动要具备形成文件的程序，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、管理邮件处置和物理安全等。

操作程序应详细规定执行每个作业的说明，其内容包括：

a）信息处理和处置；
b）备份（见10.5）；
c）进度要求，包括与其他系统的相互关系、最早作业开始时间和最后作业完成期限；
d）在作业执行期间可能出现的处置差错或其它异常情况的说明，包括对使用系统实用程序的限制（见11.5.4）；
e）在有不期望的操作或技术上的困难的情况下，支持进行联络；
f）特定输出处置说明，诸如使用特殊信纸或管理保密输出，包括失败作业输出的安全处置程序（见10.7.2 和10.7.3）；
g）供万一系统失效用的系统重新起动和恢复程序；
h）审计跟踪和系统日志信息的管理（见10.10）。

要将操作程序和系统活动的文件化程序看作正式的文件，其变更由管理者授权。技术上可行时，信息系统应使用相同的程序、工具和实用程序进行一致的管理。

10.1.2 变更管理

控制：

应控制信息处理设施及系统的变更

实施指南：

操作系统和应用软件应有严格的变更管理控制。

特别是，下列条款应予以考虑。

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，包括安全影响；
d） 对建议的变更的正式批准程序；
e） 向所有有关人员传递变更细节；
f） 反馈程序，包括从不成功变更和未预料事件中退出和恢复的程序和职责。

正式的管理者职责和程序应到位，以确保对设备、软件或程序的所有变更有令人满意的控制。当该计划变更时，包含所有相关信息的审计日志要予以保留。

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故障的常见原因。对操作环境的变更，特别是当系统从开发阶段向操作阶段转移时，可能影响应用的可靠性。（也见12.5.1）。

对操作系统的变更只能在存在一个有效的业务需求时进行，例如系统风险的增加。使用操作系统或应用程序的最新版本进行系统更新并不一直是业务需求，因为这样做可能会引入比现有版本更多的脆弱点和不稳定性。尤其是在移植期间，还要需要额外培训、许可证费用、支持、维护和管理开支以及新的硬件等。

10.1.3 职责分离

控制：

应分离职责和区域，以降低未授权访问、无意识修改或滥用组织资产的机会。

实施指南：

责任分离是一种减少偶然的或故意的系统误用风险的方法。应注意，在无授权或未被监测时，要使个人不能访问、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达到这种控制方法，但是就可能和可行性来说，该原则是适用的。只要难以分离，应考虑其他控制，诸如，对活动、审计踪迹和管理监督的监视等。重要的是安全评审仍保持独立。

10.1.4 开发、测试与运营设施的分离

控制：

应分离开发、测试和运营设施，以降低未授权访问或对操作系统变更的风险

实施指南：

在运行、测试和防止操作问题的开发环境之间的分离程度要加以识别并实施适当的控制。

下列条款应加以考虑：

a) 要规定从开发状态到运行状态的软件传送规则并形成文件。
b) 开发和运行软件要在不同的系统或计算机处理器上或在不同的域或目录内运行；
c) 当不要求时，编译、编辑和其他系统工具或实用程序不应从运行系统对它们进行访问；
d) 测试系统环境应尽可能的仿效操作系统环境；
e) 用户应在操作和测试系统中使用不同的用户轮廓，菜单要显示合适的标识报文以减少出错的风险；
f) 敏感数据不应拷贝到测试系统环境中（见12.4.2）。

其他信息：

开发和测试活动可能引起严重的问题，例如，不希望的修改文件或系统环境或者系统故障。在这种情况下，有必要维护一种已知的和稳定的环境，在此环境中可执行有意义的测试和防止不合适的开发者访问。

若开发和测试职员访问运行系统及其信息，那么他们可能会引入未授权的和未测试的代码或改变运行数据。在某些系统上，这种能力可能滥用于实施欺诈，或引入未测试的、恶意的代码。未测试的或恶意的代码可以引起严重的运行问题。

开发者和测试者还成为对运行信息保密性的威胁。如果开发和测试活动共享同一计算环境，那么可能引起非故意的软件和信息的变更。因此，为了减少偶然变更或未授权访问运行软件和业务数据的风险，分离开发、测试和运行设施是合乎要求的（也见 12.4.2 的测试数保护）。

10.2 第三方服务交付管理

目标：实施并保持信息安全的适当水平，确保第三方交付的服务符合协议要求

组织应检查协议的实施，监视协议执行的一致性，并管理变更，以确保交付的服务满足与第三方商定的所有要求。

10.2.1 服务交付

控制：

确保第三方实施、运行并保持第三方服务交付协议中包含的安全控制、服务定义和交付等级。

实施指南：

第三方的服务交付应包括商定的安全布置、服务定义和服务管理的方面。外包时，组织应策划必要的过渡（信息、信息处理设施和其他需要移动的任何资产），并应确保安全在整个过渡期间得以保持。

组织应确保第三方保持足够的服务能力和设计用来确保商定的服务在大的服务故障或灾难（见 14.1）后继续得以保持的可使用的计划。

10.2.2 第三方服务的监视和评审

控制：

应对服务和第三方提交的报告定期进行监视和评审，并定期进行审核。

实施指南：

第三方服务的监视和评审应确保坚持协议的信息安全条款和条件，信息安全事故和问题得以适当的管理。这将涉及一个在组织和第三方之间的服务管理关系和过程，以：

a) 监视服务执行效率以检查对协议的符合度；
b) 评审由第三方产生的服务报告，安排协议需要的定期的进展会议；
c) 提供关于下列内容的信息：信息安全事故、协议和所有支持性指南及程序所需要的第三方和组织的评审。
d) 评审第三方审核跟踪和关于交付服务的安全事件、操作问题、故障、失误追踪和破坏的记录；
e) 解决和管理所有识别的问题。

管理与第三方关系的职责应分配给指定人员或服务管理组。另外，组织应确保第三方分配了检查一致性和协议要求强制性实施的职责。应获得足够的技术技能和资源来监视满足协议的要求（见 6.2.3），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。

组织应对第三方访问、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，例如变更管理、脆弱点识别和使用清晰定义的报告过程、格式及结构的信息安全事故报告/响应机制。

其他信息：

外包时，组织需要知道属于组织的由外包方处理的信息的最终职责。

10.2.3 管理第三方服务的变更

控制：

应管理服务提供的变更（包括包括保持和改进现有信息安全方针、程序和控制措施），考虑对业务系统的关键程度、涉及的过程和风险的再评估

实施指南：

对第三方服务变更的管理过程需要考虑：

a) 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） 组织策略和程序的更改或更新；
   4） 解决信息安全事故和改进安全的新的控制措施。
b) 第三方实施的变更：
   1） 对网络的变更和加强；
   2） 新技术的使用；
   3） 新产品或新版本的采用；
   4） 新的开发工具和环境；
   5） 服务设施物理位置的变更；
   6） 提供商的变更。

10.3 系统策划与验收

目标：最小化系统失效的风险

为确保足够容量和资源的可用性以提供所需的系统性能，需要预先的规划和准备。

应作出对于未来容量需求的推测，以减少系统过载的风险。

在新系统验收和使用之前，要建立该新系统的运行要求，并形成文件，进行测试。

10.3.1 容量管理

控制：

应监督、调整资源的使用情况，并反应将来容量的要求，以确保系统的性能

实施指南：

对于每一个新的和正在进行的活动来说，应识别容量需求。应使用系统调整和监视以确保（需要时）改进系统的可用性和效率。检测控制应到位，来指示预期期间的问题。未来容量需求的推测应考虑组织信息处理中新业务和系统的要求以及当前的和预计的趋势。

具有长的订货交货周期或高花费的所有资源需要特殊的关注；因此经理应监视关键系统资源的利用。他们应标识出使用的趋势，特别是与业务应用或管理信息系统工具相关的使用。

管理者应使用该信息来标识和避免潜在的瓶颈，该瓶颈可能对系统安全或用户服务存在威胁，同时策划适当的补救措施。

10.3.2 系统验收

控制：

应建立新的信息系统、系统升级和新版本的验收准则，并在开发过程中及接收前进行适当的系统测试

实施指南：

管理者要确保验收新系统的要求和准则明确地被定义、商定、形成文件和经过测试。新信息系统、升级和新版本只有在获得正式验收后，才能移植作为产品。在验收之前，应考虑下列指南：

a）性能和计算机容量要求；
b）差错恢复和重新启动程序以及应急计划；
c）按照已定义标准，例行操作程序的准备和测试；
d）商定的一组安全控制应到位；
e）有效的手动程序；
f）按14.1 所要求的业务连续性安排；
g）新系统的安装对现有系统无负面影响的证据，特别是在高峰处理时刻，例如月末；
h）考虑新系统对组织总体安全影响的证据；
i）新系统的操作和使用方面的培训。
j）易用性，这影响到用户使用效率，避免人员出错。

对于主要的新开发，在开发过程的各阶段要征询运行职能部门和用户的意见，以确保所建议的系统设计的运行效率。要进行合适的测试，以证实全部验收准则完全被满足。

其他信息：

验收可能包括一个正式的认证认可过程，以验证已经适当解决了安全需求。

10.4 防范恶意和移动代码

目标：保护软件和信息的完整性

要求有预防措施，以防范和检测恶意代码和未授权的移动代码的引入。

软件和信息处理设施对恶意代码（例如计算机病毒、网络蠕虫、特洛伊木马和逻辑炸弹）的引入是脆弱的。要让用户了解恶意代码的危险。若合适，管理者要引入控制，以防范、检测并删除恶意代码，并控制移动代码。

10.4.1 防范恶意代码

控制：

应实施防范恶意代码的检测、预防和恢复，以及适当的用户意识程序

实施指南：

防范恶意代码要基于恶意代码监测、修复软件、安全意识、合适的系统访问和变更管理控制。应实施防范恶意软件的检测、预防控制及相应通知用户的程序。下列指南要加以考虑：

a） 建立禁止未授权软件使用的正式策略（见15.1.2）；

b） 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（也见11.5，特别是11.5.4 和11.5.5）；

c） 对支持关键业务处理的系统中的软件和数据内容进行定期审查。应正式调查存在的任何未批准的文件或未授权的修正件；

d） 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；执行的检查应包括：

1） 使用前针对恶意代码检查电子或光介质文件，以及从网络上收到的文件；

2） 使用前针对恶意代码检查电子邮件附件和下载内容；该检查可在不同位置进行，例如，在电子邮件服务器、台式计算机或进入组织的网络时；

3） 要针对恶意代码，检查web 页面；

e） 定义关于系统、系统使用培训、恶意代码攻击报告和从恶意代码攻击中恢复的恶意代码预防的管理程序和职责（见13.1 和13.2）；

f） 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的备份以及恢复安排（见14 章）；

g） 实施程序定期收集信息，例如订阅邮件列表和/或检查提供新恶意代码的web 站点；

h） 实施检验与恶意代码相关的所有信息的程序，并确保报警公告是准确情报；管理应确保使用合格的来源（例如，声誉好的期刊、可靠的Internet 网站或防恶意代码软件供应商），以区分欺骗和实际恶意代码；要让所有用户了解欺骗问题，以及在收到它们时要做什么。

其他信息：

在信息处理环境中使用来自不同供应商的防范恶意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。

可安装防恶意代码软件，提供定义文件和扫描引擎的自动更新，以确保防护措施是最新的。另外，也可安装本软件使每一台台式机都执行自动检查。

应注意防止在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控制。

10.4.2 防范移动代码

控制：

当使用移动代码获得授权时，配置管理应确保授权的移动代码按照明确定义的安全方针运行，并防止未经授权移动代码的执行。

实施指南：

应考虑下列措施以防止移动代码执行未授权的活动：

a) 在逻辑上隔离的环境中执行移动代码；
b) 阻塞移动代码的所有使用；
c) 阻塞移动代码的接收；
d) 使技术测量措施在一个特定系统中可用，以确保管理移动代码；
e) 控制移动代码访问的可用资源；
f) 使用密码控制，以唯一的认证移动代码。

其他信息：

移动代码是一种软件代码，它能从一台计算机传递到另一台计算机，随后自动执行并在很少或没有用户干预的情况下完成特定功能。移动代码与大量的中间件服务有关。

除确保移动代码不包含恶意代码外，必须控制移动代码，以避免系统、网络或应用资源的未授权使用或破坏，以及其他违反信息安全的活动。

10.5 备份

目标：保持信息和信息处理设施的完整性和可用性

应建立例行程序来执行商定的针对数据拷贝备份以及及时恢复演练的策略和战略（见14.1）

10.5.1 信息备份

控制：

应根据既定的备份策略对信息和软件进行备份并定期测试

实施指南：

应提供足够的备份设施，以确保所有必要的信息和软件能在灾难或介质故障后进行恢复。

信息备份的下列条款要加以考虑：

a） 应定义备份信息的必要级别；

b） 应有备份拷贝的准确完整的记录和文件化的恢复程序；

c） 备份的程度（例如全部备份或部分备份）和频率应反映组织的业务需求，涉及信息的安全要求和信息对组织持续运作的关键度；

d） 备份要存储在一个远程地点，有足够距离，以避免主要场地灾难时受到损坏；

e） 要给予备份信息一个与主要场地所应用标准相一致的合适的物理和环境保护等级（见第9 章）。要扩充应用于主要场地介质的控制，以涵盖备份场地；

f） 若可行，要定期测试备份介质，以确保当需要应急使用时可以依靠这些备份介质；

g） 恢复程序应定期检查和测试，以确保他们有效，并能在恢复时操作程序所分配的时间内完成；

h） 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。

各个系统的备份安排应定期测试以确保他们满足业务连续性计划（见 14 章）的要求。对于重要的系统，备份不止应覆盖所有的系统信息、应用，还应包括在灾难事件时恢复整个系统所需的必须信息。

要确定最重要业务信息的保存周期以及对要永久保存的档案拷贝的任何要求（见15.1.3）

其他信息：

为使备份和恢复过程更容易，备份可安排为自动进行。这种自动化解决方案应在实施前进行充分的测试，还应作到定期测试。

10.6 网络安全管理

目标：确保网络中的信息和支持性基础设施得到保护

可能跨越组织边界的网络安全管理，需要仔细考虑数据流、法律蕴涵、监视和保护。

还可以要求附加的控制，以保护在公共网络上传递的敏感数据。

10.6.1 网络控制

控制：

应对网络进行充分的管理和控制，以防范威胁、保持使用网络的系统和应用程序的安全，包括信息传输

实施指南：

网络管理者应实施控制，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，下列条款要予以考虑：

a） 适当时，网络的操作职责要与计算机操作分开（见10.1.3）；

b） 应建立远程设备（包括用户区域内的设备）管理的职责和程序；

c） 如有必要，要建立专门的控制，以保护在公用网络上传递数据的保密性和完整性，并且保护已连接的系统（见11.4 和12.3）；为维护所连接的网络服务和计算机的可用性，还可以要求专门的控制；

d） 为记录安全相关的活动，应使用适当的日志记录和监视措施；

e） 为优化对组织的服务和确保在信息处理基础设施上始终如一地应用若干控制，应紧密地协调管理活动。

其他信息：

关于网络安全的其他信息见 ISO/IEC 18028 网络安全。

10.6.2 网络服务安全

控制：

应识别所有网络服务的安全特性、服务等级和管理要求，并包含在网络服务协议中，无论这种服务是由内部提供的还是外包的。

实施指南：

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

应识别特殊服务的安全布置，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。

其他信息：

网络服务包括连接的提供、私有网络服务、附加价值网络和受管理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管理带宽也包括复杂的附加价值的提供。

网络服务的安全特性可以是：

a) 为网络服务应用的安全技术，例如认证、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) （若需要）网络服务使用程序，以限制对网络服务或应用的访问。

10.7 介质处理

目标：防止对资产的未授权泄漏、修改、移动或损坏，及对业务活动的干扰

应控制介质，并对其实施物理保护。
为使文件、计算机介质（如磁带、磁盘）、输入/输出数据和系统文件免遭未授权泄露、修改、
应建立适当的删除和销毁的操作程序。

10.7.1 移动介质的管理

控制：

应建立可移动介质的管理程序

实施指南：

下列对于可移动介质的管理指南要加以考虑：

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，应使其不可重用。
b） 如果需要并实用，对于从组织取走的所有介质应要求授权，所有这种移动的记录要加以保持，以保持审计踪迹；
c） 要将所有介质存储在符合制造商说明的安全、保密的环境中；
d） 如果存储在介质中的信息使用时间要比介质生命期长，则也要将信息存储在别的地方，以避免由于介质老化而导致信息丢失；
e） 应考虑可移动介质的登记，以减少数据丢失的机会；
f） 只应在有业务要求时，才使用可移动介质。

所有程序和授权级别要清晰地形成文件。

其他信息：

可移动介质包括磁带、磁盘、闪盘、可移动硬件驱动器、CD、DVD 和打印的介质。

10.7.2 介质的销毁

控制：

当介质不再需要时，应按照正式的程序进行安全可靠的销毁

实施指南：

应建立介质安全销毁的正式程序，以最小化敏感信息泄露给未授权人员的风险。包含敏感信息介质的安全销毁程序应与信息的敏感性相适宜。应考虑以下事项：

a) 包含有敏感信息的介质要可靠和安全地存储和销毁，例如，利用焚化或切碎的方法，或者将数据删除供组织内其它应用的使用；
b) 程序应到位，以识别可能需要安全销毁的项目；
c) 安排把所有介质部件收集起来并进行可靠销毁，比试图分离出敏感部件可能更容易；
d) 许多组织对记录纸、设备和介质提供收集和销毁服务；应注意选择具有足够控制和经验的合适的合同商；
e) 若有可能，销毁敏感部件要做记录，以便保持审计踪迹。

当销毁聚集介质时，对聚集的影响要予以考虑，它可能使大量不敏感信息变成敏感信息。

其他信息：

敏感信息可能由于大意的介质处置而泄露（也见 9.2.6 有关设备处置的信息）。

10.7.3 信息处置程序

控制：

应建立信息处置和存储程序，以防范该信息的未授权泄漏或误用

实施指南：

应制定处理程序；处理、存储、传达与其分类（见 7.2）一致的信息。应考虑以下事项：

a） 按照所指示的分类级别，处理和标记所有介质；
b） 标识未授权人员的访问限制；
c） 维护已授权的数据接收者的正式记录；
d） 确保输入数据完整，正确完成处理和应用输出确认；
e） 按照与其敏感性一致的级别，保护等待输出的假脱机数据；
f） 介质存储在与制造商规范一致的环境中；
g） 使分发的数据最少；
h） 清晰地标记数据的所有拷贝，以引起已授权接收者关注；
i） 以商定的时间间隔评审分发列表和已授权接收者列表。

其他信息：

这些程序应用于文件、计算系统、网络、移动计算、移动通信、邮件、话音邮件、通用话音通信、多媒体、邮政服务/设施、传真机的使用和任何其他敏感项目（例如，空白支票、发票）中的信息。

10.7.4 系统文档安全

控制：

应保护系统文档免受未授权的访问

实施指南：

对于系统文件安全，要考虑下列条款：

a） 要安全地存储系统文件；
b） 将系统文件的访问列表保持在最小范围，并且由应用责任人授权；
c） 应妥善地保护保存在公用网络上的或经由公用网络提供的系统文件。

其他信息：

系统文件可以包含一系列敏感信息，例如，应用过程的描述、程序、数据结构、授权过程。

10.8 信息交换

目标：应保持组织内部或组织与外部组织之间交换信息和软件的安全

组织间信息和软件的交换应基于一个正式的交换策略，按照交换协议执行，还应服从任何相关法律（见第15 章）。

要建立程序和标准，以保护信息和在传输中包含信息的物理介质。

10.8.1 信息交换策略和程序

控制：

应建立正式的交换策略、程序和控制，以保护通过所有类型的通讯设施交换信息的安全。

实施指南：

使用电子通信设施进行信息交换的程序和控制应考虑下列条款：

a) 设计用来防止交换信息遭受截取、复制、修改、错误寻址和破坏的程序；
b) 检测和防止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) 简述电子通信设施可接受的使用的策略或指南（见7.1.3）；
e) 无线通信使用的程序，要考虑所涉及的特定风险；
f) 员工、合同方和所有第三方用户不损害组织的职责，例如诽谤、扮演、连锁信寄送、未授权购买等；
g) 密码技术的使用，例如保护信息的机密性、完整性和可靠性（见12.3）；
h) 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；
i) 不要将敏感或重要信息留在打印设施上，例如复印机、打印机和传真机，因为这些设施可能被未授权人员访问；
j) 与通信设施传输相关的控制和限制，例如到外部邮件地址的电子邮件的自动传输；
k) 提醒工作人员，应采取相应预防措施，例如，为不泄露敏感信息，避免打电话时被下列方式无意听到或窃听：
   1） 当使用移动电话时，要特别注意在他们附近的人们；
   2） 搭线窃听和通过物理访问手持电话或电话线路的其他窃听方式，或当使用模拟移动电话时使用扫描接收器进行窃听；
   3） 受话端的人们；
l) 不要将报文留在应答机上，因为可能被未授个人重放，或者由于误拨号被存储在公用系统上或不正确地被存储；
m) 提醒人员关于传真机的使用问题，即：
   1） 未授权访问内置报文存储器，以检索报文；

2） 有意的或无意的对传真机编程，将报文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档和报文发送给错误的电话号码；

n) 提醒人员不要注册统计数据，例如任何软件中的电子邮件地址或其他人员信息，以避免未授权人员收集；

o) 提醒人员现代的传真机和影印机都有页面缓冲并在页面或传输故障时存储页面，一旦故障消除，这些将被打印。

另外，应提醒工作人员，不要在公共场所或开放办公室和薄围墙的会场进行保密会谈。信息交换设施应符合所有相关的法律要求（见第 15 章）。

其他信息：

信息交换可能通过使用很多不同类型的通信设施发生，例如电子邮件、声音、传真和视频。

软件交换可能通过很多不同类型的媒体发生，包括从互联网下载和从出售现货的供应商处获得。

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、法律和安全蕴涵。

由于对使用这些设施缺乏意识、策略或程序可能泄露信息，例如，在公开场所的移动电话被偷听、电子邮件消息的指示错误、应答机被偷听，未授权访问拨号语音邮件系统或使用传真设备偶然地将传真发送到错误的传真设备上。

如果通信设施失灵、过载或中断，则可能中断业务运行和损坏信息（见 10.3 或第 14 章）。如果上述通信设施被未授权用户所访问，也可能损害信息（见第 11 章）。

10.8.2 交换协议

控制：

应建立组织和外部组织信息和软件交换的协议

实施指南：

交换协议应考虑以下安全条件：

a) 控制和通知传输、发送和接收的管理职责；
b) 通知发送者，传输、发送和接收方面的程序；
c) 确保可追溯性和不可抵赖性的程序；
d) 打包和传输的最低技术标准；
e) 有条件转让契约；
f) 送信人辨识标准；
g) 在信息安全事故中的职责和义务，例如数据丢失；
h) 商定的标记敏感或重要信息的系统的使用，保证标记的含义能直接理解和信息受到合适保护；
i) 信息和软件的所有权以及关于数据保护、软件版权符合性及类似的所考虑事项的职责

（见15.1.2 和15.1.4）；

j) 记录和阅读信息和软件的技术标准；

k) 为保护敏感项［例如密钥（见12.3）］，可以要求任何专门的控制。

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（也见 10.8.3），这些还应在交换协议中进行引用。

任何协议的安全内容应反映涉及的业务信息的敏感度。

其他信息：

协议可以是电子的或手工的，可能采取正式合同或雇用条件的形式。对敏感信息而言，信息交换使用的专门机制应适用于所有组织和协议类型。

10.8.3 物理介质传输安全

控制：

在组织的物理边界之外进行传输的过程中，应保护包含信息的介质免受未授权的访问、误用或破坏

实施指南：

应考虑下列指南以保护不同地点间传输的信息介质：

a) 应使用可靠的运输或信使；

b) 授权的信使列表应经管理者批准；

c) 应开发检查信使识别的程序；

d) 包装要足以保护内容免遭在运输期间可能出现的任何物理损坏，并且符合制造商的规范（例如软件），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) 若需要，应采取专门的控制，以保护敏感信息免遭未授权泄露或修改；例子包括：

1） 使用可锁上的容器；

2） 手工交付；

3） 防篡改的包装（它揭示任何企图打开的迹象）；

4） 在异常情况下，把托运货物分解成多次交付，并且通过不同的路线发送；

其他信息：

信息在物理传输期间（例如通过邮政服务或信使传送）对于未授权访问、不当使用或老化是脆弱的。

10.8.4 电子消息

控制：

应适当保护电子消息的信息

实施指南：

电子消息的安全考虑应包括以下方面：

a) 防止消息遭受未授权访问、修改或拒绝服务攻击；
b) 确保正确的寻址和消息传输；
c) 服务的通用可靠性和可用性；
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（例如即时消息或文件共享）前获得批准；
f) 控制从公开可访问网络进行访问的认证的更强级别。

其他信息：

电子消息（例如电子邮件、电子数据交换（EDI）、即时消息）在业务通信中充当一个日益重要的角色。电子消息与基于通信的纸面文件相比有不同的风险。

10.8.5 业务信息系统

控制：

应开发并实施策略和程序，以保护与业务信息系统互联的信息

实施指南：

对于互连接（例如设施）的安全和业务蕴涵的考虑应包括：

a) 信息在组织的不同部分间共享时，在管理和记帐系统中已知的脆弱点；
b) 业务通信系统中的信息的脆弱点，例如，记录电话呼叫或会议呼叫，呼叫的保密性。传真的存储，打开邮件，分发邮件；
c) 管理信息共享的策略和适当的控制；
d) 如果系统不提供适当级别的保护（见7.2），则排除敏感业务信息的类别和分类的文件；
e) 限制访问与选定个人相关的日志信息，例如，正从事敏感项目的人员；
f) 允许使用系统的工作人员、合同商或业务伙伴的类别以及可以访问该系统的位置；
g) 对特定种类用户限定所选定的设施；
h) 标识出用户的身份，例如，组织的雇员，或者为了其他用户利益的目录中的合同商；
i) 系统上存放的信息的保留和备份；
j) 基本维持运行的要求和安排（见第14 章）。

其他信息：

办公信息系统通过结合使用文档、计算机、移动计算、移动通信、邮件、话音邮件、通用话音通信、多媒体、邮政服务/设施和传真机，是快速传播和共享业务信息的机会。

10.9 电子商务服务

目标：确保电子商务的安全及他们的安全使用

应考虑与使用电子商务服务相关的安全蕴涵，包括在线交易和控制要求。还应考虑通过公开可用系统以电子方式公布的信息的完整性和可用性。

10.9.1 电子商务

控制：

应保护电子商务中通过公共网络传输的信息，以防止欺诈、合同争议、未授权的泄漏和修改

实施指南：

电子商务的安全应考虑：

a） 在彼此声称的身份中，每一方要求的置信度级别，例如通过认证；
b） 与授权谁设定价钱、发布或签署关键贸易文件相关的授权；
c） 确保贸易伙伴完全接到他们的职责的通知；
d） 决定和满足保密性、完整性和关键文件的接收和发送的证明以及合同抗抵赖方面的要求，例如关于提出和订约过程；
e） 在广告价格表中的完整性所需的可信级别；
f） 任何敏感数据或信息的保密性；
g） 任何订单交易、支付信息、交付地址细节和接收证实的保密性和完整性；
h） 适于检查用户提供的支付信息的验证程度；
i） 为防止欺诈，选择最适合的支付解决形式；
j） 为维护订单信息的保密性和完整性要求的保护级别；
k） 避免交易信息的丢失或复制；
l） 与所有欺诈交易相关的责任；
m） 保险需求。

上述许多考虑可以通过应用密码技术来实现（见 12.3），并考虑到符合法律要求（见 15.1，特别见 15.1.6 密码法规）。

应通过文件化的协议来支持贸易伙伴之间的电子商务安排，该协议使双方致力于商定的贸易条款，包括授权细节（见上述 b））。与信息服务部门和增值网络提供者的其他协议可能也是必要的。

公共贸易系统应向顾客公布其业务项目。

对用于电子商务的主机受攻击的恢复能力以及其电子商务服务实现所要求的任何网络互连的安全所涉及的问题应予以考虑（见 11.4.6）。

其他信息：

电子商务易受到许多网络威胁，这些威胁可能导致欺诈活动、合同争端和信息的泄露和修改。

电子商务能充分利用安全认证方法（例如使用公开密钥系统和数字签名（也见 12.3））以减少风险。另外，当需要这些服务时，可使用可信第三方。

10.9.2 在线交易

控制：

应保护在线交易中的信息，以防止不完整的传输、路由错误、未授权的消息修改、未经授权的泄漏、未经授权的消息复制或回复

实施指南：

在线交易的安全应考虑：

a) 交易中涉及的每一方的电子签名的使用；
b) 交易的所有方面，例如确保：
   1） 各方的用户信任是有效的和验证的；
   2） 交易是保密的；
   3） 保留与涉及的各方相关的隐私；
c) 加密涉及各方的通信路径；
d) 在涉及各方之间通信的协议是安全的；
e) 确保交易细节存储于任何公开可用环境之外（例如，存储于组织内部互联网的存储平台），不留在或暴露于互联网可直接访问的存储介质上。
f) 当使用一个可信权威时，安全可集成嵌入到整个端到端认证/签名管理过程中。

其他信息：

采用控制的程度要对应于在线交易的每个形式相关的风险级别。

交易需要符合交易产生、处理、完成或存储的管理区域的法律、规则和法规。

存在很多形式的交易可用在线的方式执行，例如契约的或财政的等等

10.9.3 公共可用信息

控制：

应保护公共可用系统中信息的完整性，以防止未经授权的修改

实施指南：

应通过适当的机制（数据签名（见 12.3））保护需要高完整性级别的软件、数据和其它

信息，这些可在公共可用系统中得到。应测试公共可用系统，在信息可用前防止弱点和故障。

在信息公开可用前，应有正式的授权过程。另外，所有从外部对系统提供的输入应经过验证和批准。

应小心地控制电子发布系统，特别是允许反馈和直接录入信息的那些电子发布系统，以便：

a） 按照任何数据保护法律获得信息（见15.1.4）；

b） 对输入到发布系统并由发布系统处理的信息将以及时的方式完整而准确地予以处理；

c） 在收集信息过程期间和存储信息时，保护敏感信息；

d） 对发布系统的访问不允许无意识地访问与之连接的网络。

其他信息：

在公共可用系统上的信息（例如，经由 Internet 可访问的 Web 服务器上的信息）需要符合该系统所在的或贸易发生的或责任人居住的管辖区域内的法律、规则和规章。发布信息的未授权修改可能损害发布组织的声望。

10.10 监视

目标：检测未经授权的信息处理活动

应监视系统，记录信息安全事件。应使用操作员日志和故障日志以确保识别出信息系统的问题。
一个组织的监视和日志记录活动应遵守所有相关法律的要求。
应使用系统监视检查所采用控制措施的有效性，并验证对访问策略模型的一致性。

10.10.1 审计日志

控制：

应产生记录用户活动、以外和信息安全事件的日志，并按照约定的期限进行保留，以支持将来的调查和访问控制监视

实施指南：

审计日志应在需要时包括：

a） 用户ID；

b） 日期、时间和关键事件的细节，例如登录和退出；

c） 若有可能，终端身份或位置；

d） 成功的和被拒绝的对系统尝试访问的记录；

e） 成功的和被拒绝的对数据以及其他资源尝试访问的记录；

f） 系统配置的变化；

g） 特权的使用；
h） 系统工具和应用的使用；
i） 访问的文件和访问类型；
j） 网络地址和协议；
k） 访问控制系统引发的警报；
l） 防护系统的激活和停用，例如防病毒系统和入侵检测系统。

其他信息：

审计日志包含闯入和秘密人员的数据，应采取适当的隐私保护措施（也见15.1.4）。可能时，系统管理员不应有删除或停用他们自己活动日志的权利。

10.10.2 监视系统的使用

控制：

应建立监视信息处理系统使用的程序，并定期评审监视活动的结果

实施指南：

各个设施的监视级别应由风险评估决定。一个组织应符合所有相关的适用于监视活动的法律要求。要考虑的区域包括：

a) 授权访问，包括细节，例如：
   1） 用户ID；
   2） 关键事件的日期和时间；
   3） 事件类型；
   4） 访问的文件；
   5） 使用的程序/工具；
b) 所有私人操作，例如：
   1） 私人帐户的使用，例如监督员、根用户、管理员；
   2） 系统的启动和终止；
   3） I/O 设备的装配/拆卸；
c) 未授权访问的尝试，例如：
   1） 失败的或被拒绝的用户活动；
   2） 失败的或被拒绝的涉及数据和其他资源的活动；
   3） 访问策略违背和网络网关和防火墙的通告；
   4） 私有入侵检测系统的警报；
d) 系统警报或故障，例如：
   1） 控制台警报或消息；
   2） 系统日志异常；
   3） 网络管理警报；
   4） 访问控制系统引发的警报；

e) 系统安全设置和控制的变化或变化的尝试。

监视活动的结果多长时间进行评审应依赖于涉及的风险。应考虑的风险因素包括：

a) 应用过程的重要程度；
b) 所涉及信息的价值、敏感度和重要度；
c) 系统渗透和不当使用的经验，脆弱点被利用的频率；
d) 系统互连接的程度（尤其是公共网络）；
e) 设备被停用的日志记录。

其他信息：

必须使用监视程序以确保用户只执行被明确授权的活动。

日志评审包括系统所面临威胁的理解和出现的方式。更多关于事件的例子见信息安全事故的 13.1.1。

10.10.3 保护日志信息

控制：

应保护日志设施和日志信息免受破坏和未授权的访问

实施指南：

应实施控制防止日志设施被未授权变更和出现操作问题，例如：

a) 被记录消息类型的更改；
b) 日志文件被编辑或删除；
c) 使日志文件介质被耗尽，或者不能记录事件或者自身覆盖重写。

一些审核日志可能需要作为记录保持策略或由于收集和保持证据的要求（也见 13.2.3）的一部分进行存档。

其他信息：

系统日志通常包含大量的信息，其中许多与安全监督无关。为帮助标识出对安全监督目的有重要意义的事件，应考虑将相应的报文类型自动地拷贝到第二份日志，和/或使用适合的系统实用程序或审核工具执行文件询问。

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断定。

10.10.4 管理员和操作者日志

控制：

应记录系统管理员和系统操作者的活动

实施指南：

日志要包括：

a） 事件（成功的或失败的）发生的时间；
b） 关于事件（例如处理的文件）或故障（发生的差错和采取的纠正措施）的信息；
c） 涉及的帐号和管理员或操作员；
d） 涉及的过程。

系统操作员和操作员日志须定期评审。

其他信息：

对在系统和网络管理员控制之外进行管理的入侵检测系统可以用来监视系统和网络管理活动的一致性。

10.10.5 错误日志

控制：

应记录并分析错误日志，并采取适当的措施

实施指南：

由与信息处理或通信系统的问题有关的用户或系统程序所报告的故障要加以记录。对于处理所报告的故障要有明确的规则，包括：

a） 评审故障日志，以确保已满意地解决故障；
b） 评审纠正措施，以确保控制未被损害，以及所采取的动作予以充分授权。

如果错误日志可用，应确保其处于活动状态。

其他信息：

错误和故障日志记录能影响系统的性能。这些日志记录应由胜任的职员激活，对各个系统所需的日志记录的级别应由风险评估决定，要考虑性能的降低。

10.10.6 时钟同步

控制：

组织内或同一安全域内的所有相关信息处理设施的时钟应按照约定的正确时间源保持同步

实施指南：

若计算机或通信设备有能力运行实时时钟，则时钟应置为商定的标准，例如，世界协调时间（UCT）或本地标准时间。当已知某些时钟随时间漂移，应有一个校验和校准任何重大偏差的程序。

日期/时间格式的正确解释对确保时间戳反映实时的日期/时间是重要的。还应考虑局部

特异性（例如夏令时间）。

其他信息：

正确设置计算机时钟对确保审核记录的准确性是重要的，审核日志可用于调查或作为法律、法律案例的证据。不准确的审核日志可能妨碍调查，并损害这种证据的可信性。链接到国家原子钟无线电广播时间的时钟可用于保持所有服务器与主时钟同步。

11 访问控制

11.1 访问控制的业务要求

目标：控制信息访问

对信息、信息处理设施和业务过程的访问应在业务和安全要求的基础上予以控制。

访问控制规则应考虑到信息传播和授权的策略。

11.1.1 访问控制策略

控制：

应建立文件化的访问控制策略，并根据对访问的业务和安全要求进行评审

实施指南：

在访问策略中应清晰地叙述每个用户或一组用户的访问控制规则和权利。访问控制既是逻辑的也是物理的（也见第 9 章），他们应一起考虑。须将通过访问控制要满足的业务要求的清晰说明提供给用户和服务提供者。

策略应考虑到下列内容：

a） 各个业务应用的安全要求；
b） 与业务应用相关的所有信息的标识和信息面临的风险；
c） 信息传播和授权的策略，例如，了解原则和安全等级以及信息分类的需求（见7.2）；
d） 不同系统和网络的访问控制策略和信息分类策略之间的一致性；
e） 关于保护访问数据或服务的相关法律和合同义务（见15.1）；
f） 关于组织内通常工作种类的标准用户访问轮廓；
g） 在认可各种现有连接类型的分布式和网络化环境中访问权力的管理；
h） 访问控制角色的分离，例如访问请求、访问授权、访问管理；
i） 访问要求的正式授权要求（见11.2.1）；
j） 访问控制的周期性评审要求（见11.2.4）；
k） 访问权力的取消（见8.3.3）。

其他信息：

在规定访问控制规则时，应注意考虑下列内容：

a） 区分必须强制的规则和任选的或有条件的规则；
b） 在前提为“未经允许，必须一律禁止”的基础上建立规则，而不是弱的“未经明确禁止，一律允许”的规则；

c） 信息处理设施自动启动的信息标记（见7.2）和用户任意启动的那些信息标记的变更；
d） 信息系统自动启动的用户许可变更和管理员启动的那些用户许可变更；
e） 在颁发之前，要求专门批准的规则以及无须批准的规则。

访问控制规则应由正式的程序支持，并清晰的定义职责（见，例如，6.1.3、11.3、10.4.1、11.6）

11.2 用户访问管理

目标：确保授权用户的访问，并预防信息系统的非授权访问。

应有正式的程序来控制对信息系统和服务的访问权力的分配。

这些程序应涵盖用户访问生存周期内的各个阶段，从新用户注册到不再要求访问信息系统和服务的用户的最终注销。在合适的情况下，应特别注意对有特权的访问权力的分配的控制需要，这种权力允许用户超越系统控制。

11.2.1 用户注册

控制：

应建立正式的用户注册和解除注册程序，以允许和撤销对于所有信息系统和服务的访问

实施指南：

用户注册和注销的访问控制程序应包括：

a） 使用唯一用户ID，使得用户可以与其动作链接起来，并对其动作负责；若他们对于业务或操作的原因是必须的，才允许使用组ID，并应经批准和形成文件；
b） 检验用户使用信息系统和服务是否具有该系统拥有者的授权；经管理者单独批准的访问权力也是合适的；
c） 检验所授予的访问级别是否适合于业务目的（见11.1），以及是否与组织的安全策略一致，例如，它没有放弃责任分割原则（见10.1.3）；
d） 给予用户访问权力的书面声明；
e） 要求用户签署表示理解访问条件的书面声明；
f） 确保直到已经完成授权程序，服务提供者才提供访问；
g） 维护注册使用该服务的所有个人的正式记录；
h） 立即取消已经变更的工作或离开该组织的用户访问权力；
i） 周期性检验和取消多余的用户ID 和账户（见11.2.4）；
j） 确保对其他用户不发布多余的用户ID。

其他信息：

应考虑基于业务要求建立用户访问角色，它将大量的访问权力归结到典型的用户访问轮廓中。访问请求和评审（见 11.2.4）在这种角色级别上比特定权力级别容易管理。

在人员合同和服务合同中要考虑包括如果员工或服务代理试图未授权访问时规定处罚的条款（也见 6.1.5、8.1.3 和 8.2.3）。

11.2.2 特权管理

控制：

应限制和控制特权的使用和分配

实施指南：

要求免遭未授权访问的多用户系统应通过正式的授权过程使特权分配受到控制。下列步骤要予以考虑：

a） 应标识出与每个系统产品（例如，操作系统、数据库管理系统和每个应用）相关的访问特权，以及需要分配给特权的用户；
b） 特权应在需要使用的基础上和逐个事件的基础上按照访问控制策略（1.1.1）分配给用户，例如仅当需要时，才为其职能角色分配最低要求；
c） 应维护所分配的各个特权的授权过程及其记录。直到授权过程完成，才授予特权；
d） 应促进开发和使用系统例行程序，以避免必需把特权授予用户；
e） 应促进开发和使用程序，使其可避免必需有特权才可运行；
f） 特权应分配给其身份与正常业务使用的用户身份不同的用户。

其他信息：

系统特权的不恰当使用（使用户越过系统或应用控制的信息系统的任何特性或设施）常常是一种导致系统故障或安全违规的主要因素。

11.2.3 用户口令管理

控制：

应通过正式的管理流程控制口令的分配

实施指南：

此过程应包括下列 ：

a） 要求用户签署一份声明，以保持个人口令的保密性和组口令仅在该组成员范围内使用；签署的条款可包括在雇用条款和条件内（见8.1.3）；
b） 若要求用户维护自己的口令，应确保他们一开始就具有可强制使其立即变更的临时保密口令（见11.3.1）；
c） 在提供一个新的、代替的或临时的口令之前，要建立验证用户身份的程序；

d） 要求以安全的方式将临时口令给予用户；要避免使用在第三方或不受保护的（明文）电子邮件报文中；

e） 临时口令对个人而言应是唯一的，应是不可猜测的；

f） 用户应确认收到口令；

g） 口令决不能以不受保护的形式存储在计算机系统内；

h） 应在系统或软件安装后改变提供商的默认口令。

其他信息：

口令是一种按照用户授权给予其访问信息系统或服务的权力前验证用户身份的常用手段。关于用户标识和认证参见其他技术，诸如生物统计学，例如，指纹验证，签名验证和硬件标记的使用，例如，芯片卡，这些技术均可用，如果合适，要考虑这些技术。

11.2.4 用户访问权限的评审

控制：

管理者应按照策划的时间间隔通过正式的流程对用户的访问权限进行评审

实施指南：

访问权限的评审应考虑下列指南：

a) 定期（推荐周期为6 个月）和在任何变更之后（例如的提升、降级或工作的终止（见11.2.1））， 用户的访问权限要受到评审；

b) 当在同一个组织中从一个岗位换到另一个岗位时，应评审和重新分配用户的访问权限；

c) 以更频繁的时间间隔评审专门的有特权的访问权限的授权（见11.2.2）；推荐周期为3个月；

d) 应定期检查特权分配，以确保不能获得未授权的特权；

e) 特权帐户的变更应在周期性评审时记入日志。

其他信息：

必须定期评审用户的访问权限以保持对数据和信息服务的有效控制。

11.3 用户责任

目标：避免未授权用户的访问，信息和信息处理设施的破坏或被盗

已授权用户的合作是有效安全的基础。

要让用户了解他对维护有效的访问控制的职责，特别是关于口令的使用和用户设备的安全的职责。

应实施桌面清空和屏幕清空策略以减少未授权访问或破坏纸质文件、介质和信息处理设施的风险。

11.3.1 口令的使用

控制：

应要求用户在选择和使用口令时遵循良好的安全惯例

实施指南：

建议所有用户：

a） 保密口令；
b） 避免保留口令的副本（例如在纸上、软件文件中或手持设备中），除非可以安全地保存，存储方法得到批准；
c） 每当有任何迹象表明系统或口令可能受到损害时就变更口令；
d） 选择具有最小长度的优质口令，这些口令：
  1） 要易于记忆；
  2） 不能基于别人可能易于猜出或获得的与使用人相关的信息，例如，名字、电话号码和生日等等；
  3） 不容易遭受字典攻击（例如不包含存在于字典中的词）；
  4） 避免连续的相同的字符或全数字或全字母组。
e） 定期或以访问次数为基础变更口令（有特权的账户用的口令应比常规口令更频繁地予以变更），并且避免重新使用旧的口令或周期性使用旧的口令；
f） 在初次登录时更换临时口令；
g） 在任何自动登录过程（例如，以宏或功能键存储）中，不要包含口令；
h） 个人的用户口令不要共享；
i） 不在业务目的和非业务目的中使用相同的口令。

如果用户需要访问多服务、系统或平台，并且要求维护多个隔离的口令，则应建议他们可以使用同一个优质的口令（见上述 d））用于所有服务，用户要确信对每一个服务、系统或平台所存储的口令建立了合理级别的保护。

其他信息：

要专门注意处理口令丢失或忘记的桌面帮助系统的管理，因为这些也可能是对口令系统攻击的一种手段。

11.3.2 无人值守的用户设备

控制：

用户应确保无人值守的设备得到适当的保护

实施指南：

所有用户应了解保护无人值守设备的安全要求和程序以及他们实现这种保护的职责。建议用户应：

a） 当结束时，终止有效会话，除非利用一种合适的锁定机制使它们安全，例如，有口令保护的屏幕保护程序；

b） 当会话结束时退出主计算机、服务器和办公PC（即，不仅仅关掉PC 屏幕或终端）；

c） 当不使用设备时，利用带钥匙的锁或等价控制措施来保护PC 或终端不被未授权使用，例如，口令访问。

其他信息：

在用户区安装的设备（例如工作站或文件服务器）在长期无人值守时可能需要专门的保护，以防止未授权访问。

11.3.3 桌面和屏幕清空策略

控制：

应采用针对文件、可移动储存介质的桌面清空策略和针对信息处理设施的屏幕清空策略。

实施指南：

清空桌面和清空屏幕策略要考虑到信息安全分类（见 7.2）、法律和合同要求（见 15.1）、相应的风险和组织的文化方面。下列指南要予以考虑：

a） 当不用时，特别是当离开办公室时，敏感或关键业务信息应藏起来（理想的是，藏在耐火保险柜或箱中）；

b） 当无人值守时，计算机和终端应注销或使用由口令、令牌或类似的用户认证机制控制的屏幕和键盘锁定机制进行保护，当不使用时，要利用带钥匙的锁、口令或其他控制进行保护；

c） 进来和出去的邮件点和无人值守的传真机要受到保护；

d） 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） 包含敏感或分类信息的文件应立即从打印机中清除。

其他信息：

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

要考虑使用带有个人识别码功能的打印机，使得原始操作人员是能获得打印输出的唯一人员，也几乎是位于打印机边的唯一人员。

11.4 网络访问控制

目标：防止对网络服务未经授权的访问

对内部和外部网络服务的访问均应加以控制。

访问网络和网络服务的用户不应损害网络服务的安全，应确保：

a) 在本组织的网络和其他组织拥有的网络或公共网络之间有合适的分界；
b) 对用户和设备有合适的认证机制；
c) 对用户访问信息服务的强制控制。

11.4.1 网络服务使用策略

控制：

用户应只能访问经过明确授权使用的服务

实施指南：

应制定关于使用网络和网络服务的策略。这应包括：

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和程序；
d） 访问网络和网络服务使用的手段（例如，拨号访问互联网服务提供商或远程系统的条件）。

网络服务使用策略应与业务访问控制策略相一致（见 11.1）。

其他信息：

与网络服务的未授权和不安全连接可以影响整个组织。对于与敏感或关键业务应用连接的网络或与高风险位置（例如，超出组织安全管理和控制的公共区域或外部区域）的用户连接的网络而言，这种控制特别重要。

11.4.2 外部连接用户鉴别

控制：

应使用适当的鉴别方法控制远程用户的访问

实施指南：

远程用户的鉴别可以使用基于密码技术硬件令牌或询问/响应协议来实现。在各种各样的虚拟专用网络（VPN）解决方案中存在这种技术可能的实现。专线也可用来提供连接来源的

保证。

回拨程序和控制，例如使用回拨调制解调器，可以防止与组织信息处理设施的未授权和不希望的连接。这种控制类型可鉴别从远程地点试图与组织网络建立连接的用户。当使用这种控制时，组织应不使用包括前向呼叫的网络服务，或者，如果他们使用了上述这种网络服务，则他们应使这种特性不能使用，以避免与前向呼叫相关的弱点。反向呼叫过程包括确保在组织一侧出现有效断开也是重要的。否则，远程用户可以保持线路开路，假装已出现反向呼叫验证。对于这种可能性，应充分地测试反向呼叫程序和控制。

若远程用户组被连接到安全共享的计算机设施，那么，结点鉴别可用作鉴别他们的可替代手段。密码技术（例如基于机器证书）能用于结点鉴别。这是有些 VPN 解决方案的一部分。

应实施附加的鉴别以控制对无线网络的访问。尤其是由于存在未监测截取和网络流插入的大量机会，在为无线网络选择控制时需要专门注意。

其他信息：

外部连接为未授权访问业务信息提供了可能，例如，通过拨号方法的访问。因此，远程用户的访问应受鉴别限制。具有不同类型的鉴别方法，其中某些方法提供比其他方法更高级别的保护，例如，基于使用密码技术的方法可以提供强鉴别。重要的是根据风险评估确定所要求的保护级别。这需要选择合适的鉴别方法。

与远程计算机自动连接的设施可能提供获得对业务应用进行未授权访问的方法。如果该连接使用超出组织安全管理控制的网络，这样做特别重要。

11.4.3 网络设备标识

控制：

应考虑自动设备标识，将其作为鉴别特定位置和设备连接的方法。

实施指南：

如果通信只能从特定位置或设备进行启动，则可使用设备标识。设备的或与设备连接的标识符能用于指示此设备是否允许连接网络。如果存在多个网络，尤其是如果这些网络有不同的敏感度，这些标识符应清晰的指明设备允许连接到哪个网络。可能需要考虑设备的物理保护以维持设备标识符的安全。

其他信息：

本控制可补充其他技术以认证设备的用户（见 11.4.2）。设备标识也可用于用户认证。

11.4.4 远程诊断和配置端口保护

控制：

应控制对诊断和配置端口的物理和逻辑访问

实施指南：

访问诊断和配置端口的潜在控制包括带钥匙的锁和支持程序的使用，以确保对端口的物理访问。这种支持程序的一个例子是确保诊断和配置端口只有按照计算机服务管理者和要求访问的硬件/软件支持人员之间的安排才可访问它们。

如果业务功能没有专门需要，安装在一个计算机或网络设施中的端口、服务和类似的设施， 则应停止或取消。

其他信息：

许多计算机系统、网络系统和通信系统装配了远程诊断或配置设施，以便供维护工程师使用。如果不受保护，则这些诊断端口提供未授权访问的手段。

11.4.5 网络隔离

控制：

应隔离信息系统内的信息服务组、用户和信息系统

实施指南：

控制大型网络安全的一种方法是将该大型网络分成若干独立的逻辑网络域，例如，组织的内部网络域和外部网络域，每个域均受已定义的安全边界所保护。划分为不同等级的控制集能应用到不同的逻辑网络域，以进一步隔离网络安全环境，例如公共可访问系统、内部网络和关键资产。域应基于风险评估和每个域内的不同安全要求来定义。

这样的边界可以通过在被互连的两个网络之间安装一个安全网关来实现，以控制这两个域之间的访问和信息流。这种网关要配置成能过滤这些域之间的通信量（见 11.4.6 和 11.4.7），并且能按照组织的访问控制策略阻挡未授权访问（见 11.1）。这种类型的网关例子是通常称作防火墙的东西。另外一个隔离逻辑域的隔离方法是通过为组织内的用户组使用虚拟专用网来限制网络访问。

网络也可以使用网络设备进行功能性隔离，例如 IP 转换。隔离域能通过使用路由/转换能力（例如访问控制列表）控制网络数据流而实现。

将网络隔离成若干域的准则应基于访问控制策略和访问要求（见 10.1），还要考虑到相关成本和加入适合的网络路由选择的性能影响或网关技术（见 11.4.6 和 11.4.7）。

另外，为减少服务破坏的总的影响，网络的隔离应基于网络中存储或处理信息的价值和分类、信任级别或业务线。

应考虑无线网络与内部和专用网络的隔离。因为无线网络的边界不好定义，在这种情况下，应执行风险评估识别控制措施（例如，强认证、密码手段和频率选择），以维持网络隔离。

其他信息：

网络正在日益扩充超出传统组织边界范围，因为形成的业务伙伴可能需要信息处理和网络设施的互连接或共享。这样的扩充可能增加对早已存在使用此网络的信息系统进行未授权访问的风险，其中的某些系统由于它们的敏感性或关键性可能要求阻止其他网络用户未授权

访问。

11.4.6 网络连接控制

控制：

在公共网络中，尤其是那些延展到组织边界之外的网络，应限制用户联接的能力，并与业务应用系统的访问控制策略和要求一致（见 11.1）

实施指南：

访问控制策略要求维护和更新用户的网络访问权力（见 11.1.1）。

用户的连接能力可通过网关来限制，该网关借助预先定义的表或规则过滤通信量。施加限制的应用例子有：

a） 消息传递，例如电子邮件；
b） 文件传送；
c） 交互式访问；
d） 应用访问。

应考虑将网络访问权力限制到日或日期的确定时间。

其他信息：

共享网络特别是扩充跨越组织边界的那些共享网络的访问控制策略要求，可能需要引入限制用户连接能力的控制。

11.4.7 网络路由控制

控制：

应对网络进行路由控制，以确保信息联接和信息流不违反业务应用系统的访问控制策略

实施指南：

路由选择控制应基于确定的源地址和目的地址检验机制。

如果使用了代理和/或网络地址转换技术，安全网关能在内部和外部网络控制点验证源地址和目的地址。实现者要了解所采用的机制的强度和缺点。网络路由控制的要求应基于访问控制策略（见 11.1）。

其他信息：

共享网络，可能要求附加的路由选择控制，特别是扩充跨越组织边界的那些共享网络。对于与第三方（非组织）用户共享的网络，这种控制通常是必需的。

11.5 操作系统访问控制

目标：防止对操作系统的未授权访问

安全设施应该用来限制授权用户访问操作系统。这些设施应该包括下列内容：
a) 按照已定义的访问控制策略鉴别授权用户；
b) 记录成功和失败的系统认证尝试；
c) 记录专用系统特权的使用；
d) 当违背系统安全策略时发布警报；
e) 提供合适的认证手段；
f) 恰当处可限制用户的连接次数。

11.5.1 安全登陆程序

控制：

应通过安全登陆程序对操作系统的访问进行控制

实施指南：

登录到操作系统的程序应设计成使未授权访问的机会减到最小的。因此，登录程序应泄露最少有关系统的信息，以避免提供给未授权用户不必要的帮助。良好的登录程序应：

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本计算机通用告警通知；
c） 在登录过程期间，不提供对未授权用户有辅助作用的帮助消息；
d） 仅在所有输入数据完成时才验证登录信息。如果出现差错情况，该系统不应指出数据的哪一部分是正确的或不正确的；
e） 限制所允许的不成功登录尝试的次数（推荐3 次）并考虑：
  1） 记录不成功的尝试和成功的尝试；
  2） 在允许进一步登录尝试之前，强加一次延迟，或在没有特定授权情况下拒绝任何进一步的尝试；
  3） 断开数据链路连接；
  4） 如果达到登录的最大尝试次数，向系统控制台发送警报消息；
  5） 结合口令的最小长度和被保护系统的价值一起考虑口令重试的次数的设置；
f） 限制登录程序所允许的最大和最小时间。如果超时，则系统应终止登录；
g） 在成功登录完成时，显示下列信息：
  1） 前次成功登录的日期和时间；
  2） 上次成功登录之后的任何不成功登录尝试的细节；
h） 不显示输入的口令或考虑通过符号隐藏口令字符；
i） 不在网络上以明文传输口令。

其他信息：

如果在网络上登录会话期间，口令以明文传输，他们可能会被网络上的网络“嗅探器”程序捕获。

11.5.2 用户标识与鉴别

控制：

所有的用户应有一个唯一的识别码（用户 ID）且仅供本人使用，应使用适当的鉴别技术来证实用户所声称的身份

实施指南：

应对所有类型的用户（包括技术支持人员，操作员，网络管理员、系统程序员和数据库管理员）应用控制。

用户标识符（用户 ID）应唯一，以使得各个活动可以追踪到各个责任人。正常的用户活动不应使用特权帐户执行。

在例外环境下，如果存在明显的业务利益，可以使用一群用户或一项特定作业共享同一个用户 ID 的做法。对于这样的情况，应将管理层的批准形成文件。为维护可核查性，可以要求附加的控制。

个人使用的普通 ID 应只允许 ID 执行的可访问功能或行动不需要追踪时（例如只读访问），或者有其他合适的控制时（例如，每次发给职员普通 ID 口令，并记录这种情况）使用。

需要强认证和身份验证时，应使用认证方法代替口令，例如密码手段、智能卡、令牌或生物手段。

其他信息：

口令（也见 11.3.1 和 11.5.3）是一种很通常的提供识别和认证的方法，因为它基于只有该用户知道的秘密。使用密码手段和认证协议也可以获得同样的效果。用户识别和认证的强度应对应于被访问信息的敏感度。

用户拥有的客体（诸如记忆令牌或智能卡）也可以用于识别和认证。利用个人的唯一特征或属性的生物统计认证技术也可用来认证个人的身份。机制和技术的安全组合将产生更强的认证

11.5.3 口令管理系统

控制：

应是使用交互式口令管理系统，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，并且包括确认程序，以便考虑到输入出错的情况；
c） 强制选择优质口令（见11.3.1）；
d） 强制口令变更（见11.3.1）；
e） 在第一次登录时强制用户变更临时口令（见11.2.3）；
f） 维护一份先前用户口令的记录，并且防止重复使用；
g） 当正在录入时，在屏幕上不显示口令；
h） 分开存储口令文件和应用系统数据；
i） 以保护的形式（例如加密或哈希）存储和传输口令。

其他信息：

口令是确认用户访问计算机服务权限的主要手段之一。

某些应用要求由某个独立机构分配的用户口令；在这种情况下，上述指南 b)、d)和 e)不适用。在大多数情况下，口令由用户选择和维护。使用口令的指南见 11.3.1。

11.5.4 系统设施的使用

控制：

应限制并严格控制设施程序的使用和应用系统控制的使用

实施指南：

应考虑系统使用程序的下列指南：

a） 对于系统实用程序，使用识别、认证和授权程序；
b） 将系统实用程序和应用软件分开；
c） 限制系统实用程序的使用，将实际的所信任的、已授权的用户数降到最小（也见11.2.2）；
d） ad hoc 系统实用程序的授权；
e） 限制系统实用程序的可用性，例如，在已授权变更的持续期内；
f） 记录系统实用程序的所有使用；
g） 对系统实用程序的授权级别进行定义并形成文件；
h） 移去基于实用程序和系统软件的所有不必要软件；
i） 责任要求分离时，系统中访问应用的用户不可使用系统实用程序。

其他信息：

大多数计算机安装有一个或多个系统实用程序能越过系统和应用的控制。

11.5.5 会话超时

控制：

不活动的会话应在一个设定的不活动周期后关闭。

实施指南：

超过一段设定的不活动的时限，超时设施应清空会话屏幕并且，也可能在超时更长时，关闭应用和网络会话。超时的延迟应反映区域的安全风险，被处理的信息和被使用应用的类别，以及与用户的设备相关的风险。

对某些清空其屏幕并防止未授权访问，但没有关闭应用或网络会话的系统可以提供一种受限制的终端超时设施形式。

其他信息：

这种控制在高风险位置特别重要，包括超出组织安全管理的公共或外部区域。会话应关闭以防止未授权人员访问和拒绝服务攻击。

11.5.6 连接时间限制

控制：

应使用连接时间限制以提供高风险应用程序的额外安全保障

实施指南：

敏感的计算机应用，特别是安装在高风险位置（例如，超出组织安全管理的公共区域或外部区域）的应用，应考虑连接时间控制。

这种限制的例子包括：

a） 使用预先定义的时隙，例如，对成批文件传输或短持续期的定期交互会话；
b） 如果对超出时间或延长时间的操作没有要求，则将连接时间限于正常办公时间；
c） 考虑以定时的间隔进行重新认证。

其他信息：

限制允许终端连接计算机服务的周期以减少未授权访问机会。活动会话持续时间的限制防止用户长时间拥有会话阻碍重新认证。

11.6 应用系统和信息访问控制

目标：防止对应用系统中信息的未授权访问

安全设施应该将访问限制在应用系统之内。

对应用软件和信息的逻辑访问只限于已授权的用户。应用系统应：

a) 按照定义的访问控制策略，控制用户访问信息和应用系统功能；
b) 防止能够越过系统控制或应用控制的任何实用程序、操作系统软件和恶意软件进行未授权访问；
c) 不损坏共享信息资源的其他系统的安全；

11.6.1 信息访问限制

控制：

应根据规定的访问控制策略，限制用户和支持人员对信息和应用系统功能的访问

实施指南：

对访问的限制应基于各个业务应用要求。访问控制策略也应与组织的访问策略（见 11.1）一致。

为支持访问限制要求，应考虑应用以下指南：

a） 提供控制访问应用系统功能的选单；
b） 控制用户的访问权力，例如，读、写、删除和执行；
c） 控制其他应用的访问权力；
d） 确保处理敏感信息的应用系统的输出仅包含与使用输出相关的信息，并且仅发送给已授权的终端和地点，包括周期性评审这种输出，以确保去掉多余信息。

11.6.2 敏感系统隔离

控制：

敏感系统应使用独立的计算环境

实施指南：

对于敏感系统隔离，应考虑以下内容：

a） 应由应用责任人显式地标识出应用系统的敏感性，并将其形成文件（见7.1.2）。
b） 当敏感应用在共享的环境中运行时，与其共享资源的应用系统应予以标识并与敏感应用的责任人商定。

其他信息：

某些应用系统对信息的可能丢失十分敏感，因此要求特别处理这些信息。敏感性可以指示该应用系统：

a) 应运行在专用的计算机上；
b) 仅与可信的应用系统共享资源。

隔离可通过使用物理或逻辑手段实现（也见 11.4.5）。

11.7 移动计算和远程工作

目标：确保在使用移动计算和远程工作设施时信息的安全

所要求的保护应与那些特定工作方法引起的风险相匹配。当使用移动计算时，应考虑不受保护的环境中的工作风险，并且要应用合适的保护。在远程工作的情况下，组织要把保护应用于远程工作场地，并且对这种工作方法，确保合适的安排到位。

11.7.1 移动计算及通讯

控制：

应建立正式的策略并实施适当的控制，以防范使用移动计算和通讯设施的风险

实施指南：

当使用移动计算和通信设施时，例如，笔记本机、掌上机、膝上机、智能卡和移动电话，应特别小心确保业务信息不被泄露。移动运算策略应考虑到在不受保护的环境下使用移动计算设施的工作风险。

移动运算策略应包括对物理保护、访问控制、密码技术、备份和病毒预防的要求。这种策略也应包括关于移动设施与网络连接的规则和建议以及关于在公共场合使用这些设施的指南。

当在组织建筑物之外的公共场所、会议室和其他不受保护的区域使用移动计算设施时，应多加小心。为避免未授权访问或泄露这些设施所存储和处理的信息，保护应到位，例如，使用密码技术（见 12.3）。

当这样的设施用于公共场合时，应小心避免未授权的个人窥视的风险。防范恶意软件的程序应到位并且保持经常更新（见 10.4）。

应定期对关键业务信息进行备份。设备应能快速、简便备份信息。对这些备份应给予足够的保护，诸如防止信息被偷窃或丢失。

对与网络连接的移动设施的使用应提供合适的保护。在成功标识和认证之后，同时在合适的访问控制机制到位的情况下，才可利用移动计算设施通过公共网络远程访问业务信息（见 11.4）。

移动计算设施，在物理上也应防止被偷窃，例如，特别是遗留在汽车和其他形式的运输工具、旅馆房间、会议中心和会议室的这种设施。携带重要、敏感和/或关键业务信息的设备不应丢下无人值守，若有可能，在物理上应能锁起来，或使用专用锁来保护设备。关于物理保护移动设备的更多信息可在 9.2.5 中找到。

对于使用移动计算的人员应安排培训，以提高他们对于由这种工作方法导致的附加风险的意识，并且应实施若干控制。

其他信息：

移动网络无线连接类似于其他类型的网络连接，但在识别控制时，应考虑其重要的区别。典型的区别是 1）一些无线安全协议是不成熟的，并有已知的弱点，2）在移动计算机上存储的信息可能不需要备份，因为受限的网络带宽和/或因为移动设备在备份时不会进行连接。

11.7.2 远程工作

控制：

应开发并实施远程工作的策略、操作计划和程序

实施指南：

如果合适的安全布置和控制到位并且符合组织的安全策略，组织才能授权远程工作活动。

远程工作场地的合适保护应到位，以防止偷窃设备和信息、未授权泄露信息、未授权远程访问组织内部系统或滥用设施等。远程工作要由管理层授权和控制以及对远程工作方法要有到位的合适安排。

应考虑下列内容：

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) 所建议的远程工作环境；
c) 通信安全要求，要考虑到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) 住处的其他人们（例如，家人和朋友）未授权访问信息或资源的威胁；
e) 家庭网络的使用和无线网络服务配置的要求或限制；
f) 针对私有设备开发的防止关于知识产权权利争论的策略和程序；
g) 法律阻止的对私有设备的访问（检查机器安全或在调查期间）；
h) 使组织对许可雇员、订约人或第三方用户使用工作站上的私有客户端软件负有责任的软件许可协议；
i) 防病毒保护和防火墙需求。

要考虑的指南和安排包括：

a) 当不允许使用处于组织控制之外的私有设备时，对远程工作活动提供适合的设备和存储器具；
b) 定义所允许的工作、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) 备份和业务连续性的程序；
i) 审核和安全监督；
j) 当远程工作活动停止时，撤销授权和访问权，并返回设备。

其他信息：

远程工作使用通信技术使得职员可以在组织之外的固定地点进行远程的工作。

12 信息系统的获取、开发和保持

12.1 信息系统的安全要求

目标：确保安全成为信息系统的内置部分

这将包括操作系统、基础设施、业务应用、非定制的产品、服务和用户开发的应用。支持应用或服务的业务过程的设计和实施可能是安全的关键。在信息系统开发之前应标识出并商定全要求。

应在项目的要求阶段标识出所有安全要求，并证明这些安全要求是正确的，对这些安全要求加以商定，并且将这些安全要求形成文档作为信息系统整个业务情况的一部分。

12.1.1 安全要求分析和规范

控制：

新的信息系统或对现有信息系统的更新的业务要求声明中应规定安全控制的要求

实施指南：

控制需求规范应考虑在系统中所包含的自动化控制以及支持人工控制的需要。当评价业务应用（开发或购买）的软件包时，应进行类似的考虑。

安全要求和控制应反映出所涉及信息资产的业务价值和潜在的业务损坏，这可能是由于安全失败或缺少安全引起的。

信息安全系统需求与实施安全的过程应该在信息安全工程的早期阶段集成。在设计阶段引入控制其实施和维护的费用明显低于实现期间或实现后所包含的控制费用。

如果产品是购买的，则购买产品之后就进行常规的测试和需求处理。与供货商签的合同上应确切地标明安全需求。一旦推荐商品的安全功能不能满足安全要求，则在购买商品之前应重新考虑引进和相关控制的风险。如果产品的附加功能引起了一些安全风险，则这个产品是不能用的，或者增加的功能优点突出，则可以对推荐的控制结构重新讨论决定。

其他信息：

如果适当考虑花费的因素，管理层可能更愿意使用已独立评价和认证的产品。关于 IT 安全产品的评估准则的其它信息可 ISO/IEC 15408，或者其它评估和认证标准。ISO/IEC TR13335-3 提供了应用风险管理过程去确认安全控制要求的指南。

12.2 应用系统的正确处理

目标：防止应用系统信息的错误、丢失、未授权的修改或误用

应用系统（包括用户开发的应用）内应设计合适的控制以确保处理的正确性。这些控制应包括输入数据、内部处理和输入数据的确认。

对于处理敏感的、有价值的或关键的组织资产的系统或对上述组织资产有影响的系统可以要求附加控制。这样的控制应在安全要求和风险评估的基础上加以确定。

12.2.1 输入数据确认

控制：

应验证应用系统输入数据，以确保正确和适当

实施指南：

检验应适用于业务事务处理、常备数据（名字和地址，信贷限值，顾客引用号码）和参数表（销售价，货币兑换率，税率）的输入。应考虑下列控制：

a) 双输入或其他输入检验，比如边界检查或者限制具体范围的输入数据，以检测下列差错：

1） 范围之外的值；
2） 数据字段中的无效字符；
3） 丢失或不完整的数据；
4） 超过数据的上下容量极限；
5） 未授权的或不相容的控制数据；

b） 周期性评审关键字段或数据文件的内容，以证实其有效性和完整性；

c） 检查硬拷贝输入文档是否有任何未授权的变更输入数据（输入文档的所有变更均应予以授权）；

d） 响应确认差错的程序；

e） 测试输入数据真实性的程序；

f） 定义在数据输入过程中所涉及的全部人员的职责。

g） 创建一个数据输入过程中的行为日志。

其他信息：

考虑在应用中对输入数据进行自动检查和确认，以减少出错的风险，防止缓冲区溢出和代码注入等标准攻击。

12.2.2 内部处理控制

控制：

应用系统中应包含确认检查，以检测数据处理过程中的错误

实施指南：

应用系统的设计与实施应确保由于处理失败导致的完整性被损坏的风险减至最小。考虑的特定风险区域包括：

a) 使用程序中的增加、修改和删除功能，以实现数据变更；
b) 防止程序以错误次序运行或在前面的处理故障后运行的程序（也见8.1.1）；
c) 使用从失效中恢复的正确程序，以确保正确处理数据。
d) 防止利用缓冲区溢出进行的攻击。

应该准备适当的检测列表，检测行为需要记录文档，检测结果要保持安全。可以包括的检验的例子包括如下：

a) 会话或批量控制，以便在事务处理更新之后调解数据文件平衡；
b) 平衡控制，对照先前的封闭平衡来检验开放平衡，即：
   1） 运行至运行的控制；
   2） 文件更新总量；
   3） 程序至程序的控制；
c) 确认系统生成的输入数据（见10.2.1）；
d) 检验在中央计算机和远程计算机之间所下载或上载的数据或软件的完整性、真实性或者其他任何安全特性（见10.3.3）；
e) 求所有记录和文件的散列函数值；
f) 检验以确保应用程序在正确时刻运行；
g) 检验以确保程序以正确的次序运行并且在故障情况下终止；进一步处理被停止，直到解决问题为止。
h) 创建一个有关处理的行为日志。

其他信息：

正确输入的数据可能被硬件错误、处理错误和故意的行为破坏。确认性检查的需求取决于应用的特点和毁坏的数据对业务的影响。

12.2.3 消息完整性

控制：

应识别应用系统中确保鉴别和保护消息完整性的要求，识别并实施适当的控制

实施指南：

需要进行安全风险的评估以确定是否需要报文完整性，以确定实施中的最合适的方法。

其他信息：

密码技术（见 10.3.2 和 10.3.3）是一种能用作实现报文鉴别的合适手段。

12.2.4 输出数据确认

控制：

应确认应用系统输出的数据，以确保存储的信息的处理是正确的并与环境相适宜

实施指南：

输出确认可以包括：

a) 真实性检验，以测试输出数据是否合理；
b) 调解控制计数，以确保处理所有数据；
c) 对信息阅读者或后续处理系统提供足够的信息，以确定信息的准确性、完备性、精确性和分类；
d) 响应输出确认测试的程序；
e) 定义在数据输出过程中所涉及的全部人员的职责。
f) 创建一个输出数据确认行为的日志。

其他信息：

典型地，系统和应用是在假设已经具备了适当的确认、认证、测试和输出数据总是正确的条件下构建的。然而这种假设不总是正确的，例如，一个经过检测的系统在一些环境下会产生不正确的输出。

12.3 加密控制

目标：通过加密手段来保护细腻的保密性、真实性或完整性

应该制定使用密码的策略。密钥管理应该支持使用密码技术。

12.3.1 使用加密控制的策略

控制：

为保护信息，应开发并实施加密控制的使用策略

实施指南：

制定密码策略时，应考虑下列内容：

a) 关于跨越组织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) 基于风险评估确认要求的保护级别，包括要求的加密算法的类型、强度和质量。
c) 使用密码技术保护用移动电话、可移动介质、设备或者通过通讯线路传输的敏感信息。
d) 密钥管理方法，包括密码密钥的保护，密钥遗失、泄密和毁坏后加密数据的恢复。
e) 角色和职责。谁负责：
   1） 策略的实施；
   2） 密钥管理，包括密钥的生成；
f) 为在整个组织有效实施而采用的标准（哪种解决方法用于哪些业务过程）。
g) 使用密码技术对控制的影响依赖于内容检查（例如病毒检查）。

当实施整个组织的密码策略时，应该考虑世界不同地区应用密码技术的规定和限制，也应考虑加密信息在出入境时的限制。（见 15.1.6）

可以使用密码技术去获得不同的安全目标：

a) 保密性：用信息加密去保护存储的和传输中的敏感和重要数据。
b) 完整性/可认证性：用数字签名和消息验证码去保护存储的和传输中的敏感和重要数据的可认证性和完整性。
c) 不可否认性：利用密码技术获得事件和行为发生或未发生的证明。

其他信息：

一个密码解决方案是否合适，需要根据广泛的风险评估和选择控制来做出决定。这些评估可以用来判断一个密码控制是否合适，应该用什么类型的控制以及是应用于什么目的和业务流程。

一个应用密码控制的策略需要使其利益最大化，使利用密码技术的风险最小化，并尽量避免不合适和不正确的使用。在应用数字签名时，需要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）。

提供需要的保护和实施安全密钥管理系统需要由专家确认适当的保护级别和定义适当的规范。

ISO/IEC JTC1 SC27 已经制定了几个与密码控制有关的标准。更多的信息可以从 IEEEP1363 和 OECD 指南中获得。

12.3.2 密钥管理

控制：

应进行密钥管理，以支持组织对密码技术的使用

实施指南：

所有的密码密钥要防止修改、遗失和毁坏。另外，秘密和私有密钥需要防止非授权的泄露。用来生成、贮存和归档密钥的设备需要进行物理保护。

密钥管理系统应基于一组已商定的标准、规程和方法，以便：

a) 生成用于不同密码系统和不同应用的密钥；
b) 生成和获得公开密钥证书；
c) 分发密钥给预期用户，包括应如何激活收到的密钥；
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，包括何时变更密钥以及如何变更密钥的规则；
f) 处理已泄露的密钥；
g) 撤销密钥，包括如何取消或解除激活的密钥，例如，当密钥已泄露时或当用户离开组织时（在这种情况下，密钥也要归档）；
h) 恢复密钥，作为业务连续性管理的一部分，恢复已丢失或损坏的密钥，例如，加密信息的恢复；
i) 归档密钥，例如，对已归档的或备份的信息的密钥归档；
j) 销毁密钥；
k) 记录和审核与密钥管理相关的活动。

为了减少泄露密钥的可能性，密钥应具有已定义的激活日期和解除激活日期，以使它们只能用于有限的时间周期。这个时间周期应根据所使用的密码控制的情况和所评估的风险而定。

除了安全管理秘密密钥和私有密钥外，还要考虑公开密钥的保护。这些认证过程可以由证书认证机构颁发的公钥证书来完成，该认证机构是一公认的组织，具有合适的控制和规程，可提供所要求的可信等级。

与外部密码服务提供者（例如与认证机构）签署的服务级协议或合同的内容应涵盖服务条款方面的服务责任、服务可靠性和响应次数的若干问题（见 6.2.3）。

其他信息：

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。下面给出了两密钥管理技术：

a) 秘密密钥技术，其中双方或更多方共享同一密钥，并且该密钥用来加密和解密信息。这个密钥必须被秘密地保存，因为访问过它的任何人能使用该密钥来解密被加密的所有信息，或引入未授权的信息。
b) 公开密钥技术，其中每个用户拥有一对密钥，一个公开密钥（它可以被展现给任何人）和一个私有密钥（它必须被秘密地保存）。公开密钥技术可用于加密，并可用来产生数字签名（参见ISO/IEC 9796 和ISO/IEC 14888）。

存在某人用他自己的公开密钥替换某用户的公开密钥伪造数字签名的威胁。

密码技术可以用来保护密钥。规程可以考虑处理访问密钥的合法请求，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。

12.4 系统文件安全

目标：确保系统文件的安全。

要严格控制访问系统文件和程序源代码。按安全方式管理IT 项目和支持活动。在测试环境中应注意不能泄露敏感数据。

12.4.1 操作软件控制

控制：

应建立程序，对操作系统软件安装进行控制

实施指南：

为使运行系统被损坏的风险减到最小，应考虑下列控制。

a) 仅由受过专业培训的管理员根据相应的管理授权进行操作软件、应用和运行程序库的更新（见12.4.3）；
b) 运行系统只安装经核准的可执行代码，不安装开发代码和编译器；
c) 应用和操作系统软件只有在全面正确的测试后才能安装，测试包括实用性、安全性、在其它系统上的有效性，用户友好性，测试需要在独立的系统上完成，必须确保对应的程序库已经更新；
d) 应用配置控制系统去控制所有已开发的软件和系统文件；
e) 系统在修改之前应进行反复考虑；
f) 应维护对运行程序库的所有更新的审核日志；
g) 应保留软件的先前版本作为应急措施；
h) 软件的旧版本，包括需要的信息、参数、过程、配置细节都要归档，配套有文件和数据也要归档。

在运行系统中所使用的由厂商供应的软件应在供应商支持的级别上加以维护。过时后，软件供应商应停止提供旧版本的软件，组织应考虑依赖不支持软件的风险。

升级到新版的任何判定应考虑到该新版的安全，即，新安全功能度的引入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时，应使用软件补丁（见12.6.1）。

必要时在管理层批准的情况下，仅为了支持目的，才授予供应商物理或逻辑访问权。应监督供应商的访问活动。

计算机软件可能依赖于外部提供的软件和模块，对这些产品应该进行监控，以防止非授权的修改，因为这些修改可能带来安全问题。

其他信息：

操作系统只有在需要升级的时候才进行升级，比如说，当操作系统的当前版本不能支持业务需求的时候。只有有了新版本的操作系统后才能进行升级。新版本的操作系统可能在安全、稳定和便于理解方面不如当前版本的操作系统。

12.4.2 系统测试数据的保护

控制：

应谨慎选择测试数据，并加以保护和控制

实施指南：

应避免使用包含个人信息和其它敏感信息的运行数据库作为测试目的用。如果使用这种信息，在使用之前应除去个人化信息。当用于测试目的时，应使用下列控制保护运行数据：

a) 访问控制规程，适用于运行应用系统，还应适用于测试应用系统；
b) 运行信息每次被拷贝到测试应用系统应予以分别授权；
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) 为提供审核踪迹，应记录运行信息的拷贝和使用。

其他信息：

系统和验收测试常常要求相当大的尽可能接近运行数据的测试数据量。

12.4.3 对程序源代码的访问控制

控制：

应限制对程序源代码的访问

实施指南：

对程序源代码和相关事项（包括设计、规范、证明设计和确认设计）的访问应该严格禁止，以防止带入一些非授权功能，避免对源代码的无意识的修改。程序源代码可以放在中央存储区中，最好放在程序代码库中。为了控制对程序源代码库的访问以减少对计算机程序破坏的可能，应该遵守下面的指南：

a) 若有可能，在运行系统中不应保留源程序库；
b) 程序源代码和程序源库应根据制定的程序进行管理；
c) 支持人员不应不受限制地访问源程序库；
d) 更新源程序库和有关事项、向程序员发布源程序应在授权之后进行；
e) 程序列表应保持在安全的环境中（见12.7.4）；
f) 应维护对源程序库所有访问的审核日志；
g) 维护和拷贝源程序库应受严格变更控制规程的制约（见12.5.1）。

其他信息：

程序源代码是由程序员编写的代码，经编译（连接）后产生执行代码。有的语言不能正常区分源程序代码和执行代码，这是因为执行代码是随程序产生而产生的。

标准ISO 1007 和ISO/IEC 12207 提供了更多关于配置管理和软件生命周期过程的信息

12.5 开发和支持过程安全

目标：保持应用系统软件和信息的安全

应严格控制项目和支持环境。

负责应用系统的管理者，也应负责项目和支持环境的安全。他们应确保评审所有建议的系统变更，以检验这些变更既不损坏该系统亦不损害操作环境的安全。

12.5.1 变更控制程序

控制：

应通过正式的变更控制程序，控制变更的实施

实施指南：

为使信息系统的损坏减到最小应实施正式的变更控制规程。它们应确保不损坏安全和控制规程，并将变更控制规程文档化，引进新的系统和对已有系统进行大的变更要按照从文档、规范、测试、质量管理到实施管理这个正常的过程进行。

这个过程应包括风险评估、变更效果分析、安全控制规范。它们应确保不损坏安全和控制规程，确保支持性程序员仅能访问其工作所需的系统的某些部分，确保对任何变更要获得正式商定和批准。

只要可行，应用和操作变更控制规程应集成起来（也见 10.1.2）。该过程应包括：

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损坏；
d) 标识要求修正的所有计算机软件、信息、数据库实体和硬件；
e) 在工作开始之前，获得对详述建议的正式批准；
f) 确保在任何实施之前，已授权的用户接受变更；
g) 为使业务损坏减到最小，确保完成实施；
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核踪迹；
j) 当需要时，确保对操作文档（见10.1.1）和用户规程作合适的修改；
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。

其他信息：

变更软件会影响运行环境。

实践表明，要在一个与生产与开发完全隔离的环境中测试新软件（也见 10.1.4）。这提

供对新软件进行控制和允许对运行信息（用于测试目的）给予附加保护的手段。这包括打补丁、服务包和其它更新。自动更新可以用在重要系统中，在这些系统中一些更新会引起一些重要应用的失败（见 12.6）。

12.5.2 操作系统变更后的应用系统技术评审

控制：

当操作系统变更后，应评审并测试关键的业务应用系统，以确保变更不会对组织的运营或安全产生负面影响

实施指南：

该过程应涵盖：

a) 评审应用控制和完整性规程，以确保它们不因操作系统变更而损坏；
b) 确保年度支持计划和预算将包括由于操作系统变更而引起的评审和系统测试；
c) 确保及时提供操作系统变更的通知，以允许在实施之前进行合适的评审；
d) 确保按业务连续性计划进行合适的变更（见第14 章）。

应该指定专门的组织和个人负责监视系统的弱点和供货商发布的补丁和修正。

12.5.3 软件包的变更限制

控制：

不鼓励对软件包进行变更。对必要的更改严格控制

实施指南：

在可能和可行范围内，应使用厂商供应的软件包，而无需修改。若认为修改软件包是必要的，应考虑下列各点：

a) 内置控制完整性过程被损坏的风险；
b) 是否要获得厂商的同意；
c) 按标准程序更新从厂商获得所要求的变更的可能性；
d) 如果作为变更的结果，组织要负责进一步维护此软件所带来的影响。

如果认为变更是重要的，则原始的软件要予以保留，并将变更应用于明确标识的拷贝。应建立软件更新管理流程以确保大部分最新的补丁和应用更新已经安装在所有的授权软件中（见 12.6）。应全面地测试所有变更，并将其形成文档，若需要，可以使它们重新应用于进一步的软件升级。如果需要的话，所有的更新应由独立的评估机构进行测试和验证。

12.5.4 信息泄漏

控制：

防止信息泄漏的机会

实施指南：

为了限制信息泄露的风险，如通过应用隐蔽通道，则应考虑下列事项：

a) 扫描隐藏信息的外部介质和通信。
b) 掩盖和调整系统和通信的行为，以减少类似第三方从那些行为中推断信息的能力。
c) 使用具有高信誉的系统和软件，比如用已评估的产品（见ISO/IEC 15408）。
d) 在法律和法规允许的前提下，定期监视个人的系统的行为。
e) 监视计算机系统的源码使用。

其他信息：

隐蔽信道不是故意设计用来引导信息泄露的通道，但它毫无疑问存在于系统或网络中。例如，通信协议包中的隐藏比特能够用来作为隐藏的信号的方法。从本质上说，防止所有可能的隐蔽通道的出现是很困难的。然而特洛伊木马经常利用隐蔽通道（见 10.4.1）。采取措施防止特洛伊木马能够减少隐蔽通道被利用的风险。

防止非授权的访问（11.4），采取措施和方法防止滥用个人信息服务会有助于保护隐蔽通道。

12.5.5 软件委外开发

控制：

组织应对软件委外开发进行监控

实施指南：

在软件委外开发的情况下，应考虑下列各点：

a） 落实准许证、代码所有权和知识产权（见15.1.2）；
b） 所完成工作的质量和准确性的认证；
c） 发生故障时第三方的契约安排；
d） 审核所做工作质量和准确性的访问权；
e） 代码质量和安全功能的合同要求；
f） 在安装前，检测恶意代码和特洛伊代码。

12.6 技术脆弱点管理

目标：减少由利用公开的技术脆弱点带来的风险

技术脆弱点管理应该以一种有效的、系统的、可反复的方式连同可确保其有效性的措施来实施。这些考虑应包括在用操作系统和任何其它的应用。

12.6.1 技术脆弱点控制

控制：

应及时获得组织所使用的信息系统的技术脆弱点的信息，评估组织对此类技术脆弱点的保护，并采取适当的措施

实施指南：

当前的完整的财产清单（见 7.1）是进行有效技术脆弱点管理的先决条件。支持技术脆弱点管理需要的特定信息包括软件供应商、版本号、软件部署的当前状态（即在什么系统上安装什么软件），和机构内负责软件的人员。

要采取适当的、及时的行动来确认潜要的技术脆弱点。建立有效的技术脆弱点管理流程要遵循以下原则：

a）机构应当定义和建立与技术脆弱点管理相应的角色和责任，这包括脆弱点监视、脆弱点风险评估、打补丁、资产跟踪、和任意需要的等价责任。

b）确认软件和其它技术的相关技术脆弱点的信息资源应予以标识（基于资产详细列表，见7.1.1），这些信息应根据清单列表的变化而更新，当发现其它新的或有用的信息后，信息资源也应该更新；

c）制定时间表对潜在的相关技术脆弱点通知做出反映；

d）一旦潜在的技术脆弱点被确认，机构应该确认相关的风险并采取措施；这些措施可能包括对脆弱点系统打补丁，或者应用其它控制；

e）根据技术脆弱点需要解决的紧急程度，根据改变管理相关的控制，或者根据信息安全事故应答规程完成采取的行为；

f）如果要安装补丁，则应先评估安装补丁可能带来的风险（脆弱点引起的风险应该同安装补丁带来的风险进行比较）。

g）补丁在安装之前应该进行测试与评估，以确保补丁是有效的，且不会带来不能容忍的副作用；如果没有合适的补丁，应该考虑采取其它控制措施，如：

1） 关掉与脆弱点有关的服务和性能；
2） 在网络国界上采用或增加访问控制，如防火墙（见11.4.5）
3） 增加监控以检测或防止实际的攻击；
4） 提高对脆弱点的意识能力；

h）对行为的所有过程应做审核日志；

i） 应定期对技术脆弱点管理过程进行监控和评估，以确保其效力和效率；

j） 处理高风险的系统应该先解决。

其他信息：

一个机构的技术脆弱点管理过程的正确实施对每个机构来说都是非常重要的，因此应该定期对其进行监控。要对潜在的相关技术脆弱点进行确认，一个准确的详细列表是最基本的。技术脆弱点管理可看作变化管理的一个子功能，因此可以利用变化管理的流程和规范（见 10.1.2 和 12.5.1）。

供货商往往是在面对很大的压力下才发布补丁，因此一个补丁可能不能准确地解决问题，也可能存在负作用。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准确的测试（可能因为费用或缺少资源），需要根据其它用户的经验报告，考虑推迟打补丁，评估相应的风险。

13 信息安全事故管理

13.1 报告信息安全事故和弱点

目标：确保与信息系统有关的安全事件和弱点的沟通能够及时采取纠正措施

应该准备好正常的事件报告和分类程序，这类程序用来报告可能对机构的财产安全造成影响的不同种类的事件和弱点，所有的员工、合同方和第三方用户都应该知晓这套报告程序。他们需要尽可能快地将信息安全事件和弱点报告给指定的联系方。

13.1.1 报告信息安全事件

控制：

应通过适当的管理途径尽快报告信息安全事件

实施指南：

应该建立正常的信息安全事件报告、事故应答和分类机制，在接到信息安全事件报告后着手采取措施。应该建立信息安全事件报告联系方，确保整个机构都知道这个联系方，这个联系方容易得到，并能做当及时的应答。

所有的员工、合同方和第三方用户都应该知晓他们有责任尽可能快地报告信息安全事件。他们应该知道报告信息安全事件的程序和联系方。报告机制应该包括：

a） 采取适当的反馈机制，以确保在信息安全事件处理完成后，能够将处理结果通知给事件报告方；

b） 信息安全事件的报告形式应该支持报告行为，帮助报告者去记下信息安全事件中的所有行为。

c） 信息安全事件发生后应该采取正确的行为，即

1） 立即记录下所有重要的细节（如冲突类型，发生的故障，屏幕上显示的消息，异常行为）；

2） 自己不要采取任何行动，只能立即向联系方报告；

d） 参考已建立的正常约束机制，来处理员工、合同方或第三方用户中的违反安全行为。在高风险环境下，可以提供强制报警，由此一个人在强制下可以指出那样的问题。对强制报警的应答机制应能反映那样的报警所指明的高风险情况。

其他信息：

信息安全事件和事故实例如下：

a) 服务、器材和设备的丢失，

b) 系统故障或超载，

c) 人为错误，
d) 策略或指南的冲突，
e) 违背物理安全设置，
f) 非控的系统改变，
g) 软件或硬件故障，
h) 非法访问。

从正当机密性方面考虑，信息安全事故可以用来对用户进行意识训练（见 8.2.2），如可能发生什么样的事故，对那样的事故应该怎样应对，怎样避免将来再发生此类事故。为了完全解决信息安全事件和事故，在其发生后应该尽可能搜集证据（见 13.2.3）。

故障或其它异常的系统行为可能是安全攻击和实际安全问题的指示器，因此应该将其当作信息安全事件进行报告。

关于信息安全事件的报告和信息安全事故的管理方面的信息可以参见 ISO/IEC TR18044。

13.1.2 报告安全弱点

控制：

应要求所有的员工、合同方和第三方用户注意并报告系统或服务中已发现或疑似的安全弱点

实施指南：

为了防止信息安全事故的发生，所有员工、合同方和第三方用户应该尽可能将这些事情报告给他们的管理者，或者直接报告给服务供应商。报告机制应该尽可能容易、易理解和方便可用。在任何情况下，他们都无需试图去证明他们怀疑的弱点。

其他信息：

应通知员工、合同方和第三方用户不要试图去证明他们怀疑的安全弱点。测试弱点可以被解释为对系统可能的滥用，可能导致信息系统和服务的损坏，个人进行测试导致法律责任等。

13.2 信息安全事故管理和改进

目标：确保使用持续有效的方法管理信息安全事故

一旦信息安全事件和弱点报告上来，应该立即明确责任，按照规程进行有效处理。应该应用一个连续性的改进过程对信息安全事故进行响应、监视、评估和总体管理。

如果需要证据的话，则应该搜集证据以满足法律的要求。

13.2.1 职责和程序

控制：

应建立管理职责和程序，以快速、有效和有序的响应信息安全事故

实施指南：

除了对信息安全事件和弱点进行报告（见 13.1）外，还应该利用系统的监视、报警和和攻击功能来检测信息安全事故。信息安全事故管理机制应考虑下面的内容：

a） 应该建立机制以处理不同类型的信息安全事故。包括：
   1） 信息系统失败和服务丢失;
   2） 恶意代码（见10.4.1）；
   3） 拒绝服务；
   4） 不完善或不准确的业务数据导致的错误；
   5） 违背机密性和完整性；
   6） 信息系统滥用。

b） 除了正常的意外事故计划（见14.1.3）， 规程应该也包括（也见13.2.2）：
   1） 事故原因的分析和确认；
   2） 遏制事故再发生的策略；
   3） 如果需要，制定计划和实施纠正行动以防止事故再发生；
   4） 同受到事故影响和有关事故恢复的人进行交流；
   5） 向有关的机构报告发生的行为。

c） 收集和保护审计踪迹和类似的证据，在下面的行为中用：
   1） 内部问题分析；
   2） 用作违反合同、法规或民事和刑事案件的司法证据。如计算机滥用和违反数据保护法。
   3） 同软件和服务供应商谈判赔偿时用。

d） 恢复安全破坏和系统失败的行为应该受到仔细和正规的控制。恢复机制应该确保：
   1） 只有明确指定和授权的人才允许访问存活的系统和数据（也见6.2 外部访问）；
   2） 所有采取的处理紧急事件的行为都应该详细记录；
   3） 所有采取的处理紧急事件的行为应该报告给管理部门，依序进行评议；
   4） 应该以最小的延迟确保业务系统的完整性和可控性。

信息安全事故管理的目标同管理是一致的，它应该确保负责信息安全事故管理的人明白在机构内处理信息安全事故具有优先权。

其他信息：

信息安全事故可能超越机构和国家的界限，对这样的事故做出响应，越来越需要同外部的机构进行协作，共享事故的信息，共同做出响应。

13.2.2 从信息安全事故中学习

控制：

应建立能够量化和监控信息安全事故的类型、数量、成本的机制

实施指南：

从对信息安全事故评估中获取的信息应该用来识别再发生的事故和重大影响的事故。

其他信息：

对信息安全事故的评估可以指出需要增加控制来限制事故发生的频率、损失和将来再发生的费用，也可以用在安全方针评审过程中（见 5.1.2）。

13.2.3 收集证据

控制：

事故发生后，应根据相关法律的规定（无论是民法还是刑法）跟踪个人或组织的行动，应收集、保留证据，并以符合法律规定的形式提交

实施指南：

当收集和提交证据是为了在机构约束行为时，应该制定和遵循内部规程。

总的来说，证据规则包括：

a） 证据的可用性：证据是否可在法庭上使用；
b） 证据的份量：证据的质量和完全性。

为了获得证据的可用性，机构应该确保自己的信息系统是遵从任何公开的标准和实用代码来产生可用的证据。

提供证据的份量应该遵从任何可应用的需求。为了达到证据的份量，用来正确一致地保护证据（即处理控制证据）的质量和完整性控制，在从证据被发现的整个时期内，证据的存储和处理应该通过一种强的证据轨迹来描述。一般情况下，那样的强证据轨迹能在下面的条件下建立：

a） 对纸制文档：原物应该带着下面的记录进行安全保存：谁发现了这个文档，文档是在哪被发现的，文档是什么时候被发现的，谁来证明这个发现；任何调查都应确保原物不是伪造的。
b） 对计算机介质上的信息：任何可移动介质的镜像和拷贝（依赖于应用需求）、硬盘和内存中的信息都应该确保其可用性；拷贝处理过程中所有的行为日志都应该保存下来，处理的过程应该有证明；介质的原始数据和日志（如果不可能的话，至少一个镜像文件或拷贝）应该安全保存，不能修改。

任何争论性的工作只允许在拷贝证据材料时进行。所有证据材料的完整性应该得到保

护。证据材料的拷贝应该在可依赖人员的监督下进行，什么时候在什么地方进行的拷贝，谁进行的拷贝，使用了什么工具和程序进行的拷贝，这些都应该做日志。

其他信息：

当一个信息安全事件首次被检测到时，这个事件是否会导致法律行为可能不会是显而易见的。因此，在意识到事故的严重性之前，可能存在必要的证据被故意或意外毁坏的危险。建议在任何预期的法律行为中早早聘请一位律师或警察，他们会给出需要忠告。

证据可能超越机构和司法界限。在那样的情况下，应该授权机构去搜集需要的信息作证据。不同管辖权的证据需求都应该考虑，以使证据能最大化地在不同管辖区域内可用。

14 业务连续性管理

14.1 业务连续性管理的信息安全方面

目标：防止业务活动的中断，保护关键业务流程不会受信息系统重大失效或自然灾害的影响，并确保他们的及时恢复

为通过预防和恢复控制的组合，将对机构的影响减少到最低水平，并能从信息资产的损失中（例如，它们可能是自然灾害、事故、设备故障和故意动作的结果）恢复到可接受的程度，应实现业务连续性管理过程。这个过程需要确定关键的业务过程，需要将业务可连续性的信息安全管理需求同其它可连续性需求如企业动作、员工、材料、运输和设备结合起来。

应对灾难、安全故障、服务丢失和服务可行性的影响当作业务影响进行分析。应制定和实施业务连续性计划，以确保基本操作能及时恢复。信息安全应该是整体业过程和机构内其它管理过程的一个完整的部分。

业务连续性管理应包括标识和减少风险，加上大致的风险评估过程、限制有害事故的影响以及确保业务过程需要的信息能够容易地得到。

14.1.1 在业务连续性管理过程中包含信息安全

控制：

应在组织内开发并保持业务连续性管理过程，该过程阐明了组织的业务连续性对信息安全的要求

实施指南：

这个过程应集合下列业务连续性管理的关键要素：

a) 根据风险的可能性及其影响，推断组织所面临的风险，包括关键业务过程的标识和优先权（见14.1.2）
b) 确定关键业务流程中涉及的所有资产；
c) 推断由信息安全事故引起的业务中断对业务可能产生的影响（重要的是找到处理较小事故以及可能威胁组织生存能力的重大事故的解决办法），并且建立信息处理设施的业务目标；
d) 考虑购买相应的保险，该保险可以形成业务连续性过程的一部分，也作为运行风险管理的一部分；
e) 确定和考虑实施附加的预防和减轻控制。
f) 确定足够的金融的、机构的、技术的和环境资源去满足确定的信息安全需求。
g) 确保人员的安全，保护信息处理设备和机构财产。

h) 正式提出将信息安全需求同商定的业务连续战略一致的业务连续性战略，并将其形成文档(见14.1.3)；

i) 将定期测试和更新适当的计划和过程(见14.1.5)；

j) 确保把业务连续性的管理包含在组织的过程和结构中。业务连续性管理过程的职责应分配给组织范围内的适当级别的管理层（见6.1.1）。

14.1.2 业务连续性和风险评估

控制：

应识别可能导致业务过程中断的事故，以及这类中断发射给您的可能性和影响、中断的信息安全后果

实施指南：

业务连续性的信息安全方面要从标识可能引起机构业务过程中断的事件（一系列事件）开始，例如，设备故障、人为错误、盗窃、火灾、自然灾害和恐怖事件。这之后是风险评估，以确定这些中断发生的概率和影响，根据损坏程度和复原所需时间。

应在业务资源和过程的拥有者全面参与的情况下，进行业务风险评估。这种评估考虑到所有业务过程，并且不局限于信息处理设施，但要包含指定信息安全的结果。重要的是要将不同方面的风险结合起来，得到整个机构业务连续性需求的整体构图。评估应该确认、量化、确认优先级与违背机构原则和目标的风险，这些风险包括重要资源，中断影响，允许中断时间，恢复的优先级。

根据风险评估的结果，应开发业务连续性战略，以确定业务连续性的总体途径。该战略一旦被制定，就应由管理层签署，并制定计划，签署实施战略。

14.1.3 开发并实施包括信息安全的连续性计划

控制：

应开发并实施计划，以确保在关键业务流程中断或失效后能够在要求的时间内和要求的等级上保持和恢复运营并确保信息的可用性

实施指南：

业务连续性计划过程应考虑下列内容：

a） 全部职责和业务连续性规程的标识和协议；

b） 信息和服务可接受损失的标识；

c） 实施规程，以在所要求的时段内恢复和复原业务操作和可用性信息。特别注意对处于适当位置的内部和外部业务相关方和合同的评估；

d） 恢复和复原未完成时应遵循的操作规程；

e） 将已商定的规程和过程形成文档；

f） 用已商定的应急规程和过程（包括危机管理）教育员工；

g） 检验和更新计划。

计划过程应集中于所要求的业务目标，例如，在可接受的时间内恢复为顾客的特定通信服务。应确认业务连续性运行所需要的服务和资源，包括配备人员、非信息处理资源以及信息处理设施可基本维持运行的安排。那些可基本维持运行的安排包括以互惠协议的形式，或者以商业签署服务的形式安排第三方。

业务连续性计划应解决机构的弱点，因而可能包含需要适当保护的敏感信息。业务连续性计划的拷贝应在异地保存，且保存地距离应该足够远，以便主要站点的灾难性破坏不会殃及到它。应制定管理措施，以确保业务连续性计划的拷贝能够及时更新，并对其进行与主站点程序同样的保护。执行连续性计划需要的其它材料也需要在远程保存。

如果使用了一个临时站点，则对临界时站点的安全控制级别应同主站点一致。其他信息：

需要注意的是，危机管理计划与行为可能同业务连续性管理不同，例如正常管理程序可能适应危机的发生。

14.1.4 业务连续性计划框架

控制：

应保持一个单一的业务连续性计划框架，以确保所有计划的一致性，以维护信息安全要求的一致性并识别测试和保持的优先级

实施指南：

每一个业务连续性计划应该说明进行连续性的方法，如确保信息或信息系统安全可行的方法。每个计划也应清晰地规定扩大的计划和计划启动的条件，以及执行该计划每一部分的各个职责。当标识出新的要求时，应相应地修正所建立的应急规程，例如，撤离计划或任何现有的基本维持运行的安排。这些规程应包含在组织变化管理程序中，以确保业务连续性事物能够适当地解决。

每个计划应具有一个特定的责任人。应急规程、人工基本维持运行的计划和重新使用计划应属于相应业务资源或所涉及过程的责任人的职责范围。可替换技术服务，诸如信息处理和通信设施的基本维持运行的安排通常应是该服务提供者的职责。

业务连续性计划框架应该提出确定的信息安全需求，且应考虑下列内容：

a) 在启动每个计划前，启动计划的条件，而该条件描述了要遵循的过程（如何评估这种情况，谁将参与等等）；
b) 描述危及业务操作的事故之后所要采取的动作的应急规程；
c) 描述要采取行动的可依靠的规程，以便将基本业务活动或支持服务移到替代的临时地方，并在要求的时段内使业务过程回到运行状态；
d) 恢复和复原未完成时应遵循的临时操作规程；
e) 描述要采取行动的重新使用规程，以恢复正常业务操作；
f) 规定如何及何时要检验该计划以及维护该计划的过程的安排；
g) 用来创建理解业务连续性过程，并确保过程连续有效的意识和教育活动；
h) 各个人的职责，描述谁负责执行该计划的哪个部分。若要求，可指定可替换的人；

i) 关键的资产和资源能够实行紧急的、维持运行和恢复规程。

14.1.5 BCP 的测试、保持和再评估

控制：

应定期测试并更新 BCP，以确保 BCP 的更新和有效

实施指南：

业务连续性计划的测试应能确保复原队伍中的所有成员和其它有关人员能够知道这个计划，能够明确他们在业务连续性和信息安全中的责任，知道计划启动后他们的角色。

业务连续性计划的检验安排应指出如何和何时应检验该计划的每个部分，计划中的每一个部分都应该经常测试。

应使用各种方法，为该计划在实际寿命中可操作提供保障，这些应包括：

a) 会议检验各种情况（使用中断例子讨论业务恢复安排）；
b) 模拟（特别是按其事故后/危险期管理的角色来培训人们）；
c) 技术恢复检验（确保信息系统可以有效地予以恢复）；
d) 在可替换场地检验恢复（远离主场地，在恢复操作同时运行业务过程）；
e) 供应商设施和服务的检验（确保外部提供的服务和产品将满足合同的承诺）；
f) 完整的演习（组织、人员、设备、设施和过程能否应付中断的检验）。

任何组织可以使用这些方法。 这些方法可以用一种与指定恢复计划相关的方式来使用。需要的话，应该记录测试结果，并采取措施改进计划。

对于每个业务连续性计划的定期评审应分配职责；在业务连续性计划中尚未反映业务安排变更的标识，应按适当的计划更新进行。这种正式的变更控制过程应确保通过整个计划的定期评审来分配和补充已更新的计划。

可能需要更新计划的情况例子包括新设备的采办，或运行系统的升级和以下几方面的变更：

a) 人员；
b) 地址或电话号码；
c) 业务战略；
d) 位置、设备和资源；
e) 法律；
f) 合同商、供应商和关键顾客；
g) 进程或新的/撤销的进程；
h) 风险（运行的和财务的）。

15 符合性

15.1 与法律法规要求的符合性

目标：避免违反法律、法规、规章、合同要求和其他的安全要求

信息系统的设计、运行、使用和管理都要受法律法规要求的限制，以及合同安全要求的限制。特定的法律要求方面的建议应从组织的法律顾问或者合格的法律从业人员处获得。法律要求因国家而异，而且对于在一个国家所产生的信息发送到另一国家（即越境的数据流）的法律要求亦不同。

15.1.1 适用法律法规的识别

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，应加以明白地定义、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和每个人的职责应同样加以定义并形成文档。

15.1.2 知识产权（IPR）

控制：

应实施适当的程序，以确保在使用与知识产权有关的材料和软件时符合法律法规和合同要求

实施指南：

保护具有知识产权的材料时应遵循下面的指南：

a) 发布软件版权符合策略，该策略定义了软件和信息产品的合法使用；
b) 通过大的渠道来获取软件，以确保的不侵犯版权。
c) 维护软件版权和采办策略的意识，并通告对违规人员采取纪律行动的意向；
d) 维护相应资产登记本，确认需要保护产权的所有资产；
e) 维护许可证、主盘、手册等等所有权的证明和证据；
f) 实施控制，以确保不超过所允许的最大用户数目；
g) 进行检验，检验是否仅安装已授权的软件和有许可证的产品；
h) 提供维护相应许可证条件的策略；

i) 提供将软件配备或转移给其他用户机器的策略；

j) 使用合适的审核工具；

k) 遵守从公共网络获得软件和信息的条款和条件;

l) 不从版权不允许的商业录音录像产品中复制、转换和抽取东西。

m) 不从版权不允许的书籍、文章、报告和其它文档中全部或部分拷贝东西。

其他信息：

知识产权包括软件和文档的版权、设计权、商标、专利权和源代码许可证。

通常根据许可协议供应专有软件产品，许可协议指明许可项目和条件，例如限定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。由机构开发的软件的知识产权情况需要同员工澄清。

法律法规的要求和合同的要求可以对专有资料的拷贝施加限制。特别是，该限制可以要求组织只能使用组织自己开发的资料，或者使用开发者对该组织许可的资料，或者使用开发者提供给该组织的资料。版权侵害可能导致司法行为，还可能涉及犯罪。

15.1.3 组织记录的保护

控制：

应按照法律法规、合同和业务要求，保护重要记录免受损失、破坏或伪造篡改

实施指南：

记录应分类为若干记录类型，例如，财务记录、数据库记录、事务日志、审核日志和操作规程，每一种记录都带有详细的保存周期和存储介质的类型，例如，纸记录、缩微胶片、磁介质、光介质。与已加密档案或数字签名（见 12.3）有关的任何相关（密码）密钥应予以保存，以使得记录在保存的时间内能够脱密。

对存储记录的介质的性能下降的可能性应予以考虑。应按照制造商的建议实施存储和处置规程。长期保存的话，可以考虑使用纸和微缩胶片。

若选择了电子存储介质，应建立规程，以确保在整个保存周期能访问数据（介质和格式的可读性），防止由于未来技术变化而引起数据丢失。

数据存储系统应这样选择，使所要求的数据能能在可接受的时间内并以可接受的格式检索出来。

存储和处理系统应确保清晰地标识出记录及法定的保存期。如果该组织不需要这些记录，超过保存期后，应允许恰当的销毁这些记录。

为达到保护记录的目标，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) 应拟定一个保存时间表以标识出基本记录类型以及保存它们的时间。

c) 应维护关键信息来源的目录；

d) 应实施恰当的控制，以防止重要记录和信息被丢失、损坏和篡改。

其他信息：

某些记录可能需要安全地保存，以满足法规或规章的要求，以及支持基本的业务活动。举例来说，这些记录：可以要求作为某个组织在法规和规章规则范围内进行运行的证据，或者用以确保充分防御潜在的民事或刑事诉讼，或者用以证实组织与持股人、合伙人和审核员相对财务状况。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。

15.1.4 个人信息的数据保护和隐私

控制：

应确保按适用的法律法规，适用时，还有合同条款的要求来保护数据和隐私

实施指南：

应该制定和实施组织的数据保护和隐私的策略。这些应该通知到涉及私人信息处理的所有人员。

遵守这些策略和有关的数据保护法律法规需要有合适的管理结构和控制。通常最好由任命个人负责，如数据保护官员完成这件事，该数据保护官员应向管理者、用户和服务提供者提供关于他们各自的职责以及应遵守的特定规程方面的指南。数据拥有者的职责应是处理个人信息，确保认识到相关法律法规所规定的数据保护原则。采取适当的技术和组织措施保护个人信息。

其他信息：

应注意到个人数据（一般来说通过该信息标识出居住的个人的信息）的处理和传输的法律控制。这种控制可以使收集、处理和传播个人信息的人承担责任。

15.1.5 预防信息处理设施的误用

控制：

应禁止用户把信息处理设施用于非授权的目的

实施指南：

管理层应同意使用信息处理设备。在没有管理层批准（见 6.1.4）的情况下，任何出于非业务或未授权目的使用这些设施均应看作不适当使用设施。如果通过监督或其他手段标识出任何非授权的活动，应引起关注相应纪律行动和法律行为的各个管理者的注意。

在实施监督规程之前，应采取合法忠告。

所有用户都要知道允许他们访问的准确范围，知道为检测非授权使用而监视的准确范围。这件事可以这样完成：发给用户授权书，该授权书的副本应由该用户签字，由组织加以安全地保存。应通知组织的雇员和第三方用户除所授权的访问外，不允许任何访问。

登录时，在计算机屏幕上应呈现报警报文，以指示正在进入的系统是不公开的，并且不允许未授权访问。用户必须相应地确认屏幕上的报文，并对其作出适当反应，才能继续登录

过程（见 11.5.1）。

其他信息：

机构的信息处理设备主要或只能用于业务目的。

入侵检测、内容检查和其它监视工具可经用来防止和检测信息处理设备的滥用。

国家拥有防止计算机滥用的法律。对于未授权目的而使用计算机是一种刑事犯法。

监督这种使用的合法性因家而异，并且可以要求将这种监督通知给雇员或者获得他们同意。当进入的系统是用于公众访问的（如公共网络服务），并且是易于安全监控的，消息应该按照所说的进行显示。

15.1.6 密码控制的法律法规

控制：

使用密码控制时，应确保遵守相关的协议、法律法规

实施指南：

为符合相关的合同、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进口和/或出口；
b) 限制设计成使之能增加密码功能的计算机硬件和软件的进口和/或出口；
c) 限制加密的使用；
d) 利用国家的强制或任意的访问方法访问由硬件或软件所加密的信息，以提供内容的保密性。

应征求法律建议，以确保符合国家法律。在把加密的信息或密码技术传到他国之前，要遵循国家有关法律规定，或征询我国法律建议。

15.2 与安全策略和标准的符合性，以及技术符合性

目标：确保系统符合组织安全方针和标准

应定期评审信息系统的安全。

这种评审应根据相应的安全策略和技术平台进行，而对信息系统也应进行审核，看其是否符合安全实施标准和文档安全控制。

15.2.1 符合安全策略和标准

控制：

管理者应确保在其职责范围内的所有安全程序得到了正确实施，以符合安全方针和目标

实施指南：

管理者应对自己职责范围内的信息处理是否符合安全策略、标准和任何其它安全需求进行定期评审。

如果在评审发现任何不符合的情况，管理者应该：

a) 确定不符合的原因；
b) 评估要使这个不符合不再发生需要的行为；
c) 决定和实施适当的纠正行为；
d) 评审纠正行为；

管理者要对评审和为的结果进行记录，这些记录应予以保存。当在他们的职责范围内发生独立评审时，管理员应将结果报告给独立评审人（见 6.1.8）。

其他信息：

系统使用的运行监视在 10.10 中。

15.2.2 技术符合性检查

控制：

应定期检查信息系统与安全实施标准的符合程度

实施指南：

技术符合性检查可以由有经验的系统工程师手动执行（如需要，利用合适的软件工具支持），或者由技术专家用自动化软件包来执行，此软件包可生成供技术专家后续解释的技术报告。

如果使用了渗入测试和脆弱点评估，则应格外小心，因为这些行为可能导致安全系统的泄露。这样的测试应先做好计划，写成文档，且要重复多次。

任何技术符合性检验只能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：

技术性符合检查包括检查操作系统，以确保硬件和软件控制有正确进行。这种类型的检查需要专门的技术专家来进行。

符合性检验还包括几个方面，例如渗入测试，该测试可以通过为此目的专门签约的独立专家来完成。符合性检验可用于检测系统的脆弱点，并用于检验这些控制在防止由于这些脆弱点引起的未授权访问中如何起作用。应当注意渗入测试成功可能导致危及系统的安全以及非故意地产生其他脆弱点的情况。

渗入测试和脆弱点评估提供了系统在指定时间指定状态的简单记录，这个简单记录只限制在实际进行渗入测试时系统的这几个部分中。渗入测试和脆弱点评估不能代替风险评估。

15.3 信息系统审计考虑因素

目标：最大化信息系统审核的有效性，最小化来自/对信息系统审核的影响

为保护审计工具的完整性和防止滥用审计工具，也要求有保护措施。

15.3.1 信息系统审核控制

控制：

应谨慎策划对操作系统检查所涉及的审计要求和活动并获得许可，以最小化对业务过程的影响或风险

实施指南：

应遵守下列事项：

a) 审计要求应与相应管理层商定；
b) 应商定和控制检验范围；
c) 检验应限于软件和数据的只读访问；
d) 对只读以外的访问只允许针对系统文件的单独拷贝。当审计完成时，应擦除这些拷贝，或者审计文档需要保留这些文件，则要给予适当的保护；
e) 应显式地标识和提供执行检验的资源；
f) 应标识和商定特定的或附加的处理要求；
g) 应监视和记录所有访问，以产生参照踪迹；对系统关键数据可以考虑使用时间戳参照踪迹；
h) 有规程、要求和职责应形成文档。
i) 进行审计的人员不能是其它行为的审计人员。

15.3.2 信息系统审核工具的保护

控制：

应限制对信息系统审计工具的访问，以防止可能的误用或损坏

实施指南：

信息系统审计工具（如软件和数据文件）应与开发和运行系统分开，并且不能保存在磁带（程序）库或用户区域内，除非给予合适级别的附加保护。

其他信息：

如果一个审计涉及到第三方，则可能存在审计工具被第三方滥用，信息被第三方组织访问的风险。象 6.2.1（评估风险）和 9.1.2（限制物理访问）中的控制可以考虑用来解决这种

风险，应该采取措施立即改变泄露给审计者的口令。