国际标准 ISO/IEC 17799

第一版 2000－12－01

信息技术－信息安全管理业务规范

参考号：ISO/IEC 17799：2000（E）

目录

目录 3
前言 8
介绍 9
什么是信息安全？ 9
为什么需要信息安全？ 9
如何确定安全需要？ 10
评估安全风险 10
选择控制措施 11
信息安全起点 11
关键的成功因素 12
制订自己的准则 12
1 范围 13
2 名词和定义 13
2.1 信息安全 13
2.2 风险评估 13
2.3 风险管理 13
3 安全策略 14
3.1 信息安全策略 14
3.1.1 信息安全策略文档 14
3.1.2 复查和评价 14
4 组织的安全 15
4.1 信息安全的基本架构 15
4.1.1 管理信息安全论坛 15
4.1.2 信息安全协作 15
4.1.3 信息安全责任的分配 16
4.1.4 信息处理方法的授权过程。 16
4.1.5 专家信息安全建议 17
4.1.6 组织间的合作 17
4.1.7 信息安全的独立检查 17
4.2 第三方访问的安全 17
4.2.1 判断第三方访问的风险 18
4.2.2 第三方合同的安全要求 19
4.3 外部采购 20
4.3.1 外购合同的安全要求 20
5 资产分类和管理 20
5.1 资产的可计量性 20
5.1.1 资产清单 21
5.2 信息分类 21
5.2.1 分类原则 21

5.2.2 信息标识和处理.....22
6 人员安全.....22
6.1 工作定义和外包的安全.....22
6.1.1 把安全包括在工作责任中.....22
6.1.2 人员筛选和策略.....23
6.1.3 保密协议.....23
6.1.4 用工条款.....23
6.2 用户培训.....24
6.2.1 信息安全教育和培训.....24
6.3 对安全事故和故障做出反应.....24
6.3.1 报告安全事故.....24
6.3.2 报告安全缺陷.....24
6.3.3 报告软件故障.....25
6.3.4 吸取事故教训.....25
6.3.5 惩处程序.....25
7 物理的和环境的安全.....25
7.1 安全区域.....25
7.1.1 物理安全界线.....26
7.1.2 物理进入控制.....26
7.1.3 保护办公室、房间和设施.....26
7.1.4 在安全区域工作.....27
7.1.5 隔离的送货和装载区域.....27
7.2 设备安全.....28
7.2.1 设备定位和保护.....28
7.2.2 电力供应.....28
7.2.3 电缆安全.....29
7.2.4 设备维护.....29
7.2.5 外部设备的安全.....29
7.2.6 设备的安全处置或者再利用.....30
7.3 一般性管理措施.....30
7.3.1 清扫桌面和清洁屏幕策略.....30
7.3.2 财产的转移.....31
8 通信和运营管理.....31
8.1 操作过程和责任.....31
8.1.1 记录在案的操作过程.....31
8.1.2 运行变更管理.....31
8.1.3 意外事故管理程序.....32
8.1.4 责任的分离.....32
8.1.5 开发过程和运行过程的分离.....33
8.1.6 外部设施的管理.....33
8.2 系统规划和验收.....34
8.2.1 容量规划.....34
8.2.2 系统验收.....34
8.3 防止恶意软件.....35

8.3.1 防止恶意软件的管理措施.....35
8.4 内务管理.....36
8.4.1 信息备份.....36
8.4.2 操作员日志.....36
8.4.3 事故记录.....37
8.5 网络管理.....37
8.5.1 网络管理措施.....37
8.6 备份介质处理和安全.....38
8.6.1 对可移动的计算机存储介质的管理.....38
8.6.2 存储介质的处置.....38
8.6.3 信息处理程序.....39
8.6.4 系统文件的安全.....39
8.7 信息和软件的交换.....39
8.7.1 信息和软件交换协议.....40
8.7.2 转运时介质的安全.....40
8.7.3 电子商务安全.....40
8.7.4 电子邮件的安全.....41
8.7.5 电子办公系统的安全.....42
8.7.6 公众可访问的系统.....42
8.7.6 信息交换的其它形式.....43
9 访问控制.....43
9.1 访问控制的业务需要.....44
9.1.1 访问控制策略.....44
9.2 用户访问管理.....45
9.2.1 用户注册.....45
9.2.2 特权管理.....45
9.2.3 用户密码管理.....46
9.2.4 用户访问权限的复查.....46
9.3 用户责任.....46
9.3.1 密码使用.....47
9.3.2 无人值守用户设备.....47
9.4 网络访问控制.....48
9.4.1 网络服务的使用策略.....48
9.4.2 强制路径.....48
9.4.3 外部连接的用户认证.....49
9.4.4 节点鉴别.....49
9.4.5 远程诊断接口的保护.....49
9.4.6 网络分离.....50
9.4.7 网络连接管理.....50
9.4.8 网络路径选择控制.....50
9.4.9 网络访问安全.....51
9.5 操作系统访问管理.....51
9.5.1 自动终端识别.....51
9.5.2 终端登录程序.....51

9.5.3 用户识别和鉴定.....52
9.5.4 密码口令管理系统.....52
9.5.5 系统实用程序的使用.....53
9.5.7 终端暂停.....53
9.5.8 连接时间的限制.....54
9.6 应用程序访问控制.....54
9.6.1 信息访问限制.....54
9.6.2 敏感系统的隔离.....55
9.7 检测系统访问和使用.....55
9.7.1 事件记录.....55
9.7.2 检测系统使用.....55
9.7.3 时钟同步.....57
9.8 移动计算和远程工作.....57
9.8.1 移动计算.....57
9.2.8 远程工作.....58
10 系统的开发与维护.....59
10.1 系统的安全需要.....59
10.1.1 安全性要求分析和规范.....59
10.2.1 输入数据的验证.....59
10.2.2 内部作业的管理.....60
10.2.3 文电鉴别.....61
10.2.4 输出数据验证.....61
10.3 密码管理措施.....61
10.3.1 使用密码控制措施的策略.....61
10.3.2 信息加密.....62
10.3.3 数字签名.....62
10.3.4 非拒绝服务.....63
10.3.5 密钥管理.....63
10.4 信息文件的安全.....64
10.4.1 操作软件的控制.....64
10.4.2 系统测试数据的保护.....65
10.4.3 对程序资源库的访问控制.....65
10.5 开发和支持过程中的安全.....65
10.5.1 变更控制程序.....66
10.5.2 操作系统变更的技术复查.....66
10.5.3 改变软件包的限制.....66
10.5.4 隐蔽通道和特洛伊代码（渗透性代码）.....67
10.5.5 外购软件开发.....67
11 业务连续性管理.....67
11.1 业务连续性管理的几个方面.....68
11.1.1 业务连续性管理程序.....68
11.1.2 业务连续性和影响分析.....68
11.1.3 编写和执行连续性计划.....69
11.1.4 业务连续性计划框架.....69

11.1.5 测试、维护和重新评估业务连续性计划 70
12 符合性 71
12.1 符合法律要求 71
12.1.1 适用法律的辨别 71
12.1.2 知识产权(IPR) 71
12.1.3 保护组织记录 72
12.1.4 数据保护和个人信息的保密 73
12.1.5 防止信息处理设备的误用 73
12.1.6 密码管理的规定 74
12.1.7 证据的搜集 74
12.2 安全策略和技术符合性的检查 75
12.2.1 符合安全策略 75
12.2.2 技术符合性检测 75
12.3 系统审查相关事项 76
12.3.1 系统审查管理程序 76
12.3.2 系统审查工具的保护 76
索引 77

前言

ISO(国际标准化组织)和 IEC（国际电工委员会）形成了一个专门体系，进行世界性的标准化工作。 ISO 或 IEC 成员体国家通过各自机构建立的技术委员会参与了国际标准制订和推广，这些技术委员会要设法应对一些特殊领域的技术活动。 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 有联络的国际性组织、政府和非政府机构也参与了这项工作。

国际标准是根据 ISO/IEC 指导方针第 3 部分中的规定起草的。

在信息技术领域，ISO 和 IEC 已经建立了一个联合技术委员会，叫做 ISO/IEC JTC 1. 该联合技术委员会采纳的国际标准草案要经由成员体投票。 若作为国际标准正式出版，则需要至少百分之七十五的成员体投票赞成。

请您注意，该国际标准中的一些内容可能涉及专利权问题。ISO 和 IEC 不负责辨别任何或者所有这样的专利权。

国际标准 ISO/IEC 17799 由英国标准协会筹备起草（BS 7799），随后被联合技术委员会——信息技术 ISO/IEC JTC 1 按照特殊的“ 快速程序 ”所采纳。该标准同时得到了 ISO 和 IEC 各个成员体的批准。

介绍

什么是信息安全？

信息是一种资产，同其他重要的商业资产一样，它对一个组织而言具有一定价值，因而需要适当地保护。信息安全是要在很大的范围内保护信息免受各种威胁，从而确保业务的连续性、减少业务损失并且使投资和商务机会获得最大的回报。

信息可以以多种形式存在。它能被打印或者写在纸上，能够电化存储；也可以由邮局或者用电子方式发送；还可以在电影中展示或者在交谈中提到。无论以任何形式存在，或者以何种方式共享或存储， 信息都应当得到恰当的保护。
在这里，信息安全特指保护：

a） 保密性：确保信息只能够由得到授权的人访问。

b） 完整性：保护信息的正确性和完整性以及信息处理方法。

c） 有效性：保证经授权的用户可以访问到信息。如果需要的话，还能够访问相关资产。

信息安全通过实施一整套的控制达到。这些控制措施可能是策略、做法、程序、组织结构或者软件功能。需要建立这些控制措施以确保实现该机构特殊的安全目标。

为什么需要信息安全？

信息及其辅助程序、系统和网络，是重要的商业资产。信息的保密性、完整性和有效性对于保持竞争能力、资金流动、盈利率、法律柔量和商业形象都十分关键。

各种组织和它们的信息系统及网络日益面临着来自四面八方的安全威胁。 这些威胁的来源有计算机诈骗、间谍活动、蓄意破坏、火灾和水灾等等。 能够损坏信息的因素比如计算机病毒、计算机黑客和拒绝服务，已经越来越常见、越来越富于挑战性并且愈加复杂。

这些组织对信息系统及其服务的依赖，意味着它们更容易受到安全威胁。 公众网络和私有网络的互相链接和信息共享增加了实现访问控制的难度。 分布式计算的趋势已经逐渐削弱了集中化专家控制模式的效率。

很多信息系统的设计并不安全。 通过技术手段可以得到的安全是很有限的，还应当有适当的管理和程序的帮助。 为确认采用何种控制措施，需要进行认真规划而且要关注细节问题。信息安全管理至少要求组织中所有雇员参与其中。 它可能还需要供应商、客户和股东的参与。也可能需要来自组织以外的专家的建议。

如果在需求分析和设计阶段进行合作，信息安全管理的成本就会相当便宜， 而且也会更加有效。

如何确定安全需要？

确定安全需要对一个组织机构来说，是十分关键的。安全需要有三个主要来源。

第一个来源是组织风险的评估。通过风险评估，辨别出对资产的威胁、评价了组织对这种威胁的易损性和威胁发生的可能性，并且对可能的冲击进行了估计。

第二个来源是法律的、规定的和合同约定的要求。这些要求是一个组织、它的贸易伙伴、立约人和服务提供商都要满足的。

第三个来源是一个组织已经制订的特殊原则、目标和需要，它们是用来支持信息处理操作的。

评估安全风险

安全需要是由一个有系统的安全风险评估确定的。 在安全管理上的花费要同安全故障可能造成的商业利益损失相平衡。 风险评估方法可以用于整个组织，也可以只是用于它的某些部分，还可以用在独立的信息系统、特殊系统部件或者服务上。 在此范围内进行风险评估是具有可操作性的、实际的和有帮助的。

风险评估是对下面因素的系统考虑：

a) 安全事故可能造成的商业损失。要把信息和其它资产的保密性、完整性和安全性的损失的潜在后果也考虑进去;
b) 在极为普遍的危害和采取的相应管理措施的共同作用下，这样的故障实际发生的可能性。

评估的结果能够帮助指导和确定适当的管理行为， 并有助于确定管理信息安全风险的优先权和执行抵御这些风险的安全措施的优先级。风险评估和管理措施的选择可能需要重复进行多次，以便保护组织或者独立信息系统的不同部分。

对安全风险和实行的管理措施进行定期复查，是非常重要的。 这样就可以：

a) 考虑到商务需求和优先级的变化；
b) 考虑到新的威胁和危害；
c) 确认所采取的管制仍然有效、适合。

应当根据以前评估，在不同的深度层次进行复查。 而且，还要根据管理所要承受风险的不

同，在变化了的层次上做考查。风险评估常常是先在一个较高的水平进行的，这是一种在高风险领域确定优先级的方式，从而能够在更细致的水平上确定特殊的风险。

选择控制措施

安全需要一旦确定了，就应当选择并实施控制措施，来确保风险降低到可以接受的程度。 控制措施可以从本文件或其它控制措施的资料中选择， 或者从那些制订出的用来满足特殊需要的新控制措施中间选择。 有很多不同的风险管理方式，本文件给出了一些常用方式的例子。然而，有一些方法并不能够适用于每一个信息系统或者环境，并且也可能对所有组织都不合适。注意到这点是十分重要的。例如，8.1.4 阐述了怎样通过划分责任来防止错误和失误的发生。 对于比较小组织就不太可能把所有的责任都做明确划分，必须通过其它途径来达到相同的控制目标。 再比如，9.7 和 12.1 阐述了如何检测系统使用状况以及如何收集证据。其中所提到的控制措施，例如事件记录，可能与现行规范相抵触，比如要对客户或者工作间的私密性进行保护。

管理措施的选择应当根据实施成本与所减少风险的关系和执行成本与出现一个安全漏洞时可能造成损失的关系进行。非资金损失因素，比如声誉损失，也应当考虑进去。

本文件中的一些安全管理措施可以当作信息安全管理的指导性原则，并且适用于大多数组织。下面标题为“ 信息安全起点 ”一节中会更加详细地解释这些措施。

信息安全起点

有一些管理措施可以看作是指导性的原则，它们为实施信息安全提供了一个出发点。这些原则要么基于根本性的立法要求，要么被认为是应对信息安全的常用的好办法。

从法律角度看，对一个组织具有根本性的管理措施包括：

a) 数据保护和个人信息的保密性（见 12.1.4）
b) 组织的档案资料的保护；
c) 知识产权。（见 12.1.2）

被认为对信息安全是常用的好方法的管理措施有：

a) 信息安全策略文件（见 3.1）；
b) 信息安全责任的划分（见 4.1.3）；
c) 信息安全教育和培训（见 6.2.1）；
d) 安全事故报告（见 6.3.1）；
e) 业务连续性管理（见 11.1）.

这些管理措施可以用在大多数的组织和多数环境之中。 应当注意的是，尽管本文件中的所有管理措施都重要，还是应当根据一个组织所面临的特殊风险来确定任何相关的管理措施。因此，尽管上述途径被认为是一个很好的起点，它并不能替代根据风险评估所做出的管理措施的选择。

关键的成功因素

经验表明，要在一个组织内部成功的实现信息安全，下面一些因素常常是非常关键的：

a） 反映业务目标的安全策略、目的和活动；
b） 实现与组织文化相协调的安全的途径；
c） 管理方面明显的支持和承诺；
d） 对安全需要、风险评估和风险管理的清晰理解；
e） 向所有的管理者和雇员有效地传播安全知识；
f） 向所有的雇员和立约人发布信息安全策略和标准的指导；
g） 进行适当的培训和教育；
h） 综合的、平衡的测量系统。 该系统要用于评价在信息安全管理和反馈改进意见中的表现。

制订自己的准则

这个实施规则可以看成是制订组织专门准则的一个起点。 并不是所有在该实施准则中的指导和管理措施都可行。而且，还可能需要其它不包括在该文件中的管理措施。这种情况一旦发生，保持交叉引用很有用处，这将有助于审计人员和业务伙伴进行符合性审计。

信息技术－信息安全管理的业务规范

1 范围

该标准为那些在组织内的负责建立、实现或者维护安全保密性的工作人员提供推行信息安全管理的建议。其目的是为制订组织的安全标准和进行有效的安全管理实践提供公共的基础，并且为组织间的交易建立必要的信任。应当根据适用的法律法规选择使用该标准推荐的内容。

2 名词和定义

本文中使用以下定义：

2.1 信息安全

对信息保密性、完整性和有效性的保护。

保密性：确保信息只能由那些被授权的人访问。

完整性：保护信息的正确性和完整性以及信息的处理方法。

有效性：保证经授权的用户可以访问到信息。 在需要时，还能够访问其它相关资产。

2.2 风险评估

评估对信息和信息处理程序的威胁、冲击和危害，以及这些情况发生的可能性。

2.3 风险管理

在可以接受的成本范围内，识别、控制并减少或者消除可能影响信息系统的安全风险。

3 安全策略

3.1 信息安全策略

目标： 为信息安全提供管理指导和支持。 管理层应当提出一套清晰的策略指导，并且通过在组织内发布和维护信息安全策略来表明对信息安全的支持和承诺。

3.1.1 信息安全策略文档

一部策略文档经管理层批准后被公开发布并以适当的方式传达给所有雇员。 它应当声明管理承诺，并且阐明该组织实现信息安全的途径。该策略文档至少应当包括以下指导性内容：

a) 信息安全的定义，它的总体目标和范围以及安全保密性作为信息共享的许可机制的重要性（参加介绍）
b) 对管理意图、总体信息安全的目标和原理的简单说明。
c) 简短的说明安全策略、原理、标准和对该组织具有特殊重要意义的符合性要求，例如：
    1) 符合法律规定和合同要求；
    2) 安全教育的需求；
    3) 病毒和其它恶意软件的阻止及检测；
    4) 业务连续性管理；
    5) 违反安全管理策略的后果。
d) 定义信息安全管理包括报告安全事故的一般性责任和特殊性责任。
e) 参考可能支持该策略的文献资料，例如针对特殊的信息系统或者用户应当遵守的安全规则的更为详尽的安全策略和程序。

在整个组织中以一种相关的、容易理解的和易于接受的方式，把这一策略方针传达给有意的读者。

3.1.2 复查和评价

应当有一个所有者负责该策略的维护，并根据已经确定的程序对其进行检查。该程序应当确保在影响原始风险评估基础发生任何改变时，都会进行检测。例如，出现了重大安全事故、发现了新的易损性或者有新的组织或技术的基本结构的变更。还应当经常安排有以下内容的定期检查：

a) 策略的效率，由所记录的安全事故的性质、次数和影响来表示；
b) 对业务效率的管理的成本和影响；
c) 技术变革的影响；

4 组织的安全

4.1 信息安全的基本架构

目标：在一个组织内管理信息的安全。

应当建立适当管理架构，在组织内部启动和控制信息安全的实施。
管理层领导应当建立适当的管理问题论坛，以便确认信息安全策略、指派安全角色并在组织中协调安全措施的实施。如果需要的话，应当建立一个信息安全专家建议的资料来源并使其在组织内部是可以利用的。应当加强与外部的信息安全专家的联系，以跟上工业发展趋势、监控安全标准和测评方法并在处理意外安全事故时提供适当的联络点。 应当鼓励发展那些综合了各学科知识的信息安全解决方案，例如此综合解决方案可能涉及经理、用户、管理员、应用程序设计人员、审计人员和安全人员的协调和合作，以及在一些领域的专门技术，比如保险和风险管理。

4.1.1 管理信息安全论坛

信息安全是一项由所有管理层成员共同承担的运营责任。因此应当考虑建立一个管理论坛，以确保从管理上对安全能动性进行明显地支持，而且这种支持有一个清晰的方向。该论坛应当通过适当的承诺责任和足够的资源配置来提高组织内部的安全性。此论坛可以是现有管理机构的一部分。在通常情况下，这样的论坛承担以下责任：

a） 检查并批准信息安全策略和总的责任；
b） 当信息资产暴露在大多数威胁之下时，检测所发生的重要变动；
c） 复查并监测信息安全事故；
d） 支持重要的创新，以加强信息安全。

应当有一个经理负责所有相关活动的安全。

4.1.2 信息安全协作

在一个大型组织中，一个管理层代表们的多功能论坛对于协调处理信息安全策略的执行是十分必要的。这些管理层的代表都来自于组织的相关部门。一般而言，这样的论坛：

a） 批准在整个组织内安全管理的特殊角色和责任。
b） 批准信息安全的特殊方法和程序，例如：风险评估，安全分级系统；
c） 批准并支持整个组织范围内的信息安全能动性，例如安全意识计划。
d） 确保安全性是信息规划过程的一部分。
e） 评价适当性并协调对新系统或者服务的特殊安全管理措施的实施；
f） 检查信息安全事故；
g） 提高在整个组织内对信息安全业务支持的可见性；

4.1.3 信息安全责任的分配

应当清楚地定义保护个人资产的责任和执行特殊安全程序的责任。

信息安全策略（见第 3 句）应当提供在组织中确定安全角色和分配安全责任的一般性指导。如果需要的话，这些指导还应当针对特殊的地点、系统或者范围补充上更为详细的指导。应当清晰界定对个人生命财产和信息资产所承担的局部责任， 也应当明确定义对安全程序比如业务连续性规划所承担的局部责任。

很多的组织会指定一个信息安全负责人，由其总体负责信息安全的发展和实现并管理措施的确定。

然而，资源配置和实现管理措施的责任常常留给单独的管理者。通常的做法是为每项信息资产指派一个所有权人来负责其日常安全。

信息资产的所有权人可以把他们的安全责任委派给单独的管理者或者服务提供商。尽管如此， 所有权人仍然对此资产的安全负有最终的责任，并且所有权人应当能够确定任何错误分配责任的情况。

要清晰地阐明每一个管理者所负责的领域，这一点非常重要。特别是在下述情况发生时：

a） 对于不同种类资产的安全程序和与各自系统相关的安全程序，都应当进行识别并清楚地定义。
b） 负责每项资产或者安全过程的管理者都应当得到批准，而且应当把此项责任的细节记录在案。
c） 应当清楚地定义并记录授权等级；

4.1.4 信息处理方法的授权过程。

应当建立对新的信息处理方法的管理授权过程。
应当考虑以下的措施：

a） 新的信息处理方法应当有相应的客户授权，赞同其目的和用途。还应当获得负责维护当地信息系统安全环境的管理人员的同意，以确保满足所有相关策略和需要。
b） 在需要的时候，应当检测硬件和软件以确保它们和系统的其它组成部分互相兼容。注意：某些连接可能需要定型。
c） 对处理业务信息的个人信息处理程序的使用和任何必需的控制手段都应当经过授权。
d） 在工作场所中使用个人信息处理程序可能导致新的危险，因此应当进行评估和授权。

这些管理措施在网络化的环境中尤其重要。

4.1.5 专家信息安全建议

许多组织可能都需要专家安全建议。理想的状况是，一位有经验的内部信息安全专家可以提供这些建议。并不是所有的组织都愿意雇用一个咨询专家。这种情况下，建议确定一个专门人员来协调内部安全知识和安全经验，以确保处理问题时的连续性并协助做出安全决策。他们还应当能够找到适当的外部咨询专家来提供超出他们经验范围的专业建议。

信息安全建议者或者具有相同作用的接触点应当担负就信息安全的所有方面提供建议的任务。他们要么自己提出建议，要么利用来自外部的建议。他们对安全威胁所做评估的质量和对管理措施的意见决定了该组织的信息安全的效果。为了达到最大的效用、产生最好影响，应当允许他们直接接触整个组织的管理。

应当在预测到可能的安全事故或者漏洞的最早阶段就向信息安全建议者或者具有相同作用的接触点咨询，以便获得专家指导原则和调查资源。尽管正常情况下大多数内部安全调查要按照管理措施执行，仍然可以召集信息安全咨询专家来提出建议、主持或指导此类调查。

4.1.6 组织间的合作

应当保持与执法部门、管理机构、信息服务提供商和电信运营商的适当联络，以确保在发生安全事故时能够及时采取适当措施并能够及时通知。类似的，也应当考虑到与安全组成员和行业协会进行合作。

安全信息的交换应当限制在确保组织的保密信息不会发送给未经授权的个人。

4.1.7 信息安全的独立检查

信息安全策略文献（参见 3.1）宣布了信息安全策略和责任。应当独立地检查其执行情况，以确保组织的实践恰当地反映了这一策略，而且该策略是可行的和有效的。（见 12.2）

可以由内部的审查功能执行这样的检查。 此外，独立的经理或者在此种检测方面有特殊专长的第三方也可以做这种检查。这些候选人要具有检查所必备的技能和经验。

4.2 第三方访问的安全

目标：保护组织信息处理程序的安全和被第三方访问的信息资产的安全。 应当控制第三方对组织信息处理程序的访问。

如果有这样的第三方访问的业务需要，应当进行风险评估以确定安全隐患和管理对策。 所要采取的管理措施应当得到第三方的同意，并在与之签订的合同中加以定义。
第三方访问还可能包括其它的参与者。授予第三方访问权限的协议应当包括准许指定其它具备资格的参与者和相应访问的条件。
这一标准可以作为此类合同的基础，并且也可以作为考虑外购信息处理的基本原则。

4.2.1 判断第三方访问的风险

4.2.1.1 访问的类型

允许第三方使用的访问类型非常重要。例如：通过网络连接进行访问的风险不同于物理访问的风险。应当考虑的访问类型包括：

a） 物理访问，例如：访问办公室、计算机机房和档案柜。
b） 逻辑访问，例如：访问组织的数据库和信息系统。

4.2.1.2 访问的原因

可能出于多种原因授予第三方访问权限。 例如，向组织提供访问的第三方并不在现场，但是可以给以物理访问和逻辑访问的权利，比如：

a) 硬件和软件支持人员， 他们需要访问系统层次或者低层次的应用程序功能。
b) 贸易合作伙伴或者联合经营方， 他们可能交换信息、访问信息系统或者共享数据库。

如果缺乏足够的安全管理，第三方访问信息时就会将其置于危险的境地。若是有与第三方地点建立联络的业务需要，就要进行风险评估，以确定任何特殊管理措施的要求。应当考虑到所需的访问类型、信息的价值、第三方采取的管理措施和这种访问对组织信息的安全所造成的影响。

4.2.1.3 现场承包方

第三方可能按照合同规定在现场驻扎一段时间，这会增加信息系统安全隐患。现场承包方的例子包括：

a） 硬件和软件维护和支持人员。
b） 保洁、看护、安全警卫和其它外包的服务项目承包方。
c） 学生安置和其它临时的短期安排；
d） 咨询人员；

究竟要采取什么措施来管理第三方对信息处理设备的访问，理解这一点十分重要。一般说来，所有的由于第三方访问或者内部管理措施导致的安全要求，都应当反映在与第三方签订的合同中（又见 2.2）。例如，如果对信息的保密性有特殊要求，就应采用不泄露信息协议（见 6.1.3）。

在采取了适当的管理措施和签署了定义有连接或者访问相关条款的合同之前，不应当向第三方提供对信息和信息处理设备的访问。

4.2.2 第三方合同的安全要求

涉及第三方访问组织信息和信息处理设备的有关安排应当建立在一份正式的合同基础上，这一合同应当包括或者涉及所有的安全要求，以求符合组织的安全策略和安全标准。该合同应当保证在组织和第三方之间没有误解。组织应当对供应商做满意的补偿。应当考虑把以下各项条款写入合同中：

a） 总的信息管理策略

b） 资产保护，包括：

1. 保护组织资产的措施方法，包括对信息和软件的保护；
2. 确定资产是否受到什么损害的方法手段，比如确定数据是否丢失或者被修改。
3. 在合同期结束或者合同期中某个协商同意的时间，确保信息或者资产被返回或者销毁。
4. 完整性和有效性；
5. 对于信息复制和信息披露的限制；

c） 对所要采用的每项访问的一个详细描述；

d） 服务的目标水平和无法接受的服务水平；

e） 适当的人员调任的规定；

f） 合同各方各自所应承担的义务；

g） 对相关法律问题所承担的责任，例如，数据保护立法。特别是如果该合同涉及与其它国家中组织的合作，就要考虑不同国家法律体系（又见 12.1）；

h） 知识产权（IPR）和产权责任（见 12.1.2）以及对所有合作项目的保护（见 6.1.3）。

i） 服务控制协议，包括

1. 许可的访问方法、对唯一标识，比如用户 ID 和密码，的管理和使用；
2. 对用户访问和特权的授权程序；
3. 要求保留一份列表，记录得到授权可以使用现有服务的个人、他们的权限与这种使用的关系。

j) 定义可以验证的业绩标准，以及对它们的给监测和报告；

k) 监测和废除用户活动的权力

l)审查合同责任的权利，或者由第三方执行审查；

m) 为问题解决建立一个扩大程序；在适当的地方也应当考虑对偶然性事件的处置。

n) 有关硬件和软件的安装与维护的责任；

o)清晰的报告结构和协商一致的报告格式；

p) 一个清晰的和专门化的变更管理程序；

q) 任何要求的物理保护措施和机制，确保那些管理措施得到落实；

r)对客户和管理员的培训，包括方式方法、处理程序和安全性；

s) 确保能够防范恶意软件的管理措施（见 8.3）；

t）有关安全事故和安全漏洞的报告、通知和调查的安排；

u）分包合同第三方的卷入；

4.3 外包

目标：当信息处理外包给另外一个组织的时候，维护信息的安全性；

在各方签订的合同中，外包安排应当致力于解决信息系统、网络和/或者桌面环境的风险、安全管理和处置程序。

4.3.1 外包合同的安全要求

当组织将其全部的或者部分信息系统、网络和/或者桌面环境的管理控制承包给其它单位时，应当在各方同意的合同中提及相应的安全要求。
例如，此种合同应当包括：

a） 如何满足法律方面的要求，例如数据保护法规；
b） 采取什么样的措施才能够确保外包合同各个签约方包括分包合同签约方都清楚他们的安全责任；
c） 怎样维护和测试组织的业务资产的完整性和保密性；
d） 对授权的用户采取什么物理和逻辑的管理措施来限制和约束对组织的敏感业务信息的访问；
e） 如何在发生灾难性事故时维持服务的有效性；
f） 为外包的设备提供什么层次的物理安全保护；
g） 审查的权力；

还应当考虑把 4.2.2 中给出的条款作为此项合同中的一部分。该合同应当允许在即将得到双方同样的安全管理计划中扩展安全要求和安全管理程序。
尽管外包合同可能引起一些复杂的安全问题，此项操作规范中的管理措施能够作为一个起点，以获得对安全管理计划的架构和内容的认可。

5 资产分类和管理

5.1 资产的可计量性

目标：为组织的资产提供适当的保护。

应当考虑到所有主要的信息资产，并为它们指定所有权人。
资产的可计量性可以帮助确保有适当的维护措施。应当为所有主要财产确定所有权人，并且为维护适当的管理措施而分配责任。可以委派执行这些管理计划的责任。被提名的资产所有者应当保持资产的可计量性。

5.1.1 资产清单

资产清单帮助确保进行了有效的资产保护，并且其它的业务目的，例如出于健康和安全、保险或者金融（资产管理）原因，也可能要用到资产清单。编写资产清单的过程是风险评估的一个重要方面。组织要能够确定其资产、资产的相对价值和这些资产的重要性。根据该信息，组织可以提供与资产价值及其重要性相符的安全保护等级。应当为每个信息系统的重要资产都建立并保有一份资产清单。对于每种资产，都要清楚地进行确认，其所有权和安全等级划分（见 5.2），以及资产目前所处位置（当需要恢复损失和毁坏的信息时，这点就非常重要）都应当得到批准并记录在案。与信息系统密切相关的资产包括：

a） 信息资产：数据库和数据文件、系统文件、用户操作手册、培训材料、操作或执行的程序、连续性计划、撤退安排、归档的信息；
b） 软件资产：应用软件、系统软件、开发工具和设备；
c） 实物资产：计算机设备（处理器、显示器、膝上电脑、调制解调器），通信设备（路由器、专用自动交换分机、传真机、录音电话），磁性存储介质（磁带和磁盘），其它技术设备（电源、空调设备），家具、通融资金；
d） 服务：计算和通信服务、公共服务例如供暖、照明、供电、空气调节。

5.2 信息分类

目标：取保信息资产得到适当程度的保护。

应当将信息分类，指出其安全保护的需要、优先级和保护程度。
不同信息有不同的敏感性和重要性。有的信息资产可能需要额外保护或者特殊处理。应当采用信息分类系统来定义适当的安全保护等级范围，并传达特殊处理措施的需要。

5.2.1 分类原则

信息的分类和相关保护措施应当考虑到信息共享和信息限制的业务需要，还要考虑这些需要对业务的冲击，例如对信息未经授权的访问或者对信息的破坏。一般说来，信息分类是一种确定应当如何处理和保护该信息的简捷方法。

信息和处理分类数据的系统输出应当按照其对于组织的价值和敏感性加以标识。根据信息对组织的关键程度对其进行标识，比如按照其完整性和有效性进行标识，这样做也是可取的。经过一段时间以后，信息常常会变得不再敏感或者重要了，例如在信息公开发布以后。这些方面都应当考虑到。如果把安全保护的分类划定得过高就会导致不必要的业务开支。对于任何信息的分类都不一定自始至终固定不变，可能按照一些预定的策略发生改变。信息分类指南应当预料到这些结论并认可这一实际情况（见 9.1）。
应当考虑分类范畴的数量以及使用这种分类所带来的好处。 过于复杂的分类规划可能很累赘而且使用和执行起来也不经济。解释其它组织发送过来的文件上的标签时应当十分小心，相同或者相似的标签名称可能具有不同的含义。

信息的始发人或指定的所有权人应当承担确定一则信息类别的责任，例如对一份文件、数据记录、数据文件或者磁盘进行分类的责任，以及定期检查这些分类的责任。

5.2.2 信息标识和处理

为信息标识和处理定义一个符合组织所采用分类计划的适当处理程序集合是非常重要的。这些程序要涵盖实物形式和电子形式的信息。对于每种分类，应当定义包含以下信息处理活动的数据处理程序：

a） 复制
b） 存储
c） 通过邮局、传真和电子邮件的信息发送
d） 通过口头语言的信息传递，包括通过移动电话、语音邮件和录音电话传送的信息。
e） 销毁

对于那些含有被划定为敏感或者重要信息的系统，其输出应当带有适当的分类标识。该标识应当反映根据 5.2.1 中规则而建立的分类。 需要考虑的项目包括打印的报告、屏幕显示、存储介质（磁带、磁盘、CD、卡式盒带）、电子消息和文档传输。
一般来说，物理标识是最合适的标识形式。然而，一些信息资产例如电子文档无法加上物理标识，这时可以采用电子标识。

6 人员安全

6.1 工作定义和外包的安全

目标：减少人为失误、盗贼、欺诈或者设备误用所造成的风险。

在招聘时就要提到安全责任的问题，将其包括在合同中，并在雇佣期内监测这种安全责任。应当对应聘人员进行充分的筛选（见 6.2.1）,对敏感的工作尤其如此。所有雇员和使用信息处理设备的第三方都应当签署一份信息保密（不泄露）协议。

6.1.1 把安全包括在工作责任中

应当在适当的地方记录组织安全策略（见 3.1）中所设定的安全角色和安全责任。它们应当包含执行或者维护安全策略的所有总体责任，还包含保护特殊信息资产的专门责任，或者执行特殊安全管理程序或者活动的责任。

6.1.2 人员筛选和策略

在工作申请时应当严格审查长期雇员。包括采取以下措施：

a） 有满意的特征比对，例如一项业务和一个人；

b） 对申请人履历的审查（完整性和准确性）；

c） 对其所宣称的学术和职业资质进行确认；

d） 单独的身份检查（护照或者类似文件）；

当一项工作涉及到能够访问信息处理设备的个人时，无论是最初指派还是后来晋升，组织还应当做专门的信用检查，尤其对于那些处理敏感信息的设备更是如此，比如处理财务信息或者高度机密信息的设备。对于那些处于相当权力岗位的人员应当定期重复进行检查。

对合同签约方和临时雇员也要进行类似的检查。如果这些雇员是通过代理机构提供的，在与代理机构的合同中应当清楚定义该代理方所要承担的筛选责任，以及如果筛选没有完成或者对筛选的结果仍然存有疑虑时代理机构应当遵循的通知程序。

管理层应当评价对有权访问敏感系统的新雇员和没有经验的雇员所做检查监督。所有雇员的工作都要由更高级的雇员做定期检查并遵循一定的批准程序。

管理人员应当清楚他们员工的个人环境会影响到他们的工作。私人问题和财务问题、他们行动或者生活方式的改变、不断出现的消极情绪和精神压力异常，都可能导致欺诈、盗窃、失误或者其它安全隐患。这类信息应当做符合相关法规的处理。

6.1.3 保密协议

保密协议或者不泄露协议用于提醒人们注意该信息是保密的。通常情况下，雇员应当签署这样的协议以作为雇佣他们起码条件和要求。

授权尚未受合同（包含保密协议）约束的临时职员和第三方使用信息处理设备之前，还应当要求他们签订一份保密协议。

当用工合同或者协议发生变动时还要对保密协议进行检查，尤其是雇员要离开该组织或者合同即将接受的时候。

6.1.4 用工条款

用工合同条款应当阐明雇员对于信息安全所负的责任。适当的时候，在雇佣期结束后的一段确定时期内仍然要承担这种责任。其中包括如果雇员不遵守安全要求时组织所要采取的行动。

在用工合同条款中应当包括并清楚界定员工的法律责任和权利，例如：涉及到的版权法或者数据保护法规方面的责任和权利。还包括员工信息的分类和管理责任。只要情况适当，用工合同中就应当清楚阐明这些责任要延伸到组织规定范围之外并拓展到正常的工作时间之外，例如在家工作时就要考虑这些问题（又见 7.2.5 和 9.8.1）。

6.2 用户培训

目标：确保用户清楚信息安全威胁和利害关系。使用户准备好在正常工作过程中能够支持组织的安全策略。

应当在安全程序中、在信息处理设备的正确使用过程中培训用户，以降低可能的安全风险。

6.2.1 信息安全教育和培训

组织的所有雇员和相关的第三方用户都应当接受适当的培训并定期向它们传达组织更新的策略和程序。这包括安全要求，法律责任和业务管理措施，以及在授权访问信息和使用服务之前所要接受的正确使用信息处理程序的培训，例如：登录程序、软件包的使用等。

6.3 对安全事故和故障做出反应

目标：把安全事故和安全故障的损失降到最低程度，监测这些事故并从中吸取教训。

对于影响安全的事故，应当通过适当的管理途径尽快报告。
所有的雇员和签约人应当清楚报告不同类型的事故（安全漏洞、安全威胁、弱点或者故障）的程序，这些事故可能对组织资产的安全构成威胁。应当要求他们把所发现的或者预测的任何事故尽快向合同中指定的地点报告。组织应当建立一个正式的处罚制度，以处理那些造成安全漏洞的职员。为了恰当地对事故做出处理，要在事故发生之后迅速地收集证据，这一点非常重要。

6.3.1 报告安全事故

应当尽可能快速地通过适当管理渠道报告安全事故。
应当建立起正式的报告程序，还应当建立事故反应机制，以便设定在接到事故报告时所应当采取的措施。应当让所有的雇员和签约人都明白报告安全事故的程序，还应当要求他们尽快报告。应当实行适当的反馈机制，确保在处理完事故之后能够知道所报告事故的处理结果。可以用这些事故来训练用户的安全意识（见 6.2），使他们了解发生了什么情况、对这种情况怎样做出反应并且将来如何避免这些事故（见 12.1.7）。

6.3.2 报告安全缺陷

应当要求信息服务的用户注意并报告任何观察到或者预测到的系统或者服务的弱点、或者是对系统或服务的威胁。他们应当尽快向他们的管理层或者服务供应商报告此类事件。应当通

知用户，无论在任何情况下，都不要试图去证实可疑缺陷。这是出于对他们自身的保护，因为测试系统缺陷的行为可能被当作对系统的潜在所误用。

6.3.3 报告软件故障

应当建立报告软件故障的程序。应当考虑采取以下的措施：

a） 应当记录出现问题的特征和出现在屏幕上的任何信息；

b） 如果可能的话，应当将计算机隔离并停止使用。应当立即变更所用的连接。如果要检测机器，还应当在重新启动之前断开与组织中其它网络的连接。其磁盘不应当用在其它计算机上。

c） 应当立即把该事件向信息安全管理人员报告。

除非得到授权，否则用户不能试图删除可疑软件。应当由受过适当训练的有经验的人员做恢复工作。

6.3.4 吸取事故教训

应当有相应的机制来量化并监测事故和故障的类型、大小和造成的损失。这些信息可以用来确认再次发生的事故或者故障及其造成的冲击。这些信息显示出对强化和附加管理措施的需求程度。可以用这些管理措施来限制未来发生事故的频率、事故造成的损失和破坏，或者将其放入安全策略复查过程(见 3.1.2)。

6.3.5 惩处程序

对那些违反组织安全管理政策和程序的雇员（见 6.1.4, 在 12.1.7 中有关于证据保留期的内容），应当有一个正式的惩戒手段。这样的管理程序可以作为对那些易于忽视安全程序人员的警示。另外，应当确保对怀疑犯下严重或者持续安全错误的雇员做出正确的、公平的处理。

7 物理的和环境的安全

7.1 安全区域

目标：防止未经授权的访问，预防对业务基础和业务信息的破坏以及干扰。

应当把关键的和敏感的业务信息处理设备放在安全区域，受到确定的安全范围的保护，并有适当的安全屏障和接入控制。应当对他们从实体上加以保护，以防未经授权的访问并免于干扰和破坏。

所提供的保护应当与确认的风险向适应。推荐使用清楚桌面和清晰屏幕的策略，以减少未经授权情况下访问文件、存储介质和信息处理设备或者它们造成破坏的风险。

7.1.1 物理安全界线

通过在业务基础和信息处理设备的周围设立多个实体的安全屏障，可以实现对它们实体上的保护。每一个安全屏障建立了一个安全界线来保护含有信息处理设备的区域（见 7.1.3）。安全界线是指这样以下东西：它们建立了某种屏障，例如墙、要刷卡出入的大门或者人工接待前台。每种屏障的位置和保护力度取决于风险评估的结果。

适当的时候，应当考虑并执行以下的原则和管理措施：

a） 应当清楚定义安全范围；

b） 含有信息处理设备的建筑物或者场所的周边应当受到妥善保护（例如，在该安全范围和易于被闯入的区域之间不应当有明显缺口）。该场所的外墙应当建筑得十分坚固，所有入口都应当加以适当保护以防未经授权的访问，例如采用适当管理机制、障碍物、警报器、锁等等。

c） 应当有人工值守的接待区域或者其它措施控制对这些地点或者建筑的访问。应当把对这些地点或者建筑的访问限制在经过授权的人员之内。

d） 如果需要的话，应当把物理保护扩展到从地板到天花板的范围，以便防止未经授权的访问和环境污染，例如由火灾或者水灾引起的破坏。

e） 安全范围以内的所有门窗入口都应当设立警报器并把它们关严。

7.1.2 物理进入控制

应当通过适当进入管理措施保护安全区域，确保只有得到授权的用户才能访问。应当考虑以下的管理措施：

a） 应当监视进入安全区域的访问者或者将其带离安全区域，而且要把他们进入和离开的时间记录在案。只应当授权他们进行出于特殊的、得到批准的目的的访问。还应当向他们传达该安全区域的安全要求和紧急处理程序。

b） 应当控制对敏感信息和信息处理程序的访问，并只将其限制在得到授权的个人。应当使用认证管理，例如：swipe 卡和个人身份号码，对所有访问进行授权和验证。应当安全地保持对所有访问的审查跟踪。

c） 应当要求所有人员佩戴某种形式的可见标识，并鼓励他们盘查没有护送人员的陌生人和任何没有佩戴明显标识的人员。

d） 应当定期检查和更新对安全区域的访问权限。

7.1.3 保护办公室、房间和设施

安全区域可能是一个锁着的办公室或者在物理保护范围内的多个房间，这些房间可能锁着或者其中有上锁的橱柜或保险箱。安全区域的选择和设计应当考虑到防止可能发生的火灾、水灾、爆炸、民众动乱和其它形式的自然或人为灾难。还应当考虑到相关的健康和安全规范和标准。 应当考虑任何邻近房屋的所带来的安全风险，比如其它地方的渗水。

应当考虑以下管理措施：

a） 关键设备应当安置在避免公众访问的地方；
b） 建筑物应当那么不显眼，只有最低限度地指出其用途。没有明显标记，建筑内外也没有明显地指出里面正在进行信息处理活动。
c） 支持功能和设备例如复印机、传真机应当适当地放置在安全区域内以避免有人要求使用，因为那样会损坏信息。
d） 无人值守时门窗应当上锁，对门窗应当进行外部保护，尤其是对靠近地面的门窗。
e） 按照专业标准安装上适当的入侵者侦测系统并进行定期测试， 该系统应当保护所有可以通过的门窗入口。应当全时监测没有使用的区域。还应当提供对其它地区的保护，例如计算机房或者通讯设备间。
f） 应当把组织管理的信息处理设施与第三方管理的其它设备从实体上隔离开。
g） 不应当让公众很容易得知晓能够确定敏感信息处理设备位置的电话本和内部通讯录。
h） 应当把危险或者易燃材料安全地存放在距安全区域有一定距离的地方。除非有相应的要求，否则不应当把大量储备资料比如文件纸张存放在安全区域内。
i） 应当把回撤的设备和备份存储介质放置在一定安全距离以外，以免主要基地发生的灾难性事故对其造成破坏。

7.1.4 在安全区域工作

可能需要额外的管理措施和指导原则来加强安全区域的安全性。这些措施包括对在安全区域工作的人员和第三方的管理，还包括对在该地区发生的第三方活动的管理。应当考虑以下管理措施。

a) 工作人员只应当知道需要他们了解的有关安全区域的存在或者其中活动的信息。
b) 出于安全原因和为了防止给恶意活动以可乘之机，应当避免在安全区域内进行不是监督的工作。
c) 应当对空的安全区域加以物理上的保护并进行定期检查。
d) 只是在需要的时候，才授予第三方支持服务人员受严格限制的访问安全区域和敏感信息处理设备的权利。这些访问应当得到授权并对其进行监测。安全界线内部不同安全要求的区域之间可能需要建立附加屏障和界线以便控制实体接触。
e) 除非得到授权，否则不允许使用摄影、录像、录音或其它记录设备。

7.1.5 隔离的送货和装载区域

应当对交货和装货区域进行管理，如果可能的话，要把它们与信息处理设备隔离开以避免未经授权的接触。应当通过风险评估来决定此种区域的安全要求。应当考虑以下的安全措施。

a) 从建筑物外面访问一个物资储存区域时，应当将其限制在经过确认和授权的人员之内。
b) 该物资存储区域的设计应当使得送货人员能够在不必进入建筑物其它部分的情况下卸下供应物资。
c) 当物资存储区域内部通道打开的时候，应当保护外部通道。
d) 在把送来的物资从存放地点运送到使用场所之前，应当对其进行检查，看是否有潜在风险（见 7.2.1d）。
e) 如果合适的话，应当在物资存储区域的入口对送来的物资进行登记。

7.2 设备安全

目标：防止资产流失、被损坏或者破坏，防止对业务活动的破坏。

应当对设备加以实体上的保护，使其免于安全风险和环境灾难。
为减少对数据未经授权访问所造成的危险并保护其免受损失或破坏，设备保护（包括所用的外部设备）是十分必要的。这还应当包括设备的安置和处理。为防止未经授权的访问、保护其免受灾难性事故的毁坏和保护辅助设备例如电力供应设备和电缆基本架构，可能要采用一些专门管理措施。

7.2.1 设备定位和保护

应当妥善安置或保护设备，以降低环境威胁和灾难的风险、减少未经授权的访问的机会。应考虑以下管理措施：

a） 妥善安置设备，把对工作区不必要的访问降低到最低限度。
b） 处理敏感数据的信息处理和存储设备应当妥善放置以减少其使用期间忽视对其监督的风险。
c） 应当把需要特殊保护的物品隔离开，以降低所用保护等级。
d） 应当采取措施降低潜在风险，包括：
    a) 盗窃；
    b) 火灾；
    c) 爆炸
    d) 吸烟；
    e) 水灾（或者供水终端）
    f) 尘土；
    g) 振动；
    h) 化学效应；
    i) 电力供应中断；
    j) 电磁辐射；
e） 组织应当考虑对在信息处理设施附近就餐、饮水和吸烟的政策规定。
f） 应当监测那些可能对信息处理设备有负面影响的环境条件；
g） 应当为工业化环境中的设备而采用专门的保护方法，比如键盘保护膜。
h） 应当考虑到在房屋附近发生灾难所产生的影响，例如邻近建筑物的火灾、屋顶或者地表的渗水或者街道上发生的爆炸。

7.2.2 电力供应

应当对设备加以保护使其免于电力中断或者其它电力异常的影响。应当提供符合设备制造商要求的适宜电力供应。

为实现电力供应的连续性，所应采取的措施包括：

a） 有多路供电途径以避免单点电力供应发生故障的危险；

b） 不间断电源（UPS）；
c） 备用发电机。

对于辅助关键业务运营的设备推荐使用不间断电源（UPS）以支持有序的断电或者继续运行。突发事件处理计划应当包括在不间断电源发生故障时所要采取的措施。 应当定期检查 UPS 设备，确保其有足够能力并按照制造商的建议对其进行测试。

如果长期停电的情况下还有继续处理信息，就需要考虑备用发电机。发电机安装上以后，应当按照制造商的指导对其做定期检测。应当有充足的燃料可供利用，以确保长期停电时发电机仍然能够运行。

另外，应当把应急电力开关安放在设备间的紧急出口处，以便于在发生紧急事故时迅速关掉电源开关。主要电力系统出现故障时应当提供应急照明。应当对所有建筑物提供照明保护，并且应当为所有外部通信线路安装照明保护滤光器。

7.2.3 电缆安全

应当保护传输数据和辅助信息服务的电缆和通讯线路，使其免于截取或者破坏。应当考虑采取以下的管理措施。

a) 应当把连接到信息处理设备的电缆和通讯线路埋入地下。在可能的地方，还要给予足够的选择性保护；
b) 应当保护网络连线，防止被未经授权地截听或者被毁坏。例如可以使用专门管线或者避免线路通过公共地带。
c) 应当把供电线路与通讯线路隔离开，以防相互干扰；
d) 对于敏感或关键系统，还应当考虑采取进一步的管理措施，包括：
    a) 在观测点和终点安装包皮的管线并将房间或者箱子上锁；
    b) 使用替代的路径选择或者信息传送媒介；
    c) 使用光纤；
    d) 开始清除那些连接到线路上的未经授权的设备。

7.2.4 设备维护

设备应当得到正确的维护，以确保其持续有效性和完整性。应当考虑以下管理措施：

a） 应当按照设备制造商推荐的维护间隔和规定对设备进行维护；
b） 只有得到授权的维护人员才能够对设备进行维修和保养；
c） 应当把所有可疑故障和实际发生的事故记录下来，还应当记录下所有的预防性措施和矫正维护；
d） 把设备运到工作地点以外的地方进行维修的时候，应当采取适当措施（又见 7.2.6, 其中有关于删除、擦写和覆盖数据的内容）。应当遵守所有保险政策的强制要求。

7.2.5 外部设备的安全

无论所有权归谁，任何在组织外部使用的信息处理设备都应当得到管理层的授权。提供的安

全保护措施应当等同与组织内部用于相同目的的设备所受到保护，还要考虑到在组织房产之外工作的风险。信息处理设备包括所有形式的个人电脑、组织者、移动电话、纸张或者其它形式，它们用于在家工作或者被人从正常工作场所运走。应当考虑以下指导性原则。

a) 从房屋中搬走的设备和存储介质不应当放在公共场所而无人看守。在旅行的时候，应当把便携式电脑掩饰为手提箱携带。
b) 任何时候都要遵循制造商所提供的设备保护指导，例如保护设备免受强电磁场的危害。
c) 应当由风险评估来确定对在家工作的管理措施，应当实行适当的管理控制，例如：可上锁的文件柜、清洁桌面计划和对计算机的访问控制。
d) 应当有足够的保险覆盖面来保护基地以外的设备。

安全风险比如被盗、被毁和被窃听的风险，随地点不同可能有很大变化。在采取最佳保护措施的时候应当考虑到这一点。关于保护移动设备的其它更多信息可以在 9.8.1 节找到。

7.2.6 设备的安全处置或者再利用

对设备不经意的处置和重复使用可能会损害信息（又见 8.6.4）。存有敏感信息的存储介质应当从实体上加以销毁，或者是安全地加以覆盖而不只是使用标准的删除程序。

所有设备，包括存储介质例如固定硬盘，应当加以检测，以确保在处置之前将所有敏感数据和许可软件都被抹掉或者覆盖掉。毁坏了的存有敏感信息的设备需要进行风险评估，以确定应当销毁、维修或是丢弃该物。

7.3 一般性管理措施

目标：防止对信息和信息处理设备的损坏和盗窃。 应当保护信息和信息处理设备，避免把它们暴露给未经授权的个人或者被他们修改或盗走。 应当有管理措施来降低损失或者风险。 在 8.6.3 中应当考虑处理和存储程序。

7.3.1 清洁桌面和清洁屏幕策略

组织应当考虑采用一项清洁桌面计划，以整理纸张和可移动的存储介质。在正常工作时间内和工作时间外，为了降低对信息未经授权的访问所造成的损失和对信息的毁坏，还应当考虑为信息处理设备采用一项清洁屏幕计划。该策略考虑到信息安全分类（见 5.2）、相应的风险和企业文化方面。

放在桌面上的信息也可能在灾害中被损坏，比如被火灾、水灾或者爆炸所毁坏。

应当考虑以下管理措施：

a） 如果合适的话，应当把不用的纸张和计算机存储介质存放在适当的可以锁上的柜橱和/或其它有安全保护的存放设施中，特别是在工作时间之外更应如此。

b） 如果不用的话，应当把敏感或者关键的业务信息锁上（放在放火的保险柜或者柜子里就很理想）。离开办公室时尤其要注意这点。
c） 无人看守的时候，不应当把个人计算机和计算机终端以及打印机置于登录状态，而在不用的时候应当拿密码锁、命令和其它措施加以保护。
d） 应当保护引入和流出邮件存放点、无人值守的传真机和专线电报设备。
e） 在工作时间以外应当把复印机锁上（或者以其它方式保护它免受未经授权的访问）。
f） 敏感或者分类信息打印出来以后应当立即把它从打印机中清除。

7.3.2 财产的转移

在没有授权的情况下，不应当把设备、信息或者软件转移到工作场所以外。如果确实有必要将其移走，搬出设备时和归还设备时都要做登记。应当进行当场检查以发现未经授权的财产转移。进行现场检查时应当让员工知道。

8 通信和运营管理

8.1 操作过程和责任

目标：确保信息处理设备的正确安全运行。

应当确立信息处理设备的管理和操作责任和程序。其中包括建立操作指南和事故处理程序。如果合适的话，应当进行责任分离（见 8.1.4）,以减小粗心大意或者精心策划的系统错用。

8.1.1 记录在案的操作过程

应当把安全策略确立的操作程序记录在案并加以保存。应当把操作程序作为正式的文档，对它的改动应当得到管理层的授权。
这些程序应当详细说明具体执行每项工作时的做法，包括
a） 信息处理和处置；
b） 进程安排的要求，包括与其它系统的相对独立、早期工作启动和后期工作结束；
c） 处理错误或者其它异常情况的操作指导，包括对系统设施的使用限制（见 9.5）。这些异常情况可能在工作进行过程中遇到。
d） 出现意料之外的运行困难或者技术难题时建立辅助连接；
e） 在系统发生故障时要用的系统重启和恢复过程。

8.1.2 运行变更管理

应当控制对信息处理设备和系统的变更。对信息处理设备和系统改变的管理不够是信息故障或者安全事故的常见诱因。应当有正式的管理责任和程序，确保对设备、软件和程序做的所有变更都得到满意管理。运行程序应当受到严格的变更管理的控制。当程序改变时，应当保

留一份记录所有相关信息的审查日志。对操作环境所做变动可能影响到应用程序。只要是可行的话，就应当把运行和应用程序变更管理措施结合在一起（又见 10.5.1）。特别应当考虑以下措施：

a） 识别并记录重大变更；
b） 对此类变更潜在影响的评估；
c） 拟议中变更的正式批准手续；
d） 把变更的所有细节通知相关人士；
e） 能够确定从失败的变更中进行恢复时所承担责任的方法；

8.1.3 意外事故管理程序

应当建立意外事故处理责任和相应程序，以确保对安全事故做出迅速、有效和有条理的反应（又见 6.3.1）。应当考虑以下的管理措施：

a) 应当建立起覆盖所有可能的安全事故类型的处理程序，包括：
    1. 信息系统故障和服务损失；
    2. 拒绝服务；
    3. 不完整或者不准确的业务数据导致的错误；
    4. 保密性漏洞；
b) 除了正常的紧急事件处理计划（用于尽快恢复系统或者服务）之外，此项管理程序还应当包括：
    1. 分析和辨认事故原因；
    2. 如果需要的话，要规划并执行补救措施以防再次发生；
    3. 收集审查追踪记录和类似的证据；
    4. 和其它受到事故影响以及与此事故有关的人员进行沟通；
    5. 把相应的行动向适当的负责人员汇报。
c) 适当的时候，应当收集并保护审查追踪和类似的证据（见 12.1.7）。这样是为了 ：
    1. 内部问题分析；
    2. 将其用做证据证明潜在的违反合同行为、违反规定的行为或者触犯民法或刑法的行为，例如违反了有关计算机误用或数据保护相关法规。
    3. 同软件或者服务供应商进行谈判，以获得赔偿。
d) 应当认真仔细地管理修补安全漏洞和解决系统故障时采取的措施。此项措施应当确保：
    1. 只允许得到明确识别和授权的人员访问正在使用中的系统和数据（又见 4.2.2，其中涉及第三方访问）；
    2. 采取的所有紧急事故处理行为都详细地记录在案；
    3. 应当有序地把紧急事故处理行动汇报给管理层，并由他们进行复查；
    4. 以最快的速度确认业务系统和管理措施的完整性；

8.1.4 责任的分离

责任分离是一种降低偶然或者蓄意系统误用风险的方法。应当考虑把某些责任或者责任区的管理或者执行加以分离，减少对系统或者服务未经授权的访问或者改动的机会。

较小的组织可能发现这些措施难于执行，但是应当尽可能实践和利用这一指导原则。如果难于把责任分离，应当考虑采取其它的管理措施，例如：活动监测、审查追踪和管理层监督。安全审查要保持独立，这点非常重要。

应当小心注意的是，没有哪个人能够单独责任区使用欺诈手段而不被发现。应当把事情的启动和授权分开。应当考虑采取以下管理措施。

a) 应当把那些需要勾结在一起才能进行欺诈的活动分离开，例如：建立采购清单并确认已经收到货物了。这一点十分重要。
b) 如果有相互勾结的危险，就应当采取措施对两个或者更多的人进行管理，从而降低共谋的危险。

8.1.5 开发过程和运行过程的分离

应当将开发、测试和运行过程分开，这对实现相关角色的分离很重要。应当定义软件从开发到运行的状态转变要遵守的规则，并将其记录在案。

开发和测试行为可能引起严重的问题，例如，对文档或者系统环境的有害的改动，或者对系统故障弄巧成拙的处理。在运行环境、测试环境和开发环境之间进行分离时，应当考虑分离的层次。这种分离对于防止出现运行问题是必要的。另外，还应当在开发和测试功能之间做类似的划分。在这种情况下，需要保持一个已知的稳定环境，可以在其中运行有防范功能的测试程序，以防止不适当的开发人员访问。

在开发和测试人员可以访问操作系统及其信息的地方，他们可能会引入未经授权和未经测试的程序编码或者改变运行数据。在某些系统中，这种可能性会被滥用于欺诈或者引入未经授权的或恶意的代码。未经授权的或恶意的代码能够导致严重的运行问题。开发人员和测试人员本身也对操作信息的保密性构成了威胁。

如果开发和测试共享同一个计算机系统，可能在不经意间改动了软件和信息。因此，为了降低因操作软件和业务数据的意外改变或者未经授权的访问而造成的风险，建立分立的开发、测试和运行机制是个理想的解决方案。为此，应当考虑以下的管理措施。

a) 可能的话，开发和运营软件应当在不同的计算机处理器上运行或者在不同的域或目录下运行。
b) 应当尽可能的将开发和测试活动分开。
c) 如果不要求，不应当从操作系统中访问到编译器、编辑器和其它的系统工具。
d) 对操作系统和测试系统应当使用不同的登录程序以减小发生错误的风险。应当鼓励用户对这些系统使用不同的密码，并且菜单应当显示适当的身份信息。
e) 开发人员只应当有运行密码，其中管理措施负责为支持操作系统而发布密码。管理措施应当确保密码在使用后做改变。

8.1.6 外部设施的管理

如果使用外部签约方来管理信息处理过程，那么就可能导致潜在的安全漏洞，例如可能危及、

损坏或者丢失在签约方当地的数据。应当事先确定这些风险。而且，所要采取的适当对策也应当得到签约人的同意，并将其写入合同中（有关访问组织设施和外购合同的第三方协议的指导原则，参见 4.2.2 和 4.3）

应当提到的特殊议题包括：

a） 识别出那些在内部能够得到更好保存的敏感或关键应用程序；
b） 取得业务应用软件所有权人的许可；
c） 业务连续性计划的含义；
d） 专门化的安全标准和测量符合性的程序
e） 分配专门的责任和程序，以有效地监督所有相关的安全活动。
f） 报告和处理意外安全事故的责任和过程。（见 8.13）

8.2 系统规划和验收

目标：将系统故障的风险降低到最小。 为确保有足够的容量和资源可供利用，需要有先进的规划和准备工作。 应当预测未来容量需求，以减少信息超载的风险。 在新系统验收和使用前，应当确定它们的运行需要，并对其做记录和检测。

8.2.1 容量规划

为了确保有足够的处理能力和存储空间可供利用，应当监测系统容量需要并对未来的容量需求做出预测。这些预测中应当考虑到新的业务需求和系统需求、该组织当前的和预测的信息处理趋势。

需要特别关注主机，因为对主机而言征购新容量要更多的资金和时间。主机服务器的管理员应当负责监视关键系统资源的使用，包括处理器、主存储器、文件存储器、打印机和其它输出设备以及通信系统。他们应当判别容量使用的趋势，特别是系统容量与业务应用程序或者管理信息系统工具的关系。

管理员应当利用这些信息去识别和避免可能出现的危及系统安全或用户服务的瓶颈，并制订出得当的补救措施。

8.2.2 系统验收

应当建立新信息系统、系统升级和新版本的验收标准，并在验收之前做适当的系统测试。 管理员应当确保新系统的验收标准和要求得到了清楚地定义、记录和测试。应当考虑以下的管理措施：

a） 性能和计算机容量需求；
b） 错误恢复和重新启动程序，还有意外事故处理计划。
c） 按照已定标准的例行操作程序进行测试和准备。
d） 经批准的适当安全管理措施。
e） 有效的人工操作程序
f） 业务连续性安排，如 11.1 所要求的那样。
g） 找到证据证明新系统的安装不会对现有系统有负面影响，尤其是在高峰处理时段，例如月末；
h） 找到证据证明已经考虑到新系统对该组织整体安全性的影响。
i） 新系统的操作或使用培训。

对于重大的新开发，应当在开发过程的所有阶段都考虑操作功能并向用户咨询，以确保拟建系统的运行效率。应当做适当的检测，确认所有的验收条款都得到充分满足。

8.3 防止恶意软件

目标：保护软件和信息的完整性

需要小心提防，以阻止和发现恶意软件的引入。
软件和信息处理设施容易受到入侵恶意软件的危害，例如计算机病毒、网络蠕虫、特洛伊木马（Trojan horses）（参见 10.5.4）和逻辑炸弹。用户应当知晓未经授权软件或者恶意软件的危害。适当的时候，管理员应当采取专门的控制措施来发现和阻止恶意软件的引入。尤其要注意，在个人计算机上发现和阻止计算机病毒是根本性的办法。

8.3.1 防止恶意软件的管理措施

为防止恶意软件，应当采取一定的检测和预防措施，并启动适当的用户知情程序。对恶意软件的预防应当基于安全意识、适当的系统访问和变化管理措施。应当考虑以下的管理措施：

a） 一个正式的安全策略，该安全策略要符合软件许可证并且禁止使用未经授权软件。
b） 一个正式的预防风险的策略。无论文档和软件是从外部网络获得的，或者通过外部网络获得的，又或者是在任何其它媒体上得到的， 策略中的这些风险都与其密切相关。而该策略指出了应当采取怎样的预防措施（参见 10.5, 特别是 10.5.4 和 10.5.5）。
c） 安装并定期升级防病毒的检测软件和修复软件。用它们扫描计算机和存储介质，这可以作为一种预防控制手段或者作为一种例行程序。
d） 指导对于支持关键业务程序的系统中数据内容和软件的检查。无论出现任何未经验收的文件或者未经授权的修改，都要进行正式调查。
e） 对于任何在来源不明或者未经授权的电子媒介上的文件，或者从未受置信的网络上收到的文件，都需要在使用之前检查病毒。
f） 在使用之前，检测所有电子邮件的附件和下载材料。这种检测可以在不同地点进行，例如：在电子邮件服务器上、桌面电脑上或者在进入组织的网络时。
g） 系统上负责病毒防护的管理程序和责任、在程序使用方面的培训、病毒袭击的报告

和遭受袭击后的恢复（见 6.3 和 8.1.3）

h） 为从病毒袭击中恢复，需要采用适当的业务连续性计划。它包括所有必要的数据和软件备份以及恢复安排（参见第一句）。

i） 要考虑使用这样的程序：它能够验证所有与恶意软件相关的信息并且确保警报公告的内容准确翔实。管理员应当确保使用合格的信息资源，例如：具有良好声誉的期刊、可以信赖的互联网站或者防毒软件供应商。这就可以方便区分入侵软件是在愚弄人还是真的有病毒。应当提醒组织成员，可能有捉弄人的事情出现。还要告知他们收到这种东西时怎样做。

这些控制措施对于支持很多工作站的网络文件服务器尤其重要。

8.4 内务管理

目标：保持信息处理和通信服务的完整性和有效性。

应当创立例行程序，来执行已批准的备份策略（参见 11.1）、获取数据备份文件并练习对它们进行适时的恢复、还要记录意外事件和安全故障。如果合适的话，也要监测设备环境。

8.4.1 信息备份

应当定期对基本业务信息和软件进行备份。 应当提供足够的信息备份设备以确保所有重要的业务信息和软件都能够在一次事故或者存储介质故障之后得到恢复。 应当定期检测单独系统的备份任务安排，以保证这些安排能够满足对业务连续性计划的需要（见第 11 个句子）。应当考虑以下措施：

a） 在远程地点应当保有最低限度的备份信息，还包括准确和完整的备份件的记录并留有档案的恢复过程。该地点应当离主要业务地址足够远，以确保它可以免受主要业务地址发生灾难性事故所造成的损坏。对于重要的业务应用程序，应当至少保存三代或者三个周期的备份数据。

b） 应当对备份信息给以适当程度的物质的和环境上的保护（见第 7 句）。这些保护措施要与主要地址所用的标准相一致。应当把主要地址采用的保护性管理措施扩展到备份件存放地点。

c） 如果可行，应当定期检测备份介质，以确保可以在需要的时候拿它们应急。

d） 应当定期检查并测试恢复的程序，以确保它们的有效性并保证能够在指定的时间内按照恢复操作程序完成信息恢复。

应当确定重要业务信息的保存期限，还要确定对需要永久保存（见 12.1.3）的档案文件的所有要求。

.

8.4.2 操作员日志

操作人员应当保存一份他们活动的日志。该日志记录应当正确地包括：

a) 系统启动时间和关闭时间；
b) 系统错误和所采取的纠正措施。
c) 确认对数据文件和计算机输出做了正确的处理；
d) 做相应记录的人员的姓名。

应当对操作员日志做定期的和独立与操作程序的检查。

8.4.3 事故记录

应当报告发生的事故，并采取补救措施。对于用户报告的有关信息处理系统或者通信系统的故障应当做记录。对于如何处理报告上来的事故应当清楚的规定，包括：

a) 复验事故日志，确保故障得到满意地解决。
b) 考查改正措施，确保管理措施没有被打折扣而且所采取的措施得到了完全地授权。

8.5 网络管理

目标：确保对网络上信息的保卫和对基础支持设施的保护。 对于可能跨越组织界线的网络的安全管理需要加以注意。 对于经过公众网的敏感信息可能还要加上另外的管理保护措施。

8.5.1 网络管理措施

为了达到和保持计算机网络的安全需要采取广泛的管理措施。网络管理员应当执行这些管理措施以确保网络上信息的安全，并确保从未经授权的途径接入服务时对网络加以保护。 尤其应当考虑以下的管理措施：

a） 网络的运营责任应当和计算机操作在适当的地方分开。
b） 应当建立对远程设备的管理责任和管理程序，其中远程设备也包括在用户区的设备。
c） 如果需要，应当设立专门措施保护经过公众网的信息的保密性和完整性，并保护所连接的系统（见 9.4 和 10.3）。可能还需要专门措施维护网络服务和计算机连接的有效性。
d） 管理活动不但应当与优化对业务的服务紧密协作，还应当确保这些管理措施在整个信息处理的基础架构上都能得到一致的应用。

8.6 备份介质处理和安全

目标：防止对资产的毁坏和对业务活动的扰乱。
备份介质应当得到妥善的管理和物理上的保护

应当建立适当的操作程序来保护文件档案、计算机存储介质（磁带，磁盘，盒式磁带）、输入/输出数据和系统文件，使它们免遭破坏、偷盗和未经授权的访问。

8.6.1 对可移动的计算机存储介质的管理

应当有对可移动的计算机存储介质的管理程序。这些存储介质有多种，例如磁带、磁盘、盒式磁带和打印出的报告。应当考虑以下的管理措施：

a） 对于将要从组织中移走的可重复使用的存储介质，如果它上面的内容不再需要了，就应当删除。
b） 对所有从组织中移走的存储介质都应当需要得到授权，并且应当保存对所有这样的转移所做的记录（见 8.7.2）。
c） 所有的存储介质都应当保存在一个安全的环境中，该环境要符合存储介质制造商的规定。

所有的程序和授权等级都应当清楚地记录在案。

8.6.2 存储介质的处置

在不用的时候，存储介质应当得到安全地存放。 敏感信息可能会由于随意地放置存储介质而泄露给外人。应当建立存储介质安全存放的正式程序来把这种风险降低到最小。应当考虑以下的管理措施：

a） 保存有敏感信息的存储介质应当得到安全的存放和处置，例如通过焚毁或者粉碎，或者在清空其中的数据以后把它给组织中的其他人使用。
b） 下面列出了可能需要安全处置的物品清单：
  1） 纸型文献；
  2） 声音记录或其它记录；
  3） 复写纸；
  4） 输出报告；
  5） 一次性打印机色带；
  6） 磁带；
  7） 可移动磁盘或者盒式磁带；
  8） 光学存储介质（所有的形式，包括所有的制造商软件销售存储介质）；
  9） 程序列表；
  10） 测试数据；
  11） 系统文件；
c） 应当把所有要收集和安全存放的存储介质都做妥善安排，这要比试图从中分离出敏

感物品容易。

d） 很多组织提供对纸张、设备和存储介质的收集和安全处置服务。应当小心地选择提供此种服务的合适的签约人，该签约人应当具备足够的管理措施和经验。

e） 在可能的情况下应当对含有敏感信息的存储介质的处置做记录，以备审查。

在积累等候处置的存储介质的时候，应当注意聚集效应。这种聚集可能会导致大量的未经分类的信息比少量的经过分级处理的信息更为敏感。

8.6.3 信息处理程序

应当建立处理和储存信息的程序来保护这些信息免于未经授权的泄露或误用。这些处理信息程序的建立应当与对信息的分类相一致（见 5.2）。其中分类是在以下范围内的：文档、计算系统、网络、移动计算、移动通信、信件、声音邮件、一般的声音联络、多媒体、邮政服务/设备、传真机的使用和任何其它敏感物品，例如空白支票、配货单等。应当考虑以下的管理措施（见 5.2 和 8.7.2）：

a) 处理并标记所有的存储媒介（又见 8.7.2a）；
b) 对确认未经授权的人员进行访问限制。
c) 保有一份对得到授权的数据接收方的正式记录。
d) 确保输入的数据是完备的，处理过程正确地完成了并确认了输出的有效性。
e) 保护那些根据其敏感性等待输出到具有相应安全等级的形式的卷轴式数据。
f) 把存储介质存放在符合制造商要求的环境中。
g) 把数据发放的范围缩到最小。
h) 为了引起经授权的接收方的注意，应当把所有数据的备份都清晰地标明。
i) 定期复查信息发送表和得到授权的信息接收方列表。

8.6.4 系统文件的安全

系统文件可能保护有多种的敏感信息，例如对应用软件运行、程序、数据结构、授权程序等的描述（见 9.1）。应当考虑采用以下的管理措施来保护文件免受未经授权访问的侵害。

a) 应当安全地存储系统文件；
b) 系统文档的访问列表应当保持在很小的范围内，并且得到应用程序所有人的同意。
c) 应当恰当地保护在公共网络上保存的系统文档或通过公众网提供的信息。

8.7 信息和软件的交换

目标：防止在组织间交换的信息被弄丢、修改或者盗用。

在组织之间交换信息和软件应当受到控制，并且应当服从所有相关的法律(见第 12 句)。应当在协议的基础上进行交换。为了保护需要交换的信息和存储媒介，应当建立适当的程序

和标准。应当考虑到与电子数据交换、电子商务和电子邮件相关的业务和安全含义，还应当考虑到管理措施的要求。

8.7.1 信息和软件交换协议

应当为在组织之间（无论是以电子形式，还是以手工形式）交换信息和软件建立协议。这些协议有的可能是正式的。适当的时候，这些协议可包括软件条件托付协议。这样一份协议的安全内容应当反映出相关业务的敏感性。关于安全条件的协议应当包括：

a） 控制和通知发送、速递和接收的管理责任。
b） 通知发送人、发送、速递和接收的程序；
c） 包装和发送的最低技术标准；
d） 信使认证标准；
e） 发生丢失数据的事故时的责任和义务；
f） 为敏感信息和关键信息使用获得批准的标签系统，确保这些标签的含义能被马上理解并且信息得到恰当的保护；
g） 信息和软件的所有权和对于数据保护、软件版权和类似的情况所承担的责任（见 12.1.2 和 12.1.4）；
h） 记录和读取信息和软件的技术标准；
i） 保护敏感物品例如密钥所需要的所有专门的控制措施（见 10.3.5）。

8.7.2 转运时介质的安全

在从物理上运输信息，例如通过邮政服务或者通过信使递送信息存储介质的时候，信息容易受到未经授权的访问、盗用或者讹误的伤害。应当运用以下的管理措施保护在不同地点间传送的计算机存储介质。

a) 应当使用可靠的运输手段和信使。经过授权的信使的列表应当得到管理层的批准，并且利用适当的程序检查信使的身份。
b) 存储介质的包装应当足以保护其中的内容免受任何在转运中可能出现的物理损伤，而且还要符合制造商的相应规定。
c) 需要的时候，应当采用专门的管理措施来保护敏感信息免受未经授权的公开或者修改。例如：
   1） 使用上锁的容器；
   2） 人工递送；
   3） 防泄密包装（能够显示出任何企图获得数据的尝试）；
   4） 在例外的情况下，把托运货物分成多份由不同的路径来发货和递送；
   5） 使用数字签名和加密，见 10.3。

8.7.3 电子商务安全

电子商务与电子数据交换（EDI）、电子邮件和通过公众网，比如 Internet，的在线贸易的使

用相关。许多可能导致欺诈行为、合同争议和信息泄露或者信息更改的网络威胁都会对电子商务造成危害。应当用合同来保护电子商务免受这些威胁的危害。电子商务的安全措施应当包括：

a) 认证。 客户和交易人员对彼此所声称的身份应当有多大程度的信任？
b) 授权。授权谁进行定价、设定议题或者签署关键的交易文件？贸易伙伴如何知道这一点？
c) 合同和投保程序。 对保密性和完整性有何要求？对关键文件的递送与接收的证明和对合同的认证有什么要求？
d) 定价信息。对于建议价格列表的完整性和敏感的打折安排的保密性可以有多大的置信度？
e) 订单发送。如何保证对订单、支付和送货的详细地址以及接收确认的完整性和保密性？
f) 核查。对客户提供的支付信息进行什么程度的检查才是适当的？
g) 结算。怎样才是最适当的防止欺诈付款方式？
h) 订货。需要什么保护措施来保持订货信息的保密性和完整性，并避免交易损失或者重复交易。
i) 责任。欺诈性交易的风险由谁来承担？

考虑到要符合法律要求（见 12.1, 特别是 12.1.6 中的密码的相关立法），上述多个问题通过利用 10.3 列出的密码技术来处理。

交易伙伴之间的电子商务安排有书面协议的支持。协议把交易各方置于得到认可的协议条款的约束之下。这些交易条款包括授权的细节（见上述 b）。可能还需要与信息服务和增殖网络供应商签署的其它协议

公共交易系统应当向客户公开发布它们的交易条款。

应当注意到攻击电子商务所用主机之后进行的恢复和攻击其它所有为电子商务活动而设的网络连接的安全牵连之后进行的恢复（见 9.4.7）

8.7.4 电子邮件的安全

8.7.4.1 安全风险

人们使用电子邮件进行业务联系，它正在替代传统的通讯方式例如直通电话和信件。电子邮件在很多方面与传统通讯方式不同，比如它的速度、信息结构、未授权行为的知晓程度和对其易损性。应当注意到减少电子邮件造成的安全风险的管理需要。这些安全风险包括：

a） 信息对未经授权的服务或修改或者拒绝服务的易损性。
b） 对于故障例如错误指向和误导的易损性，以及服务的总体可靠性和有效性。
c） 通讯媒介的改变对业务活动的影响，例如递送速度增加的影响或者个人向个人而不是公司对公司来发送正式信息所造成的影响。
d） 法律上的考虑，例如在证明来源、速递、交货和接收时可能要涉及。

e） 对外发布可接触的人员列表时的影响。
f） 控制远程用户对电子邮件列表的访问。

8.7.4.2 电子邮件使用策略

对于电子邮件的使用，组织应当建立起一套清楚的策略，包括：

a） 对电子邮件的攻击，例如：病毒、拦截；
b） 对电子邮件附件的保护；
c） 关于在什么时候不使用电子邮件的规定；
d） 雇员所承担的不对公司造成伤害的责任，例如：发送电子邮件进行诽谤，使用电子邮件骚扰他人，或者未经授权的采购；
e） 用来保护电子信息的保密性和完整性的加密技术的使用；
f） 信息的保存。这些信息如果存储了就能够在需要进行诉讼时找到。
g） 为不能鉴别的信息核对而设立的其它管理措施。

8.7.5 电子办公系统的安全

为了控制与电子办公系统相关的业务风险和安全风险，应当准备并实施相应的策略和规定。，通过组合下列事物，包括文档、计算机、移动计算、移动通信、邮件、声音邮件、一般语音通信、多媒体、邮政服务/设备和传真机，它们提供了一种快速传播并分享业务信息的机会。在考虑与这些设备建立连接对安全的冲击和对业务的影响时应当包括：

a） 办公系统内信息的易损性，例如：录音电话或会议电话、电话的保密性、传真件的储存、开始邮件、邮件的发送。
b） 有关管理信息共享的一些策略和适当措施，例如对电子公告板的使用。
c） 如果该办公系统不能对敏感的业务信息提供适当等级的保护，就从中排除这些信息。
d） 限制访问与特定个人有关的日志信息，例如在敏感工程中工作的人员。
e） 办公系统支持具体业务实践的适宜性，例如联系订单或者授权。
f） 允许使用该办公系统的公司人员、签约方和业务伙伴的范围，以及可以访问该系统的地点（见 4.2）
g） 把选择的设备限制在用户的特殊范围内。
h） 识别用户的状态，例如：本组织的雇员或者为其他客户利益服务的用户。
i） 对该办公系统上信息的备份和保存（见 12.1.3 和 8.4）。
j） 撤退要求和安排（见 11.1）。

8.7.6 公众可访问的系统

应当认真保护以电子形式发布的信息的完整性，防止未经授权的改动，这些改动可能会影响该信息发布组织的声誉。在一个公众可访问的系统上的信息，例如一个可以通过互联网访问的 Web 服务器上的信息，需要符合相应法律法规。该系统要受到这些法规的管辖而且业务

活动也是其管辖范围内进行的。在信息被公开发布之前应当有一个正式的授权程序。

软件、数据和其它一些需要具备较高完整性的信息，如果要在公众可访问的系统上发布，应当有相应的保护机制。例如：数字签名（见 10.3.3）电子公告系统，特别是那些允许信息反馈和直接访问信息的系统，应当认真地加以管理以确保：

a） 信息的取得符合所有的数据保护立法（见 12.1.4）；
b） 对于输出到公众可访问的系统的信息和由该系统处理的信息应当按时进行完整、准确的处理。
c） 在敏感信息的收集和存储过程中，应当对它们加以保护。
d） 对信息发布系统的访问不允许对与它相连的网络的无意识的访问。

8.7.6 信息交换的其它形式

使用声音、传真和影像设备交换信息的时候，应当有相应程序和管理措施对这些信息进行保护。在使用这些设备的时候，可能会由于缺乏重视、缺少策略和相应的程序而损坏信息。例如，在公众场合打手机时被偷听，回复设备被窃听、对拨入语音邮件系统的非法访问或者用传真设备偶然地把传真件错误地发送给其他人。

如果通信设备发生故障、超负荷运行或者被干扰，业务运营可能被打断而且信息可能受到损害（见 7.2 和句 11）。如果通信设备受到未经授权的用户的访问，信息也可能受到损坏（见第 9 句）。

对组织成员在使用语音、传真和影像通讯时所要遵守的程序， 应当建立一个详细的策略声明。它应当包括：

a) 提醒员工们应当采取适当的预防措施，例如以下列方式打电话时不披露敏感信息以避免被窃听或被截获。
   1） 同近在咫尺的人通电话尤其移动电话。
   2） 通过对电话听筒或者电话线的物理接触来窃取情报，或者在使用模拟电话时通过扫描接收器窃听。
   3） 给在位于接收方的人通话时。
b) 提醒员工使用传真机时要注意的问题，即：
   1） 对内置信息存储做未经授权的访问来检索信息。
   2） 对机器蓄意的或者偶然的编程，使其向特定传真号码发送信息。
   3） 由于误拨号或者使用了不正确的存储号码而向错误的传真号发送文档和信息。

9 访问控制

9.1 访问控制的业务需要

目标：控制对信息的访问

根据业务和安全的要求应当控制对信息的访问和对业务程序的访问。
这应当把信息发布和授权的策略考虑在内。

9.1.1 访问控制策略

9.1.1.1 策略和业务的要求

应当定义并记录下对访问控制的业务要求。在访问控制策略说明中，应当清楚阐明访问控制规则和每个个人用户和用户群体的权限。用户和服务提供商应当提供一份清楚的对访问控制所要满足的业务要求的说明。

该策略应当考虑到以下内容：

a) 个人业务应用软件的安全要求。
b) 对所有与业务应用程序相关的信息的鉴别。
c) 信息传播和授权的策略，例如 需要知道原理和信息的安全等级和分类；
d) 在访问控制和不同系统和网络间信息分类的策略之间的连贯性；
e) 对数据或者服务的访问的保护所涉及的法律和所有合同义务；
f) 对一般工种而设的标准用户访问特征；
g) 在分布式的和网络化的环境中访问权限的管理。这种环境能够分辩所有可用连接的类型。

9.1.1.2 访问控制规定

为确定访问控制规定，应当仔细考虑以下问题：

a） 区分必须一直坚持的规定和那些有可选择性和有条件的规定；
b） 规定的建立基于如下前提“ 除非得到明白的许可，否则一般必须禁止此类行为 ”，而不是更弱的标准“ 除非被明令禁止，否则所有的行为都是允许的 ”；
c） 由信息处理设备自动引起的信息标签（见 5.2）的改变和那些用户判断引起的信息标签的改变。
d） 由于信息系统自动引发的用户许可的改变和管理员所做的这种改变。
e） 在执行之前，需要管理员或者其他人批准的规定和那些不需要这种批准的规定；

9.2 用户访问管理

目标：防止对信息系统的未经授权的访问

应当由正规的程序来控制对信息系统和服务的访问权限分配。
这些程序应当覆盖用户访问全过程的所有阶段，从新用户的最初注册到不再需要访问信息系统和服务的用户最终的注销。适当的情况下，应当特别注意控制特权访问权限的分配。 这些特权允许用户超越系统控制。

9.2.1 用户注册

为了授予对一个多用户的信息系统和服务的访问权限，应当由一个正式的用户注册和注销程序。
应当通过正式的用户注册程序来控制对于多用户信息服务的访问。该注册程序应当包括：

a） 使用唯一的用户身份，以便将用户与他们的行为联系上并让他们对自己的行为负责。群体身份（group ID）只允许在它们适于所要做的工作时才采用。
b） 检查用户是否有从系统所有人处得到的使用信息系统和服务的授权。管理层做出的对于访问权限的单独批准可能也是合适的
c） 检查授予的访问等级是否于业务目标相适应（见 9.1），并且是否与组织的安全策略相一致，例如：它不会损害任务的分离（见 8.1.4）。
d） 给用户一个关于他们访问权限的书面声明；
e） 要求用户签署该声明以表明他们理解访问的条件。
f） 确保访问提供商在授权程序完结之前不提供访问途径。
g） 保存一份注册使用该系统的所有人员的正式记录。
h） 立即取消已经改换工作或者离开该组织的用户的访问权限；
i） 定期检查并删除冗余的用户 ID 和帐户；
j） 确保冗余的用户帐号不被转给其它用户。

如果职工和服务代理人有未经授权的访问时要受处罚，应当注意，在员工合同和服务合同中要包涵相关条款对此做出规定（见 6.1.4 和 6.3.5）。

9.2.2 特权管理

应当严格限制特权（多用户信息系统的任何使得客户超越系统或者应用软件控制的特征或者便利）的分配和使用。对系统特权的不当使用经常成为导致被攻破的系统产生故障的一个主要因素。需要防止未经授权访问的多用户系统应当通过正式的授权程序来控制对特权的分配。 应当考虑以下的步骤：

a） 应当确定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软件相联系的特权和需要分派的职工类别；
b） 特权的分配应当建立在一种需要使用的基础和就事论事的基础上，例如只有在需要

时才对它们功能角色有最低限度的要求。

c） 应当保有一个授权程序和一份所有分配出的特权的记录。在授权程序结束之前不应当授予特权。

d） 系统程序的开发和使用应当得到提升，以避免需要向用户授予特权。

e） 特权应当分配给一个不同于常规业务使用的用户身份。

9.2.3 用户密码管理

密码是一种访问信息系统或者访问时确认用户身份的常用方式。应当通过正式的管理程序来控制密码的分配。这一程序应当：

a） 需要用户签署一项声明以保持个人密码的保密性并确保工作组密码只在该组成员的内部（这应当包括在用工合同条款中，见 6.1.4）

b） 在用户需要维护他们的密码时，确保最初为它们提供一个安全的临时密码，而迫使他们立即更改。当用户未经他们密码的时候提供的临时密码应当只按照确实的用户身份提供。

c） 需要临时密码来给用户一个安全的方式。应当避免使用第三方或者使用未受保护的明码电文的电子邮件信息。用户应当确认接收到密码了。

无论如何，密码都不能以一种未受保护的形式存储在计算机上。可以使用其它的用户识别和授权技术，例如生物测定像指纹鉴定、签字确认和硬件标识例如集成芯片卡。适当情况下应当加以考虑。

9.2.4 用户访问权限的复查

为了保持对数据和信息服务的存取访问的有效控制，管理层应当实施一个正式的程序来定期复查用户的访问权限，使得：

a） 用户的访问权限得到定期复查（推荐周期是 6 个月）并在做任何改动后进行复查（见 9.2.1）。

b） 对特殊的特权访问权限（见 9.2.2）应当以更高的频率来检查；推荐周期是 3 个月。

c） 定期核查特权分配，以确保无人得到未经授权的特权。

9.3 用户责任

目标：防止未经授权的用户访问 得到授权的用户进行合作是有效的安全基础。 为了维持有效的访问控制，应当让用户知道他们的责任，尤其是有关密码使用和用户设备的安全方面的责任。

9.3.1 密码使用

用户应当按照良好的安全操作规程来选择和使用密码。
密码提供了一种验证用户身份的手段，从而建立了对信息处理设备和服务的访问权限。 应当建议所有的用户：

a） 保护密码的保密性；
b） 避免在纸张上保留密码记录，除非可以对其安全存放。
c） 只要有系统或者密码可能被侵害的迹象，就更改密码；
d） 选择的优质密码至少要有 6 个字符的长度，这些字符要：
    1） 容易记忆；
    2） 不是基于那些别人很容易地根据个人相关信息就能够猜出来的东西。例如：名字、电话号码和生日等等。
    3） 避免使用连续的相同数字，或者全是数字或全是字母的字符组。
d) 定期更换密码或者根据一定量的访问次数来更改密码（特权帐户的密码应当比普通帐户密码更改的更为频繁）。避免重复或者循环使用旧的密码。
e) 定期更换密码或者根据一定量的访问次数来更改密码（特权帐户的密码应当比普通帐户密码更改的更为频繁）。避免重复或者循环使用旧的密码。
f) 在第一次登录时更改临时密码；
g) 不要把密码包含在任何自动登录程序之中，例如把密码存在宏代码或者功能键上。
h) 不要共用个人用户密码。

如果用户需要访问多重服务或者平台并且被要求持有多重密码，那么应当建议他们对于所有的为存储的密码提供合理保护等级的服务都使用单一的优质密码（见上述 d））。

9.3.2 无人值守用户设备

用户应当确保无人值守设备得到足够的保护。在用户区安装的设备，例如工作站或者文档服务器，可能需要特殊的保护以防止在较长的无人值守时间内被未经授权地访问。为了保护无人值守的设备，应当让所有的用户和合同伙伴明白安全要求和安全程序。而要实施这些保护还得使他们清楚自己的责任。 应当建议用户：

a） 当完成对话束时要将活动的对话终止，除非有适当的锁定机制的保护，例如一个密码保护的屏幕保存程序；
b） 当对话期结束时要注销主机（而不仅仅是关掉个人计算机和终端）；
c） 在不使用 PC 机和终端时，用密码锁或者相类似的控制手段例如密码访问，以防止对它们的未经授权的使用。

9.4 网络访问控制

目标：保护网络服务

应当控制对内部和外部网络服务的访问。
这对于确保对网络和网络访问有访问权限的用户不损害这些系统的安全是必要的。为此，要确保：

a） 在本组织的网络和其它组织的网络例如公共网之间有适当的接口；
b） 对用户和设备的适当的授权机制；

对用户访问信息服务的控制。

9.4.1 网络服务的使用策略

与网络服务的不安全的链接会影响到整个组织。只应当向用户提供对那些特别授权他们使用的服务进行直接访问。这种控制对于同敏感或者关键业务应用软件的联网或者同处于高风险地区的用户的联网都是十分重要的。其中高风险地区指公共的场所或者组织的安全管理范围以外的区域。

策略的筹划应当考虑到网络和网络服务的使用。应当包括：

a） 允许访问的网络和网络服务；
b） 用来确定谁可以访问那些网络和网络服务的授权程序；
c） 保护对网络连接和网络服务的访问的管理措施和程序。

这一策略应当与业务访问控制策略（见 9.1）相一致。

9.4.2 强制路径

从用户终端到计算机服务器的路径可能需要进行控制。 网络被设计成要允许最大程度的资源共享和最大程度的路径选择自由。而网络的这些特征也可能为那些对业务应用软件未经授权的访问或者对信息设备未经授权的使用制造了机会。限制用户终端与允许用户访问的计算机服务器之间路径的联合管理措施，例如建立一条强制路径，能够降低这种风险。

强制路径的目的是为了防止用户选择了任何用户终端与允许用户访问的计算机服务器之间路径的其它路径。

一般来说，这需要在路径的不同地点实行一定数量的控制。其原理是通过预先确定的选择来限制在网络中的各个点处的路径选取。

下面是它的例子：

a） 分配专用线路和电话号码；
b） 自动连接到指定的应用软件系统或者安全门路；

c） 为单个用户限制菜单和子菜单选项。
d） 防止不受限制的网络漫游；
e） 对外部的网络使用者，强制其使用指定的应用软件系统和/或安全门路；
f） 通过安全门路例如防火墙来积极地控制目的地通信的许可来源。
g） 为组织内部的用户群建立分离的逻辑域来限制网络访问，例如虚拟私人网络（又见9.4.6）。

对强制路径的要求应当基于业务访问控制策略（见 9.1）

9.4.3 外部连接的用户认证

外部连接可能导致对信息系统未经授权的访问，例如拨号的方法。因此，应当把远程用户的访问置于比其它方式更为严密的保护之下，例如以使用密码技术为基础的方法能够提供强大的认证。要从风险评估中确定所需保护等级，这点十分重要而且选择恰当的认证方法时也需要。

可以通过多种方式验证远程用户的身份，例如加密技术、硬件标识或者询问/应答协议。也可能用专用线路或者网络用户地址检查设备来确认连接的来源。

拨号回送程序和控制措施，例如使用回拨调制解调器，能够防止对一个组织的信息处理设备的未经授权的和有害的连接。这种控制鉴别那些试图从远处建立到组织的网络的连接的用户。使用这些管理措施时，组织不应当用网络服务包括电话发送；如果使用了这种网络服务，就应当取消这样的特征，以避免与电话发送相关的弱点。回拨过程包括确认在组织一方的连接确实断开了，这点也很重要。否则，远程用户能够持续占线假装已经做了回拨验证。应当仔细的检测回拨程序和控制的这种可能性。

9.4.4 节点鉴别

自动连接到远程计算机的设备能够提供了一种途径，从中可以获得对业务应用软件的未经授权的访问。因此应当认证连到远程计算机系统的连接。如果连接使用的网络在组织的安全管理的控制范围以外，这种做法就尤其重要了。 在上述 9.4.3 中给出了一些例子说明什么是认证和如何实现认证。

节点认证能够作为认证远程用户群的替代方式，在那里用户连接到了一个安全的共享的计算机设备（见 9.4.3）。

9.4.5 远程诊断接口的保护

应当安全地控制对诊断接口的访问。为了方便维护工程师的使用，许多计算机和通信系统安

装在一个拨号远程诊断设备之中。如果未加保护，这些诊断接口就为未经授权的访问提供了途径。因此，应当用适当的安全机制对其加以保护，例如一个密码锁和一个保护程序。通过在计算机服务管理员和需要访问通路的硬件/软件支持人员之间所做的安排，该程序确保了诊断接口只能由他们访问。

9.4.6 网络分离

网络日益被扩展到传统的组织边界以外，例如业务伙伴关系的形成可能需要互联或者共享信息处理和网络设备。网络的这种扩展可能加大使用网络的现有信息系统受未经授权的访问的风险。由于有些网络的敏感性或者关键性，它们可能需要其它网络用户的保护。在这种情形下，应当考虑在网络中引入管理措施来分离不同的信息服务、用户和信息系统。
大型网络安全管理的方法之一就是将其分解为独立的逻辑网域，例如组织的内部网域和外部网域，每个域都由一个确定的安全边界保护。在将被连接起来以控制两个域之间的访问和信息流的两个网络之间安装一个安全门路，由此可以实现上述的安全边界。这一门路经过定制可以来过滤这些域之间的通信（见 9.4.7 和 9.4.8）并能够按照组织的访问管理措施（见 9.1）堵住未经授权的访问渠道。这种门路的一个例子就是我们通常所说的防火墙。

将网络分离成域的标准应当是基于访问控制策略和访问的要求（见 9.1），而且还要考虑到合成适当的网络路径或者门路技术的相对成本和对性能的影响（见 9.4.7 和 9.4.8）。

9.4.7 网络连接管理

共享网络访问控制策略的要求，特别是那些跨越组织界线的关系网络，可能需要把控制措施结合起来以约束用户的连接能力。这种控制措施可以由一个用预先拟定的表格或者规则过滤通信的网络门路来实现。所用的这种约束措施应当基于访问控制策略和业务应用软件的需要（见 9.1），因此应当加以维护和更新。

需要加以限制的一些具体应用是：

a） 电子邮件；
b） 单向文件传送；
c） 双向文件传送；
d） 交互式访问；
e） 与每天或者某个日期的时间相关的网络通路。

9.4.8 网络路径选择控制

共享的网络，尤其是那些跨越组织边界的网络，可能需要把路径选择管理措施结合起来以确保计算机连接和信息流不会破坏业务应用软件的访问控制策略（见 9.1）。这种控制对于同第三方（非组织）用户共享的网络常常是具有根本性的。

路径选择控制应当基于确定的来源和目标地址检测机制。网络地址翻译对于隔离网络和防止路径从一个组织的网络延伸到另一个网络中也是一种非常有用的机制。它们能够在软件和硬件中实现。实施者应当清楚所配备的任何机制的作用强度。

9.4.9 网络访问安全

有广泛的公共网络服务和私有网络服务可供利用，其中有的是增值服务。网络服务可能有独特的或者复杂的安全特征。使用网络服务的组织应当确保对所有服务的安全属性做一个清晰的描述。

9.5 操作系统访问管理

目标：防止未经授权的计算机访问。

操作系统水平的安全设备应当用于限制对计算机资源的访问。这些设备应当能够做到以下事情：

a） 鉴别和验证身份，如果需要的话还能够鉴别和验证每个经授权用户的位置和终端。
b） 记录对系统的成功访问和失败访问。
c） 提供适当的授权方式；如果使用了密码管理系统，应当能够确保使用的是优质密码（见 9.3.1 d））。
d） 在适当的地方，限制用户的连接次数。

如果证明对于业务风险没有危害，那么也可以使用其它的访问控制方法，例如询问－应答方法。

9.5.1 自动终端识别

为了鉴别连到特殊地点和便携设备的连接应当考虑自动终端识别技术。如果一个对话只能从特殊的地点或者计算机终端上启动这点很重要，那么自动终端识别就是一种可以考虑的方法。终端内或者贴到终端上的一个标识可以用来指示是否允许这个特定的计算机终端启动或者接收特殊事项。为保持终端标识的安全，可能需要对计算机终端进行物理保护。也可以用其它的技术鉴别计算机终端（见 9.4.3）。

9.5.2 终端登录程序

由一个安全的登录程序应当能够获得对信息服务的访问。这一登录到计算机系统的过程的设

计应当把对系统未经授权的访问的机会降到最低限度。因此为了避免给未经授权的用户以不必要的帮助，该登录程序只会透露出最少的系统信息。一个好的登录程序应当做到：

a） 除非登录程序成功结束，否则不显示系统或者应用程序；
b） 显示一般性的警告，说明只有经过授权的用户才能够访问；
c） 在登录程序中不提供可能会帮助未经授权的用户的信息；
d） 只有完成所有数据的输入以后才开始验证。如果产生一个错误条件，该系统不应当指示出哪对哪错。
e） 限制所允许失败登录次数（推荐使用 3 次），并且考虑：
    1） 记录失败的尝试；
    2） 在重新登录之前强制等待一段时间或者拒绝任何没有特殊授权的进一步尝试。
    3） 断开数据连接。
e) 限制所允许的登录程序的最长和最短时间。如果超过了这个范围，系统应当终止登录。
f) 当成功的完成登录以后，要显示以下信息：
    1） 上一次成功登录的日期和时间；
    2） 自从上次成功登录以来，历次失败登录尝试的细节。

9.5.3 用户识别和鉴定

所有的用户（包括技术支持人员，例如操作员、网络管理员、系统程序员和数据库管理员）应当有唯一的标识（用户 ID）供他们个人并且只供他们个人使用。因此，可以追踪各种活动到负有责任的个人身上。用户 ID 不应当显示出用户的特权等级（见 9.2.2），例如管理人员、监控人员。

在例外的情况之下，如果有明显的商业利用，可能会让一个用户群或者特殊的工种共享一个用户 ID。管理层对这种情况的批准应当记录在案。为保持可计量性，可能还需要其它管理措施。

有各种授权程序，可以用来证实所声称的用户身份。密码（见 9.3.1 和下文）是一种非常通用的进行识别和鉴定（I&A）的方法。这一方法基于一个只有用户才知道的秘密。利用加密技术和鉴别协议也可以达到同样的目的。

像存储标识或者用户拥有的智能卡这类物品也可以用来进行识别和鉴定。利用个人的唯一的特征或者属性的生物鉴别技术也可以用来鉴别一个人的身份。将鉴别技术和管理机制妥善地结合到一起能够得到更为强大的鉴定能力。

9.5.4 密码口令管理系统

密码是验证用户访问计算机权限的主要形式之一。密码管理系统应当提供一个有效的、交互的设备。这样可以确保优质密码（参考 9.3.1 小节的密码使用指导）。

一些应用程序需要有独立的职权来分配用户密码。在大多数情况下，密码是由用户选择和维护的。

一个好的密码管理系统应当：

a） 强制使用个人密码以保持可计量性;
b） 适当的时候，允许用户选择和更改他们自己的密码并包括一个确认程序，它允许出现输入错误。
c） 强制选择如 9.2.1 所述的优质密码；
d） 用户维持他们自己的密码时，强制实行如 9.3.1 所述的密码变更；
e） 当用户选择密码时，强制他们在第一次登录的时候更改临时密码（见 9.2.3）；
f） 维持一份以前用户密码的记录，例如在此之前 12 个月，并避免再次使用；
g） 输入密码时不要将其在屏幕上显示出来；
h） 把密码未经与应用软件系统的数据分开存放；
i） 以使用单向加密算法的加密形式存储密码口令；
j） 软件安装完毕后，改变缺省的卖方密码。

9.5.5 系统实用程序的使用

大多数计算机安装有一个或者更多系统实用程序，它们可能有能力超越系统和应用程序的控制。限制并严格控制对它们的使用是十分重要的。应当考虑以下的控制措施：

a） 给系统实用程序使用认证程序；
b） 系统实用程序从应用软件分离出来；
c） 把使用系统实用程序的人限制在最少的值得信任的授权用户之内；
d） 为系统实用程序的特殊使用进行授权；
e） 限制系统实用程序的有效性，例如在一个经授权的变更的持续时间之内；
f） 记录系统实用程序的所有使用；
g） 系统实用程序授权等级的定义和文件证明；
h） 所有基于软件的多余实用程序和多余系统软件的删除。

9.5.7 终端暂停

为了防止未经授权的人访问，在一段确定的休止期结束后，应当关闭在高风险地区例如在组织的安全管理之外的公共场所或外部地区的暂停终端或者是正在为高风险系统提供服务的终端。 在一段确定的暂停期后，这一终端暂停手段应当清除终端屏幕内容并关闭应用程序和网络对话。该暂停应当反映出这个地区和终端用户的安全风险。

一些 PC 机可以得到有限的终端暂停手段，使其能够清楚屏幕内容并防止未经授权的访问但是不会关闭应用程序或者网络进程。

9.5.8 连接时间的限制

对连接时间的限制应当为高风险应用程序提供额外的安全保证。限制终端可以连接到计算机访问的时间缩小了未经授权访问的机会空间。对于敏感的计算机应用程序，特别是那些有终端安装在高风险地区例如在组织的安全管理范围之外的公共场所或外部地区的，应当考虑这样的管理措施。这样约束措施的例子包括：

a） 使用预先确定的时间段，例如批量的文件发送，或者定期的短时交互式对话；

b） 如果没有超时或者延时业务，限制连接到正常办公时间的次数。

9.6 应用程序访问控制

目标：防止保存在信息系统内信息被未经授权地访问。应当使用安全设施限制在应用程序系统中的访问。

对软件和信息的逻辑访问应当限制在经过授权的用户之中。应用软件系统应当：

a) 控制用户对信息和应用程序系统功能的访问，并要与确定的业务访问控制策略相一致；

b) 为任何一个能够超越系统或应用程序限制的实用程序和操作系统软件提供保护，防止未经授权的访问；

c) 不损害有共享信息资源的其它系统的安全；

d) 只能够向所有权人、其它被指派和经授权的个人或者确定的用户群提供对信息的访问权限。

9.6.1 信息访问限制

按照确定的访问控制策略，应当为应用软件系统的用户包括技术支持人员提供对信息和应用程序系统的访问。这是基于个人业务应用程序要求的并且与组织的信息访问策略（见 9.1）相吻合。为了支持访问限制要求，应当运用以下管理措施：

a） 提供菜单来控制访问应用程序系统功能；

b） 通过适当编辑用户文件，可以限制用户对于未得到授权进行访问的信息或者应用程序系统功能的了解；

c） 控制用户的访问权限，例如读取、改写、删除和执行等权限。

d） 确保处理敏感信息的应用程序系统的输出只包括与输出的使用相关的信息，而且只送到得到授权的终端和地点，包括对这种输出周期性的复查以确保多余的信息被删除了。

9.6.2 敏感系统的隔离

敏感系统可能需要专用（隔离的）计算环境。有些应用程序系统对于潜在的损失如此敏感以致于需要对它们做专门处理。这种敏感性可能表示应用程序系统应当在专用计算机上运行，而且只同受信的应用程序系统共享资源，或者没有限制。可以考虑以下几点。

a) 对一个应用程序系统的敏感性应当做清楚的定义并且有应用程序所有权人把它记录在案（见 4.1.3）。
b) 当一个敏感的应用程序将在共享的环境下运行时，应当识别出应用程序将分享其中资源的该应用程序系统，并获得敏感应用程序的所有权人的准许。

9.7 检测系统访问和使用

目标：探测未经授权的活动。

应当监视系统以发现偏离访问控制策略的行为并记录可监测事故以便方式安全事件时提供证据。
系统检测允许对所采用管理措施的有效性进行检测，并允许对一个访问策略模型（见 9.1）的确认进行验证。

9.7.1 事件记录

应当编写用来记录异常现象和其它有关安全的事件的审查日志，并在各方同意的时间段内保持该日志，以协助以后的调查研究和访问控制监测。 审核日志还应当包括：

a） 用户 ID；
b） 登录和注销的日期及时刻；
c） 如果需要，要做终端或者地点的识别；
d） 对系统成功的访问和被拒绝的尝试所做的记录；
e） 对数据和其它资源成功的和被拒绝的访问所做的记录。

某些审核日志可能需要放入档案中，作为记录保留策略的一部分或者出于收集证据的需要（另见第 12 句）

9.7.2 检测系统使用

9.7.2.1 程序和风险区域。

应当建立程序以检测信息处理设备的使用。为了确保用户只做了得到明确授权的行为，这样的程序是必需的。应当由风险评估确定个人设备所需的监测等级。应当考虑的地方有：

a） 得到授权的访问，包括细节例如：

1） 用户 ID；
2） 关键事件发生的日期和时间；
3） 事件的类型；
4） 访问的文件；
5） 使用的程序/实用程序；

c) 所有有特权的作业，例如：
1） 监督员帐户的使用；
2） 系统启动和结束；
3） 输入/输出设备附件/可拆件。

d) 未经授权的访问尝试，例如：
1） 失败的尝试；
2） 对访问策略规定的违反和对网络门路和防火墙的通告。
3） 警惕所有权人侵入检测系统；

e) 系统警报或者故障，例如：
1） 控制台警报或者消息；
2） 系统日志异常；
3） 网络管理警报。

9.7.2.2 风险因素

应当定期检查检测活动的结果。检查的频率取决于所涉及的风险。应当加以考虑的风险因素包括：

a) 应用进程的重要程度；
b) 所涉及信息的价值、敏感性和重要程度；
c) 以往的系统过滤和和误用的经验教训；
d) 系统互联的程度(特别是公共网络)；

9.7.2.3 记录和检查事件

日志检查涉及对于系统所面临威胁的理解和对这些威胁可能的产生方式的认识。在 9.7.1 中给出了为了防止安全事故可能需要深入调查的事件的例子。

系统日志常常包涵大量的信息，其中很多信息与安全检测无关。出于安全检测的目的而帮助识别重要事件时，应当考虑把适当的信息类型自动复制到第二个日志和/或者使用适当的系统实用程序或检测工具，以便进行文件审查。

当为检查日志而分配责任时，应当考虑把执行检查的人员和其活动被监测的人员之间的角色分离开。

应当尤其注意日志记录设施的安全，因为一旦遭到破坏可能给人一种十分安全的假相。管理

措施应当致力于防范未经授权的改动和操作问题包括：

a） 将记录设备置于停止状态；
b） 所记录的消息模式的变更；
c） 被编辑或者删除的日志文件；
d） 被用完的日志文件的存储器，要么不能记录事件要么覆盖了自己。

9.7.3 时钟同步

为了确保审查日志的准确性，正确的设定计算机时钟是十分重要的。这在调查研究中可能需要或者可以作为法律案件中的证据。不准确的审查日志可能会妨碍调查研究的进行，并会削弱它作为证据的可信度。在计算机或者通信设备有能力操作一个实时的时钟的地方，应当按照一个共同的标准把它设定，例如 通用协调时间（UCT）或者当地标准时间。由于有的时钟有偏差，应当有一个程序可以检测并改正任何重要的变更。

9.8 移动计算和远程工作

目标：在使用移动计算和进行远程工作时确保信息安全。
所需要的保护应当与这些工作的特殊方式引起的风险相协调。使用移动计算时应当考虑到未经保护的环境下工作的风险，并且要考虑到所采用的适当措施。在远程工作时，组织应当为远程工作地点提供保护并且确保对这种工作方式有适当的安排。

9.8.1 移动计算

使用移动计算设备例如笔记本电脑、掌上电脑、膝上电脑和移动电话等的时候，应当特别注意要确保业务信息不受损害。应当采取正式策略来考虑使用移动计算设备的风险，特别是在未加保护的环境之中。例如，该策略应当涵盖物理保护、访问控制、加密技术、备份文件和防范病毒等等方面的需要。该策略还应当包括有关把设备连接到网络的规则和建议以及对于在公共场所使用这些设备的指导。

在公共场所、会议室和其它在组织的保护范围之外的未受保护的地区。在适当的位置应当有保护措施，以避免未经授权的访问或者泄露由这些设备存储和处理的信息，例如使用加密技术（见 10.3）。

当这种设备在公共场所使用的时候应当小心避免被未经授权的个人从远处看见的危险。这一点很重要。应当有适当的防止恶意软件的程序并且要对其不断更新（见 8.3）。为了确保能够快速而方便地备份信息，这些设备应当是可用的。这些备份应当得到充分的保护例如防盗和防止信息丢失。

对连接到网络的移动设备移动给以适当的保护。只有经过成功的识别和鉴定之后才可以使用

移动计算设备通过公众网对业务信息进行访问，并且有适当的访问控制机制在（见 9.4）。还应当对移动计算设备加以物理上的保护，以防在离开时被偷窃，例如在轿车和其它交通工具上、在宾馆房间、会议中心和见面地点等。载有重要信息、敏感和/或者关键的业务信息的设备不应当没人照看，而且如果可能的话，应当把实物锁起来、或者使用特殊的锁来保护该设备。关于对移动设备进行物理保护的更多的信息可以在 7.2.5 找到。

应当训练职工使用移动设备，提高他们对这种工作方式所带来的额外风险和应当实行的管理措施的认识。

9.2.8 远程工作

远程工作用通信技术使得职工能够在组织之外的远程固定地点工作。对远程工作的适当保护应当防止设备和信息被盗走、未经授权就披露信息、对组织内部系统的未经授权的访问或者设备的误用。远程工作不但需要授权还要由管理层控制，而且对这种工作方式应当有适当的安排。这一点非常重要。

组织应当考虑开发一种策略、程序和标准来控制远程工作活动。组织应当只授权远程工作活动，如果它们能够满足有适当的安全设置和管理措施的要求而且符合组织的安全策略的话。应当考虑以下几点：

a） 对远程工作地点现有的物理上的保护，考虑建筑物理的安全和当地环境的安全。
b） 拟定的远程工作环境；
c） 通信安全要求，考虑到对组织内部系统进行远程访问的需要、即将通过通信链接并接收评估的信息的敏感性和内部系统的敏感性。
d） 在该适应范围例如家庭和朋友的其他人对信息或者资源的未经授权的访问所造成的威胁。

需要考虑的管理措施和安排应当包括：

a） 为远程工作提供适当的设备和存储家具。
b） 对允许做的工作、工作时间、可以保留的信息的分类和远程工作人员被授权访问的内部系统及其服务分别做出的定义。
c） 提供适当的通信设备包括保护远程访问的方法。
d） 物理安全；
e） 对家庭成员和来客访问设备和访问信息的有关规定和指导；
f） 软件和硬件支持和维护措施的提供。
g） 备份和业务连续性的过程。
h） 审查和安全监测；
i） 远程工作活动停止时，权力的取消、访问权限和设备的归还

10 系统的开发与维护

10.1 系统的安全需要

目的：确保将安全构建成信息系统的一部分。

这包括基础架构、业务应用软件和用户开发的软件。这种支持应用软件或者服务的商务处理的设计和实施可能对安全十分关键。在开发信息系统之前应当确定其安全需要并得到对它的赞同。
所有的安全需要包括撤退安排的需要都应当在一个项目的需求分析阶段被确认， 并且作为一个信息系统的总体经营情况得到对其合理性的证明、获得同意并被记录在案。

10.1.1 安全性要求分析和规范

对新系统业务需要所做说明或者对现有系统所给的增强作用应当规定管理措施的要求。这样的规范应当考虑到将要集成到系统中的自动控制措施并考虑到支持手动控制的需要。为商业应用目的评价软件包时应当做类似的考虑。如果被认为合适的话，管理层可能希望利用独立的评价和验证产品。

安全需要和管理措施应当反映所涉及信息资产的价值和可能有安全故障或者缺乏安全导致的潜在业务损害。分析安全需要和识别管理措施以实现它们的基本框架是风险评估和风险管理。

在设计阶段引进的管理措施要比那些在实施时或者完成后的控制措施实现和维护起来更便宜。

10.2 应用软件系统中的安全

目标：防止在应用软件系统中的用户数据的丢失、改动或者误用。

应当把适当的管理措施和查验追踪或者活动日志设计到应用软件系统中，包括用户编写的应用程序。这些措施应当包括对输入数据、内部处理和输出数据的检验。

对于那些处理敏感的、有价值的或者重要的组织资产的系统或者对其有影响的系统，可能还需要适当的管理措施。这些管理措施的确立应当基于安全需要和风险评估。

10.2.1 输入数据的验证

应当验证输入到应用软件系统中的数据，确保它是正确的和适当的。应当检查业务交易的输入、固定数据（姓名和地址、信贷限额、客户基准数）的输入和参数表（售价、货币兑换率、

税率）的输入。应当考虑以下的措施：

a） 为发现下述错误可以重新输入或者采用其它输入检查方法：
   1） 超范围数值；
   2） 数据域中的无效字符；
   3） 遗漏的或者不完整的数据；
   4） 超出数据容量的上下限；
   5） 未经授权或者不一致的控制数据；
b） 对关键域或者数据文件内容进行周期性检查，确认其有效性和完整性；
c） 检查打印的输入文件中是否有未经授权的对输入数据的变更（对输入数据文件的所有变更都应当是得到授权的）。
d） 响应验证错误的程序；
e） 检测输入数据整体的可信度的程序；
f） 确定所有涉及数据输入程序的人员的责任。

10.2.2 内部作业的管理

10.2.2.1 风险区域

正确输入的数据可能被处理中的错误或者删除行为破坏。应当把有效性验证作为系统的一部分来检测这种破坏。应用软件的设计应当确保实施限制措施把危及数据完整性的处理故障的风险降低到最小。需要加以注意的特殊地方包括：

a） 改变数据的添加和删除功能在程序中的使用和位置；
b） 防止程序按照错误的顺序运行或者在先前的处理故障之后马上运行的程序；
c） 使用恰当的程序从故障中恢复，以确保对数据的正确处理。

10.2.2.2 检查和控制

所需的管理措施取决于应用软件的性质和数据破坏对业务的冲击。以下是一些可以采用的检测措施的例子：

a） 对进程或者批处理的管理，用于在事务更新之后调节数据文件平衡。
b） 平衡控制，用于对比检测期初余额和先前的期末余额，即：
   1）运营对运营的控制；
   2) 文件更新合计；
   3) 程序对程序的控制。
b) 对系统生成数据的验证（见 10.2.1）；
c) 验证在中心和远程计算机之间下载或上载的数据或者软件的完整性（见 10.3.3）；
d) 记录和文件的数位总和；
e) 检查确保应用程序在恰当的时间运行；
f) 检查确保应用程序按照正确的顺序运行，在出现故障时程序终止并且在问题解决之

前停止运行。

10.2.3 文电鉴别

文电鉴别是一种检查手段，用于检测对传送的电子消息的内容所做未经授权的更改或者文电消息本身的损害。该方法可以用在支持物理消息鉴别设备或软件算法的硬件或者软件中。

对于需要保护消息内容完整性的应用程序应当考虑采用文电鉴别。例如，电子形式的资金传送、规定、合同、建议等具有很大重要性的消息内容，或者其它类似的电子数据交换。为了确定是否需要文电鉴别并找到最佳实施方案应当进行安全风险评估。

文电鉴别不是用来防止消息内容未经授权就被泄露的。可以用加密技术（见 10.3.2 和 10.3.3）作为实现文电鉴别的方式。

10.2.4 输出数据验证

应当验证应用系统输出的数据以确保对存储信息的处理是正确的并且与环境相适应。一般的说，系统的建造基于这样的前提，即已经采用的对输出的适当的验证、鉴别和检测将会一致是正确的。而实际情况并非如此。输出验证可以包括：

a） 可信度的检查，用来测试输出数据是否合理；
b） 协调控制计数，用于确保所有数据的处理；
c） 为读者或者后续处理系统提供充足信息以确定信息的准确性、完整性、精确度和类别；
d） 响应输出验证测试的程序；
e） 定义所有涉及数据输出过程的人员的责任。

10.3 密码管理措施

目标：保护信息的保密性、完整性和有效性。
对处于危险中而且其它管理措施无法对其进行有效保护的信息，应当用密码系统和密码技术对其进行保护。

10.3.1 使用密码控制措施的策略

对一个密码解决方案是否适当做出决定可以看作是更广泛的评估风险和选择管理措施的手段的一个部分。应当用风险评估了确定信息所应当得到的保护等级。这种评估随后可以用于评判一个密码管理措施是否得当、应当采用何种控制措施以及为了什么目的和业务处理。

组织应当为保护其信息制订一套加密管理措施的使用策略。这样的策略必须能够将利益最大化并把使用密码技术的风险降到最低，而且还要避免不适当或者不正确的使用。 在开发该策略的时候应当考虑到以下几点：

a） 在整个组织范围内使用密码技术的管理途径，包括业务信息应当受其保护的一般规则；
b） 密钥管理的途径，包括为防止密钥丢失、受损或者被毁而对加密的信息进行恢复；
c） 角色和任务，例如谁应当负责：
d） 策略的实施；
e） 怎样确定适当的密码保护等级；
f） 为在整个组织内有效实施所要采用的标准（何种解决方案用于何种商务处理）。

10.3.2 信息加密

信息加密是一种密码技术，它可以用于保护信息的保密性。保护敏感的和关键的信息时应当考虑该技术。

根据风险评估，确定所需的保护等级并且考虑到所用加密算法的类型和质量以及要用的密码关键字的长度。

当实施组织的加密策略时，应当考虑到有的法规和国家性限制可能涉及在世界的不同地方这些加密技术的使用问题，还应当考虑到加密信息的越界流动。 另外，应当注意那些用于密码技术进出口的管理措施（见 12.1.6）。

应当征求专家的建议来确定适当的保护等级、选择适当的将要用于所需保护的产品和挑选密钥管理的安全系统的实施方案（见 10.3.5）。另外，为了寻找一些法律法规，它们可能适用于组织中意的加密技术的使用，可能需要法律建议。

10.3.3 数字签名

数字签名提供了一种保护电子文档的真实性和完整性的方法。例如它们可以用于电子商务，那里需要验证是谁签署了一份电子文件并且检查签了名的文件是否被改动。

数字签名能够用于以电子化处理的任何文件形式，例如可以用它们签署电子支付单据、基金传送、合同和协议。数字签名可以用基于唯一相关的密钥对的密码技术，其中的一个密钥用于生成签字（私有密钥）而另外一个密钥用于检测该签名（公共密钥）。

应当注意保护私有密钥的保密性。应当对该密钥进行保密，因为任何取得该密钥的人都能够签署文件，例如付款单据、合同，因此伪造了密钥主人的签字。另外，保护公共密钥的完整性也很重要。可以使用公共密钥证件（见 10.3.5）来提供这种保护。

需要考虑所用签名算法的类型和质量以及将要使用的密码的长度。数字签名中使用的密码关键字应当与加密算法中使用的不同。

使用数字签名时，应当考虑到相关立法，它们描述了在什么情况下数字签名受法律约束。例如在电子商务中知道数字签名的立法角度是十分重要的。在缺乏法律框架的时候，可能需要具有约束力的合同或者其它协议来支持使用数字签名。

10.3.4 非拒绝服务

对于一个事件或行为是否发生有争议时，例如对在一份电子合同或者支付手续上数字签名的使用的争执，为解决争议需要用到非拒绝服务。它们能够帮助找到证据，以便证实一个特殊事件或者行为是否已经发生，例如是否拒绝使用电子邮件发送有数字签名的说明。这些服务基于加密和数字签名技术（见 10.3.2 和 10.3.3）的使用。

10.3.5 密钥管理

10.3.5.1 密码关键性的保护

密码关键字的管理是对密码技术的有效利用的根本。密码关键字的任何损坏或者丢失都可能危及信息的保密性、真实性和/或者完整性的安全。应当有一个管理系统适当地支持组织对两种密码技术的使用，它们是：

a） 秘密密钥技术，其中两个或者更多方共享同一个密钥并且不但使用这个密钥的加密形式还使用它的解密形式。该密钥必须是秘密的，因为任何得到它的人都能够用这个密钥把所有加密的信息解密出来，或者用它加入未经授权的信息。

b） 公共密钥技术，其中每个用户有一个密钥对：一个公共密钥（可以展示给任何人）和一个私人密钥（必须保密）。公共密钥技术能够用在加密上（见 10.3.2）也能够用于生成数字签名（见 10.3.3）。

所有的密钥应当得到保护，以防被修改或者破坏。而且秘密和私有密钥要防止未经授权的泄露。密码技术也可以用于这个目的。应当从物理上保护那些用于生成密钥、存储密钥和将其存档的设备。

10.3.5.2 标准、程序和方法

一个密钥管理系统应当基于共同的标准、程序和安全方法的集合，它们用于：

a） 为不同的密码系统和不同的应用软件生成密钥；

b） 生成和获取公共密钥证明；

c） 把密钥分发给需要的用户，包括接到密钥时应当怎样将其激活。

d） 存储密钥，包括经授权的用户怎样得到密钥；
e） 更改或者更新密钥，包括关于何时应该改变密钥和怎样改变的一些规则；
f） 处理受损的密钥；
g） 激活密钥，包括应当怎样将密钥撤出或者使其失效，例如密钥在何时被损害或者用户在何时离开了组织（在此种情况下密钥也应当被存档）；
h） 作为业务连续性管理的一部分，恢复丢失的或者毁坏的密钥。例如加密信息的恢复。
i） 存档密钥，例如用于信息存档或者备份；
j） 销毁密钥；
k） 密钥管理相关活动的记录和查验。

为了减少损害的可能性，密钥应当有确定的激活和休止日期，从而它们只能在有限的时间段内使用。该时间段的长度应当取决于运用密码管理措施的环境和所发现的风险。
为了处理访问密码关键字的法律要求，需要考虑一些程序。例如，可能需要用加密信息的解密形式做法庭上的证据。

除了安全管理的秘密和私人密钥的话题之外，还应当考虑公共密钥。有的人用自己密钥替代公共密钥来伪造数字签名，可能有这种威胁存在。这一问题可由使用公共密钥证明的方法来解决。这些证明文件应当以一种把与公共密钥/私有密钥的所有人相关的信息同公共密钥唯一地连续在一起。因此生成这些证明文件的管理过程要值得信赖，这一点很重要。该过程通常由一个权威验证机构来执行，该机构有适当的管理和控制措施提供所需的置信度。

服务等级管理的内容或者与外部密码服务供应商所签订合同的内容，例如与一个权威验证机构所签合同，应当包括有关责任、服务的可靠性和提供服务的响应时间等议题（见 4.2.2）。

10.4 信息文件的安全

目标：确保 IT 项目和支持行为以安全的方式进行。应当控制对系统文件的访问。
维护信息的完整性应当是应用程序系统或者软件所属的用户功能或者开发群体的责任。

10.4.1 操作软件的控制

应当为在操作系统中使用软件提供管理措施。为了把操作系统溃掉的风险降到最低，应当考虑一些的管理措施：

a） 操作系统程序库的更新应当只由指定的程序库管理员根据适当的管理层授权来执行（见 10.4.3）；
b） 如果可能的话，操作系统应当只包涵可执行代码；
c） 获得测试成功和用户被接受的证据之前，以及在相应的程序资料库更新之前，不能在操作系统中运行可执行代码。
d） 应当维护对层次系统程序库的所有更新的审查日志；
e） 应当保留软件的以前版本做为应急之用。

操作系统中使用的由销售商提供的软件应当维护在一个由该供应商支持的水平之上。任何升级到新版本的决定都应当考虑到该版本的安全，比如新安全功能的引入或者影响该版本的安全问题的数量和严重性。当软件补丁能够帮助消除或者减少安全缺陷的时候，就应当使用他它们。

对操作系统进行的物理或者逻辑访问应当只是在需要的时候出于技术支持的目的而授予供应商的，而且还需要得到管理层批准。应当监视供应商的活动。

10.4.2 系统测试数据的保护

应当保护并控制测试数据。系统和验收试验通常需要大量的尽可能与靠近际运行数据的测试数据。应当避免使用含有个人信息的业务数据库。如果要使用其中信息，在用之前应当使其失去个性化。当把运行数据用于测试目的时，应当采取以下措施保护运行数据。

a) 访问控制程序，它可以用于应用操作系统.也可以用于测试应用系统。
b) 每次把运行信息复制到测试应用系统都应当有单独的授权。
c) 测试完成之后，应当立即把运行信息从测试应用系统中删除。
d) 应当记录运行信息的复制和使用，以提供一种检查追踪。

10.4.3 对程序资源库的访问控制

为降低计算机程序溃掉的可能性，在对程序资源库的访问中应当保持如下所述的严格管理措施。

a) 可能的情况下，程序资源库不应当放在操作系统中；
b) 应当为每个程序指定一名程序资源库管理员；
c) IT 技术支持人员不应当对程序资源库不加限制地访问；
d) 正在开发的程序和正在维护的程序不应当放在程序资源库中；
e) 程序资源库的升级和程序资源向程序员的发布应当只由指派的程序资源库管理员根据授权从应用程序的 IT 技术支持经理那里进行；
f) 程序列表应当放在安全的环境中(见 8.6.4)。
g) 应当保留一份对程序资源库所有访问的审查日志。
h) 老版本的程序资料应当存档，清楚标明它们运行的准确日期和时间，以及所有支持软件、作业控制、数据定义和程序。
i) 程序资源库的维护和复制应当服从严格的变更管理程序（见 10.4.1）。

10.5 开发和支持过程中的安全

目标：维持应用程序系统软件和信息的安全。

应当严格控制项目和支持环境。
应用程序系统的负责主管也应当负责项目或者支持环境的安全。它们应当确保所有建议的系统变更都经过复查以验证它们不会损害系统或者运行环境的安全。

10.5.1 变更控制程序

为了降低信息系统溃掉的危险，对变更的实施应当有严格的管理措施。正式的变更管理程序应当得到加强。它们应当确保安全并且控制程序不会受到损害，确保技术支持程序员只被授予访问他们工作所必须接触的部分系统内容，并且保证所有变更都得到了的正式同意和批准。改变应用程序软件可能对运行环境产生冲击。如果合适的话，应用程序和运行变更程序应当集成到一起（见 8.1.2）。该过程应当包括：

a） 保持一份同意授权等级的记录；
b） 确保变更是由授权的用户提交的；
c） 复查控制和集成程序以确保它们不会被变更所损害；
d） 识别所有计算机软件、信息、数据库物理和需要维修的硬件；
e） 在工作开始之前得到对详细建议的赞同；
f） 确保授权的用户在任何执行之前接受改变；
g） 确保过程的执行会把业务分裂降低到最小的程度；
h） 确保每次变更完成之后更新系统文献集合并且把旧的文献存档或者进行处置；
i） 为所有软件更新维持一个版本管理；
j） 保持对所有变更要求的审查追踪；
k） 确保运行文件（见 8.1.1）和用户程序的改变必须得当；
l） 确保在正确的时候做出变更而且没有扰乱相关的业务过程。

许多组织维护一个环境，用户在其中检测新软件并且该环境与开发和生成环境相互分离。这就提供了一种控制管理新软件的方式并且允许对用于测试的运行信息的给以额外保护。

10.5.2 操作系统变更的技术复查

需要定期改变操作系统，例如安装新提供的软件版本或者补丁程序。当发生改变时，应当复查并测试应用程序系统以确保对运行或者安全没有负作用。该程序应当包括：

a) 复查应用程序控制措施和完整性程序以确保它们没有受到操作系统改变的损害；
b) 确保手动支持计划和预算会保护由操作系统变更引起的复查和系统测试；
c) 确保及时提供操作系统变更的通知，从而允许在执行之前进行适当的复查；
d) 确保对业务连续性计划做了适当改变（见句 1）。

10.5.3 改变软件包的限制

应当阻止修改软件包。只要可能，而且也可行，应当不加任何修改地使用卖方供应的软件包。如果认为必须对软件包进行改动，应当考虑以下各点：

a） 受损的内置控制措施和集成程序的风险；
b） 是否得到了供应商的许可；
c） 从供应商那里得到所需变更作为标准程序更新的可能性；
d） 如果因为软件包变更而要组织为软件未来的维护承担责任，有怎样的影响。

如果认为必须做改动，那么应当保留原始软件和对一个清楚定义的副本所做的改动。应当对所有的改动充分测试并记录在案，因此如果将来软件升级需要，就能重新应用它们。

10.5.4 隐蔽通道和特洛伊代码（渗透性代码）

隐蔽的通道可能由一些间接的和隐晦的方式披露信息。 改变一个计算系统的安全元素和不安全元素都可以访问的参数，或者把信息嵌入一个数据流中，就可以激活这一隐蔽通道。渗透性代码是要以一种未经授权、没被注意并且应用程序的接收方或者用户不需要方式和的方式影响系统。隐蔽通道和渗透性代码的出现很少是偶然的。关注隐蔽通道或渗透性代码时，应当考虑一些几点：

a) 只从有声誉的来源购买程序软件；
b) 购买程序的源代码以便进行修改；
c) 使用评价过的产品;
d) 在运行之前检查所有源代码；
e) 控制访问和修改已经安装了的程序代码；
f) 在关键系统的工作中用已经证明是可以信赖的职工；

10.5.5 外购软件开发

如果软件开发是外购的，应当考虑以下几点：

a） 对安排、代码所有权和知识产权发证照（见 12.1.2）；
b） 对所做工作的质量和准确性的验证；
c） 第三方出现故障时对由其保存的附带条件委托契约的安排；
d） 查验已完成工作的质量和准确性所需访问权；
e） 合同对代码质量的要求；
f） 在安装之前检测特洛伊代码（渗透性代码）；

11 业务连续性管理

11.1 业务连续性管理的几个方面

目标：抵消业务活动受到干扰的影响，并防止关键业务处理受大的故障或者灾难的影响

应当执行业务连续性管理程序，通过预防性和恢复性措施的结合，把灾难或者安全事故（例如可能由于自然灾害、突发事件、设备故障和故意的行为）所导致的破坏减少到一个可以接受的水平。
应当对灾难事故、安全故障和服务损失所造成的结果进行分析。应当制订并实施紧急事件处理计划以确保商务处理能够在要求的时间范围内得到恢复。应当保持这种计划并在实践中将其变成所有其它管理程序所构成整体的一部分。
业务连续性管理应当包括相关的管理测试来识别并减少风险、限制毁灭性事故的后果、确保能够及时恢复基本运行。

11.1.1 业务连续性管理程序

为了在整个组织内部发展和保持业务连续性，应当有适当的管理程序。它应当把以下业务连续性管理的关键要素集合在一起。

a) 理解组织正在面临的风险，它们发生的可能性和影响，包括识别关键商务处理程序并区分其优先次序；
b) 理解干扰可能对业务产生的影响（不但要有处理小事故的解决方案还要找到处理那些能够威胁组织运转的严重事故的方法，这一点非常重要），确立信息处理设备的经营目标；
c) 考虑购买适当的保险，这可以作为业务连续性程序的一部分；
d) 阐明并记录一个与已经确立的经营目标和经营优势相符的业务连续性计划；
e) 阐明并记录符合协商一致的策略的业务连续性计划；
f) 对所用计划和处理程序进行定期测试和更新；
g) 确保业务连续性计划的管理成为组织的处理程序和结构的一部分。应当在适当的层次上把协调业务连续性管理程序的责任在组织内部进行分派，例如在信息安全论坛上（见 4.1.1）。

11.1.2 业务连续性和影响分析

业务连续性始于辨别那些能够扰乱商务处理进程的事件，例如设备故障、水灾和火灾。接下来进行风险评估以确定这些干扰的影响（就破坏的规模和恢复周期而言）。这些活动应当有商务资源和处理程序的所有者的充分参与。评估考虑的是所有的商务处理程序，并不只是限于信息处理设备。

根据风险评估的结果，应当制订一个战略计划以全面应对业务连续性问题。 一旦该计划制订完毕，应当由管理层签字。

11.1.3 编写和执行连续性计划

应当制订计划，以便关键商务处理程序的受干扰或者发生故障后，能够在要求的时间范围内维持或者恢复经营活动。该业务连续性计划处理程序应当考虑以下方面：

a） 确认并同意所有的责任分配和紧急事故处理程序；
b） 执行紧急事故处理程序，在要求的时间范围内进行恢复和更新。应当特别注意对外部业务活动的依赖性和所签合同所做的评估。
c） 将同意的程序和过程记录在案；
d） 对批准的紧急事故处理程序中的人员包括危急管理人员进行适当教育。
e） 测试并更新计划。

该计划处理程序应当专注于要求的经营目标，例如在可接受的时间长度内恢复对客户的特殊服务。应当注意可能发生这种情况的服务和资源，包括人员提供、非信息处理资源等，还有信息处理设备的撤退安排。

11.1.4 业务连续性计划框架

应当保持单一的业务连续性计划框架，确保所有的计划相一致并且便于在测试和维护时识别优先级。每个业务连续性计划都清楚地指定了激活条件（启动条件），以及执行计划的各个部分时每个人所应承担的责任。确定了新要求时，应当适当地对已经建立的解决事件处理程序例如清空计划或者任何现有的回撤安排做修改。

一个业务连续性计划框架应当考虑以下几个方面：

a） 计划启动之前该计划要求的激活条件。它描述了后续程序（如何评估形势，确定要涉及到谁等等）；
b） 紧急事件处理程序。它描述了一个危及业务运营和/或者人员生命的事故发生后所要采取的步骤。它应当安排公共关系管理措施并设法与权威公共机构比如警察局、消防局和当地政府建立有效联络；
c） 撤退程序。它描述了把基本经营活动或者配套服务转移到临时替代地点的相关行动，并在要求的时间范围内恢复商务处理。
d） 恢复程序。它描述了恢复正常业务运行所要做的行动。
e） 维修计划。它规定了何时以何种方式对业务连续性计划进行测试，以及该连续性计划的维护方法。
f） 知情和教育活动。它们用于加深对业务连续性处理程序的理解，确保该处理持续有效；
g） 个人的责任。描述了谁负责执行该连续性计划的哪个部分。应当按照要求指定替代人员。

每个计划都要有专门的所有人。紧急事故处理程序、人工撤退计划和恢复计划应当由所涉及的适当业务资源或者处理方法的所有权人承担责任。替代技术服务例如信息处理和通信设备的撤退安排通常由服务提供商负责。

11.1.5 测试、维护和重新评估业务连续性计划

11.1.5.1 测试此项计划

被测试的业务连续性计划可能出现故障，这常常是因为不正确的假设条件、粗心大意或者设备或人员的变更。因此要定期对其进行测试，以确保它们是最新的和有效的。这种测试还应当确保计划恢复队伍的所有成员和其它相关职工知道此项计划。

业务连续性计划的测试安排应当指出在何时以怎样的方式检测该计划的各个元素。建议经常测试计划中的独立成分。为确保该计划能够在实际生活中运作，应当采用多种多样的技术措施。它们包括：

a） 对各种脚本的桌面测试 (使用干扰例子来讨论业务恢复安排)；
b） 模拟（特别用于训练负责事故/危急事后管理的人员）；
c） 技术恢复测试(确保信息系统能够有效恢复)；
d） 在不同地点测试恢复效果（在远离主基地的地方执行恢复作业的同时，运行商务处理程序）；
e） 对供应商设备和服务的测试（确保外部提供的服务和产品满足合同约定的要求）；
f） 完全排演（全面测试组织、员工、设备、方便措施以及应对干扰的程序）；

所有的组织都可以使用这些方法，而它们应当反映特殊恢复计划的性质。

11.1.5.2 维护并重新评估此项计划

应当通过定期检查和定期更新来维护该业务连续性计划，以确保它们的有效性（见 11.1.5.1 到 11.1.5.3）。这些手续应当包括在组织的变更管理程序中，以确保业务连续性问题得到正确的解决。

应当为每个业务连续性计划的定期检查分配责任；尚未反映在业务连续性计划中的营运安排的鉴定应当接续有对该计划的适当更新。这个正式的变更管理程序应当确保通过对整个计划的复查来分发和加强更新后的计划。

可能需要更新计划的情况包括有了新设备、操作系统升级了或者下述因素发生改变：

a） 人员；
b） 地址和电话号码；
c） 运营战略；
d） 地点、设备和资源；
e） 立法；
f） 签约方、供货商和主要客户；
g） 处理程序，或者加入了新程序/撤销了旧程序；

h） 风险（运行风险和金融风险）。

12 符合性

12.1 符合法律要求

目标：避免违犯任何刑法和民法、法定的或者合同约定的义务，避免破坏如何安全要求。

信息系统的设计、运行、使用和管理可能要置于法律规定的和合同约定的安全要求的约束之下。
应当从组织的法律顾问或者合适的权威法律执业人士那里寻求有关特殊法律规定的建议。各个国家对从一个国家产生又被传送到另一个国家的信息（例如过境的数据流）有不同的法律要求不同。

12.1.1 适用法律的辨别

对每个信息系统，都应当清楚地定义所有相关的法律规定和合同约定的要求并将其记录在案。应当类似地定义专门管理措施和个人的责任以满足这些要求，并且把它们记录在案。

12.1.2 知识产权(IPR)

12.1.2.1 著作权（版权）

应当采用适当的程序确保使用可能有知识产权例如著作权、设计权、商标等的材料时符合法律规定的要求。侵害著作权可能导致法律诉讼从而卷入犯罪调查中。

法律规定和合同约定的要求可能限制复制享有著作权的资料。尤其是，它们要求只有由该组织开发的或者由开发者授权或提供的资料才能够使用。

12.1.2.2 软件版权

私有的软件产品通常在一份授权协议的准许下提供。该协议把对此产品的使用限制在特定的机器上并且可能把复制权仅仅限制在制作备份上。应当考虑以下的措施：

a） 公布一个软件版权符合策略，其中定义了对软件和信息产品的法定使用。
b） 发布获得软件产品的程序的标准。
c） 对软件版权和获得策略的保持清醒认识，并注意用规章制度防止职员的破坏它们的企图。
d） 保留适当的资产注册人员；
e） 保留所有权证书、母盘、手册等的证明文件和资料。
f） 执行管理措施以确保不超过允许使用的最大用户人数；
g） 检查是否只安装了授权的软件和得到许可的产品；
h） 提供一种保持合适授权条件的策略；
i） 提供一种处理或者向他人传送软件的策略方法；
j） 使用适当的审查工具；
k） 遵守从公众网获得的软件和信息的条款规定（见 8.7.6）。

12.1.3 保护组织记录

应当防止一个组织的重要记录被丢失、损坏和篡改。有的记录可能需要安全存放，以满足法律法规的要求、支撑基本的商业活动、确保有足够的防范潜在民事和刑事破坏行为的能力或者向股东、合伙人和审计人员确认组织的财务状况。信息保留的时间长短和数据内容可能有国家的法律规定。

应当把记录分类，例如会计记录、数据库记录、交易日志（备忘录）、审查备忘录和运行程序手册。 每种类型的记录都详细记载着保存期限和存储介质种类，例如纸张、缩微胶片、磁性介质、光学介质。 应当安全地保存所有与加密的档案或者数字签名（见 10.3.2 和 10.3.3）相关的密码关键字，并使其得到授权的人在需要时可以使用。

应当考虑存储记录的介质退化变质的可能性。存储和处理方法应当按照制造商的建议进行。

如果选择的是电子存储介质，应当包括确保在整个保存期内访问数据（存储介质和格式的可读性）能力的程序，以防止由于未来技术改变造成的信息丢失。

数据储存系统的选择应当使得所需的数据能够以一种法律可以接受的形式恢复过来，例如需要的所有记录能够在可接受的时间尺度内以一种可以接受的形式得到恢复。

信息存储和处理系统应当确保记录的清晰识别，并能够清楚认定它们的法律或者规定确定的保留期限。 如果在这个保留期限之后组织不再需要这些记录了，应当允许记录有适度的损坏。

为了满足这些要求，应当在组织内部采取以下步骤：

a） 应当发布有关记录和信息保留、储存和处理的规定。
b） 应当制订保留计划，确认基本的记录类型和它们应当保留的时期。
c） 应当保有一份关键信息资源的财产清单。
d） 应当执行适当的管理措施以防止基础性的记录和信息被丢失、毁坏和篡改。

12.1.4 数据保护和个人信息的保密

有些国家已经引入立法对个人信息（能够将活着的个体区分开的信息）的处理和传送进行管理。这些管理措施可能使得那些收集、处理和散发个人信息的人承担了责任并且可能限制把这些数据向其它国家传送的能力。

符合数据保护法律的要求需要适当的管理结构和控制措施。这一点常常可以通过任命一个数据保护官员得到最好的解决，该官员应当向经理、客户和服务提供商就他们个人的责任和应当遵守的特殊程序来提供指导性意见。应当以一种结构化的文件形式保护个人信息并确保清楚相关法律中规定的数据保护原则，向数据保护官员提供任何关于这些的建议应当是数据所有权人的责任。

12.1.5 防止信息处理设备的误用

组织的信息处理设备是用于商业目的的。管理层应当对它们的使用进行授权。任何将这些设备用于非业务目的或者未经授权即没有管理层同意的目的的做法应当看作是对设备使用不当。如果这样的行为通过检测或者其它方式得到确认，应当引起该独立经理的注意，需要考虑给以适当的训诫。

监测设备使用情况的合法性在各个国家不同，而且可能需要建议雇员采用这种监测或者得到他们的同意。在执行检测措施之前应当听取法律建议。

很多国家已经有或者正在引进法律来防止滥用计算机。把计算机用于未经授权的目的可能构成犯罪。因此所有用户要清楚允许他们访问的准确范围，这一点是非常基本的。例如，通过给予用户书面授权，可以实行这一点。其中书面授权要由用户签字并由组织安全的加以保管。应当警告组织的雇员和第三方用户不要进行授权范围以外的访问。

在登录时，应当在计算机屏幕上显示一条警告信息，指出所进入的系统是私有的（秘密的）并且不允许进行未经授权的访问。用户必须承认屏幕上的信息并适当地做出回复以继续其登录过程。

12.1.6 密码管理的规定

有的国家已经实施了一些协定、法律、规定或者其它文书以控制对密码管理措施的访问和使用。这些措施可能包括：

a） 执行加密功能的计算机硬件和软件的进口和/或者出口；
b） 附带有密码功能的计算机硬件和软件的进口和/或者出口；
c） 国家访问由带有加密功能的硬件或者软件加密的信息时使用的强制或者自愿方法。

应当征求法律建议，确保符合国家法律。在把加密信息转移到境外之前，也要征求法律建议。

12.1.7 证据的搜集

12.1.7.1 证据的规定

要支持一项针对某个人或者组织的诉讼，有充足的证据是非常重要的。只要该诉讼是内部违纪事件，就需要由内部程序提供必要的证据。

如果该诉讼涉及法律，无论是民法还是刑法，所出示的证据都应当符合相关法律或者将要审理该案件的特殊法庭对证据的规定和要求。一般说来，这些规定包括：

a） 证据的可采纳性：该证据是否能够用于法庭；
b） 证据的分量：证据的质量和完备性；
c） 有足够的证据表明，在所要恢复的证据被此系统保存和处理的整个时期内，该证据管理措施的执行都是正确的和持续的。

12.1.7.2 证据的可采纳性

为了使证据能够被采纳，组织应当确保它们的信息系统遵循所有发布的有关取得可采纳证据的标准或者规定。

12.1.7.3 证据的质量和完备性

为了提供证据质量并确保其完备性，需要强有力的证据追踪。 一般说来，可以在下述条件下建立起这种证据追踪。

a) 对纸形文件：安全地保存原件，并记录下是谁发现的、在哪里发现的、什么时候发

现的和谁见证了这一发现。所有的调查取证都要确保不毁坏原件；

b) 对计算机存储的信息：应当确保任何可移动存储介质的备份、在硬盘或者内存中的信息是可以使用的。应当保存对复制过程中所有操作的记录，而且应当对该过程进行公证。该存储媒介和相应记录的一个备份应当得到安全的保存。

在首次发现事故的时候，可能并不清楚它有导致法律诉讼的可能性。因此，危险在于意识到事故的严重性之前必要的证据就被意外地毁掉了。在准备采取的任何法律行动中让律师和警察早些介入并听取他们对所需证据的建议，这是非常明智的。

12.2 安全策略和技术符合性的检查

目标：确保信息符合组织安全策略和标准。

应当定期检查信息系统的安全。
这种检查应当针对适当的安全策略，并且应当审查技术平台和信息系统是否符合安全运行标准。

12.2.1 符合安全策略

管理人员应当确保在他们责任范围内的所有安全程序都得到了正确的执行。另外，应当考虑在组织的所有范围内都进行定期检查，确保符合安全策略和标准。这些范围应当包括：

a） 信息系统；
b） 系统提供商；
c） 信息和信息资产的所有人；
d） 用户；
e） 管理层；

信息系统的所有权人（见 5.1）应当支持对他们系统进行定期检查，看是否符合适当的安全策略、标准和任何其它安全要求。系统使用的运行监测参见 9.7。

12.2.2 技术符合性检测

应当定期检查信息系统是否符合安全运行标准。技术符合性检测涉及对操作系统的测试，以确保正确地执行了硬件和软件管理措施。这种符合性检测要求专家的技术支持。应当由一位有经验的系统工程师亲手（如果需要的话，可用适当的软件工具帮助）做这种检测，或者自动软件包执行检测，它可以产生技术报告供技术专家做后续分析。

符合性检测还包括，比如，贯入试验，它可由为此而专门签约邀请的独立专家来做。 对于发现系统弱点和检测管理措施在防范由于这些弱点而造成的未经授权的访问时的有效性，这种试验是有用的。应加倍小心，防止贯入试验的成功可能导致系统安全性受损并在无意中制

造了其它弱点。

任何技术符合性检测都只能由能够胜任的权威人士亲自完成，或者受到他们的监督。

12.3 系统审查相关事项

目的：将系统审查程序的有效性最大化并把对该程序的干扰降到最低限度。

在系统审查期间，应当有管理措施来保护操作系统和审查工具。
还需要保护审查工具的完整性并防止滥用审查工具。

12.3.1 系统审查管理程序

涉及检测操作系统的审查要求和活动应当仔细地策划并得到同意，以把打断商务处理程序的风险降到最低。应当遵循以下几点：

a） 审查要求应当得到适当管理层的同意；
b） 审查的范围获得批准并得到控制；
c） 审查应当被限制在对软件和数据的只读访问的层次；
d） 只允许对独立的系统文件备份做只读以外的访问。在审查结束之后应当把备份文件删除。
e） 应当明确地确定执行审查的 IT 资源，并使其可以利用。
f） 应当辨别并同意特殊或者附加处理的要求。
g） 所有的访问都要受到监视并被记录下来以做一份参考跟踪文件。
h） 所有的程序、要求和责任都应当记录在案。

12.3.2 系统审查工具的保护

应当保护对系统审查工具例如软件或者数据文件的访问途径，防止任何可能的误用或者损坏。这种工具应当从开发系统和操作系统中分离出来，并且不应当放在录音资料馆或者用户活动区，除非有适当等级的附加保护措施。

索引

验收，系统验收 8.2.2
访问控制 9
    应用程序的访问控制 9.6
    应用程序的访问控制 9.1
    操作系统的访问控制 9.5
    访问控制策略 9.1.1
    程序资源库的访问控制 10.4.3
访问限制，信息访问限制 9.6.1
资产的可计量性 5.1
信息安全责任的分配 4.1.3
管理措施的实用性－引言
应用程序访问控制 9.6
应用程序系统，…的安全 10.2
    安全区域 7.1
    在安全区域工作 7.1.4
评估你的安全发现－引言
风险评估 2.2
资产分类和管理 5
审查
    审查的相关事项 12.3
    日志（记录）9.7.1
    记录工具，对日志的保护 12.3.2
鉴别
    文电鉴别 10.2.3
    节点鉴别 9.4.4
    用户鉴别 9.4.3
授权程序 4.1.4
自动终端识别 9.5.1
有效性 2.1
信息的备份 8.4.1
业务连续性 11
    业务连续性框架 11.1.4
    业务连续性影响分析 11.2
    业务连续性的管理 11
    业务连续性的管理程序 11.
    业务连续性的测试、维护和重新评估计划 11.1.5
    编写和执行业务连续性计划 11.1.3

访问控制的业务要求 9.1
接线安全 7.3.2
容量规划 8.2.1
证明 10.3.5.2
变更管理
    运营的变更管理 8.1.2
    变更管理的程序 10.5.1
分类
    资产分类 5
    指导方针分类 5.2.1
    信息分类 5.2
清洁桌面和清洁屏幕策略 7.3.1
时钟同步 9.7.3
证据的收集 12.1.7
组织间的合作 4.1.6
通信和运营管理 8
符合
    符合法律要求 12.1
    符合安全策略 12.2.1
保密性 2.1
保密性要求 6.1.3
用工合同条款 6.1.4
合同
    第三方合同安全 4.2.2
    外购合同安全 4.3.1
控制
    控制恶意软件 8.3.1
    内部处理程序的控制 10.2.2
    业务软件的控制 10.4.1
管理措施，一般性的，物理上的 7.3
著作权、产权
    知识产权 IPR 12.1.2.1
    软件著作权 12.1.2.2
隐蔽通道和渗透性代码 10.5.4
关键成功因素－引言
密码管理 10.3
    密码管理的使用策略 10.3.1
    密码管理的规定 10.3.2
发送和装载区域 7.1.5
制订你自己的方针，引言
开发
    系统的开发和维护 10
    开发和操作设备的分离 8.1.5
    开发和支持环境的安全 10.5

数字签名 10.3.3
惩戒程序 6.3.5
处置
    设备处置 7.2.6
    存储介质处置 8.6.2
文档, 系统文档的安全 8.6.4
记录在案的操作程序 8.1.1
信息和软件的下载 8.1.3，8.7.4，10.2.2
强制警告 9.5.6
信息安全教育和培训 6.2.1
电子的
    电子商务 8.7.3
    电子邮件 8.7.4
    电子办公系统 8.7.5
应急操作步骤 11.1.3
加密 10.3.2
强制路径 9.4.2
登录控制 7.1.2
环境和物理安全 7
设备
    设备维护 7.2.4
    设备安全 7.2
    设备定位和保护 7.2.1
    无人值守设备 9.3.2
用过的前提 5.2.5
确立安全要求－引言
安全策略的评价和回顾 3.1.2
事件记录 9.7.1
证据，证据收集 12.1.7
交换
    信息交换，其它交换形式 8.7.7
    信息和软件的交换 8.7
    信息和软件的交换，交换协议 8.7.1
外部设施管理 8.1.6
设施管理，外部设施管理 8.1.6
设施，办公安全，房间和 7.1.3
撤退计划 11.1.3
故障记录 8.4.3
信息交换形式，其它信息交换形式 8.7.7
业务连续性计划框架 11.1.4
总的实物管理措施 7.3
指定原则－引言
风险， 设备保护 7.2.1
在家工作

设备安全 7.2.5
远程工作安全 9.8.2
内务处理 8.4
适用法律的识别 12.1.1
终端识别 9.5.1
用户识别 9.5.3
意外事故
吸取意外事故教训 6.3.4
意外事故管理方法 8.1.3
意外事故报告 6.3.1
意外事故和故障，意外事故和故障的报告 6.3
独立的信息安全检查 4.1.7
信息
信息访问，控制对信息的访问 9.6.1
信息备份 8.4.1
信息分类 5.2
其它形式的信息交换 8.7.7
信息处理程序 8.6.3
标识和处理 5.2.2
信息和软件，…的交换 8.7
信息和软件交换协议 8.7.1
信息安全 2.1
信息安全协作 4.12
信息安全教育和培训 6.2.1
基本架构 4.1
基本架构策略 3.1
基本架构的策略记录 3.1
基本架构的要求－引言
输入数据验证 10.2.1
完整性 2.1
知识产权（IPR）12.1.2
内务处理，内务处理控制 10.2.2
资产清单 5.1.1
被隔离的发送和装载区域 7.1.5
敏感系统的隔离 9.6.2
工作定义和资源 6.1
工作责任，安全 6.1.1
密钥管理 10.3.5
信息的标识和处理 5.2.2
吸取事故教训 6.3.4
连接时间限制 9.5.8
记录
事件记录 9.7.1
故障记录 8.4.3

登录程序 9.5.2
日志，操作员日志 8.4.2
故障，故障报告 6.3.3
恶意软件
    控制恶意软件 8.3.1
    防止恶意软件 8.3
管理
    管理的通信和运作 8
    信息安全管理论坛 4.1.1
    网络管理 8.5
    可移动计算机存储介质的管理 8.6.1
    风险管理 2.3
    用户访问管理 9.2
存储介质
    存储介质的处置 8.6.2
    存储介质的处理和安全 8.6
    存储介质的运输 8.7.2
    可移动的存储介质 8.6.1
文电鉴别 10.2.3
信息处理设施的误用 12.1.5
移动计算 9.8.1
移动计算和远程工作 9.8
监测
    系统访问和使用 9.7
    系统使用 9.7.2
网络
    网络访问控制 9.4
    连接控制 9.4.7
    管理 8.5
    路径选择控制 9.4.8
    网络分离 9.4.6
节点鉴别 9.4.4
保密协议 6.1.3
非拒绝服务 10.3.4
办公系统，电子 8.7.5
办公室，房间和设施，保卫 7.1.3
操作、运营、运行
    操作程序 8.1.1
    操作系统访问控制 9.5
操作的、运行的、运营的
    操作变更控制 8.1.2
    运行程序和责任 8.1
    运行软件，控制 10.4.1
运营和通信管理 8

操作员日志 8.4.2
组织安全 4
组织的记录，保卫 12.1.3
信息交换的其它形式 8.7.7
输出数据验证 10.4.2
外购 4.3
    外购软件开发 10.5.5
    外购合同的安全 4.3.1
密码
    密码管理，用户 9.2.3
    密码管理系统 9.5.4
    密码使用 9.3.1
个人信息，保密 12.1.4
人员筛选和策略 6.1.2
人员安全 6
物理的
    物理和环境安全 7
    登录安全 7.1.2
    安全边界（范围）7.1.1
策略
    访问控制策略 9.1
    密码管理的使用策略 10.3.1
    网络服务的使用策略 9.4.1
    安全策略 3
电力供应安全 7.2.2
防止信息处理设施的误用 12.1.5
特权管理 9.2.2
程序资源库，访问控制 10.4.3
产权，知识产权 12.1.2
保护
    保护设备免于灾难 7.2
    防止恶意软件 8.3
    系统审查工具的保护 12.3.2
    系统测试数据的保护 10.4.2
公众可用的系统 8.7.6
远程诊断接口保护 9.4.5
财产的移动 7.3.2
报告
    安全事故 6.3.1
    安全弱点 6.3.2
    软件故障 6.3.3
安全策略的复查和评价 3.1.2
安全要求－引言
对事故做出反应 6.3

责任
    工作中的安全责任 6.1.1
    用户责任 9.3
对改动软件包的约束 10.5.3
复查
    信息安全 4.1.7
    用户访问权限 9.2.4
风险评估 2.2
风险管理 2.3
路径选择控制 9.4.8
组织记录的安全 12.1.3
范围 1
安全区域 7.1
    安全区域内设备的处置 7.2.6
    在安全区域内工作 7.1.4
保护办公室，房间和设施 7.1.3
安全
    应用软件系统的安全 10.2
    开发和支持程序的安全 10.5
    安全教育 6.2.1
    电子商务安全 8.7.3
    电子邮件安全 8.7.4
    电子办公安全 8.7.5
    安全事故 6.3，6.3.1
    存储介质传送过程中的安全 8.7.2
    组织安全 4
    安全策略 3
    安全策略，符合 12.2.1
    安全需求分析 10.1.1
    外购合同的安全要求 4.3.1
    第三方合同的安全要求 4.2
    系统的安全要求 10.1
    信息处理设备的安全检查 12.2
    系统文档的安全　8.6.4
    系统文件的安全　10.3
    第三方访问的安全 4.2
    安全弱点，报告安全弱点 6.3.2
隔离
    责任的隔离 8.1.4
    网络隔离 9.4.6
敏感系统隔离 9.6.2
开发和运行设施的分离 8.1.5
设备定位　7.2.1
软件

软件的复制
软件故障 12.1.2.1
恶意软件，免受恶意软件危害 6.3
软件的操作控制 10.4.1
软件包，软件包改动的限制 10.5.3
源程序库访问控制 10.4.3
信息安全专家的建议 4.1.5
时钟同步 9.7.3
系统
系统审查相关事项 12.3
系统审查管理措施 12.1.3
系统开发和维护 10
系统文档 8.6.4
系统文件，系统文件的安全 10.3
系统规划和验收 8.2
敏感系统，敏感系统的隔离 9.6.2
测试数据，测试数据的保护 10.4.2
技术
技术符合性检测 12.2.2
操作系统改动的技术复查 10.5.2
远程工作 9.8.2
终端
终端识别 9.5.1
终端登录程序 9.5.2
超时 9.5.7
用工合同条款 6.1.4
测试
测试数据，测试数据的保护 10.4.2
测试、维护和重新评估业务连续性计划 11.1.5
第三方
第三方访问 4.2
第三方风险识别 4.2.1
第三方培训 6.2.1
渗透性编码和隐蔽通道 10.5.4
无人值守的用户设备 9.3.2
用户
用户访问
用户管理 9.2
用户权限，用户权限复查 9.2.4
用户标识 9.2.1
用户识别 9.5.3
用户密码管理 9.2.3
用户注册 9.2.1
用户责任 9.3

用户培训 6.2
验证
验证输入数据 10.2.1
验证输出数据 10.2.3
病毒控制 8.3
工作，在安全区工作 7.1.4