ICS 35.040
L 80

中华人民共和国国家标准

GB/T 19716—2005

信息技术　信息安全管理实用规则

Information technology—Code of practice for information security management

(ISO/IEC 17799:2000,MOD)

2005-04-19 发布　　2005-10-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

前　言

本标准修改采用 ISO/IEC 17799:2000《信息技术 信息安全管理实用规则》(英文版)。

本标准适当做了一些修改:在 12.1.6 中增加了“a) 使用国家主管部门审批的密码算法和密码产品”,作为修改内容。

本标准由中华人民共和国信息产业部提出。

本标准由全国信息安全标准化技术委员会归口。

本标准由中国电子技术标准化研究所、中国电子科技集团第三十研究所、上海三零卫士信息安全有限公司、中国电子科技集团第 15 研究所、北京思乐信息技术有限公司负责起草。

本标准主要起草人:黄家英、林望重、魏忠、林中、王新杰、罗锋盈、陈星。

引　言

什么是信息安全?

像其他重要业务资产一样,信息也是一种资产。它对一个组织具有价值,因此需要加以合适地保护。信息安全防止信息受到的各种威胁,以确保业务连续性,使业务损害减至最小,使投资回报和业务机会最大。

信息可能以各种形式存在。它可以打印或写在纸上、以电子方式存储、用邮寄或电子手段发送、呈现在胶片上或用言语表达。无论信息采用什么形式或者用什么方法存储或共享,都应对它进行适当地保护。

信息安全在此表现为保持下列特征:

a) 保密性:确保信息仅被已授权访问的人访问;

b) 完整性:保护信息及处理方法的准确性和完备性;

c) 可用性:确保已授权用户在需要时可以访问信息和相关资产。

信息安全是通过实现一组合适控制获得的。控制可以是策略、惯例、规程、组织结构和软件功能。需要建立这些控制,以确保满足该组织的特定安全目标。

为什么需要信息安全?

信息和支持过程,系统和网络都是重要的业务资产。信息的保密性、完整性和可用性对维持竞争优势、现金流转、赢利、守法和商业形象可能是必不可少的。

各组织及其信息系统和网络日益面临来自各个方面的安全威胁。这些方面包括计算机辅助欺诈、间谍活动、恶意破坏、毁坏行为、火灾或水灾。诸如计算机病毒、计算机黑客捣乱和拒绝服务攻击,已经变得更普遍、更有野心和日益高科技。

对信息系统和服务的依赖意味着组织对安全威胁更为脆弱。公共网络和专用网络的互连和信息资源的共享增加了实现访问控制的难度。分布式计算的趋势已削弱集中式控制的有效性。

许多信息系统已不再单纯追求设计成安全的,因为通过技术手段可获得的安全性是有限的。应该用合适的管理和规程给予支持。标识哪些控制要到位需要仔细规划并注意细节。信息安全管理至少需要该组织内的所有员工参与,还可能要求供应商、消费者或股票持有人的参与。外界组织的专家建议可能也是需要的。

如果在制定要求规范和设计阶段把信息安全控制结合进去,那么,该信息安全控制就会更加经济和更加有效。

如何建立安全要求

最重要的是组织标识出它的安全要求。有三个主要来源。

第一个来源是由评估该组织的风险所获得的。通过风险评估,标识出对资产的威胁,评价易受威胁的脆弱性和威胁出现的可能性和预测威胁潜在的影响。

第二个来源是组织、贸易伙伴、合同方和服务提供者必须满足的法律、法规、规章和合同的要求。

第三个来源是组织开发支持其运行的信息处理的特定原则、目标和要求的特定集合。

评估安全风险

安全要求是通过安全风险的系统性评估予以标识。用于控制的经费需要针对可能由安全故障导致

的业务损害加以平衡。风险评估技术可适用于整个组织，或仅适用于组织的某些部门，若这样做切实可行、现实和有帮助，该技术也适用于各个信息系统、特定系统部件或服务。

风险评估要系统地考虑以下内容：

a) 可能由安全故障导致的业务损害，要考虑到信息或其他资产的保密性、完整性或可用性丧失的潜在后果；

b) 从最常见的威胁和脆弱性以及当前所实现的控制来看，有出现这样一种故障的现实可能性。

评估的结果将帮助指导和确定合适的管理行动，以及管理信息安全风险和实现所选择控制的优先级，以防范这些风险。评估风险和选择控制的过程可能需要进行许多次，以便涵盖组织的不同部门或各个信息系统。

重要的是对安全风险和已实现的控制进行周期性评审，以便：

a) 考虑业务要求和优先级的变更；

b) 考虑新的威胁和脆弱性；

c) 证实控制仍然维持有效和合适。

根据先前评估的结果评审宜在不同深度级别进行，以及在管理层准备接受的更改风险级别进行。作为高风险区域优化资源的一种手段，风险评估通常首先在高级别进行，然后在更细的级别进行，以提出具体的风险。

选择控制

一旦安全要求已被标识，则应选择并实现控制，以确保风险减少到可接受的程度。控制可以从本标准或其他控制集合中选择，或者当合适时设计新的控制以满足特定需求。有许多不同的管理风险的方法，本标准提供常用方法的若干例子。然而，需要认识到有些控制不适用于每种信息系统或环境，并且不是对所有组织都可行。作为一个例子，8.1.4 描述如何分割责任，以防止欺诈或出错。在较小的组织中分割所有责任是不太可能的，获得相同控制目标的其他方法可能是必要的。作为另一个例子，9.7 和 12.1 描述如何监督系统使用及如何收集证据。所描述的控制，例如事件记录可能与适用的法律相冲突，诸如消费者或在工作场地内的隐私保护。

控制应根据与风险减少相关的实现成本和潜在损失（如果安全违规出现）予以选择。也应考虑诸如丧失信誉等非金钱因素。

本标准中的某些控制可认为是信息安全管理的指导原则，并且可用于大多数组织。下面在题为“信息安全起点”中更详细解释这些控制。

信息安全起点

许多控制可认为是为实现信息安全提供良好起点的指导原则。它们或者是基于重要的法律性要求，或者被认为是信息安全常用的最佳惯例。

从法律的观点看，对某个组织重要的控制包括：

a) 个人信息的数据保护和隐私（见 12.1.4）；

b) 保护组织的记录（见 12.1.3）；

c) 知识产权（见 12.1.2）。

认为是信息安全常用最佳惯例的控制包括：

a) 信息安全策略文档（见 3.1）；

b) 信息安全职责的分配（见 4.1.3）；

c) 信息安全教育和培训（见 6.2.1）；

d) 报告安全事故（见 6.3.1）；

e) 业务连续性管理（见 11.1）。

这些控制适用于大多数组织和环境。应注意，虽然本标准中的所有控制都是重要的，但是从某个组织正面临的特定风险来看，应确定任一控制的贴切性。因此，虽然上述方法被认为是一种良好的起点，但它并不取代选择基于风险评估的控制。

关键的成功因素

经验已经表明下列因素通常对某个组织能否成功实现信息安全是关键的：

a) 反映业务目标安全策略、目的以及活动；
b) 符合组织文化的实现安全的方法；
c) 来自管理层的可视支持和承诺；
d) 正确理解安全要求、风险评估和风险管理；
e) 向所有管理者和员工传达有效的安全需求；
f) 向所有员工和合同商分发关于信息安全策略和标准的指导；
g) 提供合适的培训和教育；
h) 有一个综合和平衡的度量系统，它可用来评估信息安全管理的执行情况以及反馈改进建议。

开发你自己的指南

本实用规则可以认为是开发组织具体指导的起点。本实用规则中的指导和控制并不全都是可用的。而且，可以要求本标准中未包括的附加控制。当发生这种情况时，保持交叉引用可能是有用的，该交叉引用便于审核员和业务方进行符合性检验。

信息技术　信息安全管理实用规则

1　范围

本标准对信息安全管理给出建议，供负责在其组织启动、实施或维护安全的人员使用。本标准为开发组织的安全标准和有效的安全管理做法提供公共基础，并提供组织间交往的信任。本标准的推荐内容应按照适用的我国法律和法规加以选择和使用。

2　术语和定义

下列术语和定义适用于本标准。

2.1

信息安全　Information security

保持信息的保密性、完整性和可用性。

——保密性

确保信息仅被已授权访问的人访问。

——完整性

保护信息及处理方法的准确性和完备性。

——可用性

确保已授权用户在需要时可以访问信息和相关资产。

2.2

风险评估　Risk assessment

对信息和信息处理设施的威胁、影响及信息和信息处理设施自身的脆弱性以及它们出现的可能性的评估。

2.3

风险管理　Risk management

相对可接受的费用而言，标识、控制和尽量减少（或消除）可能影响信息系统的安全风险的过程。

3　安全策略

3.1　信息安全策略

目的：提供管理方向和支持信息安全。

管理层应制定清晰的策略方向，并通过在整个组织中颁发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

策略文件要由管理层批准，当合适时，将其发布并传递给所有员工。策略文档应说明管理承诺，并提出组织的管理信息安全的途径。至少，应包括下列指南：

a）　信息安全定义、其总目标和范围以及在信息共享允许机制下安全的重要性（见引言）；

b）　管理层意图的说明，以支持信息安全的目标和原则；

c）　对组织特别重要的安全策略、原则、标准和符合性要求的简要说明，例如：

1) 服从法律和合同要求；
2) 安全教育要求；
3) 防范和检测病毒和其他恶意软件；
4) 业务连续性管理；
5) 安全策略违反的后果；

d) 安全信息管理(包括报告安全事故)的总职责和特定职责的定义；

e) 引用可以支持策略的文档，例如，特定信息系统的更详细的安全策略和规程，或用户应遵守的安全规则。

应以预期的读者适合的、可访问的和可理解的形式将策略传递给整个组织的用户。

3.1.2 评审和评价

该策略应有专人负责，他按照所定义的评审过程负责其维护和评审。该过程应确保：根据影响原始风险评估基础的任何变更(例如，重大的安全事故、新的脆弱性和随组织上或技术上的基础设施的变更)进行相应的评审。还要安排下列周期性评审：

a) 通过所记录安全事故的性质、数目和影响证明策略的有效性；
b) 控制对业务效率和成本的影响；
c) 技术变更的影响。

4 组织的安全

4.1 信息安全基础设施

目的：管理组织范围内的信息安全。

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。

应建立有管理领导人员参加的相应的管理协调小组，以核准整个组织内的信息安全策略、指派安全角色以及协调安全的实施。若需要，要在组织范围内建立专家信息安全建议原始资料，并在组织内可利用该资料。要发展与外部安全专家的联系，以便跟上行业趋势、跟踪标准和评估方法，并且当涉及安全事故时，提供相适应的联络地点。应鼓励信息安全的多学科途径，例如，涉及诸如保险和风险管理等领域内的管理者、用户、行政管理者、应用设计者、审核员和安全职员以及专业技术熟练工人的合作和协作。

4.1.1 管理信息安全协调小组

信息安全是管理团队所有成员所共同遵守的业务职责。因此，认为管理协调小组能确保安全举措有清晰的方向和看得见的管理层支持。该协调小组要通过合适的承诺和足够的资源来促进组织范围内的安全。该协调小组可以是现有管理团体的一部分。一般，这种协调小组承担下列事项：

a) 评审和核准信息安全策略和总体职责；
b) 监督暴露于主要威胁下的信息资产重大变更；
c) 评审和监督信息安全事故；
d) 批准增强信息安全的重大举措。

由一名管理者负责与安全相关的所有活动。

4.1.2 信息安全协调

在大型组织中，有必要成立一个由各相关部门的管理代表组成的跨部门的协调小组，以协调信息安全控制措施的实施。一般地说，这样的协调小组执行以下方面的工作：

a) 商定整个组织中信息安全的特定角色和职责；
b) 商定信息安全的特定方法和过程，例如，风险评估，安全分类体系；
c) 商定和支持组织范围的信息安全举措，例如，安全意识教育计划；

d) 确保安全是信息规划过程的一部分；

e) 评估新系统或服务的特定信息安全控制的充分程度，并协调实施这些控制；

f) 评审信息安全事故；

g) 促进整个组织信息安全的业务支持的可视性。

4.1.3 信息安全职责的分配

保护各种资产以及进行特定安全处理的职责应予以清晰地定义。

信息安全策略(见第3章)应对组织内的安全角色和职责的分配提供全面指导。若需要，应用特定场地、系统或服务用的更详细的指导予以补充。各个物理及信息资产和安全过程(诸如业务连续性规划)的局部职责应予以清晰的定义。

在许多组织中，将任命一名信息安全管理者全面负责安全的开发和实施，并支持控制的标识。

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信息资产指定一名责任人，因此，他对该信息资产的日常安全负责。

信息资产的责任人可以将他们的安全职责委托给各个管理者或服务提供者。尽管如此，该责任人仍然最终负责该资产的安全，并且他应能确定任何被委托的职责是否已被正确地履行。

重要的是每个管理者负责的领域要予以清晰的规定；特别是，应进行下列工作。

a) 与每个独立系统相关的各种资产和安全过程应予以标识并清晰地定义；

b) 应商定每一资产或安全过程的管理者职责，并且应形成该职责的细节文档；

c) 授权级别应清晰地予以定义，并形成文档。

4.1.4 信息处理设施的授权过程

应建立新信息处理设施的管理授权过程。

理应考虑下列控制：

a) 新设施要有相应用户管理层的批准，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批准，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；

注：对某些连接可以要求型式批准。

c) 应对处理业务信息和所有必要控制所使用的个人信息处理设施进行授权；

d) 使用工作场地内的个人信息处理设施可能引起新的脆弱性，因此，要进行评估和授权。

这些控制在已组成网络的环境中特别重要。

4.1.5 专家的信息安全建议

专家的安全建议可能是许多组织需要的。在概念上，一个有经验的内部信息安全顾问要提供这种建议。不是所有组织都希望聘用专家顾问。在这样的情况下，建议确定专门人员协调内部知识和经验，以确保一致性，并且在作出安全判定时提供帮助。各个组织也应访问适合的外部顾问，顾问们可提供超出各组织自身经验的专家建议。

应对信息安全顾问或上述相应人员分派提供建议的任务，即使用他们自己的或外部的建议来提供关于信息安全各方面的建议。他们评定安全威胁的质量和关于控制的建议将确定该组织的信息安全的有效性。为了最高有效性和最好效果，要允许他们直接访问整个组织中的管理层。

在怀疑发生安全事故或违规之后的最早可能阶段，要咨询信息安全顾问或合同中相应的指定人，以提供专门指导或调查资源的原始资料。虽然大多数内部安全调查将通常在管理控制下进行，但可以要求信息安全顾问对调查提供建议、引导或进行这种调查。

4.1.6 组织之间的合作

要保持与法律执行机构、制订法规的机构、信息服务提供者和电信运营商的相应联系，以确保万一出现安全事故时可以快速采取适当行动并获得建议。同样，要考虑安全团体和行业协调小组的成员。

安全信息的交换要受到限制，以确保不把该组织的保密信息传递给未授权的个人。

4.1.7 信息安全的独立评审

信息安全策略文档(见3.1)提出信息安全策略和职责。其实施要独立地予以评审,以提供保证,即保证组织的实践正确地反映了策略,并且保证该策略是可行的和有效的(见12.2)。

这样的评审可以通过内部审核职能、独立的管理者或专门做这种评审的第三方组织来进行,条件是这些候选者具有相应的技能和经验。

4.2 第三方访问的安全

目的:维护被第三方所访问的组织的信息处理设施和信息资产的安全。

被第三方访问的组织的信息处理设施应予以控制。

若有一种业务需要这种第三方访问,就要进行风险评估,以确定安全蕴涵和控制要求。在与第三方签订的合同中要商定和定义控制。

第三方访问还可能包含其他参与者。给与第三方访问的合同要包括指定其他合格参与者及其访问的条件的许可限度。

本标准可以用作这种合同的基础以及考虑外包信息处理时的基础。

4.2.1 标识第三方访问的风险

4.2.1.1 访问类型

给予第三方的访问类型特别重要。例如,通过网络连接的访问风险与由于物理访问导致的风险不同。应予以考虑的访问类型有:

a) 物理访问,例如,访问办公室,计算机机房,档案室;

b) 逻辑访问,例如,访问组织的数据库,信息系统。

4.2.1.2 访问的原因

有许多原因可以授予第三方访问。例如,向组织提供服务却不在现场的第三方,可以授予物理和逻辑访问权,诸如:

a) 硬件和软件支持人员,他们需要访问系统级或低级别的应用功能度;

b) 贸易伙伴或联合投资者,他们可以交换信息,访问信息系统或共享数据库。

在不充分的安全管理情况下,由于第三方访问,可能把信息置于风险中。若有业务需要连接到第三方地址,那么应进行风险评估,以标识出特定控制的任何要求。要考虑到所要求的访问类型、信息的价值、第三方所利用的控制以及这种访问牵连到该组织的信息安全。

4.2.1.3 现场合同方

在其合同中所定义的一段时间内位于现场的第三方也可能导致安全弱点。现场第三方的例子包括:

a) 硬件和软件维护与支持人员;

b) 清洁、给养、安全保卫和其他外包支持服务;

c) 实习学生或其他短期临时工作人员;

d) 顾问。

重要的是要理解需要什么样的控制来管理第三方对信息处理设施的访问。一般来说,由第三方访问导致的所有安全要求或者内部控制应在第三方合同反映出来(也见4.2.2)。例如,如果对于信息的保密性有特定的需要,可以使用不泄露协议(见6.1.3)。

只有在实施了适当的控制措施并签定了涵盖连接和访问条款的合同之后,第三方才可以访问信息和信息处理设施。

4.2.2 第三方合同中的安全要求

涉及第三方访问组织信息处理设施的协议要以包含或引用所有重要要求的正式合同为基础,以确保符合组织的安全策略和标准。该合同要确保在该组织和第三方之间不存在误解。至于其供应商的赔

偿问题，各组织应自行解决。合同中应考虑下列条款：

a) 信息安全的通用策略；

b) 资产保护，包括：

1) 保护组织资产（包括信息和软件）的规程；

2) 确定资产是否受到损害（例如丢失数据或修改数据）的规程；

3) 确保在合同截止时或在合同执行期间双方同意的某一时段对信息和资产的归还或销毁的控制；

4) 完整性和可用性；

5) 对拷贝和泄露信息的限制；

c) 要提供每项服务的描述；

d) 服务的目标级别和不可接受的服务级别；

e) 若合适，人员转职的规定；

f) 协议双方的相关义务；

g) 关于法律事件（例如，数据保护法律）的责任。如果该合同涉及与其他国家的组织的合作，特别要考虑到不同的国家法律体系（也见 12.1）；

h) 知识产权（IPRs）和版权转让（见 12.1.2）以及任何协作性工作的保护（见 6.1.3）；

i) 访问控制协议，包括：

1) 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。

2) 用户访问和特权的授权过程；

3) 维护被授权使用正在提供的服务的个人清单的要求以及他们与这种使用相关的权利和特权是哪些；

j) 可验证的性能要求的定义、监督和报告；

k) 监督和撤销用户活动的权利；

l) 审核合同职责的权利或拥有由第三方进行这些审核的权利；

m) 建立逐级解决问题的过程；在适合的情况下，也应考虑意外事故安排；

n) 关于硬件和软件安装和维护的职责；

o) 一种清晰的报告结构和商定的报告格式；

p) 一种清晰规定的变更管理过程；

q) 任何要求的物理保护控制和机制，以确保遵守这些控制；

r) 对用户和管理者在方法、规程和安全方面的培训；

s) 确保防范恶意软件的控制措施（见 8.3）；

t) 报告、通知和调查安全事故和安全违规的安排；

u) 包括具有转包商的第三方。

4.3 外包

目的：信息处理的职责是在外包给其他组织时维护信息安全。

外包安排应在双方的合同中指出信息系统、网络和/或桌面环境的风险、安全控制和规程。

4.3.1 外包合同中的安全要求

组织的信息系统、网络和/或桌面环境的全部或某些部分的管理和控制进行外包时，要在双方所商定的合同中指出安全要求。

例如，合同中要指出：

a) 如何满足法律要求，例如，数据保护法律；

b) 有什么样的安排，可确保外包所涉及的各方（包括转包商）知道其安全职责；

c) 如何维护和测试该组织的业务资产的完整性和保密性；

d) 将使用什么样的物理和逻辑控制来限制和限定已授权用户访问该组织的敏感的业务信息；

e) 万一有自然灾害，如何维护服务的可用性；

f) 对外包设备要提供什么等级的物理安全；

g) 审核的权利。

4.2.2 的清单中所给出的条款也应考虑作为该合同的一部分。该合同要允许在双方待商定的安全管理计划中扩充安全要求和规程。

虽然外包合同可能提出某些复杂的安全问题，但在本实用规则中所包括的控制可以用作商定安全管理计划的结构和内容的起点。

5 资产分类和控制

5.1 资产的可核查性

目的：维持对组织资产的相应保护。

所有主要信息资产应是可核查的，并且有指定的责任人。

资产的可核查性有助于确保维持相应的保护。对于所有主要资产要标识出责任人，并且要赋予维护相应控制的职责。可以授予实施控制的职责。可核查性归于资产的指定责任人。

5.1.1 资产清单

资产清单有助于确保进行有效的资产保护，并且对于其他业务目的，诸如健康与安全、保险或财务(资产管理)的原因，也需要资产清单。编制资产清单的过程是风险管理的重要部分。一个组织需要能标识出资产和这些资产的相关价值和重要性。然后，根据该信息，一个组织可以提供与资产的价值和重要性相称的保护等级。每个信息系统相关的重要资产都应编制清单并加以维持。每一资产应清楚地标识，应商定其所有权和安全分类(见 5.2)以及其当前位置(尝试从丢失或损坏中恢复时是重要的)并形成文档。与信息系统相关的资产举例：

a) 信息资产：数据库和数据文件，系统文档，用户手册，培训材料，操作或支持规程，连续性计划，后备运行安排，归档的信息；

b) 软件资产：应用软件，系统软件，开发工具和实用程序；

c) 物理资产：计算机设备(处理器、监视器、便携式计算机、调制解调器)，通信设备(路由器、PABX、传真机、应答机)，磁媒体(磁带和磁盘)，其他技术设备(电源、空调装置)，家具，用具；

d) 服务：计算和通信服务，一般公用事业，例如，供暖，照明，能源，空调。

5.2 信息分类

目的：确保信息资产受到相应等级的保护。

信息要分类，以指出保护的需求、优先级和程度。

信息具有可变的敏感性和重要性。某些项可以要求附加等级的保护或特别的处理。信息分类体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。

5.2.1 分类指南

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，例如，对信息的未授权访问或损坏。一般说，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。

信息和处理分类数据的系统的输出要根据它对组织的价值和敏感性予以标记。根据它对组织的重要程度对信息进行标记也可能是合适的，例如根据它的完整性和可用性。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。过多的分类可能导致不必要的附加业务费用，上述各方面应予以考虑。分类指南要预先考虑并允许任何给定的信息项的分类在全部时间内不必固定，并且根据预先确定的策略加以变更(见 9.1)。

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不方便和不经济，或许是不实际的。在解释其他组织文档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。

定义信息项(例如，对文档，数据记录，数据文件或软件)的分类以及周期性评审该分类的职责仍然属于信息的始发者或指定的拥有者。

5.2.2 信息标记和处理

重要的是，按照组织所采纳的分类方案对信息标记和处理定义一组合适的规程。这些规程需要涵盖物理和电子格式的信息资产。对每种分类，要定义处理规程，以涵盖下列信息处理活动类型：

a) 拷贝；

b) 存储；

c) 邮政、传真和电子邮件的传输；

d) 话音传输，包括移动电话、话音邮件、应答机；

e) 销毁(数据结构)；

系统的输出含有了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记。该标记要根据 5.2.1 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、记录媒体(磁带、磁盘、CD、盒式磁带)、电子报文和文件传送。

物理标记一般是最合适的标记形式。然而，某些信息资产(诸如电子形式的文档等)在物理上不能做标记，而需要使用电子标记手段。

6 人员安全

6.1 岗位设定和人力资源的安全

目的：减少人为差错、盗窃、欺诈或滥用设施的风险。

在招聘阶段要指出安全职责，要包含在合同中并在个人聘用期间予以监督。

要对可能的新成员进行充分的筛选，特别对敏感性岗位的成员(见 6.1.2)。所有雇员和信息处理设施的第三方用户要签署保密(不泄密)协议。

6.1.1 在岗位职责中要包含的安全

在合适情况下，在组织的信息安全策略中所列出的安全角色和职责(见 3.1)，要形成文档。它们要包括实施或维护安全策略的总职责以及保护特定资产或执行特定安全过程或活动的任何特定职责。

6.1.2 人员筛选和策略

固定职员的鉴定核查要在职务申请时进行。这包括下列控制：

a) 获得令人满意的参考资料；

b) 申请人履历的核查(针对完整性和准确性)；

c) 声称的学术、专业资格的证实；

d) 独立的身份核查(身份证或护照)。

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，该组织还要进行信用核查。对于占据重要职权位置的职员而言，要周期性地重复这种核查。

对于合同商和临时职员要进行类似的筛选过程。若这些职员是通过代理提供的，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

通知规程。

在新的和无经验的职员被授权访问敏感系统时，管理层要评价对他们所要求的监督。所有职员的工作须经此类职员中更资深成员周期性评审和批准过程。

管理者要了解其职员的个人环境可能影响其工作。个人的或财务的问题、他们的行为或生活方式的变化、经常缺勤以及有压力或压抑的迹象都可能导致欺诈、盗窃、出错或其他安全隐患。要按照相关权限中的合适法律处理这些情况。

6.1.3 保密性协议

保密性协议或不泄密协议用来告知信息是保密的或秘密的。雇员们一般要签署这样的协议，作为聘用他们的最初条款和条件的一部分。

应要求现有合同(包含保密协议)中没有涉及的临时职员和第三方用户在给予访问信息处理设施之前签署保密协议。

当聘用或合同的期限有变化时，特别是，当雇员预期离开该组织或合同到期终止时，要评审保密协议。

6.1.4 雇用条款和条件

雇用条款和条件要说明雇员的信息安全职责。若合适，这些职责应在雇用结束后继续规定一段时间。应包括如果雇员漠视安全要求所要采取的行动。

雇员的合法职责和权利(例如，关于版权法或数据保护法)要予以阐明并包括在雇用的条款和条件内。也要包括雇主的数据分类和管理的职责。只要合适时，雇用的条款和条件要说明上述这些职责扩充到组织办公地点之外以及正常工作时间之外，例如，在家里工作的情况(也见 7.2.5 和 9.8.1)。

6.2 用户培训

目的：确保用户知道信息安全威胁和利害关系，并准备好在其正常工作过程中支持组织的安全策略。

为了使可能的安全风险减到最小，用户应接受安全规程和正确使用信息处理设施方面的培训。

6.2.1 信息安全教育和培训

组织的所有雇员和(若相关的)第三方用户要接受组织的策略和规程方面的适当培训和定期更新内容。这包括安全要求、合法职责和业务控制以及在给予访问信息和服务之前正确使用信息处理设施的培训，例如登录过程，使用软件包等。

6.3 对安全事故和故障的响应

目的：使安全事故和故障的损害减到最小，并监督这种事故以及从事故中学习。

影响安全的事故要尽可能快地通过合适的管理渠道予以报告。

要使所有雇员和合同商知道报告可能对组织的资产安全有影响的不同类型事故(安全违规、威胁、弱点或故障)的规程，应要求他们尽可能快地把任何观察到的或预测到的事故报告给指明的联系点。该组织对涉及安全违规的雇员应建立一个正式的纪律处理办法。为了能正确地指出事故，在出现事故之后尽可能快地收集证据可能是必要的(见 12.1.7)。

6.3.1 报告安全事故

安全事故要尽可能快地通过合适的管理渠道报告。

应建立正式的报告规程以及事故响应规程，以及在收到事故报告时提出要采取的动作。要让所有雇员和合同商知道报告安全事故的规程，并要求他们尽可能快地报告这样的事故。相应的反馈过程应予以实现，以确保在事故已经处理和结束之后将结果通知报告事故的人们。在用户安全意识培训时，这些事故可用作可能发生什么，如何响应这样的事故，如何在将来避免这样的事故(也见 12.1.7)的例子。

6.3.2 报告安全弱点

应要求信息服务的用户通知并报告任何观察到的或预测到的系统或服务的安全弱点。他们要尽可能快地向其管理层或直接向其服务提供者报告这些情况。要通知用户在任何情况下，他们不要企图证明预测到的弱点。这是为了其自身的保护，因为可能将测试的弱点看作系统的潜在滥用。

6.3.3 报告软件故障

要建立报告软件故障的规程。下列动作要予以考虑。

a) 应记录下问题的征兆和任何显示在屏幕上的消息；

b) 如有可能，计算机要加以隔离，并且停止对其的使用。要立即向相应的联系点报警。如果设备待检查，在重新加电之前，设备要与任何组织的网络断开。磁盘不要转移到其他计算机；

c) 应立即向信息安全管理者报告此情况。

用户不要试图移去可疑的软件，除非被授权这样做。要由已受过相当培训的和有经验的人员进行恢复。

6.3.4 从事故中学习

要有适当的机制，以使事故和故障的类型、数量和代价能被量化和监督。该信息要用来标识重复发生的或影响很大的事故或故障。这样做可以指出需要增强的或附加的控制，以限制未来出现事故的频度、损坏和代价，或者要将它们计入安全策略评审过程中(见 3.1.2)。

6.3.5 纪律处理

对于违反了组织安全策略和规程(见 6.1.4，关于证据的保存见 12.1.7)的雇员，要具有正式的纪律处理。对雇员来说，这样一种办法起威慑的作用，否则他可能倾向于不顾安全规程。此外，宜确保正确、公正地对待牵涉重大违规或经常违规的雇员。

7 物理和环境的安全

7.1 安全区域

目的：防止对业务办公场所和信息未授权访问、损坏和干扰。

关键和敏感的业务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周边和适合的安全屏障和入口控制的保护。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。推荐用清理台面和清空屏幕策略以减少未授权访问或损坏记录纸、媒体和信息处理设施的风险。

7.1.1 物理安全周边

物理保护可通过在业务办公场所信息处理设施周围建立若干物理屏障来达到。各个屏障建立一个安全周边，每个屏障都增强所提供的整体保护。组织要使用安全周边来保护包含信息处理设施的区域(见 7.1.3)。安全周边是指构建屏障的某样东西，例如，墙、卡控制的入口门或有人管理的接待台。各个屏障的设置地点和强度取决于风险评估的结果。

若合适，下列指南和控制应予以考虑：

a) 安全周边应清晰地予以定义；

b) 包含有信息处理设施的建筑物或场地的周边应在物理上是安全的(即，在周边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，所有外部门要有适当保护以防止未授权进入，例如，控制机制、门闩、报警器、锁等等；

c) 有人管理的接待区域或控制物理访问场地或建筑物的其他手段要到位。进入场地或建筑物应仅限于已授权人员；

d) 如果需要，物理屏障应从真正的地板扩展到真正的天花板，以防止未授权进入和由诸如火灾和水灾所引起的环境污染；

e) 安全周边的所有防火门应可发出报警信号，并应紧闭。

7.1.2 物理入口控制

安全区域要由适合的入口控制所保护，以确保只有已授权的人员才允许访问。下列控制要予以考虑。

a) 对安全区域的访问者要予以监督或办理进入手续，并记录他们进入和离开的日期和时间。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安全要求和应急规程的说明；

b) 访问敏感信息和信息处理设施要受到控制，并且仅限于已授权的人员。鉴别控制[例如，插卡加个人识别号(PIN)]应用于授权和确认所有访问。所有访问的审核踪迹要安全地加以维护；

c) 要求所有人员佩带某种形式的可视标识，并且鼓励他们询问无人护送的陌生人和未佩带可视标识的任何人；

d) 对安全区域的访问权利要定期地予以评审和更新。

7.1.3 办公室、房间和设施的安全保护

安全区域可以是在物理安全周边内侧上锁的办公室或者几个房间。这种办公室可以是上锁的并且可以包含可锁的铁柜或保险柜。安全区域的选择和设计要考虑到防止火灾、水灾、爆炸、国内动荡以及其他形式的自然或人为灾难的损坏的可能性。还要考虑到相关健康和安全的规章和标准。对于由邻接建筑物所引起的任何安全威胁(例如，来自其他区域的水泄漏)也要予以考虑。

下列控制应予以考虑。

a) 使关键设施坐落在避免公众进行访问的场地；

b) 建筑物要不引人注目，并且在建筑物内侧或外侧用不明显标记给出其用途的最少指示，以标识信息处理机构的存在；

c) 支持性功能件和设备(例如，影印机，传真机)适宜坐落在安全区域内，以避免可能泄露信息的要求访问；

d) 无人值守时门窗要上锁，外部保护时应考虑对窗户的保护，特别是对落地门窗；

e) 按照专业标准所安装的并定期测试的相应的入侵检测系统要装在合适的位置，以便涵盖所有外部门和可接近的窗户。对未占用的区域，在所有时刻也要予以监视。对于其他区域(例如，计算机机房或通信机房)也要提供掩蔽物；

f) 组织所管理的信息处理设施在物理上要与第三方所管理的那些信息处理设施分开；

g) 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；

h) 危险或易燃物品要安全地存储在离安全区域有一定的安全距离的地方。成批的供应品(诸如信纸文具之类)除非必要都不应存储在安全区域内；

i) 基本维持运行的设备和备份媒体要以一定的安全距离存放，以免受主要场地灾难的损坏。

7.1.4 在安全区域工作

可以要求附加控制和指南，以增强安全区域的安全，这包括对在安全区域中工作的人员或第三方以及在这里进行第三方活动的控制。下列控制要予以考虑。

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在其中的活动；

b) 由于安全(safety)原因和防范恶意活动的可能，均应避免在安全区域内进行不受监督的工作；

c) 未用的安全区域在物理上要锁上并周期地予以检查；

d) 仅在要求时，才同意第三方支持性服务人员对安全区域或敏感性信息处理设施进行有限制的访问。该访问要经过授权和并受到监督。在安全周边内侧具有不同安全要求的区域之间，可能需要用来控制物理访问的附加屏障和周边；

e) 除非授权，不允许携带摄影、声频、视频或其他记录设备。

7.1.5 交接区域的隔离

交接区域要受到控制，如有可能，要与信息处理设施隔离，以免未授权访问。这类区域的安全要求要根据风险评估来确定。下列控制要予以考虑。

a) 由建筑物外进入交接区限于已标识的和已授权的人员；

b) 交接区域应设计成这样，即在无需交货人员获得进入本建筑物其他部分的情况下就能卸下物资；

c) 当内部的门打开时，交接区域的外部的门应紧闭；

d) 在进来的物资从交接区域运到使用地点之前，要检查有潜在危险的进来物资(见 7.2.1d)；

e) 如果合适(见 5.1)，进来的物资应在场地的入口处进行登记。

7.2 设备安全

目的：防止资产的丢失、损坏或泄露和业务活动的中断。

在物理上应使设备免受安全威胁和环境危险。对设备的保护(包括离场使用)是减少未授权访问数据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。可以要求专门的控制用来防止危险或未授权访问和保护支持性设施，诸如电源和布缆基础设施。

7.2.1 设备安置和保护

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

a) 设备应进行安置，以尽量减少不必要的进入工作区域访问；

b) 应把处理敏感数据的信息处理设施和存储设施放在适当的位置，以减少在其使用期间被窥视的风险；

c) 要求专门保护的部件要予以隔离，以减低所要求的总体保护等级；

d) 应采取控制使包括下列潜在威胁的风险减到最小：

1) 偷窃；

2) 火灾；

3) 爆炸；

4) 烟雾；

5) 水(或供水故障)；

6) 尘埃；

7) 振动；

8) 化学影响；

9) 电源干扰；

10) 电磁辐射。

e) 一个组织要考虑关于在信息处理设施附近进食、喝饮料和抽烟的策略；

f) 对于可能负面影响信息处理设施运行状态的环境条件要予以监督；

g) 对于工业环境中的设备，要考虑使用专门保护方法(诸如，键盘保护膜)；

h) 在附近建筑物内发生灾难的影响，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等，均要予以考虑。

7.2.2 电源

设备应免受电源故障和其他电异常现象。要提供符合设备制造商规范的合适电源。

获得电源连续性的选项包括：

a) 多路馈电，以避免电源中单点故障；

b) 不间断电源(UPS)；

c) 备份发电机。

对于支持关键业务操作的设备，推荐使用支持有序关机或连续运行的 UPS。偶然事故计划要包括 UPS 故障时要采取的动作。UPS 设备要定期地检查，以确保它拥有足够能力，并按照制造商的建议予以测试。

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。如果安装，电机要按照制造商的说明定期地予以测试。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。

另外，应急电源开关应位于设备房间应急出口附近，以便万一应急时快速切断电源。在万一主电源出现故障时要提供应急照明。所有建筑物都应采用避雷保护，所有外部通信线路都应装配雷电保护过滤器。

7.2.3 布缆安全

电源和运载数据或支持信息服务的电信布缆要免受窃听或损坏。下列控制要予以考虑。

a) 进入信息处理设施的电源和电信线路宜在地下，若可能，或者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) 对于敏感的或关键的系统，更进一步控制考虑包括：

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或传输媒体；

3) 使用布光缆；

4) 清除与电缆连接的未授权装置。

7.2.4 设备维护

设备要予以正确地维护，以确保它的连续的可用性和完整性。下列控制应予以考虑。

a) 要按照供应商推荐的服务时间间隔和规范对设备进行维护；

b) 只有已授权的维护人员才可对设备进行修理和服务；

c) 要保存所有可疑的或实际的故障和所有预防和纠正维护的记录；

d) 当送设备到建筑物外维护(也见 7.2.6 关于删除、擦除和盖写数据)时要采取合适的控制。要遵守由保险策略所施加的所有要求。

7.2.5 离开建筑物的设备的安全

与所有权无关，为了信息处理在组织建筑物外使用任何设备要通过管理层授权。所提供的安全应等同于用于同一目的现场使用设备的安全，同时要考虑到组织建筑物外的工作风险。信息处理设备包括所有形式的个人计算机、电子记事簿、移动电话、记录纸或其他形式，这些是适用于家庭工作的或离开常规工作地点便于运输的设施。下列指南要予以考虑。

a) 离开建筑物的设备和媒体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，可锁的存档柜，清理桌面策略以及对计算机的访问控制；

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。关于保护移动设备其他方面的更多信息在 9.8.1 中可以找到。

7.2.6 设备的安全处置或安全重用

信息可能通过对设备的草率处置或重用而被泄漏(也见 8.6.4)。包含敏感信息的存储器在物理上应予以摧毁或者将其安全地盖写而不是使用标准删除功能。

包含存储媒体(例如，固定硬盘)的设备中的所有部件应予以检查，以确保任何敏感数据和许可的软

件在处理之前已经清除或盖写。包含敏感数据的已损坏的存储器可以要求风险评估，以确定这些部件是否要进行销毁、修理或丢弃。

7.3 一般控制

目的：防止信息和信息处理设施的受损害或被盗窃。

信息和信息处理设施应予以保护，以防止泄露给未授权人员，而被其修改或盗窃，控制应到位，以使丢失或损坏减到最小。

处理和存储规程在 8.6.3 中考虑。

7.3.1 清理桌面和清空屏幕策略

组织要考虑对记录纸和可移动的存储媒体采取清理桌面策略，对信息处理设施采取清空屏幕策略，以便减少在正常工作期间和在正常工作时间之外对信息的未授权访问、丢失和损坏的风险。该策略要考虑到信息安全分类（见 5.2）、相应的风险和组织的文化方面。

离开桌面的信息也可能在灾难中（诸如火灾、水灾或爆炸）被损坏或被摧毁。

下列控制要予以考虑。

a) 若合适，当不使用时，特别是在工作时间之外，记录纸和计算机媒体要存储在相应的上锁的柜子和/或其他形式的安全器具中；

b) 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）；

c) 当无人值守时，个人计算机和计算机终端和打印机不要保留登录，当不使用时，要利用带钥匙的锁、口令或其他控制进行保护；

d) 进来和出去的邮件点和无人值守的传真机和智能电报机要受到保护；

e) 在正常工作时间之外，复印机要予以锁上（或者以某一其他方法防止未授权使用）；

f) 当打印时，敏感的或分类的信息应立即从打印机中清除。

7.3.2 财产的移动

在未经授权的情况下，不应让设备、信息或软件离开场地。若需要并合适，要对设备作出外移的记录，当返回时，要作出送回的记录。为了检测未授权的财产移动，要进行抽查。要让每个人都知道将进行抽查。

8 通信和操作管理

8.1 操作规程和职责

目的：确保信息处理设施正确和安全的操作。

应建立所有信息处理设施的管理和操作的职责和规程。这包括制订合适的操作说明和事故响应规程。

若合适，应实施责任分割（见 8.1.4），以减少疏忽或故意滥用系统的风险。

8.1.1 文档化的操作规程

由安全策略所标识出的操作规程应形成文档并予以维护。要将操作规程看作正式的文档，其变更由管理层授权。

该规程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) 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的期限；

c) 在作业执行期间可能出现的处置差错或其他异常情况的说明，包括对使用系统实用程序的限

制(见 9.5.5)；

d) 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；

e) 特定输出处置说明，诸如使用特殊信纸或管理保密输出，包括失败作业输出安全处置的规程；

f) 供万一系统失效用的系统重新起动和恢复规程。

与信息处理和通信设施相关的系统内务活动也要形成文档的规程，诸如计算机启动和关机规程、备份、设备维护、计算机机房和邮件处置管理和物理安全(safety)。

8.1.2 操作变更控制

对信息处理设施和系统的变更要加以控制。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。正式的管理者职责和规程应到位，以确保对设备、软件或规程的所有变更有令人满意的控制。操作计划须经受严格变更控制。当该计划变更时，包含所有相关信息的审核日志要予以保留。对操作环境的变更可能影响应用。凡是可行之处，操作和应用变更控制规程要集成起来(也见 10.5.1)。特别是，下列控制要予以考虑。

a) 重大变更的标识和记录；

b) 对这种变更潜在影响的评估；

c) 对建议的变更的正式批准规程；

d) 向所有有关人员传递变更细节；

e) 标识放弃不成功变更和恢复职责的规程。

8.1.3 事故管理规程

应建立事故管理职责和规程，以确保快速、有效和有序地响应安全事故(也见 6.3.1)。下列控制要予以考虑。

a) 应建立规程，以涵盖所有潜在的安全事故类型，包括：

1) 信息系统故障和服务丢失；

2) 拒绝服务；

3) 由不完整或不准确的业务数据导致的差错；

4) 保密性违规；

b) 除正常的应急计划(设计成尽可能快地恢复系统或服务)外，还要涵盖下列规程(也见 6.3.4)：

1) 事故原因的分析和标识；

2) 若需要，规划和实施补救，以防止再次发生；

3) 收集审核踪迹和类似证据；

4) 与受事故影响或涉及从中恢复的人员的联系；

5) 向相应机构报告此动作；

c) 当合适时，应对下列内容，收集审核踪迹和类似证据(见 12.1.7)并且使其安全保密：

1) 内部问题分析；

2) 用作潜在合同违规、管理要求违规或者民事或刑事行为(例如，根据计算机滥用或数据保护法)的证据；

3) 软件和服务供应商赔偿谈判；

d) 要小心地、正式地控制从安全违规中恢复和纠正系统故障的动作。这些规程应确保：

1) 只有明确标识的和已授权的人员才允许访问运转着的系统和数据(关于第三方访问也见 4.2.2)；

2) 所采取的全部应急动作详细地形成文档；

3) 将应急动作报告给管理层并按有序的方式进行评审；

4) 以最小延迟，对业务系统和控制的完整性加以证实。

8.1.4 责任分割

责任分割是一种减少偶然或故意的系统滥用风险的方法。应考虑分割开管理或执行某些责任或职责区域，以便减少未授权修改或滥用信息或服务的机会。

小型组织可能感到难以达到这种控制方法，但是就可能和可行来说，该原则是适用的。只要难以分割，应考虑其他控制，诸如，对活动、审核踪迹和管理监督的监视等。重要的是安全评审仍保持独立。

应注意，在无检测的单个职责区域内，要使个人不能实施欺诈。事件的启动要与其授权分离。下列控制要加以考虑。

a) 重要的是分割开有可能通过勾结而产生的欺骗活动，例如，提出采购订单和验收货物；

b) 如果有勾结的危险，那么需建立控制，使得需包含两个或两个以上的人，借此降低共谋的可能性。

8.1.5 开发和运行设施分离

为达到分离所涉及角色的目的，分离开发、测试和运行设施是重要的。要规定从开发状态到运行状态的软件传送规则并形成文档。

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。为了防止运行问题，在运行、测试和开发环境之间所需要的分离程度要加以考虑。在开发和测试功能之间，类似的分离也要加以实现。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，或引入未测试的或恶意的代码。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。下列控制要加以考虑。

a) 若有可能，开发和运行的软件要在不同的计算机处理器上或在不同的域或目录内运行；

b) 开发和测试活动要尽可能分离；

c) 当不要求编译程序、编辑程序和其他系统实用程序时，不应从运行系统对它们进行访问；

d) 对运行和测试系统要用不同的登录规程，以减少出错的风险。要鼓励用户对这些系统使用不同的口令，选单要显示合适的标识报文；

e) 若发布支持运行系统的口令控制到位，那么开发人员只可使用操作口令进行访问。控制要确保这种口令在使用后就被变更。

8.1.6 外部设施管理

使用外部合同商管理信息处理设施可能引入潜在的安全泄露，诸如，在该合同商场地处有数据泄露、损坏或丢失的可能性。这些风险要预先加以标识，并且与合同商商定合适的控制，并将其加到合同中(关于涉及访问组织设施的第三方合同和外包合同的指南，也见 4.2.2 和 4.3)。

要指出的特殊问题包括：

a) 标识出最好保留在内部的敏感或关键的应用(程序)；

b) 获得业务应用责任人批准；

c) 业务连续性计划所包含的内容；

d) 规定安全标准，和测量符合性的过程；

e) 分配特定职责和规程，以有效监督所有相关的安全活动；

f) 报告和处理安全事故的职责和规程(见 8.1.3)。

8.2 系统规划和验收

目的:使系统故障的风险减到最小。

为了确保足够能力和资源的可用性,要求预先的规划和准备。

为了减少系统过载的风险,要制订进一步能力要求的项目。

在新系统验收和使用之前,要建立该新系统的运行要求。

8.2.1 能力规划

能力需求要受监督,要制订进一步能力要求的项目,以确保获得足够的处理能力和存储空间。这些项目要考虑到组织信息处理中新业务和系统要求以及当前的和预计的趋势。

主计算机需要特殊的关注,这是因为采购新的能力时要花很大的费用和订货至交货间的时间。主服务器的管理者要监督关键系统资源的利用,包括处理器、主存储器、文件存储器、打印机和其他输出设备以及通信系统。他们(管理者)应标识出使用的趋势,特别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,同时计划适合的补救动作。

8.2.2 系统验收

要建立新信息系统、升级和新版本的验收准则,在验收之前,对系统要进行适当的测试。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、形成文档和测试。下列控制要加以考虑。

a) 性能和计算机能力要求;

b) 差错恢复和重新启动规程以及应急计划;

c) 按照已定义标准,例行程序操作规程的准备和测试;

d) 商定的一组安全控制到位;

e) 有效的手动规程;

f) 按 11.1 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,诸如,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。

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。

8.3 防范恶意软件

目的:保护软件和信息的完整性。

要求有预防措施,以防范和检测恶意软件的引入。软件和信息处理设施对恶意软件(诸如,计算机病毒、网络蠕虫、特洛伊木马(也见 10.5.4)和逻辑炸弹)的引入是脆弱的。要让用户了解未授权的或恶意的软件的危险,若合适,管理者要引入专门的控制,以检测或防范它的引入。特别是,采取预防措施检测和防范个人计算机上的计算机病毒是重要的。

8.3.1 控制恶意软件

应实施防范恶意软件的检测、预防控制及相应通知用户的规程。防范恶意软件要基于安全意识、合适的系统访问和变更管理控制。下列控制要加以考虑。

a) 要求符合软件许可证和禁止使用未授权软件的正式策略(见 12.1.2.2);

b) 防范风险的正式策略,该风险与来自或经由外部网络或在任何其他媒体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 10.5，特别是 10.5.4 和 10.5.5)；

c) 安装和定期更新防病毒检测和修复软件来扫描计算机和媒体，以作为预防控制或作为例行程序的基础；

d) 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；

e) 在使用前针对病毒，检查不确定或未授权来历的电子媒体上的任何文件(file)或者在不可信的网络上收到的文件；

f) 在使用前针对恶意软件检查任何电子邮件附件和下载内容。该检查可以在不同的位置进行，例如，在电子邮件服务器、台式计算机处或者当进入组织的网络时；

g) 涉及关于系统、系统使用的培训、报告病毒攻击和从病毒攻击中恢复的病毒预防的管理规程和职责(见 6.3 和 8.1.3)；

h) 相应的从病毒攻击中恢复的业务连续性计划，包括所有必要数据和软件备份以及恢复安排(见 11 章)；

i) 检验与恶意软件相关的所有信息，并确保报警公告是准确情报的规程。管理应确保使用合格的来源(例如，声誉好的期刊、可靠的 Internet 网站或防病毒软件供应商)，以区分欺骗病毒和实际病毒。要让职员了解欺骗病毒问题，以及在收到它们时要做什么。

这些控制对于支持大量工作站的网络文件服务器特别重要。

8.4 内务处理

目的：维护信息处理和通信服务的完整性和可用性。

为执行商定的备份战略(见 11.1)，应建立例行规程，而该备份战略采取数据备份拷贝，演练数据及时恢复，记录事件和故障，若合适，还监督设备环境。

8.4.1 信息备份

要定期产生最重要业务信息和软件的备份拷贝。要提供足够的备份设施，以确保在灾难或媒体故障之后可以恢复所有最重要业务信息和软件。要定期测试各个系统的备份设备，以确保它们满足业务连续性计划的要求(见第 11 章)。下列控制要加以考虑。

a) 最低级别的备份信息以及备份拷贝准确完整的记录和文档化的恢复规程要存储在有足够距离的远程地点，以避免主要场地灾难时受到损坏。对于重要的业务应用至少要保留三代或若干周期的备份信息；

b) 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 7 章)。要扩充应用于主要场地媒体的控制，以涵盖备份场地；

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

d) 要定期检查和测试恢复规程，以确保为恢复时在操作规程所分配的时间内它们是有效的并能完成它们。

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 12.1.3)。

8.4.2 操作员日志

操作人员应维护其活动日志。若合适，日志要包括：

a) 系统启动和结束时间；

b) 系统出错和所采取的纠正动作；

c) 对正确处理数据文件和计算机输出的证实；

d) 产生日志项的人员名字。

操作员日志须经定期、独立地按操作规程检查。

8.4.3 故障记录

要报告故障并采取纠正动作。由与信息处理系统或通信系统的问题有关的用户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。

8.5 网络管理

目的：确保护卫网络中的信息和保护支持性基础设施。

要求注意可以跨过组织边界的网络的安全管理。

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。

8.5.1 网络控制

为获得和维护计算机网络的安全，要求若干控制。网络管理者要实施控制，以确保网络中的数据安全，防止未授权访问所连接的服务。特别是，下列控制要予以考虑。

a) 若合适，网络的操作职责要与计算机操作分开(见 8.1.4)；

b) 应建立远程设备(包括用户区域内的设备)管理的职责和规程；

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 9.3 和 10.3)。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) 为优化对业务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。

8.6 媒体处置和安全

目的：防止资产损坏和业务活动中断。

媒体应受到控制并且在物理上受保护。

为使文档、计算机媒体(磁带、磁盘、盒式磁带)、输入/输出数据和系统文档免遭损坏、偷窃和未授权访问，应建立合适的操作规程。

8.6.1 可移动的计算机媒体的管理

对于可移动的计算机媒体(诸如，磁带、磁盘、盒式磁带和打印的报告等)的管理要有规程。下列控制要加以考虑。

a) 对从组织取走的任何可重用的媒体中的先前内容，如果不再需要，应将其擦除掉；

b) 对于从组织取走的所有媒体应要求授权，所有这种移动的记录要加以保持，以保持审核踪迹(见 8.7.2)；

c) 要将所有媒体存储在符合制造商规范的安全、保密的环境中。

所有规程和授权级别要清晰地形成文档。

8.6.2 媒体的处置

当不再需要时，要秘密和安全地处置媒体。由于草率处置媒体，可能将敏感信息泄漏给局外人员。应建立秘密处置媒体的正式规程，以使风险减至最小。下列控制要予以考虑。

a) 包含有敏感信息的媒体要秘密和安全地存储和处置，例如，利用焚化或切碎的方法，或者将数据腾空供组织内另外应用使用；

b) 下列清单标识出可能要求秘密处置的项目：

1) 纸文件；

2) 话音或其他记录；

3) 复写纸；
4) 输出报告；
5) 一次性使用的打印机色带；
6) 磁带；
7) 可移动的磁盘或盒式磁带；
8) 光存储媒体(所有形式并且包括所有制造商软件分发媒体)；
9) 计划列表；
10) 测试数据；
11) 系统文档；

c) 安排把所有媒体部件收集起来并进行秘密处置，比试图分离出敏感部件可能更容易；
d) 许多组织对记录纸、设备和媒体提供收集和处置服务。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，处置敏感部件要做记录，以便保持审核踪迹。

当堆积处置媒体时，对聚集的影响要予以考虑，它可能使大量未分类的信息变成比小量分类信息更敏感。

8.6.3 信息处置规程

要建立信息处置和存储的规程，以便使这样的信息免遭未授权泄露或滥用。为处置文档、计算系统、网络、移动计算、移动通信、邮件、话音邮件、一般话音通信、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)中与其分类(见 5.2)一致的信息，应制定若干规程。下列控制要加以考虑(也见 5.2 和 8.7.2)。

a) 处置和标记所有媒体(也见 8.7.2a))；
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) 媒体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) 清晰地标记数据所有拷贝，以引起已授权接收者关注；
i) 以定期的时间间隔评审分发列表和已授权接收者列表。

8.6.4 系统文档的安全

系统文档可以包含一系列敏感信息，例如，应用过程的描述、规程、数据结构、授权过程(也见 9.1)。要考虑下列控制，以防止系统文档遭受未授权访问。

a) 要安全地存储系统文档；
b) 将系统文档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档。

8.7 信息和软件的交换

目的：防止组织之间交换的信息的丢失、修改或滥用。

在组织之间交换的信息和软件应受到控制，并且应符合任何相关法律(见第 12 章)。

要在协议(agreement)的基础上进行交换。要建立保护运输中信息和媒体的规程和标准。要考虑业务和电子数据交换、电子商务和电子邮件相关的安全所涉及问题及其控制要求。

8.7.1 信息和软件交换协议(agreement)

对于在组织之间交换的信息和软件(电子的或人工的)，应建立若干协议，当合适时可包括软件契约

协议，某些协议可能是正式的。这种协议的安全内容应反映所涉及的业务信息的敏感性。关于安全状态的协议应考虑：

a) 控制和通知传输、发送和接收方面的管理职责；
b) 通知发送者、传输、发送和接收方面的规程；
c) 打包和传输的最低技术标准；
d) 信使标识标准；
e) 万一数据丢失时的责任和义务；
f) 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；
g) 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所考虑事项的职责（见12.1.2和12.1.4）；
h) 记录和阅读信息和软件的技术标准；
i) 为保护敏感项[诸如密钥（见10.3.5）]，可以要求任何专门的控制。

8.7.2 运输中的媒体安全

在物理运输（例如，当借助邮政服务或借助信使发送媒体时）期间，信息可能是脆弱的，信息易受到未授权访问、滥用或损坏。为保护在场地之间所运输的计算机媒体，应使用下列控制。

a) 应使用可靠的运输或信使。已授权信使的列表应与管理层商定，并且实施检查信使标识的规程；
b) 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；
c) 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；
   5) 使用数字签名和加密，见10.3。

8.7.3 电子商务的安全

电子商务可能涉及使用跨越公用网络（诸如Internet）的电子数据交换（EDI）、电子邮件和在线事务。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。为保护电子商务免遭这样的威胁，应使用若干控制。电子商务的安全考虑应包括下列控制。

a) 鉴别。在彼此声称的身份中，顾客和贸易者要求什么样的置信度级别？
b) 授权。授权谁设定价钱、发布或签署关键贸易文档？贸易合伙人如何知道此事？
c) 合同和提出过程。保密性、完整性和关键文件接收和发送的证明以及合同抗抵赖方面的要求是什么？
d) 定价信息。在广告价格表中的完整性和敏感的折扣安排的保密性方面可以给予什么样的可信级别？
e) 订单交易。如何提供订单、支付和交付地址细节以及接收证实的保密性和完整性？
f) 检查。为检查顾客提供的支付信息，什么样的检查程度是适合的？
g) 结算。为防止欺诈，最适合的支付形式是什么？
h) 下订单。为维护订单信息的保密性和完整性和避免交易事务的丢失或重复，要求什么保护？
i) 责任。谁承担任何欺诈交易的风险？

上述许多考虑可以通过应用10.3中所提出的密码技术来实现，并考虑到符合法律要求（见12.1，特别见12.1.6密码法规）。

应通过文档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 9.4.7)。

8.7.4 电子邮件的安全

8.7.4.1 安全风险

电子邮件正用于业务通信,而取代诸如用户电报和信件等的传统通信形式。电子邮件和传统的业务通信形式不同,例如,其速度、报文结构、非正式的程序以及易遭受未授权操作(actions)的脆弱性。为减少电子邮件所产生的安全风险,需要的控制予以考虑。安全风险包括:

a) 报文存在易遭受未授权访问或修改或拒绝服务的脆弱性;

b) 存在易遭受差错的脆弱性,例如,不正确的寻址或指错方向,以及服务的一般可靠性和可用性;

c) 通信媒体变更对业务过程的影响,例如,增加发送速度的影响或者发送从个人到个人(不是从公司到公司)的正式报文的影响;

d) 法律的考虑,诸如,可能需要始发、发送、交付和接受的证据;

e) 发布外部可访问人员列表所涉及到的问题;

f) 控制远程用户访问电子邮件账户。

8.7.4.2 关于电子邮件的策略

组织应制定关于使用电子邮件的清晰策略,包括:

a) 对电子邮件的攻击,例如,病毒,截取;

b) 保护电子邮件附件;

c) 何时不使用电子邮件的指南;

d) 雇员有义务不损害公司利益,例如,不发送诽谤性电子邮件,不得使用电子邮件进行骚扰,不得进行未授权采购;

e) 使用密码技术来保护电子报文的保密性和完整性(见 10.3);

f) 报文的保留,如果提出诉讼时则可以显示保留的报文;

g) 检查不能被鉴别的报文交换用的附加控制。

8.7.5 电子办公系统的安全

为控制与电子办公系统相关的业务和安全风险,应制定和实施有关的策略和指南。这些策略和指南可通过结合使用文档、计算机、移动计算、移动通信、邮件、话音邮件、一般话音通信、多媒体、邮政服务/设施和传真机,为快速传播和共享业务信息提供机会。

有关互连这些设施所涉及到的安全和业务应考虑的事项包括:

a) 办公系统中的信息的脆弱性,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;

b) 管理信息共享的策略和相应的控制,例如,使用公共电子公告牌(见 9.1);

c) 如果系统不提供合适级别的保护,则排除包括敏感业务信息种类(见 5.2);

d) 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;

e) 支持业务应用的系统的适合性或其他等等,诸如,通信指令或授权;

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(见 4.2);

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(见 12.1.3 和 8.4.1);

j) 基本维持运行的要求和安排(见 11.1)。

8.7.6 公开可用系统

应注意保护电子发布信息的完整性，以防止可能伤害发布组织名声的未授权修改。在公开可用系统上的信息（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管辖区域内的法律、规则和规章。在所产生的信息公开可用之前，应有一正式授权过程。

在公开可用系统上可提供的并要求高级别完整性的软件、数据和其他信息要受相应机制所保护，例如，数字签名（见 10.3.3）。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 12.1.4）；

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。

8.7.7 信息交换的其他形式

为保护通过使用话音、传真和视频通信设施的信息交换，规程和控制应到位。由于对使用这些设施缺乏意识、策略或规程可能泄露信息，例如，在公开场所的移动电话被偷听，应答机被偷听，未授权访问拨号话音邮件系统或使用传真设备偶然地将传真发送给不适当的个人。

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 7.2 和第 11 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 9 章）。

在使用话音、传真和视频通信时，应建立希望工作人员遵守的规程的清晰策略说明。这应包括：

a) 提醒工作人员，应采取相应预防措施，例如，不泄露敏感信息，以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，特别要注意在他们附近的人们；

   2) 搭线窃听和通过物理访问电话手持送受话器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；

b) 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；

c) 不要将报文留在应答机上，因为可能被未授个人所重放，或者用于误拨号被存储在公用系统上或不正确地被存储；

d) 提醒工作人员有关传真机的使用问题，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。

9 访问控制

9.1 访问控制的业务要求

目的：控制对信息的访问。

对信息的访问和业务过程应在业务和安全要求的基础上予以控制。

这应考虑到信息传播和授权的策略。

9.1.1 访问控制策略

9.1.1.1 策略和业务要求

应定义访问的业务要求，并将其形成文档。在访问策略说明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。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；
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；
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（见第 12 章）；
f) 关于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利的管理。

9.1.1.2 访问控制规则

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，而不是软弱的“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 5.2）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，要求管理员批准的或另一方批准的规则以及无须批准的规则。

9.2 用户访问管理

目的：防止未授权访问信息系统。

应有正式的规程来控制对信息系统和服务的访问权利的分配。

这些规程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最终注销。在合适的情况下，应专门注意控制有特权的访问权利的分配的需要，而这种权利允许用户超越系统控制。

9.2.1 用户注册

应有授予访问所有多用户信息系统和服务的正式用户注册和注销的规程。

应通过正式的用户注册过程控制访问多用户信息服务，这些控制应包括：
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。若他们适合于所进行的工作，才允许使用组 ID；
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。经管理层单独批准的访问权利也是合适的；
c) 检验所授予的访问级别是否适合于业务目的（见 9.1），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 8.1.4）；
d) 给予用户访问权利的书面声明；
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规程，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利；
i) 周期性检验和取消多余的用户 ID 和账户；
j) 确保对其他用户不发布多余的用户 ID。

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。

9.2.2 特权管理

应限制和控制特权（使用户能超越系统或应用控制的多用户信息系统的特征或便利条件）的分配和使用。系统特权的不恰当使用常常是一种导致系统故障的主要因素。

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特权，以及需要分配特权的工作人员类别；

b) 特权应在需要使用的基础上和逐个事件的基础上分配给个人，即，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) 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。

9.2.3 用户口令管理

口令是一种确认访问信息系统或服务的用户身份的常用手段。口令的分配应通过正式的管理过程加以控制，其方法应：

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(这可包括在雇用条款和条件内，见 6.1.4)；

b) 若要求用户维护其自己的口令，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。当用户忘记其口令时，在正确识别用户之后，才提供临时口令；

c) 要求以安全的方式将临时口令给予用户。要避免用于第三方或不受保护的(明文)电子邮件报文。用户应确认收到口令。

口令决不能以不受保护的形式存储在计算机系统内(关于用户标识和鉴别参见其他技术，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)。

9.2.4 用户访问权利的评审

为维护对数据和信息服务访问的有效控制，管理层应定期实施一正式过程，以评审用户的访问权利，使得：

a) 定期(推荐周期为 6 个月)和在任何变更之后，用户的访问权利要受到评审(见 9.2.1)；

b) 以更频繁的时间间隔评审专门的有特权的访问权利的授权(见 9.2.2)；推荐周期为 3 个月；

c) 定期检查特权分配，以确保不能获得未授权的特权。

9.3 用户职责

目的：防止未授权用户访问。

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。

9.3.1 口令使用

在选择和使用口令时用户应遵守良好的安全习惯。

口令提供了确认用户身份的手段，因此，要建立访问信息处理设施和服务的权利。建议所有用户：

a) 保密口令；

b) 避免保留口令的纸记录，除非可以安全地保存；

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) 选择具有最小长度为 6 个字符的优质口令，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) 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。

如果用户需要访问多服务或平台,并且要求维护多个口令,则应建议他们可以使用一个优质的口令(见上述 d))用于所有服务,而这些服务对所存储的口令提供了合理级别的保护。

9.3.2 无人值守的用户设备

用户应确保无人值守的设备具有合适的保护。在用户区域内安装的设备(例如,工作站或文件服务器),在此时间内无人值守时,可以要求特别保护,使其免受未授权访问。所有用户和合同商应了解保护无人值守设备的安全要求和规定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,有口令保护的屏蔽保护程序;

b) 当会话结束时退出主计算机(即,不仅仅关掉 PC 或终端);

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

9.4 网络访问控制

目的:保护网络服务。

对内部和外部网络服务的访问均应加以控制。

这是确保访问网络服务的用户不损坏这些网络服务的安全所必需的,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界面;

b) 对用户和设备有合适的鉴别机制;

c) 对用户访问信息服务的控制。

9.4.1 使用网络服务的策略

与网络服务的不安全连接可以影响整个组织。仅向用户提供直接访问专门授权使用的服务。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。

应制定关于使用网络和网络服务的策略。这应包括:

a) 允许待访问的网络和网络服务;

b) 确定允许谁访问哪些网络和网络服务的授权规程;

c) 保护访问网络连接和网络服务的管理控制和规程。

该策略应与业务访问控制策略相一致(见 9.1)。

9.4.2 强制路径

可能需要控制从用户终端到计算机服务的路径。网络应设计成能允许最大范围的共享资源和路由选择灵活性。这些特征也可能对未授权访问业务应用或未授权使用信息设施提供机会。引入限制用户终端和授权其用户访问的计算机服务之间的路由的控制,例如创建强制路径可以减少这种风险。

强制路径的目的是防止任何用户选择的路由超出用户终端和授权用户访问该服务之间的路由。

这通常要求在路由的不同点处实施许多控制。该原则是为了在网络的每个点上通过预先定义的选择限制路由选择选项。

例如:

a) 分配专用线路或电话号码;

b) 自动地将端口连接到规定的应用系统或安全网关;

c) 限制各个用户的选单和子选单的选项；

d) 防止无限制的网络漫游；

e) 对外部网络用户，强制其使用所规定的应用系统和/或安全网关；

f) 主动控制所允许的源地址经由安全网关（例如，防火墙）到目的地址的通信；

g) 通过建立分离的逻辑域，例如，虚拟专用网限制组织范围内的用户群的网络访问（也见9.4.6）。

强制路径的要求应基于业务访问控制策略（见 9.1）。

9.4.3 外部连接的用户鉴别

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。

例如，可以使用基于密码技术硬件令牌或询问/响应协议获得远程用户的鉴别。专线或网络用户地址检验设施也可用来提供连接来源的保证。

回拨规程和控制，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规程和控制。

9.4.4 结点鉴别

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。因此，应鉴别与远程计算机系统的连接。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。在上述9.4.3中给出了鉴别的某些例子以及如何获得它。

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（见9.4.3）。

9.4.5 远程诊断端口保护

应安全地控制对诊断端口的访问。许多计算机和远程通信系统装配了拨号远程诊断设施，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。因此，它们应受到合适的安全机制的保护，例如，带钥匙的锁和规程，以确保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。

9.4.6 网络分离

随着可以要求互连或共享信息处理设施和网络设施的合伙方的形成，网络正在日益扩充超出传统组织边界范围。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。在这种环境下，应考虑在网络范围内引入控制以分离信息服务群、用户群和信息系统群。

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周边所保护。这样的周边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 9.4.7 和 9.4.8），并且能按照组织的访问控制策略阻挡未授权访问（见 9.1）。这种类型的网关例子是通常称作防火墙的东西。

将网络分离成若干域的准则应基于访问控制策略和访问要求（见 9.1），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 9.4.7 和 9.4.8）。

9.4.7 网络连接控制

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，可能需要引入控制，以限制用户的连接能力。这样的控制可以通过网关来实现，该网关借助预先定义的表或规则过滤通信量。所应用的限制应基于业务应用的访问策略和要求(见 9.1)并应相应地进行维护和更新。

施加限制的应用例子有：

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) 与时刻或日期相关联的网络访问。

9.4.8 网络路由选择控制

共享网络，可以要求引入路由选择控制，特别是扩充跨越组织边界的那些共享网络，以确保计算机连接和信息流不违反业务应用的访问控制策略(见 9.1)。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。

路由选择控制应基于确定的源地址和目的地址检验机制。为了隔离网络和阻止路由从某一组织的网络扩展到另一组织的网络，网络地址变换也是一种很有用的机制。它们可以用软件或硬件来实现。实现者要了解所采用的机制的强度。

9.4.9 网络服务的安全

各种各样的公共网络服务和专用网络服务都是可用的，其中某些服务提供增值服务。网络服务可以有独特的或复杂的安全特性。使用网络服务的组织应确保提供一种对所使用的各种服务的安全属性的清晰描述。

9.5 操作系统访问控制

目的：防止未授权计算机访问。

操作系统级的安全设施应该用来限制访问计算机资源。这些设施应能做下列事情：

a) 标识和验证每个授权用户的身份，如果需要，还标识和验证每个授权用户的终端或位置；

b) 记录成功和失败的系统访问；

c) 提供合适的鉴别手段，如果使用口令管理系统，则它应确保优质口令(见 9.3.1d))；

d) 若合适，限制用户的连接次数。

如果在业务风险的基础上，证明其他的访问控制方法(诸如，询问—响应)是正确的，则这些访问控制方法是可用的。

9.5.1 自动化终端标识

为鉴别与特定位置和便携式设备的连接，应考虑自动化终端标识。如果重要的会话只能从特定位置或计算机终端进行启动，那么，自动化终端标识就是一种可以使用的技术。终端的或与终端连接的标识符可用来指示是否允许这个特定终端启动或接收特定事务。将物理保护应用于终端以维护终端标识符的安全，可能是必要的。许多其他技术也可用来鉴别用户(见 9.4.3)。

9.5.2 终端登录规程

经由安全登录过程可得到对信息服务的访问。登录到计算机的规程应设计成能使未授权访问的机会减到最小。因此，登录规程泄露出关于系统的信息最少，以避免向未授权用户提供不必要的帮助。良好的登录规程应：

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) 显示通用告警通知，只有已授权的用户才能访问本计算机；

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，才确认登录信息。如果出现差错情况，则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；

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；

f) 限制登录规程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) 自最后成功登录以来，任何不成功登录尝试的细节。

9.5.3 用户标识和鉴别

所有用户(包括技术支持人员，诸如操作者，网络管理员、系统程序员和数据库管理员)应该拥有并只能使用他们个人专用的唯一标识符(用户 ID)，以使得各个活动可以追踪到各个责任人。用户 ID 应不给出用户特权级别的任何指示(见 9.2.2)，例如，管理者，超级用户。

在例外环境下，如果存在清晰的业务好处，可以使用一群用户或一项特定作业共享的用户 ID 的用法。对于这样的情况，应将经管理的批准形成文档。为维护可核查性，可以要求附加的控制。

有各种鉴别规程，它们可用来证明声称的用户身份。口令(也见 9.3.1 和下面的条款)是一种很通常的提供标识和鉴别(I&A)的方法，因为它基于只有该用户知道的秘密。使用密码手段和鉴别规程也可以获得同样的结果。

用户拥有的客体(诸如记忆令牌或智能卡)也可以用于 I&A。利用个人的唯一特征或属性的生物统计鉴别技术也可用来鉴别个人的身份。机制和技术的安全组合将产生更强的鉴别。

9.5.4 口令管理系统

口令是确认用户访问计算机服务权限的主要手段之一。口令管理系统应提供有效的、交互式的、确保优质口令的装置(关于口令使用的指南见 9.3.1)。

某些应用要求由某个独立机构分配的用户口令。在大多数情况下，口令由用户选择和维护。

良好的口令管理系统应：

a) 强制使用个人口令，以维护可核查性；

b) 若合适，允许用户选择和变更他们自己的口令，并且包括证实规程，以便考虑到输入出错的情况；

c) 强制选择 9.3.1 中描述的优质口令；

d) 若用户维护他们自己的口令，则强制口令按 9.3.1 描述进行变更；

e) 若用户选择口令，则在第一次登录时强制他们变更临时的口令；

f) 维护一份先前用户口令的记录，例如在先前 12 个月内，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) 用单向加密算法的加密形式存储口令；

j) 在软件安装之后，变更默认的厂商口令。

9.5.5 系统实用程序的使用

大多数计算机都装有一个或多个系统实用程序，而该系统实用程序可能能够超越系统控制和应用控制。必需限制和严格地控制它们的使用。应考虑下列控制：

a) 对于系统实用程序，使用鉴别规程；

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；

d) 应对系统实用程序的特别使用授权；

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) 对系统实用程序的权限级别进行定义并形成文档；

h) 移去基于实用程序和系统软件的所有不必要软件。

9.5.6 保护用户的强制报警

对于可能是强制目标的用户，应考虑强制报警措施。决定是否提供这样的报警应基于风险的评估。为响应强制报警，要有定义的职责和规程。

9.5.7 终端超时

超过一段所定义不活动的时限，应关闭在高风险位置（例如，超出组织安全管理的公共或外部区域）或服务高风险系统的不活动的终端，以防止未授权个人访问。超过一段所定义不活动的时限，该超时设备应清空终端屏幕，并关闭应用和网络会话。超时延迟应反映该区域和终端用户的安全风险。

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 PC 机可以提供一种受限制的终端超时设备形式。

9.5.8 连接时间的限制

连接时间的限制应对高风险应用提供添加的安全。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。对于敏感的计算机应用，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）的终端的那些应用，应考虑这样的控制。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。

9.6 应用访问控制

目的：防止未授权访问保存在信息系统中的信息。

安全设施应该用来将访问限制在应用系统之内。

对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) 按照定义的业务访问控制策略，控制用户访问信息和应用系统功能；

b) 对能够超越系统控制或应用控制的任何实用程序和操作系统软件提供免遭未授权访问的保护；

c) 不损坏共享信息资源的其他系统的安全；

d) 只能够向责任人、其他指定的授权个人或定义的用户群提供信息访问。

9.6.1 信息访问限制

应按照定义的访问控制策略，基于各个业务应用要求和符合组织的信息安全策略向应用系统的用户（包括支持人员）提供对信息和应用系统功能的访问（见 9.1）。为了支持访问限制要求，应考虑下列控制：

a) 提供控制访问应用系统功能的选单；

b) 使用适当编辑用户文档来限制用户对未授权访问的信息或应用系统功能的了解；

c) 控制用户的访问权利，例如，读、写、删除和执行；

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。

9.6.2 敏感系统隔离

敏感系统可能要求一种专用的（隔离的）计算环境。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应运行在专用的计算机上、仅与可信的应用系

统共享资源或该应用系统没有任何限制。下列考虑适用：

a) 应由应用拥有者显式地标识出应用系统的敏感性，并将其形成文档(见 4.1.3)；

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拥有者商定。

9.7 对系统访问和使用的监督

目的：检测未授权活动。

为检测偏离访问策略，并记录可监督事件，以便在万一有安全事故时提供证据，应对系统进行监督。

系统监督提供检验所采用的控制的有效性和验证它与访问策略模型(见 9.1)的符合性。

9.7.1 事件记录

为辅助将来调查和访问控制监督，应产生记录异常情况和其他有关安全的事件的审核日志并保存一段时间。审核日志应包括：

a) 用户 ID；

b) 登录和退出的日期和次数；

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。

某些审核日志需要存档，这是由于它可以作为记录保留策略的一部分，或由于收集证据的需要(也见第 12 章)。

9.7.2 对系统使用的监督

9.7.2.1 风险规程和区域

应建立监督信息处理设施使用的规程。这些规程对确保用户仅执行已显式授权的活动是必要的。各个设施所要求的监督级别应通过风险评估来确定。应考虑的区域包括：

a) 已授权的访问，包括诸如下列细目：

1) 用户 ID；

2) 关键事件的日期和时间；

3) 事件的类型；

4) 所访问的文件；

5) 所使用的程序/实用程序；

b) 所有有特权的操作，诸如：

1) 超级用户账户的使用；

2) 系统启动和停止；

3) I/O 设备连接/断开；

c) 未授权访问尝试，诸如：

1) 失败的尝试；

2) 对于网关和防火墙的访问策略违规和通知；

3) 来自专有的入侵检测系统的警报；

d) 系统警报或故障，诸如：

1) 控制台警报或消息；

2) 系统日志异常；

3) 网络管理报警。

9.7.2.2 风险因素

监督活动的结果应定期评审。评审的频度取决于所涉及的风险。应考虑的风险因素包括：

a) 应用进程的关键程度；

b) 所涉及信息的价值、敏感性或关键程度；

c) 过去的系统被渗入和滥用经历；

d) 系统互连(特别是公共网络)的程度。

9.7.2.3 事件的记录和评审

日志评审涉及理解系统所面对的威胁以及这些威胁出现的方式。万一有安全事故时可能要求进一步调查的事件例子在9.7.1中给出。

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。

当分配日志评审的职责时，在承担评审的人员和监督其活动的人员之间的角色应考虑分开。

应特别注意记录设施的安全，因为如果篡改记录设施，就可能提供错误的安全断定。控制应瞄准防止未授权变更和操作问题，包括：

a) 记录设施解除激活；

b) 替换所记录报文类型；

c) 编辑或删除日志文件；

d) 使日志文件媒体被耗尽，或者不能记录事件或者自身盖写。

9.7.3 时钟同步

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或法律案例的证据。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。

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(UCT)或本地标准时。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规程。

9.8 移动计算和远程工作

目的：确保使用移动计算和远程工作设施时的信息安全。

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。

9.8.1 移动计算

当使用移动计算设施时，例如，笔记本机、掌上机、膝上机和移动电话，应特别小心确保业务信息不被泄露。应采用的正式策略要考虑到特别是在不受保护的环境下使用移动计算设施的工作风险。例如，安全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10.3)。

当这样的设施用于公共场合时，小心避免未授权的个人窥视的风险是很重要的。防范恶意软件的规程应到位并且保持经常更新(见8.3)。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。在成功标识和鉴别之后，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9.4)。

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7.2.5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。

9.8.2 远程工作

远程工作使用通信技术，使员工在其组织之外的一个固定地点能远程工作。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。重要的是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。

组织应考虑制订策略、规程和标准，以控制远程工作的活动。如果合适的安全安排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。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。

要考虑的控制和安排包括：

a) 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) 物理的安全；
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) 备份和业务连续性的规程；
h) 审核和安全监督；
i) 当远程工作活动停止时，撤销授权和访问权，并返回设备。

10 系统开发和维护

10.1 系统的安全要求

目的：确保构建在信息系统内的安全。

这将包括基础设施、业务应用和用户开发的应用。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安全要求。

应在项目的要求阶段标识出所有安全要求(包括基本维持运作的安排的需求)，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。

10.1.1 安全要求分析和规范

新系统或现有系统增强部分的业务要求的说明应规定控制的要求。这种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。当评价业务应用的软件包时，应进行类似的考虑。如果认为合适，管理层可能更愿意使用已独立评价和认证的产品。

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。分析安全要求和标识(满足安全要求的)控制的框架是风险评估和风险管理。

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。

10.2 应用系统的安全

目的:防止丢失、修改或滥用应用系统中的用户数据。

应用系统内应设计合适的控制和审核跟踪或活动日志,包括用户写的应用。这些应包括输入数据、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。

10.2.1 输入数据确认

输入到应用系统的数据应予以确认,以确保它是正确的和合适的。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)和参数值(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,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) 响应确认差错的规程;
e) 测试输入数据真实性的规程;
f) 定义在数据输入过程中所涉及的全部人员的职责。

10.2.2 内部处理的控制

10.2.2.1 风险区域

已经正确录入的数据可能由于处理差错或故意动作所损坏。应在系统中加入确认检验,以检测这种损坏。应用的设计应确保实施若干限制,以使处理故障导致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) 使用和定位程序中的增加和删除功能,以实现数据变更;
b) 防止程序以错误次序运行或在前面正在处理的故障下仍在运行的规程(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。

10.2.2.2 检验和控制

所要求的控制将取决于应用的性质和任何数据损坏对业务的影响。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(file)更新总量;
   3) 程序至程序的控制;
c) 确认系统生成的数据(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(见 10.3.3);

e) 求记录和文件的散列函数值总量；

f) 检验是否确保应用程序在正确时刻运行；

g) 检验程序是否确保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。

10.2.3 报文鉴别

报文鉴别是一种技术，它用来检测未授权的变更或损坏所发送的电子报文内容。它可以用硬件或支持物理报文鉴别器件的软件或软件算法实现。

对于有安全要求的应用，例如，非常重要的电子资金转移、规范、合同、建议等或其他类似的电子数据交换，应考虑报文鉴别，以保护报文内容的完整性。应进行安全风险评估，以确定是否要求报文鉴别，并且标识出最合适的实现方法。

不将报文鉴别设计成防止未授权泄露报文内容。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。

10.2.4 输出数据确认

应用系统输出的数据应被确认，以确保存储的信息的处理是正确的并且适于这些情况。一般而言，在承担合适的确认、验证和测试以及输出总是正确的前提下来构造系统。情况并不都如此。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规程；

e) 定义在数据输出过程中所涉及的全部人员的职责。

10.3 密码控制

目的：保护信息的保密性、真实性和完整性。

密码系统和技术应该用来保护被认为处于风险的信息以及其他控制不能提供充分保护的信息。

10.3.1 使用密码控制的策略

作出关于密码解决办法是否适合的判定应看作评估风险和选择控制的广泛过程的一部分。应进行风险评估，以确定信息的保护级别。然后，该评估可用来确定密码控制是否合适，应使用什么类型的控制以及用于什么目的和业务过程。

一个组织应制定关于使用密码控制来保护其信息的策略。这种策略是使利用密码技术的好处最大化和风险最小化所必需的，是避免不合适或不正确的使用所必需的。制定策略时，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) 密钥管理的方法，包括在密钥丢失、泄露或损坏的情况下，涉及恢复已加密信息的方法；

c) 角色和职责，例如，谁负责；

d) 策略的实施；

e) 密钥管理；

f) 如何确定合适的密码保护级别；

g) 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)。

10.3.2 加密

加密是一种可以用来保护信息保密性的密码技术。为保护敏感的或关键的信息，可以考虑采用。

根据风险评估，应标识出所要求的保护级别，而并要考虑到所使用的加密算法的类型和质量以及所使用的密码密钥的长度。

当实施组织的密码策略时，应考虑到规章和国家的限制，这些规章和国家的限制可能适用于使用世

界不同地区的密码技术，并且可能适用于发布越境的已加密的信息流。另外，还应考虑到适用于密码技术的出口和进口的控制。(也见 12.1.6)。

为标识合适的保护级别，在选择提供所要求的保护和实现安全的密钥管理(也见 10.3.5)安全系统的合适的产品，应征求专家的意见。另外，在组织试图使用加密技术时，也需要征询有关可能适用的法律和规章的法律建议。

10.3.3 数字签名

数字签名提供一种保护电子文件的真实性和完整性的手段。例如，若需要验证谁签署了电子文档和检验签署的文档内容是否已变更，则数字签名可用于电子商务。

数字签名可适用于电子处理文档的任何形式，例如，数字签名可用来签署电子支付、资金转移、合同和协议。使用以唯一相关密钥对为基础[其中一个密钥(私有密钥)用来创建签名，另一密钥(公开密钥)用来检验该签名]的密码技术实现数字签名。

要小心保护私有密钥的保密性。这个密钥应该被秘密地保存，因为访问过这个密钥的任何人都可能借此伪造该密钥拥有者的签名来签署文件(例如，支付、合同)。另外，保护公开密钥的完整性很重要。通过使用公开密钥证书提供这种保护(见 10.3.5)。

对所使用的签名算法的类型和质量以及所使用的密钥长度需要给予考虑。用于数字签名的密钥应不同于用于加密的密钥。

当使用数字签名时，对描述数字签名在法律上受其约束的条件的任何相关法律，应给予考虑。例如，在电子商务的情况下，知道数字签名的法律地位是重要的。可能需要具有约束的合同或其他协议，以便在法律框架不充足的场合下支持使用数字签名。关于可能适用于组织预期的数字签名使用的法律法规，关于这些法律法规，应遵循国家相关法律法规，或征询我国法律建议。

10.3.4 抗抵赖服务

可能需要解决关于事件或动作是否发生而引起的争端，例如，涉及在电子合同上或电子支付时使用数字签名的争端，则应使用抗抵赖服务。抗抵赖服务可帮助建立证据，以证明特定事件或动作是否发生，例如，针对试图否认发送签名电子邮件使用的数字签名说明。这些服务基于使用加密和数字签名技术(也见 10.3.2 和 10.3.3)。

10.3.5 密钥管理

10.3.5.1 密钥的保护

密钥的管理对有效使用密码技术来说是必需的。密钥的任何泄露或丢失可能导致对信息的保密性、真实性和/或完整性的损害。为支持组织使用两种类型的密码技术，管理系统应到位，这两种密码技术为：

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(见 10.3.2)，并可用来产生数字签名(见 10.3.3)。

所有密钥应防止被修改和破坏，秘密密钥和私有密钥需要防止未授权泄露。密码技术也可用于上述目的。应使用物理保护方法来保护用于生成、存储和归档密钥的设备。

10.3.5.2 标准、规程和方法

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。

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。

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。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。通过使用公开密钥证书解决这个问题。应按照将与公开/私有密钥对的拥有者相关的信息与该公开密钥唯一地捆绑起来的方法产生这些证书。因此，重要的是生成这些证书的管理过程是可信的。这个过程在通常由某一认证机构完成。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 4.2.2）。

10.4 系统文件的安全

目的：确保按安全方式管理 IT 项目和支持活动。应控制对系统文件的访问。

维护系统完整性应是应用系统或软件的用户功能或开发组的职责。

10.4.1 运行软件的控制

在运行系统上实现软件，应提供控制。为使运行系统被损坏的风险减到最小，应考虑下列控制。

a) 仅由指定的（程序）库管理员根据相应的管理授权进行运行程序库的更新（见 10.4.3）；

b) 若有可能，运行系统只安装可执行的代码；

c) 直到获得成功测试和用户验收的证据和已更新相应的源程序库以前，还要向运行系统提供可执行的代码；

d) 应维护对运行程序库的所有更新的审核日志；

e) 应保留软件的先前版本作为应急措施。

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。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。

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。

10.4.2 系统测试数据的保护

应保护和控制测试数据。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。应避免使用包含个人信息的运行数据库。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。

10.4.3 源程序库的访问控制

为了减少计算机程序被损坏的可能，对源程序库的访问应维护严格的控制(也见 8.3)，例如：

a) 若有可能，在运行系统中不应保留源程序库；

b) 对于每个应用应指定一位程序库管理员；

c) IT 支持人员不应不受限制地访问源程序库；

d) 处于开发和维护的程序不应保持在运行源程序库中；

e) 更新源程序库和向程序员发布源程序应按照此应用的 IT 支持管理者的授权仅由指定的(程序)库管理员完成；

f) 程序列表应保持在安全的环境中(见 8.6.4)；

g) 应维护对源程序库所有访问的审核日志；

h) 源程序的老版本以及所有支持软件、作业控制、数据定义和规程应予以归档，同时对它们运行时的准确日期和次数有一个清晰的说明；

i) 维护和拷贝源程序库应受严格变更控制规程的制约(见 10.4.1)。

10.5 开发和支持过程的安全

目的：维护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。

10.5.1 变更控制规程

为使信息系统的损坏减到最小，对变更的实施应有严格的控制。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，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。变更应用软件可能影响操作环境。只要可行，应用和操作变更控制规程应集成起来(也见 8.1.2)。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) 确保在每次变更完成时，更新系统文档集合，旧的文档进行归档或处置；

i) 维护所有软件更新的版本控制；

j) 维护所有变更请求的审核踪迹；

k) 当需要时，确保对操作文档(见 8.1.1)和用户规程作合适的修改；

l) 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。

许多组织维持一个用户测试新软件的环境，并与开发和产品环境隔开。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。

10.5.2 操作系统变更的技术评审

有必要周期地变更操作系统，例如，安装新近供应的软件版本或补丁。当变更出现时，应评审和测试应用系统，以确保对运行或安全没有任何负面影响。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 11 章)。

10.5.3 软件包变更的限制

不鼓励修改软件包。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。

10.5.4 隐蔽信道和特洛伊代码

隐蔽信道可能通过某些间接的看不见的手段泄露信息。可以通过变更由计算机的安全和不安全要素可访问的参数来激活该信道，或者通过将信息嵌入到数据流来激活该信道。设计特洛伊代码的目的是无须由程序的接受者或用户授权、通知和要求即可影响系统。隐蔽信道和特洛伊代码几乎不可能由偶然事故出现。若关心隐蔽信道或特洛伊代码，则应考虑下列事项：

a) 仅从声誉好的来源采购软件程序；

b) 采购以源代码表示的程序，这样可以验证该代码；

c) 使用已评价的产品；

d) 在运行之前，检查所有源代码；

e) 代码一旦安装，就要控制对代码的访问和修改；

f) 使用已证明可信的人员参与系统的工作。

10.5.5 外包软件开发

在外包软件开发的情况下，应考虑下列各点：

a) 落实准许证、代码所有权和知识产权(见 12.1.2)；

b) 所完成工作的质量和准确性的认证；

c) 万一有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) 代码质量的合同要求；

f) 在安装前，测试是否检测到特洛伊代码。

11 业务连续性管理

11.1 业务连续性管理的各方面

目的：减少业务活动的中断，保护关键业务过程免受主要故障或灾难的影响。

为通过预防和恢复控制的组合，将灾难和安全故障(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)所引起的损害减少到可接受的程度，应实现业务连续性管理过程。

应分析灾难、安全故障和服务丢失的影响。为确保业务过程能在要求的时段内及时恢复，应开发和实现应急计划。这种计划应予以维护和实施，并成为所有其他管理过程的组成部分。

业务连续性管理应包括标识和减少风险、限制有害事故的影响以及确保及时重新开始基本操作的控制。

11.1.1 业务连续性管理过程

为开发和维护整个组织的业务连续性，应有一种到位的受管理的过程。它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；

b) 推断对业务可能产生中断的影响（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；

c) 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；

d) 正式提出与商定的业务目标和优先权一致的业务连续性战略，并将其形成文档；

e) 正式提出与商定的战略一致的业务连续性计划，并将其形成文档；

f) 将定期测试和更新适当的计划和过程；

g) 确保把业务连续性的管理包含在组织的过程和结构中。协调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，例如，信息安全管理协调小组（见 4.1.1）。

11.1.2 业务连续性和影响分析

业务连续性要从标识可能引起业务过程中断的事件开始，例如，设备故障、水灾和火灾。这之后是风险评估，以确定这些中断的影响（根据损坏程度和复原周所需时间两者）。应在业务资源和过程的拥有者全面参与的情况下，进行这些活动。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。

根据风险评估的结果，应开发战略计划，以确定业务连续性的总体途径。该计划一旦被制定，就应由管理层签署。

11.1.3 制定和实施连续性计划

应开发若干计划，以便在关键业务过程中断或失效之后所要求的时段内维持或恢复业务操作。业务连续性计划过程应考虑下列内容：

a) 全部职责和应急规程的标识和协议；

b) 实施应急规程，以在所要求的时段内恢复和复原。特别注意对处于适当位置的外部业务相关方和合同的评估；

c) 将已商定的规程和过程形成文档；

d) 用已商定的应急规程和过程（包括危机管理）教育员工；

e) 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服务。应考虑到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。

11.1.4 业务连续性计划框架

应维护一个业务连续性计划的框架，以确保全部计划一致，并标识出检验和维护的优先权。每一业务连续性计划应清晰地规定其启动的条件，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。

业务连续性计划框架应考虑下列内容：

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) 描述危及业务操作和/或人员的生命事件之后所要采取的动作的应急规程。这应包括公共关系管理部门和与相应公共管理局有效联系的安排，例如，警察、消防和本地政府；

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) 描述要采取行动的重新使用规程，以恢复正常业务操作；

e) 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；

f) 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；

g) 各个人员的职责，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。

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。

11.1.5 检验、维护和重新评估业务连续性计划

11.1.5.1 检验计划

在检验时，业务连续性计划可能失败，通常是因为在设备或人员方面不正确的假设、观察或变更。因此要定期地检验计划，以确保它们最新和有效。这些检验也应确保恢复小组的所有成员和其他相关人员都了解这些计划。

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。建议经常地检验计划的各个部分。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，但要反映特定恢复计划的性质。

11.1.5.2 维护和重新评估计划

业务连续性计划要通过定期评审和更新来维护，以确保它们连续有效(见11.1.5.1～11.1.5.3)。规程应包含在组织的变更管理大纲中，以确保相应地指出业务连续性事项。

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)。

12 符合性

12.1 符合法律要求

目的：避免违反任何刑法与民法、法律法规的义务或合同的义务，以及任何安全要求的义务。

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。

12.1.1 可用法律的标识

对每个信息系统应明确定义所有相关法律法规和合同的要求，并将其形成文档。为满足这些要求的特定控制和各个人员的职责应同样加以定义并形成文档。

12.1.2 知识产权(IPR)

12.1.2.1 版权

应实施合适的规程，以确保在使用有关可能存在知识产权(例如，版权、设计权、商标)的材料方面符合法律要求。违反版权可能导致可以涉及刑事诉讼的法律行动。

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。

12.1.2.2 软件版权

通常根据许可协议供应专有软件产品，而该协议限定产品用于指定的机器，并且可以限制只能拷贝到创建的备份副本上。应考虑下列控制：

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) 颁发软件产品采办规程的标准；

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；

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(也见 8.7.6)。

12.1.3 保护组织的记录

应防止丢失、破坏和篡改组织的重要记录。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。

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媒体的类型，例如，纸记录、缩微胶片、磁媒体、光媒体。应安全地保存与已加密档案或数字签名(见 10.3.2 和 10.3.3)有关的任何相关(密码)密钥，并且当需要时才提供给已授权的人员。

对存储记录的媒体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。

若选择了电子存储媒体，应建立规程，以确保在整个保存周期能访问数据(媒体和格式的可读性)，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，使所要求的数据能以法庭可接受的方式进行检索，例如，所要求的各种记录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，应允许恰当地销毁这些记录。

为履行这些义务，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。

12.1.4 个人信息的数据保护和隐私

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。

遵守数据保护法需要有合适的管理结构和控制。通常最好由任命的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：把关于在结构化文件中保存个人信息的建议通知数据保护官员；确保认识到相关法律所规定的数据保护原则。

12.1.5 防止滥用信息处理设施

组织的信息处理设施是为业务目的而提供的。管理层应授权它们的使用。在没有管理层批准的情况下，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这种活动，应引起关注相应纪律行动的各个管理者的注意。

监督这种使用合法性由国家规定，并且可以要求将这种监督通知给雇员或者获得他们同意。在实施监督规程之前，应采取合法忠告。

国家拥有防止计算机滥用的法律，或者是处于引入法律的过程中。对于未授权目的而使用计算机是一种刑事犯法。因此，最基本的是所有用户都要知道允许他们访问的准确范围。例如，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。

12.1.6 遵循密码控制的规章

应注意实施协议、法律、规章或其他指令，以控制对密码控制的访问或使用。这种控制应包括：

a) 使用国家主管部门审批的密码算法和密码产品；

b) 执行密码功能的计算机硬件和软件的进口和/或出口；

c) 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；

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。

12.1.7 证据的收集

12.1.7.1 证据规则

必需有充分的证据来支持针对个人或组织的行动。只要该行动是一种内部纪律事件，则通过内部规程描述必要的证据。

若该行动涉及民事或刑事的法律，则所提供的证据应符合相关法律或听取该案例的特定法庭的规则所提出的证据规则。一般，这些规则包括：

a) 证据的可接纳性：该证据能否用于法庭；

b) 证据的份量：该证据的质量和完整性；

c) 在由该系统存储和处理待恢复该证据的整个周期内，控制已正确地和一致地运行的充分证据(即，过程控制证据)。

12.1.7.2 证据的可接纳性

为获得证据的可接纳性，组织应确保其信息系统符合任何发布的标准或实用规则，以便产生可接纳的证据。

12.1.7.3 证据的质量和完整性

为获得证据的质量和完整性，需要强有力的证据线索。一般，可以根据下列条件建立这种强有力的线索：

a) 对于纸文件：安全地保存原件，并且将以下事件记录下来，即谁找到它，在何处找到它，何时找到它和谁目击发现。任何调查应确保原件不能被篡改；

b) 对于计算机媒体上的信息：应采用任何可移动媒体的拷贝，硬盘或存储器内信息的拷贝，以确保可用性。应保存在拷贝过程期间的所有行动日志，并目击该过程。应安全地保存该媒体和日志的一个拷贝。

当第一次检测到事故时，导致可能的法庭行动可能不明显。因此，在认识到事故严重性之前，存在偶然毁坏必要证据的危险。合理的做法是，使律师或警察早期介入任何预期的法律行动，并听取其关于所需证据方面的建议。

12.2 安全策略和技术符合性的评审

目的：确保系统符合组织安全策略和标准。

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。

12.2.1 符合安全策略

管理者应确保正确地执行其职责领域内的所有安全规程。另外，为确保符合安全策略和标准，应考虑对组织内各个领域进行定期评审。这些领域应包括如下：

a) 信息系统；

b) 系统提供者；

c) 信息和信息资产的责任人；

d) 用户；

e) 管理层。

信息系统责任人(见 5.1)应支持定期评审其系统是否符合相应的安全策略、标准和其他安全要求。在 9.7 中包括了对系统使用的运行监督。

12.2.2 技术符合性检验

为符合安全实施要求，应定期检验信息系统。技术符合性检验包括检查运行系统，以确保已正确实现的硬件和软件控制。这种类型的符合性检验需要有专家的技术帮助。它应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。

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性，并用于检验这些控制在防止由于这些脆弱性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性的情况。

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。

12.3 系统审核考虑

目的：使系统审核过程效力最大，使对系统审核过程的干扰最小。

在系统审核期间，为保护运行系统和审核工具，应有控制。

为保护审核工具的完整性和防止滥用审核工具，也要求有保护措施。

12.3.1 **系统审核控制**

应小心地规划和商定涉及运行系统检验的审核要求和活动，以使中断业务过程的风险减至最小。应遵守下列事项。

a) 审核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。当审核完成时，应擦除这些拷贝；

e) 应显式地标识和提供执行检验的 IT 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；

h) 所有规程、要求和职责应形成文档。

12.3.2 **系统审核工具的保护**

应保护对系统审核工具(即软件或数据文件)的访问，以防止任何可能的滥用或损坏。这些工具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。