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

中 华 人 民 共 和 国
国 家 标 准
信息技术 信息安全管理实用规则
GB/T 19716—2005
*
中国标准出版社出版发行
北京西城区复兴门外三里河北街16号
邮政编码:100045
http://www.spc.net.cn
电话:63787337、63787447
2005年8月第一版 2005年8月电子版制作
*
书号:155066·1-23058

目　　次

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：