ICS 35.040
L 80

中华人民共和国国家标准

GB/T 22081—2008/ISO /IEC 27002:2005
代替 GB/T 19716—2005

信息技术　安全技术
信息安全管理实用规则

**Information technology—Security techniques—
Code of practice for information security management**

(ISO/IEC 27002:2005, IDT)

2008-06-19 发布　　2008-11-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准等同采用 ISO/IEC 27002:2005《信息技术　安全技术　信息安全管理实用规则》。仅有编辑性修改。

本标准是对 GB/T 19716—2005 的修订。修订中依据 ISO/IEC 27002:2005 增删了一些技术内容。本标准代替 GB/T 19716—2005。

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、北京知识安全工程中心、上海三零卫士有限公司、北京市信息安全测评中心、北京数字认证中心负责起草。

本标准主要起草人：上官晓丽、许玉娜、胡啸、王新杰、赵战生、王连强、孔一童、曾波、刘海峰、汤永利、尚小鹏、闵京华。

本标准所代替标准的历次版本发布情况为：

——GB/T 19716—2005。

引　言

0.1　什么是信息安全

像其他重要业务资产一样，信息也是对组织业务至关重要的一种资产，因此需要加以适当地保护。在业务环境互连日益增加的情况下这一点显得尤为重要。这种互连性的增加导致信息暴露于日益增多的、范围越来越广的威胁和脆弱性当中（也可参考关于信息系统和网络的安全的 OECD 指南）。

信息可以以多种形式存在。它可以打印或写在纸上、以电子方式存储、用邮寄或电子手段传送、呈现在胶片上或用语言表达。无论信息以什么形式存在，用哪种方法存储或共享，都宜对它进行适当地保护。

信息安全是保护信息免受各种威胁的损害，以确保业务连续性，业务风险最小化，投资回报和商业机遇最大化。

信息安全是通过实施一组合适的控制措施而达到的，包括策略、过程、规程、组织结构以及软件和硬件功能。在必要时需建立、实施、监视、评审和改进这些控制措施，以确保满足该组织的特定安全和业务目标。这个过程宜与其他业务管理过程联合进行。

0.2　为什么需要信息安全

信息及其支持过程、系统和网络都是重要的业务资产。定义、实现、保持和改进信息安全对保持竞争优势、现金周转、赢利、守法和商业形象可能是至关重要的。

各组织及其信息系统和网络面临来自各个方面的安全威胁，包括计算机辅助欺诈、间谍活动、恶意破坏、毁坏行为、火灾或洪水。例如恶意代码、计算机黑客捣乱和拒绝服务攻击等导致破坏的安全威胁，已经变得更加普遍、更有野心和日益复杂。

信息安全对于公共和专用两部分的业务以及保护关键基础设施是非常重要的。在这两部分中信息安全都将作为一个使能者，例如实现电子政务或电子商务，避免或减少相关风险。公共网络和专用网络的互连、信息资源的共享都增加了实现访问控制的难度。分布式计算的趋势也削弱了集中的、专门控制的有效性。

许多信息系统并没有被设计成是安全的。通过技术手段可获得的安全性是有限的，宜通过适当的管理和规程给予支持。确定哪些控制措施宜实施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，还可能要求利益相关者、供应商、第三方、顾客或其他外部方的参与。外部组织的专家建议可能也是需要的。

0.3　如何建立安全要求

组织识别出其安全要求是非常重要的，安全要求有三个主要来源：

a）　一个来源是通过对组织进行风险的评估获得，并考虑到组织的整体业务策略与目标。通过风险评估，识别资产受到的威胁，评价易受威胁利用的脆弱性和威胁发生的可能性，估计潜在的影响；

b）　另一个来源是组织、贸易伙伴、承包方和服务提供者必须满足的法律、法规、规章和合同要求，以及他们的社会文化环境；

c）　进一步的来源是组织开发的支持其运行的信息处理的原则、目标和业务要求的特定集合。

0.4　评估安全风险

安全要求是通过对安全风险的系统评估予以识别的。用于控制措施的支出需要针对可能由安全失效导致的业务损害加以平衡。

风险评估的结果将帮助指导和决定适当的管理行动、管理信息安全风险的优先级以及实现所选择的用以防范这些风险的控制措施。

风险评估宜定期进行,以应对可能影响风险评估结果的任何变化。

更多的关于安全风险评估的信息见 4.1 的“评估安全风险”。

0.5 选择控制措施

一旦安全要求和风险已被识别并已作出风险处置决定,则宜选择并实现合适的控制措施,以确保风险降低到可接受的级别。控制措施可以从本标准或其他控制措施集合中选择,或者当合适时设计新的控制措施以满足特定需求。安全控制措施的选择依赖于组织所作出的决定,该决定是基于组织所应用的风险接受准则、风险处置选项和通用的风险管理方法,同时还宜遵守我国的法律法规。

本标准中的某些控制措施可被当作信息安全管理的指导原则,并且可用于大多数组织。下面在题为“信息安全起点”中将更详细的解释这些控制措施。

更多的关于选择控制措施和其他风险处置选项的信息见 4.2 的“处置安全风险”。

0.6 信息安全起点

许多控制措施被认为是实现信息安全的良好起点。它们或者是基于重要的法律要求,或者被认为是信息安全的常用惯例。

从法律的观点看,对某个组织重要的控制措施包括,根据适用的法律:

a) 数据保护和个人信息的隐私(见 15.1.4);

b) 保护组织的记录(见 15.1.3);

c) 知识产权(见 15.1.2)。

被认为是信息安全的常用惯例的控制措施包括:

a) 信息安全方针文件(见 5.1.1);

b) 信息安全职责的分配(见 6.1.3);

c) 信息安全意识、教育和培训(见 8.2.2);

d) 应用中的正确处理(见 12.2);

e) 技术脆弱性管理(见 12.6);

f) 业务连续性管理(见 14);

g) 信息安全事件和改进管理(见 13.2)。

这些控制措施适用于大多数组织和环境。

宜注意,虽然本标准中的所有控制措施都是重要的并且是应被考虑的,但是宜根据某个组织所面临的特定风险来确定任何一种控制措施是否是合适的。因此,虽然上述方法被认为是一种良好的起点,但它并不能取代基于风险评估而选择的控制措施。

0.7 关键的成功因素

经验表明,下列因素通常对一个组织成功地实施信息安全来说,十分关键:

a) 反映业务目标的信息安全方针、目标以及活动;

b) 与组织文化保持一致的实现、保持、监视和改进信息安全的方法和框架;

c) 来自所有级别管理者可见的支持和承诺;

d) 正确理解信息安全要求、风险评估和风险管理;

e) 向所有管理人员、员工和其他方传达有效的信息安全知识以使他们具备安全意识;

f) 向所有管理人员、员工和其他方分发关于信息安全方针和标准的指导意见;

g) 提供资金以支持信息安全管理活动;

h) 提供适当的意识、培训和教育;

i） 建立一个有效的信息安全事件管理过程；

j） 实施一个测量[1)]系统，它可用来评价信息安全管理的执行情况和反馈的改进建议。

0.8 编制组织的指南

本标准可作为是组织开发其详细指南的起点。对一个组织来说，本标准中的控制措施和指南并非全部适用，此外，很可能还需要本标准中未包括的另外的控制措施和指南。为便于审核员和业务伙伴进行符合性核查，当开发包含另外的指南或控制措施的文件时，对本标准中条款的引用可能是有用的。

1） 注意：信息安全测量不在本标准范围内。

信息技术　安全技术
信息安全管理实用规则

1　范围

本标准给出了一个组织启动、实施、保持和改进信息安全管理的指南和一般原则。本标准列出的目标为通常所接受的信息安全管理的目的提供了一般性指导。

本标准的控制目标和控制措施的实施旨在满足风险评估所识别的要求。本标准可作为建立组织的安全准则和有效安全管理实践的实用指南，并有助于在组织间的活动中构建互信。

2　术语和定义

下列术语和定义适用于本标准。

2.1

资产　asset

对组织有价值的任何东西[ISO/IEC 13335-1:2004]。

2.2

控制措施　control

管理风险的方法，包括策略、规程、指南、惯例或组织结构。它们可以是行政、技术、管理、法律等方面的。

注：控制措施也用于防护措施或对策的同义词。

2.3

指南　guideline

阐明要做什么和怎么做以达到方针策略中制定的目标的描述[ISO/IEC TR 13335-1:2004]。

2.4

信息处理设施　information processing facilities

任何信息处理系统、服务或基础设施，或放置它们的场所。

2.5

信息安全　information security

保持信息的保密性、完整性、可用性；另外也可包括例如真实性、可核查性、不可否认性和可靠性等。

2.6

信息安全事态　information security event

信息安全事态是指系统、服务或网络的一种可识别的状态的发生，它可能是对信息安全策略的违反或防护措施的失效，或是和安全关联的一个先前未知的状态[GB/Z 20985—2007]。

2.7

信息安全事件　information security incident

一个信息安全事件由单个的或一系列的有害或意外信息安全事态组成，它们具有损害业务运作和威胁信息安全的极大的可能性[GB/Z 20985—2007]。

2.8

方针　policy

管理者正式发布的总的宗旨和方向。