中国标准出版社第四编辑室　编

信息安全标准汇编

信息安全管理卷

中国标准出版社

信息安全标准汇编

信息安全管理卷

中国标准出版社第四编辑室　编

中国标准出版社

北　京

图书在版编目（CIP）数据

信息安全标准汇编. 信息安全管理卷/中国标准出版社第四编辑室编. —北京：中国标准出版社，2008
ISBN 978-7-5066-4424-2

Ⅰ.信… Ⅱ.①全… ②中… Ⅲ.信息系统-安全管理-国家标准-汇编-中国 Ⅳ.TP309-65

中国版本图书馆 CIP 数据核字（2008）第 188993 号

中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码：100045
网址 www.spc.net.cn
电话：68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 25.5 字数 774 千字
2008 年 12 月第一版 2008 年 12 月第一次印刷
*
定价 133.00 元

出 版 说 明

在信息化社会，信息技术飞速发展，随之而来的信息技术的安全问题日益突出，它关系到信息系统的正常运行和健康发展，影响到信息化社会的各个方面，不容忽视。国家标准化管理委员会已制定和发布了一系列信息安全国家标准，为我国信息系统的安全提供了技术支持，为信息安全的监督和管理提供了依据和指导。

为满足广大信息技术人员的需求，方便学习和查阅，我们将信息安全国家标准按照信息安全标准体系收集、分类、汇编成卷，共分为以下5卷：

——基础卷

——信息安全管理卷

——信息安全测评卷

——技术与机制卷

——密码技术卷

其中基础卷、信息安全测评卷、技术与机制卷根据需要又分为若干分册。

随着信息安全标准体系的完善和标准制修订情况的变化，本套汇编将陆续分卷分册出版。

本卷为信息安全管理卷，共收入截至2008年11月发布的相关标准13项。

编　　者

2008年11月

目　　录

前　言

本标准主要有三个目的：一，为计算机信息系统安全法规的制定和执法部门的监督检查提供依据；二，为安全产品的研制提供技术支持；三，为安全系统的建设和管理提供技术指导。

本标准的制定参考了美国的可信计算机系统评估准则(DoD 5200.28-STD)和可信计算机网络系统说明(NCSC-TG-005)。

在本标准文本中，黑体字表示较低等级中没有出现或增强的性能要求。

本标准是计算机信息系统安全保护等级系列标准的第一部分。计算机信息系统安全保护等级系列标准包括以下部分：

计算机信息系统安全等级划分准则；

计算机信息系统安全等级划分准则应用指南；

计算机信息系统安全等级评估准则；

……

本标准的实施应遵循配套国家标准的具体规定。

本标准由中华人民共和国公安部提出并归口。

本标准起草单位：清华大学、北京大学、中国科学院。

本标准主要起草人：胡道元、王立福、卿斯汉、景乾元、那日松、李志鹏、蔡庆明、朱卫国、陈钟。

本标准于2001年1月1日起实施。

本标准委托中华人民共和国公安部负责解释。

中华人民共和国国家标准

计算机信息系统
安全保护等级划分准则

GB 17859—1999

Classified criteria for security protection of computer information system

1 范围

本标准规定了计算机信息系统安全保护能力的五个等级，即：

第一级：用户自主保护级；

第二级：系统审计保护级；

第三级：安全标记保护级；

第四级：结构化保护级；

第五级：访问验证保护级。

本标准适用于计算机信息系统安全保护技术能力等级的划分。计算机信息系统安全保护能力随着安全保护等级的增高，逐渐增强。

2 引用标准

下列标准所包含的条文，通过在本标准中引用而构成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 5271 数据处理词汇

3 定义

除本章定义外，其他未列出的定义见 GB/T 5271。

3.1 计算机信息系统 computer information system

计算机信息系统是由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

3.2 计算机信息系统可信计算基 trusted computing base of computer information system

计算机系统内保护装置的总体，包括硬件、固件、软件和负责执行安全策略的组合体。它建立了一个基本的保护环境并提供一个可信计算系统所要求的附加用户服务。

3.3 客体 object

信息的载体。

3.4 主体 subject

引起信息在客体之间流动的人、进程或设备等。

3.5 敏感标记 sensitivity label

表示客体安全级别并描述客体数据敏感性的一组信息，可信计算基中把敏感标记作为强制访问控制决策的依据。

国家质量技术监督局 1999-09-13 批准　　2001-01-01 实施

3.6 安全策略 security policy

有关管理、保护和发布敏感信息的法律、规定和实施细则。

3.7 信道 channel

系统内的信息传输路径。

3.8 隐蔽信道 covert channel

允许进程以危害系统安全策略的方式传输信息的通信信道。

3.9 访问监控器 reference monitor

监控主体和客体之间授权访问关系的部件。

4 等级划分准则

4.1 第一级 用户自主保护级

本级的计算机信息系统可信计算基通过隔离用户与数据，使用户具备自主安全保护的能力。它具有多种形式的控制能力，对用户实施访问控制，即为用户提供可行的手段，保护用户和用户组信息，避免其他用户对数据的非法读写与破坏。

4.1.1 自主访问控制

计算机信息系统可信计算基定义和控制系统中命名用户对命名客体的访问。实施机制(例如：访问控制表)允许命名用户以用户和(或)用户组的身份规定并控制客体的共享；阻止非授权用户读取敏感信息。

4.1.2 身份鉴别

计算机信息系统可信计算基初始执行时，首先要求用户标识自己的身份，并使用保护机制(例如：口令)来鉴别用户的身份；阻止非授权用户访问用户身份鉴别数据。

4.1.3 数据完整性

计算机信息系统可信计算基通过自主完整性策略，阻止非授权用户修改或破坏敏感信息。

4.2 第二级 系统审计保护级

与用户自主保护级相比，本级的计算机信息系统可信计算基实施了粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。

4.2.1 自主访问控制

计算机信息系统可信计算基定义和控制系统中命名用户对命名客体的访问。实施机制(例如：访问控制表)允许命名用户以用户和(或)用户组的身份规定并控制客体的共享；阻止非授权用户读取敏感信息。**并控制访问权限扩散。自主访问控制机制根据用户指定方式或默认方式，阻止非授权用户访问客体。访问控制的粒度是单个用户。没有存取权的用户只允许由授权用户指定对客体的访问权。**

4.2.2 身份鉴别

计算机信息系统可信计算基初始执行时，首先要求用户标识自己的身份，并使用保护机制(例如：口令)来鉴别用户的身份；阻止非授权用户访问用户身份鉴别数据。**通过为用户提供唯一标识，计算机信息系统可信计算基能够使用户对自己的行为负责。计算机信息系统可信计算基还具备将身份标识与该用户所有可审计行为相关联的能力。**

4.2.3 客体重用

在计算机信息系统可信计算基的空闲存储客体空间中，对客体初始指定、分配或再分配一个主体之前，撤销该客体所含信息的所有授权。当主体获得对一个已被释放的客体的访问权时，当前主体不能获得原主体活动所产生的任何信息。

4.2.4 审计

计算机信息系统可信计算基能创建和维护受保护客体的访问审计跟踪记录，并能阻止非授权的用户对它访问或破坏。

计算机信息系统可信计算基能记录下述事件：使用身份鉴别机制；将客体引入用户地址空间（例如：打开文件、程序初始化）；删除客体；由操作员、系统管理员或（和）系统安全管理员实施的动作，以及其他与系统安全有关的事件。对于每一事件，其审计记录包括：事件的日期和时间、用户、事件类型、事件是否成功。对于身份鉴别事件，审计记录包含请求的来源（例如：终端标识符）；对于客体引入用户地址空间的事件及客体删除事件，审计记录包含客体名。

对不能由计算机信息系统可信计算基独立分辨的审计事件，审计机制提供审计记录接口，可由授权主体调用。这些审计记录区别于计算机信息系统可信计算基独立分辨的审计记录。

4.2.5 数据完整性

计算机信息系统可信计算基通过自主完整性策略，阻止非授权用户修改或破坏敏感信息。

4.3 第三级 安全标记保护级

本级的计算机信息系统可信计算基具有系统审计保护级的所有功能。此外，还需提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述；具有准确地标记输出信息的能力；消除通过测试发现的任何错误。

4.3.1 自主访问控制

计算机信息系统可信计算基定义和控制系统中命名用户对命名客体的访问。实施机制（例如：访问控制表）允许命名用户以用户和（或）用户组的身份规定并控制客体的共享；阻止非授权用户读取敏感信息。并控制访问权限扩散。自主访问控制机制根据用户指定方式或默认方式，阻止非授权用户访问客体。访问控制的粒度是单个用户。没有存取权的用户只允许由授权用户指定对客体的访问权。阻止非授权用户读取敏感信息。

4.3.2 强制访问控制

计算机信息系统可信计算基对所有主体及其所控制的客体（例如：进程、文件、段、设备）实施强制访问控制。为这些主体及客体指定敏感标记，这些标记是等级分类和非等级类别的组合，它们是实施强制访问控制的依据。计算机信息系统可信计算基支持两种或两种以上成分组成的安全级。计算机信息系统可信计算基控制的所有主体对客体的访问应满足：仅当主体安全级中的等级分类高于或等于客体安全级中的等级分类，且主体安全级中的非等级类别包含了客体安全级中的全部非等级类别，主体才能读客体；仅当主体安全级中的等级分类低于或等于客体安全级中的等级分类，且主体安全级中的非等级类别包含于客体安全级中的非等级类别，主体才能写一个客体。计算机信息系统可信计算基使用身份和鉴别数据，鉴别用户的身份，并保证用户创建的计算机信息系统可信计算基外部主体的安全级和授权受该用户的安全级和授权的控制。

4.3.3 标记

计算机信息系统可信计算基应维护与主体及其控制的存储客体（例如：进程、文件、段、设备）相关的敏感标记。这些标记是实施强制访问的基础。为了输入未加安全标记的数据，计算机信息系统可信计算基向授权用户要求并接受这些数据的安全级别，且可由计算机信息系统可信计算基审计。

4.3.4 身份鉴别

计算机信息系统可信计算基初始执行时，首先要求用户标识自己的身份，而且，计算机信息系统可信计算基维护用户身份识别数据并确定用户访问权及授权数据。计算机信息系统可信计算基使用这些数据鉴别用户身份，并使用保护机制（例如：口令）来鉴别用户的身份；阻止非授权用户访问用户身份鉴别数据。通过为用户提供唯一标识，计算机信息系统可信计算基能够使用户对自己的行为负责。计算机信息系统可信计算基还具备将身份标识与该用户所有可审计行为相关联的能力。

4.3.5 客体重用

在计算机信息系统可信计算基的空闲存储客体空间中，对客体初始指定、分配或再分配一个主体之前，撤销客体所含信息的所有授权。当主体获得对一个已被释放的客体的访问权时，当前主体不能获得原主体活动所产生的任何信息。

4.3.6 审计

计算机信息系统可信计算基能创建和维护受保护客体的访问审计跟踪记录，并能阻止非授权的用户对它访问或破坏。

计算机信息系统可信计算基能记录下述事件：使用身份鉴别机制；将客体引入用户地址空间（例如：打开文件、程序初始化）；删除客体；由操作员、系统管理员或（和）系统安全管理员实施的动作，以及其他与系统安全有关的事件。对于每一事件，其审计记录包括：事件的日期和时间、用户、事件类型、事件是否成功。对于身份鉴别事件，审计记录包含请求的来源（例如：终端标识符）；对于客体引入用户地址空间的事件及客体删除事件，审计记录包含客体名及**客体的安全级别。此外，计算机信息系统可信计算基具有审计更改可读输出记号的能力**。

对不能由计算机信息系统可信计算基独立分辨的审计事件，审计机制提供审计记录接口，可由授权主体调用。这些审计记录区别于计算机信息系统可信计算基独立分辨的审计记录。

4.3.7 数据完整性

计算机信息系统可信计算基通过自主和强制完整性策略，阻止非授权用户修改或破坏敏感信息。**在网络环境中，使用完整性敏感标记来确信信息在传送中未受损**。

4.4 第四级 结构化保护级

本级的计算机信息系统可信计算基建立于一个明确定义的形式化安全策略模型之上，它要求将第三级系统中的自主和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道。本级的计算机信息系统可信计算基必须结构化为关键保护元素和非关键保护元素。计算机信息系统可信计算基的接口也必须明确定义，使其设计与实现能经受更充分的测试和更完整的复审。加强了鉴别机制；支持系统管理员和操作员的职能；提供可信设施管理；增强了配置管理控制。系统具有相当的抗渗透能力。

4.4.1 自主访问控制

计算机信息系统可信计算基定义和控制系统中命名用户对命名客体的访问。实施机制（例如：访问控制表）允许命名用户和（或）以用户组的身份规定并控制客体的共享；阻止非授权用户读取敏感信息。并控制访问权限扩散。

自主访问控制机制根据用户指定方式或默认方式，阻止非授权用户访问客体。访问控制的粒度是单个用户。没有存取权的用户只允许由授权用户指定对客体的访问权。

4.4.2 强制访问控制

计算机信息系统可信计算基对外部主体能够直接或间接访问的所有资源（例如：主体、存储客体和输入输出资源）实施强制访问控制。为这些主体及客体指定敏感标记，这些标记是等级分类和非等级类别的组合，它们是实施强制访问控制的依据。计算机信息系统可信计算基支持两种或两种以上成分组成的安全级。**计算机信息系统可信计算基外部的所有主体对客体的直接或间接的访问应满足**：仅当主体安全级中的等级分类高于或等于客体安全级中的等级分类，且主体安全级中的非等级类别包含了客体安全级中的全部非等级类别，主体才能读客体；仅当主体安全级中的等级分类低于或等于客体安全级中的等级分类，且主体安全级中的非等级类别包含于客体安全级中的非等级类别，主体才能写一个客体。计算机信息系统可信计算基使用身份和鉴别数据，鉴别用户的身份，保证用户创建的计算机信息系统可信计算基外部主体的安全级和授权受该用户的安全级和授权的控制。

4.4.3 标记

计算机信息系统可信计算基维护与可被外部主体直接或间接访问到的计算机信息系统资源（例如：主体、存储客体、只读存储器）相关的敏感标记。这些标记是实施强制访问的基础。为了输入未加安全标记的数据，计算机信息系统可信计算基向授权用户要求并接受这些数据的安全级别，且可由计算机信息系统可信计算基审计。

4.4.4 身份鉴别

计算机信息系统可信计算基初始执行时，首先要求用户标识自己的身份，而且，计算机信息系统可

信计算基维护用户身份识别数据并确定用户访问权及授权数据。计算机信息系统可信计算基使用这些数据，鉴别用户身份，并使用保护机制（例如：口令）来鉴别用户的身份；阻止非授权用户访问用户身份鉴别数据。通过为用户提供唯一标识，计算机信息系统可信计算基能够使用户对自己的行为负责。计算机信息系统可信计算基还具备将身份标识与该用户所有可审计行为相关联的能力。

4.4.5 客体重用

在计算机信息系统可信计算基的空闲存储客体空间中，对客体初始指定、分配或再分配一个主体之前，撤销客体所含信息的所有授权。当主体获得对一个已被释放的客体的访问权时，当前主体不能获得原主体活动所产生的任何信息。

4.4.6 审计

计算机信息系统可信计算基能创建和维护受保护客体的访问审计跟踪记录，并能阻止非授权的用户对它访问或破坏。

计算机信息系统可信计算基能记录下述事件：使用身份鉴别机制；将客体引入用户地址空间（例如：打开文件、程序初始化）；删除客体；由操作员、系统管理员或（和）系统安全管理员实施的动作，以及其他与系统安全有关的事件。对于每一事件，其审计记录包括：事件的日期和时间、用户、事件类型、事件是否成功。对于身份鉴别事件，审计记录包含请求的来源（例如：终端标识符）；对于客体引入用户地址空间的事件及客体删除事件，审计记录包含客体名及客体的安全级别。此外，计算机信息系统可信计算基具有审计更改可读输出记号的能力。

对不能由计算机信息系统可信计算基独立分辨的审计事件，审计机制提供审计记录接口，可由授权主体调用。这些审计记录区别于计算机信息系统可信计算基独立分辨的审计记录。

计算机信息系统可信计算基能够审计利用隐蔽存储信道时可能被使用的事件。

4.4.7 数据完整性

计算机信息系统可信计算基通过自主和强制完整性策略，阻止非授权用户修改或破坏敏感信息。在网络环境中，使用完整性敏感标记来确信信息在传送中未受损。

4.4.8 隐蔽信道分析

系统开发者应彻底搜索隐蔽存储信道，并根据实际测量或工程估算确定每一个被标识信道的最大带宽。

4.4.9 可信路径

对用户的初始登录和鉴别，计算机信息系统可信计算基在它与用户之间提供可信通信路径。该路径上的通信只能由该用户初始化。

4.5 第五级 访问验证保护级

本级的计算机信息系统可信计算基满足访问监控器需求。访问监控器仲裁主体对客体的全部访问。访问监控器本身是抗篡改的；必须足够小，能够分析和测试。为了满足访问监控器需求，计算机信息系统可信计算基在其构造时，排除那些对实施安全策略来说并非必要的代码；在设计和实现时，从系统工程角度将其复杂性降低到最小程度。支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。系统具有很高的抗渗透能力。

4.5.1 自主访问控制

计算机信息系统可信计算基定义并控制系统中命名用户对命名客体的访问。实施机制（例如：访问控制表）允许命名用户和（或）以用户组的身份规定并控制客体的共享；阻止非授权用户读取敏感信息。并控制访问权限扩散。

自主访问控制机制根据用户指定方式或默认方式，阻止非授权用户访问客体。访问控制的粒度是单个用户。**访问控制能够为每个命名客体指定命名用户和用户组，并规定他们对客体的访问模式。**没有存取权的用户只允许由授权用户指定对客体的访问权。

4.5.2 强制访问控制

计算机信息系统可信计算基对外部主体能够直接或间接访问的所有资源(例如:主体、存储客体和输入输出资源)实施强制访问控制。为这些主体及客体指定敏感标记,这些标记是等级分类和非等级类别的组合,它们是实施强制访问控制的依据。计算机信息系统可信计算基支持两种或两种以上成分组成的安全级。计算机信息系统可信计算基外部的所有主体对客体的直接或间接的访问应满足:仅当主体安全级中的等级分类高于或等于客体安全级中的等级分类,且主体安全级中的非等级类别包含了客体安全级中的全部非等级类别,主体才能读客体;仅当主体安全级中的等级分类低于或等于客体安全级中的等级分类,且主体安全级中的非等级类别包含于客体安全级中的非等级类别,主体才能写一个客体。计算机信息系统可信计算基使用身份和鉴别数据,鉴别用户的身份,保证用户创建的计算机信息系统可信计算基外部主体的安全级和授权受该用户的安全级和授权的控制。

4.5.3 标记

计算机信息系统可信计算基维护与可被外部主体直接或间接访问到的计算机信息系统资源(例如:主体、存储客体、只读存储器)相关的敏感标记。这些标记是实施强制访问的基础。为了输入未加安全标记的数据,计算机信息系统可信计算基向授权用户要求并接受这些数据的安全级别,且可由计算机信息系统可信计算基审计。

4.5.4 身份鉴别

计算机信息系统可信计算基初始执行时,首先要求用户标识自己的身份,而且,计算机信息系统可信计算基维护用户身份识别数据并确定用户访问权及授权数据。计算机信息系统可信计算基使用这些数据,鉴别用户身份,并使用保护机制(例如:口令)来鉴别用户的身份;阻止非授权用户访问用户身份鉴别数据。通过为用户提供唯一标识,计算机信息系统可信计算基能够使用户对自己的行为负责。计算机信息系统可信计算基还具备将身份标识与该用户所有可审计行为相关联的能力。

4.5.5 客体重用

在计算机信息系统可信计算基的空闲存储客体空间中,对客体初始指定、分配或再分配一个主体之前,撤销客体所含信息的所有授权。当主体获得对一个已被释放的客体的访问权时,当前主体不能获得原主体活动所产生的任何信息。

4.5.6 审计

计算机信息系统可信计算基能创建和维护受保护客体的访问审计跟踪记录,并能阻止非授权的用户对它访问或破坏。

计算机信息系统可信计算基能记录下述事件:使用身份鉴别机制;将客体引入用户地址空间(例如:打开文件、程序初始化);删除客体;由操作员、系统管理员或(和)系统安全管理员实施的动作,以及其他与系统安全有关的事件。对于每一事件,其审计记录包括:事件的日期和时间、用户、事件类型、事件是否成功。对于身份鉴别事件,审计记录包含请求的来源(例如:终端标识符);对于客体引入用户地址空间的事件及客体删除事件,审计记录包含客体名及客体的安全级别。此外,计算机信息系统可信计算基具有审计更改可读输出记号的能力。

对不能由计算机信息系统可信计算基独立分辨的审计事件,审计机制提供审计记录接口,可由授权主体调用。这些审计记录区别于计算机信息系统可信计算基独立分辨的审计记录。计算机信息系统可信计算基能够审计利用隐蔽存储信道时可能被使用的事件。

计算机信息系统可信计算基包含能够监控可审计安全事件发生与积累的机制,当超过阈值时,能够立即向安全管理员发出报警。并且,如果这些与安全相关的事件继续发生或积累,系统应以最小的代价中止它们。

4.5.7 数据完整性

计算机信息系统可信计算基通过自主和强制完整性策略,阻止非授权用户修改或破坏敏感信息。在网络环境中,使用完整性敏感标记来确信信息在传送中未受损。

4.5.8 隐蔽信道分析

系统开发者应彻底搜索隐蔽信道，并根据实际测量或工程估算确定每一个被标识信道的最大带宽。

4.5.9 可信路径

当连接用户时（如注册、更改主体安全级），计算机信息系统可信计算基提供它与用户之间的可信通信路径。可信路径上的通信只能由该用户或计算机信息系统可信计算基激活，且在逻辑上与其他路径上的通信相隔离，且能正确地加以区分。

4.5.10 可信恢复

计算机信息系统可信计算基提供过程和机制，保证计算机信息系统失效或中断后，可以进行不损害任何安全保护性能的恢复。

ICS 35.040
L 80

中华人民共和国国家标准

GB/T 19715.1—2005/ISO/IEC TR 13335-1:1996

信息技术 信息技术安全管理指南 第1部分:信息技术安全概念和模型

Information technology—Guidelines for the management of IT security—Part 1:Concepts and models of IT security

(ISO/IEC TR 13335-1:1996,IDT)

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

GB/T 19715《信息技术　信息技术安全管理指南》分为五个部分：

——第1部分：信息技术安全概念和模型；

——第2部分：管理和规划信息技术安全；

——第3部分：信息技术安全管理技术；

——第4部分：防护措施的选择；

——第5部分：外部连接的防护措施。

本部分等同采用国际标准ISO/IEC TR 13335-1:1996《信息技术　信息技术安全管理指南　第1部分：信息技术安全概念和模型》。

本部分提出基本的管理概念和模型，将这些概念和模型引入信息技术安全管理是必要的。

本部分由中华人民共和国信息产业部提出。

本部分由全国信息安全标准化技术委员会归口。

本部分由中国电子技术标准化研究所(CESI)、中国电子科技集团第十五研究所、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负责起草。

本部分主要起草人：安金海、林中、林望重、魏忠、罗锋盈、陈星。

引　言

GB/T 19715 的目的是提供关于 IT 安全管理方面的指南，而不是解决方案。那些在组织内负责 IT 安全的个人应该可以采用本标准中的资料来满足他们特定的需求。本标准的主要目标是：

a) 定义和描述与 IT 安全管理相关的概念；

b) 标识 IT 安全管理和一般的 IT 管理之间的关系；

c) 提出了几个可用来解释 IT 安全的模型；

d) 提供了关于 IT 安全管理的一般的指南。

GB/T 19715 由多个部分组成。本部分为第 1 部分，提供了描述 IT 安全管理用的基本概念和模型的概述。本部分适用于负责 IT 安全的管理者，及那些负责组织的总体安全大纲的管理者。

第 2 部分描述了管理和规划方面。它和负责组织的 IT 系统的管理者相关。他们可以是：

a) 负责监督 IT 系统的设计、实施、测试、采购或运行的 IT 管理者；

b) 负责制定 IT 系统的实际使用活动的管理者。

第 3 部分描述了在一个项目的生存周期(比如规划、设计、实施、测试、采办或运行)所涉及的管理活动中适于使用的安全技术。

第 4 部分提供了选择防护措施的指南，以及通过基线模型和控制的使用如何受到支持。它也描述了它如何补充了第 3 部分中描述的安全技术，如何使用附加的评估方法来选择防护措施。

第 5 部分为组织提供了将它的 IT 系统连接到外部网络的指南。该指南包含了提供连接安全的防护措施的选择、使用，那些连接所支持的服务，以及进行连接的 IT 系统的附加防护措施。