ICS 35.020
L 09

GA

中华人民共和国公共安全行业标准

GA/T 391—2002

计算机信息系统安全等级保护管理要求

Management Requirements

in Computer Information System Classified Security Protection

2002-07-18 发布　　2002-07-18 实施

中华人民共和国公安部 发布

目　　次

a）前　　言

本标准作为GB17859-1999《计算机信息系统安全保护等级划分准则》的管理要求，是根据《中华人民共和国计算机信息系统安全保护条例》(1994年2月18日中华人民共和国国务院令147号发布)的规定编制的。

本标准是GB17859-1999系列配套标准中重要标准之一，与GB17859-1999相关的通用技术要求、操作系统要求、网络要求、数据库要求、工程要求、评估要求等标准共同组成计算机信息系统的安全等级保护体系。计算机信息系统的安全等级保护体系从计算机信息系统的管理层面、物理层面、系统层面、网络层面、应用层面、运行层面对计算机信息系统资源实施保护，作为计算机信息系统安全保护的支撑服务，管理层面则贯穿了其他五个层面，是其他五个层面实施安全等级保护的保证。

本标准吸收了ISO/IEC TR 13335[1] [2] [3] [4] [5]的管理概念，并结合计算机信息系统安全过程提出了比ISO/IEC TR 13335更详细的过程要求,对ISO/IEC 17799[6]的有关内容进行了提炼，并从安全过程和安全行政管理的总体要求进行了论述。本标准明确提出了管理层、物理层、网络层、系统层、应用层和运行层的安全管理要求，并将管理要求落实到GB17859－1999的五个等级上，更有利于对安全管理的继承、理解、分工实施，更有利于对安全管理的评估和检查。由于GB17859-1999中保护等级的划分是在充分考虑安全技术和安全风险控制的关系上制定的，安全等级越高，安全技术的费用和管理成本也就越高，从而能抵御更大的安全威胁，能有效建立起安全信心，降低IT使用风险。

本标准中，如无特殊说明，信息系统即指计算机信息系统，安全管理指计算机信息系统安全管理。

本标准由公安部公共信息网络安全监察局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：北京江南科友科技有限公司。

本标准主要起草人：王志强 颜基义 赵战生 黄云飞 周思源 伏劲松 文坊

b）引　　言

GB17859-1999是我国计算机信息系统信息安全等级管理的重要标准，已于1999年9月13日发布，其配套相关的标准，包括：

a）　计算机信息系统安全等级保护技术要求系列标准；

b）　计算机信息系统安全等级保护评估准则系列标准；

c）　计算机信息系统安全等级保护工程要求系列标准；

d）　计算机信息系统安全等级保护管理要求。

本标准如有与国家有关法律、法规冲突、不一致或不兼容的内容，应按国家有关法律、法规执行。涉及国家秘密的计算机信息系统应按照国家有关部门的规定执行。

本标准为计算机信息系统提出了计算机信息系统安全管理方面的要求，提供一个安全保护等级选择基准。各单位根据对计算机信息系统的安全要求，选择计算机信息系统的安全保护等级，并在本标准相应基准的基础上建立具体的计算机信息系统安全管理体系和安全标准，实施有效的安全管理，保障计算机信息系统的安全。

计算机信息系统安全等级保护管理要求

a） 范围

本标准依据GB17859-1999规定了计算机信息系统安全等级保护的管理要求。

本标准适用于相关部门依据国家有关规定实施计算机信息系统安全等级保护的安全管理。

b） 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 17859-1999　计算机信息系统安全等级划分准则

GA/T XX1-XXXX　计算机信息系统安全等级保护通用技术要求

GA/T XX2-XXXX　计算机信息系统安全等级保护操作系统要求

GA/T XX3-XXXX　计算机信息系统安全等级保护数据库要求

GA/T XX4-XXXX　计算机信息系统安全等级保护网络要求

GA/T XXX-XXXX　计算机信息系统安全等级保护工程要求

GA/T XXX-XXXX　计算机信息系统安全等级保护评估要求

中华人民共和国计算机信息系统安全保护条例(1994年2月18日中华人民共和国国务院令147号发布)

c） 术语和定义

GB 17859-1999 确立的及下列的术语和定义适用于本标准。

i.

机密性/保密性　confidentiality

这一性质使信息不泄露给非授权的个人、实体或进程，不为其所用。[GB/T 9387.2－1995 3.3.16]

ii.

数据完整性　data integrity

这一性质表明数据没有遭受以非授权方式所作的篡改或破坏。[GB/T 9387.2－1995 3.3.21]

iii.

可用性　availability

根据授权实体的请求可被访问与使用。[GB/T 9387.2－1995 3.3.11]

iv.

可确认性　accountability

这样一种性质，它确保一个实体的作用可以被独一无二地跟踪到该实体。[GB/T 9387.2－1995 3.3.3]

v.

访问控制 access control

防止对资源的未授权使用，包括防止以未授权方式使用某一资源。[GB/T 9387.2－1995 3.3.1]

vi.

安全审计 security audit

为了测试出系统的控制是否足够，为了保证与已建立的策略和操作堆积相符合，为了发现安全中的漏洞，以及为了建议在控制、策略和堆积中作任何指定的改变，而对系统记录与活动进行的独立观察和考核。[GB/T 9387.2－1995 3.3.47]

vii.

审计跟踪 security audit trail

收集起来并可用来使安全审计易于进行的数据。[GB/T 9387.2－1995 3.3.48]

viii.

威胁 threat

一种潜在的对安全的侵害。[GB/T 9387.2－1995 3.3.55]

ix.

鉴别信息 authentication information

用以建立身份有效性的信息。[GB/T 9387.2－1995 3.3.8]

x.

授权 authorization

授予权限，包括允许基于访问权的访问。[GB/T 9387.2－1995 3.3.10]

xi.

敏感性 sensitivity

资源所具有的一种特征，它意味着该资源的价值或重要性，也可能包含这一资源的脆弱性。[GB/T 9387.2－1995 3.3.53]

xii.

口令 password

机密的鉴别信息，通常由一串字符组成。[GB/T 9387.2－1995 3.3.39]

xiii.

信息系统安全管理体系 information system security management architecture

通过规划、组织、领导、控制等措施以实现组织或机构计算机信息系统安全目标的相互关联或相互作用的一系列支撑服务要素的集合。这些要素包括计算机信息系统安全组织或机构、计算机信息系统安全管理体系文件、控制措施、操作过程和程序等相关资源。

xiv.

风险评估 risk assessment

对信息、信息处理设施、信息处理过程和信息系统管理所受威胁、系统弱点保护不当等风险因素的发生可能性和后果影响的资产价值评估。

xv.

安全策略 security policy

对计算机信息系统中与安全相关的资源，尤其是敏感信息，进行管理、保护、控制和发布的规定和实施细则。一个计算机信息系统中可以有一个或多个安全策略。

d） 信息系统安全管理概述

i. 信息系统安全管理内涵

信息系统安全管理是对一个组织或机构中信息系统的生命周期全过程实施符合安全等级责任要求的科学管理，它包括：

e） 落实安全组织及安全管理人员，明确角色与职责，制定安全规划；

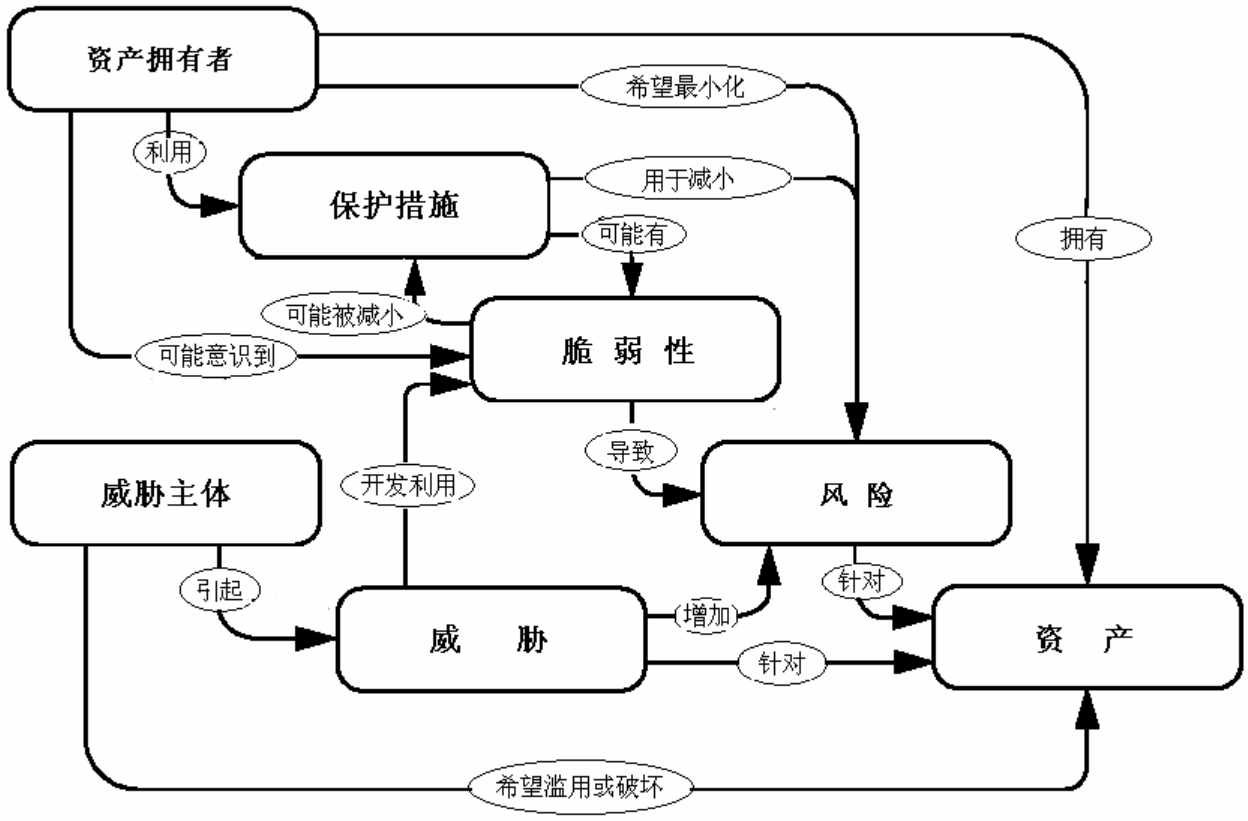
f） 开发安全策略；

g） 实施风险管理；

h） 制定业务持续性计划和灾难恢复计划；

i） 选择与实施安全措施；
j） 保证配置、变更的正确与安全；
k） 进行安全审计；
l） 保证维护支持；
m） 进行监控、检查，处理安全事件；
n） 安全意识与安全教育；
o） 人员安全管理等。

ii. 主要安全要素



a） 主要安全要素与关系

1. 资产

主要包括：

π) 支持设施（例如，建筑、供电、供水、空调等）；
θ) 硬件资产（例如，计算机设备如处理器、监视器、膝上型电脑、调制解调器，通信设施如路由器、数字程控交换机、传真机、应答机，存储媒体如磁盘、光盘等）；
ρ) 信息资产（例如，数据库和数据文档，系统文件，用户手册，培训资料，操作和支持程序，持续性计划，备用系统安排，访问信息等）；
σ) 软件资产（例如，应用软件，系统软件，开发工具和实用程序等）；
τ) 生产能力或服务能力；
υ) 人员；
ϖ) 无形资产（例如，信誉，形象）；
ω) 等。

2. 威胁

主要包括自然威胁和人为威胁。

自然威胁有地震、雷击、洪水、火灾、静电、鼠害和电力故障等。

人为威胁分为：

x） 盗窃类型的威胁，如偷窃设备、窃取数据、盗用计算资源等；

y） 破坏类型的威胁，如破坏设备、破坏数据文件、引入恶意代码等；

z） 处理类型的威胁，如插入假的输入、隐瞒某个输出、电子欺骗、非授权改变文件、修改程序和更改设备配置等；

aa）操作错误和疏忽类型的威胁，如数据文件的误删除、误存和误改、磁盘误操作等。

bb）管理类型威胁，如安全意识淡薄、安全制度不健全、岗位职责混乱、审计不力、设备选型不当、人事管理漏洞等；

cc）等。

3. 脆弱性

与资产相关的脆弱性包括物理布局、组织、规程、人事、管理、行政、硬件、软件或信息等的弱点；与系统相关的脆弱性如分布式系统易受伤害的特征等。

4. 意外事件影响

影响资产安全的事件，无论是有意或是突发，其后果可能毁坏资产，破坏信息系统，影响保密性、完整性、可用性和可控性等。可能的间接后果包括危及国家安全，社会稳定，造成经济损失，破坏组织或机构的社会形象等。

5. 风险

风险是某种威胁利用暴露系统脆弱性对组织或机构的资产造成损失的潜在可能性。风险由意外事件发生的概率及发生后可能产生的影响两种指标来评估。

由于保护措施的局限性，信息系统总会面临或多或少的残留风险，组织或机构应考虑对残留风险的接受程度。

6. 保护措施

保护措施是对付威胁，减少脆弱性，限制意外事件影响，检测意外事件并促进灾难恢复而实施的各种实践、规程和机制的总称。应考虑采用保护措施实现下述一种或多种功能：预防、延缓、阻止、检测、限制、修正、恢复、监控以及意识性提示或强化。保护措施作用的区域可以包括物理环境、技术环境（如硬件、软件和通信）、人事和行政。保护措施可为：访问控制机制、抗病毒软件、加密、数字签名、防火墙、监控和分析工具、备用电源以及信息备份等。

选择保护措施时要考虑由组织或机构运行环境决定的影响安全的因素，例如，组织的、业务的、财务的、环境的、人事的、时间的、法律的、技术的边界条件以及文化的或社会的因素等。

iii. 信息系统安全管理的基本原则

1. 信息系统安全管理的总原则

a） 主要领导人负责原则

信息安全保护工作事关大局，影响组织和机构的全局，组织和机构的主要领导人应把信息安全列为其最重要的任务之一，并负责提高、加强部门人员的安全意识，组织有效队伍，调动并优化配置必要的资源和经费，协调安全管理工作与各部门工作的关系，确保落实、有效。

b） 规范定级原则

组织和机构应根据其计算机信息系统及应用的重要程度、敏感程度以及自身资源的客观条件，确定相应的计算机信息系统安全保护等级，在履行相应的审批手续后，切实遵从相应等级的规范要求，制定相应的安全策略，并认真实施。

c） 依法行政原则

信息安全管理工作主要体现为行政行为，因此应保证信息系统安全行政主体合法、行政行为合法、行政内容合法、行政程序合法。

d） 以人为本原则

威胁和保障是安全管理工作的主题，它们在很大程度上受制于人为的因素。加强信息安全教育、培训和管理，强化安全意识和法治观念，提升职业道德，掌握安全技术，确保措施落实是做好信息安全管理工作的重要保证。

e） 适度安全原则

安全需求的不断增加和现实资源的局限性使安全决策处于两难境地，恰当地平衡安全投入与效果是从全局上处置好安全管理工作的出发点。

f） 全面防范、突出重点原则

全面防范是保障计算机信息系统安全的关键。它需要从人员、管理和技术多方面，在预警、保护、检测、反应、恢复和跟踪等多个环节上采用多种技术实现。同时，又要从组织和机构的实际情况出发，突出自身的安全管理重点。

g） 系统、动态原则

安全管理工作的系统特征突出。要按照系统工程的要求，注意各方面，各层次、各时期的相互协调、匹配和衔接，以便体现系统集成效果和前期投入的效益。同时，安全又是一种状态和动态反馈过程，随着安全利益和系统脆弱性的时空分布的变化，威胁程度的提高，系统环境的变化以及人员对系统安全认识的深化等，应及时地将现有的安全策略、风险接受程度和保护措施进行复查、修改、调整以至提升安全管理等级。

h） 控制社会影响原则

对安全事件的处理应由授权者适时披露与发布准确一致的有关信息，避免带来不良的社会影响。

2. 主要安全管理策略

a） 分权制衡

采取分权制衡的原则减小未授权的修改或滥用系统资源的机会，对特定职能或责任领域的管理执行功能实施分离、独立审计，避免操作权力过分集中。

b） 最小特权

任何实体（如用户、管理员、进程、应用或系统）仅享有该实体需要完成其任务所必须的特权，不应享有任何多余特权。

c） 选用成熟技术

成熟的技术提供可靠性、稳定性保证，采用新技术时要重视其成熟的程度。如果新技术势在必行，应该首先局部试点然后逐步推广，减少或避免可能出现的损失。

d） 普遍参与

不论信息系统的安全等级如何，要求信息系统所涉及人员普遍参与并与社会相关方面协同、协调，共同保障信息系统安全。

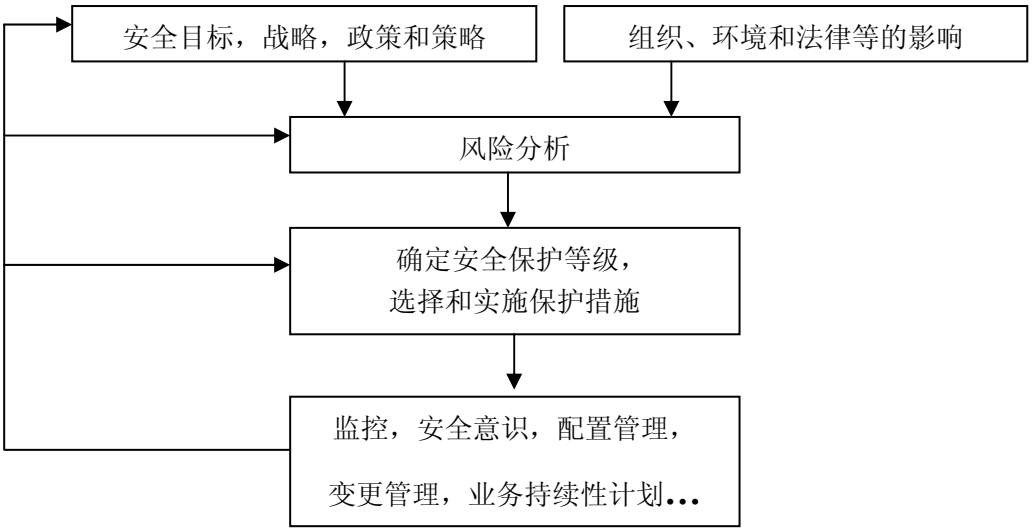
iv. 安全管理的过程

1. 安全管理过程模型

图1给出了一个计算机信息系统安全管理过程模型。

安全管理是一个不断发展、不断修正的过程，贯穿于信息系统生命周期，涉及到信息系统管理层面、物理层面、网络层面、操作系统层面、应用系统层面和运行层面的安全风险管理。对信息系统上述几个层面的安全管理是保证信息系统安全技术、安全工程、安全运行正确、安全、有效的基础。

在安全管理过程模型中，每个阶段的管理工作重点不同，要求不同。



β)　**计算机信息系统安全管理过程模型**

安全目标

防止国家秘密和单位敏感信息的失密、泄密和窃密，防止数据的非授权修改、丢失和破坏，防止系统能力的丧失、降低，防止欺骗，保证信息及系统的可信度和资产的安全。

安全保护等级的确定

计算机信息系统的使用单位主管应根据国家有关法律法规、计算机信息系统所处理信息的安全要求和运行安全要求确定计算机信息系统的保护等级，并按照GA/T XX1-XXXX(技术要求)、GA/T XXX-XXXX(工程要求)和本标准的管理要求实施等级保护。

安全风险分析与评估

目的

识别需要控制或可接受的风险并形成风险的分析评估报告。

方法

安全风险分析时应依据有关的信息系统安全标准和规定，采用多层面、多角度的系统分析方法，制定详细的分析计划和分析步骤，避免遗漏，以保证结果的可靠和科学，并形成文档，做到有据可查。

内容与范围

信息系统安全组织、制度和人员情况，信息系统的体系结构，策略与技术运用，安全设施布控及外包服务状况，动态安全运行状况等。

分析过程

1)　信息及信息系统的分类；
2)　识别要保护的资产及价值；
3)　分析信息资产之间的相互依赖性；
4)　识别存在的脆弱性和威胁；
5)　分析可能的入侵者和入侵活动的影响；
6)　编制安全风险分析报告。

制定安全策略

a） 目的

为保证信息系统的安全提供框架，提供安全管理的方法，规定各部门要遵守的规范及应负的责任，为信息系统的安全具体实施提供依据和基础。以调动、协调和组织各方面的资源共同保障信息系统的安全。

b） 方法

安全策略应由计算机信息系统使用单位的相关部门负责制定，该部门由使用单位的主管成员和专业安全技术人员以及来自该单位不同部门的相关成员组成。有条件的部门，可聘请安全专家。安全策略在制定时应兼顾结构上的系统性、内容上的可理解性、技术上的可实现性、管理上的可执行性。安全策略应与时俱进，定期加以调整和更新。

安全策略的内容

1） 保护的内容和目标：安全策略中应包含计算机信息系统中要保护的所有资产以及每件资产的重要性，对计算机信息系统中的要素或资产进行分类，分类应体现各类资产的重要程度，所面临的主要威胁，并规定它们的受保护等级；

2） 明确人员的职责：明确每个人在信息安全保护中的责任和义务，以便有效地组织全员协同工作；

3） 实施保护的方法：确定保护计算机信息系统中各类资产的具体方法，如对于实体可以采用隔离、防辐射、防自然灾害的措施，对于数据信息可以采用授权访问控制技术，对于网络传输可以采用安全隧道技术等；

4） 事故的处理：为了确保任务的落实，提高安全意识和警惕性，应规定相关的奖惩条款，并建立监管机制，以保证各项条款的严格执行。

安全需求分析

c） 目的

提高计算机信息系统安全服务和安全机制等安全保障措施的有效性和针对性，并形成安全需求分析报告。

方法

1） 结合实际：针对计算机信息系统的实际环境和安全目标提出安全要求；

2） 依据标准：为了保证质量，做到有据可查，安全需求分析应符合有关标准；

3） 分层分析：从涉及的策略、体系结构、技术、管理等各个层次逐次进行分析；

4） 动态反馈：安全需求分析是一个不断发展的过程，随着系统更新换代或功能扩展、内部环境和外部环境的变化，安全需求随之发生变化。安全需求分析应保持结果的有效性、适应性，保证分析方法的科学性和系统性，安全需求分析过程应与系统发展过程同步。

内容

1） 管理层面：根据组织和机构的实际情况，确定管理机构或部门的形态和规模，并明确其目标、原则、任务、功能和人员配置等；

2） 物理层面：根据组织或机构的实际情况，确定各类实体财产的安全级别，以及需要保护的程度和方法；

3） 系统层面：明确操作平台应该具备的安全级别，以及为达到所要求的级别，应选用的操作系统等；

4） 网络层面：根据信息系统的业务方向，分析系统的网络，特别是网络边界的安全需求，确定应采用的防护体系；

5） 应用层面：基于网络的应用以及应用供应商的多样性和复杂性，相应的安全防护体系和技术措施不尽相同，需要根据实际情况来确定、选择其安全需求。

安全措施的实施

目的

实现安全防护体系，保证达到GA/T XXX-XXXX(工程要求)的要求。

方法

遵从保质、经济、高效的原则，正确选择实施单位，依据一份详细、准确、完备的文档化实施方案，对实施过程进行严格控制。

对方案要详细说明安全过程各个阶段的建设目标、工作内容、施工人员、任务分工、进度安排、产品选型、产品采购、资金投入等情况，并给出每一项的依据和理由，分析每项工作的作用、意义和局限性，明确实施各方的工作关系、责权和协调协同机制。

对实施方案进行评审时既要兼顾整体，又要注意细节，严格对照组织或机构的安全策略、安全需求和实际情况进行检验，并对所有的备选方案进行认真的分析比较，确保选中的方案达到设想的要求和标准。

在安全措施实施过程中，所采用的技术与产品应经过严格的测试选型，符合国家信息安全方面的法律法规，特别是涉及密码技术的产品，应严格按照国家和主管部门的有关规定选型和采购。

实施应按照GA/T XXX-XXXX(工程要求)的要求进行。

如本单位没有实施条件，应选择具备相应资质和合适、可靠的实施单位来实施信息系统安全措施。

安全实施过程的监理

目的

在安全实施过程中建立安全监理制度，检验施工单位的质量水平和责任心，保证工程各阶段的质量。

d） 方法

安全实施过程的监理主要从实施的规范、流程、进度等方面进行监督与检查，确保各环节的质量。

安全监理单位或个人应是经过有关部门批准的第三方中立机构或具有相应资质的个人，保证安全措施实施按照合理的流程与技术标准进行，保证实施过程的有效性。

1) 实施前的监理：对所选安全产品的真实性、质量、到货时间进行检查；对工程实施人员进行身份及资质审核；对实施单位的具体实施步骤及每个步骤中的具体实施计划文档进行审核；对实施单位开始实施工程的时间和完工的时间进行事前记录；

2) 实施中的监理：对工程实施进度进行计划和督促，防止延误工期；对工程实施过程的真实性和与方案的符合性进行监督；对工程实施人员的身份在实施过程中进行再检查;对软硬件产品在工程实施中的完好性和真实性进行检查;对工程实施中已完成的部分进行局部验收，发现问题令其及时纠正；对实施人员的能力和态度进行审核；对于敏感性、关键性信息系统，应由该组织或机构委派专人在现场实施全过程监控，负责零事故的安全保障；

3) 实施后的监理：对是否达到相应的安全级别进行严格验收；对产品配置的合理性、有效性进行验收；对安全配置是否影响系统的性能进行验收；对实施的进度进行验收；对信息系统的安全现状进行测试与评估；聘请安全专家或有关安全部门对信息系统的安全现状进行评估。

安全措施实施过程检查的结果应由实施和检查单位法人代表和检查人员签字，以便有关部门和使用单位检查。

信息系统的安全审核

目的

检验、监督安全工作的落实情况，确保信息系统达到GB17859-1999要求的相应安全等级。

e） 方法

应根据国家有关部门的具体规定实施信息系统的安全检查工作，实施独立审计。

信息系统的各应用单位有关人员或组织除实施自查外，应积极配合国家有关部门对所用系统实施安全检查。

对技术上的安全措施要通过其使用、配置情况，检查它们是否达到了有关的要求。检查的方法有多种，例如，通过查看系统的日志，分析出系统在运行过程中遇到的意外情况以及使用情况；或者对安全措施进行测试，查看它们能否达到规定的安全水平等。

对安全管理的检查，可以通过审阅有关机构或人员的工作记录，规定他们定期进行总结汇报，并对检查的结果进行核实，还可以发动单位内的所有人员对管理机构的运作进行监督。

对人员安全意识的检查可以通过问卷、座谈等方式进行，并建立定期考核制度。

应建立不定期的抽查制度，避免作弊行为或虚假的检查结果。

内容

1) 安全策略的检查：检查结构上的系统性、内容上的可理解性、技术上的可实现性、管理上的可执行性；

2) 技术措施的检查：根据有关的技术标准，结合实际情况，分析安全措施的保护能力及能够满足需求的程度，并进一步研究该项措施在当前环境和将来环境中的作用以及可行性；涉及多个技术领域时，检查过程中需要聘请相关专业专家共同参与，并将检查结果形成详细准确的报告，再由小组进行论证评审，以确定该措施当前的有效性；涉及密码技术时，检查密码体制、密码产品和密钥管理体系的使用和管理是否符合国家有关部门的规定；

3) 管理措施的检查：主要是检查安全管理机构是否健全，管理职能和管理职责是否明确，有关的政策、法规、制度、规定是否完善，人员的安全意识如何，相关的安全教育和培训工作开展的怎样，效果如何。

2. 生命周期管理

a） 目的

对计算机信息系统实施生命周期全程管理。

b） 方法

计划阶段：通过风险分析明确安全需求，确定安全目标，制定安全策略，拟定安全要求的性能指标。

实施阶段：依据安全要求选择相应的安全措施，采购或设计安全系统，根据工程要求实施和部署，并对安全措施进行验证、验收。

运行维护阶段：通过检查、检测、审计和对风险变更的监视和评估保证运行安全。

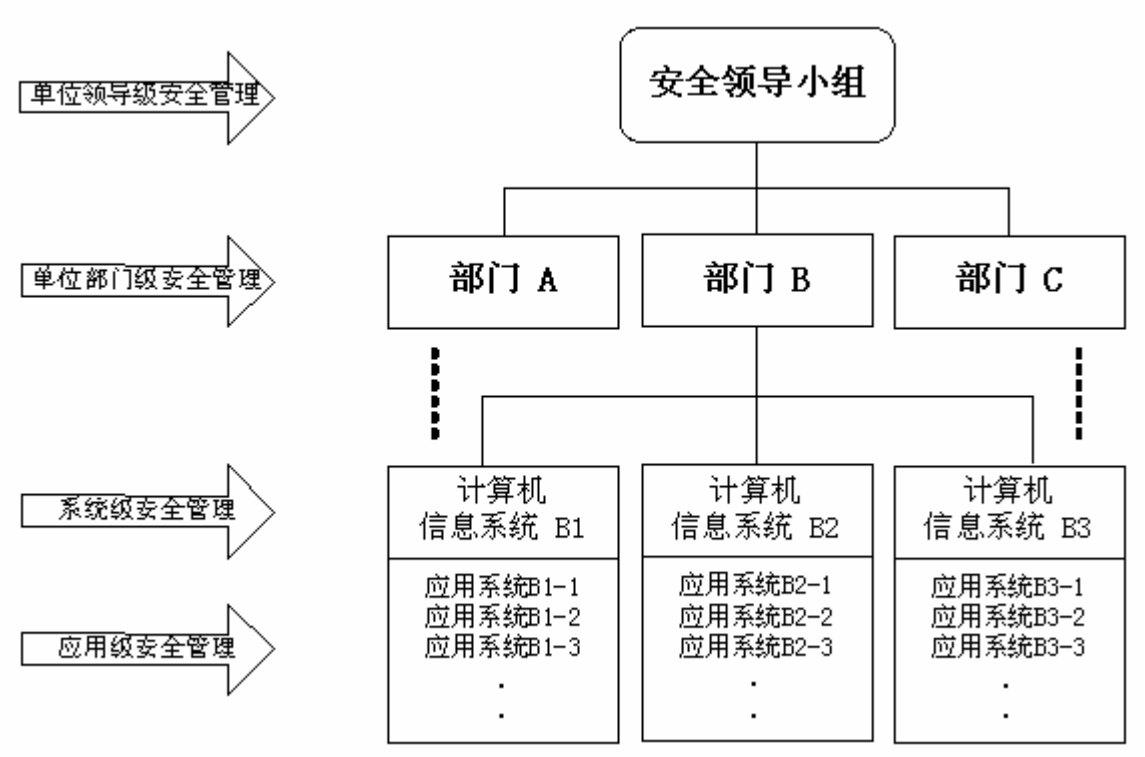
生命周期结束阶段：对计算机信息系统的信息进行安全处置。

安全管理组织

单位的最高主管对本单位计算机信息系统安全负有主要责任，应根据使用的计算机信息系统的保护等级和计算机信息系统规模设立安全管理职责体系，明确安全管理人员的职责，保证安全管理人员有效行使计算机信息系统安全管理的权利。

如无特殊说明，在下列叙述中涉及的安全管理机构要求，均指根据实际情况建立的安全管理职责体系要求。

常见的安全管理组织结构如图2所示。



c） 安全管理组织结构

安全领导小组的主要职责：

1） 负责与国家各级计算机信息系统安全主管部门建立日常工作关系；
2） 定期向当地公安机关信息安全监察部门报告本单位信息安全保护管理情况，及时报告重大安全事件；
3） 组织、协调、指导计算机信息系统的安全开发工作；
4） 组织并领导有关人员制定、评审本单位计算机信息系统安全策略、标准、安全工作流程、各种规章制度；
5） 确定计算机信息系统各类人员的职责和权限；
6） 审议并通过安全规划，年度安全报告，有关安全的宣传、教育、培训计划；

系统安全管理人员的主要职责：

1） 负责应承担的日常安全工作；
2） 遇到违法犯罪事件，应妥善保护案发现场，协助公安机关调查、取证；
3） 对已证实的重大的安全违规、违纪事件及泄密事件及时进行处理；
4） 安全审计跟踪分析和安全检查，及时发现安全隐患和犯罪嫌疑，防患于未然；
5） 负责定期向所属组织或机构的领导层（或管理层）汇报安全工作。

人员安全

3. 人员审查

制定人员审查制度。

应根据计算机信息系统安全等级的需要确定人员审查内容。

信息系统的有关人员应具有政治可靠、思想进步、作风正派、技术合格、职业道德良好等基本素质。

录用关键工作岗位的工作人员时应按照其申请表中的个人历史逐一审查，必要时要亲自会见证明人，对以前的经历和人品进行确认。

对在职人员应进行定期审查，当工作人员婚姻、经济、身体等状况发生变化，或被怀疑违反了安全规则，或对其可靠性产生怀疑时，都应进行重新审查。

4. 岗位责任和授权

根据分权制衡和最小特权原则，建立岗位责任制度和授权制度。

明确所有人员在系统中的安全职责和权限，职责和权限要文档化，并要求签字确认。所有人员的工作和活动范围应当被限制在完成其任务的最小范围内。

关键岗位人员不允许兼职。

5. 人员培训

建立人员培训制度，明确培训内容。

定期对计算机信息系统的操作和维护人员进行培训，经过培训的人员才能上岗工作。

6. 人员考核

建立人员考核制度。

定期从政治思想、业务水平、工作表现、遵守安全规程等方面对计算机信息系统工作人员进行考核。对考核合格者应予表扬和奖励，考核发现不合格者应予以教育、批评或处罚直至调离岗位。

7. 签订保密合同

计算机信息系统所涉及的工作人员（长期或临时），应签订保密合同，承诺其对系统应尽的安全保密义务，保证在岗工作期间和离岗后一定时期内，均不得违反保密合同、泄露系统秘密。保密合同的内容应符合国家有关规定。对违反保密合同的应设有惩处条款。

8. 人员调离

建立人员调离安全管理制度。

对调离人员，应严格办理调离手续，交回所有钥匙及证件，退还全部技术手册、软件及其它相关资料。系统应及时更换系统口令和相关机要锁、撤销其用过的所有账号。重要机房或岗位的工作人员一旦辞职或调离，应立即撤销其出入安全区域、接触敏感信息的授权。

安全管理制度

9. 物理安全方面的规章制度

主要包括：机房安全管理制度、主机设备安全管理制度、网络设施安全管理制度、物理设施分类标记管理制度等。

10. 系统与数据库安全方面的规章制度

主要包括：安全配置管理制度、系统分发和操作规章制度、系统文档安全管理制度、测试和脆弱性评估制度、系统信息安全备份制度等。

11. 网络安全方面的规章制度

主要包括：网络连接检查评估制度、网络使用授权制度、网络检测制度、网络设施（设备和协议）变更控制制度等。

12. 应用安全方面的规章制度

主要包括：应用安全评估制度、应用系统使用授权制度、应用系统配置管理制度、应用系统文档管理制度等。

13. 运行安全方面的规章制度

主要包括：人员安全管理制度、安全意识与安全技术教育制度、操作安全管理制度、操作系统和数据库安全管理制度、系统运行记录编写制度、病毒防护管理制度、系统维护管理制度、网络互联安全管理制度、安全审计管理制度、安全事件报告制度、事故处理制度、应急管理制度和灾难恢复管理制度等。

14. 信息安全方面的规章制度

主要包括：信息分类标记制度、涉密信息安全管理制度、技术文档管理制度、存储介质管理制度、信息披露与发布审批管理制度等。

安全等级信息系统的管理要求

不论计算机信息系统规模如何，为保障信息的机密性、完整性、可用性、可控性和抗抵赖性，都应遵从4.3条的有关原则，建立有效的安全管理体系，按计算机信息系统安全等级保护的要求实施安全管理。

计算机信息系统保护等级技术要求、工程要求、评估要求的等级是可以浮动的，浮动的条件是对信息的机密性、完整性、可用性、可控性和抗抵赖性要求的改变或安全风险的改变。等级向上浮动的前提是当前计算机信息系统保障能力能满足相应等级的信息安全的更高要求，能控制相应等级的更大的安全风险。向下浮动不作要求。跨越不同安全等级系统的信息可能受到威胁，对由较高等级向较低等级系统传送信息时，应采取保护措施，得到管理层的授权。

第一级 （用户自主保护级）实施基本的管理

管理目标和范围

制定安全管理计划，明确计算机信息系统的安全目标和安全范围，并经单位主管领导批准。

安全管理计划文件在下列方面应有基本描述：安全策略、风险管理、安全措施检查、行为准则、生命周期管理、处理授权、人员安全、物理和环境安全、技术支持与运行安全、应急计划、技术文档管理、教育与培训、事件响应、访问控制、审计跟踪等。

保证计算机信息系统安全保护等级达到GA/T XX1-XXXX(技术要求)、GA/T XXX-XXXX(工程要求)的标准要求。

人员与职责要求

单位主管委任安全管理人员，并赋予安全管理的权力。

安全管理人员应具有基本的专业技术水平，掌握计算机信息系统安全管理基本知识，负责组织规划有关人员的安全意识教育和培训，组织协调有关人员对计算机信息系统的安全性进行评估，理解计算机信息系统面临的安全威胁，并对管理层、物理层、系统层、网络层和应用层有基本的风险分析，确定安全需求，制定安全计划，并负责落实和监督安全计划的实施。

物理安全管理要求

通过正式授权程序委派专人负责物理安全工作。建立物理安全规章制度。

通过科学分类对计算机信息系统的物理环境和物理设施进行分类登记。

保证计算机信息系统的物理安全达到GA/T XXX-XXXX(技术要求)中本级有关环境、设备和介质安全所提出的基本要求。

系统安全管理要求

通过正式授权程序委派专人负责系统环境安全管理。建立操作系统和数据库的安全配置、操作系统和数据库的备份等安全管理规章制度。

保证人员能按照GA/T XXX-XXXX(技术要求)、GA/T XXX-XXXX(操作系统要求)和GA/T XXX-XXXX(数据库要求)的基本要求，对操作系统和数据库进行安全管理。

网络安全管理要求

通过正式授权程序委派专人负责网络环境安全工作。建立有关网络配置安全管理制度。

保证人员能按照GA/T XXX-XXXX(技术要求)和GA/T XXX-XXXX(网络要求)对本级网络安全的基本要求，对网络进行安全管理。

应用系统安全管理要求

通过正式授权程序委派专人负责应用系统环境，包括应用系统软件的安全配置、备份等安全工作。制定有关规章制度。

保证人员能按照应用系统操作文档和应用系统有关安全要求，对应用系统软件和应用业务数据进行安全管理。

运行安全管理要求

dd) 安全管理人员应协同计算机信息系统应用部门对计算机信息系统的运行进行安全管理。建立有关安全规章制度。

ee) 确保为计算机信息系统可靠运行而采取的各种检测、监控、审计、分析、备份及容错等方法和措施的正确实施。

ff) 要求制定风险分析计划，制定网络安全检测、网络防病毒、网络安全事件报告、应急计划管理等制度。制定安全意识和安全技术教育培训计划。对运行安全进行监督检查。明确计算机信息系统各类人员对计算机信息系统各类资源的安全责任。明确计算机信息系统安全管理人员和计算机信息系统普通用户对计算机信息系统资源和控制系统中命名客体的访问权限。

第二级 （系统审计保护级）实施操作规程管理

管理目标和范围

建立安全管理机构并满足第一级的管理要求外，还应进一步根据管理计划制定一系列安全操作规程，并实施计算机信息系统生命周期的全程管理。

安全操作规程文件应由单位主管领导批准，安全操作规程文件中应明确计算机信息系统的安全岗位，并指明是否需要更细致的指导，说明例外情况。特定规程中要明确规定其适用场所、适用对象、有效期限和规程责任人，对其中适用对象要明确适用的主体和客体。

通过管理活动保证计算机信息系统达到GA/T XXX-XXXX(技术要求)、GA/T XXX-XXXX(工程要求)的本级标准。

人员与职责要求

单位主管领导负责建立正式的安全管理机构，委任并授权该机构的安全管理负责人负责安全管理工作的组织和实施。安全管理机构由单位各级主管和有关专家组成。

安全管理负责人至少从事过二年以上的计算机信息系统的技术工作，一年以上的计算机信息系统安全管理工作或经过正规院校计算机信息系统安全技术和管理的培训。

安全管理负责人负责召集有关人员制定本单位安全计划，设立安全管理岗位，明确岗位职责；制定明确的安全管理目标和安全策略；制定计算机信息系统各层安全管理规程；制定系统管理、信息管理、网络管理、存储介质管理、操作管理、软硬件维修、审计、服务外包等安全管理规章制度，并监督执行；对关键的计算机信息系统制定风险管理计划；组织规划有关人员的安全意识教育和培训。

物理安全管理要求

除满足第一级的物理安全管理要求外，应建立物理安全区域，制定专人负责物理安全区计算机信息系统场地和物理设施的日常安全管理，制定物理设施的购置计划、设备的验收、运行、维护、处置管理制度，监督、检查物理设施安全管理制度的落实。编制物理设施安装、运行、操作流程，制定并实施物理设施管理培训计划；所有物理设施要分类编目，指定每个物理设施安全责任人。

对计算机信息系统使用的关键设备建立严格的登记制度，保证设备购置、安装、调试、维护、维修、报废等处置活动可控。

操作系统安全管理要求

指定操作系统安全管理责任人，负责操作系统的日常安全管理和安全审计，对用户安全使用进行指导、登记和监视。

操作系统应使用符合GA/T XXX-XXXX(操作系统要求)的本级操作系统。

依据操作规程安全使用、配置操作系统，操作系统安全管理责任人依据操作规程确定审计事件、审计内容、审计归档、审计报告。

授权用户应使用唯一的标识和口令，遵照规定的登录规程登录系统，遵照授权说明使用许可的资源。

对操作系统中的系统工具的使用进行授权管理，并对系统工具使用情况进行审计。

对操作系统安全性进行及时维护，对操作系统的安全弱点和漏洞进行控制。

依据变更控制规程对操作系统的变更进行控制，保证变更不影响应用系统的可用性、稳定性、安全性，保证变更过程的有效性和可审计性。

应及时对操作系统资源和系统文档进行安全备份。

网络安全管理要求

除满足第一级的网络安全管理要求外，网络安全管理负责人应按照有关规程召集有关人员对计算机信息系统运行的网络安全进行定期评估，不断完善网络安全策略，建立、健全网络安全管理规章制定。

制定使用网络和网络服务的策略。依据总体安全方针、策略制定允许提供的网络服务、制定网络访问许可和授权管理制度、保证计算机信息系统网络连接和服务的安全技术正确实施，并达到GA/T XXX-XXXX(网络要求)的要求。

制定网络安全教育和培训计划，保证计算机信息系统的各类用户熟知自己在网络安全方面的安全责任和安全规程。

建立网络访问授权制度，保证经过授权的用户才能在指定终端，使用指定的安全措施，按设定的可审计路由访问许可的网络服务。

对安全区域外部移动用户的网络访问实施严格的审批制度，实施用户安全认证和审计技术措施，保证网络连接的可靠性、保密性，保证用户对外部连接的安全性负责。

定义与外部网络连接的接口边界，建立安全规范，定期对外部网络连接接口的安全进行评估，对通过外部连接的可信计算机信息系统之间的网络信息提供加密服务，有关加密设备和算法的使用按国家有关规定执行。

对外进行公共服务的计算机信息系统，应采取严格的安全措施实施访问控制，保证外部用户对服务的访问得到控制和审计，并保证外部用户对特定服务的访问不危及内部计算机信息系统的安全，对外传输的数据和信息要经过审查，防止内部人员通过内外网的边界泄露敏感信息。

对可能从内部网络向外发起的连接资源（如拨号上网）实施严格控制，建立连接资源使用授权制度，建立检查制度防止计算机信息系统使用未经许可和授权的连接资源。

不同安全保护等级的计算机信息系统网络之间的连接按访问控制策略实施可审计的安全措施，如使用防火墙、安全路由器等，实现必要的网络隔离。

保证网络安全措施的日常管理责任到人，并对网络安全措施的使用进行审计。

按网络设施和网络服务变更控制制度执行网络配置变更控制。

建立网络安全事件、事故报告处理流程，保证事件和事故处理过程的可审计性。

对网络连接、网络安全措施、网络设备及操作规程定期进行安全检查和评估，提交正式的网络安全报告。

指定网络安全审计人员，负责对网络安全事件的审计，对审计活动实施控制，保证网络设施提供的审计记录的完整性和可用性。

计算机信息系统的关键网络设备设施应有必要的备份。

对可用性要求高的网络指定专人进行不间断的监控，并定期对应急计划的可行性进行验证。

应用系统安全管理要求

计算机信息系统的各应用单位和部门应指定专人负责应用系统的安全管理。应用系统的安全管理要求不低于操作系统的安全管理要求。

制定并落实应用系统的安全操作规程，安全操作规程应包括安全措施的设计、部署、维护、运行和用户安全培训等。

应指定信息安全管理人员依据信息安全操作规程，负责信息的分类管理和信息的安全发布。

对任何可能超越系统或应用程序控制的实用程序和系统软件都应得到正式的授权和许可，并对使用情况进行登记。保证对应用系统信息或软件的访问不影响其他计算机信息系统共享信息的安全性。

应用系统的内部用户，包括支持人员，应按照规定的程序办理授权许可，并根据信息的敏感程度签署安全协议，保证应用系统信息的保密性、完整性和可用性。

应指定专人负责应用系统的审计工作。审计人员仅从事审计工作，不参与系统的其它任务，实现审计人员和被审计人员的职能分离，保证审计日志的准确性、完整性和可用性。

组织有关人员定期或不定期对应用系统的安全性进行审查，并根据应用系统的变更或风险变化提交正式的报告，提出安全建议。

对应用系统关键岗位的工作人员实施资质管理，保证人员的可靠性和可用性。

制定切实可用的应用系统及数据的备份计划和应急计划，并由专人负责落实和管理。

运行安全管理要求

gg）对计算机信息系统应按风险管理计划和操作规程定期对系统进行风险分析与评估，识别出可能存在的风险，并向管理层提交正式的风险分析报告。风险分析报告中应明确管理上、技术上存在的问题与对策。

hh）对病毒防护系统的使用制定管理规定，没有得到许可，用户不能私自终止病毒防护系统的运行，操作系统安全管理责任人负责病毒防护系统的管理（安装、升级、停止），操作系统应对病毒防护系统的使用建立日志。

ii）制定应用软件安全管理规章制度，对应用软件的采购实施批准制度，对应用软件的安全性进行调查，未获明确验证的软件不得装入运行的操作系统。对应用软件的使用采取授权管理制度，没有取得许可的用户不得安装、调试、运行、卸载应用软件，并对应用软件的使用进行审计。

jj）制定外部服务方对计算机信息系统访问的安全制度。对外部服务方访问系统可能发生的安全性进行评估，采取安全措施对访问实施控制，与外部服务方签署安全保密合同，并要求有关合同不违背总的安全策略。

kk）安全管理负责人应会同计算机信息系统应用各方制定应急计划和灾难恢复计划，并制定应急计划和灾难恢复计划的实施规程，并实施必要验证和实际演练。对应急计划涉及的人员进行培训，并要求应急人员具备执行应急计划的能力。对需外部资源的应急计划要与有关各方签署正式合同，合同中应规定服务质量，并包括安全责任和保密条款。

ll）制定安全事件处理规程，保证在短时间内对安全事件进行处理。

mm）制定计算机信息系统的信息和文档的备份制度，要求指定专人负责备份管理，保证计算机信息系统自动备份和人工备份的准确性、可用性。

nn）制定设备、操作系统、数据库、应用系统、人员、服务、内外风险等变更控制制度，保证变更后的计算机信息系统能满足既定的安全目标。

oo）制定运行安全管理检查制度，定期或不定期对所有计划和制度执行情况进行监督检查，并对安全策略和管理计划进行修订。协助上级或国家有关部门对计算机信息系统安全进行评估，对计算机信息系统安全工作的监督和检查。

pp）根据各种变更不断修订、完善各种规章制度。

qq）建立严格的运行过程管理文档，其中包括责任书、授权书、许可证、各类策略文档、事故报告处理文档、安全配置文档、系统各类日志等，保证文档的一致性。

第三级 （安全标记保护级）实施标记制度化管理

管理目标和范围

在实现第二级管理目标的基础上，要求计算机信息系统的用户熟知计算机信息系统的安全策略和安全规程，要求用户定期确认其安全意识和安全责任，保证安全策略和安全规程的有效实施；使用自动或其它方式监视系统的安全状态，保证在已建立的安全规程中明确规定系统日志的检查、系统穿透性测试和对内与对外的安全审计；保证安全管理贯穿计算机信息系统的整个生命周期；在安全规程中明确规定如何建设系统，如何验收系统，如何对系统的使用按正式的授权过程实施。

通过对用户、系统资源进行标记，建立健全一系列的安全管理制度，实现制度化管理。

通过管理活动保证计算机信息系统达到GA/T XXX-XXXX(技术要求)、GA/T XXX-XXXX(工程要求)的本级标准。

人员和职责要求

在满足第二级要求的基础上，要求对计算机信息系统安全风险控制、管理过程的安全事务明确分工负责。对风险分析与评估、安全策略的制定、安全技术和管理的实施、安全意识培养与教育、安全审核、安全事件和事故响应、安全评估等工作指定管理责任人，分配明确的职责和权利。

对工作岗位和职责编制正式的文件，明确各岗位的职责和技能要求；对不同岗位制定和实施安全培训计划，并对安全培训计划进行维护和评估。

对计算机信息系统的工作人员、资源实施等级标记管理。

物理安全管理要求

除满足第二级的物理安全管理要求外，对安全区域实施分级标记管理，对出入标记安全区的员工验证标记，安全标记不符的人员不得出入；对出入标志安全区的活动进行监视和记录；所有物理设施要设置安全标记。

保证物理安全达到GA/T XXX-XXXX(技术要求)要求的相应等级标准。

操作系统安全管理要求

除满足第二级的要求外，安全管理负责人应按本级操作系统内置角色分别指定操作系统安全管理责任人，负责计算机信息系统可信计算基内操作系统的安全配置管理、帐户管理、备份管理、打印管理和安全审计。并根据操作系统关键程度，为关键岗位制定人员备用制度。

对操作系统，指定的操作系统日常安全管理人员要对用户使用情况进行监视和登记，并验证用户的安全标记。

对使用系统工具建立使用授权、标记管理制度，并对操作系统的系统工具使用情况进行审计。对可能危及操作系统安全的系统工具进行严格的技术控制和管理控制。

制定严格的变更控制制度，保证变更不影响应用系统的可用性、安全性，保证变更过程的有效性、可审计性和可恢复性。

应及时对操作系统资源和系统文档进行标记处理、安全备份，并制定、实施应急安全计划，保证操作系统的可用性、完整性、可靠性。

网络安全管理要求

除满足第二级的要求外，对网络安全措施的使用建立严格的审计、标记制度，保证安全措施配有具体责任人，按标记等级负责网络安全措施的日常管理。

指定网络安全审计人员，负责安全事件的标记管理，网络安全事件的审计；对审计活动进行控制，保证网络设施或审计工具提供的审计记录完整性和可用性。

对可用性要求高的网络指定专人进行不间断的监控，并能及时处理安全事故。

应用系统安全管理要求

除满足第二级的要求外，要求安全管理负责人有明确管理范围、管理事务、管理规程，保证应用系统的安全措施配置正确、有效。

应用系统中的信息是应用系统安全管理的重点，应指定信息安全管理人员负责信息的分类、分级、标记管理和信息的安全发布。

制定应用软件安全管理规章制度，对应用软件的设计、开发、采购实施批准制度；对应用软件的安全性进行评估，未获明确验证的软件不得装入运行的系统；对应用软件的使用采取授权、标记管理制度。未授权用户不得安装、调试、运行、卸载应用软件，并对应用软件的使用进行审计。应用系统应安装强制标记信息访问控制的机制，按安全标记对应用系统软件和信息的访问进行控制，只对具有相应标记的授权用户开放，并对访问进行审计，对事件进行标记管理。

应指定专人负责应用系统的安全事件和安全标记的审计工作。

定期或不定期对应用系统的安全性进行评估，并根据应用系统的变更或风险变化提交正式的评估报告，提出安全建议，修订、完善有关安全管理制度和规程。

对应用系统关键岗位的工作人员实施资质调查和标记工作。

应用系统的开发人员不得从事应用系统日常运行和安全审计工作。操作系统的管理人员不得参与应用系统的安全配置管理和应用管理。

制定切实可行的应用系统及数据的备份计划和应急计划，并由专人负责落实和管理，对备份信息介质制定严格的标记制度，并按信息等级的要求制定不同的备份策略。

运行安全管理要求

除满足第二级的要求外：

rr）风险管理应使用规范的方法对计算机信息系统的各个方面进行风险管理。

ss）要求对关键岗位的人员实施严格的背景调查和管理控制，切实落实最小特权原则和分权制衡原则，关键安全事务要求双人共管。

tt）要求实施集中的病毒防护管理制度，要求计算机信息系统的所有操作终端能有效防范病毒或恶意代码的引入。

uu）要求定期对外部服务方访问计算机信息系统的风险进行分析和评估，对外部服务方实施严格的访问控制，并对外部服务方的访问实施监视。

vv）要求有专人负责应急计划和灾难恢复计划的管理工作，保证应急计划和灾难恢复计划重点突出、有效执行。

ww）要求系统中的关键设备和数据采取可靠的备份措施。

xx）要求保证安全策略、安全计划、风险管理、安全措施检查、行为准则、生命周期管理、处理授权、人员安全、物理和环境安全、技术支持与运行安全、应急计划、技术文档管理、教育与培训、应急响应、存取控制、审计跟踪等安全事务的一致性。

第四级 （结构化保护级）实施标准化管理

管理目标和范围

在实现第三级管理目标的基础上，要求计算机信息系统的使用单位将安全策略、操作规程、规章制度和安全措施的有效性评估程序化、周期化。进行评估时采用的测试类型、频率应有正式的文件，并得到相关领导的批准，并保证按照批准的文件进行评估工作；对关键的控制措施要根据其风险制定严格测试计划；对内外明显的风险变化应立即组织风险评估；对有可能暴露系统脆弱性的安全事件记录制定例行评估制度，安全事件记录不仅包括内部安全事件或安全警告，还要考虑外部可信渠道得到的安全事件和安全警告信息；建立安全事件例行报告制度。

通过定期的安全评估提示工作人员关注其相关安全责任，表明管理层对安全管理的重视，确保人员在安全管理中的主导作用。

强制实施分权管理机制，保证系统管理员和操作员的职能分离；提供可信设施管理；增强配置管理控制。保证系统具有强壮的抗渗透能力。

通过管理活动保证计算机信息系统达到GA/T XXX-XXXX(技术要求)、GA/T XXX-XXXX(工程要求)的本级标准。

人员与职责要求

在满足第三级要求的基础上，要求安全管理渗透到计算机信息系统各级应用部门，对安全管理活动实施质量控制，建立质量管理体系文件。要求独立的审计机构对使用单位的安全管理职责体系、计算机信息系统安全风险控制、管理过程的有效性进行评审。对风险分析、安全策略、安全技术和管理的实施、安全意识培养与教育、安全审核、安全事件和事故响应、安全评估工作管理责任人进行例行考核，保证安全管理工作的有效性。

要求计算机信息系统所有用户将安全管理纳入日常工作，并定期对计算机信息系统的所有用户进行检查和评估，保证安全教育是单位工作计划的一部分。

要求对所有关键岗位的人员实施全面的背景审查和管理控制，关键安全事务应多人共管。

物理安全管理要求

除满足第三级的物理安全管理要求外，对不同安全区域实施隔离；建立出入审查、登记管理制度，保证出入得到明确授权，并且出入人员持有授权书，授权书中要明确出入的目的、操作的对象、操作的步骤和操作的结果证明；对出入标记安全区的活动进行不间断实时监视记录；建立出入安全检查制度，保证出入人员没有携带危及计算机信息系统安全的设施或物品。

保证物理安全达到GA/T XXX-XXXX(技术要求)相应等级标准。

操作系统安全

除满足第三级的要求外，安全管理机构应按本级操作系统内置角色分别指定操作系统安全管理责任人。

定期对操作系统安全性进行评估，及时对操作系统的安全弱点和漏洞进行控制；保证操作系统管理过程的可审计性。

网络安全管理要求

除满足第三级的要求外，要求建立独立的网络安全审计，对网络服务、网络安全策略、安全控制措施进行有效性检查。保证网络安全管理人员达到相应的资质。

计算机信息系统网络之间的连接实现物理或逻辑的网络隔离。

应用系统安全管理要求

除满足第三级的要求外，要求建立独立的应用安全审计，对应用系统的总体安全策略、应用系统安全措施的设计、部署、维护和运行管理进行检查。审计人员仅实施审计工作，不参与系统的其它任务。

应用系统的开发人员不应从事应用系统日常运行和安全审计工作。操作系统的管理人员不应参与应用系统的安全配置管理和应用管理，对应用系统的配置信息应进行标记。

为不同等级的应用系统制定切实可行的应用系统备份计划和应急计划，并保证监督、落实。定期对应用系统和数据的备份和应急计划进行演练和验证，保证备份的准确性、可用性，保证应急计划的可行性、有效性、完整性。对备份信息介质制定严格的分类标记制度，并按信息等级的要求制定不同的备份策略。

运行安全管理要求

除满足第三级的要求外：

yy) 要求建立风险管理质量管理体系文件，对风险管理过程实施独立的审计，保证安全管理过程的有效性。

zz) 要求计算机信息系统生命周期各个阶段的安全管理工作有明确的目标、明确的职责，并对计算机信息系统生命周期管理建立质量控制体系文件，对生命周期管理实施独立的审计，保证

生命周期管理活动的有效性。

aaa)要求对病毒防护管理制度实施定期和不定期的检查。

bbb)要求对外部服务方每次访问计算机信息系统的风险进行控制。

ccc)要求实施独立的审计，定期对应急计划和灾难恢复计划的管理工作进行评估，保证应急计划和灾难恢复计划有效性。

ddd)要求实施独立的安全审计，对使用单位的安全策略、安全计划、风险管理、安全措施检查、行为准则、生命周期管理、处理授权、人员安全、物理和环境安全、技术支持与运行安全、应急计划、技术文档管理、教育与培训、应急响应、存取控制、审计跟踪等安全事务的一致性进行检查和评估。

第五级 （访问验证保护级）实施安全文化管理

管理目标和范围

除满足第四级的要求外，要求单位的全面安全计划成为单位文化的有机组成部分，保证有持续完善的安全计划、安全规程、安全措施。保证所有的决议有利于不断化解计算机信息系统的安全风险。要求安全脆弱性得到了很好理解，并得到切实的管理和控制。安全威胁能得到不间断的评估，对安全威胁的控制措施能适应安全环境的变化。

对计算机信息系统的安全实施全面质量管理保证体系。

通过管理活动保证计算机信息系统达到GA/T XXX-XXXX(技术要求)、GA/T XXX-XXXX(工程要求)的本级标准。

人员与职责要求

除满足第四级的要求外，计算机信息系统所有人员都能理解并有能力执行规定的安全管理要求，保证所有人员达到相应岗位的安全资质。

要求计算机信息系统的所有工作人员资质管理能得到保障。

要求对所有岗位的人员实施全面质量管理，保证内部人员的工作得到全面的控制。

物理安全管理要求

除满足第四级的要求外，要求对物理安全的保障有持续的改善。

操作系统安全

除满足第四级的要求外，要求保证操作系统的安全管理工作在多方在场并签署责任书情况下进行。

用户对操作系统的使用应经过正式授权和许可，并保证授权用户熟悉系统的操作流程，并对操作人员的操作过程实施人机操作监视。

网络安全管理要求

除满足第四级的要求外，至少有两名以上的网络安全管理人员实施网络安全管理事务，并保证网络安全管理本身的安全风险得到控制。

计算机信息系统网络之间的连接实现物理网络隔离。

应用系统安全

除满足第四级的要求外，要求对应用系统的安全状态实施周期更短的审计和检查，并保证对应用系统的安全措施能适应安全环境的变化。

运行安全管理要求

除满足第四级的要求外:

eee)要求风险管理计划已成为单位业务管理的有机组成部分，并对风险管理活动实施全面的质量管理。

fff)要求计算机信息系统生命周期各个阶段的安全管理已成为单位业务管理的有机组成部分，并对计算机信息系统生命周期管理实施全面的质量管理。

ggg)要求制定全面的应急计划和灾难恢复计划管理细则，并通过持续评估，保证应急计划和灾难恢复计划的时效性和有效性。

hhh)要求对所有变更进行安全评估，保证变更控制计划的不断完善。

a） 安全管理等级要素

（参考性附录）

管理等级要素是根据安全管理要求按等级分解的一组简约实施条款，便于比较、理解和操作，其内容与本标准第5章“安全等级信息系统管理要求”基本上是一致的，高等级的要求包含低等级的要求。

a） 管理目标和范围

a） 安全目标与范围等级要求

要求 等级	安全目标与范围要求
1	1） 包含系统安全目标和安全范围、系统设施和操作等内容的安全计划文件的制定。 2） 保证达到 GB17859-1999 相应等级技术要求的标准。
2	3） 安全管理机构的建立，安全操作规程的制定； 4） 针对关键的系统，风险管理计划的建立；
3	5） 用户及相关人员对安全策略和安全规程的熟知，并保证实施； 6） 系统安全的自动监视和审计； 7） 保证安全管理在生命周期中的贯穿实施； 8） 系统认证、验收的规定，系统使用的授权； 9） 工作岗位及职责文件的建立； 10） 一系列安全管理制度的建立；
4	11） 针对安全策略、操作规程、规章制度和安全措施的程序化、周期化的评估； 12） 针对关键控制措施的失效风险，测试计划的建立； 13） 针对明显的风险变化，风险评估的立即实施； 14） 针对安全事件记录，例行评估制度的实施； 15） 针对识别出的系统脆弱性的有效控制； 16） 通过定期评估，确保人员的主导作用；； 17） 分权管理机制的强制实施，可信管理的实施；
5	18） 全面安全管理计划对单位文化的有机嵌入，并适应安全环境的变化； 19） 实施全面质量管理。

b） 人员与职责要求

b） 人员与职责等级要求

要求 等级	人员与职责要求
1	1） 安全管理人员条件、职责的确定和配置；
2	2） 安全管理机构的建立，及其职责的确定和人员的配置； 3） 针对关键的系统，风险管理计划的建立；
3	4） 在系统安全风险控制和管理过程中，对安全事务的明确分工； 5） 针对系统工作人员和资源，等级标记管理的实施；
4	6） 针对系统应用部门，安全管理延伸和渗透的实施； 7） 独立审计的实施； 8） 针对全面安全管理活动的例行检查；

5	9） 所有人员对安全管理规定和要求的充分理解和有效执行； 10）针对所有岗位，所有人员的资质达标，并实施全面质量管理。

c） 物理安全管理要求

c） 物理安全管理等级要求

要求 等级	物理安全管理要求
1	1） 物理安全管理人员的配置； 2） 物理安全规章制度的建立； 3） GB17859-1999 相应等级技术要求的保证；
2	4） 物理安全区域管理的实施； 5） 设施配置计划、安装、运行、操作流程的制定； 6） 系统关键物理设施登记制度的建立；
3	7） 安全区域标记管理的实施；
4	8） 安全区域隔离管理的实施； 9） 出入人员授权书的建立； 10）对安全区域活动的实时监视；
5	11）物理安全保障的持续改善。

d） 系统安全要求

d） 系统安全管理等级要求

要求 等级	系统安全管理要求
1	1） 安全责任人的配置； 2） 有关安全管理规章制度的建立；
2	3） 操作系统配置、使用的审计； 4） 强制性唯一标示、口令的使用； 5） 资源使用的控制和授权； 6） 用户在关键操作系统上使用情况的登记和监视； 7） 系统工具使用授权管理制度的建立，相应技术控制和管理控制的实施； 8） 操作系统的安全评估、对安全弱点和漏洞的控制； 9） 操作系统变更控制制度的建立； 10）操作系统资源和系统文档的备份；
3	11）系统工具标记管理制度的建立； 12）对系统工具使用情况的审计； 13）应用软件安全管理制度的建立； 14）针对操作系统资源和系统文档的标记处理、安全备份； 15）应急安全计划的制定、实施； 16）关键岗位人员备用制度的建立；
4	17）针对系统内置角色，操作系统安全管理人员的分别配置； 18）操作系统管理过程的可审计性保证；
5	19）安全责任书在多方在场情况下的签署； 20）对操作人员的操作过程人机操作监视的实施。

e） 网络安全管理要求

e） 网络安全管理等级要求

要求 等级	网络安全管理要求
1	1) 网络安全责任人的配置； 2) 有关安全制度的建立； 3) 达到 GB17859-1999 相应等级技术要求的保证；
2	4) 针对网络使用情况的审计制度和标记制度的建立； 5) 网络使用和网络服务政策的制定； 6) 网络安全教育培训计划的制定； 7) 网络访问制度的制定； 8) 与外部网络接口的安全边界的确定和定期的评估； 9) 对外部访问接入点的控制和审计； 10) 对从内部网络向外发起的连接资源的控制； 11) 连接资源授权制度的建立； 12) 针对网络之间的连接，可审计的安全措施的实施，物理或逻辑网络隔离的实现； 13) 针对网络安全措施使用情况的审计； 14) 网络设施，网络服务变更控制制度的建立 15) 网络安全事件、事故报告制度的建立，及相应可审计性的保证； 16) 针对网络连接、网络安全措施、网络设备的定期评估； 17) 关键网络设施的备份； 18) 针对可用性要求高的网络，不间断监控的实施、相应应急计划的可行性验证；
3	19) 针对安全措施的使用情况，严格审计制度、标记制度的建立； 20) 网络安全审计人员的配置；
4	21) 独立安全审计的建立； 22) 网络安全管理人员资质的保证；
5	23) 至少两名以上网络安全管理人员的配置； 24) 物理网络隔离的实现。

f） 应用系统安全管理要求

f） 应用系统安全管理等级要求

要求 等级	应用系统安全管理要求
1	1） 系统安全责任人的配置； 2） 有关规章制度的制定；
2	3） 总体安全策略的制定、执行； 4） 系统安全操作规程的制定； 5） 信息的分类管理和信息的安全发布； 6） 信息访问控制机制的安装、授权和审计； 7） 针对内部用户的安全协议的签署； 8） 审计人员的配置； 9） 系统安全性的定期和不定期评估；

	10）针对关键岗位工作人员资质调查的实施； 11）备份计划和应急计划的制定、实施；
3	12）安全管理机构对系统安全措施的正确性和有效性的保证； 13）强制性标记信息访问控制机制的安装； 14）针对标记信息访问的授权和审计； 15）针对备份信息介质的标记制度的制定； 16）针对不同的信息等级，不同备份策略的制定；
4	17）独立的应用安全审计； 18）应用系统开发人员与审计工作的隔离，操作系统管理人员与应用系统安全管理工作的隔离； 19）针对不同等级的应用系统，不同的备份计划和应急计划的制定，及相应的定期测试；
5	20）周期更短的安全审计和检查； 21）适应安全环境变化的保证。

g） 运行安全管理要求

运行安全管理主要涉及的内容包括：风险管理、信息系统的生命周期管理、安全意识教育与培训、病毒防护、第三方访问安全管理、应急计划和灾难恢复计划管理、变更控制等，为便于理解，将本标准第5章中五个等级的运行安全管理要求在以上几个方面进行了分解。

g） 运行安全管理等级要求

要求 / 等级	运行安全管理要求
1	1) 系统负责人对运行管理的组织、指导和保证； 2) 采购计划和采购制度的建立； 3) 风险分析计划的建立； 4) 系统各类人员对系统资源安全责任的认知； 5) 系统安全管理人员和系统普通用户对系统资源以及控制系统中命名客体访问权限的认知； 6) 有关安全管理制度的建立。
2	
3	
4	
5	

i. 风险管理要求

h） 风险管理等级要求

要求 / 等级	风险管理要求
1	
2	1) 针对关键系统资源的定期风险分析和评估； 2) 风险分析报告向管理层的提交；
3	3) 在风险管理中，使用规范方法的保证；
4	4) 风险管理质量管理体系文件的建立； 5) 针对风险管理过程，独立审计的实施；

	6) 安全管理过程有效性的保证；
5	7) 风险管理计划成为单位业务管理有机组成部分； 8) 针对风险管理活动，全面质量管理的实施。

ii. **生命周期管理要求**

i） 生命周期管理等级要求

要求/等级	生命周期管理要求
1	
2	1) 在计划阶段 a) 针对系统敏感程度的评估； b) 保护标准的确定； c) 安全需求的确定； d) 安全系统的设计和采购； 2) 在实施阶段 e) 安全措施的实施、部署、验证和验收； 3) 在运行维护阶段 f) 对安全措施的评估； g) 对风险变更的监视和评估； 4) 在结束阶段 h) 对系统信息的安全处置；
3	5) 针对生命周期各个阶段的安全管理工作，相应目标和职责的确定； 6) 正式管理报告的提交；
4	7) 针对系统生命周期管理，质量控制体系文件的建立； 8) 针对系统生命周期管理，独立审计的实施；
5	9) 生命周期各阶段的安全管理工作，成为单位业务管理的有机组成部分； 10) 针对生命周期管理，全面安全质量管理的实施。

iii. **安全意识教育和培训要求**

j） 安全意识教育和培训等级要求

要求/等级	安全意识教育和培训要求
1	
2	1) 系统各类人员安全意识，安全教育和培训计划的制定、实施；
3	2) 系统所有工作人员对安全政策和操作规程的认知； 3) 针对不同岗位，不同等级培训计划的制定；
4	4) 所有工作人员资质的检查和评估； 5) 安全教育成为单位工作计划的一部分；
5	6) 针对所有工作人员资质管理的实施； 7) 安全意识成为所有工作人员的自觉存在。

iv. **病毒防护管理要求**

k） 病毒防护管理等级要求

要求/等级	病毒防护管理要求
1	

2	1) 病毒防护系统使用管理制度的制定； 2) 应用软件安全管理制度的建立； 3) 应用软件采购批准制度； 4) 应用软件使用授权制度的建立；
3	5) 病毒防护管理制度的集中实施； 6) 在系统所有终端有效防范病毒或恶意代码引入的实现；
4	7) 针对病毒防护管理制度，定期或不定期检查的实现。
5	

v. 对第三方访问的安全管理要求

l） 对第三方访问的安全管理等级要求

要求 / 等级	对第三方访问的安全管理要求
1	
2	1) 针对第三方访问的安全管理制度的建立； 2) 针对第三方访问的安全性评估； 3) 针对第三方的保密合同的签署；
3	4) 针对第三方访问的风险分析和评估； 5) 针对第三方访问的严格控制制度的实施； 6) 针对第三方访问监视的实施；
4	7) 针对第三方每次访问的风险控制。
5	

vi. 应急计划和灾难恢复计划安全管理要求

m） 应急计划和灾难恢复计划安全管理等级要求

要求 / 等级	应急计划和灾难恢复计划安全管理要求
1	
2	1) 应急计划和灾难恢复计划的制定、测试； 2) 针对关键应用系统和支持系统的应急计划和灾难恢复计划的制定、测试； 3) 计划涉及人员的培训，相应执行能力的保证； 4) 与计划涉外资源的合同签署； 5) 安全事件处理制度的制定； 6) 系统信息和文档备份制度的制定；
3	7) 专人负责应急计划和实施恢复计划管理工作的保证； 8) 应急计划和灾难恢复计划做到重点突出、有效执行的保证；
4	9) 针对应急计划和灾难恢复计划独立审计的实施； 10) 针对应急计划和灾难恢复计划的定期评估；
5	11) 应急计划和灾难恢复计划全面管理细则的制定； 12) 针对应急计划和灾难恢复计划的持续评估。

vii. 变更控制管理要求

n） 变更控制管理等级要求

要求 / 等级	变更控制管理要求

1	
2	1) 针对操作系统、数据库、应用系统、人员、服务、内外风险等的变更控制制度的制定； 2) 运行管理安全制度的制定； 3) 针对所有计划和制度执行情况的定期或不定期的监督、检查； 4) 针对安全策略和管理计划的修订； 5) 基于变更带来的各种规章制度的修订和完善； 6) 运行过程管理文档的建立；
3	7) 全面安全事务一致性的实现；
4	8) 独立的安全审计的实施； 9) 对全面安全事务一致性的检查和评估；
5	10) 针对所有变更的安全评估； 11) 变更计划和效果持续改善的保证。

h) 人员安全管理要求

o) 人员安全管理等级要求

要求 / 等级	人员安全管理要求
1	
2	1) 根据分权制衡原则和最小特权原则，对工作岗位、岗位职责和敏感程度的确定； 2) 人员选择、录用标准、资质标准的确定； 3) 人员背景调查程序的确定； 4) 保密协议的签署； 5) 用户管理制度的建立、实施 6) 针对用户授权和安全协议的签署； 7) 针对用户访问情况的审计和检查； 8) 针对非授权访问和违规操作的调查、取证和惩罚制度的建立、实施； 9) 针对离岗人员可能威胁的评估，以及相应措施的实施；
3	10) 针对关键岗位工作人员，严格的背景调查和管理控制的实施； 11) 关键安全事务双人共管的实现；
4	12) 关键安全事务多人共管的实现；
5	13) 针对所有岗位工作人员，全面安全质量管理的实施； 14) 针对内部人员全面控制的保证。

参考文献

1、ISO/IEC TR 13335-1：2000, Information Technology - Security Techniques . Guidelines for the Management of IT Security (GMITS). Part 1: Concepts and Models for IT Security。（ISO/IEC TR 13335-1：2000, 信息技术-安全技术-IT安全管理指南，第1部分：IT安全的概念和模型）

2、ISO/IEC TR 13335-2：2000,Information Technology - Guidelines for the Management of IT Security -Part 2: Managing and Planning IT Security（ISO/IEC TR 13335-2：2000, 信息技术-安全技术-IT安全管理指南，第2部分：IT安全的管理和规划）

3、ISO/IEC TR 13335-3：2000, Information Technology - Security Techniques .Guidelines for the Management of IT Security (GMITS):Part 3 - Techniques for the Management of IT Security（ISO/IEC TR 13335-3：2000, 信息技术-安全技术-IT安全管理指南，第3部分：IT安全管理技术）

4、ISO/IEC TR 13335-4：2000, Information Technology -Guidelines for the Management of IT Security (GMITS) - Part 4: Selection of Safeguards（ISO/IEC TR 13335-4：2000, 信息技术-安全技术-IT安全管理指南，第4部分：安全措施选择）

5、ISO/IEC TR 13335-5：2000，Information Technology . Guidelines for the Management of IT Security. Part 5: Management Guidance of Network Security（ISO/IEC TR 13335-5：2000, 信息技术-安全技术-IT安全管理指南，第5部分：网络安全管理指南）

6、ISO/IEC TR 17799：2000 Information security Management —Code of Practice for Information Security Management（ISO/IEC TR 17799：2000 信息安全管理－信息安全管理实践规范）