ICS 35.020
L 09

中华人民共和国国家标准

GB/T 20282—2006

信息安全技术
信息系统安全工程管理要求

Information security technology—
Information system security engineering management requirements

2006-05-31 发布　　2006-12-01 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
信息安全技术
信息系统安全工程管理要求
GB/T 20282—2006
*
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:(010)51299090、68522006
2006 年 9 月第一版
*
书号:155066·1-27972

目　　次

前　言

本标准的附录 A 是资料性附录。

本标准由信息安全标准化技术委员会提出并归口。

本标准起草单位：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、上海标准化研究院。

本标准主要起草人：张建军、魏忠、叶铭、陈长松、孔一童。

信息安全技术
信息系统安全工程管理要求

1 范围

本标准规定了信息系统安全工程(以下简称安全工程)的管理要求,是对信息系统安全工程中所涉及到的需求方、实施方与第三方工程实施的指导,各方可以此为依据建立安全工程管理体系。

本标准按照 GB 17859—1999 划分的五个安全保护等级,规定了信息系统安全工程管理的不同要求。

本标准适用于信息系统的需求方和实施方的安全工程管理,其他有关各方也可参照使用。

2 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 安全保护等级划分准则

GB/T 20269—2006 信息安全技术 信息系统安全管理要求

GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

3 术语和定义

下列术语和定义适用于本标准。

3.1

安全工程 security engineering

为确保信息系统的保密性、完整性、可用性等目标而进行的系统工程过程。

3.2

安全工程的生存周期 security engineering lifecycle

在整个信息系统生存周期中执行的安全工程活动包括:概念形成、概念开发和定义、验证与确认、工程实施开发与制造、生产与部署、运行与支持和终止。

3.3

安全工程指南 security engineering guide

由工程组做出的有关如何选择工程体系结构、设计与实现的指导性信息。

3.4

脆弱性 vulnerability

能够被某种威胁利用的某个或某组资产的弱点。

3.5

风险 risk

某种威胁会利用一种资产或若干资产的脆弱性使这些资产损失或破坏的可能性。

3.6

需求方 owner

信息系统安全工程建设的拥有者或组织者。

3.7

实施方　developer

信息系统安全工程的建设与服务的提供方。

3.8

第三方　third party

独立于需求方、实施方，从事信息系统安全工程建设相关活动的中立组织或机构。

3.9

项目　project

项目是各种相关实施活动和资源的总和，这些实施活动和资源用于开发或维护信息系统安全工程。一个项目往往有相关的资金，成本账目和交付时间表。

3.10

过程　process

把输入转化为输出的一组相关活动。

3.11

过程管理　process management

一系列用于预见、评价和控制过程执行的活动和体系结构。

4　安全工程体系

4.1　概述

在整个工程范围内确定了不同等级工程的具体要求构成了安全工程管理要求体系。通过这个体系从安全工程中分离出实施和保证的基本特征，建立信息系统安全分级保护要求与工程管理的关系。

4.2　安全工程目标

理解需求方的安全风险，根据已标识的安全风险建立合理的安全要求，将安全要求转换成安全指南，这些安全指南指导项目实施的其他活动，在正确有效的安全机制下建立对信息安全的信心和保证；判断系统中和系统运行时残留的安全脆弱性，及其对运行的影响是否可容忍(即可接受的风险)，使安全工程成为一个可信的工程活动，能够满足相应等级信息系统设计的要求。

4.3　基本关系

安全工程由安全等级、保证与实施要求两个维度组成，不同等级要求的安全工程对应不同的保证与实施要求。其中保证是由资格保证要求和组织保证要求构成，实施是由工程实施要求和项目实施要求构成。资格保证要求表示信息安全工程中对应具备一定能力级别的实施方或与工程相关第三方资质的要求；组织保证要求表示信息安全工程过程要求中对需求方组织保证的要求；工程实施要求表示信息安全工程中对安全实施过程的要求；项目实施要求表示信息安全工程中对项目实施过程的要求。

5　资格保证要求

5.1　系统集成资质要求

国家主管部门认可的系统集成资质。

5.2　人员资质要求

国家主管部门认可的安全服务人员资质。

5.3　第三方服务要求

国家主管部门认可的服务单位资质。

5.4　安全产品要求

信息安全产品应具有在国内生产、经营、销售的许可证，并符合相应的等级。

5.5　工程监理要求

5.5.1　应具备信息安全系统建设工程实施监理管理制度。

5.5.2 系统聘请专业监理公司，且监理公司具有国家主管部门认可监理资质证书。

5.6 法律、法规、政策符合性要求

系统应符合国家相关的法律、法规和政策。

6 组织保证要求

6.1 定义组织的系统工程过程

6.1.1 基本要求

应为系统工程定义一套标准有明确目标的过程，这套标准的过程可以通过裁剪应用于定义新工程项目的过程。

6.1.2 制定过程目标

6.1.2.1 从组织的应用目标出发为组织的系统工程过程制定目标。

6.1.2.2 系统工程过程在业务环境中运行，为了使组织的标准实现制度化，该目标应得到明确的认可；这个过程的目标应考虑财力、质量、人力资源和对业务成功起重要作用的问题。

6.1.3 收集过程资产

6.1.3.1 收集和维护系统工程过程资产。

6.1.3.2 在组织和项目层次中，由过程定义活动所产生的信息都需要存储(在过程资产库中)，使得那些剪裁、过程设计活动中的资产能被使用人理解，并得到维护与保持。

6.1.4 开发组织的系统工程过程

6.1.4.1 为组织开发一个充分定义的标准系统工程过程。

6.1.4.2 在开发组织的标准系统工程过程中，可能使用到过程资产库中的设备；在开发任务时，可能需要一些新的过程资产，应该将这些资产添加到过程资产库中；应该将组织的标准系统工程过程置于过程资产库中。

6.1.5 定义剪裁指南

定义剪裁组织的标准系统工程过程的指南，该指南在开发项目的定义过程中使用。

6.2 改进组织的系统工程过程

6.2.1 基本要求

应实施测量和改进系统工程过程的连续活动，以标准系统工程过程定义为基础，通过不断改进活动提高组织系统工程过程的效益和效率。

6.2.2 评定过程

6.2.2.1 评定组织中现有的执行过程以便了解它们的强项和弱项，了解组织现有的执行过程的强项和弱项是建立改进活动基线的关键。

6.2.2.2 评定时应考虑过程执行的测量与课程学习过程；评定可以多种形式进行，评定方法的选择应与文化和组织需求相匹配。

6.2.3 规划过程改进

应基于对潜在改进所产生影响的分析，为组织制定过程改进计划，以达到过程的目标。

6.2.4 改变标准过程

改变组织的标准系统工程过程以便反映目标的改进。

6.2.5 沟通过程改进

适当地同现有项目和其他相关团体共同沟通过程的改进。

6.3 管理系列产品演化

6.3.1 基本要求

应通过引进服务、设备和新技术实现产品更新与工程费用降低，获取工程进度和执行的最佳收益。

6.3.2 定义产品演化

6.3.2.1 定义要提供产品的类型。

6.3.2.2 定义支持组织战略目标的系列产品。

6.3.2.3 考虑组织的强项和弱项、竞争力、潜在的市场份额和可利用的技术。

6.3.3 标识新生产技术

6.3.3.1 标识新生产技术或加强基础设施建设，将有助于组织获取、开发和应用新生产技术来提高竞争优势。

6.3.3.2 确定可能引入到系列产品的新生产技术，为确定新技术和基础设施改进而建立并能维护的原始资料和方法。

6.3.4 适应开发过程

6.3.4.1 在产品开发周期中采取必要的变动以支持新产品的开发。

6.3.4.2 适应组织的产品开发过程，熟悉并利用准备在将来使用的组件。

6.3.5 确保关键组件的可用性

6.3.5.1 确保关键组件都可利用，并可以支持有计划的产品改进。

6.3.5.2 组织应确定产品系列的关键组件及其可用性的计划。

6.3.6 插入产品技术

6.3.6.1 将新的技术插入到产品开发、市场营销和制造过程中。

6.3.6.2 管理将新技术引入到系列产品的工作(包括现有产品系列组件的改进、新组件的引进)；标识和管理与产品设计变化有关的风险。

6.4 管理系统工程支持环境

6.4.1 基本要求

应能够为不同需求的系统工程提供支持环境，并可以通过剪裁适应不同的项目。根据技术、环境状态的变化对支持环境进行改进。

6.4.2 维持技术认识

6.4.2.1 维持对支持实现组织目标的那些技术的认识。

6.4.2.2 对工艺现状或实施现状应该插入新的技术，组织应具有对新技术的充分认识。

6.4.3 确定支持需求

根据组织的需要确定组织的系统工程支持环境的需求。

6.4.4 获得系统工程支持环境

6.4.4.1 获得一个系统工程支持环境，该环境要满足在确定支持需求中通过利用分析候选解决要求项的实施而建立的要求。

6.4.4.2 针对所需的系统工程支持环境，确定其评价标准和潜在的候选解决方案；利用分析候选解决要求项选择一个解决方案；得到并实现所选的系统工程支持环境。

6.4.5 剪裁系统工程支持环境

剪裁系统工程支持环境，以满足单个项目的要求。

6.4.6 插入新技术

6.4.6.1 根据组织的应用目标和项目需要将新技术插入到系统工程支持环境中。

6.4.6.2 组织的系统工程支持环境应用新技术更新，并要支持组织的应用目标及工程需要；在系统工程支持环境中，应提供使用新技术的培训。

6.4.7 维护环境

6.4.7.1 维护系统工程支持环境以持续支持依赖该环境的项目。

6.4.7.2 维护活动包括计算机系统管理、培训、热线支持、专家的作用、发展或者扩充一个技术库等。

6.4.8 监视系统工程支持环境

6.4.8.1 监视系统工程支持环境以发现改进的机会。

6.4.8.2 确定影响系统工程支持环境有用性的因素，包括任何新插入的技术；监视新技术和整个系统工程支持环境的接受情况。

6.5 培训

6.5.1 基本要求

应建立一套完整的培训体系，能够为员工提供满足组织需求并适用于系统工程活动的、及时有效的知识与技能培训。

6.5.2 确定培训要求

6.5.2.1 以项目的要求、组织的战略计划和现有的员工技能情况为指导，确定组织在技能与知识方面所需的改进。

6.5.2.2 综合现有的程序、组织的战略计划和现有员工的技能等各方面信息确定这些要求。

6.5.3 选择知识或技能的获取模式

6.5.3.1 评价和选择通过培训或其他资源获取知识或技能的适当模式。

6.5.3.2 应确保所选择的方法是最佳的，以使得所需技能和知识对项目及时有效。

6.5.4 确保技能和知识的可用性

确保技能和知识对系统工程活动是适用的。

6.5.5 准备培训材料

6.5.5.1 根据确定的培训要求准备培训材料。

6.5.5.2 为每一个由组织内部人员建成的班编制培训材料，或为每一个已存在的班准备培训材料。

6.5.6 培训人员

6.5.6.1 培训教员要具备执行赋予他们的角色的技能与知识。

6.5.6.2 要根据培训计划和编制的材料进行人员培训。

6.5.7 评估培训的有效性

6.5.7.1 评估培训的有效性以满足所确定的培训要求。

6.5.7.2 评估有效性的方法应与培训计划编制和培训材料的拟定同时列出；应及时获取有效性评估的结果，以便对培训做出相应调整。

6.5.8 维护培训记录

6.5.8.1 维护培训与取得经验的记录。

6.5.8.2 维护记录以追踪每个人员接受培训的情况，以及受训后的技能和能力。

6.5.9 维护培训材料

6.5.9.1 维护知识库中的培训材料。

6.5.9.2 维护知识库中的课件材料以供员工今后访问，并且在课程材料变动时可供跟踪。

6.6 与供应商协调

6.6.1 基本要求

应能够根据工程的需求建立与维护供应商的关系，确保供应商能够为系统工程提供满足要求的产品或服务。

6.6.2 确定系统的组件或服务

确定应由其他外部组织提供的系统组件或服务。

6.6.3 确定胜任的供应商或销售商

6.6.3.1 标识在特定领域中具有专门技术的供应商。

6.6.3.2 供应商的能力包括胜任开发过程、制造过程、验证责任、及时交付、生存周期支持过程及远程有效通信能力，上述能力应符合本组织的各项要求。

6.6.4 选择供应商或销售商

6.6.4.1 依照 7.1 选择供应商。

6.6.4.2 以合乎逻辑和公平的方式选择供应商以满足产品的目标；提供最能弥补本组织能力的供应商特征，标识合格的候选者；通过要求项 7.1 的实施来选择出合适的供应商。

6.6.5 **提出要求**

6.6.5.1 对供应商提出组织对系统组件或服务的要求、期望和效果指标。

6.6.5.2 在合同签署时组织应将它的要求和期望清楚地指明并排出优先顺序，并且要指明对供应商方面的所有限制；组织要与供应商密切合作，使其充分了解产品达到的要求和自己要承担的责任，并达成相互理解。

6.6.6 **维持沟通**

6.6.6.1 与供应商维持及时的双向沟通。

6.6.6.2 组织与供应商要对期望的和所需的沟通建立相互谅解。所建立的沟通的特点包括：双方公认的公开的没有任何限制的信息类型，受限的信息类型（如策略或合同关系），所期望的信息请求与回应的及时性，用于沟通的工具和方法，安全、保密以及期望的分布情况。

7 工程实施要求

7.1 管理安全控制

7.1.1 **基本要求**

应保证系统在运行状态下达到设计预期的安全特性，安全控制措施被配置且能正常使用。

7.1.2 **建立安全职责**

7.1.2.1 建立安全控制措施的职责和责任并通知到组织中的每一个人。

7.1.2.2 本项目应该保证承担相应安全责任的人员是负责的，并获得相应的授权；应该保证采用的所有安全控制措施是明确的，并被广泛和一致地应用。

7.1.3 **管理安全配置**

7.1.3.1 所有设备的安全配置都需要管理。

7.1.3.2 管理系统安全控制措施的配置。

7.1.4 **管理安全意识、培训和教育大纲**

7.1.4.1 组织和管理对所有员工进行安全意识的培训和教育。

7.1.4.2 管理所有的需求方和管理员的安全意识、培训和教育大纲。

7.1.5 **管理安全服务及控制机制**

7.1.5.1 安全服务及控制机制的一般管理类似于其他服务及机制的管理，包括保护它们避免损伤、偶然事故和人为故障，并根据法律和政策要求进行整理并归档。

7.1.5.2 对安全服务及控制机制进行定期的维护和管理。

7.2 评估影响

7.2.1 **基本要求**

应标识对该系统有关系的影响，并对发生影响的可能性进行评估。

7.2.2 **对影响进行优先级排列**

对在系统中起关键作用的运行、业务或任务的能力进行标识、分析和按优先级排列。

7.2.3 **标识系统资产**

7.2.3.1 对支持系统的安全目标或关键性能力（运行，业务或任务功能）进行标识。

7.2.3.2 对必需的系统资源和数据进行标识；通过对给定环境中提供这种支持的每项资产的意义进行评估，来对每项资产进行定义。

7.2.3.3 对支持系统的关键性运行能力或安全目标的系统资产进行标识和特征化。

7.2.4 **选择影响的度量**

应预先确定适合的度量用于评估影响。

7.2.5 **标识度量关系**

标识所选影响的评估度量与度量转换因子之间的关系。

7.2.6 标识和特征化影响

利用多重度量或统一度量的方法对意外事件的意外影响进行标识和特征化。

7.2.7 监视影响

监视影响中的变化，本条与 7.8.3 中的通用性监视活动紧密相连。

7.3 评估安全风险

7.3.1 基本要求

应对在特定环境中运行该系统相关的安全风险进行标识与评价，并按照一定的方法对风险问题进行优先级排序。

7.3.2 选择风险分析方法

7.3.2.1 本要求项包括定义用于标识给定环境中的系统安全风险的方法，该方法是对安全风险进行分析、评估和比较；应该包括一个对风险进行分类和分级的方案，其依据是威胁、运行功能、已建立的系统脆弱性、潜在损失、安全需求等相关问题。

7.3.2.2 选择用于分析、评估和比较给定环境中系统安全风险所依据的方法、技术和准则。

7.3.3 标识安全风险

7.3.3.1 标识该风险，认识这些威胁和脆弱性的利害关系，进而标识出威胁和脆弱性造成的影响；这些风险在选择系统保护措施中应予以考虑。

7.3.3.2 标识威胁、脆弱性、影响三组合(风险)。

7.3.4 评估安全风险

7.3.4.1 标识每个风险出现的可能性。

7.3.4.2 评估与每个风险有关的风险。

7.3.5 评估总体不确定性

7.3.5.1 每种风险都有与之相关的不确定性；总体风险不确定性是在 7.4.6、7.5.4 中已被标识的威胁、脆弱性及其特征和影响不确定性的累积。本要求项与 7.6 密切相关，因为证据能用于追踪修改，从而在某种输入下降低不确定性。

7.3.5.2 评估与该风险有关的总体不确定性。

7.3.6 安全风险优先级排列

7.3.6.1 已经被标识的风险应以组织优先权、风险出现的可能性与这些因素相关的不确定性和可用财力为依据进行排序；风险可以被减轻、避免、转移或接受，也可以使用这些措施的组合。“减轻”这一措施能够对付威胁、脆弱性、影响或风险本身；安全措施的选择要适当考虑到 7.10 中的要求、业务优先级和整个系统体系结构。

7.3.6.2 按优先级对风险进行排列。

7.3.7 监视安全风险及其特征

7.3.7.1 定期地检查新的风险，本条与 7.8.3 中一般性监视活动紧密相联。

7.3.7.2 监视安全风险频度变化和风险特征的变化。

7.4 评估威胁

7.4.1 基本要求

应标识安全威胁及其性质和特征，对系统安全的威胁进行标识和特征化；应定期地对威胁进行监视，以保证由本要求项所产生的安全理解始终得到维持。

7.4.2 标识自然威胁

标识由自然原因引起的相应威胁。

7.4.3 标识人为威胁

标识由人为偶然原因引起的威胁与故意行为引起的威胁。

7.4.4 **标识威胁的测量尺度**

7.4.4.1 对可能在特定位置中出现的预料事件，应根据具体情况建立最大和最小测量单位范围。

7.4.4.2 标识特定环境中相应的测量尺度和适用范围。

7.4.5 **评估威胁影响的效果**

7.4.5.1 确定对系统进行成功攻击的黑客潜在的能力。

7.4.5.2 评估由人为原因引起的威胁影响的动因和结果。

7.4.6 **评估威胁的可能性**

对威胁事件如何发生的可能性进行评估，评估出现威胁事件的可能性。

7.4.7 **监视威胁及其特征**

7.4.7.1 有规律地对现有威胁及其特征进行监视，并检查新的威胁；本条与 7.7.2 的一般化监视活动紧密相连。

7.4.7.2 监视威胁范围中不断的变化以及相应特征的变化。

7.5 **评估脆弱性**

7.5.1 **基本要求**

应标识和特征化系统的安全脆弱性。实施系统资产分析、定义特殊的脆弱性以及提供对整个系统脆弱性的评估，并获得对一确定环境中系统安全脆弱性的理解。

7.5.2 **选择脆弱性分析方法**

7.5.2.1 所有分析应在预先安排和指定时间内，在一个已知的并记录有配置的框架内进行；分析的方法论应包括预期结果；分析的特定目标应陈述清楚。

7.5.2.2 选择对一确定环境中系统安全脆弱性进行标识和特征化的方法、技术和标准。

7.5.3 **标识脆弱性**

7.5.2 中研究过的脆弱性分析方法论应延伸到对脆弱性的证实；所有发现的系统安全脆弱性应予以记录、标识。

7.5.4 **收集脆弱性数据**

收集与脆弱性相关的数据。

7.5.5 **综合系统脆弱性**

分析哪些脆弱性或脆弱性的组合会对系统造成问题，所有分析应标识出该脆弱性的特征；评估由特定脆弱性和特定脆弱性组合所产生的系统脆弱性与总体脆弱性。

7.5.6 **监视脆弱性及其特征**

7.5.6.1 本项要求与 7.8.3 中变化的一般性监视活动紧密相连。

7.5.6.2 监视脆弱性及其特征的连续变化。

7.6 **建立保证论据**

7.6.1 **基本要求**

应对需求相关的保证证据进行标识和定义，包括证据的产生和分析的活动，包括支持保证需求所需的附加证据、文档清单和过程以及那些能清晰地向需求方提供已满足其安全需求的证据。

本项目要求建立保证证据有关的活动记录，包括管理、标识、计划、封装和提交安全保证证据。

7.6.2 **标识保证目标**

7.6.2.1 标识安全保证目标。

7.6.2.2 系统安全保证目标应规定强制性系统安全策略的保密性等级；目标的充分性由开发者、集成者、需求方和签名授权者确定。

7.6.2.3 新的和修改过的安全保证目标的标识应与所有内部和外部工程组织等安全相关性团体保持协调一致。

7.6.2.4 对安全保证目标进行修改的内容需及时解释其中变化。

7.6.2.5 安全保证目标应清晰地沟通。

7.6.3 定义保证策略

7.6.3.1 规划并确保正确地实现强制性安全目标;通过实现安全保证策略所产生的证据应(向系统签名授权者)提供一个可接受的保密性等级,此等级安全的测量足以管理安全风险。通过开发并颁布安全保证策略,获得对保证的相关活动进行有效管理;工程早期应对需求相关的保证进行的标识和定义产生必要的支持证据;通过不断外部协调,对保证需求方需求的满意程度进行理解和监视,确保高质量组合保证要求。

7.6.3.2 为所有保证目标定义一个安全保证策略。

7.6.4 控制保证证据

安全保证证据通过与所有工程实施要求项相互配合,在安全保证策略内标识出的不同层面抽象的证据的方法进行收集;证据应受到控制。

7.6.5 分析证据

对安全保证证据进行分析,保证工程产品相对于基线系统是完善和正确的。

7.6.6 提供保证论据

7.6.6.1 开发出一个完整的证明与安全目标一致的安全保证论据,并提供给需求方;保证论据是由多层抽象中获得的保证证据的组合所支持的一系列声明性保证目标;应对提交证据中的缺陷和安全保证目标中的缺陷进行评审。

7.6.6.2 提供证明需求方安全需求得到满足的安全保证性论据。

7.7 协调安全

7.7.1 基本要求

应协调并保持安全工程所涉及到安全组织、其他工程组织和外部组织之间的关系;以保证所有部门都有一种参与安全工程的意识。

7.7.2 定义协调目标

定义和建立与其他组织之间的联系和义务关系;这些关系应被全体参与部门所接受。

7.7.3 标识协调机制

标识安全工程的协调机制,明确协调机制实现的方法。

7.7.4 促进协调

7.7.4.1 确保不同优先级的不同组织间进行沟通有可能发生的一些冲突和争端以合适的、富有成果的方式得到解决。

7.7.4.2 促进安全工程的协调。

7.7.5 协调安全确定和建议

在各种安全工程组织、其他工程组织、外部实体及其他合适的部门中沟通安全确定和建议,用标识出的机制去协调有关安全的确定和建议。

7.8 监视安全态势

7.8.1 基本要求

应标识并报告所有的安全违规行为;监视外部和内部环境中可能影响系统安全的所有因素;探测和跟踪内部和外部与安全有关的事件。根据策略制定响应突发事件的措施;根据安全目标标识并处理运行安全态势的变化。

7.8.2 分析事件记录

检测安全相关性信息的历史和事件记录,通过多条记录中的事件相关元素,标识出安全事件;分析事件记录,以确定事件的原因、预测可能发生的事件。

7.8.3 监视变化

监视威胁、脆弱性、影响、风险和环境方面的变化,查找可能影响当前安全状态有效性的任何变化;

监视所有因素的变化并分析这些变化以评估它们对安全有效性的意义。

7.8.4 标识安全突发事件

7.8.4.1 确定是否发生了一个有关安全的突发事件，标识出事件详细情况并且在必要时提出报告；有关安全的突发事件可利用历史事件的数据、系统配置数据、完整性工具和其他系统信息诊断。

7.8.4.2 标识与安全相关的突发事件。

7.8.5 监视安全防护措施

7.8.5.1 检测安全防护措施的执行情况，标识出安全防护措施执行中的变化。

7.8.5.2 监视安全防护措施的性能和有效性。

7.8.6 检查安全态势

检查系统安全态势以标识出必要的更正，评审实施安全的理由并根据其他的规则检查需要安全的地方。

7.8.7 管理安全突发事件响应

应急计划要求标识出系统失效的最长时间、系统正常工作的基本元素；开发一个可恢复策略和计划，测试并维护该计划。

7.8.8 保护安全监视的记录数据

保证与安全监视有关的设备得到相应的保护，监视活动包括封存和归档相关的日志、审计报告和相关分析结果。

7.9 提供安全输入

7.9.1 基本要求

应为系统的规划者、设计者、实施者或需求方提供他们所需的安全信息，信息应包括安全体系结构、设计或实施选择以及安全指南；开发、分析并提供安全输入并与基于7.10中定义的安全需求中的适当组织机构成员协调一致；要求所有具有安全意义的系统问题都应受到检查并按照安全目标的要求予以解决；所有项目组成员都要理解安全问题，解决方法应反映出所提供的安全输入。

本要求项适用于标定开发(设计者和实现者)和运行(用户和管理员)的安全输入。

7.9.2 理解安全输入要求

7.9.2.1 安全输入包括任何种类的、应被其他项目所考虑的、与安全相关的指南、设计、文档或思想；输入可以为多种形式包括文档、备忘录、电子邮件、培训和咨询。

7.9.2.2 安全输入要求可基于7.10中确定的需求。

7.9.2.3 设计者、开发者和需求方应一起确保相应部门对安全输入有一个共同的理解。

7.9.3 确定安全约束和考虑因素

确定做出有科学依据的工程决策所需的所有安全约束和考虑因素。安全工程组进行分析以确定在需求、设计、实现、配置和文档方面的任何安全限制和考虑；约束可在系统生存周期内的所有时间进行标识，可在许多不同的抽象层上进行标识。

7.9.4 标识安全选项

标识出与安全相关的工程问题的解决办法选项；解决办法可以多种形式提供。

7.9.5 分析工程选项的安全性

7.9.5.1 分析和区分工程选项的优先级；确定安全约束与考虑因素(见7.9.3)，根据标识的安全约束和考虑因素，设计组可以评估每个工程选项并提出对工程组的建议；安全工程组应考虑其他工程组的工程指南。

7.9.5.2 这些工程选项不受所标识的安全选项的限制(见7.9.4)，还应包括来自其他项目的选项。

7.9.5.3 利用安全约束和考虑因素来分析和区分工程选项的优先级。

7.9.6 提供安全工程指南

制定出与安全相关的指南，并将它提供给工程组。

7.9.7 提供运行安全指南

7.9.7.1 制定出与安全相关的指南并提供给系统用户和管理员；运行安全指南的制定应在生存周期内提早开始。

7.9.7.2 运行安全指南包含用户和管理员在以安全模式进行安装、配置、运行和终止系统时应做的内容。

7.10 指定安全要求

7.10.1 基本要求

应明确地为系统标识出与安全相关的要求；指定安全要求涉及到系统安全定义的基本原则，遵循有关安全的所有法律、策略和组织需求；定义与安全相关的要求集合成系统安全的基线。所有部门，包括用户之间应达成对安全要求的共识；应定义整个信息系统中所有安全方面的活动，通过在整个项目中收集、提炼、使用和更新(见 7.9)这一要求项所获得和产生的信息，提出安全要求。

7.10.2 获得对安全要求的理解

通过收集所有用于全面理解需求方安全要求所需的信息，获得对安全要求的理解。

7.10.3 标识可用的法律、策略和约束

为给定系统确定法律、策略、标准、外部影响和约束；收集所有对系统安全产生影响的外部影响；标识出支配系统目标环境的法律、规则、策略和业务标准；应进行全局和局部间优先级的决策；系统需求方提出的系统安全需求应被标识并说明安全意义。

7.10.4 标识系统安全关联性

7.10.4.1 标识出系统间的关系是如何影响安全的，任务的处理和运行概要应作为安全因素加以评估；标识出系统遭受到的或可能遭受到的威胁，评估性能和功能需求对安全可能产生的影响。

7.10.4.2 定义系统的安全边界；组织的许多外部因素也影响组织安全要求的变化程度，监视和定期地评估策略上的倾向性和策略重点的改变、技术开发、经济影响、全局性事件以及信息战等变化带来的潜在影响。

7.10.4.3 标识系统的用途以确定其安全的关联性。

7.10.5 获取系统运行的安全思想

7.10.5.1 应明确总体的、面向安全的指导思想，包括任务、职责信息流、资产、资源、人员保护以及物理保护的指导思想。

7.10.5.2 明确系统运行的面向安全的总体指导思想。

7.10.6 获取安全的高层目标

确定在运行环境中对系统安全性是足够的安全目标；获取高层安全目标就是定义系统的安全性。

7.10.7 定义安全相关需求

7.10.7.1 定义与系统安全相关的需求，应保证需求的完备性和一致性，为系统安全的评价提供基础。

7.10.7.2 定义一套一致性需求，该需求定义了在系统中将实现的保护。

7.10.8 达成安全协议

应在系统的安全需求中将所有的适用部分与特定安全之间达成协议；对于未被标识的特殊用户而不是一个通用用户组的情况下，特定安全要满足目标设置；特定的安全应该完整地、一致地反映出对策略、法律和用户需求的管理；应标识并修改所发现的问题，直到达成满足需求方要求的协议。

7.11 验证和确认安全性

7.11.1 基本要求

应确保解决安全问题的办法已经被验证与证实。通过观察、示范、分析和测试，依照安全需求、体系结构和设计确认解决办法；依照需求方的运行安全需求证实解决办法；解决办法应满足需求方安全需求与运行安全要求。

7.11.2 确定验证和确认的目标

确定验证和确认的目标；确定验证和确认的解决办法。

7.11.3 **定义验证和确认方法**

7.11.3.1 应定义验证和确认每种解决方案的方法和严格等级；

7.11.3.2 严密等级应表明验证和确认的审查到底应有多严格；该要求项要受到 7.6 中保证策略输出的影响。

7.11.4 **执行验证**

7.11.4.1 应通过显示解决办法实现与上一抽象层相关的要求，包括确定的保证需求正是作为 7.6 的结果所标识的保证需要；所用的方法在 7.11.3 中有标识；个人需求和整个系统都要受到检测。

7.11.4.2 验证解决办法实现了与上一抽象层相关的要求。

7.11.5 **执行证实**

7.11.5.1 通过显示能满足与上一抽象层相关的要求，最终满足需求方的运行安全要求，实现对解决办法的证实。

7.11.5.2 证实解决办法满足与上一抽象层关联的需要；所使用的方法应在 7.11.3 中确定。

7.11.6 **提供验证和确认的结果**

为其他工程组收集并提供验证和确认的结果；验证和确认的结果应以某种易被理解和使用的方式所提供；所有结果应被跟踪。

8 项目实施要求

8.1 质量保证

8.1.1 **基本要求**

应通过对过程的测量与监视，工作产品的测量发现其中的偏离；应通过质量分析、改进活动，以及质量修正监测活动确保工程质量目标的实现。

本要求项与 7.6 有关。保证可以认为是安全相关质量的特殊类型。

8.1.2 **监视所定义过程的一致性**

8.1.2.1 确保项目是按照所定义的系统工程过程来执行的；应按相应的时间间隔来检查一致情况；应将与所定义的过程相偏离以及该偏离所带来的影响记录下来。

8.1.2.2 确保所定义的系统工程过程在系统生存周期中是稳定的。

8.1.3 **测量工作产品的质量**

8.1.3.1 应当运用所设计的测量工作产品的方法来评估工作产品是否能符合需求方或工程的要求；产品测量还有助于解决隔离系统开发过程中的问题。

8.1.3.2 根据工作产品的质量要求对工作产品的测量进行评价。

8.1.4 **测量过程质量**

对项目所使用的系统工程过程的质量进行测量。

8.1.5 **分析质量测量**

8.1.5.1 分析质量测量以对质量改进或操作改进方面提出相应的开发性建议。

8.1.5.2 绘制因果图。

8.1.6 **参与质量活动**

在确定和报告质量问题时，有关员工应参与其中。

8.1.7 **发起改进质量的活动**

应发起以质量问题或质量改进问题为主题的有关活动。

8.1.8 **检测修正行为要求**

8.1.8.1 建立一种或一套机制来检测过程或产品中修正行为的要求。

8.1.8.2 故障报告。

8.2 管理配置

8.2.1 基本要求

应维持系统中已确定的配置单元的数据和状况，并对系统及其配置单元的变化进行分析和控制；管理系统配置包括为开发者和需求方提供准确的当前配置数据和状况；该要求项对置于配置管理之下的所有工作产品都是适用的。

对一个系统(项目)而标识的配置单元级别的确定应当考虑 7.6 的保证目标所详细要求的级别。

管理配置提供了 7.6 的证据；选择的配置管理(CM)系统自身管理也应当通过 7.1 来管理。

配置管理功能应允许在生存周期的任一点上通过系统要求的层次来对配置进行跟踪，从而支持可追溯性；可追溯性作为要求项 8.2 中实施的一部分应建立起来。

8.2.2 建立配置管理方法

8.2.2.1 应有配置管理方法；

8.2.2.2 应将要求项 8.1 作为实现业务研究的指南。

8.2.2.3 配置管理过程的描述。

8.2.3 确定配置单元

8.2.3.1 确定构成基线的配置单元。

8.2.3.2 配置管理所选择的工作产品应基于所选配置管理策略建立的准则；配置单元应当在有利于开发者和需求方的层面之上进行选择，但不应将不合理的管理负担加在开发者的身上。

8.2.4 维护工作产品基线

维护工作产品基线库，建立和维护一个关于工作产品配置的信息库；维护配置数据，为审计跟踪提供在系统生存周期任一点上的原始资料。

8.2.5 控制变化

8.2.5.1 对已建立的配置项的变化进行控制，包括跟踪每个配置项的配置；如需要批准新的配置，应更新系统的基线。

8.2.5.2 应对工作产品的标识问题或改变工作产品的需求进行分析，以便确定此变化对工作产品、项目进度和费用，以及其他工作产品产生的影响。

8.2.6 沟通配置状况

在状况发生变化时，应将配置数据状况告诉相关的部门或人员。状况报告应当包含何时处理、已接受的配置单元变化和受变化影响的有关工作产品等信息；应为开发者、需求方和其他受影响的团体提供配置数据和状况的访问权利。

8.3 管理项目风险

8.3.1 基本要求

应标识、评估、监视和降低风险以使系统工程活动和全部技术活动均取得成功；这个要求项要持续整个工程生存周期。与 8.4 和 8.3 要求项相类似，本要求项的范围包括系统工程活动和全部技术项目活动。

“项目风险”指与项目成功完成有关的风险，与费用和进度有关的一系列问题。工程实施要求项列出“安全风险”活动，这些活动是用来确定是否可容忍残余安全脆弱性对运行的影响。

应当考虑到 7.7，以确保安全问题都已列出。

8.3.2 制定项目风险管理方法

8.3.2.1 为项目风险管理活动制定出一个计划，对于整个项目生存周期来说，该计划是标识、评估、降低和监视安全风险的基础。

8.3.2.2 本要求实施的目的是制定一个有效的计划以指导项目的风险管理活动；计划元素应当包括风险管理队伍成员的标识及其责任；应有用于标识和降低风险的常规风险管理活动、方法和工具列表以及风险降低活动的跟踪和控制方法；计划也应当为风险管理结果的评估提供帮助。

8.3.3 **标识项目风险**

8.3.3.1 通过检查项目目标(并考虑到选择和限制)确定可能出现哪些差错并以这两种方法来标识项目的风险。

8.3.3.2 有条理地审查项目目标、项目计划(包括活动或事件依赖性)以及系统需求,确定可能的困难区以及在这些区中会出现哪些差错;上述活动在要求项 8.5 中制定;建立关键的发展依赖性和提供跟踪和修正行为将在要求项 8.4 中完成。

8.3.4 **评估项目风险**

评估项目风险,确定风险发生的可能性与可能造成的后果。

8.3.5 **评审项目风险评估**

8.3.5.1 获得项目风险评估的正式认可。

8.3.5.2 评审项目风险评估的充分性,以确定是否需要修改或取消基于风险的承诺。

8.3.6 **执行项目风险降低活动**

8.3.6.1 实施项目风险降低活动。

8.3.6.2 可列出风险降低活动减少风险发生的可能性或减少风险发生时所造成损失程度的列表;对需要特别关注的风险,可以同时实施几种降低风险的活动。

8.3.7 **跟踪项目风险降低活动**

8.3.7.1 监视项目安全风险降低活动以确保得到预期结果。

8.3.7.2 定期检查已经有效实施的降低项目风险活动,测量结果并确定该活动是否成功。

8.4 **监视技术活动**

8.4.1 **基本要求**

应为实际进步和风险提供充分的可见性;可见性是在执行计划发生严重偏差时及时促进修正的行为。

“监视技术活动”将根据项目估计、承诺和计划的文档来指导、跟踪和评审项目的完成情况、结果和风险;一个计划的文档是用来作为跟踪活动和风险,交流情况和修改方案的基础。

类似于要求项 8.4,此要求项适用于项目技术性行为以及系统工程活动。

在开发和系统运行时,需要考虑到 7.8 和 7.1。

需要考虑到要求项 7.7 以确保安全问题都已经列出。

8.4.2 **指导技术活动**

8.4.2.1 根据技术性管理计划指导技术性活动。

8.4.2.2 贯彻落实在“计划技术活动”要求项中创建的技术管理计划;这一实施涉及到项目中所有工程活动的技术指导。

8.4.3 **跟踪项目资源**

8.4.3.1 根据技术性管理计划跟踪资源的实际利用情况。

8.4.3.2 提供在项目中资源使用的当前信息,在需要时及时调整活动和计划。

8.4.4 **跟踪技术参数**

8.4.4.1 根据已建立的技术性参数跟踪执行。

8.4.4.2 通过测量在技术管理计划中建立的技术性参数来跟踪项目和它的产品的实际执行;将测量结果与技术管理方案中建立的阈值进行比较,将问题通知给管理人员。

8.4.5 **评审项目执行**

8.4.5.1 根据技术性管理计划执行评审。

8.4.5.2 应定期对项目和其产品的执行情况进行评审,当超出正常技术参数的阈值时也要进行评审;评审技术执行的测量分析结果和技术执行的其他指标,批准修正行动计划。

8.4.6 **分析项目问题**

8.4.6.1 分析跟踪和评审技术性参数的结果，确定修正行动。

8.4.6.2 及时标识、分析和跟踪项目问题控制项目的执行。

8.4.7 **采取修正行动**

8.4.7.1 当实际结果偏离计划时或技术参数预示着将有问题时，应采取修正行动。

8.4.7.2 当修正行动批准后，通过再分配资源，改变方法和步骤或加强对原计划的支持来执行修正行动；当需要改变技术管理计划时，采用 8.5 以修改该计划。

8.5 **计划技术活动**

8.5.1 **基本要求**

应建立计划，这些计划能为在系统开发、制造、使用和配置过程中涉及到的技术性工作的进度、费用、控制、跟踪与商议的性质和范围提供基础；应将系统工程行为集成到整个项目的综合性技术计划中。

“计划技术活动”涉及对所要执行工作量的估算，从有相关的部门或人员中获得必要的承诺，并对要进行的工作计划进行定义。

特别是在执行 8.4.6 和 8.4.7 时应考虑到 7.7。

计划应从对要进行的工作范围的理解开始，然后定义项目的限制和约束、风险和目标；计划过程应包括估算工作产品的规格，估算所需资源，制定时间安排表，考虑风险和协商承诺等步骤。

8.5.2 **标识关键资源**

标识对项目技术上的成功起关键作用的资源。

8.5.3 **估计项目范围**

8.5.3.1 对影响项目的规模和技术可行性的因素进行估计。

8.5.3.2 应通过将系统分解成与其他项目相似的组成单元的办法来对项目范围和规模进行估计；对规模的估计可以调整为如复杂性差异或其他参数等因素。

8.5.3.3 历史原始资料可为初始规模估计提供最有用的信息。

8.5.4 **估算项目费用**

针对项目实施要求的所有技术资源建立费用估算。

8.5.5 **确定工程过程**

8.5.5.1 确定项目使用的技术过程。

8.5.5.2 在最高层的技术过程应遵循基于工程特征、组织特征和组织的标准过程的生存周期模型。

8.5.6 **确定技术活动**

8.5.6.1 为项目的整个生存周期确定技术活动。

8.5.6.2 参照组织的历史经验，从可适用的标准与业界最佳实践中选择项目和系统工程活动。

8.5.7 **定义项目界面**

定义支持与需求方和供应商进行有效交互作用的特定过程。

8.5.8 **开发项目进度表**

8.5.8.1 为项目的整个生存周期制定技术进度表。

8.5.8.2 项目进度表包括系统和组件的开发与采购，相关人员的培训以及工程所需支持环境的准备；进度表是基于可验证模型或已确定任务的数据，以及它们任务相互依赖性和采购项的可用性；进度表应当包括为已标识的风险留有余地；所有受影响的部门或个人应复审并提交该进度表。

8.5.9 **设立技术参数**

8.5.9.1 为项目和系统设立有阈值的技术参数。

8.5.9.2 设立可在工程整个生存周期中都需要跟踪的关键技术参数，这些参数作为进度指示，以便满足最后的技术目标；通过交互用户、用户需求、市场调查、原型、已标识项目风险或类似项目的历史经验来确定这些关键技术参数。每个可跟踪的技术参数应该有一个期望的校正阈值或公差；在项目进度表

中的重要时间点关键技术参数应进行事先估算。

8.5.10 开发技术管理计划

8.5.10.1 利用在计划活动中收集到的信息开发技术管理计划，这种计划可以作为跟踪项目和系统工程的基础。

8.5.10.2 制定并维护所有技术活动需要的内部、外部组织项目活动的完整计划。

8.5.11 评审并认可工程计划

8.5.11.1 与所有有关团体和个人一同评审技术管理计划并需得到团体认可。

8.5.11.2 应确保在整个工程中通过有影响的团体和个人，对过程、资源、进度表和信息需求有自上而下的共同理解。

9 安全工程管理分等级要求

9.1 第一级：用户自主保护级

9.1.1 工程目标和范围

目标：在这一级别，要求满足资格保证的基本要求项，应基本达到组织保证、工程实施和项目实施的基本要求项。此级别组织内的个人可标识出一个行动应被执行，并同意这个行动会在需要时执行。

范围：这个级别应该制定安全工程计划，明确计算机信息系统的安全目标和安全范围并经组织内或具有所有权单位的主管领导批准。

保证计算机信息系统安全保护等级达到 GB/T 20271—2006 中 6.1、GB/T 20269—2006 中 6.1 的要求。

9.1.2 资格保证要求

资格保证要求满足下列 2 个基本要求项：

a) 信息安全产品应具有在国内生产、经营、销售的许可证，并符合相应的等级(见 5.4)；

b) 系统应符合国家相关的法律、法规和政策(见 5.6)。

9.1.3 组织保证要求

组织保证过程中下列 6 个要求项的过程应完整、明确，应基本达到每个要求项的目标；此级别组织内的个人可标识出一个行动应被执行，并同意这个行动会在需要时执行。

a) 定义组织的系统工程过程(见 6.1)；

b) 改进组织的系统工程过程(见 6.2)；

c) 管理系列产品演化(见 6.3)；

d) 管理系统工程支持环境(见 6.4)；

e) 提供不断发展的技能和知识(见 6.5.1)；

f) 与供应商协调(见 6.6)。

9.1.4 工程实施要求

安全工程中 11 个要求项的过程完整、明确，应基本达到每个要求项的目标；组织内的个人可标识出一个行动应被执行，并同意这个行动会在需要时执行。

a) 管理安全控制(见 7.1)；

b) 评估影响(见 7.2)；

c) 评估安全风险(见 7.3)；

d) 评估威胁(见 7.4)；

e) 评估脆弱性(见 7.5)；

f) 建立保证论据(见 7.6)；

g) 协调安全(见 7.7)；

h) 监视安全态势(见 7.8)；

i) 提供安全输入(见 7.9);

j) 指定安全要求(见 7.10);

k) 验证和确认安全性(见 7.11)。

9.1.5 项目实施要求

安全项目过程中下列 5 个要求项的过程完整、明确,应基本达到每个要求项的目标;组织内的个人可标识出一个行动应被执行,并同意这个行动会在需要时执行。

a) 质量保证(见 8.1);

b) 管理配置(见 8.2);

c) 管理项目风险(见 8.3);

d) 监视技术活动(见 8.4);

e) 计划技术活动(见 8.5)。

9.2 第二级:系统审计保护级

9.2.1 工程目标和范围

目标:在这一级别,资格保证要求满足,组织保证、工程实施和项目实施的基本要求项是经过计划并被跟踪。

范围:应验证特定步骤的执行工作产品应符合指定的标准和需求;测量用于跟踪要求项的执行情况;组织能够基于实际执行活动进行管理;本级别除去对基本要求项的要求外,还对要求项中的要求子项提出了特别要求;

保证计算机信息系统安全保护等级达到 GB/T 20271—2006 中 6.2、GB/T 20269—2006 中 6.2 的要求。

9.2.2 资格保证要求

资格保证要求满足下列 5 个要求项:

a) 国家主管部门认可的集成资质(见 5.1);

b) 国家主管部门认可的服务人员资质(见 5.2);

c) 国家主管部门认可的服务单位资质(见 5.3);

d) 信息安全产品应具有在国内生产、经营、销售的许可证,并符合相应的等级(见 5.4);

e) 系统符合国家相关的法律、法规和政策(见 5.6)。

9.2.3 组织保证要求

组织保证基本要求项应经计划并被跟踪。应验证特定步骤的执行;测量用于跟踪要求项的执行情况;工作产品应符合指定的标准和需求;组织能够基于实际执行活动进行管理。本级别对组织保证要求中 6 个要求项除需要过程完整、明确,完全达到每个要求项的要求外,还对下列要求项中的要求子项提出了特别要求。

a) 定义剪裁指南(见 6.1.5);

b) 评定过程(见 6.2.2);

c) 监视系统工程支持环境(见 6.4.8);

d) 确定培训要求(见 6.5.2);

e) 评估培训的有效性(见 6.5.7);

f) 维护培训材料(见 6.5.9);

g) 确定系统的组件或服务(见 6.6.2);

h) 选择供应商或销售商(见 6.6.4);

i) 提出要求(见 6.6.5)。

9.2.4 工程实施要求

工程实施基本要求项须经计划并被跟踪。应验证特定步骤的执行,测量用于跟踪要求项的执行情

况，工作产品应符合指定的标准和需求，工程实施能够基于实际执行活动进行管理。本级别对安全工程实施中11个要求项除需要过程完整、明确，完全达到每个要求项的要求外，还对下列要求项中的要求子项提出了特别要求。

a） 管理安全服务及控制机制（见7.1.5）；
b） 监视影响（见7.2.7）；
c） 监视安全风险及其特征（见7.3.7）；
d） 监视威胁及其特征（见7.4.7）；
e） 监视脆弱性及其特征（见7.5.6）；
f） 控制保证证据（见7.6.4）；
g） 提供保证论据（见7.6.6）；
h） 分析事件记录（见7.8.2）；
i） 监视变化（见7.8.3）；
j） 监视安全防护措施（见7.8.5）；
k） 检查安全态势（见7.8.6）；
l） 管理安全突发事件响应（见7.8.7）；
m） 保护安全监视的记录数据（见7.8.8）；
n） 标识安全选项（见7.9.4）；
o） 标识可用的法律、策略和约束（见7.10.3）；
p） 定义安全相关需求（见7.10.7）；
q） 确定验证和确认的目标（见7.11.2）；
r） 定义验证和确认方法（见7.11.3）；
s） 执行验证（见7.11.4）；
t） 执行证实（见7.11.5）；
u） 提供验证和确认的结果（见7.11.6）。

9.2.5 项目实施要求

项目实施基本要求项须经计划并被跟踪。应验证特定步骤的执行，测量用于跟踪要求项的执行情况，工作产品应符合指定的标准和需求，项目实施能够基于实际执行活动进行管理。本级别对安全项目实施中5个要求项除需要过程完整、明确，完全达到每个要求项的要求外，还对下列要求项中的要求子项提出了特别要求。

a） 监视所定义过程的一致性（见8.1.2）；
b） 测量工作产品的质量（见8.1.3）；
c） 测量过程质量（见8.1.4）；
d） 分析质量测量（见8.1.5）；
e） 检测修正行为要求（见8.1.8）；
f） 标识项目风险（见8.3.3）；
g） 评估项目风险（见8.3.4）；
h） 评审项目风险评估（见8.3.5）；
i） 执行项目风险降低活动（见8.3.6）；
j） 跟踪项目风险降低活动（见8.3.7）；
k） 跟踪项目资源（见8.4.3）；
l） 跟踪技术参数（见8.4.4）；
m） 评审项目执行（见8.4.5）；
n） 采取修正行动（见8.4.7）；

o) 设立技术参数(见 8.5.9);

p) 评审并认可工程计划(见 8.5.11)。

9.3 第三级:安全标记保护级

9.3.1 工程目标和范围

目标:在这一级别,要求满足资格保证要求;组织保证、工程实施和项目实施按照充分定义的过程执行(充分定义的过程是依据对文档化的标准过程进行裁剪并经批准的过程)。

范围:本级别利用组织范围内的过程标准来管理和规划,在实现第二级工程管理目标的基础上,要求对需求方、系统资源和工程过程进行规范记录,对要求和文档清单建立健全的一系列安全管理制度,实现制度化管理。

保证计算机信息系统安全保护等级达到 GB/T 20271—2006 中 6.3、GB/T 20269—2006 中 6.3 的要求。

9.3.2 资格保证要求

满足下列资格清单要求子项的目标:

a) 国家主管部门认可的集成资质(见 5.1);

b) 国家主管部门认可的服务人员资质(见 5.2);

c) 国家主管部门认可的服务单位资质(见 5.3);

d) 信息安全产品应具有在国内生产、经营、销售的许可证,并符合相应的等级(见 5.4);

e) 应具备信息安全系统建设工程实施监理管理制度(见 5.5.1);

f) 系统聘请专业监理公司,且监理公司具有国家主管部门认可监理资质证书(见 5.5.2);

g) 系统符合国家相关的法律、法规和政策(见 5.6)。

9.3.3 组织保证要求

在这一级别,组织保证按照充分定义的过程执行,充分定义的过程是依据对文档化的标准过程进行裁剪并经批准的过程版本;本级别利用组织范围内的过程标准来管理和规划,在实现第二级工程管理目标的基础上,要求实现制度化管理。

除满足二级组织保证要求项外还应满足下列要求子项的目标并规范化、制度化管理:

a) 收集过程资产(见 6.1.3);

b) 开发组织的系统工程过程(见 6.1.4);

c) 沟通过程改进(见 6.2.5);

d) 确保关键组件的可用性(见 6.3.5);

e) 插入产品技术(见 6.3.6);

f) 维持技术认识(见 6.4.2);

g) 确定支持需求(见 6.4.3);

h) 确保技能和知识的可用性(见 6.5.4);

i) 准备培训材料(见 6.5.5);

j) 培训人员(见 6.5.6);

k) 维护培训记录(见 6.5.8);

l) 确定胜任的供应商或销售商(见 6.6.3);

m) 维持沟通(见 6.6.6)。

9.3.4 工程实施要求

在这一级别,工程实施按照充分定义的过程执行,充分定义的过程是依据对文档化的标准过程进行裁剪并经批准的过程;利用组织范围内的过程标准来管理和规划,在达到第二级工程管理目标的基础上,要求对需求方、系统资源和工程过程进行规范记录,建立健全一系列的安全管理制度,实现制度化管理。除满足二级所有要求项和要求子项外,还应满足下列子项的要求并实现规范化、制度化管理:

a) 建立安全职责(见 7.1.2);
b) 管理安全配置(见 7.1.3);
c) 管理安全意识、培训和教育大纲(见 7.1.4);
d) 对影响进行优先级排列(见 7.2.2);
e) 标识系统资产(见 7.2.3);
f) 选择影响的度量(见 7.2.4);
g) 标识度量关系(见 7.2.5);
h) 标识和特征化影响(见 7.2.6);
i) 标识安全风险(见 7.3.3);
j) 评估安全风险(见 7.3.4);
k) 评估总体不确定性(见 7.3.5);
l) 标识自然威胁(见 7.4.2);
m) 标识人为威胁(见 7.4.3);
n) 标识威胁的测量尺度(见 7.4.4);
o) 评估威胁影响的效果(见 7.4.5);
p) 评估威胁的可能性(见 7.4.6);
q) 标识脆弱性(见 7.5.3);
r) 收集脆弱性数据(见 7.5.4);
s) 促进协调(见 7.7.4);
t) 分析工程选项的安全性(见 7.9.5);
u) 提供安全工程指南(见 7.9.6);
v) 标识系统安全关联性(见 7.10.4)。

9.3.5 项目实施要求

在这一级别,项目实施按照充分定义的过程执行,充分定义的过程是依据对文档化的标准过程进行裁剪并经批准的过程;本级别利用组织范围内的过程标准来管理和规划,在实现第二级项目管理目标的基础上,要求对需求方、系统资源和工程过程进行规范记录,建立健全一系列的安全管理制度,实现制度化管理。除满足二级所有要求项外,还应满足下列要求子项的要求并规范化、制度化管理:

a) 发起改进质量的活动(见 8.1.7);
b) 确定配置单元(见 8.2.3);
c) 控制变化(见 8.2.5);
d) 沟通配置状况(见 8.2.6);
e) 分析项目问题(见 8.4.6);
f) 标识关键资源(见 8.5.2);
g) 估计项目范围(见 8.5.3);
h) 开发项目进度表(见 8.5.8);
i) 开发技术管理计划(见 8.5.10)。

9.4 第四级:结构化保护级

9.4.1 工程目标和范围

目标:在这一级别,要求满足更高一级的资格保证要求;通过有效的控制手段将安全工程过程、安全项目过程和组织保证过程的有效性程序化、周期化。

范围:在达到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能够使用有效的控制手段对各项要求和文档清单进行管理。

保证计算机信息系统安全保护等级达到 GB/T 20271—2006 中 6.4、GB/T 20269—2006 中 6.4 的要求。

9.4.2 资格保证要求

满足下列要求子项的资格目标要求：

a) 国家主管部门认可的集成资质(见 5.1)；

b) 国家主管部门认可的服务人员资质(见 5.2)；

c) 国家主管部门认可的服务单位资质(见 5.3)；

d) 信息安全产品应具有在国内生产、经营、销售的许可证,并符合相应的等级(见 5.4)；

e) 应具备信息安全系统建设工程实施监理管理制度(见 5.5.1)；

f) 系统聘请专业监理公司,且监理公司具有国家主管部门认可监理资质证书(见 5.5.2)；

g) 系统符合国家相关的法律、法规和政策(见 5.6)。

9.4.3 组织保证要求

在文档清单要求中除了满足第三级要求外,还应满足下列文档清单的要求,且所有文档清单的描述应完整、全面,文档化管理应能够与日常运行和历史资料进行对比,能够使用有效的控制手段对要求和文档清单进行过程管理。

a) 制定过程目标(见 6.1.2)；

b) 改变标准过程(见 6.2.4)；

c) 获得系统工程支持环境(见 6.4.4)；

d) 维护环境(见 6.4.7)；

e) 选择知识或技能的获取模式(见 6.5.3)。

9.4.4 工程实施要求

安全工程中 11 个要求项的过程完整、明确,完全达到每个要求项的目标、概述要求,所有要求子项提供的证据材料应完整、全面,文档化管理应能够与日常运行和历史资料进行对比,能使用有效的控制手段对要求和要求子项进行过程管理。

a) 标识安全风险(见 7.3.3)；

b) 安全风险优先级排列(见 7.3.6)；

c) 选择脆弱性分析方法(见 7.5.2)；

d) 综合系统脆弱性(见 7.5.5)；

e) 标识保证目标(见 7.6.2)；

f) 控制保证证据(见 7.6.4)；

g) 定义协调目标(见 7.7.2)；

h) 促进协调(见 7.7.4)；

i) 理解安全输入要求(见 7.9.2)；

j) 提供安全工程指南(见 7.9.6)；

k) 标识系统安全关联性(见 7.10.4)；

l) 获取系统运行的安全思想(见 7.10.5)；

m) 定义安全相关需求(见 7.10.7)；

n) 提供验证和确认的结果(见 7.11.6)。

9.4.5 项目实施要求

项目过程中 5 个要求项的过程完整、明确,除完全达到每个要求项的所有要求外,所有要求子项提供的证据材料应完整、全面,文档化管理应能够与日常运行和历史资料进行对比,能使用有效的控制手段对要求和要求子项进行过程管理。

a) 参与质量活动(见 8.1.6)；

b) 建立配置管理方法(见 8.2.2)；

c) 维护工作产品基线(见 8.2.4)；

d) 制定项目风险管理方法(见 8.3.2);
e) 指导技术活动(见 8.4.2);
f) 估算项目费用(见 8.5.4);
g) 确定工程过程(见 8.5.5);
h) 确定技术活动(见 8.5.6);
i) 定义项目界面(见 8.5.7)。

9.5 第五级:访问验证保护级

9.5.1 工程目标和范围

目标:在这一级别应基于组织的目标针对过程有效性和效率建立量化执行指标,通过已定义过程和新概念、新技术的量化反馈来保证对实现这些目标的过程进行连续改进。

范围:除满足第四级的要求外,组织的全面安全计划应成为组织文化的有机组成部分,保证具有持续完善的工程过程管理、项目过程管理和组织保证管理,并对计算机信息系统安全实施全面的质量管理,能够利用历史资料和使用模型对工程进行优化。

保证计算机信息系统安全保护等级达到 GB/T 20271—2006 中 6.5、GB/T 20269—2006 中 6.5 的要求。

9.5.2 资格保证要求

满足下列关键资格保证要求子项的目标:

a) 国家主管部门认可的集成资质(见 5.1);
b) 国家主管部门认可的服务人员资质(见 5.2);
c) 国家主管部门认可的服务单位资质(见 5.3);
d) 信息安全产品应具有在国内生产、经营、销售的许可证,并符合相应的等级(见 5.4);
e) 应具备信息安全系统建设工程实施监理管理制度(见 5.5.1);
f) 系统聘请专业监理公司,且监理公司具有国家主管部门认可监理资质证书(见 5.5.2);
g) 系统符合国家相关的法律、法规和政策(见 5.6)。

9.5.3 组织保证要求

在这个级别上,应基于组织的目标针对过程有效性和效率建立量化执行目标;通过执行已定义过程新概念、新技术的量化反馈来保证对实现这些目标的过程进行连续改进;除满足第四级的要求外,还应要求组织的全面安全计划成为组织文化的有机组成部分;保证具有持续完善的组织保证管理,并对计算机信息系统安全实施全面的质量管理;安全组织保证过程中 6 个要求项的过程应完整、明确,除完全达到每个要求项的所有要求外,所有要求项中的要求子项应完整并满足要求,也就是在满足第四级的组织保证基础上,还应满足下列要求子项的要求并且能与历史资料进行对比,利用模型进行优化:

a) 规划过程改进(见 6.2.3);
b) 定义产品演化(见 6.3.2);
c) 标识新生产技术(见 6.3.3);
d) 适应开发过程(见 6.3.4);
e) 剪裁系统工程支持环境(见 6.4.5);
f) 插入新技术(见 6.4.6)。

9.5.4 工程实施要求

在这个级别上,应基于组织的目标针对过程有效性和效率建立量化执行目标;通过执行已定义过程和新概念、新技术的量化反馈来保证对实现这些目标的过程进行连续改进;除满足第四级的要求外,要求组织的全面安全计划应成为组织文化的有机组成部分;保证具有持续完善的工程实施管理,并对计算机信息系统安全实施全面的质量管理;工程实施要求中 11 个要求项的过程应完整、明确,要完全达到每个要求项的所有要求,所有要求项中的要求子项也应完整并满足要求,要求项和要求子项能够根据组织

的特点进行添加与升级，并且能与历史资料进行对比，利用模型进行优化。

9.5.5 项目实施要求

在这个级别上，应基于组织的应用目标针对过程有效性和效率建立量化执行目标；通过执行已定义过程和有创建的新概念、新技术的量化反馈来保证对这些目标进行连续过程改进；除满足第四级的要求外，要求组织的全面安全计划成为组织文化的有机组成部分；保证具有持续完善的项目过程管理，并对计算机信息系统安全实施全面的质量管理保证体系；项目实施要求中5个要求项的过程应完整、明确，除完全达到每个要求项的所有要求外，所有要求项中的要求子项应完整并满足要求；要求项和要求子项能够根据组织的特点进行添加与升级，以及能与历史资料进行对比，利用模型对资料进行优化。

9.6 安全保护等级划分与安全工程要求对照表

按GB 17859—1999所描述的每一个安全保护级对安全工程的不同要求，可以得到每个安全保护级的资格保证要求、组织保证要求、工程实施要求、项目实施要求的表，详见附录A的表A.1。

10 安全工程流程与安全工程要求

10.1 安全工程流程

信息系统安全工程的全部流程可被划分为5个阶段，即：起始、设计、建设、运行和维护、废弃。安全保护的各级安全工程要求体现在安全过程的部分或全部阶段中。需求方可以选择某些关键节点对安全工程要求实现与否进行审核，这些审核的结果一般会对整个安全工程的品质产生较为重要的影响。审核通常可以安排在设计阶段末，以及建设阶段的验收期。

10.1.1 起始阶段

10.1.1.1 中长期规划

信息系统的需求方应根据市场要求，结合自身的应用目标、需求程度以及建设规划的具体要求，以市场发展总体规划为主要依据，编制信息系统安全工程的中长期规划。

中长期规划应作为具体建设项目立项的主要依据。

中长期规划应指出信息系统建设中安全工程所要具备的能力。规划可以由投资者选定开发者或委托专家协助完成，并需经过专家组认证，以确保其适合市场和技术的发展，并与需求方的切实需要相符合。

10.1.1.2 项目立项

需求方应根据系统构建情况，对信息系统安全风险进行分析，得出清晰明确的安全需求。需求方应根据安全需求，结合工程建设总投资和资金来源、质量、人力资源和对业务成功起重要作用的问题的考虑，经过可行性研究之后，向主管部门或者投资者申报信息系统安全工程的立项。

投资者可委托专家组对项目立项报告进行评审。

立项项目应作为将来系统建设流程生成的要求文档和规范的出发点。

在本阶段需要考虑的其他问题还包括安全政策法规限制、确定工程实施者、安全问题解决的进度等。

10.1.1.3 方案的初步确立

在方案的初步确立中，需求方应该确定安全保证目标，并为所有保证目标定义一个安全保证策略；识别并控制安全保证证据和对安全保证证据进行分析；确定的草案必须能提供证明顾客安全需求得到满足的安全保证性论据。

具体操作上，投资方可利用招投标的形式，借助应标者和开发者的方案，来丰富备选方案，进而初步确定建设方案。

初步方案应调研与系统工程有关的所有问题，如系统开发、生产、运行、支持、认证，如果有问题间的冲突，都需要解决。

在方案初步确立后，投资者应基本选定开发者，并得到初步的系统技术、成本、风险方面的情况以及

系统获取和工程管理战略。

10.1.1.4 需求分析

在需求分析中，各方应进一步发展上一阶段得出的系统需求和概念，总结出一份正式的系统需求报告，为系统的设计和测试做好准备。该报告应包括系统所有的需求指标，包括针对信息系统的风险威胁进行相应的安全防护措施需求列表。

风险分析是确定信息系统具体安全需求的重要手段，在需求分析中应突出对信息系统的安全风险评估。

需求分析应由需求方和开发者共同完成，各方应就系统的安全要求形成一致的理解，对系统需求达到共识。需求分析通常在信息系统建设中出现，也有可能在重大的系统修改中出现。

需求分析中应周全地考虑法律、策略、标准、外部影响和约束的因素，识别系统的用途以确定其安全的关联性，明确系统运行的面向安全的总体指导思想，获取安全的高层目标定义和与系统安全相关的需求，并保证需求的完备性和一致性，最终达成满足顾客要求的安全协议。

需求分析中，各方应对所选中的系统方案继续论证，得到更为具体的系统建设方案。系统工程有关的所有问题都应考虑到，且各问题间的关系也应理顺。

需求分析应完成一份功能需求草案。草案应得到各方初步认可，应对系统的功能、性能、互操作性、接口要求作出描述，还应给出系统是否达到这些要求的检验手段。应建立起需求管理机制，以处理未来的要求，并对相关设计和测试资料进行确认。

10.1.2 设计阶段

在设计阶段中，应针对本信息系统的安全需求设计安全防护解决方案，建立全新信息系统安全机制。本阶段的目的是：完成系统的顶层设计、初步设计和详细设计，决定组成系统的配置项，定下系统指标。本阶段应由开发者委托设计者，或由开发者自己完成。设计方案应经过投资方以及专家组的评审。

设计方案应能深刻理解网络现状并能提供直接的解决方案，应从技术和管理两个方面进行考虑，应是管理制度和网络解决方案的结合。按照业务系统构建和信息流动的特点，可从五个层次对信息系统进行安全工程设计：物理安全、网络安全、系统安全、应用安全和管理安全。

设计者、开发者和需求方应一起确保相应部门对安全输入有一个共同的理解，做出有科学依据的工程决策所需的所有安全约束和考虑，标识出与安全相关的工程问题替换解决方法，利用安全约束和考虑因素对工程的比较方案进行分析并区分优先级，并提供安全工程指南和安全运行指南供建设及其后阶段其他工程组参考。

本阶段的任务还包括挑选合适的供货商。首先，需求方和设计者应先确定应由其他外部组织提供的系统组件或服务；然后标识在特定领域中具有专门技术的供应商，在考虑供应商的能力时应该包括具备资质条件、胜任开发过程、制造过程、验证责任、及时交付、生命期支持过程，以及远程有效通信能力，上述能力应符合本组织的各项要求；最后以合乎逻辑和公平的方式选择供应商以满足产品的目标。

面对众多的硬件商、系统软件商、数据库厂商、应用软件商，其产品和服务的开放性、兼容性、可扩展性和可维护性是考察的一个重要标准。安全产品和供应商的正确选择需要考虑技术方案的正常实施，安全功能的正确实现，安全目标的如期达到。在安全产品选择和采购等方面要采取资质保证的方法，选择时要求其产品必须符合国家各方面的相关规定，拥有相应的证书。同时安全产品的后期服务与升级也应是考虑安全产品的一个重要因素。

在此阶段，需求方还应清楚地指明它的要求和期望并排出优先顺序，并应指明对供应商方面的所有限制，使供应商充分了解产品需达到的要求和它要承担的责任。在工程的进展中，需求方和开发者还应保持与供应商维持及时的双向沟通。

10.1.3 建设阶段

10.1.3.1 工程建设和系统开发

在本阶段中，应根据详细设计方案对信息系统进行工程建设实施和系统开发。

在开始工程实施前后，实施方应向需求方提交相应文档资料，直到工程移交。这些文档主要包括：工程实施计划、工程进度安排、工程进展状况、工程问题报告、工程解决方案等工程资料。

工程应该按详细设计进行建设。在建设期间，应确保项目是按照所定义的系统工程过程来执行的；应按适当的时间间隔来检查一致情况；应将与所定义的过程相偏离以及该偏离所带来的影响记录下来；确保所定义的系统工程过程在系统生命期中是稳定的。如果工程的实际建设与原详细设计有差别或变更的，应提交实施方通过，如遇重大改动，还应提请专家组重新审议，并经通过后方可进行。

10.1.3.2 测试

信息系统安全工程在建设中和建成之后都应通过各种相关测试和质量测量。

a） 建设中的测试

系统工程建设中，实施者应对工程进展中安装的设备或产品“边建设边测试”，以评估产品是否能符合需求方或工程的要求；项目所使用的系统工程过程的质量同样也应进行测量。测试和测量的内容应作详细的工作文档记录，这些文档包括工程测试方法、测试结果、测试指标结果等。

应对产品、过程和项目执行所获得的测试和测量数据进行仔细检查进而找到问题的原因，并将这些信息用于改进产品和过程的质量；应分析质量测量结果，以对质量改进或操作改进方面提出适当的开发性建议；在确定和报告质量问题时应得到所有相关人员的参与，发起指出已确定的质量问题或质量改进机会的有关活动，并建立一种或一套机制来检测过程或产品中的修正行为。产品测试过程可由供货商和承建者共同完成，对于产品质量上的问题，应由承建者和设备销售人员双方全面负责，及时加以解决。

b） 移交测试

在系统建设完成之后，在开通和交付需求方验收、使用之前，应进行总体测试。

承建者应作好各项准备工作，包括用户设置、网络配置、操作注意事项等；需求方则应提供行政上的支持，包括召集相关单位技术人员配合工作，传输通道管理技术人员协同实施问题。

在移交测试中，应由开发者和承建者共同拟定测试内容、测试指标、测试结果说明、测试仪器及方法等内容，并报告给需求方和投资者审查通过。

移交测试的结果应经过需求方审查，若其中有未达到要求之项目，应按相关合同条款检查，按双方商定的结果执行下一步解决办法。

c） 试运转测试

试运转测试期间，承建者应观察记录产品的各项功能实施情况，并主要对以下问题进行测试及观察，包括：

1） 交换机等核心设备各项功能在运转时情况；

2） 服务器各项功能在运转时状况；

3） 对各终端运行情况记录，了解各终端在使用时，是否有障碍及发生的概率。

10.1.3.3 验收

系统验收前应先进行系统的测试和试运行，并且有详细的文档记录。

验收应该根据详细设计书及相关部门颁发的有关文件、各专业的设计规范、建设规范和验收规范。

信息系统安全工程的验收应在主管部门的主持下，按照以下程序完成：

a） 需求方向相应的主管部门提出验收申请；

b） 主管部门委托国家授权的信息安全测评机构对申请验收的信息系统实施系统安全性测评并提出测评结论；

c） 在主管部门主持下，召开系统验收会议，参加单位一般包括需求方、投资者、承建者、安全工程监理方等。

在工程验收中，还应确保解决安全问题的办法已被验证与证实。首先应确定验证和证实的目标并确定解决办法；定义验证和证实每种解决方案的方法和严密等级；验证解决办法实现了与上一抽象层相关的要求；最后执行验证并提供验证和证实的结果。

10.1.4 运行和维护阶段

在运行和维护阶段，信息系统开始投入使用，直到信息系统被最终废弃。

在本阶段中，应保持安全工程照常发挥作用，确保系统安全得到维护，包括处理系统在现场运行时的安全问题，以及采取措施保证系统的安全水平在系统运行期间不会下降。

转入运行和维护阶段的系统应在安全运行维护、安全管理执行、应急响应体系、专业安全服务等主要方面保证信息系统的安全功能正确实现。

建立配置的管理方法是安全运行维护的主要内容。首先应确定构成基线的配置单元，并建立和维护一个关于工作产品配置的信息库，对已建立的配置项的变化进行控制，包括跟踪每个配置项的配置（如需要批准新的配置，应更新系统的基线）；配置管理中应为开发者、需求方和其他受影响的团体提供配置数据和状况的访问权利，在状况发生变化时，应将配置数据状况告诉相关的部门或人员。

应通过预防措施和恢复控制相结合的方式，建立信息系统安全应急响应体系，使由意外事故（如：自然灾害、事故、设备故障和故意行为）引起的破坏减少至可接受的水平。

在安全服务方面，可考虑构建外部服务体系，由拥有国家相应安全服务资质的专业安全服务公司为需求方提供包括相关制度支撑体系、安全咨询服务体系、安全应急响应体系、安全培训体系等在内的一套专业的安全服务。

10.1.5 废弃阶段

计算机系统生命周期的废弃阶段涉及到信息、硬件和软件的处置。信息可转移到其他系统、存档、丢弃或销毁。当存档信息时应考虑未来取回信息的方法。用于创建记录的技术在未来可能无法随时获得。

硬件和软件可被出售，赠送或丢弃。除了一些包含保密信息的存储介质只有用销毁的方式清除以外，很少有硬件需要被销毁。如果有必要的话，软件的处置应遵循许可证和其他与开发商的协议。一些许可证是针对站点的或包含防止软件被转移的其他协议。也可能要采取措施对数据进行加密以便将来使用，如采取适当的步骤确保对密钥的长期和安全存储。

10.2 安全工程流程各阶段的安全工程要求

对安全保护等级划分的各项安全功能要求体现在安全工程各阶段的活动中。虽然安全工程要求和安全工程流程各阶段的活动并不存在严格的对应关系，但安全工程各个阶段确实有其需重点注意的安全工程要求。在全部安全工程要求中，组织保证要求和项目实施要求贯穿于项目实施的各个阶段，而资格保证要求和工程实施要求则与具体的一个或多个项目实施阶段有较强的联系，这种联系体现在附录A的表A.2中。

附 录 A
（资料性附录）
安全工程要求与安全保护等级、安全工程流程的对应关系

安全工程要求与安全保护等级的对应关系见表 A.1，安全工程要求与安全工程流程的对应关系见表 A.2。

表 A.1 安全工程要求与安全保护等级对应关系

安全工程要求	安全保护等级				
	第一级	第二级	第三级	第四级	第五级
资格保证要求					
5.1 系统集成资质要求					
国家主管部门认可的系统集成资质		√	√	√	√
5.2 人员资质要求					
国家主管部门认可的安全服务人员资质		√	√	√	√
5.3 第三方服务要求					
国家主管部门认可的服务单位资质		√	√	√	√
5.4 安全产品要求					
信息安全产品应具有在国内生产、经营、销售的许可证，并符合相应的等级		√	√	√	√
5.5 工程监理要求					
5.5.1 应具备信息安全系统建设工程实施监理管理制度		√	√	√	√
5.5.2 系统聘请专业监理公司，且监理公司具有国家主管部门认可监理资质证书			√	√	√
5.6 法律、法规、政策符合性要求					
系统应符合国家相关的法律、法规和政策	√	√	√	√	√
组织保证要求					
6.1 定义组织的系统工程过程					
6.1.1 基本要求	√	√	√	√	√
6.1.2 制定过程目标				√	√
6.1.3 收集过程资产			√	√	√
6.1.4 开发组织的系统工程过程			√	√	√
6.1.5 定义剪裁指南		√	√	√	√
6.2 改进组织的系统工程过程					
6.2.1 基本要求	√	√	√	√	√
6.2.2 评定过程		√	√	√	√
6.2.3 规划过程改进					√

表 A.1（续）

安全工程要求	安全保护等级				
	第一级	第二级	第三级	第四级	第五级
6.2.4 改变标准过程				√	√
6.2.5 沟通过程改进			√	√	√
6.3 管理系列产品演化					
6.3.1 基本要求	√	√	√	√	√
6.3.2 定义产品演化					√
6.3.3 标识新生产技术					√
6.3.4 适应开发过程					√
6.3.5 确保关键组件的可用性			√	√	√
6.3.6 插入产品技术			√	√	√
6.4 管理系统工程支持环境					
6.4.1 基本要求	√	√	√	√	√
6.4.2 维持技术认识			√	√	√
6.4.3 确定支持需求			√	√	√
6.4.4 获得系统工程支持环境				√	√
6.4.5 剪裁系统工程支持环境					√
6.4.6 插入新技术					√
6.4.7 维护环境				√	√
6.4.8 监视系统工程支持环境		√	√	√	√
6.5 培训					
6.5.1 基本要求	√	√	√	√	√
6.5.2 确定培训要求		√	√	√	√
6.5.3 选择知识或技能的获取模式				√	√
6.5.4 确保技能和知识的可用性			√	√	√
6.5.5 准备培训材料			√	√	√
6.5.6 培训人员			√	√	√
6.5.7 评估培训的有效性		√	√	√	√
6.5.8 维护培训记录			√	√	√
6.5.9 维护培训材料		√	√	√	√
6.6 与供应商协调					
6.6.1 基本要求	√	√	√	√	√
6.6.2 确定系统的组件或服务		√	√	√	√
6.6.3 确定胜任的供应商或销售商			√	√	√
6.6.4 选择供应商或销售商		√	√	√	√
6.6.5 提出要求		√	√	√	√

表 A.1（续）

安全工程要求	安全保护等级				
	第一级	第二级	第三级	第四级	第五级
6.6.6 维持沟通			√	√	√
工程实施要求					
7.1 管理安全控制					
7.1.1 基本要求	√	√	√	√	√
7.1.2 建立安全职责		√	√	√	√
7.1.3 管理安全配置			√	√	√
7.1.4 管理安全意识、培训和教育大纲			√	√	√
7.1.5 管理安全服务及控制机制			√	√	√
7.2 评估影响					
7.2.1 基本要求	√	√	√	√	√
7.2.2 对影响进行优先级排列		√	√	√	√
7.2.3 标识系统资产			√	√	√
7.2.4 选择影响的度量			√	√	√
7.2.5 标识度量关系			√	√	√
7.2.6 标识和特征化影响			√	√	√
7.2.7 监视影响			√	√	√
7.3 评估安全风险					
7.3.1 基本要求	√	√	√	√	√
7.3.2 选择风险分析方法		√	√	√	√
7.3.3 标识安全风险				√	√
7.3.4 评估安全风险			√	√	√
7.3.5 评估总体不确定性			√	√	√
7.3.6 安全风险优先级排列				√	√
7.3.7 监视安全风险及其特征		√	√	√	√
7.4 评估威胁					
7.4.1 基本要求	√	√	√	√	√
7.4.2 标识自然威胁			√	√	√
7.4.3 标识人为威胁			√	√	√
7.4.4 标识威胁的测量尺度			√	√	√
7.4.5 评估威胁影响的效果			√	√	√
7.4.6 评估威胁的可能性			√	√	√
7.4.7 监视威胁及其特征		√	√	√	√
7.5 评估脆弱性					
7.5.1 基本要求	√	√	√	√	√

表 A.1（续）

安全工程要求	安全保护等级				
	第一级	第二级	第三级	第四级	第五级
7.5.2 选择脆弱性分析方法				√	√
7.5.3 标识脆弱性			√	√	√
7.5.4 收集脆弱性数据			√	√	√
7.5.5 综合系统脆弱性				√	√
7.5.6 监视脆弱性及其特征		√	√	√	√
7.6 建立保证论据					
7.6.1 基本要求	√	√	√	√	√
7.6.2 标识保证目标				√	√
7.6.3 定义保证策略		√	√	√	√
7.6.4 控制保证证据				√	√
7.6.5 分析证据		√	√	√	√
7.6.6 提供保证论据		√	√	√	√
7.7 协调安全					
7.7.1 基本要求	√	√	√	√	√
7.7.2 定义协调目标				√	√
7.7.3 标识协调机制			√	√	√
7.7.4 促进协调				√	√
7.7.5 协调安全确定和建议		√	√	√	√
7.8 监视安全态势					
7.8.1 基本要求		√	√	√	√
7.8.2 分析事件记录			√	√	√
7.8.3 监视变化		√	√	√	√
7.8.4 标识安全突发事件		√	√	√	√
7.8.5 监视安全防护措施		√	√	√	√
7.8.6 检查安全态势		√	√	√	√
7.8.7 管理安全突发事件响应		√	√	√	√
7.8.8 保护安全监视的记录数据		√	√	√	√
7.9 提供安全输入					
7.9.1 基本要求	√	√	√	√	√
7.9.2 理解安全输入要求				√	√
7.9.3 确定安全约束和考虑因素		√	√	√	√
7.9.4 标识安全选项			√	√	√
7.9.5 分析工程选项的安全性			√	√	√
7.9.6 提供安全工程指南				√	√

表 A.1（续）

安全工程要求	安全保护等级				
	第一级	第二级	第三级	第四级	第五级
7.9.7 提供运行安全指南		√	√	√	√
7.10 指定安全要求					
7.10.1 基本要求	√	√	√	√	√
7.10.2 获得对安全要求的理解		√	√	√	√
7.10.3 标识可用的法律、策略和约束			√	√	√
7.10.4 标识系统安全关联性				√	√
7.10.5 获取系统运行的安全思想				√	√
7.10.6 获取安全的高层目标		√	√	√	√
7.10.7 定义安全相关需求				√	√
7.10.8 达成安全协议		√	√	√	√
7.11 验证和确认安全性					
7.11.1 基本要求	√	√	√	√	√
7.11.2 确定验证和确认的目标		√	√	√	√
7.11.3 定义验证和确认方法		√	√	√	√
7.11.4 执行验证		√	√	√	√
7.11.5 执行证实		√	√	√	√
7.11.6 提供验证和确认的结果				√	√
项目实施要求					
8.1 质量保证					
8.1.1 基本要求	√	√	√	√	√
8.1.2 监视所定义过程的一致性		√	√	√	√
8.1.3 测量工作产品的质量		√	√	√	√
8.1.4 测量过程质量		√	√	√	√
8.1.5 分析质量测量		√	√	√	√
8.1.6 参与质量活动				√	√
8.1.7 发起改进质量的活动			√	√	√
8.1.8 检测修正行为要求		√	√	√	√
8.2 管理配置					
8.2.1 基本要求	√	√	√	√	√
8.2.2 建立配置管理方法				√	√
8.2.3 确定配置单元			√	√	√
8.2.4 维护工作产品基线				√	√
8.2.5 控制变化			√	√	√
8.2.6 沟通配置状况			√	√	√

表 A.1（续）

安全工程要求	安全保护等级				
	第一级	第二级	第三级	第四级	第五级
8.3 管理项目风险					
8.3.1 基本要求	√	√	√	√	√
8.3.2 制定项目风险管理方法				√	√
8.3.3 标识项目风险		√	√	√	√
8.3.4 评估项目风险		√	√	√	√
8.3.5 评审项目风险评估		√	√	√	√
8.3.6 执行项目风险降低活动		√	√	√	√
8.3.7 跟踪项目风险降低活动		√	√	√	√
8.4 监视技术活动					
8.4.1 基本要求	√	√	√	√	√
8.4.2 指导技术活动				√	√
8.4.3 跟踪项目资源		√	√	√	√
8.4.4 跟踪技术参数		√	√	√	√
8.4.5 评审项目执行		√	√	√	√
8.4.6 分析项目问题			√	√	√
8.4.7 采取修正行动		√	√	√	√
8.5 计划技术活动					
8.5.1 基本要求	√	√	√	√	√
8.5.2 标识关键资源			√	√	√
8.5.3 估计项目范围			√	√	√
8.5.4 估算项目费用				√	√
8.5.5 确定工程过程				√	√
8.5.6 确定技术活动				√	√
8.5.7 定义项目界面				√	√
8.5.8 开发项目进度表			√	√	√
8.5.9 设立技术参数		√	√	√	√
8.5.10 开发技术管理计划			√	√	√
8.5.11 评审并认可工程计划		√	√	√	√
注：“√”表示具有该要求。					

表 A.2　安全工程要求与安全工程流程对应关系

安全工程要求	安全工程流程				
	起始	设计	建设	运行和维护	废弃
资格保证要求					
5.1　系统集成资质要求			√		
5.2　人员资质要求				√	
5.3　第三方服务要求				√	
5.4　安全产品要求		√	√		
5.5　工程监理要求	√				
5.6　法律、法规、政策符合性要求				√	
工程实施要求					
7.1　管理安全控制				√	√
7.2　评估影响	√			√	
7.3　评估安全风险	√			√	
7.4　评估威胁	√			√	
7.5　评估脆弱性	√			√	
7.6　建立保证论据	√	√	√	√	
7.7　协调安全	√	√	√	√	
7.8　监视安全态势				√	
7.9　提供安全输入	√	√		√	
7.10　指定安全要求	√				
7.11　验证和确认安全性	√		√		
注：“√”表示该组要求与该流程阶段相关。					

GB/T 20282—2006

参 考 文 献

[1] GB/T 18336—2001 信息技术 安全技术 信息技术安全性评估准则(idt ISO/IEC 15408:1999)

[2] GB/T 9387.2—1995 信息处理系统 开放系统互连 基本参考模型 第2部分:安全体系结构(idt ISO/IEC 7498-2:1989)

[3] GB/T 19716—2005 信息技术 信息安全管理实用规则(ISO/IEC 17799:2000,MOD)

[4] GB/T 20261—2006 信息技术 系统安全工程 能力成熟度模型(ISO/IEC 21827:2002,MOD)

GB/T 20282-2006

*

书号:155066·1-27972