ICS 35.040
L 80

中华人民共和国国家标准

GB/T 28453—2012

信息安全技术
信息系统安全管理评估要求

Information security technology—
Information system security management assessment requirements

2012-06-29 发布　　2012-10-01 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

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:北京江南天安科技有限公司。

本标准主要起草人:陈冠直、吉增瑞、陈硕、景乾元、王志强。

引　言

本标准依据国家有关信息安全等级保护的政策法规，提出了用于规范信息系统安全管理评估的要求。主要包括信息系统安全管理评估的原则和模式、组织和活动、方法工具和实施等要求，以及在信息系统生存周期各个阶段，针对第一级到第五级信息系统安全管理评估的要求。

信息系统安全管理评估的主体包括信息系统的主管领导部门、信息安全监管机构、信息系统的管理者、第三方评估机构等，对应的评估可以是检查评估、自评估或第三方评估。本标准中对三种评估模式提出共同要求时统称评估。信息系统安全管理评估以信息安全管理体系为主线进行评估，必要时采集信息安全技术测评结果进行综合分析。信息系统安全管理评估可以是独立的评估，也可以与信息安全技术测评联合进行综合评估。信息系统安全管理评估贯穿于信息系统的整个生存周期，各阶段管理评估的原则和方法是一致的，各阶段安全管理的内容、对象、安全需求存在一定不同，使得安全管理评估的目的、要求等各方面也有所不同。信息系统安全管理评估针对信息安全保护各个等级的信息系统，安全管理评估的要求随着保护等级的提高而增强。

本标准第 4 章阐述管理评估的原则和模式；第 5 章阐述管理评估的组织、评估目标范围和依据、管理活动的内容；第 6 章阐述管理评估方法、管理评估工具、管理评估实施，给出了各个安全保护等级的安全管理评估需要执行的共同要求和评估方法；第 7 章分等级评估，以 GB/T 20269—2006 规定的信息系统安全管理要求为基本依据，从信息系统生存周期的规划立项阶段、设计实施阶段、运行维护阶段、终止处置阶段，对五个安全保护等级的安全管理评估要求分别进行描述。附录 A 中提供的信息系统安全管理评估参照表，描述了本标准中有关各等级信息系统安全管理评估要求的具体评估内容要点。

本标准仍沿用 GB/T 20269—2006 中的称谓，对于信息系统的所有者可包括国家机关、事业单位、厂矿企业、公司、集团等各种类型和不同规模的组织机构，统称为“组织机构”。

信息安全技术
信息系统安全管理评估要求

1 范围

本标准依据GB/T 20269—2006规定的信息系统分等级安全管理要求，从信息系统生存周期的不同阶段，规定了对信息系统进行安全管理评估的原则和模式、组织和活动、方法和实施，提出了信息安全等级保护第一级到第五级的信息系统安全管理评估的要求。

本标准适用于相关组织机构（部门）对信息系统实施安全等级保护所进行的安全管理评估与自评估，以及评估者和被评估者对评估的管理。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

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 20282—2006 信息安全技术 信息系统安全工程管理要求

GB/T 25070—2010 信息安全技术 信息系统等级保护安全设计技术要求

3 术语和定义

GB 17859—1999、GB/T 20269—2006中界定的以及下列术语和定义适用于本文件。

3.1

安全评估 security assessment

依照国家有关法规与标准，对信息系统的安全保障程度进行评估的活动，包括安全技术评估和安全管理评估。本标准所述评估是指信息系统安全管理评估。

3.2

自评估 self-assessment

由信息系统所有者自身发起，组成组织机构内部的评估机构，依据国家有关法规与标准，对信息系统安全管理进行的评估活动。

3.3

检查评估 inspection assessment

由被评估信息系统所有者的上级主管部门、业务主管部门或国家相关监管部门发起的，依据国家有关法规与标准，对信息系统安全管理进行的评估活动。

3.4

第三方评估 third party assessment

由信息系统所有者委托商业评估机构或其他评估机构，依据国家有关法规与标准，对信息系统安全管理进行的评估活动。

3.5

安全审计　security audit

对信息系统的各种安全相关事件的行为，按规定进行信息收集、记录和分析，并采取相应动作的过程。

3.6

验证　verification

通过客观证据，对事务是否达到规定要求进行认定的过程，包括真实性验证和有效性验证。客观证据是指支持事务的真实性、有效性的数据，可通过观察、测量、试验或其他手段获得。

3.7

有效性　effectiveness

完成策划的活动并得到相应结果的程度的表征。

3.8

质量控制　quality assurance

质量管理的一部分，致力于满足质量要求。本标准中的质量控制是指对信息安全管理过程的各种行为质量的控制。

4　评估原则和模式

4.1　管理评估的原则

对信息系统安全管理的评估应坚持以下原则：

a）　科学性原则：按照科学的评估方法和过程，以严谨的科学态度，全面、准确、客观地开展评估工作，做出科学的评估结论；

b）　公正性原则：评估机构是中立权威的，自评估团队是相对独立的，检查评估机构是符合法规和组织原则的，同时要防止被评估对象的影响，并排除外界因素的干扰，从而确保评估结果是客观公正的；

c）　针对性原则：针对性地选用评估方法和评估工具；针对被评估信息系统安全管理的实际情况和特征，收集有关资料对系统进行全面地分析；针对主要管理环节及主要部位进行重点评估；

d）　实用性原则：系统分析和评价方法要适合被评估信息系统的实际情况，操作简单，结论明确，成效显著。

4.2　管理评估的工作模式

从评估主体的角度，信息系统安全管理评估可分为检查评估、自评估和第三方评估等工作模式，其适用范围包括：

a）　检查评估：

——是指由被评估信息系统所有者的上级主管部门、业务主管部门或国家相关监管部门发起的，依据国家有关法规与标准，对信息系统安全管理进行的评估活动；

——适用于上级主管机关、业务主管部门或国家相关监管部门，对其下属或监管范围内组织机构信息系统安全管理进行的检查性的评估活动；

b）　自评估：

——是指由信息系统所有者自身发起，组成组织机构内部的评估机构，依据国家有关法规与标准，对信息系统安全管理进行的评估活动；

——适用于组织机构对自身所拥有、运营或使用的信息系统安全管理进行的评估活动；

c）　第三方评估：

——是指由信息系统所有者委托商业评估机构或其他评估机构，依据国家有关法规与标准，对信息系统安全管理进行的评估活动；

——适用于组织机构委托商业评估机构或其他评估机构，对自身所拥有、运营或使用的信息系统安全管理进行的评估活动。

5 评估组织和活动

5.1 评估组织

5.1.1 评估实施团队

5.1.1.1 检查评估实施团队

检查评估实施团队组成的要求如下：

a) 检查评估实施团队由信息系统上级管理部门或国家有关职能部门委派；

b) 派出机构有关领导和相关部门负责人作为检查评估实施团队的领导；

c) 派出机构相关部门的信息技术、信息安全以及相关业务有经验的技术和管理人员参加；

d) 必要时，检查评估实施团队可聘请相关专业的技术专家和技术骨干组成专家小组。

5.1.1.2 自评估实施团队

组织机构对自身所拥有、运营或使用的信息系统安全管理进行的评估，自评估实施团队组成的要求如下：

a) 组织机构信息安全主管领导或信息安全领导小组应指派信息部门或业务部门负责人任自评估实施团队负责人；

b) 自评估实施团队负责人根据参与评估的范围确定评估组成员的数量，为自评估团队选择成员，并报请主管领导批准；

c) 自评估实施团队应由管理层、相关业务骨干、信息技术和信息安全人员、信息安全人员等组成，主要来自信息部门和业务部门，核心成员为3～5人；

d) 在评估过程中，自评估实施团队与被评估方应是相对独立地进行评估工作，被评估方不应干涉或干扰评估结论；

e) 必要时，可聘请相关专业的技术专家和技术骨干组成专家小组。

5.1.1.3 第三方评估实施团队

第三方评估实施团队组成的要求如下：

a) 第三方评估实施团队由受委托的安全评估服务技术支持方委派；

b) 受委托的安全评估服务技术支持方相关部门或项目主管任评估实施团队负责人；

c) 第三方评估实施团队由熟悉信息技术、信息安全技术、信息安全管理，熟悉委托方业务，具有相关资质的人员组成；

d) 对信息安全等级第三级及以上的信息系统进行评估的第三方评估实施团队，应符合国家职能部门有关评估机构选择的规定，可参见附录A的A.4.3。

5.1.2 评估管理机构

应针对不同模式的信息安全管理评估组建评估管理机构：

a) 评估工作组：检查评估时，接受检查的组织机构应组建由主管领导和相关部门负责人参加的评估工作组，配合检查评估团队的工作；

b) 自评估工作领导小组：组织机构信息安全主管领导或信息安全领导小组主管自评估工作，应组建由主管领导和相关部门负责人参加的自评估工作领导小组，指导和监督自评估团队的工作；

c) 评估工作领导小组：第三方评估时，应组建由评估方、被评估方领导及相关部门负责人参加的安全评估工作领导小组，指导和控制第三方评估团队的工作；安全评估工作领导小组中被评估方领导应负责监督或指派有关部门负责人监督第三方评估团队的工作。

5.1.3 被评估方相关人员

被评估方相关人员应包括：

a) 高级管理层：组织机构的领导、信息化主管领导、信息安全主管领导等；

b) 执行管理层：信息部门负责人、信息安全部门负责人、业务部门负责人、人事部门负责人等；

c) 信息技术和信息安全相关人员，包括：

——系统建设主管及系统设计、软件开发、系统集成人员；

——运行维护主管及网络系统、操作系统、数据库系统、应用系统、硬件设备等系统管理及运维人员；

——信息安全主管及安全管理、审计管理人员、文档介质管理人员；

——物理安全主管及资产管理、机房值守、机房维护人员；

——外包服务方主管及外包方运行、维护人员；

d) 业务应用人员，包括业务部门主管、业务应用系统管理人员[1]、业务应用系统开发人员和操作人员。

5.2 评估目标范围和依据

5.2.1 评估目标

5.2.1.1 具体评估目标

信息系统安全管理评估的一般目标是，识别信息系统安全管理存在的信息安全风险，并确定其大小，为制定信息安全方针，选择适当的控制目标与控制方式提供决策依据。每一次评估的具体目标可能会存在一定差异，应明确每一次评估的具体目标，可以是：

a) 针对规划立项阶段的安全管理评估，主要从策略和制度管理、机构和人员管理、风险管理、监督和检查管理、规划和立项管理等方面，评价信息系统的系统分析和安全定级、信息系统安全需求分析、信息系统总体安全规划、信息系统安全项目立项等关键环节的安全管理状况；

b) 针对信息系统设计实施阶段的安全管理评估，主要从策略和制度管理、机构和人员管理、风险管理、环境和资源管理、安全机制保障管理、业务连续性管理、监督和检查管理、建设过程管理等方面，评价信息系统的系统安全设计、系统采购控制、系统开发控制、管理措施制定、集成及配置管理、测试及验收管理等关键环节的安全管理状况；

c) 针对信息系统运行维护阶段的安全管理评估，主要从策略和制度管理、机构和人员管理、风险管理、环境和资源管理、日常运维管理、业务连续性管理、监督和检查管理等方面，评价信息系统的运行操作、系统维护、安全监控、业务连续性、变更控制、外包、安全检查、持续改进等关键环节的安全管理状况；

d) 针对信息系统终止处置阶段的安全管理评估，主要从策略和制度管理、机构和人员管理、风险

1) 应用系统管理人员主要负责应用系统用户账户、权限管理，以及应用系统其他日常运行维护；与一般信息技术人员不同，应用系统管理人员应熟悉应用系统所支持的业务流程和业务管理。

管理、环境和资源管理、监督和检查管理、终止处置过程管理等方面，评价信息系统的系统终止审批、信息转移及清除、设备迁移或废弃、存储介质清除或销毁等关键环节的安全管理状况。

也可以是针对系统故障或安全事件的评估、针对组织机构变动或系统变更的评估，或定期进行的信息系统安全管理评估。

5.2.1.2 具体评估目标的提出

不同评估工作模式的具体评估目标的提出，要求如下：

a) 检查评估的具体评估目标，由被评估信息系统所有者的上级主管部门、业务主管部门或国家相关监管部门（评估发起部门）提出；

b) 自评估的具体评估目标，由信息系统所属组织机构领导提出，可听取自评估实施团队的意见；

c) 第三方评估的具体评估目标，由信息系统所属单位（委托方）领导提出，受委托的第三方评估机构的实施团队应充分理解委托方提出的评估目标，必要时可提出建议。

5.2.2 评估范围

信息系统安全管理评估的一般评估范围，可以是与全部业务处理相关的信息系统，也可以是某个特定业务处理的信息系统。针对某一次评估，应根据具体评估目标，确定评估的具体范围，并形成相关文档。不同评估工作模式的具体评估范围的确定，要求如下：

a) 检查评估的具体评估范围，由被评估信息系统所有者的上级主管部门、业务主管部门或国家相关监管部门（评估发起单位）确定；

b) 自评估的具体评估范围，由信息系统所属组织机构的领导确定，可听取自评估实施团队的意见；

c) 第三方评估的具体评估范围，由信息系统所属组织机构（委托方）的领导确定，受委托的第三方评估机构的实施团队应充分理解委托方确定的评估范围，确认具体评估范围能够满足评估目标的要求，如不能满足应及时提出并与被评估方协商解决。

对于涉及国家秘密的信息和信息系统安全管理的评估，应按照国家有关保密管理、密码管理规定和相关测评标准执行。

5.2.3 评估依据

信息系统安全管理评估以 GB/T 20269—2006 的安全管理要求为主要依据，并参考业务应用对信息系统安全运行的需求，确定相关的判断依据，如：

a) 行业主管部门对信息系统的业务和安全要求；

b) 信息系统互联单位的业务和安全要求；

c) 信息系统本身的实时性或性能要求。

5.3 评估活动内容

5.3.1 评估准备及启动

5.3.1.1 评估准备

评估方应通过与被评估方评估管理机构沟通从以下方面开展评估准备工作：

a) 确定评估实施团队的成员及职责等；

b) 对评估实施团队的成员进行培训；

c) 获得被评估方高级管理层对评估的支持；

d) 确定评估的系统范围和管理界限；

e) 确定评估的具体判断依据(见 5.2.3);
f) 协商选择被评估方的参与人员;
g) 协调解决评估所需的后勤保障工作;
h) 协商确定评估工作计划和时间进度安排;
i) 取得以下阶段性成果及文档:
——被评估方高级管理层对评估工作支持的决议、批示或表态;
——评估实施团队成员名单;
——对评估实施团队的成员进行信息安全评估方法的培训;
——实施信息安全评估的工作范围;
——被评估方参与人员名单,包括涉及的高级管理层、执行管理层、信息技术和信息安全人员、业务应用人员等;
——评估的详细计划,包括工作内容、工作形式、工作成果等内容,以及实施的时间进度安排;
——参与人员应了解在评估工作中的岗位责任。

5.3.1.2 评估工作需获得的支持

通过评估准备应从以下方面获得对评估工作的支持:
a) 评估工作应得到被评估方最高管理者的批准同意;
b) 评估实施团队应将评估的过程、存在的风险、花费的时间和人员的使用情况等告知被评估方主管评估的领导;
c) 从以下方面得到被评估方主管评估的领导的明确支持:
——对评估工作持续支持的明确表示;
——明确激励员工参与的措施;
——完成所有评估工作需要的职责和授权;
——承诺提供评估所需的资源;
——参加评估结果和改进建议的审核。

5.3.1.3 评估启动

在评估准备工作完成的基础上,召开评估启动会,向与会被评估方领导及所有参与者进行工作简介,并宣布评估工作启动。

5.3.2 确定信息系统资产及安全需求

5.3.2.1 对高级管理层的访谈调查

对高级管理层有关信息系统资产及安全需求的访谈调查,要求做到:
a) 确定高级管理层识别的信息系统基本情况,信息系统资产及其优先顺序,记录在资产调查表(见 6.2.1.1);
b) 确定高级管理层认识到信息系统面临的威胁,对信息系统安全的关注范围,记录在关注范围调查表(见 6.2.1.2);
c) 确定高级管理层认为最关键资产及其管理的安全需求,记录在安全需求调查表(见 6.2.1.3);
d) 应取得以下阶段性成果及文档:
——按优先级排列的高级管理层识别的资产;
——高级管理层关注的范围;
——高级管理层认为最关键资产及其管理的安全需求;

——高级管理层的访谈记录。

5.3.2.2 对执行管理层的访谈调查

对执行管理层有关信息系统资产及安全需求的访谈调查，要求做到：

a) 确定执行管理层识别的信息系统基本情况，信息系统资产及其优先顺序，记录在资产调查表；

b) 确定执行管理层认识到信息系统面临的威胁，对信息系统安全的关注范围，记录在关注范围调查表；

c) 确定执行管理层认为最关键资产及其管理的安全需求，记录在安全需求调查表；

d) 应取得以下阶段性成果及文档：

——按优先级排列的执行管理层识别的资产；

——执行管理层关注的范围；

——执行管理层认为最关键资产及其管理的安全需求；

——执行管理层的访谈记录。

5.3.2.3 对信息技术和信息安全人员的访谈调查

对信息技术和信息安全人员有关信息系统资产及安全需求的访谈调查，要求做到：

a) 确定信息技术和信息安全人员识别的信息系统基本情况，信息系统资产及其优先顺序，记录在资产调查表；

b) 确定信息技术和信息安全人员认识到信息系统面临的威胁，对信息系统安全的关注范围，记录在关注范围调查表；

c) 确定信息技术和信息安全人员认为最关键资产及其管理的安全需求，记录在安全需求调查表；

d) 应取得以下阶段性成果及文档：

——按优先级排列的信息技术和信息安全人员识别的资产；

——信息技术和信息安全人员关注的范围；

——信息技术和信息安全人员认为最关键资产及其管理的安全需求；

——信息技术和信息安全人员的访谈记录。

5.3.2.4 对业务应用人员的访谈调查

对业务应用人员有关信息系统资产及安全需求的访谈调查，要求做到：

a) 确定业务应用人员识别的信息系统基本情况，信息系统资产及其优先顺序，记录在资产调查表；

b) 确定业务应用人员认识到信息系统面临的威胁，对信息系统安全的关注范围，记录在关注范围调查表；

c) 确定业务应用人员认为最关键资产及其管理的安全需求，记录在安全需求调查表；

d) 应取得以下阶段性成果及文档：

——按优先级排列的业务应用人员识别的资产；

——业务应用人员关注的范围；

——业务应用人员认为最关键资产及其管理的安全需求；

——业务应用人员的访谈记录。

5.3.2.5 对信息系统资产及安全需求的确定

对信息系统资产及安全需求的确定，要求做到：

a) 汇总归纳访谈调查得到的信息系统的基本描述、资产调查表、关注范围调查表和安全需求调

查表；

b) 按照支撑业务或岗位的重要程度为资产、安全需求、关注范围等分组；

c) 选择并确定信息系统关键资产及其管理的安全需求；

d) 标注信息系统资产表中的资产面临的威胁及关注范围；

e) 应取得以下阶段性成果及文档：

——信息系统的基本描述；

——资产、安全需求、关注范围分类；

——关键资产及其管理的安全需求；

——关键资产的关注范围。

5.3.2.6 对关键环节和核心部位的确定

根据信息系统资产及安全需求，对信息系统安全管理的关键环节和核心部位的确定，要求做到：

a) 确定待审核的信息系统安全策略和管理制度文档；

b) 确定待检查的信息系统物理环境和工作记录；

c) 确定待检测的信息系统核心部位及关键组件；

d) 确定待核查的信息系统安全管理关键环节；

e) 应取得以下阶段性成果及文档：

——信息系统安全策略和管理制度文档的范围和审核方法；

——信息系统物理环境及工作记录的范围和检查方法；

——信息系统核心部位及关键组件的范围和测评结果收集方法；

——信息系统安全管理关键环节的范围和核查方法。

5.3.3 确定信息系统安全管理现状

5.3.3.1 对高级管理层的访谈调查

使用相应的访谈问卷(见 6.2.2)，对高级管理层有关信息系统安全管理现状的访谈调查，应做到：

a) 确定高级管理层识别的信息系统安全策略及其优先顺序，与业务需求的一致性；

b) 确定高级管理层认为已实施的信息系统安全保护措施和管理制度以及执行情况，记录在保护措施调查表(见 6.2.1.4)；

c) 确定高级管理层认为信息系统安全管理机构和相关人员的职责要求以及执行情况；

d) 确定高级管理层对现行安全策略和安全管理存在不足的了解程度，包括发生过的安全事件；

e) 应取得以下阶段性成果及文档：

——按优先级排列的高级管理层认为的信息系统安全策略；

——高级管理层认为已实施的信息系统安全保护措施和管理制度以及执行情况；

——高级管理层认为信息系统安全管理机构和相关人员的职责要求以及执行情况；

——高级管理层对现行安全策略和安全管理存在不足的了解程度，以及与安全管理要求存在的差距，包括发生过的安全事件；

——高级管理层的访谈记录、保护措施调查表。

5.3.3.2 对执行管理层的访谈调查

使用相应的访谈问卷，对执行管理层有关信息系统安全管理现状的访谈调查，应做到：

a) 确定执行管理层认为的信息系统安全策略及其优先顺序，与业务需求的一致性；

b) 确定执行管理层认为已实施的信息系统安全保护措施和管理制度以及执行情况，记录在保护

措施调查表；

c) 确定执行管理层认为信息系统安全管理机构和相关人员的职责要求及其执行情况；

d) 确定执行管理层对信息系统规划立项、设计实施、运行维护、终止处置的安全管理要求和实践措施；

e) 确定执行管理层对现行安全策略和安全管理存在不足的了解程度，包括发生过的安全事件；

f) 应取得以下阶段性成果及文档：

——按优先级排列的执行管理层识别的信息系统安全策略；

——执行管理层认为已实施的信息系统安全保护措施和管理制度以及执行情况；

——执行管理层认为信息系统安全管理机构和相关人员的职责要求以及执行情况；

——执行管理层对信息系统规划立项、设计实施、运行维护、终止处置的安全管理要求和实践措施；

——执行管理层对现行安全策略和安全管理存在不足的了解程度，以及与安全管理要求存在的差距，包括发生过的安全事件；

——执行管理层的访谈记录、保护措施调查表。

5.3.3.3 对信息技术和信息安全人员的访谈调查

使用相应的访谈问卷，对信息技术人员和信息安全人员有关信息系统安全管理现状的访谈调查，应做到：

a) 确定信息技术和信息安全人员认为的信息系统安全策略及其优先顺序，与业务需求的一致性；

b) 确定信息技术和信息安全人员认为已实施的信息系统安全保护措施和管理制度以及执行情况，记录在保护措施调查表；

c) 确定信息技术和信息安全人员认为的信息系统安全管理机构和相关人员（包括被访谈人）的职责要求，以及执行情况；

d) 确定信息技术和信息安全人员认为的信息系统规划立项、设计实施、运行维护、终止处置的安全管理要求和实践措施；

e) 确定信息技术和信息安全人员对现行安全策略和安全管理存在不足的了解程度，包括发生过的安全事件；

f) 应取得以下阶段性成果及文档：

——按优先级排列的信息技术和信息安全人员识别的信息系统安全策略；

——信息技术和信息安全人员认为已实施的信息系统安全保护措施和管理制度以及执行情况；

——信息技术和信息安全人员认为信息系统安全管理机构和相关人员的职责要求以及执行情况；

——信息技术和信息安全人员对信息系统规划立项、设计实施、运行维护、终止处置的安全管理要求和实践措施；

——信息技术和信息安全人员对现行安全策略和安全管理存在不足的了解程度，以及与安全管理要求存在的差距，包括发生过的安全事件；

——信息技术和信息安全人员的访谈记录、保护措施调查表。

5.3.3.4 对业务应用人员的访谈调查

使用相应的访谈问卷，对业务应用人员有关信息系统安全管理现状的访谈调查，应做到：

a) 确定业务应用人员认为的信息系统安全策略及其优先顺序，与业务需求的一致性；

b) 确定业务应用人员认为已实施的信息系统安全保护措施和管理制度以及执行情况，记录在保

护措施调查表；

c) 确定业务应用人员认为的信息系统安全管理机构和相关人员（包括被访谈人）的职责要求，以及执行情况；

d) 确定业务应用人员认为的信息系统规划立项、设计实施、运行维护、终止处置的安全管理要求和实践措施；

e) 确定业务应用人员对现行安全策略和安全管理存在不足的了解程度，包括发生过的安全事件；

f) 应取得以下阶段性成果及文档：

——按优先级排列的业务应用人员识别的信息系统安全策略；

——业务应用人员认为已实施的信息系统安全保护措施和管理制度以及执行情况；

——业务应用人员认为信息系统安全管理机构和相关人员的职责要求以及执行情况；

——业务应用人员对信息系统规划立项、设计实施、运行维护、终止处置的安全管理要求和实践措施；

——业务应用人员对现行安全策略和安全管理存在不足的了解程度，以及与安全管理要求存在的差距，包括发生过的安全事件；

——业务应用人员的访谈记录、保护措施调查表。

5.3.3.5 对安全策略制度文档的符合性检查

按照5.3.2.6确定的安全策略制度文档范围进行符合性检查，必要时可根据访谈调查结果调整检查范围，应做到：

a) 对确定的安全策略及管理制度文档、操作规程等使用文档检查表（见6.2.3.1）逐一进行审查；

b) 对信息系统安全策略及管理制度文档体系框架的总体分析；

c) 对信息系统安全策略及制度文档的内容和结构进行逐一评价；

d) 应取得以下阶段性成果及文档：

——信息系统安全策略及制度文档审查原始材料；

——信息系统安全策略及制度文档体系和内容结构存在问题的描述；

——实施自评估时，应提供信息系统安全策略及制度文档体系和内容结构的改进建议（概述）。

5.3.3.6 对关键环节安全管理的有效性验证

按照5.3.2.6确定的信息系统物理环境和工作记录范围，以及访谈调查中确认已采取的安全保护措施进行有效性验证，必要时可根据访谈调查结果调整验证范围，应做到：

a) 对信息系统设计中采取的安全机制、贯彻总体安全策略，是否存在缺失或不当问题按照现场检查表（见6.2.3.2）进行检查；

b) 对信息系统的物理环境（如机房、办公场地、网络通讯线路、供电等）按照现场检查表进行检查；

c) 对信息系统的工作记录（如运行日志、安全配置记录、数据备份记录、变更记录、用户及权限审批记录、设备维修记录、人员培训记录等）按照现场检查表进行检查；

d) 对信息系统发生的安全事件报告记录、应急响应处置记录、应急响应演练记录按照现场检查表进行检查；

e) 对信息系统运行中产生的安全状态监视信息记录、安全审计信息记录按照现场检查表进行检查；

f) 对访谈调查中确认已采取的安全保护措施的执行情况按照现场检查表进行检查；

g) 对各类现场检查表进行汇总归纳，分析和评价信息系统安全策略、管理制度、保护措施的有效性，形成信息系统安全管理有效性验证结果文档；

h) 应取得以下阶段性成果及文档：

——信息系统各种现场检查表记录；

——信息系统安全管理有效性验证结果文档；

——信息系统安全管理有效性存在问题的描述；

——实施自评估时，应提供信息系统安全管理有效性存在问题的改进建议(概述)。

5.3.3.7 收集被选组件的技术检测结果[2)]

按照5.3.2.6确定待检测的核心部位及关键组件的范围，收集技术检测结果，必要时可根据访谈调查结果调整收集范围，应做到：

a) 收集近期的信息系统技术性检测结果中有关被选关键组件的脆弱性评估材料；

b) 收集信息系统安全技术保障总体结构设计及现状材料；

c) 对信息系统技术脆弱性和总体结构进行审核；

d) 对于无法收集且直接影响评估结论的技术检测结果，必要时可进行相应的技术检测，否则应在产生评估结论时予以说明；

e) 应取得以下阶段性成果及文档：

——信息系统技术脆弱性测试原始材料；

——信息系统技术脆弱性问题的描述；

——实施自评估时，应提供信息系统安全技术脆弱性问题的改进建议(概述)。

5.3.3.8 编制信息系统安全管理现状明细表

编制信息系统安全管理现状明细表，应做到：

a) 按照信息系统规划立项、设计实施、运行维护、终止处置不同阶段分别归纳安全管理现状；

b) 按照信息系统的政策和制度、机构和人员管理、风险管理、环境和资源管理、规划和立项管理、建设过程管理、运行和维护管理、系统终止管理、业务连续性管理、监督和检查管理等方面对安全管理现状进行描述；

c) 按照信息系统安全管理要求逐一对现状描述，给出与安全管理要求之间的差距分析意见，并提供相应的证据材料及来源；

d) 按照信息系统安全管理要求逐一对现状描述时，应吸收对应的访谈调查、符合性检查、有效性验证和技术检测结果并作为证据材料，进一步给出差距分析意见；

e) 实施自评估时，应根据与安全管理要求之间的差距分析，提出针对单项的初步改进意见；

f) 应取得以下阶段性成果及文档：

——所有访谈调查材料的汇编及说明；

——信息系统安全管理现状明细表；

g) 信息系统安全管理现状明细表，包括以下信息：

——评估要求的信息系统安全保护等级的说明；

——评估要求的信息系统生存周期不同阶段的说明；

——信息系统安全管理评估内容分类、评估项、评估内容条目；

——按照评估项及评估内容条目对安全管理现状的描述、差距分析意见、证据材料说明；

——实施自评估时，应针对单项的初步改进建议。

---

2) 由于独立的信息系统安全管理评估一般不进行技术检测，故采用“收集”技术性检测结果的办法，对管理评估分析依据的来源进行补充，以丰富和完善管理评估结论的例证。

5.3.3.9 关键管理环节的安全核查

在信息系统安全管理现状明细表的基础上，按照5.3.2.6确定的信息系统安全管理关键环节范围进行安全核查，必要时可根据访谈调查结果调整关键环节范围，应做到：

a) 对确定的信息系统安全管理环节使用安全管理核查表(见6.2.3.3)逐一进行核查；
b) 对安全管理核查表的每一项均应给出符合、基本符合、不符合的结论；
c) 对安全管理核查表的每一项结论，均应注明证据；
d) 对确定安全管理核查表的每一项结论时，出现与安全管理现状明细表或其他材料不一致时，应进行必要的复查；
e) 应取得以下阶段性成果及文档：
——信息系统安全管理核查表；
——信息系统安全管理核查依据和原始材料说明；
——实施自评估时，应提供信息系统安全管理基本符合、不符合项的改进建议(概述)。

5.3.4 确定信息系统安全管理评估结论

5.3.4.1 安全管理评估结论要求

信息系统安全管理评估结论，应做到：

a) 以信息系统安全管理现状明细表、信息系统安全管理核查表结果材料为评估分析依据；
b) 以信息系统安全管理评估中访谈调查、符合性检查、有效性验证、技术检测等结果材料为评估分析的原始证据；
c) 确定信息系统安全管理关键环节、信息系统核心部位及关键组件对信息系统安全管理的影响的加权方法及条件(见6.3.2)；
d) 确定信息系统安全管理的各个评估项评价的度量方法及条件；
e) 汇集各方面分析结果，进行综合评估，得出结论性意见；
f) 应取得以下阶段性成果及文档：
——信息系统安全管理评估分析依据材料及清单；
——信息系统安全管理评估分析证据材料及清单；
——信息系统关键资产及其管理所受威胁的影响；
——信息系统安全管理评估分析有关加权方法、度量方法及条件的说明(见6.3.2)；
——信息系统安全管理评估的结论性意见。

5.3.4.2 编制信息系统安全管理评估报告

编制信息系统安全管理评估报告应做到：

a) 编制信息系统安全管理评估报告文档；
b) 确定需提交的评估成果文件清单；
c) 整合需提交的评估成果文件；
d) 应取得以下最终成果文件：
——信息系统安全管理评估报告；
——评估成果文件清单，包括需提交的阶段性成果文档或材料；
——信息系统安全管理现状明细表、信息系统安全管理核查表；
——信息系统安全管理评估中访谈调查、符合性检查、有效性验证、技术检测等结果材料；
——实施自评估时，应提供信息系统安全管理改进建议稿。

5.3.4.3 信息系统安全管理改进建议

实施自评估时，信息系统安全管理改进建议稿应包括：

a) 信息系统已有的安全管理措施和存在的差距；

b) 信息系统安全管理现状明细表、信息系统安全管理核查表中针对单项的改进建议；

c) 信息系统拥有、运营或使用单位应采取的信息安全管理改进建议，并作为阶段性成果文档提供信息系统的安全管理改进建议稿。

5.3.5 评估结束及后续安排

5.3.5.1 评估结束

评估团队与被评估方配合，在评估结束时应完成以下工作：

a) 评估方与被评估方关于评估成果及报告的沟通和交换意见；

b) 评估报告及评估验收会议，要求评估实施团队、评估管理机构及有关领导、被评估方的信息部门和业务部门代表参加，必要时可邀请有关专家参与评审；

c) 对检查评估的总结，确认评估结果；

d) 通过自评估的评审，确认评估结果和整改建议内容；

e) 通过第三方评估的验收，确认评估结果，并依据评估发起时的委托要求确定是否需要确认整改建议内容；

f) 提交评估结果文件及有关材料；

g) 应取得以下工作成果及文档：

——评估报告及评估验收会议纪要；

——经评估团队与被评估方签署的评估总结、评审或验收的结论性文件；

——评估结果文件及有关材料，包括评估报告及全部文档资料；

——实施自评估时，应包括信息系统的安全整改建议及计划，及其形成的任务(项目)清单。

5.3.5.2 后续安排

在评估结束以后，被评估方的评估管理机构应依据评估报告，给出的信息系统安全保护策略以及风险缓解计划、整改建议措施清单(实施自评估时已提供)，并以此形成的任务清单，考虑本次评估的后续安排，要求如下：

a) 明确具体部门(如信息部门或信息安全部门)参与实施信息系统的安全风险缓解和整改建议计划，及其形成的任务(项目)；

b) 确定实施信息系统的安全风险缓解和整改建议计划的时间安排和任务分配，包括评估后一周内、一月内、一个季度内的具体安排；

c) 对于近期内不能完成的任务，应采取应急措施避免造成损失；

d) 确定对信息系统的安全风险缓解和整改建议计划的实施情况进行监控的措施；

e) 应注意及时发现在整改过程中产生新风险或已知风险发生的新变化，以及进行持续的评估和改进的计划；

f) 应取得工作成果，要求如下：

——信息系统的安全管理改进建议计划实施的具体安排；

——信息系统的安全管理改进建议计划实施的监督措施；

——对于近期内不能完成的任务所采取的应急措施；

——信息系统安全的持续评估和改进计划。

6 安全管理评估的方法、工具和实施

6.1 评估方法

6.1.1 访谈调查

6.1.1.1 访谈调查主要对象

访谈调查的主要对象一般可包括：

a) 高级管理层；

b) 执行管理层；

c) 信息技术和信息安全人员；

d) 业务应用人员。

6.1.1.2 访谈调查方法

访谈调查方法可包括：

a) 访谈调查前，应准备访谈问卷，并与访谈对象进行必要的沟通；

b) 初步访谈：用于收集信息安全管理体系的一般信息，策划后续各种访谈战略；

c) 实例收集访谈：用于根据安全管理体系特定要求，针对特定对象的访谈，注意收集实例；

d) 后续深入访谈：在对实例收集访谈收集到的信息进行分析并发现问题后进行，目的是寻找解决问题的答案；

e) 结案性访谈：在评估工作结束前，通过与被评估单位的讨论，保证评估结论、评估发现、建议的正确性。

访谈调查中根据评估的具体情况，选用适当的方法。

6.1.1.3 访谈调查质量控制

对访谈调查的质量，应从访谈对象的广度和访谈内容的深度进行控制。根据不同安全等级的不同要求，访谈调查的质量控制分为：

a) 第一级信息系统访谈调查质量控制要求如下：

——访谈对象以执行管理层为主；

——进行一般性访谈，内容可简要，对安全管理规范、安全管理机制以及安全管理工作相关的基本情况有一个广泛、大致了解。

b) 第二级信息系统访谈调查质量控制要求如下：

——访谈对象以执行管理层、信息技术和信息安全人员为主，必要时可选择业务应用人员、高级管理层及其他相关人员；

——进行重点访谈，内容应充分，对安全管理规范、安全管理机制以及安全管理工作相关的具体情况有较深入了解。

c) 第三级信息系统访谈调查质量控制要求如下：

——访谈对象以执行管理层、信息技术和信息安全人员、业务应用人员为主，并选择高级管理层及其他相关人员；

——进行较全面访谈，内容应覆盖各方面；对安全管理规范、安全管理机制以及安全管理工作的具体情况有全面了解。

d) 第四级信息系统访谈调查质量控制要求如下：

——访谈对象以执行管理层、信息技术和信息安全人员、业务应用人员为主，并选择高级管理

层及其他相关人员；

——进行全面访谈，内容应覆盖各方面；对安全管理体系相关的具体方面进行研究性或探究性讨论，力求准确、全面掌握安全管理要求落实情况细节。

e) 第五级信息系统访谈调查质量控制要求如下：

——访谈对象以执行管理层、信息技术和信息安全人员、业务应用人员为主，并选择高级管理层、保密部门及其他相关人员；

——进行全面深入访谈，内容应覆盖各方面，或设定专项内容；对安全管理体系的具体方面进行研究性或探究性讨论，应准确、全面掌握安全管理要求落实情况细节。

6.1.2 符合性检查[3)]

6.1.2.1 符合性检查主要对象

符合性检查的主要对象包括：

a) 信息安全方针、政策、计划、规程、系统要求文档；

b) 系统设计和接口规格文档；

c) 系统操作、使用、管理及各类日志管理的相关规定；

d) 备份操作、安全应急处置和复审，以及意外防范计划演练的相关文档；

e) 安全配置设定的有关文档；

f) 技术手册和用户指南、管理员指南；

g) 其他需要进行符合性检查的内容。

6.1.2.2 符合性检查方法

符合性检查可采用以下方法：

a) 明确提出需检查的文档清单；

b) 依据文档检查表对文档逐一检查，并填写文档检查表相关科目内容；

c) 对文档的格式检查，包括对文档的名称、发布日期、发布者、编号以及文本样式的规范化，以及同类文档的一致性进行评价；

d) 对文档的内容检查，根据与被检查文档相关的安全管理标准和被评估单位的安全管理要求，检查文档中是否包含了相关的安全管理要素，是否存在缺失或多余的内容，对文档的内容完整性和必要性进行评价；

e) 必要时，对文档相关的信息系统安全管理环节的一致性，以及相关材料(如记录、日志、报告、检验/评估/审计结果等)进行评价；

f) 归纳汇总并进行分析，形成结果文档。

6.1.2.3 符合性检查质量控制

对符合性检查的质量，应从检查对象的广度和检查内容的深度进行控制。根据不同安全等级的不同要求，符合性检查的质量控制分为：

a) 第一级信息系统符合性检查质量控制要求如下：

——对符合性检查的对象的种类和数量上抽样，种类和数量都较少；

——进行一般检查，利用有限证据或文件对安全管理控制进行概要的高层次检查、观察或核查，这类检查通常是利用规范、机制或活动的功能层面描述进行的。

b) 第二级信息系统符合性检查质量控制要求如下：

3) 本标准中符合性检查主要用于相关文档的检查。

——对符合性检查的对象的种类和数量上抽样，种类和数量都较多；
——进行重点检查，利用大量证据或文件对安全管理控制进行详细分析检查，这类检查通常是利用规范、机制、活动的功能层面描述或者高层次设计信息进行的。

c) 第三级信息系统符合性检查质量控制要求如下：
——对符合性检查的对象的种类和数量上抽样，基本覆盖；
——进行较全面检查，在重点检查的基础上，对主要安全管理控制措施实施的相关信息进行检查。

d) 第四级信息系统符合性检查质量控制要求如下：
——对符合性检查的对象应逐项进行检查；
——进行全面检查：在重点检查的基础上，对各项安全管理控制措施实施的相关信息进行检查。

e) 第五级信息系统符合性检查质量控制要求如下：
——对符合性检查的对象应逐项检查，或设定专项内容。
——进行全面深入检查：在重点检查的基础上，对各项安全管理控制措施实施的相关信息进行检查，对设定专项内容进行专门检查。

6.1.3 有效性验证[4)]

6.1.3.1 有效性验证主要对象

有效性验证的对象主要是安全管理机制，具体对象是：

a) 针对信息系统总体安全策略，以及信息系统设计实施中采取的安全保护措施，信息系统运行维护中执行的安全管理措施，验证其是否充分必要；
b) 针对信息系统物理环境，包括信息系统开发和运行的物理环境安全状况，物理访问控制的功能验证；
c) 针对信息系统运行维护，日常各种工作记录中反映的实际管理状况，安全配置设定的功能验证，访问控制、身份鉴别等实际控制能力的验证；
d) 针对信息系统业务连续性，包括安全事件和应急响应记录中反映的实际管理状况，事件响应和意外防范能力的验证，信息系统备份操作的功能验证；
e) 针对信息系统监视和审计，包括系统状态监视及安全审计信息记录中反映的实际管理状况，系统监视功能及安全审计能力的验证；
f) 针对被评估方认为已有的信息系统安全保护措施，验证其实际落实、执行以及效果状况。

6.1.3.2 有效性验证方法

针对被评估信息系统确立的安全管理目标，通过对管理活动的实际考查，检验证明安全管理机制的有效性。有效性验证方法及评价主要包括：

a) 确定有效性验证的主要对象，并按照信息系统设计、物理环境、工作记录、安全事件应急响应、安全监视及审计、已有保护措施执行等方面分类列出清单；
b) 编制用于本次评估的有效性验证的各类现场检查表(见 6.2.3.2)，并填写各个有效性验证对象的相关安全要求及管理目标等科目；
c) 依据现场检查表分别对有效性验证的各类主要对象进行检验，通过观察和判断，适当时结合测试等辅助手段所进行的综合性的评价，并填写现场检查表相关科目内容；

4) 本标准中有效性验证，主要是指对信息系统安全管理机制的一种基于业务性能的可用性，以及完成其策划的活动和达到策划结果的程度的检验证明。

d) 归纳汇总并进行分析，形成结果文档。

6.1.3.3 有效性验证质量控制

对有效性验证的质量，应从验证对象的广度和验证内容的深度进行控制。根据不同安全等级的不同要求，有效性验证的质量控制分为：

a) 第一级信息系统有效性验证质量控制要求如下：
——必要时可进行简要验证，以验证信息系统安全管理体系相关文件材料的完整性和可操作性为主，对贯彻实施的情况有初步的了解；
——对有效性验证的对象以验证管理控制措施为主。

b) 第二级信息系统有效性验证质量控制要求如下：
——应进行简要验证，以验证信息系统安全管理体系相关文件材料的完整性和可操作性为主，对贯彻实施的情况有基本的了解；
——对有效性验证的对象以验证管理控制措施为主，兼顾其他方面。

c) 第三级信息系统有效性验证质量控制要求如下：
——应进行充分验证，在简要验证的基础上，以验证信息系统安全管理体系相关文件得到贯彻实施为主，对贯彻实施的效果有充分的了解；
——对有效性验证的对象以验证管理控制措施、业务流程、运营措施、技术控制措施为主，兼顾其他方面。

d) 第四级信息系统有效性验证质量控制要求如下：
——应进行较全面验证，在充分验证的基础上，以验证贯彻实施是否取得了预期期望的结果，对贯彻实施的效果有较全面的了解；
——对有效性验证的对象以验证管理控制措施、业务流程、运营措施、技术控制措施为主，还应验证内审、外审、技术符合性等方面。

e) 第五级信息系统有效性验证质量控制要求如下：
——应进行全面验证，或设定专项验证，以验证贯彻实施是否取得了预期期望的结果，对贯彻实施的效果有全面的了解；
——对有效性验证的对象以验证管理控制措施、业务流程、运营措施、技术控制措施为主，还应验证内审、外审、技术符合性等方面，对设定专项内容进行专门验证。

6.1.4 技术检测

6.1.4.1 技术检测主要内容

独立的安全管理评估一般不进行技术检测，通常只是收集有关技术监测的结果作为管理评估分析的补充依据。

技术检测主要内容是与安全管理有关的审计信息和检测、监控信息，包括：

a) 信息系统的各种审计信息，如操作系统、数据库管理系统、应用系统、网络设备、安全专用设备以及终端设备等生成的安全审计信息；

b) 信息系统的各种安全检测、监控信息，包括独立检测、监控设备和集中管控的监测、监控设备所收集的信息；

c) 信息系统的物理环境的有关的安全检测、监控信息，如门禁系统、机房屏蔽系统、温湿度控制系统、供电系统、接地系统、防雷系统等收集的安全检测、监控信息；

d) 信息系统安全性检测的结果，包括针对操作系统、数据库管理系统、网络系统、应用系统、硬件系统进行的安全性检测获得的人工检查、工具扫描、应用分析、硬件检测、渗透测试等结果

信息；

e） 其他涉及信息系统安全管理方面的检测、监控信息。

6.1.4.2 技术检测方法

安全管理技术检测的方法包括：

a） 以对安全管理的有关信息的分析为依据，对安全策略、操作规程和规章制度的符合性、一致性程度逐一进行评价；

b） 安全性检测，主要采取以下手段：

——人工检查：以管理员身份评估文件许可、文件宿主、网络服务设置、安全策略配置、账户设置、程序真实性以及一般的与用户相关的安全点、入侵迹象等，发现存在的安全隐患；

——工具扫描：通过工具扫描，发现与鉴别、授权、访问控制和系统完整性设置等相关的安全脆弱性；

——应用分析：通过对所开发的应用系统进行系统运行的安全性检测分析，发现与鉴别、授权、访问控制和系统完整性设置等相关的安全脆弱性；

——硬件检测：通过对支持系统运行的硬件系统进行安全性检测，发现与系统运行和数据保护有关的特定安全脆弱性，如电磁泄漏发射和电磁干扰等；

——渗透测试：通过专业技术攻击检测，检查信息系统存在的缺陷和漏洞。

c） 安全管理技术检测分为：

——基本的技术检测：指被测试对象抽样种类和数量都选择较少的样本，覆盖范围小；以人工检查、工具扫描手段为主；

——充分的技术检测：指被测试对象抽样种类和数量都选择较多的样本，覆盖范围大；以人工检查、工具扫描、渗透测试手段为主，必要时可进行应用分析；

——全面的技术检测：指被测试对象抽样种类和数量都选择很多的样本，达到基本覆盖；以人工检查、工具扫描、渗透测试手段为主，并可进行应用分析、硬件检测。

d） 安全管理技术检测的过程，包括搜集素材、加工整理、综合评价、把握主题，以及形成报告等。

6.1.4.3 技术检测质量控制

对安全技术检测的质量，应从检测的广度和深度进行控制。根据不同安全等级的不同要求，安全技术检测的质量控制分为：

a） 第一级信息系统安全技术检测质量控制，要求如下：

——可进行基本的安全技术检测，通过对规章制度的符合性进行典型分析，了解安全管理实施的基本情况；

——以操作系统、数据库管理系统的日志信息为基本依据，进行技术检测；

——可通过对特定时段的日志信息的分析进行安全技术检测；

——可收集系统中重要部位的安全技术检测结果，为安全机制管理的验证和评价提供支持。

b） 第二级信息系统安全技术检测质量控制，要求如下：

——应进行必要的安全技术检测，通过对操作规程和规章制度的符合性进行分析，了解安全管理实施的主要情况；

——应以操作系统、数据库管理系统、应用系统、网络设备、安全专用设备等的审计信息为主要依据进行技术检测；

——应通过对特定时段的监测信息的分析进行检测验证；

——应收集系统中重要部位的安全技术检测结果，为进行安全机制管理的验证和评价提供支持。

c) 第三级信息系统安全技术检测质量控制，要求如下：

——应进行充分的安全技术检测，通过对安全策略、操作规程和规章制度的符合性进行综合性分析，充分了解安全管理实施的效果；

——应以操作系统、数据库管理系统、应用系统、网络设备、安全专用设备等的审计信息，信息系统的部分安全监测、监控信息，以及部分物理环境的安全监测、监控信息为依据，通过对这些信息的分析进行技术检测；

——应通过对较长的特定时段的监测信息的分析进行检测验证；

——应较全面收集系统中的安全技术检测结果，为安全机制管理的验证和评价提供支持。

d) 第四级信息系统安全技术检测质量控制，要求如下：

——应进行全面的安全技术检测，通过对安全策略、操作规程和规章制度的符合性、一致性进行综合性分析，验证安全管理实施是否取得了预期的结果，较全面的了解安全管理实施的效果；

——应以操作系统、数据库管理系统、应用系统、网络设备、安全专用设备、端设备等的审计信息，信息系统的各种安全监测、监控信息，以及物理环境的安全监测、监控信息为依据，通过对这些信息的分析进行较全面的安全技术检测；

——应通过对较长时段的连续监测信息的分析进行检测验证；

——应全面收集系统中的安全技术检测结果，为安全机制管理的验证和评价提供支持。

e) 第五级信息系统安全技术检测质量控制，要求如下：

——应进行全面系统的安全技术检测，通过对安全策略、操作规程和规章制度的符合性、一致性进行全面系统的综合性分析，以及对设定专项进行专题分析，验证安全管理实施是否取得了预期的结果，全面了解安全管理实施的效果；

——应以操作系统、数据库管理系统、网络设备系统、应用系统、安全专用设备、端设备等的审计信息，信息系统的各种安全监测、监控信息，以及物理环境的安全监测、监控信息为依据，通过对这些信息的分析进行全面系统的安全技术检测；

——应通过对长期的连续监测信息的分析进行安全技术检测；

——应全面系统地收集系统中的安全技术检测结果，为安全机制管理的验证和评价提供支持。

6.2 评估工具

6.2.1 调查表

6.2.1.1 资产调查表

资产调查表用于调查信息系统的资产，并针对高级管理层、执行管理层、信息技术和信息安全人员、业务应用人员对信息系统资产的认识进行调查。

资产调查表应首先调查被评估信息系统的基本情况，包括信息化现状概述，管理方法，信息系统列表，每个信息系统的概述，每个信息系统的边界，每个信息系统的设备部署，每个信息系统支撑的业务应用，信息系统列表、安全保护等级以及保护要求组合，其他内容等。

资产调查表应主要调查被评估信息系统的关键资产、重要资产和其他资产。被调查资产的粒度可控制在单个业务应用系统，描述具体应用系统的主要处理流程、提供的应用服务、涉及的业务数据，以及支撑环境设备等。列为重要资产、关键资产的，应说明确定的依据。

在调查信息系统的基本情况后，资产调查表从以下方面提出问题：

a) 被调查人认为需要保护的关键资产是什么，考虑信息系统的信息、系统、网络、软件、硬件、人员等方面；

b) 被调查人认为需要保护的重要资产是什么，考虑信息系统的信息、系统、网络、软件、硬件、人

员等方面；

c) 被调查人认为需要保护的其他资产是什么，考虑信息系统的信息、系统、网络、软件、硬件、人员等方面；

d) 被调查人选择这些关键资产、重要资产的基本原则是什么。

6.2.1.2 关注范围调查表

关注范围调查表用于调查信息系统面临的威胁，并针对高级管理层、执行管理层、信息技术和信息安全人员、业务应用人员对信息系统威胁的认识进行调查，了解哪些方面会威胁信息系统的资产，以及哪些资产属于主要关注范围。

关注范围调查表从以下方面提出问题：

a) 存在哪些人的故意行为可能会造成威胁，考虑被评估方内部人员及外部人员等方面；

b) 存在哪些系统问题可能会造成威胁，考虑硬件错误、软件错误、相关系统的不可用、恶意代码(病毒、蠕虫、特洛伊木马、后门)以及其他方面；

c) 存在哪些环境问题可能会造成威胁，考虑电源供电、网络通讯不可用、机房安全、自然灾害及其他方面；

d) 上述威胁可能对信息系统造成哪些损害和影响，考虑泄露或观察敏感信息，修改重要或敏感信息，毁坏或丢失重要信息、硬件或软件，访问重要信息、软件应用程序或服务中断等方面，如果发生过相关的安全事件应进行必要的描述。

6.2.1.3 安全需求调查表

安全需求调查表用于调查信息系统的安全需求，并针对高级管理层、执行管理层、信息技术和信息安全人员、业务应用人员对信息系统安全需求的认识进行调查。

安全需求调查表从以下方面提出问题：

a) 了解针对信息系统每种信息资产的安全需求，考虑保密性、完整性、可用性及其他方面，了解具体细节；

b) 每种信息资产的安全需求应达到何种保护等级，哪些安全需求最迫切。

6.2.1.4 保护措施调查表

保护措施调查表用于调查信息系统的已经采取的安全保护措施，并针对高级管理层、执行管理层、信息技术和信息安全人员、业务应用人员对信息系统已有安全保护措施的认识进行调查。

保护措施调查表从以下方面提出问题：

a) 了解被调查人员愿意深入讨论调查中的哪些问题，即认识到的安全问题；

b) 了解被调查人员认为有哪些重要问题是调查中没有涉及的，需要进一步了解；

c) 了解信息系统对某种资产已经采取的安全策略、保护措施都有哪些，逐一对被调查的资产进行了解；

d) 了解被调查人员认为已经采取的安全策略、保护措施是否有效，是否发生过相关的安全事件，并说明依据。

6.2.2 访谈问卷

6.2.2.1 访谈问卷分级分类

访谈问卷是管理评估重要的评估工具，涉及到具体的评估要点，关系到管理评估是否到位。访谈问卷根据本次评估的目的和范围，包括全部或部分信息系统生存周期的规划立项管理、设计实施管理、运

行维护管理、终止处置管理等阶段评估内容。访谈问卷依据被评估信息系统的安全保护等级可分为五个等级，与信息安全保护等级相对应。

访谈问卷针对高级管理层、执行管理层、信息技术和信息安全人员、业务应用人员分为不同类型的问卷，适用于不同访谈对象。

6.2.2.2 访谈问卷内容

访谈问卷针对信息系统安全管理体系各安全保护等级的要求，准备调查问卷时应做到结构清晰、系统、详细，问题的答案要求是“是/否/不确定”的选择，访谈时可记录选择的依据。

访谈问卷的内容依据本标准第7章内容确定，按照本次评估针对信息系统生存周期的具体阶段，确定各个阶段的侧重范围；按照被评估信息系统的信息安全保护等级，选择不同等级的访谈问卷内容。具体评估内容要点应根据第7章的要求，在附录A中选择对应内容。

访谈问卷针对高级管理层、执行管理层、信息技术和信息安全人员、业务应用人员不同要求，对本标准第7章内容进行剪裁和编辑形成问卷，其中：

a) 针对高级管理层的访谈问卷，至少选取策略和制度、机构和人员管理、监督和检查管理等方面；

b) 针对执行管理层的访谈问卷，一般为全部内容，根据具体情况允许对个别访谈对象的内容作出调整，但至少有一位访谈对象应访谈全部内容；

c) 针对信息技术和信息安全人员的访谈问卷，对信息安全人员的访谈应为全部内容，其他信息技术人员可依据承担的具体工作进行一定的裁剪；

d) 针对业务应用人员的访谈问卷，对应用系统管理员的访谈应为全部内容或少量剪裁，一般业务操作人员的访谈问卷至少选取策略和制度、环境和资源管理、运行和维护管理的部分内容。

6.2.3 检查表

6.2.3.1 文档检查表

文档检查表用于对被评估对象的信息安全策略、管理制度、操作规程以及相关文档的评价。

文档检查表包括评估规定审查的文档清单及针对文档清单中每一份文档的检查表。文档清单包括评估规定审查的文档和实际收到的文档。针对文档清单中每一份文档的检查表包括文档的名称、发布日期、发布者、内容要点、符合性完整性的评价、文本格式的评价等。

6.2.3.2 现场检查表

现场检查表用于对被评估信息系统安全策略、管理制度、保护措施的有效性进行评价和验证。

现场检查表按照信息系统设计、物理环境、工作记录、安全事件应急响应、安全监视及审计、已有保护措施执行等方面分类建立。现场检查表具体内容应根据第7章要求确定，可参见附录A。

各类现场检查表均包括相应的安全管理要求，实际落实或执行情况，发挥作用或实际效果，存在问题及原因，有效性验证结论等科目。根据具体检查项目逐一填写并进行评价。

6.2.3.3 安全管理核查表

安全管理核查表用于对信息系统安全管理进行评价。根据第7章要求，安全管理核查可分为信息系统规划立项管理、设计实施管理、运行维护管理、终止处置管理等信息系统生存周期不同阶段。安全管理核查表内容包括安全策略和制度管理、安全机构和人员管理、安全风险管理、环境和资源管理、运行和维护管理、业务连续性管理、监督和检查管理、生存周期管理等8个方面的信息安全管理要素（参见附录A），以及评价的结论（见6.3.2）。

安全管理核查表是评估报告结论的直接依据。

信息系统生存周期不同阶段、不同安全保护等级安全管理核查表的编制依据本标准第7章。

6.2.3.4 其他评估工具

信息系统安全管理评估对于评估工具的要求，仅对表格工具提出规范要求，对于数据库系统及专用程序等工具暂不作规范要求。

6.3 评估的实施

6.3.1 评估实施控制

6.3.1.1 评估过程控制点

信息系统安全管理评估过程的控制点主要包括：

a) 评估范围控制，根据本次评估目的以及被评估信息系统生存周期的不同阶段，确定安全管理评估的范围；

b) 评估进度控制，根据评估活动内容，在充分考虑被评估信息系统的安全目标和安全要求的基础上，确定评估过程的计划安排、评估过程深度和强度，以及评估进度；

c) 评估质量控制，根据评估方法要求，对评估实施过程中采取的访谈调查、符合性检查、有效性验证以及技术检测进行相应的质量控制；

d) 评价方法控制，根据评估结论判断的要求，对评估实施过程中单项结论和总体结论的评价方法和判断过程进行控制。

6.3.1.2 评估结果处理

信息系统安全管理评估结果应按下列要求进行处理：

a) 按规定的报告格式记录评估结果，报告内容的分类应与所进行的安全控制评估相一致，评估记录应及时归档；

b) 对评估记录进行分析，确定某一特定安全控制的总体效果，说明控制是否按确定的目标正确实施，并达到要求的预期结果；

c) 评估人员所给出的评估应能导致作出“符合、基本符合、不符合”的结论(具体见6.3.2)：

——符合：表明对特定要求，按照评估规程，通过评估后认为相关的安全管理控制产生了完全可以接受的结果；

——基本符合：表明通过评估后的安全管理措施产生了可部分接受但不能完全接受的结果，并能指出哪些安全管理控制措施尚未实施，以及信息系统的哪些脆弱性可能导致了这种情况的出现；

——不符合：表明通过评估，发现安全管理措施不能达到安全管理目标要求，产生了不可接受的结果，并能指出哪些安全管理控制措施尚未落实或实施，以及信息系统的哪些脆弱性可能导致了这种情况的出现；

d) 评估人员应识别并记录由于一个或多个安全管理控制的部分失效或完全失效带给信息系统的任何脆弱性，可用于：

——作为一项重要内容纳入信息系统的安全规划或重要整改建议中，为纠正安全控制缺陷提供详细的技术思路；

——提供信息安全主管领导和相关信息系统支持单位，利用评估结果和有关信息系统残余脆弱性信息，确定被评估信息系统和相关资产面临的总体风险。

6.3.1.3 保障证据收集

保障证据用来证明安全管理措施选择得当并正确实施，以及安全管理体系按照既定目标运行，符合信息系统安全要求的预期结果。建立保障证据的工作包括：

a) 通过从各种来源收集获保障证据，主要来源是信息系统相关人员，如信息系统开发者、系统集成方、认证机构、信息系统拥有者、审计人员、安全检查人员和安全管理人员等；

b) 收集来自产品层面的评估结果，进行系统层面的评估，用以确定信息系统采用的安全控制的总体效果，也可反映安全管理体系运行的总体效果；

c) 收集被评估信息系统在各个阶段中发生重要安全事件时相关的工作记录、审计信息、安全信息以及当时采取的行之有效的安全控制措施；

d) 收集被评估信息系统生存周期各个阶段关键环节的安全管理措施所产生效果的相关文档和记录信息。

6.3.1.4 生存周期划分

对信息系统的安全管理评估可分阶段进行，应注意：

a) 信息系统安全管理评估应贯穿于信息系统的整个生存周期，信息系统安全管理评估划分为信息系统规划立项管理、设计实施管理、运行维护管理、终止处置管理等阶段评估进行；

b) 信息系统生存周期各阶段管理评估的原则和方法是一致的；

c) 信息系统生存周期的各阶段安全管理的内容、对象、安全需求不同，使得安全管理评估的对象、目的、要求等各方面也有所不同。

6.3.1.5 评估风险规避

信息系统安全管理评估实施过程中可能存在以下风险，应注意规避：

a) 评估影响信息系统正常运行：在现场评估时需要对设备和系统的验证或测试操作，可能对系统运行造成一定影响，甚至可能出现误操作；

b) 信息系统敏感信息泄漏：泄漏被评估系统状态信息，如网络拓扑、IP 地址、业务流程、业务信息、安全机制、安全隐患和有关文档信息，以及敏感的安全策略；

c) 对评估结果存有争议：评估团队和被评估单位对评估结果可能存在争议；

d) 评估进程未能按计划完成：在评估中的访谈调查、符合性检查、有效性验证、技术检测可能由于被评估对象特别是被访谈人员某些不确定因素造成延误。

6.3.2 评估结论判断

6.3.2.1 评估内容条目设置

信息系统安全管理评估的内容条目可设置如下：

a) 关键条目

——信息系统安全管理评估的内容条目分为类、族、评估项、评估内容要点等四层，其中有部分评估条目比其他条目具有更为重要，对于所在的类、或族、或评估项是否符合可起到决定性作用，则对这样的评估内容条目称为关键条目；

——在信息系统安全管理评估所有内容条目中，设置了关键条目和非关键条目；在附录 A 的各个表中，标识出了关键条目，其中包括关键类、关键族、关键评估项、关键评估内容要点，未标识的条目则为非关键条目(可参见附录 A)。

b) 重要条目

——在关键条目以外，允许评估者根据被评估方业务应用的需求，在本次评估中可设置少量的重要条目，并应逐一说明其适用性；

——重要条目仅包括重要评估项、重要评估内容要点；

——重要评估项数量应控制在关键评估项总数的10%以下，同族内的重要评估项数量控制在非关键评估项的30%以下；

——重要评估内容要点数量应控制在关键评估内容要点总数的10%以下，同评估项内的重要评估内容要点数量控制在非关键评估内容要点的30%以下。

c) 一般条目

——信息系统安全管理评估内容条目中，除去重要条目的非关键条目均称为一般条目。

6.3.2.2 评估项结论

信息系统安全管理评估中评估项结论的判断，应按以下条件判断：

a) 评估项符合：评估项中所有评估内容要点均符合；

b) 评估项基本符合：评估项中所有评估内容要点符合或基本符合的数量超过一半，且所有的关键评估内容要点和重要评估内容要点均符合或基本符合；

c) 评估项不符合：评估项中所有评估内容要点符合或基本符合的数量不能超过一半，或关键评估内容要点和重要评估内容要点有不符合的。

6.3.2.3 评估族结论

信息系统安全管理评估中评估族结论，应按以下条件判断：

a) 评估族符合：评估族中所有关键评估项和重要评估项均符合且其他评估项为符合或基本符合的；

b) 评估族基本符合：评估族中所有评估项符合或基本符合的数量超过一半，且所有的关键评估项和重要评估项均符合或基本符合；

c) 评估族不符合：评估族中所有评估项符合或基本符合的数量不能超过一半，或关键评估项和重要评估项有不符合的。

6.3.2.4 评估类结论

信息系统安全管理评估中评估类结论，应按以下条件判断：

a) 评估类符合：评估类中所有关键评估族均符合且其他评估族为符合或基本符合的；

b) 评估类基本符合：评估类中所有评估族符合或基本符合的数量超过一半，且所有的关键评估族均符合或基本符合；

c) 评估类不符合：评估类中所有评估族符合或基本符合的数量不能超过一半，或关键评估族有不符合的。

6.3.2.5 总体评估结论

信息系统安全管理评估得出的总体评估类结论，应按以下条件判断：

a) 总体符合：总体评估中所有关键评估类均符合且其他评估类为符合或基本符合的；

b) 总体基本符合：总体评估中所有评估类符合或基本符合的数量超过一半，且所有的关键评估类均符合或基本符合；

c) 总体不符合：总体评估中所有评估类符合或基本符合的数量不能超过一半，或关键评估类有不符合的。

7 分等级管理评估

7.1 规划立项管理评估要求

7.1.1 本阶段评估范围

7.1.1.1 评估范围概述

在信息系统规划立项阶段，信息安全管理评估范围包括：

a) 规划立项阶段的关键管理环节：
   ——系统分析和安全定级；
   ——信息系统安全需求分析；
   ——信息系统总体安全规划；
   ——信息系统安全项目立项；
b) 规划立项阶段的安全策略和制度、机构和人员管理等保障措施；
c) 规划立项阶段的规划和立项管理等日常措施；
d) 规划立项阶段的风险管理、监督和检查管理等监督措施。

7.1.1.2 系统分析和安全定级

对信息系统的系统分析和信息安全保护等级定级管理的评估范围包括：

a) 信息系统分析：调查新建信息系统或现有信息系统基本情况，检查信息系统总体描述文件；
b) 信息系统划分：检查被评估的信息系统作为定级对象的区域划分，调查作为定级对象的信息系统详细描述文件；
c) 安全保护等级确定：调查被评估的信息系统的安全保护等级，检查组织机构领导层或上级主管部门的定级审批结果，以及信息系统定级结果报告。

7.1.1.3 信息系统安全需求分析

对新建信息系统或改造现有信息系统的安全需求分析管理的评估范围包括：

a) 调查对新建信息系统或改造现有信息系统的安全需求分析情况；
b) 检查安全需求分析报告，包括从法律、政策、适用的标准和指导方针、系统的功能需要，以及成本效益的平衡取舍等的因素。

7.1.1.4 信息系统总体安全规划

对新建信息系统或改造现有信息系统的总体安全规划管理的评估范围包括：

a) 调查信息系统的总体安全策略，包括信息系统的安全技术体系结构和安全管理体系结构；
b) 检查信息系统总体安全方案，包括与信息系统安全需求的符合性。

7.1.1.5 信息系统安全项目立项

对于新建信息系统或改造现有信息系统的安全项目立项管理的评估范围包括：

a) 安全建设规划：调查信息系统建设安全建设目标，检查可实施的项目规划；
b) 安全建设立项：调查安全项目立项情况，检查立项报告及审批结果。

7.1.2 第一级信息系统

7.1.2.1 策略和制度管理

信息系统规划立项阶段有关策略和制度管理方面，本级评估要求如下：

a) 评估信息系统规划立项阶段的管理目标和范围是否涵盖了规划立项阶段的关键管理环节(见7.1.1),具有基本的管理目标和范围;

b) 评估信息系统规划立项阶段提出的信息系统总体安全管理策略,是否确定了信息系统安全等级,形成了信息系统总体安全方案,是否达到基本的安全管理策略的要求,评估其制定和发布过程;

c) 评估信息系统规划立项阶段是否具有基本的安全管理规章制度,是否有规划、定级、立项管理制度,与系统规划立项相关的机构和人员管理、风险管理、监督检查管理制度,以及其他管理制度的规划,评估其制定和发布过程;

d) 评估信息系统规划立项阶段的策略与制度文档是否进行了基本的评审和修订,以及指定专人保管。

有关策略和制度方面的具体评估内容要点可参见附录A的A.2.1。

7.1.2.2 机构和人员管理

信息系统规划立项阶段有关机构和人员管理方面,本级评估要求如下:

a) 评估信息系统规划立项阶段工作是否有分管领导负责,并配备安全管理人员参加,对信息系统规划、定级、立项是否具有基本安全管理职能;

b) 评估信息系统规划立项阶段的人员管理,是否对与规划立项相关的信息安全人员、其他信息技术人员以及第三方人员有安全管理措施,是否对信息系统安全管理人员配备、信息系统关键岗位人员管理、人员录用管理、人员离岗管理、人员考核与审查管理、第三方人员管理具有规划;

c) 评估信息系统规划立项阶段的信息安全教育是否做到应知应会,能够听取信息安全专家建议。

有关机构和人员管理方面的具体评估内容要点可参见附录A的A.2.2。

7.1.2.3 风险管理

信息系统规划立项阶段应根据系统的安全保护等级选择基本安全措施的基础上,依据风险管理的方法补充和调整安全措施,对于规划立项阶段的风险管理,本级评估要求如下:

a) 评估信息系统规划立项阶段是否通过基本的风险管理,认识到系统的业务战略,明确系统安全需求及安全战略,能够描述信息系统建设预期对现有业务模式的作用,包括技术、管理等方面,确定应达到的安全目标;

b) 评估新建或改造信息系统的规划是否进行了风险分析,是否从新建或改造的信息系统的应用对象、应用环境、业务状况、操作要求等方面分析了可能存在的威胁,确定了系统运行环境和资产重要性;

c) 评估新建或改造信息系统的规划是否进行了风险控制,包括:

——是否建立了与业务战略相一致的信息系统安全规划,并得到最高管理者的认可;

——是否明确信息系统开发的管理、业务变更的管理、开发优先级;

——是否考虑信息系统的威胁、环境,并制定总体的安全方针;

d) 评估新建或改造信息系统的规划中是否进行了风险决策,对于新建或改造信息系统规划中存在的残余风险是否接受;

e) 评估信息系统规划立项阶段是否进行了风险评估,评估结果是否体现在新建或改造信息系统的规划中,是否按资质和信誉选择评估机构,签署保密协议,对评估信息规定交接手续。

有关风险管理方面的具体评估内容要点可参见附录A的A.2.3。

7.1.2.4 监督和检查管理

信息系统规划立项阶段的监督和检查管理方面,本级评估要求如下:

a) 评估信息系统规划立项阶段的法律符合性，新建或改造信息系统的规划、定级和立项是否符合国家有关信息安全法规要求，是否做到知晓适用法律，遵守知识产权要求，保护组织机构重要记录；

b) 评估新建或改造信息系统的规划、定级和立项过程是进行了监督控制，是否对规划立项阶段的安全状况进行自查，是否依据国家有关管理规范和技术标准进行保护。

有关监督和检查管理方面的具体评估内容要点可参见附录 A 的 A.2.7。

7.1.2.5 规划和立项管理

信息系统规划立项阶段有关规划和立项管理方面，本级评估要求如下：

a) 评估新建或改造信息系统的应用安全需求，是否与组织机构的业务发展战略一致，明确其重要性；

b) 评估信息系统建设或改造规划，是否包括了对新建或改造信息系统的总体描述，确定了安全保护等级，具有信息系统安全定级结果、总体安全方案，并得到管理层的批准；

c) 评估新建或改造信息系统的立项管理，是否在信息系统安全规划的基础上，经过管理层审批，对新建或改造信息系统的开发建设立项，并具有立项报告及审批结果。

有关规划和立项管理方面的具体评估内容要点可参见附录 A 的 A.2.8。

7.1.3 第二级信息系统

7.1.3.1 策略和制度管理

信息系统规划立项阶段有关策略和制度管理方面，本级评估要求如下：

a) 评估信息系统规划立项阶段的管理目标和范围是否涵盖了规划立项阶段的关键管理环节（见 7.1.1），具有较完整的管理目标与范围；

b) 评估信息系统规划立项阶段提出的信息系统总体安全管理策略，是否确定了信息系统安全等级，形成了信息系统总体安全方案，是否达到较完整的安全管理策略的要求，评估其制定和发布过程；

c) 评估信息系统规划立项阶段是否具有较完整的安全管理规章制度和操作规程，是否有规划、定级、立项管理制度，与系统规划立项相关的机构和人员管理、风险管理、监督检查管理制度，以及其他管理制度的规划，评估其制定和发布过程；

d) 评估信息系统规划立项阶段的策略与制度文档是否进行了较完整的评审和修订，以及指定专人保管、借阅审批和登记。

有关策略和制度方面的具体评估内容要点可参见附录 A 的 A.3.1。

7.1.3.2 机构和人员管理

信息系统规划立项阶段有关机构和人员管理方面，本级评估要求如下：

a) 评估信息系统规划立项阶段工作是否有分管领导和信息安全职能部门负责，并否配备安全管理人员参加，对信息系统规划、定级、立项是否具有安全管理领导职能；

b) 评估信息系统规划立项阶段的人员管理，是否对与规划立项相关的信息安全人员、其他信息技术人员以及第三方人员有安全管理措施，是否对信息系统安全管理人员配备、信息系统关键岗位人员管理、人员录用管理、人员离岗管理、人员考核与审查管理、第三方人员管理具有规划；

c) 评估信息系统规划立项阶段的信息安全教育是否做到应知应会，有计划开展培训，能够听取信息安全专家建议。

有关机构和人员管理方面的具体评估内容要点可参见附录 A 的 A.3.2。

7.1.3.3 风险管理

信息系统规划立项阶段应根据系统的安全保护等级选择基本安全措施的基础上，依据风险管理的方法补充和调整安全措施，对于规划立项阶段的风险管理，本级评估要求如下：

a) 评估信息系统规划立项阶段是否通过基本的风险管理，认识到系统的业务战略，明确系统安全需求及安全战略，能够描述信息系统建设预期对现有业务模式的作用，包括技术、管理等方面，确定应达到的安全目标；

b) 评估新建或改造信息系统的规划是否进行了风险分析，是否从新建或改造的信息系统的应用对象、应用环境、业务状况、操作要求等方面分析了可能存在的威胁及其发生概率，确定了系统运行环境和资产重要性；

c) 评估新建或改造信息系统的规划是否进行了风险控制，包括：

——是否建立了与业务战略相一致的信息系统安全规划，并得到最高管理者的认可；

——是否明确信息系统开发的管理、业务变更的管理、开发优先级；

——是否考虑信息系统的威胁、环境，并制定总体的安全方针；

——是否描述信息系统预期使用的信息，包括预期的应用、信息资产的重要性、潜在的价值、可能的使用限制、对业务的支持程度等；

d) 评估新建或改造信息系统的规划中是否进行了风险决策，对于新建或改造信息系统规划中存在的残余风险是否接受，以及残余风险监视措施；

e) 评估信息系统规划立项阶段是否进行了风险评估，评估结果是否体现在新建或改造信息系统的规划中，是否按资质和信誉选择评估机构，签署保密协议，对评估信息规定交接手续并替换敏感参数。

有关风险管理方面的具体评估内容要点可参见附录 A 的 A.3.3。

7.1.3.4 监督和检查管理

信息系统规划立项阶段的监督和检查管理方面，本级评估要求如下：

a) 评估信息系统规划立项阶段的法律符合性，新建或改造信息系统的规划、定级和立项是否符合国家有关信息安全法规要求，是否做到知晓适用法律，遵守知识产权要求，保护组织机构重要记录；

b) 评估信息系统规划立项阶段的依从性，对新建或改造信息系统的规划、定级和立项中有关贯彻安全策略和执行技术标准状况，进行依从性检查和分析；

c) 评估新建或改造信息系统的规划、定级和立项过程是进行了监督检查，是否对规划立项阶段的安全状况进行自查，是否依据国家有关管理规范和技术标准进行保护，接受监管部门的指导；规划中是否包括了基本的审计机制；

d) 评估信息系统规划立项阶段的责任认定，是否明确了新建或改造信息系统的规划、定级和立项过程的管理责任和技术责任，以及监督检查的责任。

有关监督和检查管理方面的具体评估内容要点可参见附录 A 的 A.3.7。

7.1.3.5 规划和立项管理

信息系统规划立项阶段有关规划和立项管理方面，本级评估要求如下：

a) 评估新建或改造信息系统的应用安全需求，是否与组织机构的业务发展战略一致，明确其重要性，分析了存在的威胁、脆弱性和风险；

b) 评估信息系统建设或改造规划，是否包括了对新建或改造信息系统的总体描述，确定了安全

保护等级，具有信息系统安全定级结果、总体安全方案，提出拟采用的主要技术和管理措施，并得到管理层的批准；

c) 评估新建或改造信息系统的立项管理，是否在信息系统安全规划的基础上，经过可行性论证和管理层审批，对新建或改造信息系统的开发建设立项，并具有立项报告及审批结果。

有关规划和立项管理方面的具体评估内容要点可参见附录 A 的 A.3.8。

7.1.4 第三级信息系统

7.1.4.1 策略和制度管理

信息系统规划立项阶段有关策略和制度管理方面，本级评估要求如下：

a) 评估信息系统规划立项阶段的管理目标和范围是否涵盖了规划立项阶段的关键管理环节（见7.1.1），具有完好定义的安全管理目标与范围；

b) 评估信息系统规划立项阶段提出的信息系统总体安全管理策略，是否确定了信息系统安全等级，形成了信息系统总体安全方案，是否达到体系化的安全管理策略的要求，评估其制定和发布过程；

c) 评估信息系统规划立项阶段是否具有体系化的安全管理规章制度和操作规程，是否有规划、定级、立项管理制度，与系统规划立项相关的机构和人员管理、风险管理、监督检查管理制度，以及其他管理制度的规划，评估其制定和发布过程；

d) 评估信息系统规划立项阶段的策略与制度文档是否进行了体系化的评审和修订，以及指定专人保管、限定借阅范围、审批和登记。

有关策略和制度方面的具体评估内容要点可参见附录 A 的 A.4.1。

7.1.4.2 机构和人员管理

信息系统规划立项阶段有关机构和人员管理方面，本级评估要求如下：

a) 评估信息系统规划立项阶段工作是否有信息安全领导小组和安全职能部门负责，并配备安全管理人员参加，对信息系统规划、定级、立项是否具有安全管理领导职能；

b) 评估信息系统规划立项阶段是否规划了安全机制集中管理机构人员职责和运行集中管理；

c) 评估信息系统规划立项阶段的人员管理是否对与规划立项相关的信息安全人员、其他信息技术人员以及第三方人员有安全管理措施，是否对信息系统安全管理人员配备、信息系统关键岗位人员管理、人员录用管理、人员离岗管理、人员考核与审查管理、第三方人员管理具有规划；

d) 评估信息系统规划立项阶段的信息安全教育是否做到应知应会，有计划开展培训，针对不同岗位培训，能够听取信息安全专家建议。

有关机构和人员管理方面的具体评估内容要点可参见附录 A 的 A.4.2。

7.1.4.3 风险管理

信息系统规划立项阶段应根据系统的安全保护等级选择基本安全措施的基础上，依据风险管理的方法补充和调整安全措施，对于规划立项阶段的风险管理，本级评估要求如下：

a) 评估信息系统规划立项阶段是否通过基本的风险管理，认识到系统的业务战略，明确系统安全需求及安全战略，能够描述信息系统建设预期对现有业务模式的作用，包括技术、管理等方面，确定应达到的安全目标；

b) 评估新建或改造信息系统的规划是否进行了风险分析，是否从新建或改造的信息系统的应用对象、应用环境、业务状况、操作要求等方面详细分析了可能存在的威胁及其发生概率，确定了系统运行环境和资产重要性；

c) 评估新建或改造信息系统的规划是否进行了风险控制，包括：
——是否建立了与业务战略相一致的信息系统安全规划，并得到最高管理者的认可；
——是否明确信息系统开发的管理、业务变更的管理、开发优先级；
——是否考虑信息系统的威胁、环境，并制定总体的安全方针；
——是否描述信息系统预期使用的信息，包括预期的应用、信息资产的重要性、潜在的价值、可能的使用限制、对业务的支持程度等；
——是否描述所有与信息系统安全相关的运行环境，包括物理和人员的安全配置，以及明确相关的法规、安全策略、习惯、专门技术和知识等；
d) 评估新建或改造信息系统的规划中是否进行了风险决策，对于新建或改造信息系统规划中存在的残余风险是否接受，以及残余风险监视措施；
e) 评估信息系统规划立项阶段是否进行了风险评估，评估结果是否体现在新建或改造信息系统的规划中，是否按资质和信誉选择评估机构，签署保密协议，对评估信息规定交接手续并替换敏感参数，对评估信息不得带出指定区域。

有关风险管理方面的具体评估内容要点可参见附录 A 的 A.4.3。

7.1.4.4 监督和检查管理

信息系统规划立项阶段的监督和检查管理方面，本级评估要求如下：

a) 评估信息系统规划立项阶段的法律符合性，新建或改造信息系统的规划、定级和立项是否符合国家有关信息安全法规要求，是否做到知晓适用法律，遵守知识产权要求，保护关键业务应用软件版权，保护组织机构重要记录，遵照国家法规使用密码技术；
b) 评估信息系统规划立项阶段的依从性，对新建或改造信息系统的规划、定级和立项中有关贯彻安全策略和执行技术标准状况，进行全面系统的依从性检查和分析；
c) 评估新建或改造信息系统的规划、定级和立项过程是进行了监督控制，是否对规划立项阶段的安全状况进行自查，是否依据国家有关管理规范和技术标准进行保护，接受监管部门的监督检查；规划中是否包括了审计机制；
d) 评估信息系统规划立项阶段的责任认定，是否明确了新建或改造信息系统的规划、定级和立项过程的管理责任和技术责任，以及审计监督的责任。

有关监督和检查管理方面的具体评估内容要点可参见附录 A 的 A.4.7。

7.1.4.5 规划和立项管理

信息系统规划立项阶段有关规划和立项管理方面，本级评估要求如下：

a) 评估新建或改造信息系统的应用安全需求，是否与业务发展战略一致，明确其重要性，分析了存在的威胁、脆弱性和风险，并结合信息系统总体安全规划的要求；
b) 评估信息系统建设或改造规划，是否包括了对新建或改造信息系统的总体描述，确定了安全保护等级，具有信息系统安全定级结果、总体安全方案，参照信息安全保障系统化建设要求，提出拟采用的主要技术和管理措施，并得到管理层的批准；
c) 评估新建或改造信息系统的立项管理，是否在信息系统安全规划的基础上，经过可行性论证、安全性评价和管理层审批，对新建或改造信息系统的开发建设立项，并具有立项报告及审批结果。

信息系统规划立项阶段有关规划和立项管理方面的具体评估内容要点可参见附录 A 的 A.4.8。

7.1.5 第四级信息系统

7.1.5.1 策略和制度管理

信息系统规划立项阶段有关策略和制度管理方面，本级评估要求如下：

a) 评估信息系统规划立项阶段的管理目标和范围是否涵盖了规划立项阶段的关键管理环节(见7.1.1),具有量化控制的安全管理目标与范围;

b) 评估信息系统规划立项阶段提出的信息系统总体安全管理策略,是否确定了信息系统安全等级,形成了信息系统总体安全方案,是否达到强制保护的安全管理策略的要求,评估其制定和发布过程;

c) 评估信息系统规划立项阶段是否具有强制保护的安全管理规章制度和操作规程,是否有规划、定级、立项管理制度,与系统规划立项相关的机构和人员管理、风险管理、监督检查管理制度,以及其他管理制度的规划,评估其制定和发布过程;

d) 评估信息系统规划立项阶段的策略与制度文档是否进行了强制保护的评审和修订,以及定专人保管、限定借阅范围、审批和登记等全面严格保管。

有关策略和制度方面的具体评估内容要点可参见附录A的A.5.1。

7.1.5.2 机构和人员管理

信息系统规划立项阶段有关机构和人员管理方面,本级评估要求如下:

a) 评估信息系统规划立项阶段工作是否有信息安全领导小组和安全职能部门负责,并配备安全管理人员参加,安全领导小组是否由主要负责人出任领导,对信息系统规划、定级、立项是否具有安全管理领导职能;

b) 评估信息系统规划立项阶段是否规划了安全机制集中管理机构人员职责和运行集中管理;

c) 评估信息系统规划立项阶段的人员管理,是否对与规划立项相关的信息安全人员、其他信息技术人员以及第三方人员有安全管理措施,是否对信息系统安全管理人员配备、信息系统关键岗位人员管理、人员录用管理、人员离岗管理、人员考核与审查管理、第三方人员管理具有规划;

d) 评估信息系统规划立项阶段的信息安全教育是否做到应知应会,有计划开展培训,针对不同岗位培训,听取信息安全专家建议,对信息安全专家的管理。

有关机构和人员管理方面的具体评估内容要点可参见附录A的A.5.2。

7.1.5.3 风险管理

信息系统规划立项阶段应根据系统的安全保护等级选择基本安全措施的基础上,依据风险管理的方法补充和调整安全措施,对于规划立项阶段的风险管理,本级评估要求如下:

a) 评估信息系统规划立项阶段是否通过基本的风险管理,认识到系统的业务战略,明确系统安全需求及安全战略,能够描述信息系统建设预期对现有业务模式的作用,包括技术、管理等方面,确定应达到的安全目标;

b) 评估新建或改造信息系统的规划是否进行了风险分析,是否从新建或改造的信息系统的应用对象、应用环境、业务状况、操作要求等方面详细分析了可能存在的威胁及其发生概率,确定了系统运行环境和资产重要性;

c) 评估新建或改造信息系统的规划是否进行了风险控制,包括:

——是否建立了与业务战略相一致的信息系统安全规划,并得到最高管理者的认可;

——是否明确信息系统开发的管理、业务变更的管理、开发优先级;

——是否考虑信息系统的威胁、环境,并制定总体的安全方针;

——是否描述信息系统预期使用的信息,包括预期的应用、信息资产的重要性、潜在的价值、可能的使用限制、对业务的支持程度等;

——是否描述所有与信息系统安全相关的运行环境,包括物理和人员的安全配置,以及明确相关的法规、安全策略、习惯、专门技术和知识等;

d) 评估新建或改造信息系统的规划中是否进行了风险决策,对于新建或改造信息系统规划中存

在的残余风险是否接受，以及残余风险监视措施；

e) 评估信息系统规划立项阶段是否进行了风险评估，评估结果是否体现在新建或改造信息系统的规划中，是否按资质和信誉选择评估机构，签署保密协议，对评估信息规定交接手续并替换敏感参数，对评估信息不得带出指定区域。

有关风险管理方面的具体评估内容要点可参见附录 A 的 A.5.3。

7.1.5.4 监督和检查管理

信息系统规划立项阶段的监督和检查管理方面，本级评估要求如下：

a) 评估信息系统规划立项阶段的法律符合性，新建或改造信息系统的规划、定级和立项是否符合国家有关信息安全法规要求，是否做到知晓适用法律，遵守知识产权要求，保护关键业务应用软件版权，保护组织机构重要记录，遵照国家法规使用密码技术；

b) 评估信息系统规划立项阶段的依从性，新建或改造信息系统的规划、定级和立项是否对贯彻安全策略情况进行了全面和系统的检查，技术依从性检查，以及监督检查的改进；

c) 评估新建或改造信息系统的规划、定级和立项过程是进行了监督控制，是否对规划立项阶段的安全状况进行自查，是否依据国家有关管理规范和技术标准进行保护，接受监管部门的强制监督检查；规划中是否包括了审计机制；

d) 评估信息系统规划立项阶段的责任认定，是否明确了新建或改造信息系统的规划、定级和立项过程的管理责任和技术责任，以及审计监督的责任。

有关监督和检查管理方面的具体评估内容要点可参见附录 A 的 A.5.7。

7.1.5.5 规划和立项管理

信息系统规划立项阶段有关规划和立项管理方面，本级评估要求如下：

a) 评估新建或改造信息系统的应用安全需求，是否与组织机构的业务发展战略一致，明确其重要性，分析了存在的威胁、脆弱性和风险，并结合信息系统总体安全规划的要求；

b) 评估信息系统建设或改造规划，是否包括了对新建或改造信息系统的总体描述，确定了安全保护等级，具有信息系统安全定级结果、总体安全方案，参照信息安全保障系统化建设要求，提出拟采用的主要技术和管理措施，并得到管理层的批准；

c) 评估新建或改造信息系统的立项管理，是否在信息系统安全规划的基础上，经过可行性论证、安全性评价和管理层审批，对新建或改造信息系统的开发建设立项，并具有立项报告及审批结果。

信息系统规划立项阶段有关规划和立项管理方面的具体评估内容要点可参见附录 A 的 A.5.8。

7.1.6 第五级信息系统

7.1.6.1 策略和制度管理

信息系统规划立项阶段有关策略和制度管理方面，本级评估要求如下：

a) 评估信息系统规划立项阶段的管理目标和范围是否涵盖了规划立项阶段的关键管理环节（见7.1.1），具有自我持续改进的安全管理目标与范围；

b) 评估信息系统规划立项阶段提出的信息系统总体安全管理策略，是否确定了信息系统安全等级，形成了信息系统总体安全方案，是否达到专控保护的安全管理策略的要求，评估其制定和发布过程；

c) 评估信息系统规划立项阶段是否具有专控保护的安全管理规章制度和操作规程，是否有规划、定级、立项管理制度，与系统规划立项的相关机构和人员管理、风险管理、监督检查管理制度，

以及其他管理制度的规划，评估其制定和发布过程；

d) 评估信息系统规划立项阶段的策略与制度文档是否进行了专控保护的评审和修订，以及定专人保管、限定借阅范围、审批和登记等全面严格保管。

有关策略和制度方面的具体评估内容要点可参见附录 A 的 A.6.1。

7.1.6.2 机构和人员管理

信息系统规划立项阶段有关机构和人员管理方面，本级评估要求如下：

a) 评估信息系统规划立项阶段工作是否有信息安全领导小组和安全职能部门负责，并配备安全管理人员参加，信息安全领导小组是否由主要负责人出任领导，对信息系统规划、定级、立项工作是否具有安全管理领导职能和信息安全保密监督管理职能；

b) 评估信息系统规划立项阶段是否规划了安全机制集中管理机构人员职责和运行集中管理；

c) 评估信息系统规划立项阶段的人员管理，是否对与规划立项相关的信息安全人员、其他信息技术人员以及第三方人员有安全管理措施，是否对信息系统安全管理人员配备、关键岗位人员管理、人员录用管理、人员离岗管理、人员考核与审查管理、第三方人员管理具有规划；

d) 评估信息系统规划立项阶段的信息安全教育是否做到应知应会，有计划开展培训，针对不同岗位培训，按人员资质要求培训，培养安全意识自觉性，听取信息安全专家建议，对信息安全专家的管理。

有关机构和人员管理方面的具体评估内容要点可参见附录 A 的 A.6.2。

7.1.6.3 风险管理

信息系统规划立项阶段应根据系统的安全保护等级选择基本安全措施的基础上，依据风险管理的方法补充和调整安全措施，对于规划立项阶段的风险管理，本级评估要求如下：

a) 评估信息系统规划立项阶段是否通过基本的风险管理，认识到系统的业务战略，明确系统安全需求及安全战略，能够描述信息系统建设预期对现有业务模式的作用，包括技术、管理等方面，确定应达到的安全目标；

b) 评估新建或改造信息系统的规划是否进行了风险分析，是否从新建或改造的信息系统的应用对象、应用环境、业务状况、操作要求等方面详细分析了可能存在的威胁及其发生概率，分析了资产重要性，确定了系统运行环境和资产重要性；

c) 评估新建或改造信息系统的规划是否进行了风险控制，包括：

——是否建立了与业务战略相一致的信息系统安全规划，并得到最高管理者的认可；

——是否明确信息系统开发的管理、业务变更的管理、开发优先级；

——是否考虑信息系统的威胁、环境，并制定总体的安全方针；

——是否描述信息系统预期使用的信息，包括预期的应用、信息资产的重要性、潜在的价值、可能的使用限制、对业务的支持程度等；

——是否描述所有与信息系统安全相关的运行环境，包括物理和人员的安全配置，以及明确相关的法规、安全策略、习惯、专门技术和知识等；

d) 评估新建或改造信息系统的规划中是否进行了风险决策，对于新建或改造信息系统规划中存在的残余风险是否接受，以及残余风险监视措施；

e) 评估信息系统规划立项阶段是否进行了风险评估，评估结果是否体现在新建或改造信息系统的规划中，是否按资质和信誉选择评估机构，签署保密协议，对评估信息规定交接手续并替换敏感参数，对评估信息不得带出指定区域。

有关风险管理方面的具体评估内容要点可参见附录 A 的 A.6.3。

7.1.6.4 监督和检查管理

信息系统规划立项阶段的监督和检查管理方面，本级评估要求如下：

a) 评估信息系统规划立项阶段的法律符合性，新建或改造信息系统的规划、定级和立项是否符合国家有关信息安全法规要求，是否做到知晓适用法律，遵守知识产权要求，保护关键业务应用软件版权，保护组织机构重要记录，遵照国家法规使用密码技术；

b) 评估信息系统规划立项阶段的依从性，新建或改造信息系统的规划、定级和立项是否对贯彻安全策略情况进行了全面和系统的检查，技术依从性检查，以及监督检查的改进；

c) 评估新建或改造信息系统的规划、定级和立项过程是进行了监督控制，是否对规划立项阶段的安全状况进行自查，是否依据国家有关管理规范和技术标准进行保护，接受监管部门的专门监督检查；规划中是否包括了审计机制；

d) 评估信息系统规划立项阶段的责任认定，是否明确了新建或改造信息系统的规划、定级和立项过程的管理责任和技术责任，以及审计监督的责任。

有关监督和检查管理方面的具体评估内容要点可参见附录 A 的 A.6.7。

7.1.6.5 规划和立项管理

信息系统规划立项阶段有关规划和立项管理方面，本级评估要求如下：

a) 评估新建或改造信息系统的应用安全需求，是否与组织机构的业务发展战略一致，明确其重要性，分析了存在的威胁、脆弱性和风险，并结合信息系统总体安全规划的要求；

b) 评估信息系统建设或改造规划，是否包括了对新建或改造信息系统的总体描述，确定了安全保护等级，具有信息系统安全定级结果、总体安全方案，参照信息安全保障系统化建设要求，提出拟采用的主要技术和管理措施，并得到管理层的批准；

c) 评估新建或改造信息系统的立项管理，是否在信息系统安全规划的基础上，经过可行性论证、安全性评价和管理层审批，对新建或改造信息系统的开发建设立项，并具有立项报告及审批结果。

信息系统规划立项阶段有关规划和立项管理方面的具体评估内容要点可参见附录 A 的 A.6.8。

7.2 设计实施管理评估要求

7.2.1 本阶段评估范围

7.2.1.1 评估范围概述

在新建信息系统或改造现有信息系统的设计实施阶段，信息安全管理评估范围包括：

a) 设计实施阶段的关键管理环节：
   ——系统安全设计；
   ——系统采购控制；
   ——系统开发控制；
   ——管理措施制定；
   ——集成及配置管理；
   ——测试及验收管理；

b) 设计实施阶段的策略和制度、机构和人员管理等保障措施；

c) 设计实施阶段的各个管理环节，以及环境和资源管理等日常措施；

d) 设计实施阶段的风险管理、监督和检查管理等监督措施。

7.2.1.2 系统安全设计

对于新建信息系统或改造现有信息系统的系统安全设计管理的评估范围包括：

a) 方案总体设计思路：描述信息系统业务功能、技术要求和安全要求，信息系统安全性指标，需保护的信息资产；

b) 技术措施实现内容设计：将信息系统安全总体方案落实到产品功能或物理形态上，提出能够实现的产品或组件及其具体规范，包括结构框架、功能及性能要求、部署方案等设计；

c) 管理措施实现内容设计：结合系统实际安全管理需要和本次技术建设内容，确定本次安全管理建设的范围和内容；

d) 设详细设计方案文档：包括总体设计思路、技术措施落实方案、管理措施落实方案，拟采取开发和采购的获取方式，及工时和费用等内容；

e) 对系统安全设计中有关技术要点的评价，见 GB/T 25070—2010 的相关要求。

7.2.1.3 系统采购控制

对于新建信息系统或改造现有信息系统的成品系统及软件硬件产品采购管理的评估范围包括：

a) 依据安全详细设计方案的设计要求，编制成品系统采购及软件硬件产品采购说明书；

b) 成品系统采购及软件硬件产品采购和使用，信息安全产品的采购和使用，应符合国家有关信息安全法规要求；

c) 检查有关市场调查、合同洽商文件，及候选产品、系统评测中的安全问题；

d) 成品系统采购及软件硬件产品选型测试，可依据国家认可的测试机构的产品测试报告；

e) 对软件硬件产品供货单位的选择和控制，保证产品采购安全。

7.2.1.4 系统开发控制

对于新建信息系统或改造现有信息系统的应用系统开发安全控制的评估范围包括：

a) 系统安全需求分析：方案设计的指标，软件设计的约束，与其他系统的接口要求；

b) 系统安全概要设计：相应安全等级的安全机制、体系结构、模块组成、接口定义；

c) 系统安全详细设计：按功能需求和模块划的各部分的详细设计，包含接口设计和管理方式设计等，作为编码工作的依据；

d) 应用软件编码实现：按照设计进行硬件调试和软件的编码，并通过论证和测试；

e) 应用系统软件测试：开发基本完成后进行的功能、性能、安全性测试；

f) 开发过程文档归档：包括需求说明书、概要设计、详细设计说明书，开发测试报告及开发说明书等。

7.2.1.5 管理措施制定

对于新建信息系统或改造现有信息系统的管理措施制定控制的评估范围包括：

a) 管理机构和人员的设置：安全管理机构及岗位设置，人员角色与职责，提供组织保障；

b) 管理制度的建设和修订：信息系统生存周期各个阶段需遵循的行为规范和操作规程；

c) 安全意识和技能培训：具有与其岗位职责相适应的职责、素质、技能、安全意识等培训；

d) 日常措施和监督检查实施计划：根据安全需要和保障机制需要确定的实施内容和计划；

e) 外包管理规定：信息系统建设和运行阶段的外包形式、内容、范围、责任及管理办法；

f) 信息系统工程管理：对新建信息系统或改造现有信息系统工程实施中安全管理的评价，见 GB/T 20282—2006 的相关要求。

7.2.1.6 集成及配置管理

对于新建信息系统或改造现有信息系统的安全集成及配置管理的评估范围包括：

a) 制定集成实施方案：包括具体指导工程的建设内容、方法和规范的指导文件；

b) 实施环境准备：包括硬件软件及环境准备，制定系统质量控制方案，指导系统实施过程；

c) 集成实施：将配置好策略的安全产品和控制模块部署到实际环境中，逐步实现质量控制目标；

d) 培训：提供信息系统使用说明书，并对系统维护人员进行必要培训；

e) 形成系统集成报告：包括集成实施方案、质量控制方案、集成实施报告及培训考核记录等。

7.2.1.7 测试及验收管理

对于新建信息系统或改造现有信息系统的测试及验收管理的评估范围包括：

a) 验收准备：准备系统验收方案和计划、定义验收方法，并审核；

b) 系统测试：根据系统验收方案，对整个系统进行集成性安全测试；

c) 系统验收：按照验收计划实施，依据系统测试结果、建设过程文档及落实情况，提出验收评审意见，形成验收报告；

d) 验收报告：验收报告需明确给出验收的结论，并经用户与建设方确认；

e) 系统交付：系统建设有关的软件及硬件设备，指导系统运行维护的文档、服务承诺书；

f) 运行审批：明确各方职责，经业务应用部门领导及高层领导审批，投入生产运行。

7.2.2 第一级信息系统

7.2.2.1 策略和制度管理

信息系统设计实施阶段有关策略和制度管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段的管理目标和范围是否涵盖了设计实施阶段的关键管理环节（见7.2.1），具有基本的管理目标和范围；

b) 评估信息系统设计实施阶段提出的信息系统总体安全管理策略，是否确定了信息系统安全总体设计思路，形成了信息系统安全详细设计方案文档，是否达到基本的安全管理策略的要求，评估其制定和发布过程；

c) 评估信息系统设计实施阶段是否具有基本的安全管理规章制度，是否有系统设计、采购、开发、集成、验收管理制度，与系统设计实施相关的机构和人员管理、风险管理、监督检查管理制度，以及其他管理制度的编制，评估其制定和发布过程；

d) 评估信息系统设计实施阶段的策略与制度文档是否进行了基本的评审和修订，以及指定专人保管。

有关策略和制度方面的具体评估内容要点可参见附录A的A.2.1。

7.2.2.2 机构和人员管理

信息系统设计实施阶段有关机构和人员管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段是否有分管领导负责，并配备安全管理人员参加，对信息系统设计实施是否具有基本安全管理职能；

b) 评估信息系统设计实施阶段的人员管理是否包括安全管理人员配备、信息系统关键岗位人员管理、人员录用管理、人员离岗管理、人员考核与审查管理，特别是与设计实施有关服务商等第三方人员管理；

c) 评估信息系统设计实施阶段的信息安全教育是否做到应知应会，能够听取信息安全专家建议。

有关机构和人员管理方面的具体评估内容要点可参见附录 A 的 A.2.2。

7.2.2.3 风险管理

信息系统设计实施阶段应根据系统的安全保护等级选择基本安全措施的基础上，依据风险管理的方法补充和调整安全措施，对于设计实施阶段的风险管理，本级评估要求如下：

a) 评估信息系统设计实施阶段是否通过基本的风险管理，提出信息系统安全功能需求，识别系统设计实施过程的风险，对系统建成后的安全功能进行验证；

b) 评估信息系统设计实施阶段是否进行了风险分析，基于信息系统设计方案的资产列表、安全措施，分析安全威胁，评价安全措施的实现程度，确定安全措施能否抵御现有威胁及脆弱性的影响；

c) 评估新建或改造信息系统的设计实施是否进行了风险控制，包括：

——设计方案是否符合系统建设规划并得到最高管理者的认可，设计方案中的安全需求是否符合规划阶段的安全目标，并基于威胁的分析制定信息系统的总体安全策略，根据设计开发计划及用户需求，对系统涉及的软件、硬件与网络进行分析和选型；

——对开发与技术/产品获取过程的评估和控制，是否包括符合法律、政策、适用标准和指导方针，满足信息系统的功能需要，考虑成本效益风险，通过安全测评和检查；

——系统交付实施过程的评估和控制，是否包括详细分析信息系统资产、面临的威胁和脆弱性，根据系统建设目标和安全需求，对系统的安全功能进行验收测试；评价安全措施能否抵御安全威胁，是否建立了与整体安全策略一致的管理制度；

d) 评估新建或改造信息系统的设计和实施中是否进行了风险决策，对于新建或改造信息系统设计实施中存在的残余风险是否接受；

e) 评估信息系统设计实施阶段的风险评估主要包括安全建设方案评审和系统测试验收，以及系统的开发与技术/产品获取、系统交付实施等过程，评估结果是否体现在新建或改造信息系统的设计和实施中，是否按资质和信誉选择评估机构，签署保密协议，对评估信息规定交接手续。

有关风险管理方面的具体评估内容要点可参见附录 A 的 A.2.3。

7.2.2.4 环境和资源管理

信息系统设计实施阶段有关环境和资源管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段的开发环境的管理，运行环境的设计实施，是否明确系统环境的管理部门和职责，以及机房安全管理措施；

b) 评估信息系统设计实施阶段的信息资源管理，是否编制了涉及系统开发使用和系统建设需采购的软件及硬件设备的基本资产清单，进行了基本的介质管理、设备管理。

有关环境和资源管理方面的具体评估内容要点可参见附录 A 的 A.2.4。

7.2.2.5 安全机制保障管理

信息系统设计实施阶段有关安全机制设计实现的管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段对信息系统用户管理的设计，是否包括用户分类，系统用户授权控制，普通用户、组织机构外部用户基本管理，临时用户设置与删除管理措施；

b) 评估信息系统设计实施阶段对信息系统信息交换的设计，是否包括了信息交换的基本管理措施；

c) 评估信息系统设计实施阶段对运行安全状态监控的设计，是否包括了运行状况监控及日志管理措施；

d) 评估信息系统设计实施阶段对信息系统有关安全机制保障管理的设计，是否包括身份鉴别、

自主访问控制、系统及网络安全、应用系统安全以及病毒防护的基本管理措施。

有关安全机制保障管理方面的具体评估内容要点可参见附录 A 的 A.2.5。

7.2.2.6 业务连续性管理

信息系统设计实施阶段有关业务连续性管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段对数据备份和恢复管理的设计，是否提出了数据备份和恢复管理职责，设计了数据备份的内容和周期；

b) 评估信息系统设计实施阶段对安全事件处理的设计，是否提出了安全事件内容和划分要求，设计了安全事件报告和处理程序；

c) 评估信息系统设计实施阶段对应急处理的设计，是否提出了应急处理的基本管理措施，设计了应急计划框架及具体应急计划。

有关业务连续性管理方面的具体评估内容要点可参见附录 A 的 A.2.6。

7.2.2.7 监督和检查管理

信息系统设计实施阶段的监督和检查管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段的法律符合性，新建或改造信息系统的系统设计、采购控制、开发控制、措施制定、集成及配置、测试及验收是否符合国家有关信息安全法规要求，是否做到知晓适用法律，遵守知识产权要求，保护组织机构重要记录；

b) 评估新建或改造信息系统的设计实施过程的监督控制，是否对设计实施阶段的安全状况进行自查，是否依据国家有关管理规范和技术标准进行保护。

有关监督和检查管理方面的具体评估内容要点可参见附录 A 的 A.2.7。

7.2.2.8 建设过程管理

信息系统设计实施阶段的建设过程管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段的建设项目准备，是否明确指定项目负责人，监督和管理系统安全设计、系统采购、系统开发、管理措施制定、集成及配置、测试及验收等全过程(见 7.2.1)；

b) 评估信息系统设计实施阶段的工程项目外包管理，是否选择具有国家主管部门的资质认证服务资质的信誉较好的厂商；

c) 评估信息系统设计实施阶段的自行开发环境控制，是否做到开发环境与运行环境分开，开发及测试活动也能分开；

d) 评估信息系统设计实施阶段的安全产品采购，是否在国家监管部门许可的产品目录中选择；

e) 评估信息系统设计实施阶段的建设项目测试验收，是否进行功能及性能测试，必要的安全性测试；

f) 评估信息系统设计实施阶段的新系统启用管理，验收后由使用者或管理者提出申请，经过相应领导审批。

有关建设过程管理方面的具体评估内容要点可参见附录 A 的 A.2.8。

7.2.3 第二级信息系统

7.2.3.1 策略和制度管理

信息系统设计实施阶段有关策略和制度管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段的管理目标和范围是否涵盖了设计实施阶段的关键管理环节(见 7.2.1)，具有较完整的管理目标和范围；

b) 评估信息系统设计实施阶段提出的信息系统总体安全管理策略，是否确定了信息系统安全总体设计思路，形成了信息系统安全详细设计方案文档，是否达到较完整的安全管理策略的要求，评估其制定和发布过程；

c) 评估信息系统设计实施阶段是否具有较完整的安全管理规章制度和操作规程，是否有系统设计、采购、开发、集成、验收管理制度，与系统设计实施相关的机构和人员管理、风险管理、监督检查管理制度，以及其他管理制度的编制，评估其制定和发布过程；

d) 评估信息系统设计实施阶段的策略与制度文档是否进行了较完整的评审和修订，以及指定专人保管、借阅审批和登记。

有关策略和制度方面的具体评估内容要点可参见附录 A 的 A.3.1。

7.2.3.2 机构和人员管理

信息系统设计实施阶段有关机构和人员管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段是否有分管领导和信息安全职能部门负责，并配备安全管理人员参加，对信息系统设计实施是否具有安全管理领导职能；

b) 评估信息系统设计实施阶段的人员管理是否包括安全管理人员配备、信息系统关键岗位人员管理、人员录用管理、人员离岗管理、人员考核与审查管理，特别是与设计实施有关服务商等第三方人员管理；

c) 评估信息系统设计实施阶段的信息安全教育是否做到应知应会，有计划开展培训，能够听取信息安全专家建议。

有关机构和人员管理方面的具体评估内容要点可参见附录 A 的 A.3.2。

7.2.3.3 风险管理

信息系统设计实施阶段应根据系统的安全保护等级选择基本安全措施的基础上，依据风险管理的方法补充和调整安全措施，对于设计实施阶段的风险管理，本级评估要求如下：

a) 评估信息系统设计实施阶段是否通过基本的风险管理，提出信息系统安全功能需求，识别系统设计实施过程的风险，对系统建成后的安全功能进行验证；

b) 评估信息系统设计实施阶段是否进行了风险分析，基于信息系统设计方案的资产列表、安全措施，进行安全威胁分析及概率分析列表、系统脆弱性分析，评价安全措施的实现程度，确定安全措施能否抵御现有威胁及脆弱性的影响；

c) 评估新建或改造信息系统的设计实施是否进行了风险控制，包括：

——设计方案是否符合系统建设规划并得到最高管理者的认可，设计方案中的安全需求是否符合规划阶段的安全目标，并基于威胁的分析制定信息系统的总体安全策略，根据设计开发计划及用户需求，对系统涉及的软件、硬件与网络进行分析和选型；

——对开发与技术/产品获取过程的评估和控制，是否包括符合法律、政策、适用标准和指导方针，满足信息系统的功能需要，考虑成本效益风险，通过安全测评和检查；

——系统交付实施过程的评估和控制，是否包括详细分析信息系统资产、面临的威胁和脆弱性，根据系统建设目标和安全需求，对系统的安全功能进行验收测试；评价安全措施能否抵御安全威胁，是否建立了与整体安全策略一致的管理制度；

d) 评估新建或改造信息系统的设计和实施中是否进行了风险决策，对于新建或改造信息系统设计实施中存在的残余风险是否接受，采取残余风险监视措施，做出信息系统投入运行的决定；

e) 评估信息系统设计实施阶段的风险评估主要包括安全建设方案评审和系统测试验收，以及系统的开发与技术/产品获取、系统交付实施等过程，评估结果是否体现在新建或改造信息系统的设计和实施中，是否按资质和信誉选择评估机构，签署保密协议，对评估信息规定交接手续

并替换敏感参数，技术检测应经授权并在监督下进行。

有关风险管理方面的具体评估内容要点可参见附录 A 的 A.3.3。

7.2.3.4 环境和资源管理

信息系统设计实施阶段有关环境和资源管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段的开发环境的管理，运行环境的设计实施，做到开发环境、测试环境与运行环境分开，是否明确系统环境的管理部门和职责，机房及办公环境的安全管理措施，对来访人员的控制管理；

b) 评估信息系统设计实施阶段的信息资源管理，是否编制了涉及系统开发使用和系统建设需采购的软件及硬件设备的详细资产清单，采取资产分类，进行了介质管理、设备管理。

有关环境和资源管理方面的具体评估内容要点可参见附录 A 的 A.3.4。

7.2.3.5 安全机制保障管理

信息系统设计实施阶段有关安全机制保障管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段对信息系统用户管理的设计，是否包括用户分类，系统用户授权控制及特权管理，普通用户及敏感信息处理，组织机构外部用户及其特定需求管理，临时用户设置、删除及审计管理措施；

b) 评估信息系统设计实施阶段对信息系统信息交换的设计，是否包括了信息交换的规范化管理措施；

c) 评估信息系统设计实施阶段对运行安全状态监控的设计，是否包括了运行状况、安全、性能监控及日志管理措施；

d) 评估信息系统设计实施阶段对信息系统有关安全机制保障管理的设计，是否包括身份鉴别、自主访问控制、系统及网络安全、应用系统安全、病毒防护管理措施，以及密码算法和密钥管理措施。

有关安全机制保障管理方面的具体评估内容要点可参见附录 A 的 A.3.5。

7.2.3.6 业务连续性管理

信息系统设计实施阶段有关业务连续性管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段对数据备份和恢复管理的设计，是否提出了数据备份和恢复管理职责，设计了数据备份的内容和周期，介质备份及设备备份；

b) 评估信息系统设计实施阶段对安全事件处理的设计，是否提出了安全事件内容和划分要求，设计了安全事件报告和处理程序，以及安全隐患问题报告和防范；

c) 评估信息系统设计实施阶段对应急处理的设计，是否提出了应急处理的基本管理措施，设计了应急计划框架及具体应急计划。

有关业务连续性管理方面的具体评估内容要点可参见附录 A 的 A.3.6。

7.2.3.7 监督和检查管理

信息系统设计实施阶段的监督和检查管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段的法律符合性，新建或改造信息系统的系统设计、采购控制、开发控制、措施制定、集成及配置、测试及验收是否符合国家有关信息安全法规要求，是否做到知晓适用法律，遵守知识产权要求，防止滥用信息处理设备，保护业务应用软件版权，保护组织机构重要记录；

b) 评估信息系统设计实施阶段的依从性，对新建或改造信息系统的设计方案及实现中有关贯彻

安全策略和执行技术标准状况，进行依从性检查和分析；

c) 评估新建或改造信息系统的设计实施过程的监督控制，是否对设计实施阶段的安全状况进行自查，是否依据国家有关管理规范和技术标准进行保护，接受监管部门的指导；规划中是否包括了基本的安全审计机制；

d) 评估信息系统设计实施阶段的责任认定，是否明确了新建或改造信息系统的设计实施过程的管理责任和技术责任，监督检查责任，以及审计及结果处理责任。

有关监督和检查管理方面的具体评估内容要点可参见附录 A 的 A.3.7。

7.2.3.8 建设过程管理

信息系统设计实施阶段的建设过程管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段的建设项目准备，是否明确指定项目负责人，监督和管理系统安全设计、系统采购、系统开发、管理措施制定、集成及配置、测试及验收等全过程（见 7.2.1），具有详细的项目实施计划；

b) 评估信息系统设计实施阶段的工程项目外包管理，是否在主管部门指定或特定范围内选择具有国家主管部门的资质认证服务资质的信誉较好的厂商；

c) 评估信息系统设计实施阶段的自行开发环境控制，是否做到开发环境与运行环境分开，开发及测试活动也能分开；是否能够保护好系统开发文档；非自行开发的软件包一般不作修改；

d) 评估信息系统设计实施阶段的安全产品采购，是否在国家监管部门许可的产品目录中选择；

e) 评估信息系统设计实施阶段的建设项目测试验收，是否进行功能、性能和安全性测试，具有系统验收要求和标准的定义文档；

f) 评估信息系统设计实施阶段的新系统启用管理，验收后由使用者或管理者提出申请，经过相应领导审批，并进行试运行。

有关建设过程管理方面的具体评估内容要点可参见附录 A 的 A.3.8。

7.2.4 第三级信息系统

7.2.4.1 策略和制度管理

信息系统设计实施阶段有关策略和制度管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段的管理目标和范围是否涵盖了设计实施阶段的关键管理环节（见 7.2.1），具有完好定义的管理目标和范围；

b) 评估信息系统设计实施阶段提出的信息系统总体安全管理策略，是否确定了信息系统安全总体设计思路，形成了信息系统安全详细设计方案文档，是否达到体系化的安全管理策略的要求，评估其制定和发布过程；

c) 评估信息系统设计实施阶段是否具有体系化的安全管理规章制度和操作规程，是否有系统设计、采购、开发、集成、验收管理制度，与系统设计实施相关的机构和人员管理、风险管理、监督检查管理制度，以及其他管理制度的编制，评估其制定和发布过程；

d) 评估信息系统设计实施阶段的策略与制度文档是否进行了体系化的评审和修订，以及指定专人保管、限定借阅范围、审批和登记。

有关策略和制度方面的具体评估内容要点可参见附录 A 的 A.4.1。

7.2.4.2 机构和人员管理

信息系统设计实施阶段有关机构和人员管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段是否有信息安全领导小组和安全职能部门负责，并配备安全管理

人员参加，对信息系统设计实施是否具有安全管理领导职能；

b) 评估信息系统设计实施阶段是否制定了安全机制集中管理机构人员职责和运行集中管理规范；

c) 评估信息系统设计实施阶段的人员管理是否包括安全管理人员配备、信息系统关键岗位人员管理、人员录用管理、人员离岗管理、人员考核与审查管理，特别是与设计实施有关服务商等第三方人员管理；

d) 评估信息系统设计实施阶段的信息安全教育是否做到应知应会，有计划开展培训，针对不同岗位培训，能够听取信息安全专家建议。

有关机构和人员管理方面的具体评估内容要点可参见附录 A 的 A.4.2。

7.2.4.3 风险管理

信息系统设计实施阶段应根据系统的安全保护等级选择基本安全措施的基础上，依据风险管理的方法补充和调整安全措施，对于设计实施阶段的风险管理，本级评估要求如下：

a) 评估信息系统设计实施阶段是否通过基本的风险管理，提出信息系统安全功能需求，识别系统设计实施过程的风险，对系统建成后的安全功能进行验证；

b) 评估信息系统设计实施阶段是否进行了风险分析，基于信息系统设计方案的资产列表、安全措施，进行安全威胁分析及概率分析列表、系统脆弱性分析，评价安全措施的实现程度，确定安全措施能否抵御现有威胁及脆弱性的影响；

c) 评估新建或改造信息系统的设计实施是否进行了风险控制，包括：

——设计方案是否符合系统建设规划并得到最高管理者的认可，设计方案中的安全需求是否符合规划阶段的安全目标，并基于威胁的分析制定信息系统的总体安全策略，根据设计开发计划及用户需求，对系统涉及的软件、硬件与网络进行分析和选型；

——对开发与技术/产品获取过程的评估和控制，是否包括符合法律、政策、适用标准和指导方针，满足信息系统的功能需要，考虑成本效益风险，通过安全测评和检查；

——系统交付实施过程的评估和控制，是否包括详细分析信息系统资产、面临的威胁和脆弱性，根据系统建设目标和安全需求，对系统的安全功能进行验收测试；评价安全措施能否抵御安全威胁，是否建立了与整体安全策略一致的管理制度；

d) 评估新建或改造信息系统的设计和实施中是否进行了风险决策，对于新建或改造信息系统设计实施中存在的残余风险是否接受，采取残余风险监视措施，做出信息系统投入运行的决定；

e) 评估信息系统设计实施阶段的风险评估主要包括安全建设方案评审和系统测试验收，以及系统的开发与技术/产品获取、系统交付实施等过程，评估结果是否体现在新建或改造信息系统的设计和实施中，是否按资质和信誉选择评估机构，签署保密协议，对评估信息规定交接手续并替换敏感参数，技术检测应经授权并在监督下进行，对评估信息不得带出指定区域。

有关风险管理方面的具体评估内容要点可参见附录 A 的 A.4.3。

7.2.4.4 环境和资源管理

信息系统设计实施阶段有关环境和资源管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段的开发环境的管理，运行环境的设计实施，做到开发环境、测试环境与运行环境物理分开，是否明确了系统环境的管理部门和职责，机房及办公环境的安全管理措施，对来访人员的控制，标识不同安全区域，配置门禁控制手段；

b) 评估信息系统设计实施阶段的信息资源管理，是否编制了涉及系统开发使用和系统建设需采购的软件及硬件设备的详细资产清单，采取资产分类，进行了介质管理、设备管理及资产信息管理。

有关环境和资源管理方面的具体评估内容要点可参见附录 A 的 A.4.4。

7.2.4.5 安全机制保障管理

信息系统设计实施阶段有关安全机制保障管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段对信息系统用户管理的设计，是否包括用户分类，系统用户授权控制、特权管理、监督性保护，普通用户及敏感信息处理，重要业务用户管理，组织机构外部用户及其特定需求管理，临时用户设置和限制、删除以及审计管理措施；

b) 评估信息系统设计实施阶段对信息系统信息交换的设计，是否包括了不同安全区域信息交换的规范化管理措施；

c) 评估信息系统设计实施阶段对运行安全状态监控的设计，是否包括了运行状况、安全、性能集中监控及日志管理措施；

d) 评估信息系统设计实施阶段对信息系统有关安全机制保障管理的设计，是否包括具有审计、证书支持的身份鉴别机制管理，自主访问控制和强制访问控制机制的管理，系统安全管理，网络安全管理，应用系统安全管理，病毒防护集中管理，以及密码算法、密钥管理、以密码技术为基础的安全管理措施；

e) 评估信息系统设计实施阶段对信息系统安全机制集中管理的设计，是否包括系统管理、安全管理、审计管理等安全机制集中控管、安全信息集中管理，安全机制整合的一般功能，安全机制整合的工作方式管理措施。

有关安全机制保障管理方面的具体评估内容要点可参见附录 A 的 A.4.5。

7.2.4.6 业务连续性管理

信息系统设计实施阶段有关业务连续性管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段对数据备份和恢复管理的设计，是否提出了数据备份和恢复管理职责，设计了数据备份的内容和周期，介质备份及设备备份，系统热备份与冗余；

b) 评估信息系统设计实施阶段对安全事件处理的设计，是否提出了安全事件内容和划分要求，设计了安全事件报告和处理程序，以及安全隐患问题报告和防范；

c) 评估信息系统设计实施阶段对应急处理的设计，是否提出了应急处理的管理措施和执行能力，设计了应急计划框架及具体应急计划。

有关业务连续性管理方面的具体评估内容要点可参见附录 A 的 A.4.6。

7.2.4.7 监督和检查管理

信息系统设计实施阶段的监督和检查管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段的法律符合性，新建或改造信息系统的系统设计、采购控制、开发控制、措施制定、集成及配置、测试及验收是否符合国家有关信息安全法规要求，是否做到知晓适用法律，遵守知识产权要求，防止滥用信息处理设备，保护关键业务应用软件版权，保护组织机构重要记录，遵照国家法规使用密码技术及选择密码技术产品；

b) 评估信息系统设计实施阶段的依从性，对新建或改造信息系统的设计方案及实现中有关贯彻安全策略和执行技术标准状况，进行全面系统的依从性检查和分析；

c) 评估新建或改造信息系统的设计实施过程的监督控制，是否对设计实施阶段的安全状况进行自查，是否依据国家有关管理规范和技术标准进行保护，接受监管部门的监督检查；规划中是否包括了安全审计机制；

d) 评估信息系统设计实施阶段的责任认定，是否明确了新建或改造信息系统的设计实施过程的管理责任和技术责任，监督检查责任，以及审计及结果处理责任。

有关监督和检查管理方面的具体评估内容要点可参见附录 A 的 A.4.7。

7.2.4.8 建设过程管理

信息系统设计实施阶段的建设过程管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段的建设项目准备，是否明确指定项目负责人，监督和管理系统安全设计、系统采购、系统开发、管理措施制定、集成及配置、测试及验收等全过程(见 7.2.1)，具有详细的项目实施计划和过程管理流程，建立工程监理；

b) 评估信息系统设计实施阶段的工程项目外包管理，是否在主管部门指定或特定范围内选择具有国家主管部门的资质认证服务资质的信誉较好的厂商，可参照评估机构的选择要求(参见附录 A 的 A.4.3)；具有对项目的保护和控制流程；

c) 评估信息系统设计实施阶段的自行开发环境控制，是否做到开发环境与运行环境分开，开发及测试活动也能分开；是否能够保护好系统开发文档，控制对程序资源库的访问；非自行开发的软件包一般不作修改；

d) 评估信息系统设计实施阶段的安全产品采购，是否在国家监管部门许可的产品目录中选择，执行国家有关信息安全等级三级及以上信息安全产品采购规定；

e) 评估信息系统设计实施阶段的建设项目测试验收，是否进行功能、性能和安全性测试，以及约定的安全措施、应急计划、应用指南、操作培训等，具有系统验收要求和标准的定义文档；

f) 评估信息系统设计实施阶段的新系统启用管理，验收后由使用者或管理者提出申请，经过相应领导审批，并进行试运行及其安全评估。

有关建设过程管理方面的具体评估内容要点可参见附录 A 的 A.4.8。

7.2.5 第四级信息系统

7.2.5.1 策略和制度管理

信息系统设计实施阶段有关策略和制度管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段的管理目标和范围是否涵盖了设计实施阶段的关键管理环节(见 7.2.1)，具有量化控制的管理目标和范围；

b) 评估信息系统设计实施阶段提出的信息系统总体安全管理策略，是否确定了信息系统安全总体设计思路，形成了信息系统安全详细设计方案文档，是否达到强制保护的安全管理策略的要求，评估其制定和发布过程；

c) 评估信息系统设计实施阶段是否具有强制保护的安全管理规章制度和操作规程，是否有系统设计、采购、开发、集成、验收管理制度，与系统设计实施相关的机构和人员管理、风险管理、监督检查管理制度，以及其他管理制度的编制，评估其制定和发布过程；

d) 评估信息系统设计实施阶段的策略与制度文档是否进行了强制保护的评审和修订，以及指定专人保管、限定借阅范围、审批和登记等全面严格保管。

有关策略和制度方面的具体评估内容要点可参见附录 A 的 A.5.1。

7.2.5.2 机构和人员管理

信息系统设计实施阶段有关机构和人员管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段是否有信息安全领导小组和安全职能部门负责，并配备安全管理人员参加，安全领导小组是否由主要负责人出任领导，对信息系统设计实施是否具有安全管理领导职能；

b) 评估信息系统设计实施阶段是否制定了安全机制集中管理机构人员职责和运行集中管理规范；

c) 评估信息系统设计实施阶段的人员管理是否包括安全管理人员配备、信息系统关键岗位人员管理、人员录用管理、人员离岗管理、人员考核与审查管理，特别是与设计实施有关服务商等第三方人员管理；

d) 评估信息系统设计实施阶段的信息安全教育是否做到应知应会，有计划开展培训，针对不同岗位培训，听取信息安全专家建议，对信息安全专家的管理。

有关机构和人员管理方面的具体评估内容要点可参见附录 A 的 A.5.2。

7.2.5.3 风险管理

信息系统设计实施阶段应根据系统的安全保护等级选择基本安全措施的基础上，依据风险管理的方法补充和调整安全措施，对于设计实施阶段的风险管理，本级评估要求如下：

a) 评估信息系统设计实施阶段是否通过基本的风险管理，提出信息系统安全功能需求，识别系统设计实施过程的风险，对系统建成后的安全功能进行验证；

b) 评估信息系统设计实施阶段是否进行了风险分析，基于信息系统设计方案的资产列表、安全措施，进行安全威胁分析及概率分析列表、系统脆弱性分析，评价安全措施的实现程度，确定安全措施能否抵御现有威胁及脆弱性的影响；

c) 评估新建或改造信息系统的设计实施是否进行了风险控制，包括：

——设计方案是否符合系统建设规划并得到最高管理者的认可，设计方案中的安全需求是否符合规划阶段的安全目标，并基于威胁的分析制定信息系统的总体安全策略，根据设计开发计划及用户需求，对系统涉及的软件、硬件与网络进行分析和选型；

——对开发与技术/产品获取过程的评估和控制，是否包括符合法律、政策、适用标准和指导方针，满足信息系统的功能需要，考虑成本效益风险，通过安全测评和检查；

——系统交付实施过程的评估和控制，是否包括详细分析信息系统资产、面临的威胁和脆弱性，根据系统建设目标和安全需求，对系统的安全功能进行验收测试；评价安全措施能否抵御安全威胁，是否建立了与整体安全策略一致的管理制度；

d) 评估新建或改造信息系统的设计和实施中是否进行了风险决策，对于新建或改造信息系统设计实施中存在的残余风险是否接受，采取残余风险监视措施，做出信息系统投入运行的决定；

e) 评估信息系统设计实施阶段的风险评估主要包括安全建设方案评审和系统测试验收，以及系统的开发与技术/产品获取、系统交付实施等过程，评估结果是否体现在新建或改造信息系统的设计和实施中，是否按资质和信誉选择评估机构，签署保密协议，对评估信息规定交接手续并替换敏感参数，技术检测应经授权并在监督下进行，对评估信息不得带出指定区域。

有关风险管理方面的具体评估内容要点可参见附录 A 的 A.5.3。

7.2.5.4 环境和资源管理

信息系统设计实施阶段有关环境和资源管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段的开发环境的管理，运行环境的设计实施，做到开发环境、测试环境与运行环境物理分开，是否明确了系统环境的管理部门和职责，机房及办公环境的安全管理措施，对来访人员的控制，标识不同安全区域并隔离，增强门禁控制手段，启用视频监控和专职警卫；

b) 评估信息系统设计实施阶段的信息资源管理，是否编制了涉及系统开发使用和系统建设需采购的软件及硬件设备的详细资产清单，采取资产分类并建立资产管理体系，进行介质加密管理、设备管理及资产信息管理。

有关环境和资源管理方面的具体评估内容要点可参见附录 A 的 A.5.4。

7.2.5.5 安全机制保障管理

信息系统设计实施阶段有关安全机制保障管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段对信息系统用户管理的设计，是否包括用户分类，系统用户授权控制、特权管理、监督性保护，普通用户及敏感信息处理，重要业务用户管理，组织机构外部用户及其特定需求管理，临时用户设置和限制、删除以及审计管理措施；

b) 评估信息系统设计实施阶段对信息系统信息交换的设计，是否包括了不同安全区域信息交换的规范化管理措施，以及高安全信息向低安全域传输的管理措施；

c) 评估信息系统设计实施阶段对运行安全状态监控的设计，是否包括了运行状况、安全、性能集中监控及日志管理措施，对关键区域监视管理措施；

d) 评估信息系统设计实施阶段对信息系统有关安全机制保障管理的设计，是否包括具有审计、证书支持的身份鉴别机制管理，自主访问控制和强制访问控制机制的管理，基于强制控制的系统安全、网络安全、应用系统安全管理，恶意代码防护管理，以及密码算法、密钥管理、以密码技术为基础的安全管理措施；

e) 评估信息系统设计实施阶段对信息系统安全机制集中管理的设计，是否包括系统管理、安全管理、审计管理等安全机制集中控管、安全信息集中管理，安全机制整合的一般功能，安全机制整合的工作方式管理措施，以及安全机制集中管理的分层级联和控管措施。

有关安全机制保障管理方面的具体评估内容要点可参见附录 A 的 A.5.5。

7.2.5.6 业务连续性管理

信息系统设计实施阶段有关业务连续性管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段对数据备份和恢复管理的设计，是否提出了数据备份和恢复管理职责，监督检查办法，设计了数据备份的内容和周期，介质备份及设备备份，系统热备份与冗余，系统远地备份；

b) 评估信息系统设计实施阶段对安全事件处理的设计，是否提出了安全事件内容和划分要求，监督检查办法，设计了安全事件报告和处理程序，以及安全隐患问题报告和防范；

c) 评估信息系统设计实施阶段对应急处理的设计，是否提出了应急处理的管理措施和执行能力，监督检查办法，设计了应急计划框架及具体应急计划。

有关业务连续性管理方面的具体评估内容要点可参见附录 A 的 A.5.6。

7.2.5.7 监督和检查管理

信息系统设计实施阶段的监督和检查管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段的法律符合性，新建或改造信息系统的系统设计、采购控制、开发控制、措施制定、集成及配置、测试及验收是否符合国家有关信息安全法规要求，是否做到知晓适用法律，遵守知识产权要求，防止滥用信息处理设备，保护关键业务应用软件版权，保护组织机构重要记录，遵照国家法规使用密码技术及选择密码技术产品；

b) 评估信息系统设计实施阶段的依从性，新建或改造信息系统的设计方案及实现有关贯彻安全策略和执行技术标准状况，进行全面系统的依从性检查和分析，并持续改进；

c) 评估新建或改造信息系统的设计实施过程是进行了监督控制，是否对设计实施阶段的安全状况进行自查，是否依据国家有关管理规范和技术标准进行保护，接受监管部门的强制监督检查；规划中是否包括了安全审计机制；

d) 评估信息系统设计实施阶段的责任认定，是否明确了新建或改造信息系统的设计实施过程的

管理责任和技术责任，监督检查责任，以及审计及结果处理责任。

有关监督和检查管理方面的具体评估内容要点可参见附录 A 的 A.5.7。

7.2.5.8 建设过程管理

信息系统设计实施阶段的建设过程管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段的建设项目准备，是否明确指定项目负责人，监督和管理系统安全设计、系统采购、系统开发、管理措施制定、集成及配置、测试及验收等全过程（见 7.2.1），具有详细的项目实施计划和过程管理流程，建立工程监理；

b) 评估信息系统设计实施阶段的工程项目外包管理，一般不采取工程项目外包方式，是否在主管部门指定或特定范围内选择具有国家主管部门的资质认证服务资质的信誉较好的厂商，应参照评估机构的选择要求（参见附录 A 的 A.5.3）；具有对项目的保护和控制流程；

c) 评估信息系统设计实施阶段的自行开发环境控制，是否做到开发环境与运行环境分开，开发及测试活动也能分开；是否能够保护好系统开发文档，控制对程序资源库的访问；非自行开发的软件包一般不作修改；应对开发全过程采取相应的保密措施；

d) 评估信息系统设计实施阶段的安全产品采购，是否在国家监管部门许可的产品目录中选择，执行国家有关信息安全等级三级及以上信息安全产品采购规定；

e) 评估信息系统设计实施阶段的建设项目测试验收，是否进行功能、性能和安全性测试，以及约定的安全措施、应急计划、应用指南、操作培训等，具有系统验收要求和标准的定义文档；

f) 评估信息系统设计实施阶段的新系统启用管理，验收后由使用者或管理者提出申请，经过相应领导审批，并进行试运行及其安全评估；对正式启用的系统审计跟踪并进行评价，决定是否继续运行。

有关建设过程管理方面的具体评估内容要点可参见附录 A 的 A.5.8。

7.2.6 第五级信息系统

7.2.6.1 策略和制度管理

信息系统设计实施阶段有关策略和制度管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段的管理目标和范围是否涵盖了设计实施阶段的关键管理环节（见 7.2.1），具有自我持续改进的管理目标和范围；

b) 评估信息系统设计实施阶段提出的信息系统总体安全管理策略，是否确定了信息系统安全总体设计思路，形成了信息系统安全详细设计方案文档，是否达到专控保护的安全管理策略的要求，评估其制定和发布过程；

c) 评估信息系统设计实施阶段是否具有专控保护的安全管理规章制度和操作规程，是否有系统设计、采购、开发、集成、验收管理制度，与系统设计实施的机构和人员管理、风险管理、监督检查管理制度，以及其他管理制度的编制，评估其制定和发布过程；

d) 评估信息系统设计实施阶段的策略与制度文档是否进行了专控保护的评审和修订，以及指定专人保管、限定借阅范围、审批和登记等全面严格保管。

有关策略和制度方面的具体评估内容要点可参见附录 A 的 A.6.1。

7.2.6.2 机构和人员管理

信息系统设计实施阶段有关机构和人员管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段是否有信息安全领导小组和安全职能部门负责，并配备安全管理人员参加，信息安全领导小组是否由主要负责人出任领导，对信息系统规划、定级、立项工作是

否具有安全管理领导职能和信息安全保密监督管理职能；

b) 评估信息系统设计实施阶段是否制定了安全机制集中管理机构人员职责和运行集中管理规范；

c) 评估信息系统设计实施阶段的人员管理是否包括安全管理人员配备、信息系统关键岗位人员管理、人员录用管理、人员离岗管理、人员考核与审查管理，特别是与设计实施有关服务商等第三方人员管理；

d) 评估信息系统设计实施阶段的信息安全教育是否做到应知应会，有计划开展培训，针对不同岗位培训，按人员资质要求培训，培养安全意识自觉性，听取信息安全专家建议，对信息安全专家的管理。

有关机构和人员管理方面的具体评估内容要点可参见附录 A 的 A.6.2。

7.2.6.3 风险管理

信息系统设计实施阶段应根据系统的安全保护等级选择基本安全措施的基础上，依据风险管理的方法补充和调整安全措施，对于设计实施阶段的风险管理，本级评估要求如下：

a) 评估信息系统设计实施阶段是否通过基本的风险管理，提出信息系统安全功能需求，识别系统设计实施过程的风险，对系统建成后的安全功能进行验证；

b) 评估信息系统设计实施阶段是否进行了风险分析，基于信息系统设计方案的资产列表、安全措施，进行安全威胁分析及概率分析列表、系统脆弱性分析，评价安全措施的实现程度，确定安全措施能否抵御现有威胁及脆弱性的影响；

c) 评估新建或改造信息系统的设计实施是否进行了风险控制，包括：

——设计方案是否符合系统建设规划并得到最高管理者的认可，设计方案中的安全需求是否符合规划阶段的安全目标，并基于威胁的分析制定信息系统的总体安全策略，根据设计开发计划及用户需求，对系统涉及的软件、硬件与网络进行分析和选型；

——对开发与技术/产品获取过程的评估和控制，是否包括符合法律、政策、适用标准和指导方针，满足信息系统的功能需要，考虑成本效益风险，通过安全测评和检查；

——系统交付实施过程的评估和控制，是否包括详细分析信息系统资产、面临的威胁和脆弱性，根据系统建设目标和安全需求，对系统的安全功能进行验收测试；评价安全措施能否抵御安全威胁，是否建立了与整体安全策略一致的管理制度；

d) 评估新建或改造信息系统的设计和实施中是否进行了风险决策，对于新建或改造信息系统设计实施中存在的残余风险是否接受，采取残余风险监视措施，做出信息系统投入运行的决定；

e) 评估信息系统设计实施阶段的风险评估主要包括安全建设方案评审和系统测试验收，以及系统的开发与技术/产品获取、系统交付实施等过程，评估结果是否体现在新建或改造信息系统的设计和实施中，是否按资质和信誉选择评估机构，签署保密协议，对评估信息规定交接手续并替换敏感参数，技术检测应经授权并在监督下进行，对评估信息不得带出指定区域。

有关风险管理方面的具体评估内容要点可参见附录 A 的 A.6.3。

7.2.6.4 环境和资源管理

信息系统设计实施阶段有关环境和资源管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段的开发环境的管理，运行环境的设计实施，做到开发环境、测试环境与运行环境物理分开并进行专门管理，是否明确了系统环境的管理部门和职责，采取机房防止电磁泄漏保护的安全管理，对来访人员的控制，标识不同安全区域并隔离，增强门禁控制手段及办公环境管理，启用视频监控和专职警卫；

b) 评估信息系统设计实施阶段的信息资源管理，是否编制了涉及系统开发使用和系统建设需采

购的软件及硬件设备的详细资产清单，采取资产分类并建立资产管理体系，进行介质加密管理、设备管理及资产信息管理。

有关环境和资源管理方面的具体评估内容要点可参见附录 A 的 A.6.4。

7.2.6.5 安全机制保障管理

信息系统设计实施阶段有关安全机制保障管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段对信息系统用户管理的设计，是否包括用户分类，系统用户授权控制、特权管理、监督性保护，普通用户及敏感信息处理，重要业务用户管理，组织机构外部用户及其特定需求管理及限制，临时用户设置和限制、删除以及审计管理措施；

b) 评估信息系统设计实施阶段对信息系统信息交换的设计，是否包括了不同安全区域信息交换的规范化管理措施，以及高安全信息向低安全域传输的管理措施；

c) 评估信息系统设计实施阶段对运行安全状态监控的设计，是否包括了运行状况、安全、性能集中监控及日志管理措施，对关键区域及核心数据监视管理措施；

d) 评估信息系统设计实施阶段对信息系统有关安全机制保障管理的设计，是否包括具有审计、证书支持的身份鉴别机制管理，自主访问控制和强制访问控制机制的管理，基于专门控制的系统安全、网络安全、应用系统安全管理，基于监督检查的恶意代码防护管理，以及密码算法、密钥管理、以密码技术为基础的安全管理措施；

e) 评估信息系统设计实施阶段对信息系统安全机制集中管理的设计，是否包括系统管理、安全管理、审计管理等安全机制集中控管、安全信息集中管理，安全机制整合的一般功能，安全机制整合的工作方式管理措施，以及安全机制集中管理的分层级联和控管措施。

有关安全机制保障管理方面的具体评估内容要点可参见附录 A 的 A.6.5。

7.2.6.6 业务连续性管理

信息系统设计实施阶段有关业务连续性管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段对数据备份和恢复管理的设计，是否提出了数据备份和恢复管理职责，监督检查办法，设计了数据备份的内容和周期，介质备份及设备备份，系统热备份与冗余，系统远地备份；

b) 评估信息系统设计实施阶段对安全事件处理的设计，是否提出了安全事件内容和划分要求，监督检查办法，设计了安全事件报告和处理程序，以及安全隐患问题报告和防范；

c) 评估信息系统设计实施阶段对应急处理的设计，是否提出了应急处理的管理措施和执行能力，监督和持续改进办法，设计了应急计划框架及具体应急计划。

有关业务连续性管理方面的具体评估内容要点可参见附录 A 的 A.6.6。

7.2.6.7 监督和检查管理

信息系统设计实施阶段的监督和检查管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段的法律符合性，新建或改造信息系统的系统设计、采购控制、开发控制、措施制定、集成及配置、测试及验收是否符合国家有关信息安全法规要求，是否做到知晓适用法律，遵守知识产权要求，防止滥用信息处理设备，保护关键业务应用软件版权，保护组织机构重要记录，遵照国家法规使用密码技术及选择密码技术产品；

b) 评估信息系统设计实施阶段的依从性，对新建或改造信息系统的设计方案及实现有关贯彻安全策略和执行技术标准状况，进行全面系统的依从性检查和分析，并持续改进；

c) 评估新建或改造信息系统的设计实施过程是进行了监督控制，是否对设计实施阶段的安全状况进行自查，是否依据国家有关管理规范和技术标准进行保护，接受监管部门的专门监督检

查；规划中是否包括了安全审计机制；

d) 评估信息系统设计实施阶段的责任认定，是否明确了新建或改造信息系统的设计实施过程的管理责任和技术责任，监督检查责任，以及审计及结果处理责任。

有关监督和检查管理方面的具体评估内容要点可参见附录 A 的 A.6.7。

7.2.6.8 建设过程管理

信息系统设计实施阶段的建设过程管理方面，本级评估要求如下：

a) 评估信息系统设计实施阶段的建设项目准备，是否明确指定项目负责人，监督和管理系统安全设计、系统采购、系统开发、管理措施制定、集成及配置、测试及验收等全过程（见 7.2.1），具有详细的项目实施计划和过程管理流程，建立工程监理；

b) 评估信息系统设计实施阶段的工程项目外包管理，一般不采取工程项目外包方式，是否在主管部门指定或特定范围内选择具有国家主管部门的资质认证服务资质的信誉较好的厂商，应参照评估机构的选择要求（参见附录 A 的 A.6.3）；具有对项目的保护和控制流程；

c) 评估信息系统设计实施阶段的自行开发环境控制，是否做到开发环境与运行环境分开，开发及测试活动也能分开；是否能够保护好系统开发文档，控制对程序资源库的访问；非自行开发的软件包一般不作修改；应对开发全过程采取相应的保密措施；

d) 评估信息系统设计实施阶段的安全产品采购，是否在国家监管部门许可的产品目录中选择，执行国家有关信息安全等级三级及以上信息安全产品采购规定；

e) 评估信息系统设计实施阶段的建设项目测试验收，是否进行功能、性能和安全性测试，以及约定的安全措施、应急计划、应用指南、操作培训等，具有系统验收要求和标准的定义文档；

f) 评估信息系统设计实施阶段的新系统启用管理，验收后由使用者或管理者提出申请，经过相应领导审批，并进行试运行及其安全评估；对正式启用的系统审计跟踪并进行评价，决定是否继续运行。

有关建设过程管理方面的具体评估内容要点可参见附录 A 的 A.6.8。

7.3 运行维护管理评估要求

7.3.1 本阶段评估范围

7.3.1.1 评估范围概述

在信息系统运行维护阶段，信息安全管理评估范围包括：

a) 运行维护阶段的关键管理环节：

——运行操作管理；

——系统维护管理；

——安全状态监控；

——业务连续性管理；

——变更控制和外包管理；

——安全检查和持续改进；

b) 运行维护阶段的策略和制度、机构和人员管理等保障措施；

c) 运行维护阶段的环境和资源管理、运行和维护管理、业务连续性管理等日常措施；

d) 运行维护阶段的风险管理、监督和检查管理等监督措施。

7.3.1.2 运行操作管理

对于信息系统运行和维护中的运行操作管理的评估范围包括：

a) 运行操作管理职责确定：通过对信息系统用户分类管理，对运行管理活动或任务的角色划分，并授予相应的操作及管理权限，来确定安全运行管理的具体人员和职责；

b) 运行管理过程控制：通过制定运行操作及管理的规章制度和操作规程，确定信息系统用户和运行管理人员的操作目的、操作内容、操作时间和地点、操作方法和流程等，并进行操作过程记录，使操作过程得到控制。

7.3.1.3 系统维护管理

对于信息系统运行和维护中的常规维护管理的评估范围包括：

a) 日常运行安全管理：包括系统运行的制度化管理，系统运行的风险控制，系统运行的安全审计管理，以及依据安全监控信息进行安全防护；

b) 软件硬件维护管理：包括明确软件硬件维护的责任，进行定期或不定期维护，提高设备完好率；设备送出维修和聘请外部人员前来维修的管理，对维修过程的可监督管理；

c) 外部服务方访问管理：外部服务方访问的申报及审批，进行外部服务方访问的监督、控制和审计管理。

7.3.1.4 安全监控管理

对于信息系统运行维护中的安全状态监控管理的评估范围包括：

a) 确定信息系统安全监控对象：确定可能会对信息系统安全造成影响的网络设备、安全设备、服务器或客户端等，确定监控对象列表；

b) 建立安全监控服务台功能：具有系统安全监控的人员值守，系统事故及安全事件的接报及响应处理的分派；

c) 收集和分析信息系统安全状态信息：收集、识别和记录监控对象安全状态信息，分析发现安全事件及其影响，形成安全状态结果分析报告；

d) 安全机制集中管理：包括对系统资源和运行进行配置、控制和管理，对系统各部分的安全审计机制集中管理，对安全设施的配置、控制和管理，部署一致的安全策略。

7.3.1.5 业务连续性管理

对于信息系统运行维护中的业务连续性管理的评估范围包括：

a) 信息系统备份与恢复：包括对信息系统的数据备份和恢复管理，设备和系统的备份与冗余管理；

b) 安全事件定义与处置：结合信息系统的实际情况将安全事件分级，对安全事件采取适当的方法处置，对安全事件影响进行分析，确定是否启动应急响应；

c) 应急预案制定与实施：在统一的应急预案框架下制定不同安全事件的应急预案，确定应急预案对象，明确各自责任，制定应急响应流程及应急预案执行条件。

7.3.1.6 变更和外包管理

对信息系统运行维护中的变更控制和外包管理的评估范围包括：

a) 变更需求和影响分析：分析变更需求和影响，确定变更的内容、资源需求和范围，判断变更的必要性和可行性，提出变更方案；

b) 变更过程控制：审批变更方案，收集变更过程的各类相关文档和记录，整理、分析和总结各类数据，形成变更结果报告，并归档保存；

c) 运行维护中的外包管理：包括外包服务商的选择，签署外包服务的书面合同，对外包服务的监控和评估。

7.3.1.7 安全检查监督管理

对信息系统运行维护中的安全检查监督管理的评估范围包括：

a) 制定检查方案：明确安全检查的范围、对象、方法、计划，准备安全检查需要的各类表单和工具；包括法律符合性、策略和技术依从性检查，审计及监管控制，责任认定；

b) 实施安全检查：检查安全状况，记录检查活动及结果数据，分析安全措施的有效性、安全事件的可能性和信息系统的改进需求；

c) 安全检查报告：总结检查结果，提出改进建议，形成安全检查报告，并归档保存检查过程文档资料。

7.3.2 第一级信息系统

7.3.2.1 策略和制度管理

信息系统运行维护阶段有关策略和制度管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的管理目标和范围是否涵盖了运行维护阶段的关键管理环节（见7.3.1），具有基本的管理目标和范围；

b) 评估信息系统运行维护阶段提出的信息系统总体安全管理策略，是否确定了信息系统安全运行和维护的总体思路，形成了信息系统安全运维整体管理办法文档，是否达到基本的安全管理策略的要求，评估其制定和发布过程；

c) 评估信息系统运行维护阶段是否具有基本的安全管理规章制度，是否有系统运行操作、系统维护、安全状态监控、业务连续性、变更控制、外包管理制度，与系统运行维护相关的机构和人员管理、风险管理、监督检查管理制度，评估其制定和发布过程；

d) 评估信息系统运行维护阶段的策略与制度文档是否进行了基本的评审和修订，以及指定专人保管。

有关策略和制度方面的具体评估内容要点可参见附录A的A.2.1。

7.3.2.2 机构和人员管理

信息系统阶段有关机构和人员管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段是否有分管领导负责，并配备安全管理人员参加，对信息系统运行维护是否具有基本安全管理职能；

b) 评估信息系统运行维护阶段的人员管理是否包括安全管理人员配备、信息系统关键岗位人员管理、人员录用管理、人员离岗管理、人员考核与审查管理，特别是与运行维护有关服务商等第三方人员管理；

c) 评估信息系统运行维护阶段的信息安全教育是否做到应知应会，能够听取信息安全专家建议。

有关机构和人员管理方面的具体评估内容要点可参见附录A的A.2.2。

7.3.2.3 风险管理

信息系统运行维护阶段有关风险管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段是否通过基本的风险管理，了解和控制信息系统运行维护过程中的安全风险，具有基本的风险管理策略；

b) 评估信息系统运行维护阶段是否进行了风险分析，基于真实运行的信息系统的资产、威胁、脆弱性，分析安全威胁，评价安全措施的实现程度，确定安全措施能否抵御现有威胁及脆弱性的影响；

c) 评估信息系统的运行维护是否进行了风险控制，包括：

——资产识别，包括实施阶段采购的软硬件资产、系统运行过程中生成的信息资产、相关的人员与服务等，也是前期资产识别的补充与增加；

——分析威胁的可能性和影响程度，对非故意威胁导致安全事件考虑其发生频率，对故意威胁导致安全事件考虑威胁的各个影响因素作出判断；

——脆弱性分析，包括运行环境中物理、网络、系统、应用、安全保障设备、管理等各方面的脆弱性，考虑安全功能的实现情况和安全保障设备本身的脆弱性；

——对重要资产的风险进行分析，描述不同资产的风险高低状况，调整和完善信息系统运行维护的安全管理措施；

d) 评估信息系统的运行维护中是否进行了风险决策，对于信息系统运行维护中存在的残余风险是否接受；

e) 评估信息系统运行维护阶段的风险评估是否定期或发生重大变更时执行，主要包括对真实运行的信息系统及资产、威胁、脆弱性等各方面；评估结果是否体现在信息系统的运行维护改进中，是否按资质和信誉选择评估机构，签署保密协议，对评估信息规定交接手续。

有关风险管理方面的具体评估内容要点可参见附录 A 的 A.2.3。

7.3.2.4 环境和资源管理

信息系统运行维护阶段有关环境和资源管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的运行环境的管理，是否明确系统环境的管理部门和职责，机房的安全管理措施；

b) 评估信息系统运行维护阶段的信息资源管理，是否编制了信息系统软件、硬件设备和信息资产的基本资产清单，进行了基本的介质管理、设备管理；

c) 评估信息系统运行维护阶段使用的安全产品，是否属于国家监管部门许可的产品目录中列出安全产品(参见附录 A 的 A.2.8)。

有关环境和资源管理方面的具体评估内容要点可参见附录 A 的 A.2.4。

7.3.2.5 日常运维管理

信息系统运行维护阶段有关日常运维管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的用户管理，是否包括用户分类清单编制，系统用户最小授权控制，普通用户基本管理，组织机构外部用户基本管理，临时用户设置与删除管理；

b) 评估信息系统运行维护阶段的运行操作管理，是否包括服务器、终端计算机、便携机操作的基本管理，网络及安全设备操作的基本管理，业务应用操作程序和权限控制，变更控制的申报和审批，信息交换的基本管理；

c) 评估信息系统运行维护阶段的运行维护管理，是否包括系统运行的基本安全管理，对运行状况监控日志管理，软件硬件维护的责任，外部服务方访问的审批控制；

d) 评估信息系统运行维护阶段的外包服务管理，是否包括外包服务合同基本管理，外包服务商基本管理，以及外包服务监控管理；

e) 评估信息系统运行维护阶段的有关安全机制的保障，是否包括身份鉴别机制基本管理，自主访问控制机制的管理，系统安全基本管理，网络安全基本管理，应用系统安全基本管理，以及病毒防护基本管理。

有关日常运维管理方面的具体评估内容要点可参见附录 A 的 A.2.5。

7.3.2.6 业务连续性管理

信息系统运行维护阶段有关业务连续性管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的数据备份和恢复管理，是否明确了数据备份和恢复管理职责，规定并执行了数据备份的内容和周期要求；
b) 评估信息系统运行维护阶段的安全事件处理，是否明确了安全事件内容和划分要求，规定并执行了安全事件报告和处理程序；
c) 评估信息系统运行维护阶段的应急处理，是否明确了应急处理的基本管理措施，规定了应急计划框架及具体应急计划的责任，编制和落实了应急计划。

有关业务连续性管理方面的具体评估内容要点可参见附录 A 的 A.2.6。

7.3.2.7 监督和检查管理

信息系统运行维护阶段的监督和检查管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的法律符合性，信息系统的运行操作、日常维护、安全监控、业务连续性、变更控制、外包管理、安全检查是否符合国家有关信息安全法规要求，是否做到知晓适用法律，遵守知识产权要求，保护组织机构重要记录；
b) 评估信息系统运行维护阶段的监督控制，是否对运行维护阶段的安全状况进行自查，是否依据国家有关管理规范和技术标准进行保护。

有关监督和检查管理方面的具体评估内容要点可参见附录 A 的 A.2.7。

7.3.3 第二级信息系统

7.3.3.1 策略和制度管理

信息系统运行维护阶段有关策略和制度管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的管理目标和范围是否涵盖了运行维护阶段的关键管理环节(见7.3.1)，具有较完整的管理目标和范围；
b) 评估信息系统运行维护阶段提出的信息系统总体安全管理策略，是否确定了信息系统安全运行和维护的总体思路，形成了信息系统安全运维整体管理办法文档，是否达到较完整的安全管理策略的要求，评估其制定和发布过程；
c) 评估信息系统运行维护阶段是否具有较完整的安全管理规章制度和操作规程，是否有系统运行操作、系统维护、安全状态监控、业务连续性、变更控制、外包管理制度，与系统运行维护相关的机构和人员管理、风险管理、监督检查管理制度，评估其制定和发布过程；
d) 评估信息系统运行维护阶段的策略与制度文档是否进行了较完整的评审和修订，以及指定专人保管、借阅审批和登记。

有关策略和制度方面的具体评估内容要点可参见附录 A 的 A.3.1。

7.3.3.2 机构和人员管理

信息系统运行维护阶段有关机构和人员管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段是否有分管领导和信息安全职能部门负责，并配备安全管理人员参加，对信息系统运行维护是否具有安全管理领导职能；
b) 评估信息系统运行维护阶段的人员管理是否包括安全管理人员配备、信息系统关键岗位人员管理、人员录用管理、人员离岗管理、人员考核与审查管理，特别是与运行维护有关服务商等第三方人员管理；
c) 评估信息系统运行维护阶段的信息安全教育是否做到应知应会，有计划开展培训，能够听取信息安全专家建议。

有关机构和人员管理方面的具体评估内容要点可参见附录 A 的 A.3.2。

7.3.3.3 风险管理

信息系统运行维护阶段有关风险管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段是否通过基本的风险管理，了解和控制信息系统运行维护过程中的安全风险，具有风险管理策略；

b) 评估信息系统运行维护阶段是否进行了风险分析，基于真实运行的信息系统的资产列表、安全措施，进行安全威胁分析及概率分析列表、系统脆弱性分析，以及安全测试，评价安全措施的实现程度，确定安全措施能否抵御现有威胁及脆弱性的影响；

c) 评估信息系统的运行维护是否进行了风险控制，包括：

——资产识别，包括实施阶段采购的软硬件资产、系统运行过程中生成的信息资产、相关的人员与服务等，也是前期资产识别的补充与增加；

——分析威胁的可能性和影响程度，对非故意威胁导致安全事件考虑其发生频率，对故意威胁导致安全事件考虑威胁的各个影响因素作出判断；

——脆弱性分析，包括运行环境中物理、网络、系统、应用、安全保障设备、管理等各方面的脆弱性，考虑安全功能的实现情况和安全保障设备本身的脆弱性；

——对重要资产的风险进行分析，描述不同资产的风险高低状况，调整和完善信息系统运行维护的安全管理措施；

d) 评估信息系统的运行维护中是否进行了风险决策，对于信息系统运行维护中存在的残余风险是否接受，以及信息系统投入运行的决定；

e) 评估信息系统运行维护阶段的风险评估是否定期或发生重大变更时执行，主要包括对真实运行的信息系统及资产、威胁、脆弱性等各方面；评估结果是否体现在信息系统的运行维护改进中，是否按资质和信誉选择评估机构，签署保密协议，对评估信息规定交接手续并替换敏感参数，技术检测应经授权并在监督下进行。

有关风险管理方面的具体评估内容要点可参见附录 A 的 A.3.3。

7.3.3.4 环境和资源管理

信息系统运行维护阶段有关环境和资源管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的运行环境的管理，是否明确系统环境的管理部门和职责，机房及办公环境的安全管理措施，对来访人员的控制管理；

b) 评估信息系统运行维护阶段的信息资源管理，是否编制了信息系统软件、硬件设备和信息资产的详细资产清单，采取资产分类，进行了介质管理、设备管理；

c) 评估信息系统运行维护阶段使用的安全产品，是否属于国家监管部门许可的产品目录中列出安全产品(见附录 A 的 A.3.8)。

有关环境和资源管理方面的具体评估内容要点可参见附录 A 的 A.3.4。

7.3.3.5 日常运维管理

信息系统运行维护阶段有关日常运维管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的用户管理，是否包括用户分类清单编制，系统用户最小授权控制及特权管理，普通用户及其处理敏感信息管理，组织机构外部用户及其特定需求管理，临时用户设置、删除及审计管理；

b) 评估信息系统运行维护阶段的运行操作管理，是否包括服务器及日志文件和监控、权限管理，终端计算机、便携机操作及限制管理，网络及安全设备操作、策略配置及检查管理，业务应用操作程序和权限控制，变更控制、设备重用、信息交换的规范化管理；

c) 评估信息系统运行维护阶段的运行维护管理，是否包括系统运行的制度化管理，对运行状况、安全、性能监控及日志管理，软件硬件维护责任及送外维修要求，外部服务方访问的制度化管理；

d) 评估信息系统运行维护阶段的外包服务管理，是否包括外包服务合同基本管理，外包服务商的选择及管理，以及外包服务监控和评估管理；

e) 评估信息系统运行维护阶段的有关安全机制的保障，是否包括具有审计支持的身份鉴别机制管理，自主访问控制机制的管理，系统安全管理，网络安全管理，应用系统安全管理，病毒防护管理，以及密码算法和密钥管理。

有关日常运维管理方面的具体评估内容要点可参见附录 A 的 A.3.5。

7.3.3.6 业务连续性管理

信息系统运行维护阶段有关业务连续性管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的数据备份和恢复管理，是否明确了数据备份和恢复管理职责，规定并执行了数据备份的内容、周期要求和检查，备份介质及其恢复的检查，设备备份；

b) 评估信息系统运行维护阶段的安全事件处理，是否明确了安全事件内容和划分要求，规定了安全事件报告和处理程序，是否按照程序处置安全事件，以及安全隐患问题报告和防范；

c) 评估信息系统运行维护阶段的应急处理，是否明确了应急处理的制度化管理，规定了应急计划框架及应急计划的责任和能力，编制并落实了应急计划。

有关业务连续性管理方面的具体评估内容要点可参见附录 A 的 A.3.6。

7.3.3.7 监督和检查管理

信息系统运行维护阶段的监督和检查管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的法律符合性，信息系统的运行操作、日常维护、安全监控、业务连续性、变更控制、外包管理、安全检查是否符合国家有关信息安全法规要求，是否做到知晓适用法律，遵守知识产权要求，防止滥用信息处理设备，保护业务应用软件版权，保护组织机构重要记录；

b) 评估信息系统运行维护阶段的依从性，对信息系统的运行和维护过程中有关贯彻安全策略和执行技术标准状况，进行依从性检查和分析；

c) 评估信息系统运行维护阶段的监督控制，是否对运行维护阶段的安全状况定期进行自查，是否依据国家有关管理规范和技术标准进行保护，接受监管部门的指导；信息系统的运行和维护是否具有审计机制；

d) 评估信息系统运行维护阶段的责任认定，是否明确了信息系统的运行和维护过程的管理责任和技术责任，监督检查责任，以及审计及结果处理责任。

有关监督和检查管理方面的具体评估内容要点可参见附录 A 的 A.3.7。

7.3.4 第三级信息系统

7.3.4.1 策略和制度管理

信息系统运行维护阶段有关策略和制度管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的管理目标和范围是否涵盖了运行维护阶段的关键管理环节（见7.3.1），具有完好定义的管理目标和范围；

b) 评估信息系统运行维护阶段提出的信息系统总体安全管理策略，是否确定了信息系统安全运行和维护的总体思路，形成了信息系统安全运维整体管理办法文档，是否达到体系化的安全管

理策略的要求，评估其制定和发布过程；

c) 评估信息系统运行维护阶段是否具有体系化的安全管理规章制度和操作规程，是否有系统运行操作、系统维护、安全状态监控、业务连续性、变更控制、外包管理制度，与系统运行维护相关的机构和人员管理、风险管理、监督检查管理制度，评估其制定和发布过程；

d) 评估信息系统运行维护阶段的策略与制度文档是否进行了体系化的评审和修订，以及指定专人保管、限定借阅范围、审批和登记。

有关策略和制度方面的具体评估内容要点可参见附录 A 的 A.4.1。

7.3.4.2 机构和人员管理

信息系统运行维护阶段有关机构和人员管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段是否有信息安全领导小组和安全职能部门负责，并配备安全管理人员参加，对信息系统运行维护是否具有安全管理领导职能；

b) 评估信息系统规划立项阶段是否包括对安全机制集中管理机构人员管理和运行集中管理；

c) 评估信息系统运行维护阶段的人员管理是否包括安全管理人员配备、信息系统关键岗位人员管理、人员录用管理、人员离岗管理、人员考核与审查管理，特别是与运行维护有关服务商等第三方人员管理；

d) 评估信息系统运行维护阶段的信息安全教育是否做到应知应会，有计划开展培训，针对不同岗位培训，能够听取信息安全专家建议。

有关机构和人员管理方面的具体评估内容要点可参见附录 A 的 A.4.2。

7.3.4.3 风险管理

信息系统运行维护阶段有关风险管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段是否通过基本的风险管理，了解和控制信息系统运行维护过程中的安全风险，具有风险管理策略及其监督机制；

b) 评估信息系统运行维护阶段是否进行了风险分析，基于真实运行的信息系统的资产列表、安全措施，进行安全威胁分析及概率分析列表、系统脆弱性分析，以及安全测试，建立并维护风险信息库，评价安全措施的实现程度，确定安全措施能否抵御现有威胁及脆弱性的影响；

c) 评估信息系统的运行维护是否进行了风险控制，包括：

——资产识别，包括实施阶段采购的软硬件资产、系统运行过程中生成的信息资产、相关的人员与服务等，也是前期资产识别的补充与增加；

——分析威胁的可能性和影响程度，对非故意威胁导致安全事件考虑其发生频率，对故意威胁导致安全事件考虑威胁的各个影响因素作出判断；

——脆弱性分析，包括运行环境中物理、网络、系统、应用、安全保障设备、管理等各方面的脆弱性，考虑安全功能的实现情况和安全保障设备本身的脆弱性；

——对重要资产的风险进行分析，描述不同资产的风险高低状况，调整和完善信息系统运行维护的安全管理措施；

d) 评估信息系统的运行维护中是否进行了风险决策，对于信息系统运行维护中存在的残余风险是否接受，采取残余风险监视措施，做出信息系统投入运行的决定；以及安全风险再评估，采取信息系统受控运行；

e) 评估信息系统运行维护阶段的风险评估是否定期或发生重大变更时执行，主要包括对真实运行的信息系统及资产、威胁、脆弱性等各方面；评估结果是否体现在信息系统的运行维护改进中，是否按资质和信誉选择评估机构，签署保密协议，对评估信息规定交接手续并替换敏感参数，技术检测应经授权并在监督下进行或由被评估方操作，对评估机构专人监督检查，对评估

信息不得带出指定区域。

有关风险管理方面的具体评估内容要点可参见附录 A 的 A.4.3。

7.3.4.4 环境和资源管理

信息系统运行维护阶段有关环境和资源管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的运行环境的管理，是否明确系统环境的管理部门和职责，机房及办公环境的安全管理措施，对来访人员的控制，标识不同安全区域，配置门禁控制手段；

b) 评估信息系统运行维护阶段的信息资源管理，是否编制了信息系统软件、硬件设备和信息资产的详细资产清单，采取资产分类，进行了介质管理、设备管理及资产信息管理；

c) 评估信息系统运行维护阶段使用的安全产品，是否属于国家监管部门许可的产品目录中列出安全产品，是否执行国家有关信息安全等级三级及以上信息安全产品使用规定(参见附录 A 的 A.4.8)。

有关环境和资源管理方面的具体评估内容要点可参见附录 A 的 A.4.4。

7.3.4.5 日常运维管理

信息系统运行维护阶段有关日常运维管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的用户管理，是否包括用户分类清单编制，系统用户最小授权控制及特权管理、监督性保护，普通用户及其处理敏感信息管理，重要业务用户管理，组织机构外部用户及其特定需求管理，临时用户设置及限制、删除及审计管理；

b) 评估信息系统运行维护阶段的运行操作管理，是否包括服务器及日志文件和监控、权限管理、配置文件管理，终端计算机、便携机操作及限制管理，网络及安全设备操作、策略配置及检查管理，业务应用操作程序、权限控制和监督，变更控制、设备重用的规范化管理，不同安全区域之间信息交换管理，高安全信息向低安全域传输管理网络及安全设备安全机制集中管理；

c) 评估信息系统运行维护阶段的运行维护管理，是否包括系统运行的制度化管理及风险评估，对运行状况、安全、性能监控及日志管理，软件硬件维护责任、送外维修要求、可监督的维修过程，外部服务方访问的制度化管理及风险评估；

d) 评估信息系统运行维护阶段的外包服务管理，是否包括外包服务的限制，外包服务合同基本管理，外包服务商的选择及管理，以及外包服务监控和评估管理；

e) 评估信息系统运行维护阶段的有关安全机制的保障，是否包括具有审计、证书支持的身份鉴别机制管理，自主访问控制和强制访问控制机制的管理，系统安全管理，网络安全管理，应用系统安全管理，病毒防护管理，以及密码算法、密钥管理、以密码技术为基础的安全管理；

f) 评估信息系统运行维护阶段的安全机制集中管理，是否包括系统管理、安全管理、审计管理等安全机制集中控管，安全信息集中管理，安全机制整合的一般功能，安全机制整合的工作方式管理。

有关日常运维管理方面的具体评估内容要点可参见附录 A 的 A.4.5。

7.3.4.6 业务连续性管理

信息系统运行维护阶段有关业务连续性管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的数据备份和恢复管理，是否包括数据备份的内容、周期要求和检查，备份介质及其恢复的检查，设备备份、系统热备份与冗余；

b) 评估信息系统运行维护阶段的安全事件处理，是否包括安全事件内容和划分，安全事件报告和处理程序，是否按照程序处置安全事件，安全隐患问题报告和防范，以及强化事件处理责任的认定；

c) 评估信息系统运行维护阶段的应急处理，是否包括应急处理的系统化管理，应急计划框架，以及应急计划的责任和能力。

有关业务连续性管理方面的具体评估内容要点可参见附录 A 的 A.4.6。

7.3.4.7 监督和检查管理

信息系统运行维护阶段的监督和检查管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的法律符合性，信息系统的运行操作、日常维护、安全监控、业务连续性、变更控制、外包管理、安全检查是否符合国家有关信息安全法规要求，是否做到知晓适用法律，遵守知识产权要求，防止滥用信息处理设备，保护关键业务应用软件版权，保护组织机构重要记录，遵照国家法规使用密码技术；

b) 评估信息系统运行维护阶段的依从性，对信息系统的运行和维护过程中有关贯彻安全策略和执行技术标准状况，进行全面系统的依从性检查和分析；

c) 评估信息系统运行维护阶段的监督控制，是否对运行维护阶段的安全状况定期进行自查，是否依据国家有关管理规范和技术标准进行保护，接受监管部门的监督检查；信息系统的运行和维护是否具有审计机制；

d) 评估信息系统运行维护阶段的责任认定，是否明确了信息系统的运行和维护过程的管理责任和技术责任，监督检查责任，以及审计及结果处理责任。

有关监督和检查管理方面的具体评估内容要点可参见附录 A 的 A.4.7。

7.3.5 第四级信息系统

7.3.5.1 策略和制度管理

信息系统运行维护阶段有关策略和制度管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的管理目标和范围是否涵盖了运行维护阶段的关键管理环节(见7.3.1)，具有量化控制的管理目标和范围；

b) 评估信息系统运行维护阶段提出的信息系统总体安全管理策略，是否确定了信息系统安全运行和维护的总体思路，形成了信息系统安全运维整体管理办法文档，是否达到强制保护的安全管理策略的要求，评估其制定和发布过程；

c) 评估信息系统运行维护阶段是否具有强制保护的安全管理规章制度和操作规程，是否有系统运行操作、系统维护、安全状态监控、业务连续性、变更控制、外包管理制度，与系统运行维护相关的机构和人员管理、风险管理、监督检查管理制度，评估其制定和发布过程；

d) 评估信息系统运行维护阶段的策略与制度文档是否进行了强制保护的评审和修订，以及指定专人保管、限定借阅范围、审批和登记等全面严格保管。

有关策略和制度方面的具体评估内容要点可参见附录 A 的 A.5.1。

7.3.5.2 机构和人员管理

信息系统运行维护阶段有关机构和人员管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段是否有信息安全领导小组和安全职能部门负责，并配备安全管理人员参加，安全领导小组是否由主要负责人出任领导，对信息系统运行维护是否具有安全管理领导职能；

b) 评估信息系统运行维护阶段是否包括对安全机制集中管理机构人员管理和运行集中管理；

c) 评估信息系统运行维护阶段的人员管理是否包括安全管理人员配备、信息系统关键岗位人员管理、人员录用管理、人员离岗管理、人员考核与审查管理，特别是与运行维护有关服务商等第

三方人员管理；

d) 评估信息系统运行维护阶段的信息安全教育是否做到应知应会，有计划开展培训，针对不同岗位培训，听取信息安全专家建议，对信息安全专家的管理。

有关机构和人员管理方面的具体评估内容要点可参见附录 A 的 A.5.2。

7.3.5.3 风险管理

信息系统运行维护阶段有关风险管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段是否通过基本的风险管理，了解和控制信息系统运行维护过程中的安全风险，具有风险管理策略及其监督机制；

b) 评估信息系统运行维护阶段是否进行了风险分析，基于真实运行的信息系统的资产列表、安全措施，进行安全威胁分析及概率分析列表、系统脆弱性分析，以及安全测试，建立并维护风险信息库，评价安全措施的实现程度，确定安全措施能否抵御现有威胁及脆弱性的影响；

c) 评估信息系统的运行维护是否进行了风险控制，包括：

——资产识别，包括实施阶段采购的软硬件资产、系统运行过程中生成的信息资产、相关的人员与服务等，也是前期资产识别的补充与增加；

——分析威胁的可能性和影响程度，对非故意威胁导致安全事件考虑其发生频率，对故意威胁导致安全事件考虑威胁的各个影响因素作出判断；

——脆弱性分析，包括运行环境中物理、网络、系统、应用、安全保障设备、管理等各方面的脆弱性，考虑安全功能的实现情况和安全保障设备本身的脆弱性；

——对重要资产的风险进行分析，描述不同资产的风险高低状况，调整和完善信息系统运行维护的安全管理措施；

d) 评估信息系统的运行维护中是否进行了风险决策，对于信息系统运行维护中存在的残余风险是否接受，采取残余风险监视措施，做出信息系统投入运行的决定；以及安全风险再评估，采取信息系统受控运行；

e) 评估信息系统运行维护阶段的风险评估是否定期或发生重大变更时执行，主要包括对真实运行的信息系统及资产、威胁、脆弱性等各方面；评估结果是否体现在信息系统的运行维护改进中，是否按资质和信誉选择评估机构，签署保密协议，对评估信息规定交接手续并替换敏感参数，技术检测应经授权并在监督下进行或由被评估方操作，对评估机构专人监督检查，对评估信息不得带出指定区域。

有关风险管理方面的具体评估内容要点可参见附录 A 的 A.5.3。

7.3.5.4 环境和资源管理

信息系统运行维护阶段有关环境和资源管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的运行环境的管理，是否明确系统环境的管理部门和职责，机房及办公环境的安全管理，对来访人员的控制，标识不同安全区域并隔离，增强门禁控制手段，启用视频监控和专职警卫；

b) 评估信息系统运行维护阶段的信息资源管理，是否编制了信息系统软件、硬件设备和信息资产的详细资产清单，采取资产分类并建立资产管理体系，进行介质加密管理、设备管理及资产信息管理；

c) 评估信息系统运行维护阶段使用的安全产品，是否属于国家监管部门许可的产品目录中列出安全产品，是否执行国家有关信息安全等级三级及以上信息安全产品使用规定（见附录 A 的 A.5.8）。

有关环境和资源管理方面的具体评估内容要点可参见附录 A 的 A.5.4。

7.3.5.5 日常运维管理

信息系统运行维护阶段有关日常运维管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的用户管理，是否包括用户分类清单编制，系统用户最小授权控制及特权管理、监督性保护，普通用户及其处理敏感信息管理，重要业务用户管理，组织机构外部用户及其特定需求管理、限制，临时用户设置及限制、删除及审计管理；

b) 评估信息系统运行维护阶段的运行操作管理，是否包括服务器及日志文件和监控、权限管理、配置文件管理，终端计算机、便携机操作及限制管理，网络及安全设备操作、策略配置及检查管理，业务应用操作程序、权限控制和监督，变更控制、设备重用的管理及安全审计，不同安全区域之间信息交换管理，高安全信息向低安全域传输管理，网络及安全设备安全机制集中管理；

c) 评估信息系统运行维护阶段的运行维护管理，是否包括系统运行的制度化管理及风险评估，对运行状况、安全、性能监控及日志管理，软件硬件维护责任、维修过程的可监督及强制管理，外部服务方访问的限制及风险管理；

d) 评估信息系统运行维护阶段的外包服务管理，是否包括外包服务的限制，外包服务合同基本管理，外包服务商的选择及管理，以及外包服务监控和评估管理；

e) 评估信息系统运行维护阶段的有关安全机制的保障，是否包括具有审计、证书支持的身份鉴别机制强制管理，自主访问控制和强制访问控制机制的监控管理，基于强制的系统安全管理、网络安全管理，基于强制的应用系统安全管理，基于监督检查的病毒防护管理，以及密码算法、密钥管理、以密码技术为基础的安全管理；

f) 评估信息系统运行维护阶段的安全机制集中管理，是否包括系统管理、安全管理、审计管理等安全机制集中控管、安全信息集中的强制管理，安全机制整合的一般功能，安全机制整合的工作方式管理，以及安全机制集中管理的分层级联和控管。

有关日常运维管理方面的具体评估内容要点可参见附录 A 的 A.5.5。

7.3.5.6 业务连续性管理

信息系统运行维护阶段有关业务连续性管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的数据备份和恢复管理，是否明确了数据备份和恢复管理职责，规定并执行了数据备份的内容、周期要求和检查，备份介质及其恢复的操作过程监督检查，设备备份、系统热备份与冗余、系统远地备份；

b) 评估信息系统运行维护阶段的安全事件处理，是否明确了安全事件内容和划分要求，规定了安全事件报告和处理程序，是否按照程序处置安全事件，安全隐患问题报告和防范，以及强化事件处理责任的认定；

c) 评估信息系统运行维护阶段的应急处理，是否明确了应急处理的强制保护管理，规定了应急计划框架及具体应急计划的责任、能力进行监督，编制并落实了应急计划。

有关业务连续性管理方面的具体评估内容要点可参见附录 A 的 A.5.6。

7.3.5.7 监督和检查管理

信息系统运行维护阶段的监督和检查管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的法律符合性，信息系统的运行操作、日常维护、安全监控、业务连续性、变更控制、外包管理、安全检查是否符合国家有关信息安全法规要求，是否做到知晓适用法律，遵守知识产权要求，防止滥用信息处理设备，保护关键业务应用软件版权，保护组织机构重要记录，遵照国家法规使用密码技术；

b) 评估信息系统运行维护阶段的依从性，对信息系统的运行和维护过程中有关贯彻安全策略和

执行技术标准状况，进行全面系统的依从性检查和分析，并持续改进；

c) 评估信息系统运行维护阶段的监督控制，是否对运行维护阶段的安全状况定期进行自查，是否依据国家有关管理规范和技术标准进行保护，接受监管部门的强制监督检查；信息系统的运行和维护是否具有审计机制；

d) 评估信息系统运行维护阶段的责任认定，是否明确了信息系统的运行和维护过程的管理责任和技术责任，监督检查责任，以及审计及结果处理责任。

有关监督和检查管理方面的具体评估内容要点可参见附录 A 的 A.5.7。

7.3.6 第五级信息系统

7.3.6.1 策略和制度管理

信息系统运行维护阶段有关策略和制度管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的管理目标和范围是否涵盖了运行维护阶段的关键管理环节（见7.3.1），具有自我持续改进的管理目标和范围；

b) 评估信息系统运行维护阶段提出的信息系统总体安全管理策略，是否确定了信息系统安全运行和维护的总体思路，形成了信息系统安全运维整体管理办法文档，是否达到专控保护的安全管理策略的要求，评估其制定和发布过程；

c) 评估信息系统运行维护阶段是否具有专控保护的安全管理规章制度和操作规程，是否有系统运行操作、系统维护、安全状态监控、业务连续性、变更控制、外包管理制度，与系统运行维护相关的机构和人员管理、风险管理、监督检查管理制度，评估其制定和发布过程；

d) 评估信息系统运行维护阶段的策略与制度文档是否进行了专控保护的评审和修订，以及指定专人保管、限定借阅范围、审批和登记等全面严格保管。

有关策略和制度方面的具体评估内容要点可参见附录 A 的 A.6.1。

7.3.6.2 机构和人员管理

信息系统运行维护阶段有关机构和人员管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段是否有信息安全领导小组和安全职能部门负责，并配备安全管理人员参加，安全领导小组是否由主要负责人出任领导，对信息系统运行维护是否具有安全管理领导职能和信息安全保密监督管理职能；

b) 评估信息系统运行维护阶段是否包括对安全机制集中管理机构人员管理和运行集中管理；

c) 评估信息系统运行维护阶段的人员管理是否包括安全管理人员配备、信息系统关键岗位人员管理、人员录用管理、人员离岗管理、人员考核与审查管理，特别是与运行维护有关服务商等第三方人员管理；

d) 评估信息系统运行维护阶段的信息安全教育是否做到应知应会，有计划开展培训，针对不同岗位培训，按人员资质要求培训，培养安全意识自觉性，听取信息安全专家建议，对信息安全专家的管理。

有关机构和人员管理方面的具体评估内容要点可参见附录 A 的 A.6.2。

7.3.6.3 风险管理

信息系统运行维护阶段有关风险管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段是否通过基本的风险管理，了解和控制信息系统运行维护过程中的安全风险，具有风险管理策略及其监督机制；

b) 评估信息系统运行维护阶段是否进行了风险分析，基于真实运行的信息系统的资产列表、安

全措施，进行安全威胁分析及概率分析列表、系统脆弱性分析，以及安全测试，建立并维护风险信息库，评价安全措施的实现程度，确定安全措施能否抵御现有威胁及脆弱性的影响；

c) 评估信息系统的运行维护是否进行了风险控制，包括：

——资产识别，包括实施阶段采购的软硬件资产、系统运行过程中生成的信息资产、相关的人员与服务等，也是前期资产识别的补充与增加；

——分析威胁的可能性和影响程度，对非故意威胁导致安全事件考虑其发生频率，对故意威胁导致安全事件考虑威胁的各个影响因素作出判断；

——脆弱性分析，包括运行环境中物理、网络、系统、应用、安全保障设备、管理等各方面的脆弱性，考虑安全功能的实现情况和安全保障设备本身的脆弱性；

——对重要资产的风险进行分析，描述不同资产的风险高低状况，调整和完善信息系统运行维护的安全管理措施；

d) 评估信息系统的运行维护中是否进行了风险决策，对于信息系统运行维护中存在的残余风险是否接受，采取残余风险监视措施，做出信息系统投入运行的决定；以及安全风险再评估，采取信息系统受控运行；

e) 评估信息系统运行维护阶段的风险评估是否定期或发生重大变更时执行，主要包括对真实运行的信息系统及资产、威胁、脆弱性等各方面；评估结果是否体现在信息系统的运行维护改进中，是否按资质和信誉选择评估机构，签署保密协议，对评估信息规定交接手续并替换敏感参数，技术检测应经授权并在监督下进行或由被评估方操作，对评估机构专人监督检查，对评估信息不得带出指定区域。

有关风险管理方面的具体评估内容要点可参见附录 A 的 A.6.3。

7.3.6.4 环境和资源管理

信息系统运行维护阶段有关环境和资源管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的运行环境的管理，是否明确系统环境的管理部门和职责，机房采取防止电磁泄漏保护的安全管理，对来访人员的控制，标识不同安全区域并隔离，增强门禁控制手段及办公环境管理，启用视频监控和专职警卫；

b) 评估信息系统运行维护阶段的信息资源管理，是否编制了信息系统软件、硬件设备和信息资产的详细资产清单，采取资产分类并建立资产管理体系，进行介质加密管理、设备管理及资产信息管理；

c) 评估信息系统运行维护阶段使用的安全产品，是否属于国家监管部门许可的产品目录中列出安全产品，是否执行国家有关信息安全等级三级及以上信息安全产品使用规定（参见附录 A 的 A.6.8）。

有关环境和资源管理方面的具体评估内容要点可参见附录 A 的 A.6.4。

7.3.6.5 日常运维管理

信息系统运行维护阶段有关日常运维管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的用户管理，是否包括用户分类清单编制，系统用户最小授权控制及特权管理、监督性保护，普通用户及其处理敏感信息管理，重要业务用户管理，组织机构外部用户及其特定需求管理、限制，临时用户设置及限制、删除及审计管理；

b) 评估信息系统运行维护阶段的运行操作管理，是否包括服务器及日志文件和监控、权限管理、配置文件管理，终端计算机、便携机操作及限制，敏感部位终端管理，网络及安全设备操作、策略配置及检查管理，业务应用操作程序、权限控制和监督，变更控制、设备重用的管理及安全审

计，不同安全区域之间信息交换管理，高安全信息向低安全域传输管理，网络及安全设备安全机制集中管理；

c) 评估信息系统运行维护阶段的运行维护管理，是否包括系统运行的全面管理及风险评估，对核心数据的监控保护，对运行状况、安全、性能监控及日志管理，软件硬件维护责任、维修过程的可监督及强制管理，外部服务方访问的限制及风险管理；

d) 评估信息系统运行维护阶段的外包服务管理，是否包括外包服务的限制，外包服务合同基本管理，外包服务商的选择及管理，以及外包服务监控和评估管理；

e) 评估信息系统运行维护阶段的有关安全机制的保障，是否包括具有审计、证书支持的身份鉴别机制专控管理，自主访问控制和强制访问控制机制的监控管理，基于专控的系统安全管理、网络安全管理，基于专控的应用系统安全管理，基于监督检查的病毒防护管理，以及密码算法、密钥管理、以密码技术为基础的安全管理；

f) 评估信息系统运行维护阶段的安全机制集中管理，是否包括系统管理、安全管理、审计管理等安全机制集中控管、安全信息集中的专控管理，安全机制整合的一般功能，安全机制整合的工作方式管理，以及安全机制集中管理的分层级联和控管。

有关日常运维管理方面的具体评估内容要点可参见附录 A 的 A.6.5。

7.3.6.6 业务连续性管理

信息系统运行维护阶段有关业务连续性管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的数据备份和恢复管理，是否明确了数据备份和恢复管理职责，规定并执行了数据备份的内容、周期要求和检查，备份介质及其恢复的操作过程监督检查，设备备份、系统热备份与冗余、系统远地备份；

b) 评估信息系统运行维护阶段的安全事件处理，是否明确了安全事件内容和划分要求，规定了安全事件报告和处理程序，是否按照程序处置安全事件，安全隐患问题报告和防范，以及强化事件处理责任的认定；

c) 评估信息系统运行维护阶段的应急处理，是否明确了应急处理的专门保护管理，规定了应急计划框架及具体应急计划的责任、能力，进行监督和持续改进，编制并落实了应急计划。

有关业务连续性管理方面的具体评估内容要点可参见附录 A 的 A.6.6。

7.3.6.7 监督和检查管理

信息系统运行维护阶段的监督和检查管理方面，本级评估要求如下：

a) 评估信息系统运行维护阶段的法律符合性，信息系统的运行操作、日常维护、安全监控、业务连续性、变更控制、外包管理、安全检查是否符合国家有关信息安全法规要求，是否做到知晓适用法律，遵守知识产权要求，防止滥用信息处理设备，保护关键业务应用软件版权，保护组织机构重要记录，遵照国家法规使用密码技术；

b) 评估信息系统运行维护阶段的依从性，对信息系统的运行和维护过程中有关贯彻安全策略和执行技术标准状况，进行全面系统的依从性检查和分析，并持续改进；

c) 评估信息系统运行维护阶段的监督控制，是否对运行维护阶段的安全状况定期进行自查，是否依据国家有关管理规范和技术标准进行保护，接受监管部门的专门监督检查；信息系统的运行和维护是否具有审计机制；

d) 评估信息系统运行维护阶段的责任认定，是否明确了信息系统的运行和维护过程的管理责任和技术责任，监督检查责任，以及审计及结果处理责任。

有关监督和检查管理方面的具体评估内容要点可参见附录 A 的 A.6.7。

7.4 终止处置管理评估要求

7.4.1 本阶段评估范围

7.4.1.1 评估范围概述

在信息系统终止处置阶段，信息安全管理评估范围包括：

a) 终止处置阶段的关键管理环节：
   ——系统终止审批；
   ——信息转移及清除；
   ——设备迁移或废弃；
   ——存储介质清除或销毁；
b) 终止处置阶段的策略和制度、机构和人员管理等保障措施；
c) 终止处置阶段的环境和资源管理、系统终止管理等日常措施；
d) 终止处置阶段的风险管理、监督和检查管理等监督措施。

7.4.1.2 系统终止审批

在信息系统终止处理过程中的终止审批的评估范围包括：

a) 根据业务应用和技术发展的需要，提出信息系统终止的申请，并经领导层或上级主管部门批准；
b) 提交拟终止的信息系统的信息资产清单、设备迁移或废弃清单、存储介质清单。

7.4.1.3 信息转移及清除

在信息系统终止处理过程中的信息转移及清除管理的评估范围包括：

a) 确认要终止的信息系统中需要转移、暂存和清除的信息资产；
b) 制定需要转移、暂存和清除信息资产的处理方案，包括信息资产的范围，以及处置方法；
c) 转移、暂存和清除信息资产的处理方案，需经过主管领导审查和批准；
d) 对要终止的信息系统中信息资产进行转移、暂存和清除；
e) 记录对信息资产的转移、暂存和清除处理过程，形成处理报告。

7.4.1.4 设备迁移或废弃

在信息系统终止处理过程中的设备迁移或废弃管理的评估范围包括：

a) 确认要终止的信息系统中需要迁移或废弃的软硬件设备；
b) 制定硬件设备的迁移或废弃处理方案，包括重用设备、废弃设备、清除敏感信息的方法；
c) 硬件设备的迁移或废弃处理方案需经过主管领导审查和批准；
d) 记录设备处理过程，形成设备迁移、废弃处理报告。

7.4.1.5 存储介质清除或销毁

在信息系统终止处理过程中的存储介质清除或销毁管理的评估范围包括：

a) 确认要终止的信息系统中需要清除或销毁的介质；
b) 确定要终止的信息系统中需要清除或销毁的存储介质的处理方式和处理流程；
c) 处理方案需经过主管领导审查和批准；
d) 根据存储介质处理方案对存储介质进行处理；
e) 形成存储介质的清除或销毁记录文档。

7.4.2 第一级信息系统

7.4.2.1 策略和制度管理

信息系统终止处置阶段有关策略和制度管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段的管理目标和范围是否涵盖了终止处置阶段的关键管理环节（见7.4.1），具有基本的管理目标和范围；

b) 评估信息系统终止处置阶段提出的信息系统总体安全管理策略，是否确定了信息系统终止处置的指导思路，形成了信息系统终止处置安全管理办法文档，是否达到基本的安全管理策略的要求，评估其制定和发布过程；

c) 评估信息系统终止处置阶段是否具有基本的安全管理规章制度，是否有系统终止审批、信息转移及清除、设备迁移或废弃、存储介质清除或销毁管理制度，与系统终止处置相关的机构和人员管理、风险管理、监督检查管理制度，评估其制定和发布过程；

d) 评估信息系统终止处置阶段的策略与制度文档是否进行了基本的评审和修订，以及指定专人保管。

有关策略和制度方面的具体评估内容要点可参见附录A的A.2.1。

7.4.2.2 机构和人员管理

信息系统终止处置阶段有关机构和人员管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段是否有分管领导负责，并配备安全管理人员参加，对信息系统终止处置是否具有基本安全管理职能；

b) 评估信息系统终止处置阶段的人员管理是否包括安全管理人员配备、信息系统关键岗位人员管理、人员考核与审查管理、第三方人员管理；

c) 评估信息系统运行终止处置的信息安全教育是否做到应知应会，能够听取信息安全专家建议。

有关机构和人员管理方面的具体评估内容要点可参见附录A的A.2.2。

7.4.2.3 风险管理

信息系统运行维护阶段有关风险管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段是否通过基本的风险管理，了解和控制信息系统终止处置过程中的安全风险，建立处置流程，具有基本的风险管理策略；

b) 评估信息系统运行终止处置是否进行了风险分析，基于废弃资产所产生的影响，确定不同的处理方式，对系统废弃可能带来新的威胁进行分析，改进新系统或管理方法，评价安全措施的实现程度，确定安全措施能否抵御现有威胁及脆弱性的影响；

c) 评估信息系统的终止处置是否进行了风险控制，包括：

——是否做到被废弃硬件和软件等资产及残留信息得到适当的处置，是否做到系统组件被合理地丢弃或更换；

——如被废弃的系统为详细系统的一部分，或与其他系统存在连接，是否关闭系统废弃后与其他系统的连接；

——如果在系统变更中废弃，除对废弃部分外，是否评估变更的部分，确定是否会增加风险或引入新的风险；

——对废弃资产的处理过程应在有效监督下实施，并执行人员进行安全教育；

d) 评估信息系统的终止处置中是否进行了风险决策，对于信息系统运行维护中存在的残余风险是否接受；

e) 评估信息系统运行终止处置的风险评估是否定期或发生重大变更时执行，主要包括对真实运行的信息系统及资产、威胁、脆弱性等各方面；评估结果是否体现在信息系统的运行维护改进中，是否按资质和信誉选择评估机构，签署保密协议，对评估信息规定交接手续。

有关风险管理方面的具体评估内容要点可参见附录 A 的 A.2.3。

7.4.2.4 环境和资源管理

信息系统终止处置阶段有关环境和资源管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段的信息资源管理，是否编制了需要终止处置的信息系统的基本资产清单、设备迁移或废弃清单、存储介质清单，进行了基本的介质、设备管理。

有关环境和资源管理方面的具体评估内容要点可参见附录 A 的 A.2.4。

7.4.2.5 监督和检查管理

信息系统终止处置阶段的监督和检查管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段的法律符合性，信息系统的终止审批、信息转移及清除、设备迁移或废弃、存储介质清除或销毁是否符合国家有关信息安全法规要求，是否做到知晓适用法律，遵守知识产权要求，保护组织机构重要记录；

b) 评估信息系统终止处置阶段的监督控制，是否对终止处置阶段的安全状况进行自查，是否依据国家有关管理规范和技术标准进行保护。

有关监督和检查管理方面的具体评估内容要点可参见附录 A 的 A.2.7。

7.4.2.6 终止处置过程管理

信息系统终止处置阶段的终止处置过程管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段的终止处置过程管理，是否明确指定负责人，监督和管理系统终止审批、信息转移及清除、设备迁移或废弃、存储介质清除或销毁等全过程(见 7.4.1)；

b) 评估信息系统终止处置阶段的终止运行管理，是否由使用者或管理者提出申请并说明原因及采取的保护措施，经过相应领导审批。

有关终止处置过程管理方面的具体评估内容要点可参见附录 A 的 A.2.8。

7.4.3 第二级信息系统

7.4.3.1 策略和制度管理

信息系统终止处置阶段有关策略和制度管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段的管理目标和范围是否涵盖了终止处置阶段的关键管理环节(见 7.4.1)，具有较完整的管理目标和范围；

b) 评估信息系统终止处置阶段提出的信息系统总体安全管理策略，是否确定了信息系统终止处置的指导思路，形成了信息系统终止处置安全管理办法文档，是否达到较完整的安全管理策略的要求，评估其制定和发布过程；

c) 评估信息系统终止处置阶段是否具有较完整的安全管理规章制度和操作规程，是否有系统终止审批、信息转移及清除、设备迁移或废弃、存储介质清除或销毁管理制度，与系统终止处置相关的机构和人员管理、风险管理、监督检查管理制度，评估其制定和发布过程；

d) 评估信息系统终止处置阶段的策略与制度文档是否进行了较完整的评审和修订，以及指定专人保管、借阅审批和登记。

有关策略和制度方面的具体评估内容要点可参见附录 A 的 A.3.1。

7.4.3.2 机构和人员管理

信息系统终止处置阶段有关机构和人员管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段是否有分管领导和信息安全职能部门负责，并配备安全管理人员参加，对信息系统终止处置是否具有安全管理领导职能；

b) 评估信息系统终止处置阶段的人员管理是否包括安全管理人员配备、信息系统关键岗位人员管理、人员考核与审查管理、第三方人员管理；

c) 评估信息系统运行终止处置的信息安全教育是否做到应知应会，有计划开展培训，能够听取信息安全专家建议。

有关机构和人员管理方面的具体评估内容要点可参见附录 A 的 A.3.2。

7.4.3.3 风险管理

信息系统终止处置阶段有关风险管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段是否通过基本的风险管理，了解和控制信息系统终止处置过程中的安全风险，建立处置流程，具有风险管理策略；

b) 评估信息系统运行终止处置是否进行了风险分析，基于废弃资产对组织的影响，确定不同的处理方式，对系统废弃可能带来新的威胁进行分析，改进新系统或管理方法，评价安全措施的实现程度，确定安全措施能否抵御现有威胁及脆弱性的影响；

c) 评估信息系统的终止处置是否进行了风险控制，包括：

——是否做到被废弃硬件和软件等资产及残留信息得到适当的处置，是否做到系统组件被合理地丢弃或更换；

——如被废弃的系统为详细系统的一部分，或与其他系统存在连接，是否关闭系统废弃后与其他系统的连接；

——如果在系统变更中废弃，除对废弃部分外，是否评估变更的部分，确定是否会增加风险或引入新的风险；

——对废弃资产的处理过程应在有效监督下实施，并执行人员进行安全教育；

d) 评估信息系统的终止处置中是否进行了风险决策，对于信息系统运行维护中存在的残余风险是否接受，采取残余风险监视措施；

e) 评估信息系统运行终止处置的风险评估是否定期或发生重大变更时执行，主要包括对真实运行的信息系统及资产、威胁、脆弱性等各方面；评估结果是否体现在信息系统的运行维护改进中，是否按资质和信誉选择评估机构，签署保密协议，对评估信息规定交接手续并替换敏感参数。

有关风险管理方面的具体评估内容要点可参见附录 A 的 A.3.3。

7.4.3.4 环境和资源管理

信息系统终止处置阶段有关环境和资源管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段的信息资源管理，是否编制了需要终止处置的信息系统详细的资产清单、设备迁移或废弃清单、存储介质清单，进行了资产分类管理，包括数据存储介质、设备管理。

有关环境和资源管理方面的具体评估内容要点可参见附录 A 的 A.3.4。

7.4.3.5 监督和检查管理

信息系统终止处置阶段的监督和检查管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段的法律符合性，信息系统的终止审批、信息转移及清除、设备迁移或废弃、存储介质清除或销毁是否符合国家有关信息安全法规要求，是否做到知晓适用法律，遵守知识产权要求，防止滥用信息处理设备，保护业务应用软件版权，保护组织机构重要记录；

b) 评估信息系统终止处置阶段的依从性，对信息系统的终止和处置操作中有关贯彻安全策略和执行技术标准状况，进行依从性检查和分析；

c) 评估信息系统终止处置阶段的监督控制，是否对终止处置阶段的安全状况进行自查，是否依据国家有关管理规范和技术标准进行保护，接受监管部门的指导；信息系统的终止和处置操作是否具有审计机制；

d) 评估信息系统终止处置阶段的责任认定，是否明确了信息系统的终止和处置操作的管理责任和技术责任，监督检查责任，以及审计及结果处理责任。

有关监督和检查管理方面的具体评估内容要点可参见附录 A 的 A.3.7。

7.4.3.6 系统终止管理

信息系统终止处置阶段的终止处置过程管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段的终止处置过程管理，是否明确指定负责人，监督和管理系统终止审批、信息转移及清除、设备迁移或废弃、存储介质清除或销毁等全过程（见 7.4.1）；具有详细的实施计划；

b) 评估信息系统终止处置阶段的终止运行管理，是否由使用者或管理者提出申请并说明原因及采取的保护措施，经过相应领导审批；终止运行前进行必要的数据备份，对终止运行的设备进行数据清除。

有关终止处置过程管理方面的具体评估内容要点可参见附录 A 的 A.3.8。

7.4.4 第三级信息系统

7.4.4.1 策略和制度管理

信息系统终止处置阶段有关策略和制度管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段的管理目标和范围是否涵盖了终止处置阶段的关键管理环节（见 7.4.1），具有完好定义的管理目标和范围；

b) 评估信息系统终止处置阶段提出的信息系统总体安全管理策略，是否确定了信息系统终止处置的指导思路，形成了信息系统终止处置安全管理办法文档，是否达到体系化的安全管理策略的要求，评估其制定和发布过程；

c) 评估信息系统终止处置阶段是否具有体系化的安全管理规章制度和操作规程，是否有系统终止审批、信息转移及清除、设备迁移或废弃、存储介质清除或销毁管理制度，与系统终止处置相关的机构和人员管理、风险管理、监督检查管理制度，评估其制定和发布过程；

d) 评估信息系统终止处置阶段的策略与制度文档是否进行了体系化的评审和修订，以及指定专人保管、限定借阅范围、审批和登记。

有关策略和制度方面的具体评估内容要点可参见附录 A 的 A.4.1。

7.4.4.2 机构和人员管理

信息系统终止处置阶段有关机构和人员管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段是否有信息安全领导小组和安全职能部门负责，并配备安全管理人员参加，对信息系统终止处置是否具有安全管理领导职能；

b) 评估信息系统终止处置阶段的人员管理是否包括安全管理人员配备、信息系统关键岗位人员

管理、人员考核与审查管理、第三方人员管理；

c) 评估信息系统运行终止处置的信息安全教育是否做到应知应会，有计划开展培训，针对不同岗位培训，能够听取信息安全专家建议。

有关机构和人员管理方面的具体评估内容要点可参见附录 A 的 A.4.2。

7.4.4.3 风险管理

信息系统终止处置阶段有关风险管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段是否通过基本的风险管理，了解和控制信息系统终止处置过程中的安全风险，建立处置流程，具有风险管理策略及其监督机制；

b) 评估信息系统运行终止处置是否进行了风险分析，基于废弃资产所产生的影响，确定不同的处理方式，对系统废弃可能带来新的威胁进行分析，改进新系统或管理方法，评价安全措施的实现程度，确定安全措施能否抵御现有威胁及脆弱性的影响；

c) 评估信息系统的终止处置是否进行了风险控制，包括：

——是否做到被废弃硬件和软件等资产及残留信息得到适当的处置，是否做到系统组件被合理地丢弃或更换；

——如被废弃的系统为详细系统的一部分，或与其他系统存在连接，是否关闭系统废弃后与其他系统的连接；

——如果在系统变更中废弃，除对废弃部分外，是否评估变更的部分，确定是否会增加风险或引入新的风险；

——对废弃资产的处理过程应在有效监督下实施，并执行人员进行安全教育；

d) 评估信息系统的终止处置中是否进行了风险决策，对于信息系统运行维护中存在的残余风险是否接受，采取残余风险监视措施；

e) 评估信息系统运行终止处置的风险评估是否定期或发生重大变更时执行，主要包括对真实运行的信息系统及资产、威胁、脆弱性等各方面；评估结果是否体现在信息系统的运行维护改进中，是否按资质和信誉选择评估机构，签署保密协议，对评估信息规定交接手续并替换敏感参数，对评估信息不得带出指定区域。

有关风险管理方面的具体评估内容要点可参见附录 A 的 A.4.3。

7.4.4.4 环境和资源管理

信息系统终止处置阶段有关环境和资源管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段的信息资源管理，是否编制了需要终止处置的信息系统详细的资产清单、设备迁移或废弃清单、存储介质清单，进行了资产分类管理，包括数据存储介质、设备管理及资产信息管理。

有关环境和资源管理方面的具体评估内容要点可参见附录 A 的 A.4.4。

7.4.4.5 监督和检查管理

信息系统终止处置阶段的监督和检查管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段的法律符合性，信息系统的终止审批、信息转移及清除、设备迁移或废弃、存储介质清除或销毁是否符合国家有关信息安全法规要求，是否做到知晓适用法律，遵守知识产权要求，防止滥用信息处理设备，保护业务应用软件版权，保护组织机构重要记录，遵照国家法规处置密码技术设施；

b) 评估信息系统终止处置阶段的依从性，对信息系统的终止和处置操作中有关贯彻安全策略和执行技术标准状况，进行全面系统的依从性检查和分析；

c) 评估信息系统终止处置阶段的监督控制，是否对终止处置阶段的安全状况进行自查，是否依据国家有关管理规范和技术标准进行保护，接受监管部门的监督检查；信息系统的终止和处置操作是否具有审计机制；

d) 评估信息系统终止处置阶段的责任认定，是否明确了信息系统的终止和处置操作的管理责任和技术责任，监督检查责任，以及审计及结果处理责任。

有关监督和检查管理方面的具体评估内容要点可参见附录 A 的 A.4.7。

7.4.4.6 系统终止管理

信息系统终止处置阶段的终止处置过程管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段的终止处置过程管理，是否明确指定负责人，监督和管理系统终止审批、信息转移及清除、设备迁移或废弃、存储介质清除或销毁等全过程（见 7.4.1）；具有详细的实施计划，进行系统终止安全评估；

b) 评估信息系统终止处置阶段的终止运行管理，是否由使用者或管理者提出申请并说明原因及采取的保护措施，经过相应领导审批；终止运行前进行必要的数据备份，对终止运行的设备进行数据清除，存储设备损坏则进行销毁，得到有关领导和技术负责人认可。

有关终止处置过程管理方面的具体评估内容要点可参见附录 A 的 A.4.8。

7.4.5 第四级信息系统

7.4.5.1 策略和制度管理

信息系统终止处置阶段有关策略和制度管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段的管理目标和范围是否涵盖了终止处置阶段的关键管理环节（见 7.4.1），具有量化控制的管理目标和范围；

b) 评估信息系统终止处置阶段提出的信息系统总体安全管理策略，是否确定了信息系统终止处置的指导思路，形成了信息系统终止处置安全管理办法文档，是否达到强制保护的安全管理策略的要求，评估其制定和发布过程；

c) 评估信息系统终止处置阶段是否具有强制保护的安全管理规章制度和操作规程，是否有系统终止审批、信息转移及清除、设备迁移或废弃、存储介质清除或销毁管理制度，与系统终止处置相关的机构和人员管理、风险管理、监督检查管理制度，评估其制定和发布过程；

d) 评估信息系统终止处置阶段的策略与制度文档是否进行了强制保护的评审和修订，以及指定专人保管、限定借阅范围、审批和登记等全面严格保管。

有关策略和制度方面的具体评估内容要点可参见附录 A 的 A.5.1。

7.4.5.2 机构和人员管理

信息系统终止处置阶段有关机构和人员管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段是否有信息安全领导小组和安全职能部门负责，并配备安全管理人员参加，安全领导小组是否由主要负责人出任领导，对信息系统终止处置是否具有安全管理领导职能；

b) 评估信息系统终止处置阶段的人员管理是否包括安全管理人员配备、信息系统关键岗位人员管理、人员考核与审查管理、第三方人员管理；

c) 评估信息系统运行终止处置的信息安全教育是否做到应知应会，有计划开展培训，针对不同岗位培训，能够听取信息安全专家建议，对信息安全专家的管理。

有关机构和人员管理方面的具体评估内容要点可参见附录 A 的 A.5.2。

7.4.5.3 风险管理

信息系统终止处置阶段有关风险管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段是否通过基本的风险管理，了解和控制信息系统终止处置过程中的安全风险，建立处置流程，具有风险管理策略及其监督机制；

b) 评估信息系统运行终止处置是否进行了风险分析，基于废弃资产所产生的影响，确定不同的处理方式，对系统废弃可能带来新的威胁进行分析，改进新系统或管理方法，评价安全措施的实现程度，确定安全措施能否抵御现有威胁及脆弱性的影响；

c) 评估信息系统的终止处置是否进行了风险控制，包括：

——是否做到被废弃硬件和软件等资产及残留信息得到适当的处置，是否做到系统组件被合理地丢弃或更换；

——如被废弃的系统为详细系统的一部分，或与其他系统存在连接，是否关闭系统废弃后与其他系统的连接；

——如果在系统变更中废弃，除对废弃部分外，是否评估变更的部分，确定是否会增加风险或引入新的风险；

——对废弃资产的处理过程应在有效监督下实施，并执行人员进行安全教育；

d) 评估信息系统的终止处置中是否进行了风险决策，对于信息系统运行维护中存在的残余风险是否接受，采取残余风险监视措施；

e) 评估信息系统运行终止处置的风险评估是否定期或发生重大变更时执行，主要包括对真实运行的信息系统及资产、威胁、脆弱性等各方面；评估结果是否体现在信息系统的运行维护改进中，是否按资质和信誉选择评估机构，签署保密协议，对评估信息规定交接手续并替换敏感参数，对评估信息不得带出指定区域。

有关风险管理方面的具体评估内容要点可参见附录 A 的 A.5.3。

7.4.5.4 环境和资源管理

信息系统终止处置阶段有关环境和资源管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段的信息资源管理，是否编制了需要终止处置的信息系统详细的资产清单、设备迁移或废弃清单、存储介质清单，进行了资产分类管理并建立资产管理体系，包括数据存储介质加密管理、设备管理及资产信息管理。

有关环境和资源管理方面的具体评估内容要点可参见附录 A 的 A.5.4。

7.4.5.5 监督和检查管理

信息系统终止处置阶段的监督和检查管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段的法律符合性，信息系统的终止审批、信息转移及清除、设备迁移或废弃、存储介质清除或销毁是否符合国家有关信息安全法规要求，是否做到知晓适用法律，遵守知识产权要求，防止滥用信息处理设备，保护业务应用软件版权，保护组织机构重要记录，遵照国家法规处置密码技术设施；

b) 评估信息系统终止处置阶段的依从性，对信息系统的终止和处置操作中有关贯彻安全策略和执行技术标准状况，进行全面系统的依从性检查和分析，并持续改进；

c) 评估信息系统终止处置阶段的监督控制，是否对终止处置阶段的安全状况进行自查，是否依据国家有关管理规范和技术标准进行保护，接受监管部门的强制监督检查；信息系统的终止和处置操作是否具有审计机制；

d) 评估信息系统终止处置阶段的责任认定，是否明确了信息系统的终止和处置操作的管理责任

和技术责任，监督检查责任，以及审计及结果处理责任。

有关监督和检查管理方面的具体评估内容要点可参见附录 A 的 A.5.7。

7.4.5.6 系统终止管理

信息系统终止处置阶段的终止处置过程管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段的终止处置过程管理，是否明确指定负责人，监督和管理系统终止审批、信息转移及清除、设备迁移或废弃、存储介质清除或销毁等全过程（见 7.4.1）；具有详细的实施计划，进行系统终止安全评估；

b) 评估信息系统终止处置阶段的终止运行管理，是否由使用者或管理者提出申请并说明原因及采取的保护措施，经过相应领导审批；终止运行前进行必要的数据备份和保管，对终止运行的设备进行数据清除，存储设备损坏则进行销毁，得到有关领导和技术负责人认可。

有关终止处置过程管理方面的具体评估内容要点可参见附录 A 的 A.5.8。

7.4.6 第五级信息系统

7.4.6.1 策略和制度管理

信息系统终止处置阶段有关策略和制度管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段的管理目标和范围是否涵盖了终止处置阶段的关键管理环节（见 7.4.1），具有自我持续改进的管理目标和范围；

b) 评估信息系统终止处置阶段提出的信息系统总体安全管理策略，是否确定了信息系统终止处置的指导思路，形成了信息系统终止处置安全管理办法文档，是否达到专控保护的安全管理策略的要求，评估其制定和发布过程；

c) 评估信息系统终止处置阶段是否具有专控保护的安全管理规章制度和操作规程，是否有系统终止审批、信息转移及清除、设备迁移或废弃、存储介质清除或销毁管理制度，与系统终止处置相关的机构和人员管理、风险管理、监督检查管理制度，评估其制定和发布过程；

d) 评估信息系统终止处置阶段的策略与制度文档是否进行了专控保护的评审和修订，以及指定专人保管、限定借阅范围、审批和登记等全面严格保管。

有关策略和制度方面的具体评估内容要点可参见附录 A 的 A.6.1。

7.4.6.2 机构和人员管理

信息系统终止处置阶段有关机构和人员管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段是否有信息安全领导小组和安全职能部门负责，并配备安全管理人员参加，安全领导小组是否由主要负责人出任领导，对信息系统终止处置是否具有安全管理领导职能和信息安全保密监督管理职能；

b) 评估信息系统终止处置阶段的人员管理是否包括安全管理人员配备、信息系统关键岗位人员管理、人员考核与审查管理、第三方人员管理；

c) 评估信息系统运行终止处置的信息安全教育是否做到应知应会，有计划开展培训，针对不同岗位培训，培养安全意识自觉性，能够听取信息安全专家建议，对信息安全专家的管理。

有关机构和人员管理方面的具体评估内容要点可参见附录 A 的 A.6.2。

7.4.6.3 风险管理

信息系统终止处置阶段有关风险管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段是否通过基本的风险管理，了解和控制信息系统终止处置过程中

的安全风险，建立处置流程，具有风险管理策略及其监督机制；

b) 评估信息系统运行终止处置是否进行了风险分析，基于废弃资产所产生的影响，确定不同的处理方式，对系统废弃可能带来新的威胁进行分析，改进新系统或管理方法，评价安全措施的实现程度，确定安全措施能否抵御现有威胁及脆弱性的影响；

c) 评估信息系统的终止处置是否进行了风险控制，包括：

——是否做到被废弃硬件和软件等资产及残留信息得到适当的处置，是否做到系统组件被合理地丢弃或更换；

——如被废弃的系统为详细系统的一部分，或与其他系统存在连接，是否关闭系统废弃后与其他系统的连接；

——如果在系统变更中废弃，除对废弃部分外，是否评估变更的部分，确定是否会增加风险或引入新的风险；

——对废弃资产的处理过程应在有效监督下实施，并执行人员进行安全教育；

d) 评估信息系统的终止处置中是否进行了风险决策，对于信息系统运行维护中存在的残余风险是否接受，采取残余风险监视措施；

e) 评估信息系统运行终止处置的风险评估是否定期或发生重大变更时执行，主要包括对真实运行的信息系统及资产、威胁、脆弱性等各方面；评估结果是否体现在信息系统的运行维护改进中，是否按资质和信誉选择评估机构，签署保密协议，对评估信息规定交接手续并替换敏感参数，对评估信息不得带出指定区域。

有关风险管理方面的具体评估内容要点可参见附录 A 的 A.6.3。

7.4.6.4 环境和资源管理

信息系统终止处置阶段有关环境和资源管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段的信息资源管理，是否编制了需要终止处置的信息系统详细的资产清单、设备迁移或废弃清单、存储介质清单，进行了资产分类管理并建立资产管理体系，包括数据存储介质加密管理、设备管理及资产信息管理。

有关环境和资源管理方面的具体评估内容要点可参见附录 A 的 A.6.4。

7.4.6.5 监督和检查管理

信息系统终止处置阶段的监督和检查管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段的法律符合性，信息系统的终止审批、信息转移及清除、设备迁移或废弃、存储介质清除或销毁是否符合国家有关信息安全法规要求，是否做到知晓适用法律，遵守知识产权要求，防止滥用信息处理设备，保护业务应用软件版权，保护组织机构重要记录，遵照国家法规处置密码技术设施；

b) 评估信息系统终止处置阶段的依从性，对信息系统的终止和处置操作中有关贯彻安全策略和执行技术标准状况，进行全面系统的依从性检查和分析，并持续改进；

c) 评估信息系统终止处置阶段的监督控制，是否对终止处置阶段的安全状况进行自查，是否依据国家有关管理规范和技术标准进行保护，接受监管部门的专门监督检查；信息系统的终止和处置操作是否具有审计机制；

d) 评估信息系统终止处置阶段的责任认定，是否明确了信息系统的终止和处置操作的管理责任和技术责任，监督检查责任，以及审计及结果处理责任。

有关监督和检查管理方面的具体评估内容要点可参见附录 A 的 A.6.7。

7.4.6.6 系统终止管理

信息系统终止处置阶段的终止处置过程管理方面，本级评估要求如下：

a) 评估信息系统终止处置阶段的终止处置过程管理，是否明确指定负责人，监督和管理系统终止审批、信息转移及清除、设备迁移或废弃、存储介质清除或销毁等全过程（见 7.4.1）；具有详细的实施计划，进行系统终止安全评估；

b) 评估信息系统终止处置阶段的终止运行管理，是否由使用者或管理者提出申请并说明原因及采取的保护措施，经过相应领导审批；终止运行前进行必要的数据备份和保管，对终止运行的设备进行数据清除，存储设备损坏则进行销毁，得到有关领导和技术负责人认可。

有关终止处置过程管理方面的具体评估内容要点可参见附录 A 的 A.6.8。

附 录 A
（资料性附录）
信息系统安全管理评估参照表

A.1 综述

为配合本标准第7章分等级评估的使用需要，特编制“信息系统安全管理评估参照表”（以下称“本表”），提供信息系统安全管理评估者参考，特别是自评估者参考。

本表中的类、族、评估项（列）与GB/T 20269—2006中信息系统安全管理要素及其分级分类相对应。本表中的评估内容要点（列）依据GB/T 20269—2006中的信息系统安全管理要素作进一步分解得出。本表中的标准依据（列）直接引用标题编号的均指向GB/T 20269—2006，以其他法规或标准为依据的则在引用处说明。

本表分为第一级至第五级信息系统安全管理评估参照表，为清晰表示每一个安全等级比较低一级安全等级的安全管理评估内容要点的增加和增强，每一级的新增部分用**“宋体加粗字”**表示。

本表中带有★的条目，表示已设定为关键条目。信息系统安全管理评估者根据信息系统具体情况，可增设新的关键条目。一般不应删除原有的关键条目，如确有不适用的关键条目，应在最终评估文档中明确说明其不适用的理由。

本表在用于信息系统生存周期的规划立项阶段、设计实施阶段、运行维护阶段、终止处置阶段等不同阶段的安全管理评估时，应分别根据正文中的7.1、7.2、7.3、7.4的评估要求进一步的调整和细化。

A.2 第一级信息系统安全管理评估参照表

A.2.1 策略和制度管理

表A.1 策略和制度管理（第一级信息系统）

类	族	评估项	评估内容要点	标准依据
★策略和制度	★信息安全管理策略	★安全管理目标与范围	管理对象（信息系统）的基本描述	5.1.1.1 a)
			明确信息系统的管理范围	
			★业务数据和系统服务达到的安全要求，符合第一级信息系统安全要求	
		★总体安全管理策略	制定了基本的安全管理策略文档	5.1.1.2 a)
			明确管理者对信息系统安全的责任，管理方法、支持意向	
			简要说明对信息系统有重大意义的安全方针、原则、标准和符合性要求	
			★说明信息系统安全的总体目标、范围、管理原则和安全框架	
			依据国家有关管理规范和技术标准进行保护	
		安全管理策略的制定	由分管信息安全工作的负责人召集	5.1.1.3 a)
			以安全管理人员为主制定	
			信息技术及业务人员参加制定	
			★形成基本的信息系统安全管理策略	
		安全管理策略的发布	由组织机构负责人签发	5.1.1.3 a)
			向信息系统的有关用户传达说明	

表 A.1（续）

类	族	评估项	评估内容要点	标准依据
★策略和制度	★安全管理规章制度	★安全管理规章制度内容	制定了基本的安全管理制度文档	5.1.2.1 a)
			★包括日常管理活动中常用的安全管理制度，如网络、系统、数据、防病毒、机房等管理和安全管理规定，以及必要的操作规程等内容	
		安全管理规章制度的制定	由安全管理人员负责制订	5.1.2.2 a)
			由分管信息安全工作的负责人审批	
			★有正式发布的制度文件或文档	
	策略与制度文档管理	策略与制度文档的评审和修订	由分管信息安全的负责人和安全管理人员负责文档的评审和修订	5.1.3.1 a)
			★检查策略和制度的有效性，对存在不足或需要改进的策略和制度进行修订	
		★策略与制度文档的保管	修订后的策略和制度按规定程序发布	5.1.3.2 a)
			★指定专人保管	

A.2.2 机构和人员管理

表 A.2 机构和人员管理（第一级信息系统）

类	族	评估项	评估内容要点	标准依据
★机构和人员管理	★安全管理机构	★建立安全管理机构	★管理层中应有一人分管信息系统安全工作	5.2.1.1 a)
			配备专职或兼职的安全管理人员	
	人员管理	★安全管理人员配备	★可配备兼职安全管理人员，可由网络管理人员兼任	5.2.3.1 a)
		关键岗位人员管理	明确关键岗位，如安全管理员、系统管理员、数据库管理员、网络管理员、重要业务开发人员、系统维护人员、重要业务应用操作人员	5.2.3.2 a)
			允许一人多岗，但业务应用操作人员不能由其他关键岗位人员兼任	
			定期安全培训，加强安全和风险防范意识	
		人员录用管理	进行审查，确认其具有基本的专业技术水平，能够掌握信息安全管理基本知识	5.2.3.3 a)
			对关键岗位的人员注重思想品质方面考察	
		★人员离岗	★立即中止被解雇的、退休的、辞职的或其他原因离开的人员的所有访问权限	5.2.3.4 a)
			收回所有相关证件、密钥、访问控制标记等	
			收回组织机构提供的设备等	
		人员考核与审查	定期对各个岗位的人员进行不同侧重的安全认知和安全技能的考核，作为人员是否适合当前岗位的参考	5.2.3.5 a)
		★第三方人员管理	★签署相关安全责任的合同书或保密协议	5.2.3.6 a)
			规定各类人员的活动范围，进入计算机房需要得到批准，并有专人负责	
			必须进行逻辑访问时，应划定范围并经过负责人批准，必要时应有人监督或陪同	

表 A.2（续）

类	族	评估项	评估内容要点	标准依据
★机构和人员管理	教育和培训	★信息安全教育	让员工知晓信息的敏感性和信息安全的重要性	5.2.4.1 a)
			认识其自身的责任和安全违例会受到纪律惩罚	
			★掌握的信息安全基本知识和技能	
		信息安全专家	听取信息安全专家的建议	5.2.4.2 a)
			组织专家参与安全威胁的评价，对安全事件给予专业指导和原因调查等	

A.2.3 风险管理

表 A.3 风险管理（第一级信息系统）

类	族	评估项	评估内容要点	标准依据
风险管理	风险管理要求和策略	风险管理要求	进行基本的风险管理活动	5.3.1.1 a)
			★编制资产清单，对资产价值/重要性进行分析，对信息系统面临的威胁进行初步分析	
	风险分析和评估	资产识别和分析	确定信息系统的资产范围，进行统计和编制资产清单	5.3.2.1 a)
			进行资产分类和重要性标识	
		威胁识别和分析	对威胁的基本认识	5.3.2.2 a)
			★根据以往发生的安全事件、外部提供的资料和积累的经验，对威胁进行粗略的分析	
		脆弱性识别和分析	★通过扫描工具获取对系统脆弱性的认识	5.3.2.3 a)
			编制信息系统脆弱性列表	
		风险分析和评估要求	由用户和部分专家通过经验来判断风险，并对风险进行评估，形成风险评估报告	5.3.2.4 a)
			★评估报告中包括风险级别、风险点等内容，确定信息系统的安全风险状况	
	风险控制	选择和实施风险控制措施	基于安全等级标准，选择相应等级的安全技术和管理措施	5.3.3.1 a)
			★确定需要实施的信息系统安全控制措施	
	基于风险的决策	安全确认	★针对信息系统的资产清单、威胁列表、脆弱性列表，结合已采用的安全控制措施，分析存在的残余风险	5.3.4.1 a)
			形成残余风险分析报告，由组织机构的高层管理人员决定残余风险是否可接受	
		信息系统运行的决策	信息系统的主管者或运营者应根据安全确认的结果，判断残余风险是否可接受，决定是否允许信息系统继续运行	5.3.4.2 a)

表 A.3（续）

类	族	评估项	评估内容要点	标准依据
风险管理	★风险评估的管理	★评估机构的选择	★有国家主管部门认可的安全服务资质	5.3.5.1 a)
			有良好信誉的评估机构	
		评估机构保密要求	评估机构人员应按照第三方人员管理要求签署保密协议	5.3.5.2 a)
		评估信息的管理	★提交涉及评估需要的资料、数据等各种信息，应规定办理交接手续，防止丢失	5.3.5.3 a)
		技术检测过程管理	★使用工具或手工进行技术检测，应事先提交测试的技术方案，得到授权方可进行	5.3.5.4 a)

A.2.4 环境和资源管理

表 A.4 环境和资源管理（第一级信息系统）

类	族	评估项	评估内容要点	标准依据
环境和资源管理	环境安全管理	环境安全管理要求	★应配置物理环境安全的责任部门和管理人员	5.4.1.1 a)
			建立有关物理环境安全方面的规章制度	
			物理安全方面应达到 GB/T 20271—2006 中 6.1.1 的有关要求	
		★机房安全管理要求	★明确机房安全管理的责任人	5.4.1.2 a)
			机房钥匙由专人管理，未经批准，不准任何人私自复制机房钥匙或服务器开机钥匙	
			未经允许的人员不准进入机房	
			获准进入机房的来访人员，其活动范围应受到限制，并有接待人员陪同	
			没有指定管理人员的明确准许，任何记录介质、文件材料及各种被保护品均不准带出机房，与工作无关的物品均不准带入机房	
			机房内严禁吸烟及带入火种和水源	
	资源管理	资产清单管理	★应编制并维护与信息系统相关的资产清单	5.4.2.1 a)
			信息资产：应用数据、系统数据、安全数据等数据库和数据文档、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、存档信息	
			软件资产：应用软件、系统软件、开发工具和实用程序	
			有形资产：计算机设备（服务器、终端、存储设备等），网络设备（路由器、交换机、安全设备等），移动存储介质（移动硬盘、磁带等），其他技术装备（电源，空调设备等），家具和机房	
			应用业务相关资产：由信息系统控制的或与信息系统密切相关的应用业务的各类资产，由于信息系统或信息的泄露或破坏，这些资产会受到相应的损坏	
			服务：计算和通信服务，通用设备如供暖、照明、供电和空调等	

表 A.4（续）

类	族	评估项	评估内容要点	标准依据
环境和资源管理	资源管理	资产的分类与标识要求	根据资产的价值/重要性对资产进行标识，可基于资产的价值选择保护措施和进行资产管理	5.4.2.2 a)
		介质管理	★脱机存放的数据和软件介质应储放在安全的环境中，防止被盗、被毁、被修改以及信息泄漏	5.4.2.3 a)
			介质的归档和查询应有记录，对存档介质的目录清单应定期盘点	
			需要送出维修或销毁的介质，应防止信息泄漏	
		★设备管理要求	对于信息系统的各种软硬件设备的选型、采购、发放或领用，使用者应提出申请，报经相应领导审批，才可以实施	5.4.2.4 a)
			★设备的选型、采购、使用和保管应明确责任人	

A.2.5 运行和维护管理

表 A.5 运行和维护管理（第一级信息系统）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	★用户管理	★用户分类管理	★按审查和批准的用户分类清单建立用户和分配权限	5.5.1.1 a)
			用户分类清单应包括信息系统的所有用户的清单，以及各类用户的权限	
			用户权限发生变化时应及时更改用户清单内容	
			用户分类应包括系统用户、普通用户、外部客户用户、临时用户	
		系统用户要求	★系统用户应由信息系统的主管领导指定	5.5.1.2 a)
			系统用户应保护自己的身份鉴别信息的安全	
			授权应以满足工作需要的最小权限为原则	
		普通用户要求	★用户应保护自己的身份鉴别信息的安全	5.5.1.3 a)
			发现系统的漏洞、滥用或违背安全行为应及时报告	
			不应透露与组织机构有关的非公开信息	
			不应故意进行违规的操作	
		机构外部用户要求	★应对外部用户明确说明使用者的责任、义务和风险，并要求提供合法使用的声明	5.5.1.4 a)
			外部用户应保护自己的身份鉴别信息的安全	
			外部用户只能是应用层的用户	
		临时用户要求	★临时用户的设置和期限必须经过审批	5.5.1.5 a)
			临时用户应保护自己的身份鉴别信息的安全	
			使用完毕或到期应及时删除	
			设置与删除均应记录备案	
	运行操作管理	★服务器操作管理	★服务器操作系统、数据库系统的操作应由授权的系统管理员、数据库管理员实施	5.5.2.1 a)
			遵照操作规程对服务器进行操作，设置服务器的运行环境，设定服务器的系统及安全配置，操作系统、数据库系统用户管理	
			系统管理员、数据库管理员应以自己的账户及身份鉴别信息登录操作系统、数据库系统进行操作	

表 A.5（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	运行操作管理	终端计算机操作管理	★用户应设置终端计算机的开机、屏幕保护口令，保护身份鉴别信息，进行必要的安全设置	5.5.2.2 a)
			非组织机构配备的终端计算机未获批准，不能在办公场所使用	
			及时安装经许可的软件和补丁程序，不得自行安装及使用其他软件和自由下载软件	
			未获批准，严禁使用 Modem 拨号、无线网卡等方式或另辟通路接入其他网络	
		便携机操作管理	在接入组织机构内部网络时遵守“终端计算机操作管理”（上一节）的要求	5.5.2.3 a)
			对不再使用或转为其他用途的便携机，应删除机内的敏感数据	
			在外网使用的便携机，接入本地网络前应进行必要的安全检查	
		★网络及安全设备操作管理	★对网络及安全设备的操作应由授权的网络管理员、安全管理员实施	5.5.2.4 a)
			应按操作规程对网络设备和安全设备进行操作，进行网络和安全设备的运行环境配置和服务设定	
			网络管理员、安全管理员应以自己的账户及身份鉴别信息登录网络设备和安全设备进行操作	
		业务应用操作管理	应用系统管理员及业务操作人员应以自己的账户及身份鉴别信息登录业务应用系统（提供对外或专门服务的公共用户可除外）	5.5.2.5 a)
			★应用系统管理员根据安全策略和专门授权对应用系统的操作人员等用户及其权限进行管理，监控应用系统的运行	
			用户对业务应用系统的访问权限应受到控制，如以菜单等方式限制操作	
			用户应按照操作规程使用业务应用系统，操作规程应指明具体作业的指令，处理和使用的信息，以及操作步骤	
			业务应用系统操作规程应形成正式文档或帮助文件，需要进行改动时应得到管理层授权	
			操作规程应说明处理错误或其他异常情况的指令，以及在出现意外的操作或技术问题时需要技术支持的联系方法	
		★变更控制和重用管理	★信息系统的变更应经过申报和审批才能进行	5.5.2.6 a)
			进行变更应进行记录，对重大变更应评估其潜在影响，向所有相关人员通报变更细节	
			明确中止变更并从失败变更中恢复的责任和处理方法	
			设备重用应经过申报和审批才能进行，应清除重用设备中原有信息	

表 A.5（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	运行操作管理	信息交换管理	★在信息系统中发布信息和用户交换信息，应符合国家有关政策法规的规定	5.5.2.7 a)
			应采取适当的安全措施保护信息系统中发布信息和用户交换信息的完整性	
			应保护业务应用中的信息交换的安全性，防止欺诈、合同纠纷以及泄露或修改信息事件的发生	
	运行维护管理	日常运行安全管理	★应通过正式授权程序委派专人负责信息系统运行的安全管理	5.5.3.1 a)
			应明确运行值班的日常处理工作和安全管理职责	
			应对运行安全进行监督检查，包括检测、监控、分析等措施	
			应明确各个岗位人员对信息系统各类资源的安全责任，包括日常操作、备份及容错等	
			应明确信息系统安全管理人员和系统用户、普通用户对信息系统资源的访问权限	
			应检查和维护信息系统中业务应用数据完整性、可用性	
		运行状况监控	★委派专人负责监视信息系统重要应用、网络系统、核心服务器等是否运行正常	5.5.3.2 a)
			信息系统应使用统一的时间，以确保记录日志准确	
			信息系统日志应保留一定期限，有脱机保存的介质，不能被改变，只允许授权用户访问	
			定期分析信息系统日志并产生报告	
		软件硬件维护管理	★应明确信息系统的软件、硬件维护的人员和责任，规定维护的时限	5.5.3.3 a)
			应明确信息系统的硬件设备维修、替换和更新的申报、审批和管理流程	
			应明确信息系统软件维护的申报、审批和管理流程	
		外部服务方访问管理	对外部服务方访问的要求，应经过相应的申报和审批程序	5.5.3.4 a)
	★外包服务管理	外包服务合同	★对由组织机构外部服务商承担完成的外包服务，应签署正式的书面合同	5.5.4.1 a)
			对符合法律要求的说明，如数据保护法规	
			对外包服务的风险的说明，包括风险的来源、具体风险描述和风险的影响，明确如何维护并检测组织机构的业务资产的完整性和保密性	
			对外包服务合同各方的安全责任界定，应确保外包合同中的参与方（包括转包商）都了解各自的安全责任	

表 A.5（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	★外包服务管理	外包服务合同	对控制安全风险应采用的控制措施的说明，包括物理和逻辑控制措施，限制授权用户对组织机构的敏感业务信息的访问，以及设备的物理安全保护	5.5.4.1 a)
			对外包服务风险发生时应采取措施的说明，如在发生灾难事故时，应如何维护服务的可用性	
			对外包服务的期限、中止的条件和善后处理的事宜以及由此产生责任问题的说明	
			对审计人员权限的说明	
		外包服务商	应选择具有相应服务资质并信誉好的外包服务商	5.5.4.2 a)
		★外包服务的运行管理	★对外包服务的业务应用系统运行的安全状况应进行监控和检查	5.5.4.3 a)
			对外包服务出现问题应遵照合同规定及时处理和报告	
	有关安全机制保障	★身份鉴别机制管理要求	信息系统所有用户均应明确使用身份鉴别机制的责任，保护用户自己的身份鉴别信息	5.5.5.1 a)
			在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份	
			★在每次用户登录系统时，采用口令鉴别机制进行用户身份鉴别，并对口令数据进行保护	
			应指定安全管理人员定期检查信息系统用户身份鉴别机制和身份鉴别信息的安全性，特别是跨网络的远程用户鉴别信息的安全性	
		★访问控制机制管理要求	应根据自主访问控制安全策略，允许授权用户/用户组对其创建的客体具有相应的访问操作权限，包括对客体的创建、读、写、修改和删除等	5.5.5.2 a)
			实施访问控制机制主体的粒度为用户/用户组，客体的粒度为文件或数据库表级	
			★能够阻止非授权用户读取敏感信息并能将这些权限的部分或全部授予其他用户/用户组	
		系统安全管理要求	应对操作系统和数据库管理系统实施相应的安全管理	5.5.5.3 a)
			应通过正式授权程序委派专人负责系统安全管理	
			建立系统安全配置、备份等安全管理规章制度及操作规程	
			★按规章制度的要求进行正确的系统安全配置、备份等操作，及时进行补丁升级	
		网络安全管理要求	应通过正式授权程序指定网络管理人员	5.5.5.4 a)
			★应按网络区域边界安全控制策略，实施数据包过滤措施，采用常规校验机制检验数据传输的完整性等安全管理，能够发现数据完整性被破坏	
			应制定有关网络系统安全管理和配置的规定，保证网络管理人员按相应规定对网络进行安全管理	

表 A.5（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	有关安全机制保障	应用系统安全管理要求	应通过正式授权程序委派专人负责应用系统的安全管理	5.5.5.5 a)
			对应用系统按其安全技术和机制的要求实施相应的安全管理	
			★具有明确的应用系统管理员对于特定应用系统安全管理内容，如用户及权限管理等，以及应用系统软件的安全配置、备份等	
			应结合业务需求制定相关规章制度，并严格按照规章制度的要求实施应用系统安全管理	
		病毒防护管理要求	安排专人负责计算机病毒防护，定期进行检查报告主机和网络的病毒安全状况	5.5.5.6 a)
			★在主机和网络区域边界安装防病毒软件，并及时升级	
			使用外部移动存储设备之前应进行病毒检查	
			从不信任网络上所接收的文件或邮件，在使用前应首先检查是否有病毒	

A.2.6 业务连续性管理

表 A.6 业务连续性管理（第一级信息系统）

类	族	评估项	评估内容要点	标准依据
业务连续性管理	★备份与恢复	★数据备份和恢复	★应明确说明需定期备份重要业务信息、系统数据及软件等内容和备份周期	5.6.1.1 a)
			确定重要业务信息的保存期以及其他需要保存的归档拷贝的保存期	
			采用离线备份或在线备份方案，定期进行数据增量备份	
			可使用手工或软件产品进行备份和恢复	
	安全事件处理	安全事件划分	安全事件的处置需要贯穿整个安全管理的全过程	5.6.2.1 a)
			安全事件包括不可抗拒的事件、设备故障事件、病毒爆发事件、外部网络入侵事件、内部信息安全事件、内部误用和误操作等事件等	
			应依据安全事件对信息系统的破坏程度、所造成的社会影响及涉及的范围，确定具体信息系统安全事件处置等级的划分原则	
		★安全事件报告和响应	信息安全事件实行分等级响应和处置	5.6.2.2 a)
			★具有通过评审及批准的安全事件报告流程和响应处理流程	
			使所有员工知道报告安全事件程序和责任	
			★信息安全事件发生后，根据其危害和发生的部位，迅速确定事件等级，并根据等级启动相应的响应和处置预案	
			事件处理后应有相应的反馈程序	

表 A.6（续）

类	族	评估项	评估内容要点	标准依据
业务连续性管理	★应急处理	应急处理和灾难恢复	应对信息系统的应急处理有明确的要求，确定应急处理小组，制定具体的应急处理措施	5.6.3.1 a)
			安全管理人员应协助分管领导落实应急处理措施	
		★应急计划	★制定了应急计划（应急计划框架内容包括）	5.6.3.2 a)
			制定应急计划策略，明确制定应急计划所需的职权和相应的管理部门	
			进行业务影响分析，识别关键信息系统和部件，确定优先次序	
			确定防御性控制，减小系统中断的影响，提高系统的可用性；注意采取措施，减少应急计划生存周期费用	
			制定恢复策略，确保系统可以在中断后快速和有效的恢复	
			制定信息系统应急计划，包括恢复受损系统所需的指导方针和规程	
			计划测试、培训和演练，发现计划的不足，培训技术人员	
			计划维护，有规律地更新适应系统发展	
		应急计划的实施保障	应明确应急计划的机构和实施人员，并使其知道在应急计划实施过程中各自的责任	5.6.3.3 a)

A.2.7 监督和检查管理

表 A.7 监督和检查管理（第一级信息系统）

类	族	评估项	评估内容要点	标准依据
监督和检查管理	符合法律要求	★知晓适用的法律	应认识对于信息系统应用范畴适用的所有法律法规	5.7.1.1 a)
			★对信息系统的设计、操作、使用和管理，以及信息管理方面，应认识和规避法律法规禁区，防止出现违法行为	
			保护组织机构的数据信息和个人信息隐私	
			对于详细而准确的法律要求应从组织机构的法律顾问，或者合格的法律从业人员处获得帮助	
		知识产权管理	应建立关于尊重知识产权的策略，防止发生侵犯版权的行为，并形成书面文档	5.7.1.2 a)
			涉及软件开发的工作人员和承包商应做到符合和遵守相关的法律、法规	
		保护证据记录	规定组织机构的重要记录的内容范围，如财务记录、数据库记录、审计日志等	5.7.1.3 a)
			★应按照法律法规的要求保护组织机构的重要记录，防止丢失、毁坏和被篡改	
			被作为证据的记录，信息的内容和保留的时间应遵守国家法律法规的规定	
	审计及监管控制	监管控制	自主保护：依照国家有关法规和 GB 17859—1999 第一级的要求进行自主保护	5.7.3.2 a)

A.2.8 生存周期管理

表 A.8 生存周期管理(第一级信息系统)

类	族	评估项	评估内容要点	标准依据
生存周期管理	★规划和立项管理	系统规划要求	信息系统的管理者应对信息系统的建设和改造,以及近期和远期的发展制定工作计划,并应得到组织机构管理层的批准	5.8.1.1 a)
		系统需求的提出	信息系统应用部门或业务部门需要开发新的业务应用系统或更改已运行的业务应用系统时,以书面形式提出申请	5.8.1.2 a)
		★系统开发的立项	★接到需求申请,须经主管领导审批,或管理层讨论批准后立项	5.8.1.3 a)
	★建设过程管理	★建设项目准备	★对信息系统建设和改造项目应明确指定项目负责人,监督和管理项目的全过程	5.8.2.1 a)
		工程项目外包要求	信息系统工程项目外包,应选择具有服务资质的信誉较好的厂商,要求其已获得国家规定的资质证书、有成功的实施案例	5.8.2.2 a)
		自行开发环境控制	★自行开发项目,要求开发环境与实际运行环境做到物理分开,建立完全独立的两个环境	5.8.2.3 a)
			开发及测试活动也应尽可能分开	
		★安全产品使用要求	信息安全产品包括构成信息系统安全保护功能的信息技术硬件、软件、固件设备,以及安全检查、检测验证工具等	5.8.2.4 a)
			★信息系统使用的信息安全产品应按照相应的安全保护等级的要求选择相应等级的产品	
		★建设项目测试验收	★对信息系统建设和改造项目进行功能及性能测试,保证信息系统建设项目的可用性	5.8.2.5 a)
			应指项目定测试验收负责人	
	系统启用和终止管理	★新系统启用管理	★在新的信息系统或子系统、信息系统设备在启用以前,应经过正式测试验收	5.8.3.1 a)
			由使用者或管理者提出申请,经过相应领导审批才能正式投入使用	
		★终止运行管理	终止运行包括现有信息系统或子系统、主要设备	5.8.3.2 a)
			应由使用者或管理者提出申请并说明原因	
			应由使用者或管理者提出采取的保护措施	
			★经相应领导审批才能正式终止运行	

A.3 第二级信息系统安全管理评估参照表

A.3.1 策略和制度管理

表 A.9 策略和制度管理(第二级信息系统)

类	族	评估项	评估内容要点	标准依据
★策略和制度	★信息安全管理策略	★安全管理目标与范围	★管理对象(信息系统)的基本描述	5.1.1.1 b)
			明确信息系统的管理范围	
			★业务数据和系统服务达到的安全目标,**符合第二级信息系统安全要求**	
		★总体安全管理策略	**制定了较完整的安全管理策略文档**	5.1.1.2 b)
			★明确管理者对信息系统安全的责任,管理方法、支持意向	
			说明对组织机构信息系统有重大意义的安全方针、原则、标准和符合性要求	
			★说明信息系统安全的总体目标、范围、管理原则和**安全技术框架及安全管理框架**	
			划分信息系统不同安全保护等级的管理策略	
			依据国家有关管理规范和技术标准进行保护,**接受国家信息安全监管部门的指导**	
		安全管理策略的制定	由分管信息安全工作的负责人召集	5.1.1.3 b)
			由信息安全职能部门负责制定	
			信息技术及业务人员参加制定	
			★形成**比较完整**的信息系统安全管理策略	
		安全管理策略的发布	**由组织机构负责人签发**	5.1.1.4 b)
			按照有关文件管理程序发布	
	★安全管理规章制度	★安全管理规章制度内容	**制定了较完整的安全管理制度文档**	5.1.2.1 b)
			★包括安全管理活动中重要的管理方面的制度,以及安全管理人员或操作人员的重要操作规程,如信息安全责任、人员安全、系统建设、系统运维、监督检查等方面管理制度	
		安全管理规章制度的制定	**由信息安全职能部门负责制订**	5.1.2.2 b)
			由分管信息安全工作的负责人审批	
			★有正式发布的制度文件或文档	
	策略与制度文档管理	策略与制度文档的评审和修订	由分管信息安全的负责人和安全管理人员负责文档的评审和修订	5.1.3.1 b)
			★**定期或阶段性**检查策略和制度的有效性,对存在不足或需要改进的策略和制度进行修订	
			修订后的策略和制度按规定程序发布	
			发生重大安全事故,组织机构或技术结构发生变化时,对策略和制度进行相应的评审和修订	
			对评审后需要修订的策略和制度文档,应明确指定人员限期完成	

表 A.9（续）

类	族	评估项	评估内容要点	标准依据
★策略和制度	策略与制度文档管理	★策略与制度文档的保管	★指定专人保管	5.1.3.2 b)
			借阅策略和制度文档，以及相关的操作规程文档，应有相应级别负责人审批和登记	

A.3.2 机构和人员管理

表 A.10 机构和人员管理（第二级信息系统）

类	族	评估项	评估内容要点	标准依据
★机构和人员管理	★安全管理机构	★建立安全管理机构	★管理层中应有一人分管信息系统安全工作	5.2.1.1 b)
			★建立管理信息系统安全工作的职能部门，或明确指定一个职能部门兼管信息安全工作	
			配备专职或兼职的安全管理人员	
		★信息安全职能部门	★确定信息安全职能部门基本的安全管理职能	5.2.1.3 a)
			起草组织机构信息系统的安全策略和发展规划	
			★管理信息系统安全日常事务，检查和指导下级单位信息系统安全工作	
			负责或组织安全措施的实施，并参加对安全重要事件的处理	
			监控信息系统安全状况，提出安全分析报告	
			指导和检查各部门和下级单位信息系统安全人员及要害岗位人员的信息系统安全	
			与有关部门共同组成应急处理小组或协助有关部门建立应急处理小组实施相关应急处理	
	★人员管理	★安全管理人员配备	★可配备安全管理人员，安全管理人员不能兼任网络管理人员、系统管理员、数据库管理员等	5.2.3.1 b)
		关键岗位人员管理	★明确关键岗位，如安全管理员、系统管理员、数据库管理员、网络管理员、重要业务开发人员、系统维护人员、重要业务应用操作人员	5.2.3.2 b)
			允许一人多岗，但业务应用操作人员不能由其他关键岗位人员兼任	
			业务开发人员和系统维护人员不能兼任或担负安全管理员、系统管理员、数据库管理员、网络管理员、重要业务应用操作人员等岗位或工作	
			必要时关键岗位人员应采取定期轮岗制度	
			定期安全培训，加强安全和风险防范意识	
		人员录用管理	由人事部门进行人员背景、资质审查，技能考核等，确认其具有基本的专业技术水平，能够掌握信息安全管理基本知识	5.2.3.3 b)
			对关键岗位的人员注重思想品质方面考察	
			安全管理人员应具有基本的系统安全风险分析和评估能力	
			签署保密协议方可上岗	

表 A.10（续）

类	族	评估项	评估内容要点	标准依据
★机构和人员管理	★人员管理	★人员离岗	★立即中止被解雇的、退休的、辞职的或其他原因离开的人员的所有访问权限	5.2.3.4 b)
			收回所有相关证件、密钥、访问控制标记等	
			收回组织机构提供的设备等	
			★管理层和信息系统关键岗位人员调离岗位，应经单位人事部门严格办理调离手续，承诺其调离后的保密要求	
		人员考核与审查	定期对各个岗位的人员进行不同侧重的安全认知和安全技能的考核，作为人员是否适合当前岗位的参考	5.2.3.5 b)
			★定期审查关键岗位人员，如发现其违反安全规定，应控制使用	
		★第三方人员管理	★签署相关安全责任的合同书或保密协议	5.2.3.6 b)
			★规定各类人员的活动范围，进入计算机房**应有书面申请、批准和过程记录，有专人全程监督或陪同**	
			★进行逻辑访问时，应划定范围并**经书面申请**、负责人**批准和过程记录，有专人全程监督或陪同**	
			进行逻辑访问应使用专门设置的临时用户，并进行审计	
	教育和培训	★信息安全教育	让员工知晓信息的敏感性和信息安全的重要性	5.2.4.1 b)
			认识其自身的责任和安全违例会受到纪律惩罚	
			★掌握的信息安全基本知识和技能，**进行对安全政策和操作规程的认知教育和训练**	
			制定并实施安全教育和培训计划，培养信息系统各类人员安全意识	
		信息安全专家	听取信息安全专家的建议	5.2.4.2 a)
			组织专家参与安全威胁的评价，对安全事件给予专业指导和原因调查等	

A.3.3 风险管理

表 A.11 风险管理（第二级信息系统）

类	族	评估项	评估内容要点	标准依据
风险管理	★风险管理要求和策略	风险管理要求	★编制资产清单，对资产价值/重要性进行分析，对信息系统面临的威胁进行初步分析	5.3.1.1 b)
			对关键的系统资源进行定期风险分析和评估	
			产生风险分析报告并向管理层提交	
		★风险管理策略	**制定基本的风险管理策略**	5.3.1.2 a)
			★定期进行信息安全和业务应用方面的风险评估	
			确定信息安全风险管理的基本方法	
			提供风险管理的组织和资源保证	

表 A.11（续）

类	族	评估项	评估内容要点	标准依据
风险管理	风险分析和评估	★资产识别和分析	确定信息系统的资产范围，进行统计和编制资产清单	5.3.2.1 a)
			★进行资产分类和重要性标识	
		威胁识别和分析	★根据以往发生的安全事件、外部提供的资料和积累的经验，对威胁进行分析	5.3.2.2 b)
			结合业务应用、系统结构特点以及访问流程等因素，建立并维护威胁列表	
			根据不同业务系统面临的威胁，对每个或者每类资产有一个威胁列表	
		脆弱性识别和分析	★通过扫描工具、人工检查和渗透测试，获取对系统脆弱性的认识	5.3.2.3 b)
			针对信息系统资产组合、资产分类编制脆弱性列表和脆弱性检查表	
			应了解测试可能带来的后果，并做好充分准备	
			对不同的方法和工具所得出的评估结果，进行综合分析，得到脆弱性等级	
		风险分析和评估要求	**由用户和专家对资产、威胁和脆弱性等方面进行定性综合评估，建议处理和减缓风险的措施，形成风险评估报告**	5.3.2.4 b)
			★评估报告中包括风险级别、风险点等内容，确定信息系统的安全风险状况	
			基于这些报告，要求评估者对信息系统安全措施提出建议	
	风险控制	选择和实施风险控制措施	基于安全等级标准，选择相应等级的安全技术和管理措施	5.3.3.1 b)
			★根据风险评估结果，结合信息系统安全现状，决定信息系统安全的控制措施	
	基于风险的决策	安全确认	★针对信息系统的资产清单、威胁列表、脆弱性列表，结合已采用的安全控制措施，分析存在的残余风险	5.3.4.1 b)
			形成残余风险分析报告，由组织机构的高层管理人员决定残余风险是否可接受	
			编制信息系统残余风险清单，监视残余风险可能诱发的安全事件，及时采取防护措施	
		信息系统运行的决策	信息系统的主管者或运营者应根据安全确认的结果，判断残余风险是否可接受，决定是否允许信息系统继续运行	5.3.4.2 a)
	★风险评估的管理	★评估机构的选择	★有国家主管部门认可的安全服务资质	5.3.5.1 b)
			有良好信誉的评估机构	
			在经过本行业主管部门认可或上级行政领导部门批准的范围内选择	
		评估机构保密要求	★评估机构人员应按照第三方人员管理要求签署保密协议	5.3.5.2 a)
		评估信息的管理	★提交涉及评估需要的资料、数据等各种信息，应规定办理交接手续，防止丢失	5.3.5.3 b)
			提交涉及评估需要的资料、数据等各种信息，必要时可以隐藏或替换核心的或敏感的参数	
		技术检测过程管理	★使用工具或手工进行技术检测，应事先提交测试的技术方案，得到授权方可进行	5.3.5.4 b)
			使用工具或手工进行技术检测，应在被测试方专人监督下按技术方案进行	

A.3.4 环境和资源管理

表 A.12 环境和资源管理(第二级信息系统)

类	族	评估项	评估内容要点	标准依据
环境和资源管理	环境安全管理	环境安全管理要求	★应配置物理环境安全的责任部门和管理人员	5.4.1.1 b)
			建立有关物理环境安全方面的规章制度	
			物理安全方面应达到 GB/T 20271—2006 中 6.2.1 的有关要求	
			★对物理环境划分不同保护等级的安全区域进行管理	
			制定对物理安全设施进行检验、配置、安装、运行的有关制度和保障措施	
			实行关键物理设施的登记制度	
		★机房安全管理要求	★明确机房安全管理的责任人	5.4.1.2 b)
			机房钥匙由专人管理,未经批准,不准任何人私自复制机房钥匙或服务器开机钥匙	
			未经允许的人员不准进入机房	
			机房来访人员应经过正式批准,登记记录应妥善保存以备查	
			获准进入机房的来访人员,**一般应禁止携带个人计算机等电子设备进入机房,其活动范围和操作行为应受到限制,并有机房接待人员负责和陪同**	
			没有指定管理人员的明确准许,任何记录介质、文件材料及各种被保护品均不准带出机房,与工作无关的物品均不准带入机房	
			机房内严禁吸烟及带入火种和水源	
		办公环境安全管理要求	**★防止利用终端系统窃取敏感信息或非法访问**	5.4.1.3 a)
			工作人员下班后,终端计算机应关闭	
			存放敏感文件或信息载体的文件柜应上锁或设置密码	
			工作人员调离部门或更换办公室时,应立即交还办公室钥匙	
			设立独立的会客接待室,不在办公环境接待来访人员	
	资源管理	资产清单管理	★应编制并维护与信息系统相关**详细的资产清单,能够清晰识别每项资产的拥有权、责任人、安全分类以及资产所在的位置等**	5.4.2.1 b)
			信息资产:应用数据、系统数据、安全数据等数据库和数据文档、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、存档信息	
			软件资产:应用软件、系统软件、开发工具和实用程序	
			有形资产:计算机设备(服务器、终端、存储设备等),网络设备(路由器、交换机、安全设备等),移动存储介质(移动硬盘、磁带等),其他技术装备(电源,空调设备等),家具和机房	
			应用业务相关资产:由信息系统控制的或与信息系统密切相关的应用业务的各类资产,由于信息系统或信息的泄露或破坏,这些资产会受到相应的损坏	
			服务:计算和通信服务,通用设备如供暖、照明、供电和空调等	

表 A.12（续）

类	族	评估项	评估内容要点	标准依据
环境和资源管理	资源管理	资产的分类与标识要求	★根据资产的价值/重要性对资产进行标识，可基于资产的价值选择保护措施和进行资产管理	5.4.2.2 b)
			★对信息资产进行分类管理，对信息系统内分属不同业务范围的各类信息，按其对安全性的不同要求分类加以标识	
			用户数据的重要性分类，如国家秘密信息、商业秘密和个人隐私信息、内部专有信息、公开信息等	
			系统数据重要性一般与其所在的系统或子系统的安全保护等级相关	
			根据业务应用的具体情况进行分类分级和标识，纳入规范化管理	
		介质管理	★脱机存放的数据和软件介质，根据重要程度进行标识和分类，存放在由专人管理的介质库中，防止被盗、被毁、被修改以及信息泄漏	5.4.2.3 b)
			介质的归档和查询应有记录，其借阅、拷贝、传输须经相应级别的领导批准后方可执行，并登记在册，对存档介质的目录清单应定期盘点	
			存储介质的销毁必须经批准并按指定方式进行，不得自行销毁，需要销毁的介质，应防止信息泄漏	
			介质应保留 2 个以上的副本，而且要求介质异地存储，存储地的环境要求和管理方法应与本地相同	
		★设备管理要求	对于信息系统的各种软硬件设备的选型、采购、发放或领用，使用者应提出申请，报经相应领导审批，才可以实施	5.4.2.4 b)
			★设备的选型、采购、使用和保管应明确责任人	
			要求设备有专人负责，实行分类管理	
			★通过对资产清单的管理，记录资产的状况和资产使用、转移、废弃及其授权过程	
			★保证设备的完好率	

A.3.5 运行和维护管理

表 A.13 运行和维护管理（第二级信息系统）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	★用户管理	★用户分类管理	用户分类应包括系统用户、普通用户、外部客户用户、临时用户	5.5.1.1 b)
			★按审查和批准的用户分类清单建立用户和分配权限	
			★用户分类清单应包括信息系统的所有用户的清单，包括所有特权用户的权限，以及特权用户的责任人员和授权记录	
			用户权限发生变化时应及时更改用户清单内容	
			定期检查特权用户的实际分配权限是否与特权用户清单符合	
			对特权用户开启审计功能，必要时可对其他有关用户开启审计功能	

表 A.13（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	★用户管理	系统用户要求	★系统用户应由信息系统的主管领导指定	5.5.1.2 b)
			★授权应以满足工作需要的最小权限为原则	
			系统用户应保护自己的身份鉴别信息的安全	
			系统用户应接受审计	
			对重要信息系统的系统用户，应进行审查并经过授权	
			对系统用户应能区分责任到个人，不应以部门或组作为责任人	
		普通用户要求	★用户应保护自己的身份鉴别信息的安全	5.5.1.3 b)
			发现系统的漏洞、滥用或违背安全行为应及时报告	
			不应透露与组织机构有关的非公开信息	
			不应故意进行违规的操作	
			不应在不符合敏感信息保护要求的系统中保存和处理高敏感度的信息	
			不应使用各种非正版软件和不可信的自由软件	
		机构外部用户要求	★应对外部用户明确说明使用者的责任、义务和风险，并要求提供合法使用的声明	5.5.1.4 b)
			外部用户应保护自己的身份鉴别信息的安全	
			外部用户只能是应用层的用户	
			可对特定外部用户提供专用通信通道，端口，特定的应用或数据协议，以及专用设备等	
		临时用户要求	★临时用户的设置和期限必须经过审批	5.5.1.5 b)
			临时用户应保护自己的身份鉴别信息的安全	
			★使用完毕或到期应及时删除	
			设置与删除均应记录备案	
			对主要部位的临时用户应进行审计，并进行风险评估	
	运行操作管理	★服务器操作管理	★服务器操作系统、数据库系统的操作应由授权的系统管理员、数据库管理员实施	5.5.2.1 b)
			★遵照操作规程对服务器进行操作，设置服务器的运行环境，设定服务器的系统及安全配置，操作系统、数据库系统用户管理，并检查实际配置与安全策略要求的符合性	
			系统管理员、数据库管理员应以自己的账户及身份鉴别信息登录操作系统、数据库系统进行操作	
			监控管理，包括监控系统性能，如 CPU 和内存的利用率、检测进程运行及磁盘使用情况	
			日志管理，包括对操作系统、数据库系统以及业务系统等日志的管理	

表 A.13（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	运行操作管理	终端计算机操作管理	★用户应设置终端计算机的开机、屏幕保护口令，保护身份鉴别信息，进行必要的安全设置	5.5.2.2 a)
			非本组织机构配备的终端计算机未获批准，不能在办公场所使用	
			及时安装经许可的软件和补丁程序，不得自行安装及使用其他软件和自由下载软件	
			未获批准，严禁使用 Modem 拨号、无线网卡等方式或另辟通路接入其他网络	
		便携机操作管理	在接入组织机构内部网络时遵守“终端计算机操作管理”（上一节）的要求	5.5.2.3 b)
			对不再使用或转为其他用途的便携机，应删除机内的敏感数据	
			在外网使用的便携机，接入本地网络前应进行必要的安全检查	
			★在组织机构内使用或存有敏感信息的便携机，未获批准，没有安全防护措施的，严禁接入其他网络	
		★网络及安全设备操作管理	★对网络及安全设备的操作应由授权的网络管理员、安全管理员实施，**按照安全策略要求进行网络及安全设备配置**	5.5.2.4 b)
			应按操作规程对网络设备和安全设备进行操作，进行网络和安全设备的运行环境配置和服务设定	
			网络管理员、安全管理员应以自己的账户及身份鉴别信息登录网络设备和安全设备进行操作	
			★定期检查实际配置与安全策略要求的符合性	
		业务应用操作管理	应用系统管理员及业务操作人员应自己的账户及身份鉴别信息登录业务应用系统（提供对外或专门服务的公共用户可除外）	5.5.2.5 b)
			★应用系统管理员根据安全策略和专门授权对应用系统的操作人员等用户及其权限进行管理，监控应用系统的运行	
			用户对业务应用系统的访问权限应受到控制，如以菜单等方式限制操作	
			用户应按照操作规程使用业务应用系统，操作规程应指明具体作业的指令，处理和使用的信息，以及操作步骤	
			业务应用系统操作规程应形成正式文档或帮助文件，需要进行改动时应得到管理层授权	
			操作规程应说明处理错误或其他异常情况的指令，以及在出现意外的操作或技术问题时需要技术支持的联系方法	
			对重要的业务应用操作应根据特别许可的权限执行	
			业务应用操作应进行审计	

表 A.13（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	运行操作管理	★变更控制和重用管理	★信息系统的变更应经过申报和审批才能进行	5.5.2.6 b)
			进行变更应进行记录，对重大变更应评估其潜在影响，向所有相关人员通报变更细节	
			明确中止变更并从失败变更中恢复的责任和处理方法	
			对变更执行情况、过程文档管理，进行定期或不定期的检查	
			设备重用应经过申报和审批才能进行，应清除重用设备中原有信息	
			对设备重用执行情况、过程文档管理，进行定期或不定期的检查	
		信息交换管理	★在信息系统中发布信息和用户交换信息，应符合国家有关政策法规的规定	5.5.2.7 b)
			应采取适当的安全措施保护信息系统中发布信息和用户交换信息的完整性	
			应保护业务应用中的信息交换的安全性，防止欺诈、合同纠纷以及泄露或修改信息事件的发生	
			在组织机构之间进行信息交换应建立安全条件的协议	
			明确业务信息交换管理责任及数据传输的最低安全要求	
	运行维护管理	日常运行安全管理	★应通过正式授权程序委派专人负责信息系统运行的安全管理	5.5.3.1 b)
			应明确运行值班的日常处理工作和安全管理职责，**建立和维护信息系统运行过程管理文档**	
			应对运行安全进行监督检查，包括检测、监控、分析等措施	
			应明确各个岗位人员对信息系统各类资源的安全责任，包括日常操作、备份及容错等	
			应明确信息系统安全管理人员和系统用户、普通用户对信息系统资源的访问权限	
			应检查和维护信息系统中业务应用数据完整性、可用性	
			★应用软件的使用采取授权管理，未经验证的软件不得运行系统中安装，对应用软件的使用进行审计	
			依据总体安全策略，控制和检查外部服务方对信息系统访问的安全	
			执行信息系统的数据备份、病毒防范、安全事件处理、变更控制等安全管理规定的日常工作任务	
			进行应急响应和灾难恢复计划规定的实际演练和技术培训	
			根据组织机构和信息系统出现的各种变化及时修订、完善各种规章制度	
			接受上级或国家有关部门对信息系统安全工作的监督和检查	

表 A.13（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	运行维护管理	运行状况监控	★委派专人负责监视信息系统重要应用、网络系统、核心服务器等是否运行正常，**监视系统性能及与安全机制相关的服务器、网络性能变化**	5.5.3.2 b)
			信息系统应使用统一的时间，以确保记录日志**和审计信息**准确	
			信息系统**审计**日志应保留一定期限，有脱机保存的介质，不能被改变，只允许授权用户访问	
			定期分析信息系统日志并产生报告	
			应告知用户某些行为是会被审计的	
		软件硬件维护管理	★应明确信息系统的软件、硬件维护的人员和责任，规定维护的时限	5.5.3.3 b)
			应明确信息系统的硬件设备维修、替换和更新的申报、审批和管理流程	
			应明确信息系统软件维护的申报、审批和管理流程	
			★对需要外出维修的设备，应经过审批，磁盘数据应进行删除	
			★外部维修人员进入机房维修，应经过审批，并有专人负责陪同	
		外部服务方访问管理	**具有对外部服务方访问管理的相应安全措施**	5.5.3.4 b)
			外部服务方访问应签署了相应的保密合同	
			★对外部服务方访问的要求，应经过相应的申报和审批程序	
	★外包服务管理	★外包服务合同	★对由外部服务商承担完成的外包服务，应签署正式的书面合同	5.5.4.1 a)
			对符合法律要求的说明，如数据保护法规	
			对外包服务的风险的说明，包括风险的来源、具体风险描述和风险的影响，明确如何维护并检测业务资产的完整性和保密性	
			对外包服务合同各方的安全责任界定，应确保外包合同中的参与方（包括转包商）都了解各自的安全责任	
			对控制安全风险应采用的控制措施的说明，包括物理和逻辑控制措施，限制授权用户对敏感业务信息的访问，以及设备的物理安全保护	
			对外包服务风险发生时应采取措施的说明，如在发生灾难事故时，应如何维护服务的可用性	
			对外包服务的期限、中止的条件和善后处理的事宜以及由此产生责任问题的说明	
			对审计人员权限的说明	
		外包服务商	**在行业认可或者是经过上级主管部门批准的范围内**，选择具有相应服务资质并信誉好的可信的外包服务商	5.5.4.2 b)
		★外包服务的运行管理	★对外包服务的业务应用系统运行的安全状况应进行监控和检查，**应定期进行评估**	5.5.4.3 b)
			对外包服务出现问题应遵照合同规定及时处理和报告	
			★当出现重大安全问题或隐患时应进行重新评估，提出改进意见，直至停止外包服务	

表 A.13（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	有关安全机制保障	★身份鉴别机制管理要求	信息系统所有用户均应明确使用身份鉴别机制的责任，保护用户自己的身份鉴别信息**的保密性和完整性**	5.5.5.1 b)
			在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，**并确保在系统整个生存周期用户标识的唯一性**	
			★在每次用户登录系统时，采用受控的口令或具有相应安全强度的其他机制进行用户身份鉴别	
			应指定安全管理人员定期检查信息系统用户身份鉴别机制和身份鉴别信息的安全性，特别是跨网络的远程用户鉴别信息的安全性	
		★访问控制机制管理要求	应根据自主访问控制安全策略，允许授权用户对其创建的客体具有相应的访问操作权限，包括对客体的创建、读、写、修改和删除等	5.5.5.2 b)
			实施访问控制机制主体的粒度为**用户**，客体的粒度为文件或数据库表级	
			★能够阻止非授权用户读取敏感信息并能将这些权限的部分或全部授予其他**用户**	
			实现对自主访问控制过程的审计，告知访问者须为自己的行为负责	
		系统安全管理要求	应通过正式授权程序委派专人负责系统安全管理，包括对操作系统和数据库管理系统管理（系统管理员、数据库管理员）	5.5.5.3 b)
			建立系统安全配置、备份等安全管理规章制度及操作规程	
			★按规章制度的要求进行正确的系统安全配置、备份等操作，及时进行补丁升级	
			对操作系统和数据库系统进行用户账号安全使用和授权管理，并进行审计	
			对授权用户登录系统和使用许可的资源，进行身份鉴别和审计	
			依据安全策略确定审计事件、审计内容、审计归档、审计报告	
			应对系统的安全弱点和漏洞进行控制	
			应依据变更控制规程对系统的变更进行控制	
			应及时对系统资源和系统文档进行备份	
		网络安全管理要求	应通过正式授权程序指定网络管理人员对网络系统进行配置和安全管理	5.5.5.4 b)
			★应按网络区域边界安全控制策略，实施数据包过滤措施，采用常规校验机制检验数据传输的完整性等安全管理，能够发现数据完整性被破坏	
			信息系统网络安全区域边界按访问控制策略设置自主访问控制机制，对进出安全区域边界的数据信息进行控制，阻止非授权访问	
			依据总体安全策略制定网络访问控制策略，并定期检查和完善网络安全策略	

表 A.13（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	有关安全机制保障	网络安全管理要求	采取网络访问授权管理，保证经过授权的用户才能得到许可的网络服务	5.5.5.4 b)
			告知用户使用网络的安全责任和操作规程	
			用户在外部访问组织机构内部网络应经审批，可采用由密码技术支持的保密性、完整性保护机制或具有相应强度的其他安全机制，保护网络数据传输安全	
			定期对外部网络连接接口的安全进行评估，可采用由密码技术支持的保密性、完整性保护机制或具有相应强度的其他安全机制，保护网络数据传输安全	
			对外公共服务的信息系统，应采取严格访问控制，保证外部用户的访问得到控制和审计，不危及内部信息系统的安全	
			对外传输的数据和信息要经过批准和审查，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实施控制和检查，探测非法外联等行为，保护网络及区域边界完整性	
			信息系统的关键网络设备设施的备份进行管理，保证可用性	
			对网络安全日常管理、网络配置变更、网络故障及事件处理等，定期进行安全检查和评估，提交正式的网络安全报告	
		应用系统安全管理要求	应通过正式授权程序委派专人负责应用系统的安全管理(应用系统管理员)	5.5.5.5 b)
			★具有明确的应用系统管理员对于特定应用系统安全管理内容，如用户及权限管理等，以及应用系统软件的安全配置、备份等	
			应结合业务需求制定相关规章制度，制定并落实应用系统的安全操作规程，并严格按照规章制度的要求实施应用系统安全管理	
			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，保证应用系统数据的保密性、完整性和可用性	
			应指定专人负责应用系统的审计工作，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	

表 A.13（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	有关安全机制保障	病毒防护管理要求	安排专人负责计算机病毒防护，定期进行检查报告主机和网络的病毒安全状况	5.5.5.6 b)
			★在主机安装防病毒软件，**在安全区域边界设置防恶意代码网关**，并及时升级，**检查病毒库的升级情况并进行记录**	
			对非在线的内部计算机设备及其他移动存储设备，以及外来或新增计算机做到入网前进行杀毒和防病毒软件版本检测	
			从不信任网络上所接收的文件或邮件，在使用前应首先检查是否有病毒	
		密码管理要求	★**应按国家密码主管部门的规定，对信息系统中使用的密码算法和密钥进行管理**	5.5.5.7 a)
			应按国家有关法律法规要求，对信息系统中包含密码的软、硬件信息处理模块的进、出口进行管理	

A.3.6 业务连续性管理

表 A.14 业务连续性管理（第二级信息系统）

类	族	评估项	评估内容要点	标准依据
业务连续性管理	★备份与恢复	★数据备份和恢复	★应明确说明需定期备份重要业务信息、系统数据及软件等内容和备份周期，**根据数据的重要程度和更新频率设定备份周期**	5.6.1.1 b)
			确定重要业务信息的保存期以及其他需要保存的归档拷贝的保存期	
			采用离线备份或在线备份方案，定期进行数据增量备份	
			指定专人负责数据备份和恢复，可使用手工或软件产品进行备份和恢复，**同时保存几个版本的备份**	
			定期检查备份介质，保证在紧急情况时可以使用	
			定期检查及测试恢复程序，确保在预定的时间内正确恢复	
		设备和系统的备份与冗余	★**实现信息系统的关键设备备份与容错**	5.6.1.2 a)
			指定专人定期维护和检查备份设备的状况，确保需要接入系统时能够正常运行	
			根据实际需求确定备份设备接入的工作流程和操作时间	
	安全事件处理	安全事件划分	安全事件的处置需要贯穿整个安全管理的全过程，**建立信息安全事件分等级响应和处置的制度**	5.6.2.1 b)
			安全事件包括不可抗拒的事件、设备故障事件、病毒爆发事件、外部网络入侵事件、内部信息安全事件、内部误用和误操作等事件等	
			应依据安全事件对信息系统的破坏程度、所造成的社会影响及涉及的范围，确定具体信息系统安全事件处置等级的划分原则	

表 A.14（续）

类	族	评估项	评估内容要点	标准依据
业务连续性管理	安全事件处理	安全事件划分	**★对信息系统中发生的各类事件制定相应安全保护等级的处置预案，确定事件响应和处置的范围、程度及工作流程**	5.6.2.1 b)
			信息安全事件发生后，按预案分等级进行响应和处置	
			在发现或怀疑系统或服务出现安全漏洞或受到威胁时，应按照安全事件处置要求处理	
		★安全事件报告和响应	信息安全事件实行分等级响应和处置	5.6.2.2 b)
			★具有通过评审及批准的安全事件报告流程和响应处理流程，还包括安全弱点和可疑事件的报告	
			对于暂不能确定为事故或入侵等的可疑事件也应报告	
			对于所有安全事件的报告应记录在案归档留存	
			使所有员工知道报告安全事件程序和责任，**告知员工未经许可测试弱点属于滥用系统**	
			★信息安全事件发生后，根据其危害和发生的部位，迅速确定事件等级，并根据等级启动相应的响应和处置预案	
			事件处理后应有相应的反馈程序	
	★应急处理	应急处理和灾难恢复	**安全管理机构应制定总体应急计划和灾难恢复计划，应急处理小组负责落实**	5.6.3.1 b)
			制定关键应用系统和支持系统的应急预案和灾难恢复预案，并进行测试	
			对计划涉及人员进行培训，保证这些人员具有相应执行能力	
			与应急需要应急的外部支持单位，应签订合同	
			做好应急处理和灾难恢复的基础工作，包括安全事件处理，系统及数据备份的管理	
		★应急计划	★制定了应急计划（应急计划框架内容包括）	5.6.3.2 a)
			制定应急计划策略，明确制定应急计划所需的职权和相应的管理部门	
			进行业务影响分析，识别关键信息系统和部件，确定优先次序	
			确定防御性控制，减小系统中断的影响，提高系统的可用性；注意采取措施，减少应急计划生存周期费用	
			制定恢复策略，确保系统可以在中断后快速和有效的恢复	
			制定信息系统应急计划，包括恢复受损系统所需的指导方针和规程	
			计划测试、培训和演练，发现计划的不足，培训技术人员	
			计划维护，有规律地更新适应系统发展	
		应急计划的实施保障	★应明确应急计划的组织和实施人员，并使其知道在应急计划实施过程中各自的责任	5.6.3.3 b)
			对系统相关的人员进行培训和组织演练，知道如何以及何时使用应急计划中的控制手段及恢复策略，保证执行应急计划应具有的能力	

A.3.7 监督和检查管理

表 A.15 监督和检查管理(第二级信息系统)

类	族	评估项	评估内容要点	标准依据
监督和检查管理	符合法律要求	★知晓适用的法律	应认识对于信息系统应用范畴适用的所有法律法规	5.7.1.1 b)
			★对信息系统的设计、操作、使用和管理,以及信息管理方面,应认识和规避法律法规禁区,防止出现违法行为	
			保护组织机构的数据信息和个人信息隐私	
			对于详细而准确的法律要求应从组织机构的法律顾问,或者合格的法律从业人员处获得帮助	
			应知晓不允许滥用信息处理设备,以免危害组织机构和社会利益,并有措施防止滥用	
		知识产权管理	应建立关于尊重知识产权的策略,防止发生侵犯版权的行为,并形成书面文档	5.7.1.2 b)
			涉及软件开发的工作人员和承包商应做到符合和遵守相关的法律、法规	
			应明确规定外包开发的应用系统软件的有关软件版权问题	
			应防止外包开发的应用系统因软件升级或改造发生侵犯软件版权问题	
		保护证据记录	规定组织机构的重要记录的内容范围,如财务记录、数据库记录、审计日志等	5.7.1.3 a)
			★应按照法律法规的要求保护组织机构的重要记录,防止丢失、毁坏和被篡改	
			被作为证据的记录,信息的内容和保留的时间应遵守国家法律法规的规定	
	依从性检查	检查和改进	**要求定期对安全管理活动的各个方面进行检查和评估工作**	5.7.2.1 a)
			★对照组织机构的安全策略和管理制度做到自管、自查、自评、并应落实责任制	
		安全策略依从性检查	**定期检查信息系统的网络、操作系统、数据库系统等系统管理员,对安全策略的遵守情况,包括是否能正确执行安全制度,遵从安全策略**	5.7.2.2 a)
		技术依从性检查	**按照信息系统应达到安全保护等级第二级技术要求**定期进行检查,根据检查信息系统对安全实施标准的符合情况进行初步评价并形成意见	5.7.2.3 a)
	审计及监管控制	★审计控制	**应有独立的审计机构或人员对组织机构的安全管理体系、信息系统的安全风险控制、管理过程的有效性和正确性进行审计**	5.7.3.1 a)
			★对审计过程进行控制,应制定审计的工作程序和规范化工作流程,将审计活动周期化,同时加强安全事件发生后的审计	
		监管控制	**指导保护:在信息安全监管职能部门指导下依照国家有关法规和 GB 17859—1999 第二级的要求进行自主保护**	5.7.3.2 b)

表 A.15（续）

类	族	评估项	评估内容要点	标准依据
监督和检查管理	责任认定	审计结果的责任认定	对于审计及监管过程发现的问题应限期解决	5.7.4.1 a)
			★应认定技术责任和管理责任，明确责任当事人，提出问题解决办法和责任处理意见	
		审计及监管者责任的认定	审计及监管者应按有关监督和检查的规定定期进行审计，逾期未进行审计及监管，使本应审计的问题因未审计而造成信息系统损失，应承担相应的责任	5.7.4.2 a)

A.3.8 生存周期管理

表 A.16 生存周期管理（第二级信息系统）

类	族	评估项	评估内容要点	标准依据
生存周期管理	★规划和立项管理	系统规划要求	信息系统的管理者应对信息系统的建设和改造，以及近期和远期的发展制定工作计划，并应得到管理层的批准	5.8.1.1 b)
			应制定安全策略规划并得到管理层的批准	
			安全策略规划主要包括信息系统的总体安全策略、安全保障体系的安全技术框架和安全管理策略等	
			能够为信息系统安全保障体系的规划、建设和改造提供依据，使管理者和使用者都了解信息系统安全防护的基本原则和策略，知道应采用的各种技术和管理措施对抗各种威胁	
		系统需求的提出	★信息系统应用部门或业务部门需要开发新的业务应用系统或更改已运行的业务应用系统时，以书面形式提出申请	5.8.1.2 b)
			★信息系统的安全管理职能部门应根据信息系统的安全状况和存在隐患的分析，以及信息安全评估结果等提出加强系统安全的具体需求，并以书面形式提出申请	
			安全需求的分析和说明，至少包括组织机构的业务特点和需求，威胁、脆弱性和风险的说明，安全的要求和保护目标	
		★系统开发的立项	接到系统需求的书面申请，必须组织有关部门负责人和有关安全技术专家进行可行性论证	5.8.1.3 b)
			★通过论证后由主管领导审批，或者经过管理层的讨论批准，才能正式立项	
	★建设过程管理	★建设项目准备	★对信息系统建设和改造项目应明确指定项目负责人，监督和管理项目的全过程	5.8.2.1 b)
			应制定详细的项目实施计划，作为项目管理过程的依据	
		工程项目外包要求	信息系统工程项目外包，应选择具有服务资质的信誉较好的厂商，要求其已获得国家规定的资质证书、有成功的实施案例	5.8.2.2 b)
			对重要的信息系统工程项目外包，应在主管部门指定或特定范围内选择具有服务资质的信誉较好的厂商，并应经实践证明是安全可靠的厂商	

表 A.16（续）

类	族	评估项	评估内容要点	标准依据
生存周期管理	★建设过程管理	自行开发环境控制	★自行开发项目，要求开发环境与实际运行环境做到物理分开，建立完全独立的两个环境	5.8.2.3 b)
			开发及测试活动也应尽可能分开	
			系统开发文档和软件应有专人负责保管，系统开发文档的使用须经管理层的批准	
			系统开发文档和软件的变更应按照变更管理流程进行控制	
			一般不鼓励对非自行开发的软件包进行修改，必须改动时应注意内置的控制措施和整合过程被损害的风险，软件的改动对将来的维护带来影响，应保留原始软件并在完全一样的复制件上进行改动，所有的改动应经过充分的测试并形成文件，以便必要时用于将来的软件升级	
		★安全产品使用要求	信息安全产品包括构成信息系统安全保护功能的信息技术硬件、软件、固件设备，以及安全检查、检测验证工具等	5.8.2.4 a)
			★信息系统使用的信息安全产品应按照相应的安全保护等级的要求选择相应等级的产品	
		★建设项目测试验收	★对信息系统建设和改造项目进行功能及性能测试，**进行安全测试验收，保证信息系统建设项目的保密性、完整性、可用性**	5.8.2.5 b)
			应指定项目测试（**包括安全测试**）验收负责人	
			应制订测试和接收标准，确保信息系统建设和改造项目的接收要求和标准被清晰定义并文档化	
			对安全系统的测试至少包括对组成系统的所有部件进行安全性测试，对系统进行集成性安全测试，对业务应用进行安全测试等	
	系统启用和终止管理	★新系统启用管理	★在新的信息系统或子系统、信息系统设备在启用以前，应经过正式测试验收	5.8.3.1 b)
			由使用者或管理者提出申请，经过相应领导审批才能正式投入使用	
			应进行一定期限的试运行，并得到相应领导和技术负责人认可才能正式投入使用，并形成文档备案	
		★终止运行管理	终止运行包括现有信息系统或子系统、主要设备	5.8.3.2 b)
			应由使用者或管理者提出申请并说明原因	
			应由使用者或管理者提出采取的保护措施	
			★在任何新的信息系统或子系统、信息系统设备需要终止运行以前，应进行必要数据和软件备份，对终止运行的设备进行数据清除	
			得到相应领导和技术负责人认可才能正式终止运行，并形成文档备案	

A.4 第三级信息系统安全管理评估参照表

A.4.1 策略和制度管理

表 A.17 策略和制度管理(第三级信息系统)

类	族	评估项	评估内容要点	标准依据
★策略和制度	★信息安全管理策略	★安全管理目标与范围	★管理对象(信息系统)的基本描述	5.1.1.1 c)
			信息系统的管理范围	
			★业务数据和系统服务达到的安全目标,符合第三级信息系统安全要求	
		★总体安全管理策略	制定了体系化的安全管理策略文档	5.1.1.2 c)
			★明确管理者对信息系统安全的责任,管理方法、支持意向	
			说明信息系统的安全方针、原则、标准和符合性要求	
			★说明信息系统安全的总体目标、范围、管理原则和安全技术框架及安全管理框架	
			划分信息系统不同安全保护等级的管理策略	
			依据国家有关管理规范和技术标准进行保护,接受国家信息安全监管部门的监督、检查	
		安全管理策略的制定	由信息安全领导小组组织制定	5.1.1.3 c)
			由信息安全职能部门负责制定	
			由信息安全领导小组组织并提出指导思想,信息安全职能部门负责具体制定	
			信息技术及业务人员参加制定	
			★形成体系化的信息系统安全管理策略,以文件形式表述	
		安全管理策略的发布	由组织机构负责人签发	5.1.1.4 c)
			按照有关文件管理程序发布	
			安全管理策略文档应注明发布范围,并有收发文登记	
	★安全管理规章制度	★安全管理规章制度内容	制定了体系化的安全管理制度文档	5.1.2.1 c)
			包括安全管理活动中各类管理方面的制度,以及安全管理人员或操作人员的操作规程,形成全面的信息安全管理制度体系	
			★信息安全责任管理制度,包括信息安全主管领导、责任部门、人员及有关岗位的信息安全责任管理内容	
			★人员安全管理制度,包括人员录用、离岗、考核、教育培训等管理内容	
			★系统建设管理制度,包括系统定级、方案设计、产品采购使用、密码使用、软件开发、工程实施、验收上线、外包服务等管理内容	
			★系统运维管理制度,包括机房环境安全、存储介质安全、设备设施安全、安全监控、网络安全、系统安全、恶意代码防范、密码保护、备份与恢复、事件处置、应急预案等管理内容	
			★监督检查管理制度,包括对各项制度的落实情况进行自查和监督检查,以及风险评估等管理内容	

表 A.17（续）

类	族	评估项	评估内容要点	标准依据
★策略和制度	★安全管理规章制度	安全管理规章制度的制定	由信息安全职能部门负责制订	5.1.2.2 c)
			经信息安全领导小组评审，由信息安全领导小组负责人审批	
			★有正式发布的制度文件或文档	
			应注明发布范围并有收发文登记	
	策略与制度文档管理	策略与制度文档的评审和修订	由信息安全领导小组和信息安全职能部门负责文档的评审和修订，并保留必要的评审记录和依据	5.1.3.1 c)
			★定期或阶段性检查策略和制度的有效性，对存在不足或需要改进的策略和制度进行修订	
			修订后的策略和制度按规定程序发布	
			★发生重大安全事故，组织机构或技术结构发生变化时，对策略和制度进行相应的评审和修订	
			对评审后需要修订的策略和制度文档，应明确指定人员限期完成	
			每个策略和制度文档应有相应责任人，根据明确规定的评审和修订程序对策略进行维护	
		★策略与制度文档的保管	★指定专人保管	5.1.3.2 c)
			借阅策略和制度文档，以及相关的操作规程文档，应限定借阅范围，并经过相应级别负责人审批和登记	

A.4.2 机构和人员管理

表 A.18 机构和人员管理（第三级信息系统）

类	族	评估项	评估内容要点	标准依据
★机构和人员管理	★安全管理机构	★建立安全管理机构	★管理层中应有一人分管信息系统安全工作，成立信息系统安全管理委员会或信息系统安全领导小组	5.2.1.1 c)
			对覆盖全国或跨地区的组织机构，应在总部和下级单位建立各级信息系统安全领导小组	
			★建立管理信息系统安全工作的职能部门，或明确指定一个职能部门兼管信息安全工作	
			配备专职安全管理人员，在基层至少要有一位专职的安全管理人员负责信息系统安全工作	
		★信息安全领导小组	★具有信息系统安全管理的领导职能	5.2.1.2 a)
			依据国家和行业有关信息安全的政策法规，批准信息系统的安全策略和发展规划	
			确定各有关部门在信息系统安全工作中的职责，领导安全工作的实施	
			监督安全措施的执行，并对重要安全事件的处理进行决策	
			指导和检查信息系统安全职能部门及应急处理小组的各项工作	
			建设和完善信息系统安全的集中控管机制	

表 A.18（续）

类	族	评估项	评估内容要点	标准依据
★机构和人员管理	★安全管理机构	★信息安全职能部门	★确定信息安全职能部门基本的安全管理职能	5.2.1.3 b)
			起草信息系统的安全策略和发展规划	
			★管理信息系统安全日常事务，检查和指导下级单位信息系统安全工作	
			负责或组织安全措施的实施，并参加对安全重要事件的处理	
			监控信息系统安全状况，提出安全分析报告	
			指导和检查各部门和下级单位信息系统安全人员及要害岗位人员的信息系统安全	
			★与有关部门共同组成应急处理小组或协助有关部门建立应急处理小组实施相关应急处理	
			管理信息系统安全机制集中管理机构的各项工作，实现信息系统安全的集中控制管理	
			完成信息系统安全领导小组交办的工作，并向领导小组报告信息系统安全工作	
	安全机制集中管理机构	设置集中管理机构	★明确集中管理机构人员和职责，接受信息安全职能部门的直接领导	5.2.2.1 a)
			配备必要的领导和技术管理人员	
			选用熟悉安全技术、网络技术、系统应用等方面技术人员，明确责任，协同工作	
			统一承担信息系统的安全管理、系统管理、审计管理的运行监控、系统及安全配置	
			对与安全有关的信息进行汇集与分析	
			对与安全有关的事件进行响应与处置	
			对分布在信息系统中有关的安全机制进行集中管理	
		★集中管理机构职能	★集中管理机构统一管理信息系统运行安全，包括系统管理、安全管理和审计管理	5.2.2.2 a)
			建立物理、系统、网络、应用、管理等安全控制机制，构成整体安全控制机制	
			统一进行信息系统安全机制的配置与管理，确保各个安全机制按照设计要求运行	
			对服务器、路由器、防火墙等网络部件、系统安全运行性状态、信息（包括有害内容）的监控和检查	
			汇集各种安全机制所获取的与系统安全运行有关的信息，对所获取的信息进行综合分析	
			及时发现系统运行中的安全问题和隐患，提出解决的对策和方法	
			事件发现、响应、处置、应急恢复、根据应急处理预案，作出快速处理	
			对各种事件和处理结果有详细的记载并进行档案化管理，作为对后续事件分析的参考和可查性的依据	
			安全机制集中管理控制，完善管理信息系统安全运行的技术手段，进行信息系统安全的集中控制管理	
			负责接受和配合政府有关部门的信息安全监管工作	

表 A.18（续）

类	族	评估项	评估内容要点	标准依据
★机构和人员管理	★人员管理	★安全管理人员配备	**★安全管理人员不可兼任，属于专职人员，应具有安全管理工作权限和能力**	5.2.3.1 c)
		关键岗位人员管理	★关键岗位包括安全管理员、系统管理员、数据库管理员、网络管理员、重要业务开发人员、系统维护人员、重要业务应用操作人员	5.2.3.2 c)
			允许一人多岗，但业务应用操作人员不能由其他关键岗位人员兼任	
			业务开发人员和系统维护人员不能兼任或担负安全管理员、系统管理员、数据库管理员、网络管理员、重要业务应用操作人员等岗位或工作	
			★关键岗位人员的权限应分散、不得交叉覆盖，系统管理员、数据库管理员、网络管理员不能相互兼任岗位或工作	
			必要时关键岗位人员应采取定期轮岗制度	
			定期安全培训，加强安全和风险防范意识	
		人员录用管理	由人事部门进行人员背景、资质审查，技能考核等，确认其具有基本的专业技术水平，能够掌握信息安全管理基本知识，**合格者还要签署保密协议方可上岗**	5.2.3.3 c)
			★对关键岗位的人员注重思想品质方面考察，**重要区域或部位的安全管理人员一般可从内部符合条件人员选拔，要求认真负责和保守秘密**	
			安全管理人员应具有基本的系统安全风险分析和评估能力	
		★人员离岗	★立即中止被解雇的、退休的、辞职的或其他原因离开的人员的所有访问权限	5.2.3.4 c)
			收回所有相关证件、密钥、访问控制标记等，	
			收回组织机构提供的设备等	
			管理层和信息系统关键岗位人员调离岗位，应经单位人事部门严格办理调离手续，承诺其调离后的保密要求	
			★管理层和信息系统关键岗位人员调离单位，应进行离岗安全审查，在规定的脱密期限后，方可调离	
		人员考核与审查	定期对各个岗位的人员进行不同侧重的安全认知和安全技能的考核，作为人员是否适合当前岗位的参考	5.2.3.5 c)
			★定期审查关键岗位人员，如发现其违反安全规定，应控制使用	
			★对关键岗位人员的工作，应通过例行考核进行审查，并保留审查结果	
		★第三方人员管理	★签署相关安全责任的合同书或保密协议	5.2.3.6 c)
			★规定各类人员的活动范围，进入计算机房应有书面申请、批准和过程记录，有专人全程监督或陪同	
			★进行逻辑访问时，应划定范围并经书面申请、负责人批准和过程记录，有专人全程监督或陪同	
			进行逻辑访问应使用专门设置的临时用户，并进行审计	

表 A.18（续）

类	族	评估项	评估内容要点	标准依据
★机构和人员管理	★人员管理	★第三方人员管理	**在关键区域，一般不允许第三方人员进入或进行逻辑访问**	5.2.3.6 c)
			如确有必要，除有书面申请外，可采取由组织机构内部人员代为操作的方式，对结果进行必要的过滤后再提供第三方人员，并进行审计	
			必要时对上述过程进行风险评估和记录备案，并对相应风险采取必要的安全补救措施	
	教育和培训	★信息安全教育	让员工知晓信息的敏感性和信息安全的重要性	5.2.4.1 c)
			认识其自身的责任和安全违例会受到纪律惩罚	
			掌握的信息安全基本知识和技能	
			★进行对安全政策和操作规程的认知教育和训练，以及**安全知识、安全技术、安全标准、安全要求、法律责任和业务控制措施等方面培训**	
			制定并实施安全教育和培训计划，**针对不同岗位制定不同的专业培训计划**，培养信息系统各类人员安全意识	
		信息安全专家	听取信息安全专家的建议	5.2.4.2 b)
			组织专家参与安全威胁的评价，对安全事件给予专业指导和原因调查等	
			对于邀请或聘用信息安全专家可提供必要的内部信息，同时应告知专家这些信息的敏感性和保密性	
			应采取必要的安全措施，保证提供的信息在安全可控的范围内	

A.4.3 风险管理

表 A.19 风险管理（第三级信息系统）

类	族	评估项	评估内容要点	标准依据
风险管理	★风险管理要求和策略	风险管理要求	★编制资产清单，对资产价值/重要性进行分析，对信息系统面临的威胁进行初步分析	5.3.1.1 c)
			对关键的系统资源进行定期风险分析和评估	
			使用规范方法和工作流程，进行规范化的风险评估	
			产生风险分析报告**和留存重要过程文档**，并向管理层提交	
		★风险管理策略	制定基本的风险管理策略	5.3.1.2 b)
			★定期进行信息安全和业务应用方面的风险评估	
			确定信息安全风险管理的基本方法	
			提供风险管理的组织和资源保证	
			★**建立风险管理的监督机制，对风险管理相关过程的活动和影响进行评估和监控**	

表 A.19（续）

类	族	评估项	评估内容要点	标准依据
风险管理	风险分析和评估	★资产识别和分析	确定信息系统的资产范围，进行统计和编制资产清单	5.3.2.1 b)
			★进行资产分类和重要性标识	
			★对信息系统的硬件、软件、系统边界、接口、数据和信息、人员等方面的分析和识别	
			对信息系统的描述，包括信息系统的使命、功能，以及系统和数据的关键性、敏感性等内容	
		威胁识别和分析	★根据以往发生的安全事件、外部提供的资料和积累的经验，对威胁进行分析	5.3.2.2 c)
			★结合业务应用、系统结构特点以及访问流程等因素，建立并维护威胁列表	
			根据不同业务系统面临的威胁，对每个或者每类资产有一个威胁列表	
			考虑威胁源在保密性、完整性或可用性等方面造成损害，对威胁的可能性和影响等属性进行分析，从而确定威胁的等级	
			通过综合威胁的可能性和强度的评价，修正威胁等级	
		脆弱性识别和分析	★通过扫描工具、人工检查和渗透测试，获取对系统脆弱性的认识	5.3.2.3 c)
			针对信息系统资产组合、资产分类编制脆弱性列表和脆弱性检查表	
			应了解测试可能带来的后果，并做好充分准备	
			★对不同的方法和工具所得出的评估结果，进行综合分析，得到脆弱性等级	
			坚持制度化脆弱性评估，应明确规定进行脆弱性评估的时间和系统范围、人员和责任、评估结果的分析和报告程序，以及报告中包括新发现的漏洞、已修补的漏洞、漏洞趋势分析等	
		风险分析和评估要求	由用户和专家对资产、威胁和脆弱性等方面进行定性综合评估，建议处理和减缓风险的措施，形成风险评估报告	5.3.2.4 c)
			★评估报告中包括风险级别、风险点等内容，确定信息系统的安全风险状况	
			基于这些报告，要求评估者对信息系统安全措施提出建议	
			应将风险评估中的信息资产、威胁、脆弱性、防护措施等评估项信息综合到一个数据库中进行管理	
			应在后续的项目和工具中持续地维护该数据库	
	风险控制	选择和实施风险控制措施	基于安全等级标准，选择相应等级的安全技术和管理措施	5.3.3.1 c)
			★根据风险评估结果，结合信息系统安全现状和需求，决定信息系统安全的控制措施	
			对相关的各种控制措施进行综合分析，得出紧迫性、优先级、投资比重等评价，形成体系化的防护控制系统	

表 A.19（续）

类	族	评估项	评估内容要点	标准依据
风险管理	基于风险的决策	安全确认	★针对信息系统的资产清单、威胁列表、脆弱性列表，结合已采用的安全控制措施，分析存在的残余风险	5.3.4.1 c)
			形成残余风险分析报告，由组织机构的高层管理人员决定残余风险是否可接受	
			★编制信息系统残余风险清单，监视残余风险可能诱发的安全事件，及时采取防护措施	
			对信息系统安全风险实施再次评估，验证防护措施的有效性	
		信息系统运行的决策	★信息系统的主管者或运营者应根据安全确认的结果，判断残余风险是否可接受，决定是否允许信息系统继续运行	5.3.4.2 b)
			如果信息系统的残余风险不可接受，而现实情况又要求系统必须投入运行，且当前没有其他资源能胜任组织机构的使命，经过管理层的审批，可临时批准信息系统投入运行	
			应同时采取相应的风险规避和监测控制措施，并明确风险一旦发生的责任陈述	
	★风险评估的管理	★评估机构的选择	★有国家主管部门认可的安全服务资质	5.3.5.1 b) 及公通字[2007]43号文件第22条
			在经本行业主管部门认可或上级行政领导部门批准的范围内，选择有良好信誉的评估机构	
			★在中华人民共和国境内注册成立（港澳台地区除外）	
			★由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）	
			★从事相关检测评估工作两年以上，无违法记录	
			★工作人员仅限于中国公民	
			★法人及主要业务、技术人员无犯罪记录	
			★使用的技术装备、设施应当符合本办法对信息安全产品的要求	
			★具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度	
			★对国家安全、社会秩序、公共利益不构成威胁	
		评估机构保密要求	★评估机构人员应按照第三方人员管理要求签署保密协议	5.3.5.2 b)
			应有专人在整个评估过程中监督检查评估机构对保密协议的执行情况	
		评估信息的管理	★提交涉及评估需要的资料、数据等各种信息，应规定办理交接手续，防止丢失	5.3.5.3 c)
			提交涉及评估需要的资料、数据等各种信息，必要时可以隐藏或替换核心的或敏感的参数	
			所有提交涉及评估需要的资料、数据等各种信息，只能存放在被评估方指定的计算机内，不得带出指定办公区域	

表 A.19（续）

类	族	评估项	评估内容要点	标准依据
风险管理	★风险评估的管理	技术检测过程管理	★使用工具或手工进行技术检测，应事先提交测试的技术方案，得到授权方可进行	5.3.5.4 c)
			使用工具或手工进行技术检测，应在被测试方专人监督下按技术方案进行	
			使用工具或手工进行技术检测，可采用由被评估方技术人员按技术方案进行操作，评估机构技术人员进行场外指导	

A.4.4 环境和资源管理

表 A.20 环境和资源管理（第三级信息系统）

类	族	评估项	评估内容要点	标准依据
环境和资源管理	环境安全管理	环境安全管理要求	★应配置物理环境安全的责任部门和管理人员	5.4.1.1 c)
			建立有关物理环境安全方面的规章制度	
			物理安全方面应达到 GB/T 20271—2006 中 6.3.1 的有关要求	
			★对物理环境划分不同保护等级的安全区域进行**明确标识**和管理，**包括机房、办公区域、介质库房等**	
			介质库房的管理可以参照同等级的机房的要求	
			制定对物理安全设施进行检验、配置、安装、运行的有关制度和保障措施	
			实行关键物理设施的登记制度	
		★机房安全管理要求	★明确机房安全管理的责任人	5.4.1.2 c)
			机房钥匙由专人管理，未经批准，不准任何人私自复制机房钥匙或服务器开机钥匙	
			★未经允许的人员不准进入机房	
			机房来访人员应经过正式批准，登记记录应妥善保存以备查	
			获准进入机房的来访人员，一般应禁止携带个人计算机等电子设备进入机房，其活动范围和操作行为应受到限制，并有机房接待人员负责和陪同，**进入机房的人员应佩戴相应证件**	
			任何进出机房的人员应经过门禁设施的监控和记录，应有防止绕过门禁设施的手段	
			门禁系统的电子记录应妥善保存以备查	
			未经批准，禁止任何人移动计算机相关设备或带离机房	
			★没有指定管理人员的明确准许，任何记录介质、文件材料及各种被保护品均不准带出机房，与工作无关的物品均不准带入机房	
			机房内严禁吸烟及带入火种和水源	

表 A.20（续）

类	族	评估项	评估内容要点	标准依据
环境和资源管理	环境安全管理	办公环境安全管理要求	★防止利用终端系统窃取敏感信息或非法访问	5.4.1.3 b)
			工作人员下班后，终端计算机应关闭	
			存放敏感文件或信息载体的文件柜应上锁或设置密码	
			工作人员调离部门或更换办公室时，应立即交还办公室钥匙	
			设立独立的会客接待室，不在办公环境接待来访人员	
			工作人员离开座位应将桌面上含有敏感信息的纸件文档放在抽屉或文件柜内	
			工作人员离开座位，终端计算机应退出登录状态、采用屏幕保护口令保护或关机	
	资源管理	资产清单管理	★应编制并维护与信息系统相关详细的资产清单，能够清晰识别每项资产的拥有权、责任人、安全分类以及资产所在的位置等	5.4.2.1 c)
			信息资产：应用数据、系统数据、安全数据等数据库和数据文档、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、存档信息	
			软件资产：应用软件、系统软件、开发工具和实用程序	
			有形资产：计算机设备（服务器、终端、存储设备等），网络设备（路由器、交换机、安全设备等），移动存储介质（移动硬盘、磁带等），其他技术装备（电源，空调设备等），家具和机房	
			应用业务相关资产：由信息系统控制的或与信息系统密切相关的应用业务的各类资产，由于信息系统或信息的泄露或破坏，这些资产会受到相应的损坏	
			服务：计算和通信服务，通用设备如供暖、照明、供电和空调等	
			★必要时应包括主要业务应用系统处理流程和数据流的描述，以及业务应用系统用户分类说明	
		资产的分类与标识要求	★根据资产的价值/重要性对资产进行标识，可基于资产的价值选择保护措施和进行资产管理	5.4.2.2 c)
			★对信息资产进行分类管理，对信息系统内分属不同业务范围的各类信息，按其对安全性的不同要求分类加以标识	
			用户数据的重要性分类，如国家秘密信息、商业秘密和个人隐私信息、内部专有信息、公开信息等	
			系统数据重要性一般与其所在的系统或子系统的安全保护等级相关	
			根据业务应用的具体情况进行分类分级和标识，纳入规范化管理	
			以业务应用为主线，用体系架构的方法描述信息资产	
			通过对各个资产之间的关联，进行结构性描述	

表 A.20（续）

类	族	评估项	评估内容要点	标准依据
环境和资源管理	资源管理	介质管理	★脱机存放的数据和软件介质，根据重要程度进行标识和分类，存放在由专人管理的介质库中，防止被盗、被毁、被修改以及信息泄漏	5.4.2.3 c)
			介质的归档和查询应有记录，其借阅、拷贝、**分发传递**须经相应级别的**领导的书面审批后方可执行**，并登记在册，对存档介质的目录清单应定期盘点，**介质的分发传递以及带出工作环境应采取保护措施**	
			存储介质的销毁必须经批准并按指定方式进行，不得自行销毁，**对于需要送出维修或销毁的介质，应首先删除信息，再重复写操作进行覆盖，防止数据恢复和信息泄漏**	
			介质应保留 2 个以上的副本，而且要求介质异地存储，存储地的环境要求和管理方法应与本地相同，**对重要介质的数据和软件必要时可以加密存储**	
			★**对存放在介质库中的介质应定期进行完整性和可用性检查，确认其数据或软件没有受到损坏或丢失**	
		设备管理要求	对于信息系统的各种软硬件设备的选型、采购、发放或领用，使用者应提出申请，报经相应领导审批，才可以实施	5.4.2.4 c)
			★设备的选型、采购、使用和保管应明确责任人	
			要求设备有专人负责，实行分类管理	
			★通过对资产清单的管理，记录资产的状况和资产使用、转移、废弃及其授权过程	
			★**对各种资产进行全面管理，提高资产安全性和使用效率**，保证设备的完好率	
			建立资产管理登记系统，提供资产分类标识、授权与访问控制、变更管理、系统安全审计等功能，为整个系统提供基础技术支撑	

A.4.5 运行和维护管理

表 A.21 运行和维护管理（第三级信息系统）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	★用户管理	★用户分类管理	用户分类应包括系统用户、普通用户、外部客户用户、临时用户	5.5.1.1 c)
			★按审查和批准的用户分类清单建立用户和分配权限	
			★用户分类清单应包括信息系统的所有用户的清单，包括所有特权用户、**重要业务用户**的权限，以及特权用户的责任人员和授权记录	
			用户权限发生变化时应及时更改用户清单内容	
			对特权用户、**重要业务用户开启审计功能**	
			定期检查特权用户、**重要业务用户的实际分配权限是否与用户清单符合**	

表 A.21（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	★用户管理	系统用户要求	★系统用户应由信息系统的主管领导指定	5.5.1.2 c)
			★授权应以满足工作需要的最小权限为原则	
			系统用户应保护自己的身份鉴别信息的安全	
			系统用户应接受审计	
			对重要信息系统的系统用户，应进行审查并经过授权	
			★对系统用户应能区分责任到个人，不应以部门或组作为责任人	
			在关键信息系统中，对系统用户的授权操作，应有两人在场，经双重认可后方可操作	
			系统用户不准更改操作过程产生的审计日志	
		普通用户要求	★用户应保护自己的身份鉴别信息**和载体**的安全，**不得转借他人**	5.5.1.3 c)
			发现系统的漏洞、滥用或违背安全行为应及时报告	
			不应透露与组织机构有关的非公开信息	
			不应故意进行违规的操作	
			不应在不符合敏感信息保护要求的系统中保存和处理高敏感度的信息	
			不应使用各种非正版软件和不可信的自由软件	
			在系统规定的权限内进行操作，必要时某些重要操作应得到批准	
		机构外部用户要求	★应对外部用户明确说明使用者的责任、义务和风险，并要求提供合法使用的声明	5.5.1.4 c)
			外部用户应保护自己的身份鉴别信息的安全	
			外部用户只能是应用层的用户	
			可对特定外部用户提供专用通信通道，端口，特定的应用或数据协议，以及专用设备等	
			在关键部位，一般不允许设置外部用户	
		临时用户要求	★临时用户的设置和期限必须经过审批	5.5.1.5 c)
			临时用户应保护自己的身份鉴别信息的安全	
			★使用完毕或到期应及时删除	
			设置与删除均应记录备案	
			对主要部位的临时用户应进行审计，并进行风险评估	
			★**在关键部位，一般不允许设置临时用户**	
	运行操作管理	★服务器操作管理	★服务器操作系统、数据库系统的操作应由授权的系统管理员、数据库管理员实施	5.5.2.1 c)
			★遵照操作规程对服务器进行操作，设置服务器的运行环境，设定服务器的系统及安全配置，操作系统、数据库系统用户管理，并检查实际配置与安全策略要求的符合性	

表 A.21（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	运行操作管理	★服务器操作管理	系统管理员、数据库管理员应以自己的账户及身份鉴别信息登录操作系统、数据库系统进行操作	5.5.2.1 c)
			监控管理，包括监控系统性能，如 CPU 和内存的利用率、检测进程运行及磁盘使用情况	
			日志管理，包括对操作系统、数据库系统以及业务系统等日志的管理	
			负责系统配置和安全配置文件管理，包括服务器的操作系统和数据库系统的配置文件	
			★定期对操作系统和数据库系统安全进行检查，及时发现系统的缺陷或漏洞	
		终端计算机操作管理	★用户应设置终端计算机的开机、屏幕保护口令，保护身份鉴别信息，进行必要的安全设置	5.5.2.2 b)
			非本组织机构配备的终端计算机未获批准，不能在办公场所使用	
			及时安装经许可的软件和补丁程序，不得自行安装及使用其他软件和自由下载软件	
			未获批准，严禁使用 Modem 拨号、无线网卡等方式或另辟通路接入其他网络	
			应有措施防止终端计算机机箱被私自开启，如需拆机箱应经批准后由维修部门人员负责	
			高安全等级业务系统的终端计算机不得直接接入低级别系统或网络，应先作清理检查	
		便携机操作管理	在接入组织机构内部网络时遵守“终端计算机操作管理”（上一节）的要求	5.5.2.3 c)
			对不再使用或转为其他用途的便携机，应删除机内的敏感数据	
			在外网使用的便携机，接入本地网络前应进行必要的安全检查	
			★在组织机构内使用或存有敏感信息的便携机，未获批准，没有安全防护措施的，严禁接入其他网络	
			便携机离开重要区域时不应存储敏感或涉密数据，外出使用应经有关领导批准并记录在案	
			在重要区域使用的便携机必须启用两个及两个以上身份鉴别技术的组合来进行身份鉴别	
		★网络及安全设备操作管理	★对网络及安全设备的操作应由授权的网络管理员、安全管理员实施，按照安全策略要求进行网络及安全设备配置	5.5.2.4 c)
			应按操作规程对网络设备和安全设备进行操作，进行网络和安全设备的运行环境配置和服务设定	
			网络管理员、安全管理员应以自己的账户及身份鉴别信息登录网络设备和安全设备进行操作	
			★定期检查实际配置与安全策略要求的符合性	
			应通过集中安全管理设施对网络及安全设备的安全机制进行监控管理和部署策略	

表 A.21（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	运行操作管理	业务应用操作管理	应用系统管理员及业务操作人员应自己的账户及身份鉴别信息登录业务应用系统（提供对外或专门服务的公共用户可除外）	5.5.2.5 c）
			★应用系统管理员根据安全策略和专门授权对应用系统的操作人员等用户及其权限进行管理，监控应用系统的运行	
			用户对业务应用系统的访问权限应受到控制，如以菜单等方式限制操作	
			用户应按照操作规程使用业务应用系统，操作规程应指明具体作业的指令，处理和使用的信息，以及操作步骤	
			业务应用系统操作规程应形成正式文档或帮助文件，需要进行改动时应得到管理层授权	
			操作规程应说明处理错误或其他异常情况的指令，以及在出现意外的操作或技术问题时需要技术支持的联系方法	
			对重要的业务应用操作应根据特别许可的权限执行，**关键的业务应用操作应有 2 人同时在场或同时操作，并对操作过程进行记录**	
			业务应用操作应进行审计	
		★变更控制和重用管理	★信息系统的变更，应**提出更改方案并得到系统主管领导的审批**才能进行	5.5.2.6 c）
			进行变更应进行记录，对重大变更应评估其潜在影响，**考虑全面安全事务一致性，更改后将变更结果书面**向所有相关人员通报	
			操作系统、数据库系统的变更控制与应用系统的更改控制应相互配合	
			通过审计日志和过程记录，记载更改中的所有有关信息	
			明确中止变更并从失败变更中恢复的责任和处理方法	
			对变更执行情况、过程文档管理，进行定期或不定期的检查	
			设备重用，应**提出设备重用方案并得到系统主管领导的审批**才能进行，应清除重用设备中原有信息	
			对设备重用执行情况、过程文档管理，进行定期或不定期的检查	
		信息交换管理	★在信息系统中发布信息和用户交换信息，应符合国家有关政策法规的规定	5.5.2.7 c）
			应采取适当的安全措施保护信息系统中发布信息和用户交换信息的完整性	
			应保护业务应用中的信息交换的安全性，防止欺诈、合同纠纷以及泄露或修改信息事件的发生	
			在组织机构之间进行信息交换应建立安全条件的协议	
			明确业务信息交换管理责任及数据传输的最低安全要求	
			还对于信息系统内部不同安全区域之间的信息传输，应有明确的安全要求	

表 A.21（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	运行维护管理	日常运行安全管理	★应通过正式授权程序委派专人负责信息系统运行的安全管理和**风险控制**	5.5.3.1 c)
			应明确运行值班的日常处理工作和安全管理职责，建立和维护信息系统运行过程管理文档	
			应对运行安全进行监督检查，包括检测、监控、分析等措施	
			应明确各个岗位人员对信息系统各类资源的安全责任，包括日常操作、备份及容错等	
			应明确信息系统安全管理人员和系统用户、普通用户对信息系统资源的访问权限	
			对信息系统关键岗位人员采取最小授权和分权制衡措施，如关键安全操作双人共管	
			应检查和维护信息系统中业务应用数据完整性、可用性	
			★应用软件的使用采取授权管理，未经验证的软件不得运行系统中安装，对应用软件的使用进行审计	
			依据总体安全策略，控制和检查外部服务方对信息系统访问的安全，**对外部服务方访问实施监视，并定期进行风险分析**	
			执行信息系统的数据备份、病毒防范、安全事件处理、变更控制等安全管理规定的日常工作任务	
			进行应急响应和灾难恢复计划规定的实际演练和技术培训，**明确专人负责执行情况检查，如数据备份和备用设备的可用性**	
			根据组织机构和信息系统出现的各种变化及时修订、完善各种规章制度，**控制各方面安全事务管理的一致性等**	
			接受上级或国家有关部门对信息系统安全工作的监督和检查	
		运行状况监控	★委派专人负责监视信息系统重要应用、网络系统、核心服务器等是否运行正常，监视系统性能及与安全机制相关的服务器、网络性能变化	5.5.3.2 c)
			信息系统应使用统一的时间，以确保记录日志和审计信息准确	
			信息系统审计日志应保留一定期限，有脱机保存的介质，不能被改变，只允许授权用户访问	
			定期分析信息系统日志并产生报告	
			应告知用户某些行为是会被审计的	
			安全机制集中管理机构负责信息系统安全管理、系统管理、审计管理的集中监控和分析	

表 A.21（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	运行维护管理	软件硬件维护管理	★应明确信息系统的软件、硬件维护的人员和责任，规定维护的时限	5.5.3.3 c)
			对涉及维修的重要区域的数据和软件系统采取保护措施，防止因维修造成破坏和泄漏	
			应明确信息系统的硬件设备维修、替换和更新的申报、审批和管理流程	
			应明确信息系统软件维护的申报、审批和管理流程	
			★对需要外出维修的设备，应经过审批，磁盘数据应进行删除	
			★外部维修人员进入机房维修，应经过审批，并有专人负责陪同	
			应对维修过程及有关故障现象记录备案	
		外部服务方访问管理	**对外部服务方访问实施严格控制，采取对外部服务方访问实施监视等安全措施**	5.5.3.4 c)
			应对外部服务方访问的要求**进行风险分析**，并经过相应的申报和审批程序	
			★外部服务方访问应签署了相应的保密合同	
	★外包服务管理	★外包服务合同	★对由外部服务商承担完成的外包服务，应签署正式的书面合同	5.5.4.1 a)
			对符合法律要求的说明，如数据保护法规	
			对外包服务的风险的说明，包括风险的来源、具体风险描述和风险的影响，明确如何维护并检测业务资产的完整性和保密性	
			对外包服务合同各方的安全责任界定，应确保外包合同中的参与方（包括转包商）都了解各自的安全责任	
			对控制安全风险应采用的控制措施的说明，包括物理和逻辑控制措施，限制授权用户对组织机构的敏感业务信息的访问，以及设备的物理安全保护	
			对外包服务风险发生时应采取措施的说明，如在发生灾难事故时，应如何维护服务的可用性	
			对外包服务的期限、中止的条件和善后处理的事宜以及由此产生责任问题的说明	
			对审计人员权限的说明	
		外包服务商	**外包服务的限制，关键的或敏感的业务应用，一般不应采用业务应用系统外包服务方式**	5.5.4.2 c)
			★在行业认可或者是经过上级主管部门批准的范围内，选择具有相应服务资质并信誉好的可信的外包服务商	
		★外包服务的运行管理	**★系统运行的外包限制，关键的或敏感的业务应用，一般不应采用业务应用系统运行的外包方式**	5.5.4.3 b)
			★对外包服务的业务应用系统运行的安全状况应进行监控和检查，应定期进行评估	
			对外包服务出现问题应遵照合同规定及时处理和报告	
			★当出现重大安全问题或隐患时应进行重新评估，提出改进意见，直至停止外包服务	

表 A.21（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	有关安全机制保障	★身份鉴别机制管理要求	信息系统所有用户均应明确使用身份鉴别机制的责任，保护用户自己的身份鉴别信息的保密性和完整性	5.5.5.1 c)
			在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性	
			★在每次用户登录系统时，采用受安全管理中心控制的口令、令牌、基于生物特征、数字证书以及其他具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别	
			应指定安全管理人员定期检查信息系统用户身份鉴别机制和身份鉴别信息的安全性，特别是跨网络的远程用户鉴别信息的安全性	
		★访问控制机制管理要求	应根据自主访问控制安全策略，允许授权用户对其创建的客体具有相应的访问操作权限，包括对客体的创建、读、写、修改和删除等	5.5.5.2 c)
			实施访问控制机制主体的粒度为用户，客体的粒度为文件或数据库表级**和（或）记录或字段级，强制访问控制客体的粒度为文件或数据库表级**	
			★能够阻止非授权用户读取敏感信息并能将这些权限的部分或全部授予其他用户	
			实现对自主访问控制过程的审计，告知访问者须为自己的行为负责	
			应由授权的安全管理员通过特定专用方式对主、客体进行安全标记；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制	
			应确保信息系统内的所有主、客体具有一致的标记信息，并实施同一安全策略的强制访问控制规则	
		系统安全管理要求	应通过正式授权程序委派专人负责系统安全管理，包括对操作系统和数据库管理系统管理（系统管理员、数据库管理员）	5.5.5.3 c)
			建立系统安全配置、备份等安全管理规章制度及操作规程	
			由授权的系统安全员通过系统提供的操作界面，根据访问控制安全策略设置、维护用户及主、客体的标记信息	
			★按规章制度的要求进行正确的系统安全配置、备份等操作，及时进行补丁升级	
			对操作系统和数据库系统进行用户账号安全使用和授权管理，并进行审计	
			对授权用户登录系统和使用许可的资源，进行身份鉴别和审计	
			依据安全策略确定审计事件、审计内容、审计归档、审计报告	
			应对系统的安全弱点和漏洞进行控制，**对可能危及系统安全的系统工具进行严格的控制**	
			应依据变更控制规程对系统的变更进行控制，**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**	
			应及时对系统资源和系统文档进行备份**和安全标识**	
			制定操作系统和数据库管理系统应急计划	

表 A.21（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	有关安全机制保障	网络安全管理要求	应通过正式授权程序指定网络管理人员对网络系统进行配置和安全管理	5.5.5.4 c)
			★应按网络区域边界安全控制策略，实施数据包过滤措施，采用常规校验机制检验数据传输的完整性等安全管理，能够发现数据完整性被破坏，**并在发现完整性被破坏时进行恢复**	
			信息系统网络安全区域边界按访问控制策略设置自主和强制访问控制机制，对进出安全区域边界的数据信息进行控制，阻止非授权访问	
			依据总体安全策略制定网络访问控制策略，并定期检查和完善网络安全策略	
			采取网络访问授权管理，保证经过授权的用户才能得到许可的网络服务	
			告知用户使用网络的安全责任和操作规程	
			用户在外部访问组织机构内部网络应经审批，可采用由密码技术支持的保密性、完整性保护机制或具有相应强度的其他安全机制，保护网络数据传输安全	
			定期对外部网络连接接口的安全进行评估，可采用由密码技术支持的保密性、完整性保护机制或具有相应强度的其他安全机制，保护网络数据传输安全	
			对外公共服务的信息系统，应采取严格访问控制，保证外部用户的访问得到控制和审计，不危及内部信息系统的安全	
			对外传输的数据和信息要经过批准和审查，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实施控制和检查，探测非法外联等行为，保护网络及区域边界完整性	
			信息系统的关键网络设备设施的备份进行管理，保证可用性	
			对网络安全日常管理、网络配置变更、网络故障及事件处理等，定期进行安全检查和评估，提交正式的网络安全报告	
			可采用由密码技术支持的可信网络连接机制，通过对连接到通信网络的设备进行可信检验，确保接入通信网络的设备真实可信，防止设备的非法接入	
			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	

表 A.21（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	有关安全机制保障	应用系统安全管理要求	应通过正式授权程序委派专人负责应用系统的安全管理(应用系统管理员)	5.5.5.5 c)
			★具有明确的应用系统管理员对于特定应用系统安全管理内容，如用户及权限管理等，以及应用系统软件的安全配置、备份等	
			应结合业务需求制定相关规章制度，制定并落实应用系统的安全操作规程，并严格按照规章制度的要求实施应用系统安全管理	
			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，保证应用系统数据的保密性、完整性和可用性	
			应指定专人负责应用系统的审计工作，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	
			对应用系统软件的使用采取授权管理，未授权用户不得在在运行系统中安装、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	
			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负责应用系统的安全配置管理和应用管理	
		病毒防护管理要求	安排专人负责计算机病毒防护，定期进行检查报告主机和网络的病毒安全状况	5.5.5.6 c)
			★在主机安装防病毒软件，在安全区域边界设置防恶意代码网关，并及时升级，检查病毒库的升级情况并进行记录	
			对非在线的内部计算机设备及其他移动存储设备，以及外来或新增计算机做到入网前进行杀毒和防病毒软件版本检测	
			从不信任网络上所接收的文件或邮件，在使用前应首先检查是否有病毒	
			在网络内部建立专门的防病毒软件升级服务，实行整体策略、定期升级、统一控制，紧急情况下增加升级次数	
			采取对系统所有终端防范病毒软件集中管理的措施	

表 A.21（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	有关安全机制保障	密码管理要求	★应按国家密码主管部门的规定，对信息系统中使用的密码算法和密钥进行管理	5.5.5.7 b)
			应按国家有关法律法规要求，对信息系统中包含密码的软、硬件信息处理模块的进、出口进行管理	
	安全集中管理	★安全机制集中控管	★对信息系统所涉及的服务器、网络、安全设备以及应用系统等的安全管理、系统管理、审计管理机制实施集中的监控、配置和管理	5.5.6.1 a)
			建立一体化和开放性平台，提供标准的接口，具备对安全资源管理能力	
			对系统的资源和运行进行配置、控制和管理，包括用户身份管理、系统资源配置、系统加载和启动、系统运行的异常处理以及支持管理本地和（或）异地灾难备份与恢复等	
			对系统中的主体、客体进行统一标记，对主体进行授权，对服务器、网络设备、安全设备等配置一致的安全策略	
			对分布在系统各个组成部分的安全审计机制进行集中管理，对审计记录应进行分析，并根据分析结果进行处理	
			授权的安全、系统、审计管理员应以自己的账户和身份鉴别信息进行登录和操作	
		安全信息集中管理	★将信息系统安全管理信息、系统管理信息、审计管理信息实施集中管理、综合分析	5.5.6.2 a)
			提供可视化报表和安全事件分析过程，以及安全事件的管理与辅助分析机制	
		安全机制整合要求	进行信息系统资产信息管理	5.5.6.3 a)
			进行信息系统网络异常流量监控	
			进行信息系统安全事件监控管理	
			进行信息系统脆弱性管理	
			进行信息系统安全策略管理	
			进行信息系统安全预警管理	
		安全机制整合的处理方式	主要工作方式可包括自动处理、人工干预处理、远程处理、辅助决策分析处理、记录和事后处理等	5.5.6.4 a)

A.4.6 业务连续性管理

表 A.22 业务连续性管理(第三级信息系统)

类	族	评估项	评估内容要点	标准依据
业务连续性管理	★备份与恢复	★数据备份和恢复	★应明确说明需定期备份重要业务信息、系统数据及软件等内容和备份周期,根据数据的重要程度和更新频率设定备份周期	5.6.1.1 c)
			确定重要业务信息的保存期以及其他需要保存的归档拷贝的保存期	
			采用离线备份或在线备份方案,定期进行数据增量备份**和应用系统全备份,必要时应采用热备份方式保存数据**	
			指定专人负责数据备份和恢复,可使用手工或软件产品进行备份和恢复,同时保存几个版本的备份	
			定期检查备份介质,保证在紧急情况时可以使用	
			定期检查及测试恢复程序,确保在预定的时间内正确恢复	
			应分别指定专人负责不同方式的数据备份和恢复,并保存必要的操作记录	
		设备和系统的备份与冗余	★实现信息系统的关键设备备份与容错,**实现系统热备份与冗余**	5.6.1.2 b)
			★指定专人定期维护和检查备份设备**和冗余设备**的状况,确保需要接入系统时能够正常运行	
			根据实际需求确定备份设备接入的工作流程和操作时间,**根据实际需求限定系统热备份和冗余设备切换的时间**	
			指定专人定期维护和检查热备份的运行状况,定期进行切换试验,确保需要时能正常运行	
	安全事件处理	安全事件划分	安全事件的处置需要贯穿整个安全管理的全过程,建立信息安全事件分等级响应和处置的制度	5.6.2.1 c)
			安全事件包括不可抗拒的事件、设备故障事件、病毒爆发事件、外部网络入侵事件、内部信息安全事件、内部误用和误操作等事件等	
			应依据安全事件对信息系统的破坏程度、所造成的社会影响及涉及的范围,确定具体信息系统安全事件处置等级的划分原则	
			★对信息系统中发生的各类事件制定相应安全保护等级的处置预案,确定事件响应和处置的范围、程度及工作流程	
			信息安全事件发生后,按预案分等级进行响应和处置	
			在发现或怀疑系统或服务出现安全漏洞或受到威胁时,应按照安全事件处置要求处理	
			明确不同安全事件的管理责任,制定不同安全事件的管理流程,包括制定处理预案、分析原因、收集证据、处理过程控制、总结吸取教训、责任划分和追究等内容	

表 A.22（续）

类	族	评估项	评估内容要点	标准依据
业务连续性管理	安全事件处理	★安全事件报告和响应	信息安全事件实行分等级响应和处置	5.6.2.2 c)
			★具有通过评审及批准的安全事件报告流程和响应处理流程，还包括安全弱点和可疑事件的报告	
			对于暂不能确定为事故或入侵等的可疑事件也应报告	
			对于所有安全事件的报告应记录在案归档留存	
			使所有员工知道报告安全事件程序和责任，告知员工未经许可测试弱点属于滥用系统	
			★信息安全事件发生后，根据其危害和发生的部位，迅速确定事件等级，并根据等级启动相应的响应和处置预案	
			要求安全管理机构或职能部门负责接报安全事件报告，并及时进行处理，注意记录事件处理过程	
			对于重要区域或业务应用发生的安全事件，应注意控制事件的影响	
			事件处理后应有相应的反馈程序，**应追究安全事件发生的技术原因和管理责任，写出处理报告，并进行必要的评估**	
	★应急处理	应急处理和灾难恢复	**★信息安全领导小组应有人负责或指定专人负责应急计划和灾难恢复计划管理工作**	5.6.3.1 c)
			信息系统安全机制集中管理机构应协助应急处理小组负责具体落实	
			检查或验证（演练）应急计划和灾难恢复计划，保证应急计划和灾难恢复计划能够有效执行	
			安全管理机构应制定总体应急计划和灾难恢复计划，应急处理小组负责落实	
			制定**关键和重要的**应用系统和支持系统的应急预案和灾难恢复预案，并进行测试	
			对计划涉及人员进行培训，保证这些人员具有相应执行能力	
			与应急需要应急的外部支持单位，应签订合同	
			做好应急处理和灾难恢复的基础工作，包括安全事件处理、系统及数据备份的管理	
		★应急计划	★制定了应急计划（应急计划框架内容包括）	5.6.3.2 a)
			制定应急计划策略，明确制定应急计划所需的职权和相应的管理部门	
			进行业务影响分析，识别关键信息系统和部件，确定优先次序	
			确定防御性控制，减小系统中断的影响，提高系统的可用性；注意采取措施，减少应急计划生存周期费用	
			制定恢复策略，确保系统可以在中断后快速和有效的恢复	
			制定信息系统应急计划，包括恢复受损系统所需的指导方针和规程	
			计划测试、培训和演练，发现计划的不足，培训技术人员	
			计划维护，有规律地更新适应系统发展	

表 A.22（续）

类	族	评估项	评估内容要点	标准依据
业务连续性管理	★应急处理	应急计划的实施保障	★应明确应急计划的组织和实施人员，并使其知道在应急计划实施过程中各自的责任	5.6.3.3 c)
			对系统相关的人员进行培训和组织演练，知道如何以及何时使用应急计划中的控制手段及恢复策略，保证执行应急计划应具有的能力	
			进行系统化管理用于实施和维护整个应急计划体系，并记录计划实施过程	
			确保应急计划的执行有足够资源的保证	

A.4.7 监督和检查管理

表 A.23 监督和检查管理（第三级信息系统）

类	族	评估项	评估内容要点	标准依据
监督和检查管理	符合法律要求	★知晓适用的法律	应认识对于信息系统应用范畴适用的所有法律法规	5.7.1.1 c)
			★对信息系统的设计、操作、使用和管理，以及信息管理方面，应认识和规避法律法规禁区，防止出现违法行为	
			保护组织机构的数据信息和个人信息隐私	
			对于详细而准确的法律要求应从组织机构的法律顾问，或者合格的法律从业人员处获得帮助	
			应知晓不允许滥用信息处理设备，以免危害组织机构和社会利益，并有措施防止滥用	
			★信息系统中采用的密码技术应使用国家主管部门批准的算法，符合国家有关法规的要求	
		知识产权管理	应建立关于尊重知识产权的策略，防止发生侵犯版权的行为，并形成书面文档	5.7.1.2 c)
			涉及软件开发的工作人员和承包商应做到符合和遵守相关的法律、法规	
			应明确规定外包开发的应用系统软件的有关软件版权问题	
			应防止外包开发的应用系统因软件升级或改造发生侵犯软件版权问题	
			★对关键业务应用，必要时应要求使用具有自主知识产权的软件，以保护关键业务应用的安全	
		保护证据记录	规定组织机构的重要记录的内容范围，如财务记录、数据库记录、审计日志等	5.7.1.3 a)
			★应按照法律法规的要求保护组织机构的重要记录，防止丢失、毁坏和被篡改	
			被作为证据的记录，信息的内容和保留的时间应遵守国家法律法规的规定	

表 A.23（续）

类	族	评估项	评估内容要点	标准依据
监督和检查管理	依从性检查	检查和改进	要求定期对安全管理活动的各个方面进行检查和评估工作	5.7.2.1 b)
			建立检查和改进制度，做到定期检查实施的所有安全程序是否遵从了组织机构制定的安全方针和政策，检查信息系统在技术方面是否依从了安全标准，根据检查过程中发现的不足对安全管理体系进行不断改进	
			★对照组织机构的安全策略和管理制度做到自管、自查、自评，并应落实责任制，**接受国家监管部门的监管**	
		★安全策略依从性检查	定期检查信息系统的网络、操作系统、数据库系统等系统管理员，对安全策略的遵守情况，包括是否能正确执行安全制度，遵从安全策略	5.7.2.2 b)
			★定期检查信息系统各个岗位对操作规程和管理制度的执行情况，确保遵从组织的安全策略	
			检查范围应包括信息系统本身，以及系统供应商、信息和信息资产的所有者、用户和管理层，保证其符合安全策略和标准	
		★技术依从性检查	**★按照信息系统应达到安全保护等级第三级技术要求定期进行检查，**根据检查信息系统对安全实施标准的符合情况进行初步评价并形成意见（依据技术评估结果）	5.7.2.3 b)
			对硬件和软件的检验，以及技术依从检查应由有能力的、经过授权的人员来进行	
			对于技术检测应由有经验的系统工程师手工或使用软件包进行并生成检测结果，经技术专家解释并产生技术报告	
			应根据检查结果，对存在的缺陷进行不断改进	
	审计及监管控制	★审计控制	应有独立的审计机构或人员对组织机构的安全管理体系、信息系统的安全风险控制、管理过程的有效性和正确性进行审计	5.7.3.1 b)
			★对审计过程进行控制，应制定审计的工作程序和规范化工作流程，将审计活动周期化，同时加强安全事件发生后的审计	
			应对系统的审计活动进行规划，尽量减小中断业务流程的风险	
			系统审计过程控制要求，审计的范围必须经过授权并得到控制，审计所需的资源应明确定义并保证可用性，应审计和记录所有的访问，对所有的流程、需求和责任都应文档化	
		监管控制	**依照国家有关法规和 GB 17859—1999 第三级的要求进行自主保护，信息安全监管职能部门对其进行监督、检查**	5.7.3.2 c)
	责任认定	审计结果的责任认定	对于审计及监管过程发现的问题应限期解决	5.7.4.1 b)
			★应认定技术责任和管理责任，明确责任当事人，提出问题解决办法和责任处理意见	
			应对审计及监管过程发现的问题认定相关领导者的责任，组织机构领导层应就此提出问题解决办法和责任处理意见，以及监督问题解决情况	
		审计及监管者责任的认定	审计及监管者应按有关监督和检查的规定定期进行审计，逾期未进行审计及监管，使本应审计的问题因未审计而造成信息系统损失，应承担相应的责任	5.7.4.2 b)
			审计及监管者虽能够按有关监督和检查的规定进行审计，但因未能及时发现本应审计出问题而造成信息系统损失的，应承担相应的责任	

A.4.8 生存周期管理

表 A.24 生存周期管理(第三级信息系统)

类	族	评估项	评估内容要点	标准依据
生存周期管理	★规划和立项管理	系统规划要求	信息系统的管理者应对信息系统的建设和改造,以及近期和远期的发展制定工作计划,并应得到管理层的批准	5.8.1.1 c)
			应制定安全策略规划并得到管理层的批准	
			安全策略规划主要包括信息系统的总体安全策略、安全保障体系的安全技术框架和安全管理策略等	
			能够为信息系统安全保障体系的规划、建设和改造提供依据,使管理者和使用者都了解信息系统安全防护的基本原则和策略,知道应采用的各种技术和管理措施对抗各种威胁	
			依据安全策略规划,制定安全建设和安全改造的规划,并应得到组织机构管理层的批准	
		系统需求的提出	★信息系统应用部门或业务部门需要开发新的业务应用系统或更改已运行的业务应用系统时,以书面形式提出申请	5.8.1.2 c)
			★信息系统的安全管理职能部门应根据信息系统的安全状况和存在隐患的分析,以及信息安全评估结果等提出加强系统安全的具体需求,并以书面形式提出申请	
			安全需求的分析和说明,至少包括组织机构的业务特点和需求,威胁、脆弱性和风险的说明,安全的要求和保护目标	
			信息系统的管理者应根据信息系统安全建设规划的要求,提出当前应进行安全建设和安全改造的具体需求,并以书面形式提出申请	
		★系统开发的立项	接到系统需求的书面申请,必须组织有关部门负责人和有关安全技术专家进行可行性论证和**安全性评价**	5.8.1.3 c)
			★**通过可行性论证和确认项目安全性符合要求后**由主管领导审批,或者经过管理层的讨论批准,才能正式立项	
	★建设过程管理	★建设项目准备	★对信息系统建设和改造项目应明确指定项目负责人,监督和管理项目的全过程,**明确信息系统建设和改造项目的管理流程**	5.8.2.1 c)
			应制定详细的项目实施计划,作为项目管理过程的依据	
			建立工程实施监理管理制度,明确指定项目实施监理负责人	
		工程项目外包要求	信息系统工程项目外包,应选择具有服务资质的信誉较好的厂商,要求其已获得国家规定的资质证书、有成功的实施案例	5.8.2.2 c)
			对重要的信息系统工程项目外包,应在主管部门指定或特定范围内选择具有服务资质的信誉较好的厂商,并应经实践证明是安全可靠的厂商	
			对外包中被废止和暂停的项目,要确保相关的系统设计、文档、代码等的安全	
			对代码的所有权和知识产权、软件开发过程质量控制、代码质量检测、上线前的安全测试等制定控制措施	

表 A.24（续）

类	族	评估项	评估内容要点	标准依据
生存周期管理	★建设过程管理	自行开发环境控制	★自行开发项目，要求开发环境与实际运行环境做到物理分开，建立完全独立的两个环境	5.8.2.3 c)
			开发及测试活动也应尽可能分开	
			系统开发文档应有专人负责保管，系统开发文档的使用须经管理层的批准	
			系统开发文档的变更应按照变更管理流程进行控制	
			一般不鼓励对非自行开发的软件包进行修改，必须改动时应注意内置的控制措施和整合过程被损害的风险，软件的改动对将来的维护带来影响，应保留原始软件并在完全一样的复制件上进行改动，所有的改动应经过充分的测试并形成文件，以便必要时用于将来的软件升级	
			应严格控制对源程序的访问，源程序不应被保存在运行系统中，技术开发人员不应具有对程序资源库不受限制的访问权，源程序库的更新和向程序员发布的程序源应经授权，应保留程序的所有版本，程序清单应被保存在一个安全的环境中，应保存对所有源程序库访问的审计记录	
		★安全产品使用要求	信息安全产品包括构成信息系统安全保护功能的信息技术硬件、软件、固件设备，以及安全检查、检测验证工具等	5.8.2.4 a) 及公通字[2007]43号文件第21条
			★信息系统使用的信息安全产品应按照相应的安全保护等级的要求选择相应等级的产品	
			★产品研制、生产单位是由中国公民、法人投资或者国家投资或者控股的，在中华人民共和国境内具有独立的法人资格	
			★产品的核心技术、关键部件具有我国自主知识产权	
			★产品研制、生产单位及其主要业务、技术人员无犯罪记录	
			★产品研制、生产单位声明没有故意留有或者设置漏洞、后门、木马等程序和功能	
			★对国家安全、社会秩序、公共利益不构成危害	
			★对已列入信息安全产品认证目录的，应当取得国家信息安全产品认证机构颁发的认证证书	
		★建设项目测试验收	★对信息系统建设和改造项目进行功能及性能测试，进行安全测试验收，保证信息系统建设项目的保密性、完整性、可用性	5.8.2.5 c)
			应指定项目测试（包括安全测试）验收负责人	
			应制订测试和接收标准，确保信息系统建设和改造项目的接收要求和标准被清晰定义并文档化	
			对安全系统的测试至少包括对组成系统的所有部件进行安全性测试，对系统进行集成性安全测试，对业务应用进行安全测试等	
			在信息系统建设和改造项目验收时至少还应考虑系统性能和容量的要求，错误恢复、重启程序及应急计划，制定并测试日常的操作程序以达到规定的标准，实施了设计方案规定的安全控制措施，提供了有效的用户指南，新系统对组织机构业务的安全影响，操作和使用新系统的培训	

表 A.24（续）

类	族	评估项	评估内容要点	标准依据
生存周期管理	系统启用和终止管理	★新系统启用管理	★在新的信息系统或子系统、信息系统设备在启用以前，应经过正式测试验收	5.8.3.1 c)
			由使用者或管理者提出申请，经过相应领导审批才能正式投入使用	
			应进行一定期限的试运行，并得到相应领导和技术负责人认可才能正式投入使用，并形成文档备案	
			组织有关管理者、技术负责人、用户和安全专家，对新的信息系统或子系统、信息系统设备的试运行进行专项安全评估，得到认可并形成文档备案才能正式投入使用	
		★终止运行管理	终止运行包括现有信息系统或子系统、主要设备	5.8.3.2 c)
			应由使用者或管理者提出申请并说明原因	
			应由使用者或管理者提出采取的保护措施	
			★在任何新的信息系统或子系统、信息系统设备需要终止运行以前，应进行必要数据和软件备份，对终止运行的设备进行数据清除	
			得到相应领导和技术负责人认可才能正式终止运行，并形成文档备案	
			★应采取必要的安全措施，并进行数据和软件备份，对终止运行的设备进行不可恢复的数据清除，如果存储设备损坏则必须采取销毁措施，在得到相应领导和技术负责人认可才能正式终止运行，并形成文档备案	

A.5 第四级信息系统安全管理评估参照表

A.5.1 策略和制度管理

表 A.25 策略和制度管理（第四级信息系统）

类	族	评估项	评估内容要点	标准依据
★策略和制度	★信息安全管理策略	★安全管理目标与范围	★管理对象（信息系统）的基本描述	5.1.1.1 d)
			信息系统的管理范围	
			★业务数据和系统服务达到的安全目标，**符合第四级信息系统安全要求**	
		★总体安全管理策略	**制定了强制保护的安全管理策略文档**	5.1.1.2 d)
			★明确管理者对信息系统安全的责任，管理方法、支持意向	
			说明信息系统的安全方针、原则、标准和符合性要求	
			★说明信息系统安全的总体目标、范围、管理原则和安全技术框架及安全管理框架	
			划分信息系统不同安全保护等级的管理策略	
			依据国家有关管理规范和技术标准进行保护，**接受国家信息安全监管部门的强制监督、检查**	

表 A.25（续）

类	族	评估项	评估内容要点	标准依据
★策略和制度	★信息安全管理策略	安全管理策略的制定	由信息安全领导小组组织制定**并提出指导思想**	5.1.1.3 d)
			由信息安全职能部门负责**指派专人负责**制定	
			由信息安全领导小组组织并提出指导思想，信息安全职能部门负责具体制定	
			信息技术及业务人员参加制定	
			★形成体系化的信息系统安全管理策略，**包括总体策略和具体策略**，以文件形式表述	
			涉密系统安全策略的制定应限定在相应范围内进行	
			必要时可征求信息安全监管职能部门的意见	
		安全管理策略的发布	由组织机构负责人签发	5.1.1.4 d)
			按照有关文件管理程序发布	
			安全管理策略文档应注明发布范围，并有收发文登记	
			安全管理策略文档应注明密级，并在监管部门备案	
	★安全管理规章制度	★安全管理规章制度内容	**制定了强制保护的安全管理制度文档**	5.1.2.1 d)
			包括安全管理活动中各类管理方面的制度，以及安全管理人员或操作人员的操作规程，形成全面的信息安全管理制度体系	
			★信息安全责任管理制度，包括信息安全主管领导、责任部门、人员及有关岗位的信息安全责任管理内容	
			★人员安全管理制度，包括人员录用、离岗、考核、教育培训等管理内容	
			★系统建设管理制度，包括系统定级、方案设计、产品采购使用、密码使用、软件开发、工程实施、验收上线、外包服务等管理内容	
			★系统运维管理制度，包括机房环境安全、存储介质安全、设备设施安全、安全监控、网络安全、系统安全、恶意代码防范、密码保护、备份与恢复、事件处置、应急预案等管理内容	
			★监督检查管理制度，包括定期对各项制度的落实情况进行自查和监督检查，以及风险评估等管理内容	
			★有关业务应用安全方面的管理制度	
		安全管理规章制度的制定	由信息安全职能部门负责制定，**指派专人负责专项信息系统安全管理制度维护**	5.1.2.2 d)
			经信息安全领导小组讨论通过，由信息安全领导小组负责人审批	
			★有正式发布的制度文件或文档	
			应注明发布范围、**注明密级**，并有收发文登记	
			对信息系统涉密的安全管理制度的制定应在相应范围内进行，必要时可征求信息安全监管职能部门的意见	

表 A.25（续）

类	族	评估项	评估内容要点	标准依据
★策略和制度	策略与制度文档管理	策略与制度文档的评审和修订	由信息安全领导小组和信息安全职能部门负责文档的评审和修订，**必要时可征求信息安全监管职能部门的意见**，并保留必要的评审记录和依据	5.1.3.1 d)
			★定期或阶段性检查策略和制度的有效性，对存在不足或需要改进的策略和制度进行修订	
			修订后的策略和制度按规定程序发布	
			★发生重大安全事故，组织机构或技术结构发生变化时，对策略和制度进行相应的评审和修订	
			对评审后需要修订的策略和制度文档，应明确指定人员限期完成	
			每个策略和制度文档应有相应责任人，根据明确规定的评审和修订程序对策略进行维护	
			对涉密的信息安全策略、规章制度和相关的操作规程文档的评审和修订应在相应范围内进行	
		★策略与制度文档的保管	★指定专人保管	5.1.3.2 d)
			借阅策略和制度文档，以及相关的操作规程文档，应限定借阅范围，并经过相应级别负责人审批和登记	
			对涉密的策略和制度文档，以及相关的操作规程文档的保管应按照有关涉密文档管理规定进行；对保管的文档以及借阅的记录定期进行检查	

A.5.2 机构和人员管理

表 A.26 机构和人员管理（第四级信息系统）

类	族	评估项	评估内容要点	标准依据
★机构和人员管理	★安全管理机构	★建立安全管理机构	★成立信息系统安全管理委员会或信息系统安全领导小组，**由组织机构的主要负责人出任信息系统安全领导小组负责人**	5.2.1.1 d)
			对覆盖全国或跨地区的组织机构，应在总部和下级单位建立各级信息系统安全领导小组	
			★建立管理信息系统安全工作的职能部门，或明确指定一个职能部门兼管信息安全工作	
			配备专职安全管理人员，在基层至少要有一位专职的安全管理人员负责信息系统安全工作	
		★信息安全领导小组	★具有信息系统安全管理的领导职能	5.2.1.2 a)
			依据国家和行业有关信息安全的政策法规，批准信息系统的安全策略和发展规划	
			确定各有关部门在信息系统安全工作中的职责，领导安全工作的实施	
			监督安全措施的执行，并对重要安全事件的处理进行决策	
			指导和检查信息系统安全职能部门及应急处理小组的各项工作	
			建设和完善信息系统安全的集中控管的组织体系和管理机制	

表 A.26（续）

类	族	评估项	评估内容要点	标准依据
★机构和人员管理	★安全管理机构	★信息安全职能部门	★确定信息安全职能部门基本的安全管理职能	5.2.1.3 b)
			起草信息系统的安全策略和发展规划	
			★管理信息系统安全日常事务，检查和指导下级单位信息系统安全工作	
			负责安全措施的实施或组织实施，组织并参加对安全重要事件的处理	
			监控信息系统安全状况，提出安全分析报告	
			★指导和检查各部门和下级单位信息系统安全人员及要害岗位人员的信息系统安全	
			★与有关部门共同组成应急处理小组或协助有关部门建立应急处理小组实施相关应急处理	
			管理信息系统安全机制集中管理机构的各项工作，实现信息系统安全的集中控制管理	
			完成信息系统安全领导小组交办的工作，并向领导小组报告信息系统安全工作	
	安全机制集中管理机构	设置集中管理机构	★明确集中管理机构人员和职责，接受信息安全职能部门的直接领导	5.2.2.1 a)
			配备必要的领导和技术管理人员	
			选用熟悉安全技术、网络技术、系统应用等方面技术人员，明确责任，协同工作	
			统一承担信息系统的安全管理、系统管理、审计管理的运行监控、系统及安全配置	
			对与安全有关的信息进行汇集与分析	
			对与安全有关的事件进行响应与处置	
			对分布在信息系统中有关的安全机制进行集中管理	
		★集中管理机构职能	★集中管理机构统一管理信息系统运行安全，包括系统管理、安全管理和审计管理	5.2.2.2 b)
			集中管理机构对关键区域的安全运行进行管理，控制知晓范围，对获取的有关信息进行相应安全等级的保护	
			建立物理、系统、网络、应用、管理等安全控制机制，构成整体安全控制机制	
			统一进行信息系统安全机制的配置与管理，确保各个安全机制按照设计要求运行	
			对服务器、路由器、防火墙等网络部件、系统安全运行性状态、信息（包括有害内容）的监控和检查	
			汇集各种安全机制所获取的与系统安全运行有关的信息，对所获取的信息进行综合分析	

表 A.26（续）

类	族	评估项	评估内容要点	标准依据
★机构和人员管理	安全机制集中管理机构	★集中管理机构职能	及时发现系统运行中的安全问题和隐患，提出解决的对策和方法	5.2.2.2 b)
			事件发现、响应、处置、应急恢复，根据应急处理预案，作出快速处理	
			对各种事件和处理结果有详细的记载并进行档案化管理，作为对后续事件分析的参考和可查性的依据	
			安全机制集中管理控制，完善管理信息系统安全运行的技术手段，进行信息系统安全的集中控制管理	
			负责接受和配合政府有关部门的信息安全监管工作	
	★人员管理	★安全管理人员配备	★安全管理人员不可兼任，属于专职人员，应具有安全管理工作权限和能力	5.2.3.1 d)
			安全管理人员应按照机要人员条件配备	
		★关键岗位人员管理	★关键岗位包括安全管理员、系统管理员、数据库管理员、网络管理员、重要业务开发人员、系统维护人员、重要业务应用操作人员，安全审计人员	5.2.3.2 d)
			允许一人多岗，但业务应用操作人员不能由其他关键岗位人员兼任	
			业务开发人员和系统维护人员不能兼任或担负安全管理员、系统管理员、数据库管理员、网络管理员、重要业务应用操作人员等岗位或工作	
			★关键岗位人员的权限应分散、不得交叉覆盖，系统管理员、数据库管理员、网络管理员不能相互兼任岗位或工作	
			关键岗位人员处理重要事务或操作时，应保持二人同时在场，关键事务应多人共管	
			必要时关键岗位人员应采取定期轮岗制度	
			定期安全培训，加强安全和风险防范意识	
		人员录用管理	由人事部门进行人员背景、资质审查，技能考核等，确认其具有基本的专业技术水平，能够掌握信息安全管理基本知识，合格者还要签署保密协议方可上岗	5.2.3.3 d)
			★对关键岗位的人员注重思想品质方面考察，重要区域或部位的安全管理人员一般可从内部符合条件人员选拔，要求认真负责和保守秘密	
			安全管理人员应具有基本的系统安全风险分析和评估能力	
			关键区域或部位的安全管理人员应选用实践证明精干、内行、忠实、可靠的人员，必要时可按机要人员条件配备	
		★人员离岗	★立即中止被解雇的、退休的、辞职的或其他原因离开的人员的所有访问权限	5.2.3.4 d)
			收回所有相关证件、密钥、访问控制标记等	
			收回组织机构提供的设备等	
			★管理层和信息系统关键岗位人员调离岗位，应经单位人事部门严格办理调离手续，承诺其调离后的保密要求	
			管理层和信息系统关键岗位人员调离单位，应进行离岗安全审查，在规定的脱密期限后，方可调离	
			关键部位的信息系统安全管理人员离岗，应按照机要人员管理办法办理	

表 A.26（续）

类	族	评估项	评估内容要点	标准依据
★机构和人员管理	★人员管理	★人员考核与审查	定期对各个岗位的人员进行不同侧重的安全认知和安全技能的考核，作为人员是否适合当前岗位的参考	5.2.3.5 d)
			★定期审查关键岗位人员，如发现其违反安全规定，应控制使用	
			★对关键岗位人员的工作，应通过例行考核进行审查，并保留审查结果	
			★对所有安全岗位人员的工作，应通过全面考核进行审查，如发现其违反安全规定，应采取必要的应对措施	
		★第三方人员管理	★签署相关安全责任的合同书或保密协议	5.2.3.6 c)
			★规定各类人员的活动范围，进入计算机房应有书面申请、批准和过程记录，有专人全程监督或陪同	
			★进行逻辑访问时，应划定范围并经书面申请、负责人批准和过程记录，有专人全程监督或陪同	
			进行逻辑访问应使用专门设置的临时用户，并进行审计	
			★在关键区域，一般不允许第三方人员进入或进行逻辑访问	
			如确有必要，除有书面申请外，可采取由组织机构内部人员带为操作的方式，对结果进行必要的过滤后再提供第三方人员，并进行审计	
			必要时对上述过程进行风险评估和记录备案，并对相应风险采取必要的安全补救措施	
	教育和培训	★信息安全教育	让员工知晓信息的敏感性和信息安全的重要性	5.2.4.1 d)
			认识其自身的责任和安全违例会受到纪律惩罚	
			掌握的信息安全基本知识和技能	
			★进行对安全政策和操作规程的认知教育和训练，以及安全知识、安全技术、安全标准、安全要求、法律责任和业务控制措施等方面培训	
			制定并实施安全教育和培训计划，针对不同岗位制定不同的专业培训计划，培养信息系统各类人员安全意识	
			定期检查人员安全资质的取得情况，将安全资质教育作为信息安全教育工作计划的一部分	
		信息安全专家	听取信息安全专家的建议	5.2.4.2 b)
			★组织专家参与安全威胁的评价，对安全事件给予专业指导和原因调查等	
			对于邀请或聘用信息安全专家可提供必要的组织机构内部信息，同时应告知专家这些信息的敏感性和保密性	
			应采取必要的安全措施，保证提供的信息在安全可控的范围内	

A.5.3 风险管理

表 A.27 风险管理(第四级信息系统)

类	族	评估项	评估内容要点	标准依据
风险管理	★风险管理要求和策略	风险管理要求	★编制资产清单,对资产价值/重要性进行分析,对信息系统面临的威胁进行初步分析	5.3.1.1 d)
			对关键的系统资源进行定期风险分析和评估	
			使用规范方法和工作流程,进行规范化的风险评估	
			产生风险分析报告和留存重要过程文档,并向管理层提交,**建立风险管理体系文件**	
			针对风险管理过程,实施独立审计,确保风险管理的有效性	
		★风险管理策略	制定基本的风险管理策略	5.3.1.2 c)
			★定期进行信息安全和业务应用方面的风险评估	
			确定信息安全风险管理的基本方法	
			提供风险管理的组织和资源保证	
			★建立风险管理的监督机制,对风险管理相关过程的活动和影响进行评估和监控	
			针对风险的变化重新启动风险评估,明确规定重新启动风险评估的条件	
	风险分析和评估	★资产识别和分析	确定信息系统的资产范围,进行统计和编制资产清单	5.3.2.1 b)
			★进行资产分类和重要性标识	
			★对信息系统的硬件、软件、系统边界、接口、数据和信息、人员等方面的分析和识别	
			对信息系统的描述,包括信息系统的使命、功能,以及系统和数据的关键性、敏感性等内容	
		威胁识别和分析	★根据以往发生的安全事件、外部提供的资料和积累的经验,对威胁进行分析	5.3.2.2 d)
			★结合业务应用、系统结构特点以及访问流程等因素,建立并维护威胁列表	
			根据不同业务系统面临的威胁,对每个或者每类资产有一个威胁列表	
			考虑威胁源在保密性、完整性或可用性等方面造成损害,对威胁的可能性和影响等属性进行分析,从而确定威胁的等级	
			通过综合威胁的可能性和强度的评价,修正威胁等级	
			★对关键区域或部位进行威胁分析,在业务应用许可并得到批准的条件下,可使用检测工具在特定时间捕捉攻击信息进行威胁分析	

表 A.27（续）

类	族	评估项	评估内容要点	标准依据
风险管理	风险分析和评估	脆弱性识别和分析	★通过扫描工具、人工检查和渗透测试，获取对系统脆弱性的认识	5.3.2.3 c)
			针对信息系统资产组合、资产分类编制脆弱性列表和脆弱性检查表	
			应了解测试可能带来的后果，并做好充分准备	
			★对不同的方法和工具所得出的评估结果，进行综合分析，得到脆弱性等级	
			坚持制度化脆弱性评估，应明确规定进行脆弱性评估的时间和系统范围、人员和责任、评估结果的分析和报告程序，以及报告中包括新发现的漏洞、已修补的漏洞、漏洞趋势分析等	
		风险分析和评估要求	由用户和专家对资产、威胁和脆弱性等方面进行定性综合评估，建议处理和减缓风险的措施，形成风险评估报告	5.3.2.4 c)
			★评估报告中包括风险级别、风险点等内容，确定信息系统的安全风险状况	
			基于这些报告，要求评估者对信息系统安全措施提出建议	
			应将风险评估中的信息资产、威胁、脆弱性、防护措施等评估项信息综合到一个数据库中进行管理	
			应当在后续的项目和工具中持续地维护该数据库	
	风险控制	选择和实施风险控制措施	基于安全等级标准，选择相应等级的安全技术和管理措施	5.3.3.1 c)
			★根据风险评估结果，结合信息系统安全现状和需求，决定信息系统安全的控制措施	
			对相关的各种控制措施进行综合分析，得出紧迫性、优先级、投资比重等评价，形成体系化的防护控制系统	
	基于风险的决策	安全确认	★针对信息系统的资产清单、威胁列表、脆弱性列表，结合已采用的安全控制措施，分析存在的残余风险	5.3.4.1 c)
			形成残余风险分析报告，由组织机构的高层管理人员决定残余风险是否可接受	
			★编制信息系统残余风险清单，监视残余风险可能诱发的安全事件，及时采取防护措施	
			对信息系统安全风险实施再次评估，验证防护措施的有效性	
		信息系统运行的决策	★信息系统的主管者或运营者应根据安全确认的结果，判断残余风险是否可接受，决定是否允许信息系统继续运行	5.3.4.2 b)
			如果信息系统的残余风险不可接受，而现实情况又要求系统必须投入运行，且当前没有其他资源能胜任组织机构的使命，经过管理层的审批，可临时批准信息系统投入运行	
			应同时采取相应的风险规避和监测控制措施，并明确风险一旦发生的责任陈述	

表 A.27（续）

类	族	评估项	评估内容要点	标准依据
风险管理	★风险评估的管理	★评估机构的选择	★有国家主管部门认可的安全服务资质	5.3.5.1c)及公通字[2007]43号文件第22条
			按照国家主管部门有关管理规定选择可信评估机构，必要时应由国家指定专门部门、专门机构组织进行信息系统风险评估	
			★在中华人民共和国境内注册成立（港澳台地区除外）	
			★由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）	
			★从事相关检测评估工作两年以上，无违法记录	
			★工作人员仅限于中国公民	
			★法人及主要业务、技术人员无犯罪记录	
			★使用的技术装备、设施应当符合本办法对信息安全产品的要求	
			★具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度	
			★对国家安全、社会秩序、公共利益不构成威胁	
		评估机构保密要求	★评估机构人员应按照第三方人员管理要求签署保密协议	5.3.5.2c)
			★应有专人在整个评估过程中监督检查评估机构对保密协议的执行情况	
			对专门评估组的保密要求应参照《中华人民共和国保守国家秘密法》的要求，结合实际情况制定具体实施办法	
		评估信息的管理	★提交涉及评估需要的资料、数据等各种信息，应规定办理交接手续，防止丢失	5.3.5.3c)
			提交涉及评估需要的资料、数据等各种信息，必要时可以隐藏或替换核心的或敏感的参数	
			★所有提交涉及评估需要的资料、数据等各种信息，只能存放在被评估方指定的计算机内，不得带出指定办公区域	
		技术检测过程管理	★使用工具或手工进行技术检测，应事先提交测试的技术方案，得到授权方可进行	5.3.5.4d)
			使用工具或手工进行技术检测，应在被测试方专人监督下按技术方案进行	
			使用工具或手工进行技术检测，可采用由被评估方技术人员按技术方案进行操作，评估机构技术人员进行场外指导	
			使用工具或手工进行技术检测，应由被评估方技术人员按技术方案进行操作，对测试结果过滤敏感或涉及国家秘密信息后再交评估方分析	

A.5.4 环境和资源管理

表 A.28 环境和资源管理(第四级信息系统)

类	族	评估项	评估内容要点	标准依据
环境和资源管理	环境安全管理	环境安全管理要求	★应配置物理环境安全的责任部门和管理人员	5.4.1.1 d)
			建立有关物理环境安全方面的规章制度	
			物理安全方面应达到 GB/T 20271—2006 中 6.4.1 的有关要求	
			★对物理环境划分不同保护等级的安全区域进行明确标识和管理,包括机房、办公区域、介质库房等,**实施不同保护等级安全区域的隔离管理**	
			介质库房的管理可以参照同等级的机房的要求	
			制定对物理安全设施进行检验、配置、安装、运行的有关制度和保障措施	
			实行关键物理设施的登记制度	
			对重要安全区域的活动应实时监视和记录,出入人员应经过相应级别的授权并有监控措施	
		★机房安全管理要求	★明确机房安全管理的责任人	5.4.1.2 d)
			机房钥匙由专人管理,未经批准,不准任何人私自复制机房钥匙或服务器开机钥匙	
			★未经允许的人员不准进入机房	
			机房来访人员应经过正式批准,登记记录应妥善保存以备查	
			获准进入机房的来访人员,一般应禁止携带个人计算机等电子设备进入机房,其活动范围和操作行为应受到限制,并有机房接待人员负责和陪同,进入机房的人员应佩戴相应证件	
			任何进出机房的人员应经过门禁设施的监控和记录,应有防止绕过门禁设施的手段	
			所有来访人员的登记记录、门禁系统的电子记录**以及监视录像记录应妥善保存以备查**	
			未经批准,禁止任何人移动计算机相关设备或带离机房	
			★没有指定管理人员的明确准许,任何记录介质、文件材料及各种被保护品均不准带出机房,与工作无关的物品均不准带入机房	
			禁止携带移动电话、电子记事本等具有移动互连功能的个人物品进入机房	
			机房所在地应有专职警卫,通道和入口处应设置视频监控点,24 小时值班监视	
			机房内严禁吸烟及带入火种和水源	

表 A.28（续）

类	族	评估项	评估内容要点	标准依据
环境和资源管理	环境安全管理	办公环境安全管理要求	★防止利用终端系统窃取敏感信息或非法访问	5.4.1.3 c)
			工作人员下班后，终端计算机应关闭	
			存放敏感文件或信息载体的文件柜应上锁或设置密码	
			工作人员调离部门或更换办公室时，应立即交还办公室钥匙	
			设立独立的会客接待室，不在办公环境接待来访人员	
			工作人员离开座位应将桌面上含有敏感信息的纸件文档放在抽屉或文件柜内	
			工作人员离开座位，终端计算机应退出登录状态、采用屏幕保护口令保护或关机	
			在关键区域或部位，应使办公环境与相关机房的物理位置在一起，以便进行统一的物理保护	
	资源管理	资产清单管理	★应编制并维护与信息系统相关详细的资产清单，能够清晰识别每项资产的拥有权、责任人、安全分类以及资产所在的位置等	5.4.2.1 c)
			信息资产：应用数据、系统数据、安全数据等数据库和数据文档、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、存档信息	
			软件资产：应用软件、系统软件、开发工具和实用程序	
			有形资产：计算机设备（服务器、终端、存储设备等），网络设备（路由器、交换机、安全设备等），移动存储介质（移动硬盘、磁带等），其他技术装备（电源，空调设备等），家具和机房	
			应用业务相关资产：由信息系统控制的或与信息系统密切相关的应用业务的各类资产，由于信息系统或信息的泄露或破坏，这些资产会受到相应的损坏	
			服务：计算和通信服务，通用设备如供暖、照明、供电和空调等	
			★必要时应包括主要业务应用系统处理流程和数据流的描述，以及业务应用系统用户分类说明	
		资产的分类与标识要求	★根据资产的价值/重要性对资产进行标识，可基于资产的价值选择保护措施和进行资产管理	5.4.2.2 c)
			★对信息资产进行分类管理，对信息系统内分属不同业务范围的各类信息，按其对安全性的不同要求分类加以标识	
			用户数据的重要性分类，如国家秘密信息、商业秘密和个人隐私信息、内部专有信息、公开信息等	
			系统数据重要性一般与其所在的系统或子系统的安全保护等级相关	
			根据业务应用的具体情况进行分类分级和标识，纳入规范化管理	
			以业务应用为主线，用体系架构的方法描述信息资产	
			通过对各个资产之间的关联，进行结构性描述	

表 A.28（续）

类	族	评估项	评估内容要点	标准依据
环境和资源管理	资源管理	介质管理	★脱机存放的数据和软件介质，根据重要程度进行标识和分类，存放在由专人管理的介质库中，防止被盗、被毁、被修改以及信息泄漏	5.4.2.3 d)
			介质的归档和查询应有记录，其借阅、拷贝、分发传递须经相应级别的领导的书面审批后方可执行，并登记在册，对存档介质的目录清单应定期盘点，介质的分发传递以及带出工作环境应采取保护措施	
			存储介质的销毁**在经主管领导审批后应由两人完成，一人执行销毁一人负责监销，销毁过程应记录，**不得自行销毁，对于需要送出维修或销毁的介质，应首先删除信息，再重复写操作进行覆盖，防止数据恢复和信息泄漏	
			介质应保留 2 个以上的副本，而且要求介质异地存储，存储地的环境要求和管理方法应与本地相同，对重要介质的数据和软件必要时可以加密存储	
			★对存放在介质库中的介质应定期进行完整性和可用性检查，确认其数据或软件没有受到损坏或丢失，**介质受损但无法执行删除操作的，必须销毁**	
			对介质中的重要数据应使用加密技术或数据隐藏技术进行存储	
		★设备管理要求	对于信息系统的各种软硬件设备的选型、采购、发放或领用，使用者应提出申请，报经相应领导审批，才可以实施	5.4.2.4 c)
			★设备的选型、采购、使用和保管应明确责任人	
			要求设备有专人负责，实行分类管理	
			★通过对资产清单的管理，记录资产的状况和资产使用、转移、废弃及其授权过程	
			★对各种资产进行全面管理，提高资产安全性和使用效率，保证设备的完好率	
			建立资产管理登记系统，提供资产分类标识、授权与访问控制、变更管理、系统安全审计等功能，为整个系统提供基础技术支撑	

A.5.5 运行和维护管理

表 A.29 运行和维护管理（第四级信息系统）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	★用户管理	★用户分类管理	用户分类应包括系统用户、普通用户、外部客户用户、临时用户	5.5.1.1 d)
			★按审查和批准的用户分类清单建立用户和分配权限，**应对关键部位用户采取逐一审批和授权的程序，并记录备案**	
			★用户分类清单应包括信息系统的所有用户的清单，包括所有特权用户、重要业务用户、**关键部位用户**的权限，以及用户的责任人员和授权记录	
			用户权限发生变化时应及时更改用户清单内容	
			对特权用户、重要业务用户、**关键部位用户**开启审计功能	
			定期检查特权用户、重要业务用户、**关键部位用户**的实际分配权限是否与用户清单符合	

表 A.29（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	★用户管理	系统用户要求	★系统用户应由信息系统的主管领导指定	5.5.1.2 c)
			★授权应以满足工作需要的最小权限为原则	
			系统用户应保护自己的身份鉴别信息的安全	
			系统用户应接受审计	
			对重要信息系统的系统用户，应进行审查并经过授权	
			★对系统用户应能区分责任到个人，不应以部门或组作为责任人	
			在关键信息系统中，对系统用户的授权操作，应有两人在场，经双重认可后方可操作	
			系统用户不准更改操作过程产生的审计日志	
		普通用户要求	★用户应保护自己的身份鉴别信息和载体的安全，不得转借他人	5.5.1.3 c)
			发现系统的漏洞、滥用或违背安全行为应及时报告	
			不应透露与组织机构有关的非公开信息	
			不应故意进行违规的操作	
			不应在不符合敏感信息保护要求的系统中保存和处理高敏感度的信息	
			不应使用各种非正版软件和不可信的自由软件	
			在系统规定的权限内进行操作，必要时某些重要操作应得到批准	
		机构外部用户要求	★应对外部用户明确说明使用者的责任、义务和风险，并要求提供合法使用的声明	5.5.1.4 c)
			外部用户应保护自己的身份鉴别信息的安全	
			外部用户只能是应用层的用户	
			可对特定外部用户提供专用通信通道、端口、特定的应用或数据协议以及专用设备等	
			在关键部位，一般不允许设置外部用户	
		临时用户要求	★临时用户的设置和期限必须经过审批	5.5.1.5 c)
			临时用户应保护自己的身份鉴别信息的安全	
			★使用完毕或到期应及时删除	
			设置与删除均应记录备案	
			对主要部位的临时用户应进行审计，并进行风险评估	
			★在关键部位，一般不允许设置临时用户	
	运行操作管理	★服务器操作管理	★服务器操作系统、数据库系统的操作应由授权的系统管理员、数据库管理员实施	5.5.2.1 c)
			★遵照操作规程对服务器进行操作，设置服务器的运行环境，设定服务器的系统及安全配置，操作系统、数据库系统用户管理，并检查实际配置与安全策略要求的符合性	

表 A.29（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	运行操作管理	★服务器操作管理	系统管理员、数据库管理员应以自己的账户及身份鉴别信息登录操作系统、数据库系统进行操作	5.5.2.1 c)
			监控管理，包括监控系统性能，如 CPU 和内存的利用率、检测进程运行及磁盘使用情况	
			日志管理，包括对操作系统、数据库系统以及业务系统等日志的管理	
			负责系统配置和安全配置文件管理，包括服务器的操作系统和数据库系统的配置文件	
			★定期对操作系统和数据库系统安全进行检查，及时发现系统的缺陷或漏洞	
		终端计算机操作管理	★用户应设置终端计算机的开机、屏幕保护口令，保护身份鉴别信息，进行必要的安全设置	5.5.2.2 c)
			非本组织机构配备的终端计算机未获批准，不能在办公场所使用	
			及时安装经许可的软件和补丁程序，不得自行安装及使用其他软件和自由下载软件	
			未获批准，严禁使用 Modem 拨号、无线网卡等方式或另辟通路接入其他网络	
			应有措施防止终端计算机机箱被私自开启，如需拆机箱应经批准后由维修部门人员负责	
			高安全等级业务系统的终端计算机不得直接接入低级别系统或网络，应先作清理检查	
		便携机操作管理	在接入组织机构内部网络时遵守“终端计算机操作管理”（上一节）的要求	5.5.2.3 d)
			对不再使用或转为其他用途的便携机，应删除机内的敏感数据	
			在外网使用的便携机，接入本地网络前应进行必要的安全检查	
			★在组织机构内使用或存有敏感信息的便携机，未获批准，**没有足够强度安全防护措施**，严禁接入其他网络	
			便携机离开重要区域时不应存储敏感或涉密数据，外出使用应经有关领导批准并记录在案	
			在重要区域使用的便携机必须启用两个及两个以上身份鉴别技术的组合来进行身份鉴别	
			敏感数据应采用一定强度的加密储存技术，以规避便携机丢失的风险，必要时应对便携机采取物理保护措施	

表 A.29（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	运行操作管理	★网络及安全设备操作管理	★对网络及安全设备的操作应由授权的网络管理员、安全管理员实施，按照安全策略要求进行网络及安全设备配置	5.5.2.4 c)
			应按操作规程对网络设备和安全设备进行操作，进行网络和安全设备的运行环境配置和服务设定	
			网络管理员、安全管理员应以自己的账户及身份鉴别信息登录网络设备和安全设备进行操作	
			★定期检查实际配置与安全策略要求的符合性	
			应通过集中安全管理设施对网络及安全设备的安全机制进行监控管理和部署策略	
		业务应用操作管理	应用系统管理员及业务操作人员应自己的账户及身份鉴别信息登录业务应用系统（提供对外或专门服务的公共用户可除外）	5.5.2.5 c)
			★应用系统管理员根据安全策略和专门授权对应用系统的操作人员等用户及其权限进行管理，监控应用系统的运行	
			用户对业务应用系统的访问权限应受到控制，如以菜单等方式限制操作	
			用户应按照操作规程使用业务应用系统，操作规程应指明具体作业的指令，处理和使用的信息，以及操作步骤	
			业务应用系统操作规程应形成正式文档或帮助文件，需要进行改动时应得到管理层授权	
			操作规程应说明处理错误或其他异常情况的指令，以及在出现意外的操作或技术问题时需要技术支持的联系方法	
			对重要的业务应用操作应根据特别许可的权限执行，关键的业务应用操作应有 2 人同时在场或同时操作，并对操作过程进行记录	
			业务应用操作应进行审计	
		★变更控制和重用管理	★信息系统的变更，应提出更改方案并得到系统主管领导的审批才能进行	5.5.2.6 d)
			进行变更应进行记录，对重大变更应评估其潜在影响，考虑全面安全事务一致性，更改后将变更结果书面向所有相关人员通报	
			操作系统、数据库系统的变更控制与应用系统的更改控制应相互配合	
			通过审计日志和过程记录，记载更改中的所有有关信息，**过程记录应妥善保存**	
			对重要的变更控制应实施安全审计，并对全面安全事务一致性进行检查，防止因变更而开放危险端口或服务	
			明确中止变更并从失败变更中恢复的责任和处理方法	
			对变更执行情况、过程文档管理，进行定期或不定期的检查	
			设备重用，应提出设备重用方案并得到系统主管领导的审批才能进行，应清除重用设备中原有信息，**过程记录应妥善保存**	
			对设备重用执行情况、过程文档管理，进行定期或不定期的检查	

表 A.29（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	运行操作管理	信息交换管理	★在信息系统中发布信息和用户交换信息，应符合国家有关政策法规的规定	5.5.2.7 d)
			应采取适当的安全措施保护信息系统中发布信息和用户交换信息的完整性	
			应保护业务应用中的信息交换的安全性，防止欺诈、合同纠纷以及泄露或修改信息事件的发生	
			在组织机构之间进行信息交换应建立安全条件的协议	
			明确业务信息交换管理责任及数据传输的最低安全要求	
			还对于信息系统内部不同安全区域之间的信息传输，应有明确的安全要求	
			对高安全等级信息向低安全域的传输应经过领导层的批准，明确部门和人员的责任，并采取的安全专控措施	
	运行维护管理	日常运行安全管理	★应通过正式授权程序委派专人负责信息系统运行的安全管理和风险控制	5.5.3.1 d)
			应明确运行值班的日常处理工作和安全管理职责，建立和维护信息系统运行过程管理文档	
			应对运行安全进行监督检查，包括检测、监控、分析等措施，**评估运行安全策略的落实情况和一致性**	
			应明确各个岗位人员对信息系统各类资源的安全责任**和目标**，包括日常操作、备份及容错等，**以及对责任履行情况的审计**	
			应明确信息系统安全管理人员和系统用户、普通用户对信息系统资源的访问权限	
			对信息系统关键岗位人员采取最小授权和分权制衡措施，如关键安全操作双人共管	
			应检查和维护信息系统中业务应用数据完整性、可用性、**保密性，可根据需要提出技术改进的建议**	
			★应用软件的使用采取授权管理，未经验证的软件不得运行系统中安装，对应用软件的使用进行审计	
			一般不允许外部服务方对信息系统访问，必要时应对外部服务方访问实施监视，并对外部服务方对信息系统访问的安全进行风险分析	
			执行信息系统的数据备份、病毒防范、安全事件处理、变更控制等安全管理规定的日常工作任务	
			进行应急响应和灾难恢复计划规定的实际演练和技术培训，明确专人负责执行情况检查**和评价**，如数据备份和备用设备的可用性	
			根据组织机构和信息系统出现的各种变化**进行风险分析**，及时修订、完善各种规章制度，保证各方面安全事务管理的一致性**和有效性**	
			接受上级或国家有关部门对信息系统安全工作的监督和检查	

表 A.29（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	运行维护管理	运行状况监控	★委派专人负责监视信息系统重要应用、网络系统、核心服务器等是否运行正常，监视系统性能及与安全机制相关的服务器、网络性能变化	5.5.3.2 d)
			信息系统应使用统一的时间，以确保记录日志和审计信息准确	
			信息系统审计日志应保留一定期限，有脱机保存的介质，不能被改变，只允许授权用户访问	
			定期分析信息系统日志并产生报告	
			应告知用户某些行为是会被审计的	
			安全机制集中管理机构负责信息系统安全管理、系统管理、审计管理的集中监控和分析	
			安全机制集中管理机构应对关键区域和关键业务应用系统运行的监视，并与主管部门共同制定具体的管理办法	
		软件硬件维护管理	★应明确信息系统的软件、硬件维护的人员和责任，规定维护的时限	5.5.3.3 d)
			对涉及维修的重要区域的数据和软件系统采取保护措施，防止因维修造成破坏和泄漏	
			应明确信息系统的硬件设备维修、替换和更新的申报、审批和管理流程	
			应明确信息系统软件维护的申报、审批和管理流程	
			★对需要外出维修的设备，应经过审批，磁盘数据应进行删除	
			★一般不应允许外部维修人员进入关键区域，必须进入机房维修，应经过审批，并有专人负责陪同	
			应根据维修方案和风险评估的结果确定维修方式，可采用更新设备的方法解决	
			应对维修过程及有关故障现象记录备案	
		外部服务方访问管理	对外部服务方访问实施严格控制，采取对外部服务方访问实施监视等安全措施，**必要时应外部服务方的访问进行限制**	5.5.3.4 d)
			应对外部服务方访问的要求进行风险分析，并经过相应的申报和审批程序，**在重要安全区域对外部服务方每次访问进行风险控制**	
			★外部服务方访问应签署了相应的保密合同	
	★外包服务管理	★外包服务合同	★对由外部服务商承担完成的外包服务，应签署正式的书面合同	5.5.4.1 a)
			对符合法律要求的说明，如数据保护法规	
			对外包服务的风险的说明，包括风险的来源、具体风险描述和风险的影响，明确如何维护并检测组织机构的业务资产的完整性和保密性	
			对外包服务合同各方的安全责任界定，应确保外包合同中的参与方（包括转包商）都了解各自的安全责任	

表 A.29（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	★外包服务管理	★外包服务合同	对控制安全风险应采用的控制措施的说明，包括物理和逻辑控制措施，限制授权用户对组织机构的敏感业务信息的访问，以及设备的物理安全保护	5.5.4.1 a)
			对外包服务风险发生时应采取措施的说明，如在发生灾难事故时，应如何维护服务的可用性	
			对外包服务的期限、中止的条件和善后处理的事宜以及由此产生责任问题的说明	
			对审计人员权限的说明	
		外包服务商	外包服务的限制，关键的或敏感的业务应用，一般不应采用业务应用系统外包服务方式	5.5.4.2 c)
			★在行业认可或者是经过上级主管部门批准的范围内，选择具有相应服务资质并信誉好的可信的外包服务商	
		★外包服务的运行管理	★外包服务的限制，关键的或敏感的业务应用，一般不应采用业务应用系统外包服务方式	5.5.4.3 b)
			★对外包服务的业务应用系统运行的安全状况应进行监控和检查，应定期进行评估	
			对外包服务出现问题应遵照合同规定及时处理和报告	
			★当出现重大安全问题或隐患时应进行重新评估，提出改进意见，直至停止外包服务	
	有关安全机制保障	★身份鉴别机制管理要求	信息系统所有用户均应明确使用身份鉴别机制的责任，保护用户自己的身份鉴别信息的保密性和完整性	5.5.5.1 d)
			在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性	
			★在每次用户登录系统时**和重新连接系统时**，采用受安全管理中心控制的口令、令牌、基于生物特征、数字证书以及其他具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别，**且其中一种鉴别技术产生的鉴别数据是不可替代的**	
			应指定安全管理人员定期检查信息系统用户身份鉴别机制和身份鉴别信息的安全性，特别是跨网络的远程用户鉴别信息的安全性	
			必要时，采用身份鉴别信息分段由多人保管，输入时由多人进行操作，操作过程需要留有操作记录和审批记录	
		★访问控制机制管理要求	应根据自主访问控制安全策略，允许授权用户对其创建的客体具有相应的访问操作权限，包括对客体的创建、读、写、修改和删除等	5.5.5.2 d)
			实施访问控制机制主体的粒度为用户，客体的粒度为文件或数据库表级和(或)记录或字段级，强制访问控制客体的粒度为文件或数据库表级，**将自主和强制访问控制扩展到所有主体与客体**	

表 A.29（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	有关安全机制保障	★访问控制机制管理要求	★能够阻止非授权用户读取敏感信息并能将这些权限的部分或全部授予其他用户	5.5.5.2 d)
			实现对自主访问控制过程的审计，告知访问者须为自己的行为负责	
			应由授权的安全管理员通过特定专用方式对主、客体进行安全标记；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制	
			应确保信息系统内的所有主、客体具有一致的标记信息，并实施同一安全策略的强制访问控制规则	
			对访问控制进行监控管理，对系统、用户或环境进行持续性检查，注意保护监控数据	
		系统安全管理要求	应通过正式授权程序委派专人负责系统安全管理，包括对操作系统和数据库管理系统管理（系统管理员、数据库管理员）	5.5.5.3 d)
			建立系统安全配置、备份等安全管理规章制度及操作规程	
			由授权的系统安全员通过系统提供的操作界面，根据访问控制安全策略设置、维护用户及主、客体的标记信息	
			★按规章制度的要求进行正确的系统安全配置、备份等操作，及时进行补丁升级	
			对操作系统和数据库系统进行用户账号安全使用和授权管理，并进行审计	
			对授权用户登录系统和使用许可的资源，进行身份鉴别和审计	
			依据安全策略确定审计事件、审计内容、审计归档、审计报告	
			应对系统的安全弱点和漏洞进行控制，对可能危及系统安全的系统工具进行严格的控制	
			应依据变更控制规程对系统的变更进行控制，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	
			应及时对系统资源和系统文档进行备份和安全标识	
			制定操作系统和数据库管理系统应急计划	
			应按系统内置角色强制指定系统安全管理责任人	
			保证系统管理过程的可审计，对系统管理过程留有记录	
			定期对操作系统、数据库系统的安全性进行检查	
		网络安全管理要求	应通过正式授权程序指定网络管理人员对网络系统进行配置和安全管理	5.5.5.4 d)
			★应按网络区域边界安全控制策略，实施数据包过滤措施，采用常规校验机制检验数据传输的完整性等安全管理，能够发现数据完整性被破坏，并在发现完整性被破坏时进行恢复	

表 A.29（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	有关安全机制保障	网络安全管理要求	信息系统网络安全区域边界按访问控制策略设置自主和强制访问控制机制，对进出安全区域边界的数据信息进行控制，阻止非授权访问	5.5.5.4 d)
			依据总体安全策略制定网络访问控制策略，并定期检查和完善网络安全策略	
			采取网络访问授权管理，保证经过授权的用户才能得到许可的网络服务	
			告知用户使用网络的安全责任和操作规程	
			用户在外部访问组织机构内部网络应经审批，可采用由密码技术支持的保密性、完整性保护机制或具有相应强度的其他安全机制，保护网络数据传输安全	
			定期对外部网络连接接口的安全进行评估，可采用由密码技术支持的保密性、完整性保护机制或具有相应强度的其他安全机制，保护网络数据传输安全	
			对外公共服务的信息系统，应采取严格访问控制，保证外部用户的访问得到控制和审计，不危及内部信息系统的安全	
			对外传输的数据和信息要经过批准和审查，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实施控制和检查，探测非法外联等行为，保护网络及区域边界完整性	
			信息系统的关键网络设备设施的备份进行管理，保证可用性	
			对网络安全日常管理、网络配置变更、网络故障及事件处理等，定期进行安全检查和评估，**对网络服务、网络安全策略、安全控制措施进行有效性检查和监督**，提交正式的网络安全报告	
			可采用由密码技术支持的可信网络连接机制，通过对连接到通信网络的设备进行可信检验，保证接入通信网络的设备真实可信，防止设备的非法接入，**保证信息系统网络之间的连接应使用可信路径**	
			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	应通过正式授权程序委派专人负责应用系统的安全管理（应用系统管理员）	5.5.5.5 d)
			★具有明确的应用系统管理员对于特定应用系统安全管理内容，如用户及权限管理等，以及应用系统软件的安全配置、备份等	
			应结合业务需求制定相关规章制度，制定并落实应用系统的安全操作规程，并严格按照规章制度的要求实施应用系统安全管理	
			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发布	

表 A.29（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	有关安全机制保障	应用系统安全管理要求	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	5.5.5.5 d)
			保证对应用系统信息或软件的访问不影响其他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，保证应用系统数据的保密性、完整性和可用性	
			应指定专人负责应用系统的审计工作，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	
			对应用系统软件的使用采取授权管理，未授权用户不得在运行系统中安装、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	
			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负责应用系统的安全配置管理和应用管理	
			定期对应用系统的总体安全策略、应用系统安全措施的落实情况和运行管理进行检查	
			采取独立的应用安全审计，审计人员仅实施审计工作，不参与系统的其他任务，防止应用系统信息的泄漏	
		病毒防护管理要求	安排专人负责计算机病毒防护，定期进行检查报告主机和网络的病毒安全状况	5.5.5.6 d)
			★在主机安装防病毒软件，在安全区域边界设置防恶意代码网关，并及时升级，检查病毒库的升级情况并进行记录	
			对非在线的内部计算机设备及其他移动存储设备，以及外来或新增计算机做到入网前进行杀毒和防病毒软件版本检测	
			从不信任网络上所接收的文件或邮件，在使用前应首先检查是否有病毒	
			在网络内部建立专门的防病毒软件升级服务，实行整体策略、定期升级、统一控制，紧急情况下增加升级次数	
			采取对系统所有终端防范病毒软件集中管理的措施	
			定期检查信息系统病毒防护执行和管理情况	

表 A.29（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	有关安全机制保障	密码管理要求	★应按国家密码主管部门的规定，对信息系统中使用的密码算法和密钥进行管理	5.5.5.7 b)
			应按国家有关法律法规要求，对信息系统中包含密码的软、硬件信息处理模块的进、出口进行管理	
	安全集中管理	★安全机制集中控管	★对信息系统所涉及的服务器、网络、安全设备以及应用系统等的安全管理、系统管理、审计管理机制实施集中的监控、配置和管理	5.5.6.1 b)
			建立一体化和开放性平台，提供标准的接口，具备对安全资源管理能力	
			对系统的资源和运行进行配置、控制和管理，包括用户身份管理、系统资源配置、系统加载和启动、系统运行的异常处理以及支持管理本地和(或)异地灾难备份与恢复等	
			对系统中的主体、客体进行统一标记，对主体进行授权，对服务器、网络设备、安全设备等配置一致的安全策略	
			对分布在系统各个组成部分的安全审计机制进行集中管理，对审计记录应进行分析，并根据分析结果进行处理	
			授权的安全、系统、审计管理员应以自己的账户和身份鉴别信息进行登录和操作	
			根据信息系统网络结构需要，可按照分布式多层次的管理结构，进行分层分级联合方式的集中安全管理	
		安全信息集中管理	★将信息系统安全管理信息、系统管理信息、审计管理信息实施集中管理、综合分析	5.5.6.2 b)
			提供可视化报表和安全事件分析过程，以及安全事件的管理与辅助分析机制	
			对关键区域安全信息的集中管理，应采用相应安全级别的访问控制和保护措施	
		安全机制整合要求	进行信息系统资产信息管理	5.5.6.3 a)
			进行信息系统网络异常流量监控	
			进行信息系统安全事件监控管理	
			进行信息系统脆弱性管理	
			进行信息系统安全策略管理	
			进行信息系统安全预警管理	
		安全机制整合的处理方式	主要工作方式可包括自动处理、人工干预处理、远程处理、辅助决策分析处理、记录和事后处理等	5.5.6.4 a)

A.5.6 业务连续性管理

表 A.30 业务连续性管理(第四级信息系统)

类	族	评估项	评估内容要点	标准依据
业务连续性管理	★备份与恢复	★数据备份和恢复	★应明确说明需定期备份重要业务信息、系统数据及软件等内容和备份周期,根据数据的重要程度和更新频率设定备份周期	5.6.1.1 d)
			确定重要业务信息的保存期以及其他需要保存的归档拷贝的保存期	
			采用离线备份或在线备份方案,定期进行数据增量备份和应用系统全备份,必要时应采用热备份方式保存数据	
			指定专人负责数据备份和恢复,可使用手工或软件产品进行备份和恢复,同时保存几个版本的备份	
			定期检查备份介质,保证在紧急情况时可以使用	
			定期检查及测试恢复程序,确保在预定的时间内正确恢复	
			应分别指定专人负责不同方式的数据备份和恢复,并保存必要的操作记录	
			根据数据实时性和其他安全要求,采用本地或远地备份方式,制定适当的备份和恢复方式以及操作程序	
			必要时对备份后的数据采取加密或数据隐藏处理,操作时要求两名工作人员在场并登记备案	
		设备和系统的备份与冗余	★实现信息系统的关键设备备份与容错,实现系统热备份与冗余	5.6.1.2 c)
			★指定专人定期维护和检查备份设备和冗余设备的状况,确保需要接入系统时能够正常运行	
			根据实际需求确定备份设备接入的工作流程和操作时间,根据实际需求限定系统热备份和冗余设备切换的时间	
			指定专人定期维护和检查热备份的运行状况,定期进行切换试验,确保需要时能正常运行	
			选择远离市区的地方或其他城市,建立系统远地备份中心,确保主系统在遭到破坏中断运行时,远地系统能替代主系统运行,保证信息系统所支持的业务系统能按照需要继续运行	
	安全事件处理	安全事件划分	安全事件的处置需要贯穿整个安全管理的全过程,建立信息安全事件分等级响应和处置的制度	5.6.2.1 c)
			安全事件包括不可抗拒的事件、设备故障事件、病毒爆发事件、外部网络入侵事件、内部信息安全事件、内部误用和误操作等事件等	
			应依据安全事件对信息系统的破坏程度、所造成的社会影响及涉及的范围,确定具体信息系统安全事件处置等级的划分原则	
			★对信息系统中发生的各类事件制定相应安全保护等级的处置预案,确定事件响应和处置的范围、程度及工作流程	

表 A.30（续）

类	族	评估项	评估内容要点	标准依据
业务连续性管理	安全事件处理	安全事件划分	信息安全事件发生后，按预案分等级进行响应和处置	5.6.2.1 c)
			在发现或怀疑系统或服务出现安全漏洞或受到威胁时，应按照安全事件处置要求处理	
			明确不同安全事件的管理责任，制定不同安全事件的管理流程，包括制定处理预案、分析原因、收集证据、处理过程控制、总结吸取教训、责任划分和追究等内容	
		★安全事件报告和响应	信息安全事件实行分等级响应和处置	5.6.2.2 c)
			★安全事件应尽快通过适当的管理渠道报告，注意安全弱点和可疑事件的报告，制定正式的报告程序和事故响应程序	
			对于暂不能确定为事故或入侵等的可疑事件也应报告	
			对于所有安全事件的报告应记录在案归档留存	
			使所有员工知道报告安全事件程序和责任，告知员工未经许可测试弱点属于滥用系统	
			★信息安全事件发生后，根据其危害和发生的部位，迅速确定事件等级，并根据等级启动相应的响应和处置预案	
			要求安全管理机构或职能部门负责接报安全事件报告，并及时进行处理，注意记录事件处理过程	
			对于重要区域或业务应用发生的安全事件，应注意控制事件的影响	
			事件处理后应有相应的反馈程序，应追究安全事件发生的技术原因和管理责任，写出处理报告，并进行必要的评估	
	★应急处理	应急处理和灾难恢复	★信息安全领导小组应有人负责或指定专人负责应急计划和灾难恢复计划管理工作	5.6.3.1 d)
			信息系统安全机制集中管理机构应协助应急处理小组负责具体落实	
			检查或验证（演练）应急计划和灾难恢复计划，保证应急计划和灾难恢复计划能够有效执行	
			安全管理机构应制定总体应急计划和灾难恢复计划，应急处理小组负责落实	
			制定**关键的和重要的，以及其他业务需要的**应用系统和支持系统的应急预案和灾难恢复预案，并进行测试	
			对计划涉及人员进行培训，保证这些人员具有相应执行能力	
			与应急需要应急的外部支持单位，应签订合同	
			做好应急处理和灾难恢复的基础工作，包括安全事件处理，系统及数据备份的管理	
			针对应急计划和灾难恢复计划实施进行独立审计	
			针对应急计划和灾难恢复计划进行定期评估，不断改进和完善	

表 A.30（续）

类	族	评估项	评估内容要点	标准依据
业务连续性管理	★应急处理	★应急计划	★制定了应急计划(应急计划框架内容包括)	5.6.3.2 a)
			制定应急计划策略,明确制定应急计划所需的职权和相应的管理部门	
			进行业务影响分析,识别关键信息系统和部件,确定优先次序	
			确定防御性控制,减小系统中断的影响,提高系统的可用性;注意采取措施,减少应急计划生存周期费用	
			制定恢复策略,确保系统可以在中断后快速和有效的恢复	
			制定信息系统应急计划,包括恢复受损系统所需的指导方针和规程	
			计划测试、培训和演练,发现计划的不足,培训技术人员	
			计划维护,有规律地更新适应系统发展	
		应急计划的实施保障	★应明确应急计划的组织和实施人员,并使其知道在应急计划实施过程中各自的责任	5.6.3.3 d)
			对系统相关的人员进行培训和组织演练,知道如何以及何时使用应急计划中的控制手段及恢复策略,保证执行应急计划应具有的能力	
			进行系统化管理用于实施和维护整个应急计划体系,并记录计划实施过程	
			确保应急计划的执行有足够资源的保证	
			应对系统运行过程的风险进行评估,识别可能引起业务过程中断的事件,听取业务人员的建议,完善应急计划的实施	

A.5.7 监督和检查管理

表 A.31 监督和检查管理（第四级信息系统）

类	族	评估项	评估内容要点	标准依据
监督和检查管理	符合法律要求	★知晓适用的法律	应认识对于信息系统应用范畴适用的所有法律法规	5.7.1.1 c)
			★对信息系统的设计、操作、使用和管理,以及信息管理方面,应认识和规避法律法规禁区,防止出现违法行为	
			保护组织机构的数据信息和个人信息隐私	
			对于详细而准确的法律要求应从组织机构的法律顾问,或者合格的法律从业人员处获得帮助	
			应知晓不允许滥用信息处理设备,以免危害组织机构和社会利益,并有措施防止滥用	
			★信息系统中采用的密码技术应使用国家主管部门批准的算法,符合国家有关法规的要求	

表 A.31（续）

类	族	评估项	评估内容要点	标准依据
监督和检查管理	符合法律要求	知识产权管理	应建立关于尊重知识产权的策略，防止发生侵犯版权的行为，并形成书面文档	5.7.1.2 c)
			涉及软件开发的工作人员和承包商应做到符合和遵守相关的法律、法规	
			应明确规定外包开发的应用系统软件的有关软件版权问题	
			应防止外包开发的应用系统因软件升级或改造发生侵犯软件版权问题	
			★对关键业务应用，必要时应要求使用具有自主知识产权的软件，以保护关键业务应用的安全	
		保护证据记录	规定组织机构的重要记录的内容范围，如财务记录、数据库记录、审计日志等	5.7.1.3 a)
			★应按照法律法规的要求保护组织机构的重要记录，防止丢失、毁坏和被篡改	
			被作为证据的记录，信息的内容和保留的时间应遵守国家法律法规的规定	
	依从性检查	检查和改进	要求定期对安全管理活动的各个方面进行检查和评估工作	5.7.2.1 b)
			建立检查和改进制度，做到定期检查实施的所有安全程序是否遵从了组织机构制定的安全方针和政策，检查信息系统在技术方面是否依从了安全标准，根据检查过程中发现的不足对安全管理体系进行不断改进	
			★对照组织机构的安全策略和管理制度做到自管、自查、自评，并应落实责任制，接受国家监管部门的监管	
		★安全策略依从性检查	定期检查信息系统的网络、操作系统、数据库系统等系统管理员，对安全策略的遵守情况，包括是否能正确执行安全制度，遵从安全策略	5.7.2.2 c)
			★定期检查信息系统各个岗位对操作规程和管理制度的执行情况，确保遵从组织机构的安全策略	
			检查范围应包括信息系统本身，以及系统供应商、信息和信息资产的所有者、用户和管理层，保证其符合安全策略和标准	
			检查有关系统使用情况和操作等监控过程，根据检查结果，对信息系统安全管理体系和安全管理执行过程存在的问题进行不断改进	
		★技术依从性检查	**★按照信息系统应达到安全保护等级第四级技术要求**定期进行检查，根据检查信息系统对安全实施标准的符合情况进行初步评价并形成意见	5.7.2.3 c)
			对硬件和软件的检验，以及技术依从检查应由有能力的、经过授权的人员来进行	
			对于技术检测应由有经验的系统工程师手工或使用软件包进行并生成检测结果，经技术专家解释并产生技术报告	
			应根据检查结果，对存在的缺陷进行不断改进	
			对关键区域或敏感系统的技术依从性检查应严格控制，并注意对有关检测过程和检测结果的安全进行保护	

表 A.31（续）

类	族	评估项	评估内容要点	标准依据
监督和检查管理	审计及监管控制	★审计控制	应有独立的审计机构或人员对组织机构的安全管理体系、信息系统的安全风险控制、管理过程的有效性和正确性进行审计	5.7.3.1 c)
			★对审计过程进行控制，应制定审计的工作程序和规范化工作流程，将审计活动周期化，同时加强安全事件发生后的审计	
			应对系统的审计活动进行规划，尽量减小中断业务流程的风险	
			系统审计过程控制要求，审计的范围必须经过授权并得到控制，审计所需的资源应明确定义并保证可用性，应审计和记录所有的访问，对所有的流程、需求和责任都应文档化	
			应对系统审计工具进行保护，防止误用造成危害	
			审计工具应与开发系统和运行系统分开管理	
			应明确审计工具的适用范围，使用过程应经过批准，应记录审计工具的所有使用过程，应明确审计工具的保存方式、责任人员等	
		监管控制	**依照国有关法规和 GB 17859—1999 第四级的要求进行自主保护，信息安全监管职能部门对其进行强制监督、检查**	5.7.3.2 d)
	责任认定	审计结果的责任认定	对于审计及监管过程发现的问题应限期解决	5.7.4.1 c)
			★应认定技术责任和管理责任，明确责任当事人，提出问题解决办法和责任处理意见	
			应对审计及监管过程发现的问题认定相关领导者的责任，组织机构领导层应就此提出问题解决办法和责任处理意见，以及监督问题解决情况	
			应对审计及监管过程发现问题的处理结果进行必要的复查，并明确进行审计及监管复查的期限和责任	
		审计及监管者责任的认定	审计及监管者应按有关监督和检查的规定定期进行审计，逾期未进行审计及监管，使本应审计的问题因未审计而造成信息系统损失，应承担相应的责任	5.7.4.2 c)
			审计及监管者虽能够按有关监督和检查的规定进行审计，但因未能及时发现本应审计出问题而造成信息系统损失的，应承担相应的责任	
			审计及监管者应对审计及监管过程发现问题的处理结果进行必要的跟踪检查直至问题的解决，如因未进行跟踪检查而造成损失的，应承担相应的责任	

A.5.8 生存周期管理

表 A.32 生存周期管理（第四级信息系统）

类	族	评估项	评估内容要点	标准依据
生存周期管理	★规划和立项管理	系统规划要求	信息系统的管理者应对信息系统的建设和改造，以及近期和远期的发展制定工作计划，并应得到管理层的批准	5.8.1.1 c)
			应制定安全策略规划并得到管理层的批准	
			安全策略规划主要包括信息系统的总体安全策略、安全保障体系的安全技术框架和安全管理策略等	
			能够为信息系统安全保障体系的规划、建设和改造提供依据，使管理者和使用者都了解信息系统安全防护的基本原则和策略，知道应采用的各种技术和管理措施对抗各种威胁	
			依据安全策略规划，制定安全建设和安全改造的规划，并应得到组织机构管理层的批准	
		系统需求的提出	★信息系统应用部门或业务部门需要开发新的业务应用系统或更改已运行的业务应用系统时，以书面形式提出申请	5.8.1.2 c)
			★信息系统的安全管理职能部门应根据信息系统的安全状况和存在隐患的分析，以及信息安全评估结果等提出加强系统安全的具体需求，并以书面形式提出申请	
			安全需求的分析和说明，至少包括组织机构的业务特点和需求，威胁、脆弱性和风险的说明，安全的要求和保护目标	
			信息系统的管理者应根据信息系统安全建设规划的要求，提出当前应进行安全建设和安全改造的具体需求，并以书面形式提出申请	
		★系统开发的立项	接到系统需求的书面申请，必须组织有关部门负责人和有关安全技术专家进行可行性论证和安全性评价	5.8.1.3 c)
			★通过可行性论证和确认项目安全性符合要求后由主管领导审批，或者经过管理层的讨论批准，才能正式立项	
	★建设过程管理	★建设项目准备	★对信息系统建设和改造项目应明确指定项目负责人，监督和管理项目的全过程，明确信息系统建设和改造项目的管理流程	5.8.2.1 c)
			应制定详细的项目实施计划，作为项目管理过程的依据	
			建立工程实施监理管理制度，明确指定项目实施监理负责人	
		工程项目外包要求	**对于安全保护等级较高的信息系统工程项目，一般不应采取工程项目外包方式**	5.8.2.2 d)
			信息系统工程项目外包，应选择具有服务资质的信誉较好的厂商，要求其已获得国家规定的资质证书、有成功的实施案例	
			对重要的信息系统工程项目外包，应在主管部门指定或特定范围内选择具有服务资质的信誉较好的厂商，并应经实践证明是安全可靠的厂商	
			对外包中被废止和暂停的项目，要确保相关的系统设计、文档、代码等的安全	
			对代码的所有权和知识产权、软件开发过程质量控制、代码质量检测、上线前的安全测试等制定控制措施	

表 A.32（续）

类	族	评估项	评估内容要点	标准依据
生存周期管理	★建设过程管理	自行开发环境控制	★自行开发项目，要求开发环境与实际运行环境做到物理分开，建立完全独立的两个环境	5.8.2.3 d)
			开发及测试活动也应尽可能分开	
			系统开发文档应有专人负责保管，系统开发文档的使用须经管理层的批准	
			系统开发文档的变更应按照变更管理流程进行控制	
			一般不鼓励对非自行开发的软件包进行修改，必须改动时应注意内置的控制措施和整合过程被损害的风险，软件的改动对将来的维护带来影响，应保留原始软件并在完全一样的复制件上进行改动，所有的改动应经过充分的测试并形成文件，以便必要时用于将来的软件升级	
			应严格控制对源程序的访问，源程序不应被保存在运行系统中，技术开发人员不应具有对程序资源库不受限制的访问权，源程序库的更新和向程序员发布的程序源应经授权，应保留程序的所有版本，程序清单应被保存在一个安全的环境中，应保存对所有源程序库访问的审计记录	
			对于安全保护等级较高的信息系统建设项目及涉密项目，应对开发全过程采取相应的保密措施，对参与开发的有关人员进行保密教育和管理	
		★安全产品使用要求	信息安全产品包括构成信息系统安全保护功能的信息技术硬件、软件、固件设备，以及安全检查、检测验证工具等	5.8.2.4 a) 及公通字[2007]43号文件第21条
			★信息系统使用的信息安全产品应按照相应的安全保护等级的要求选择相应等级的产品	
			★产品研制、生产单位是由中国公民、法人投资或者国家投资或者控股的，在中华人民共和国境内具有独立的法人资格	
			★产品的核心技术、关键部件具有我国自主知识产权	
			★产品研制、生产单位及其主要业务、技术人员无犯罪记录	
			★产品研制、生产单位声明没有故意留有或者设置漏洞、后门、木马等程序和功能	
			★对国家安全、社会秩序、公共利益不构成危害	
			★对已列入信息安全产品认证目录的，应当取得国家信息安全产品认证机构颁发的认证证书	

表 A.32（续）

类	族	评估项	评估内容要点	标准依据
生存周期管理	★建设过程管理	★建设项目测试验收	★对信息系统建设和改造项目进行功能及性能测试，进行安全测试验收，保证信息系统建设项目的保密性、完整性、可用性	5.8.2.5 c)
			应指定项目测试（包括安全测试）验收负责人	
			应制订测试和接收标准，确保信息系统建设和改造项目的接收要求和标准被清晰定义并文档化	
			对安全系统的测试至少包括对组成系统的所有部件进行安全性测试，对系统进行集成性安全测试，对业务应用进行安全测试等	
			在信息系统建设和改造项目验收时至少还应考虑系统性能和容量的要求，错误恢复、重启程序及应急计划，制定并测试日常的操作程序以达到规定的标准，实施了设计方案规定的安全控制措施，提供了有效的用户指南，新系统对组织机构业务的安全影响，操作和使用新系统的培训	
	系统启用和终止管理	★新系统启用管理	★在新的信息系统或子系统、信息系统设备在启用以前，应经过正式测试验收	5.8.3.1 d)
			由使用者或管理者提出申请，经过相应领导审批才能正式投入使用	
			应进行一定期限的试运行，并得到相应领导和技术负责人认可才能正式投入使用，并形成文档备案	
			组织有关管理者、技术负责人、用户和安全专家，对新的信息系统或子系统、信息系统设备的试运行进行专项安全评估，得到认可并形成文档备案才能正式投入使用	
			新系统正式投入使用的一定时间内，应进行审计跟踪，定期对审计结果做出风险评价，对安全进行确认以决定是否能够继续运行，并形成文档备案	
		★终止运行管理	终止运行包括现有信息系统或子系统、主要设备	5.8.3.2 c)
			应由使用者或管理者提出申请并说明原因	
			应由使用者或管理者提出采取的保护措施	
			★在任何新的信息系统或子系统、信息系统设备需要终止运行以前，应进行必要数据和软件备份，对终止运行的设备进行数据清除	
			得到相应领导和技术负责人认可才能正式终止运行，并形成文档备案	
			★应采取必要的安全措施，并进行数据和软件备份，对终止运行的设备进行不可恢复的数据清除，如果存储设备损坏则必须采取销毁措施，在得到相应领导和技术负责人认可才能正式终止运行，并形成文档备案	

A.6 第五级信息系统安全管理评估参照表

A.6.1 策略和制度管理

表 A.33 策略和制度管理(第五级信息系统)

类	族	评估项	评估内容要点	标准依据
★策略和制度	★信息安全管理策略	★安全管理目标与范围	★管理对象(信息系统)的基本描述	5.1.1.1 e)
			信息系统的管理范围	
			★业务数据和系统服务达到的安全目标,**符合第五级信息系统安全要求**	
		★总体安全管理策略	**制定了专控保护的安全管理策略文档**	5.1.1.2 e)
			★明确管理者对信息系统安全的责任,管理方法、支持意向	
			说明信息系统的安全方针、原则、标准和符合性要求	
			★说明信息系统安全的总体目标、范围、管理原则和安全技术框架及安全管理框架	
			划分信息系统不同安全保护等级的管理策略	
			依据国家有关管理规范和技术标准进行保护,**接受国家指定专门部门的专门监督、检查**	
		安全管理策略的制定	由信息安全领导小组组织制定并提出指导思想	5.1.1.3 e)
			由信息安全职能部门负责指派专人负责制定	
			由信息安全领导小组组织并提出指导思想,信息安全职能部门负责具体制定	
			信息技术及业务人员参加制定	
			★形成体系化的信息系统安全管理策略,包括总体策略和具体策略,以文件形式表述	
			涉密系统安全策略的制定应限定在相应范围内进行	
			必要时应征求国家指定的专门部门或机构的意见,或者共同制定专控保护的信息系统安全管理策略,包括总体策略和具体策略	
		安全管理策略的发布	由组织机构负责人签发	5.1.1.4 e)
			按照有关文件管理程序发布	
			安全管理策略文档应注明发布范围,并有收发文登记	
			安全管理策略文档应注明密级,并在监管部门备案	
			必要时安全管理策略文档应在国家指定的专门部门或机构进行备案	
	★安全管理规章制度	★安全管理规章制度内容	**制定了专控保护的安全管理制度文档**	5.1.2.1 e)
			包括安全管理活动中各类管理方面的制度,以及安全管理人员或操作人员的操作规程,形成全面的信息安全管理制度体系	
			★信息安全责任管理制度,包括信息安全主管领导、责任部门、人员及有关岗位的信息安全责任管理内容	

表 A.33（续）

类	族	评估项	评估内容要点	标准依据
★策略和制度	★安全管理规章制度	★安全管理规章制度内容	★人员安全管理制度，包括人员录用、离岗、考核、教育培训等管理内容	5.1.2.1 e)
			★系统建设管理制度，包括系统定级、方案设计、产品采购使用、密码使用、软件开发、工程实施、验收上线、外包服务等管理内容	
			★系统运维管理制度，包括机房环境安全、存储介质安全、设备设施安全、安全监控、网络安全、系统安全、恶意代码防范、密码保护、备份与恢复、事件处置、应急预案等管理内容	
			★监督检查管理制度，包括定期对各项制度的落实情况进行自查和监督检查，以及风险评估等管理内容	
			★有关业务应用安全方面的管理制度，**根据业务需要并与主管部门共同制定的专项安全管理制度**	
		安全管理规章制度的制定	由信息安全职能部门负责制订，指派专人负责专项信息系统安全管理制度维护	5.1.2.2 e)
			经信息安全领导小组讨论通过，由信息安全领导小组负责人审批	
			★有正式发布的制度文件或文档	
			应注明发布范围、注明密级，并有收发文登记	
			对信息系统涉密的安全管理制度的制定应在相应范围内进行	
			必要时，应征求组织机构的保密管理部门及国家指定的专门部门或机构的意见，或者共同制定	
	策略与制度文档管理	策略与制度文档的评审和修订	由信息安全领导小组和信息安全职能部门负责文档的评审和修订，必要时**组织机构的保密管理部门及应征求国家指定的专门部门或机构的意见**，并保留必要的评审记录和依据	5.1.3.1 e)
			★定期或阶段性检查策略和制度的有效性，对存在不足或需要改进的策略和制度进行修订	
			修订后的策略和制度按规定程序发布	
			★发生重大安全事故，组织机构或技术结构发生变化时，对策略和制度进行相应的评审和修订	
			对评审后需要修订的策略和制度文档，应明确指定人员限期完成	
			每个策略和制度文档应有相应责任人，根据明确规定的评审和修订程序对策略进行维护	
			对涉密的信息安全策略、规章制度和相关的操作规程文档的评审和修订应在相应范围内进行	
		★策略与制度文档的保管	★指定专人保管	5.1.3.2 e)
			借阅策略和制度文档，以及相关的操作规程文档，应限定借阅范围，并经过相应级别负责人审批和登记	
			对涉密的策略和制度文档，以及相关的操作规程文档的保管应按照有关涉密文档管理规定进行；对保管的文档以及借阅的记录定期进行检查	
			应与相关业务部门协商制定专项控制的管理措施	

A.6.2 机构和人员管理

表 A.34 机构和人员管理(第五级信息系统)

类	族	评估项	评估内容要点	标准依据
★机构和人员管理	★安全管理机构	★建立安全管理机构	★成立信息系统安全管理委员会或信息系统安全领导小组,由组织机构的主要负责人出任信息系统安全领导小组负责人	5.2.1.1 e)
			对覆盖全国或跨地区的组织机构,应在总部和下级单位建立各级信息系统安全领导小组	
			★建立管理信息系统安全工作的职能部门,或明确指定一个职能部门兼管信息安全工作	
			配备专职安全管理人员,在基层至少要有一位专职的安全管理人员负责信息系统安全工作	
			应建立信息系统安全保密监督管理的职能部门,或对原有保密部门明确信息安全保密管理责任,加强对信息系统安全管理重要过程和管理人员的保密监督管理	
		★信息安全领导小组	★具有信息系统安全管理的领导职能	5.2.1.2 b)
			依据国家和行业有关信息安全的政策法规,批准信息系统的安全策略和发展规划	
			确定各有关部门在信息系统安全工作中的职责,领导安全工作的实施	
			监督安全措施的执行,并对重要安全事件的处理进行决策	
			指导和检查信息系统安全职能部门及应急处理小组的各项工作	
			建设和完善信息系统安全的集中控管的组织体系和管理机制	
			对保密管理部门进行有关信息系统安全保密监督管理方面的指导和检查	
		★信息安全职能部门	★确定信息安全职能部门基本的安全管理职能	5.2.1.3 b)
			起草信息系统的安全策略和发展规划	
			★管理信息系统安全日常事务,检查和指导下级单位信息系统安全工作	
			负责安全措施的实施或组织实施,组织并参加对安全重要事件的处理	
			监控信息系统安全状况,提出安全分析报告	
			★指导和检查各部门和下级单位信息系统安全人员及要害岗位人员的信息系统安全	
			★与有关部门共同组成应急处理小组或协助有关部门建立应急处理小组实施相关应急处理	
			管理信息系统安全机制集中管理机构的各项工作,实现信息系统安全的集中控制管理	
			完成信息系统安全领导小组交办的工作,并向领导小组报告信息系统安全工作	

表 A.34（续）

类	族	评估项	评估内容要点	标准依据
★机构和人员管理	安全机制集中管理机构	设置集中管理机构	★明确集中管理机构人员和职责，接受信息安全职能部门的直接领导	5.2.2.1 a)
			配备必要的领导和技术管理人员	
			选用熟悉安全技术、网络技术、系统应用等方面技术人员，明确责任，协同工作	
			统一承担信息系统的安全管理、系统管理、审计管理的运行监控、系统及安全配置	
			对与安全有关的信息进行汇集与分析	
			对与安全有关的事件进行响应与处置	
			对分布在信息系统中有关的安全机制进行集中管理	
		★集中管理机构职能	★集中管理机构统一管理信息系统运行安全，包括系统管理、安全管理和审计管理	5.2.2.2 c)
			★集中管理机构对关键区域的安全运行进行管理，控制知晓范围，对获取的有关信息进行相应安全等级的保护	
			建立物理、系统、网络、应用、管理等安全控制机制，构成整体安全控制机制	
			统一进行信息系统安全机制的配置与管理，确保各个安全机制按照设计要求运行	
			对服务器、路由器、防火墙等网络部件、系统安全运行性状态、信息（包括有害内容）的监控和检查	
			汇集各种安全机制所获取的与系统安全运行有关的信息，对所获取的信息进行综合分析	
			及时发现系统运行中的安全问题和隐患，提出解决的对策和方法	
			事件发现、响应、处置、应急恢复，根据应急处理预案，作出快速处理	
			对各种事件和处理结果有详细的记载并进行档案化管理，作为对后续事件分析的参考和可查性的依据	
			安全机制集中管理控制，完善管理信息系统安全运行的技术手段，进行信息系统安全的集中控制管理	
			负责接受和配合政府有关部门的信息安全监管工作	
			集中管理机构应与有关业务应用的主管部门协调，定制更高安全级别的管理方式	
	★人员管理	★安全管理人员配备	★安全管理人员不可兼任，属于专职人员，应具有安全管理工作权限和能力	5.2.3.1 d)
			安全管理人员应按照机要人员条件配备	
		★关键岗位人员管理	★关键岗位包括安全管理员、系统管理员、数据库管理员、网络管理员、重要业务开发人员、系统维护人员、重要业务应用操作人员，安全审计人员	5.2.3.2 e)
			允许一人多岗，但业务应用操作人员不能由其他关键岗位人员兼任	

表 A.34（续）

类	族	评估项	评估内容要点	标准依据
★机构和人员管理	★人员管理	★关键岗位人员管理	业务开发人员和系统维护人员不能兼任或担负安全管理员、系统管理员、数据库管理员、网络管理员、重要业务应用操作人员等岗位或工作	5.2.3.2 e)
			★关键岗位人员的权限应分散、不得交叉覆盖，系统管理员、数据库管理员、网络管理员不能相互兼任岗位或工作	
			关键岗位人员处理重要事务或操作时，应保持二人同时在场，关键事务应多人共管	
			必要时关键岗位人员应采取定期轮岗制度	
			定期安全培训，加强安全和风险防范意识	
			★应采取对内部人员全面控制的安全保证措施，对所有岗位工作人员实施全面安全管理	
		人员录用管理	由人事部门进行人员背景、资质审查，技能考核等，确认其具有基本的专业技术水平，能够掌握信息安全管理基本知识，合格者还要签署保密协议方可上岗	5.2.3.3 d)
			★对关键岗位的人员注重思想品质方面考察，重要区域或部位的安全管理人员一般可从内部符合条件人员选拔，要求认真负责和保守秘密	
			安全管理人员应具有基本的系统安全风险分析和评估能力	
			关键区域或部位的安全管理人员应选用实践证明精干、内行、忠实、可靠的人员，必要时可按机要人员条件配备	
		★人员离岗	★立即中止被解雇的、退休的、辞职的或其他原因离开的人员的所有访问权限	5.2.3.4 d)
			收回所有相关证件、密钥、访问控制标记等	
			收回机构提供的设备等	
			★管理层和信息系统关键岗位人员调离岗位，应经单位人事部门严格办理调离手续，承诺其调离后的保密要求	
			管理层和信息系统关键岗位人员调离单位，应进行离岗安全审查，在规定的脱密期限后，方可调离	
			关键部位的信息系统安全管理人员离岗，应按照机要人员管理办法办理	
		★人员考核与审查	定期对各个岗位的人员进行不同侧重的安全认知和安全技能的考核，作为人员是否适合当前岗位的参考	5.2.3.5 d)
			★定期审查关键岗位人员，如发现其违反安全规定，应控制使用	
			★对关键岗位人员的工作，应通过例行考核进行审查，并保留审查结果	
			★对所有安全岗位人员的工作，应通过全面考核进行审查，如发现其违反安全规定，应采取必要的应对措施	

表 A.34（续）

类	族	评估项	评估内容要点	标准依据
★机构和人员管理	★人员管理	★第三方人员管理	★签署相关安全责任的合同书或保密协议	5.2.3.6 c)
			★规定各类人员的活动范围，进入计算机房应有书面申请、批准和过程记录，有专人全程监督或陪同	
			★进行逻辑访问时，应划定范围并经书面申请、负责人批准和过程记录，有专人全程监督或陪同	
			进行逻辑访问应使用专门设置的临时用户，并进行审计	
			★在关键区域，一般不允许第三方人员进入或进行逻辑访问	
			如确有必要，除有书面申请外，可采取由组织机构内部人员带为操作的方式，对结果进行必要的过滤后再提供第三方人员，并进行审计	
			必要时对上述过程进行风险评估和记录备案，并对相应风险采取必要的安全补救措施	
	教育和培训	★信息安全教育	让员工知晓信息的敏感性和信息安全的重要性	5.2.4.1 e)
			认识其自身的责任和安全违例会受到纪律惩罚	
			掌握的信息安全基本知识和技能	
			★进行对安全政策和操作规程的认知教育和训练，以及安全知识、安全技术、安全标准、安全要求、法律责任和业务控制措施等方面培训	
			制定并实施安全教育和培训计划，针对不同岗位制定不同的专业培训计划，培养信息系统各类人员安全意识	
			定期检查人员安全资质的取得情况，将安全资质教育作为信息安全教育工作计划的一部分	
			对所有工作人员进行相应的安全资质管理，并使安全意识成为所有工作人员的自觉存在	
		信息安全专家	听取信息安全专家的建议	5.2.4.2 b)
			★组织专家参与安全威胁的评价，对安全事件给予专业指导和原因调查等	
			对于邀请或聘用信息安全专家可提供必要的组织机构内部信息，同时应告知专家这些信息的敏感性和保密性	
			应采取必要的安全措施，保证提供的信息在安全可控的范围内	

A.6.3 风险管理

表 A.35 风险管理(第五级信息系统)

类	族	评估项	评估内容要点	标准依据
风险管理	★风险管理要求和策略	风险管理要求	★编制资产清单,对资产价值/重要性进行分析,对信息系统面临的威胁进行初步分析	5.3.1.1 e)
			对关键的系统资源进行定期风险分析和评估	
			使用规范方法和工作流程,进行规范化的风险评估	
			产生风险分析报告和留存重要过程文档,并向管理层提交,建立风险管理体系文件	
			针对风险管理过程,实施独立审计,确保风险管理的有效性	
			将风险管理贯穿信息系统安全管理的全过程,成为信息系统安全管理的组成部分,并具有可验证性	
		★风险管理策略	制定基本的风险管理策略	5.3.1.2 c)
			★定期进行信息安全和业务应用方面的风险评估	
			确定信息安全风险管理的基本方法	
			提供风险管理的组织和资源保证	
			★建立风险管理的监督机制,对风险管理相关过程的活动和影响进行评估和监控	
			针对风险的变化重新启动风险评估,明确规定重新启动风险评估的条件	
	风险分析和评估	★资产识别和分析	确定信息系统的资产范围,进行统计和编制资产清单	5.3.2.1 b)
			★进行资产分类和重要性标识	
			★对信息系统的硬件、软件、系统接口、数据和信息、人员等方面的分析和识别	
			对信息系统的描述,包括信息系统的使命、边界、功能,以及系统和数据的关键性、敏感性等内容	
		威胁识别和分析	★根据以往发生的安全事件、外部提供的资料和积累的经验,对威胁进行分析	5.3.2.2 d)
			★结合业务应用、系统结构特点以及访问流程等因素,建立并维护威胁列表	
			根据不同业务系统面临的威胁,对每个或者每类资产有一个威胁列表	
			考虑威胁源在保密性、完整性或可用性等方面造成损害,对威胁的可能性和影响等属性进行分析,从而确定威胁的等级	
			通过综合威胁的可能性和强度的评价,修正威胁等级	
			★对关键区域或部位进行威胁分析,在业务应用许可并得到批准的条件下,可使用检测工具在特定时间捕捉攻击信息进行威胁分析	
		脆弱性识别和分析	★通过扫描工具、人工检查和渗透测试,获取对系统脆弱性的认识	5.3.2.3 c)
			针对信息系统资产组合、资产分类编制脆弱性列表和脆弱性检查表	

表 A.35（续）

类	族	评估项	评估内容要点	标准依据
风险管理	风险分析和评估	脆弱性识别和分析	应了解测试可能带来的后果，并做好充分准备	5.3.2.3 c)
			★对不同的方法和工具所得出的评估结果，进行综合分析，得到脆弱性等级	
			坚持制度化脆弱性评估，应明确规定进行脆弱性评估的时间和系统范围、人员和责任、评估结果的分析和报告程序，以及报告中包括新发现的漏洞、已修补的漏洞、漏洞趋势分析等	
		风险分析和评估要求	由用户和专家对资产、威胁和脆弱性等方面进行定性综合评估，建议处理和减缓风险的措施，形成风险评估报告	5.3.2.4 c)
			★评估报告中包括风险级别、风险点等内容，确定信息系统的安全风险状况	
			基于这些报告，要求评估者对信息系统安全措施提出建议	
			应将风险评估中的信息资产、威胁、脆弱性、防护措施等评估项信息综合到一个数据库中进行管理	
			应当在后续的项目和工具中持续地维护该数据库	
	风险控制	选择和实施风险控制措施	基于安全等级标准，选择相应等级的安全技术和管理措施	5.3.3.1 c)
			★根据风险评估结果，结合信息系统安全现状和需求，决定信息系统安全的控制措施	
			对相关的各种控制措施进行综合分析，得出紧迫性、优先级、投资比重等评价，形成体系化的防护控制系统	
	基于风险的决策	安全确认	★针对信息系统的资产清单、威胁列表、脆弱性列表，结合已采用的安全控制措施，分析存在的残余风险	5.3.4.1 c)
			形成残余风险分析报告，由组织机构的高层管理人员决定残余风险是否可接受	
			★编制信息系统残余风险清单，监视残余风险可能诱发的安全事件，及时采取防护措施	
			对信息系统安全风险实施再次评估，验证防护措施的有效性	
		信息系统运行的决策	★信息系统的主管者或运营者应根据安全确认的结果，判断残余风险是否可接受，决定是否允许信息系统继续运行	5.3.4.2 b)
			如果信息系统的残余风险不可接受，而现实情况又要求系统必须投入运行，且当前没有其他资源能胜任组织机构的使命，经过管理层的审批，可临时批准信息系统投入运行	
			应同时采取相应的风险规避和监测控制措施，并明确风险一旦发生的责任陈述	
	★风险评估的管理	★评估机构的选择	★有国家主管部门认可的安全服务资质	5.3.5.1 c) 及公通字[2007]43号文件第22条
			由国家指定专门部门、专门机构组织进行信息系统风险评估	
			★在中华人民共和国境内注册成立（港澳台地区除外）	
			★由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）	

表 A.35（续）

类	族	评估项	评估内容要点	标准依据
风险管理	★风险评估的管理	★评估机构的选择	★从事相关检测评估工作两年以上，无违法记录	5.3.5.1 c) 及公通字[2007]43号文件第22条
			★工作人员仅限于中国公民	
			★法人及主要业务、技术人员无犯罪记录	
			★使用的技术装备、设施应当符合本办法对信息安全产品的要求	
			★具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度	
			★对国家安全、社会秩序、公共利益不构成威胁	
		评估机构保密要求	★评估机构人员应按照第三方人员管理要求签署保密协议	5.3.5.2 c)
			★应有专人在整个评估过程中监督检查评估机构对保密协议的执行情况	
			对专门评估组的保密要求应参照《中华人民共和国保守国家秘密法》的要求，结合实际情况制定具体实施办法	
		评估信息的管理	★提交涉及评估需要的资料、数据等各种信息，应规定办理交接手续，防止丢失	5.3.5.3 c)
			提交涉及评估需要的资料、数据等各种信息，必要时可以隐藏或替换核心的或敏感的参数	
			★所有提交涉及评估需要的资料、数据等各种信息，只能存放在被评估方指定的计算机内，不得带出指定办公区域	
		技术检测过程管理	★使用工具或手工进行技术检测，应事先提交测试的技术方案，得到授权方可进行	5.3.5.4 d)
			使用工具或手工进行技术检测，应在被测试方专人监督下按技术方案进行	
			使用工具或手工进行技术检测，可采用由被评估方技术人员按技术方案进行操作，评估机构技术人员进行场外指导	
			使用工具或手工进行技术检测，应由被评估方技术人员按技术方案进行操作，对测试结果过滤敏感或涉及国家秘密信息后再交评估方分析	

A.6.4 环境和资源管理

表 A.36 环境和资源管理（第五级信息系统）

类	族	评估项	评估内容要点	标准依据
环境和资源管理	环境安全管理	环境安全管理要求	★应配置物理环境安全的责任部门和管理人员	5.4.1.1 e)
			建立有关物理环境安全方面的规章制度	
			物理安全方面应达到 GB/T 20271—2006 中 6.5.1 的有关要求	
			★对物理环境划分不同保护等级的安全区域进行明确标识和管理，包括机房、办公区域、介质库房等，实施不同保护等级安全区域的隔离管理	

表 A.36（续）

类	族	评估项	评估内容要点	标准依据
环境和资源管理	环境安全管理	环境安全管理要求	介质库房的管理可以参照同等级的机房的要求	5.4.1.1 e)
			制定对物理安全设施进行检验、配置、安装、运行的有关制度和保障措施	
			实行关键物理设施的登记制度	
			对重要安全区域的活动应实时监视和记录，出入人员应经过相应级别的授权并有监控措施	
			对物理安全保障措施，定期进行监督、检查和不断改进，实现持续改善	
		★机房安全管理要求	★明确机房安全管理的责任人	5.4.1.2 e)
			机房钥匙由专人管理，未经批准，不准任何人私自复制机房钥匙或服务器开机钥匙	
			★未经允许的人员不准进入机房	
			机房来访人员应经过正式批准，登记记录应妥善保存以备查	
			获准进入机房的来访人员，一般应禁止携带个人计算机等电子设备进入机房，其活动范围和操作行为应受到限制，并有机房接待人员负责和陪同，进入机房的人员应佩戴相应证件	
			任何进出机房的人员应经过门禁设施的监控和记录，应有防止绕过门禁设施的手段	
			所有来访人员的登记记录、门禁系统的电子记录以及监视录像记录应妥善保存以备查	
			未经批准，禁止任何人移动计算机相关设备或带离机房	
			★没有指定管理人员的明确准许，任何记录介质、文件材料及各种被保护品均不准带出机房，与工作无关的物品均不准带入机房	
			禁止携带移动电话、电子记事本等具有移动互连功能的个人物品进入机房	
			机房所在地应有专职警卫，通道和入口处应设置视频监控点，24 小时值班监视	
			机房内严禁吸烟及带入火种和水源	
			对需要防止电磁泄漏的计算机设备配备电磁干扰设备，在被保护的计算机设备工作时电磁干扰设备不准关机	
			可使用屏蔽机房（机柜），随时关闭屏蔽门，不得在屏蔽墙上打钉钻孔，不得在波导管以外或不经过过滤器对屏蔽机房（机柜）内外连接任何线缆	
			应定期测试屏蔽机房、机柜的泄漏情况并进行必要的维护	
		办公环境安全管理要求	★防止利用终端系统窃取敏感信息或非法访问	5.4.1.3 c)
			工作人员下班后，终端计算机应关闭	
			存放敏感文件或信息载体的文件柜应上锁或设置密码	
			工作人员调离部门或更换办公室时，应立即交还办公室钥匙	

表 A.36（续）

类	族	评估项	评估内容要点	标准依据
环境和资源管理	环境安全管理	办公环境安全管理要求	设立独立的会客接待室，不在办公环境接待来访人员	5.4.1.3 c)
			工作人员离开座位应将桌面上含有敏感信息的纸件文档放在抽屉或文件柜内	
			工作人员离开座位，终端计算机应退出登录状态、采用屏幕保护口令保护或关机	
			在关键区域或部位，应使办公环境与相关机房的物理位置在一起，以便进行统一的物理保护	
	资源管理	资产清单管理	★应编制并维护与信息系统相关详细的资产清单，能够清晰识别每项资产的拥有权、责任人、安全分类以及资产所在的位置等	5.4.2.1 c)
			信息资产：应用数据、系统数据、安全数据等数据库和数据文档、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、存档信息	
			软件资产：应用软件、系统软件、开发工具和实用程序	
			有形资产：计算机设备（服务器、终端、存储设备等），网络设备（路由器、交换机、安全设备等），移动存储介质（移动硬盘、磁带等），其他技术装备（电源，空调设备等），家具和机房	
			应用业务相关资产：由信息系统控制的或与信息系统密切相关的应用业务的各类资产，由于信息系统或信息的泄露或破坏，这些资产会受到相应的损坏	
			服务：计算和通信服务，通用设备如供暖、照明、供电和空调等	
			★必要时应包括主要业务应用系统处理流程和数据流的描述，以及业务应用系统用户分类说明	
		资产的分类与标识要求	★根据资产的价值/重要性对资产进行标识，可基于资产的价值选择保护措施和进行资产管理	5.4.2.2 c)
			★对信息资产进行分类管理，对信息系统内分属不同业务范围的各类信息，按其对安全性的不同要求分类加以标识	
			用户数据的重要性分类，如国家秘密信息、商业秘密和个人隐私信息、内部专有信息、公开信息等	
			系统数据重要性一般与其所在的系统或子系统的安全保护等级相关	
			根据业务应用的具体情况进行分类分级和标识，纳入规范化管理	
			以业务应用为主线，用体系架构的方法描述信息资产	
			通过对各个资产之间的关联，进行结构性描述	
		介质管理	★脱机存放的数据和软件介质，根据重要程度进行标识和分类，存放在由专人管理的介质库中，防止被盗、被毁、被修改以及信息泄漏	5.4.2.3 e)
			介质的归档和查询应有记录，其借阅、拷贝、分发传递须经相应级别的领导的书面审批后方可执行，并登记在册，对存档介质的目录清单应定期盘点，介质的分发传递以及带出工作环境应采取保护措施	

表 A.36（续）

类	族	评估项	评估内容要点	标准依据
环境和资源管理	资源管理	介质管理	存储介质的销毁在经主管领导审批后应由两人完成，一人执行销毁一人负责监销，销毁过程应记录，不得自行销毁，对于需要送出维修或销毁的介质，应首先删除信息，再重复写操作进行覆盖，防止数据恢复和信息泄漏	5.4.2.3 e)
			介质应保留 2 个以上的副本，而且要求介质异地存储，存储地的环境要求和管理方法应与本地相同，对重要介质的数据和软件必要时可以加密存储	
			★对存放在介质库中的介质应定期进行完整性和可用性检查，确认其数据或软件没有受到损坏或丢失，介质受损但无法执行删除操作的，必须销毁	
			对介质中的重要数据应使用加密技术或数据隐藏技术进行存储	
			对极为重要数据的介质应该使用高强度的加密技术或数据隐藏技术进行存储，并对有关密钥和数据隐藏处理程序严格保管	
		★设备管理要求	对于信息系统的各种软硬件设备的选型、采购、发放或领用，使用者应提出申请，报经相应领导审批，才可以实施	5.4.2.4 c)
			★设备的选型、采购、使用和保管应明确责任人	
			要求设备有专人负责，实行分类管理	
			★通过对资产清单的管理，记录资产的状况和资产使用、转移、废弃及其授权过程	
			★对各种资产进行全面管理，提高资产安全性和使用效率，保证设备的完好率	
			建立资产管理登记系统，提供资产分类标识、授权与访问控制、变更管理、系统安全审计等功能，为整个系统提供基础技术支撑	

A.6.5 运行和维护管理

表 A.37 运行和维护管理（第五级信息系统）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	★用户管理	★用户分类管理	用户分类应包括系统用户、普通用户、外部客户用户、临时用户	5.5.1.1 d)
			★按审查和批准的用户分类清单建立用户和分配权限，应对关键部位用户采取逐一审批和授权的程序，并记录备案	
			★用户分类清单应包括信息系统的所有用户的清单，包括所有特权用户、重要业务用户、关键部位用户的权限，以及用户的责任人员和授权记录	
			用户权限发生变化时应及时更改用户清单内容	
			对特权用户、重要业务用户、关键部位用户开启审计功能	
			定期检查特权用户、重要业务用户、关键部位用户的实际分配权限是否与用户清单符合	

表 A.37（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	★用户管理	系统用户要求	★系统用户应由信息系统的主管领导指定	5.5.1.2 c)
			★授权应以满足工作需要的最小权限为原则	
			系统用户应保护自己的身份鉴别信息的安全	
			系统用户应接受审计	
			对重要信息系统的系统用户，应进行审查并经过授权	
			★对系统用户应能区分责任到个人，不应以部门或组作为责任人	
			在关键信息系统中，对系统用户的授权操作，应有两人在场，经双重认可后方可操作	
			系统用户不准更改操作过程产生的审计日志	
		普通用户要求	★用户应保护自己的身份鉴别信息和载体的安全，不得转借他人	5.5.1.3 c)
			发现系统的漏洞、滥用或违背安全行为应及时报告	
			不应透露与组织机构有关的非公开信息	
			不应故意进行违规的操作	
			不应在不符合敏感信息保护要求的系统中保存和处理高敏感度的信息	
			不应使用各种非正版软件和不可信的自由软件	
			在系统规定的权限内进行操作，必要时某些重要操作应得到批准	
		机构外部用户要求	★应对外部用户明确说明使用者的责任、义务和风险，并要求提供合法使用的声明	5.5.1.4 c)
			外部用户应保护自己的身份鉴别信息的安全	
			外部用户只能是应用层的用户	
			可对特定外部用户提供专用通信通道，端口，特定的应用或数据协议，以及专用设备等	
			在关键部位，一般不允许设置外部用户	
		临时用户要求	★临时用户的设置和期限必须经过审批	5.5.1.5 c)
			临时用户应保护自己的身份鉴别信息的安全	
			★使用完毕或到期应及时删除	
			设置与删除均应记录备案	
			对主要部位的临时用户应进行审计，并进行风险评估	
			★在关键部位，一般不允许设置临时用户	
	运行操作管理	★服务器操作管理	★服务器操作系统、数据库系统的操作应由授权的系统管理员、数据库管理员实施	5.5.2.1 c)
			★遵照操作规程对服务器进行操作，设置服务器的运行环境，设定服务器的系统及安全配置，操作系统、数据库系统用户管理，并检查实际配置与安全策略要求的符合性	
			系统管理员、数据库管理员应以自己的账户及身份鉴别信息登录操作系统、数据库系统进行操作	

表 A.37（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	运行操作管理	★服务器操作管理	监控管理，包括监控系统性能，如 CPU 和内存的利用率、检测进程运行及磁盘使用情况	5.5.2.1 c)
			日志管理，包括对操作系统、数据库系统以及业务系统等日志的管理	
			负责系统配置和安全配置文件管理，包括服务器的操作系统和数据库系统的配置文件	
			★定期对操作系统和数据库系统安全进行检查，及时发现系统的缺陷或漏洞	
		终端计算机操作管理	★用户应设置终端计算机的开机、屏幕保护口令，保护身份鉴别信息，进行必要的安全设置	5.5.2.2 c)
			非本组织机构配备的终端计算机未获批准，不能在办公场所使用	
			及时安装经许可的软件和补丁程序，不得自行安装及使用其他软件和自由下载软件	
			未获批准，严禁使用 Modem 拨号、无线网卡等方式或另辟通路接入其他网络	
			应有措施防止终端计算机机箱被私自开启，如需拆机箱应经批准后由维修部门人员负责	
			高安全等级业务系统的终端计算机不得直接接入低级别系统或网络，应先作清理检查	
		便携机操作管理	在接入组织机构内部网络时遵守“终端计算机操作管理”（上一节）的要求	5.5.2.3 d)
			对不再使用或转为其他用途的便携机，应删除机内的敏感数据	
			在外网使用的便携机，接入本地网络前应进行必要的安全检查	
			★在组织机构内使用或存有敏感信息的便携机，未获批准，没有足够强度安全防护措施，严禁接入其他网络	
			便携机离开重要区域时不应存储敏感或涉密数据，外出使用应经有关领导批准并记录在案	
			在重要区域使用的便携机必须启用两个及两个以上身份鉴别技术的组合来进行身份鉴别	
			敏感数据应采用一定强度的加密储存技术，以规避便携机丢失的风险，必要时应对便携机采取物理保护措施	
		★网络及安全设备操作管理	★对网络及安全设备的操作应由授权的网络管理员、安全管理员实施，按照安全策略要求进行网络及安全设备配置	5.5.2.4 c)
			应按操作规程对网络设备和安全设备进行操作，进行网络和安全设备的运行环境配置和服务设定	
			网络管理员、安全管理员应以自己的账户及身份鉴别信息登录网络设备和安全设备进行操作	
			★定期检查实际配置与安全策略要求的符合性	
			应通过集中安全管理设施对网络及安全设备的安全机制进行监控管理和部署策略	

表 A.37（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	运行操作管理	业务应用操作管理	应用系统管理员及业务操作人员应自己的账户及身份鉴别信息登录业务应用系统（提供对外或专门服务的公共用户可除外）	5.5.2.5 c)
			★应用系统管理员根据安全策略和专门授权对应用系统的操作人员等用户及其权限进行管理，监控应用系统的运行	
			用户对业务应用系统的访问权限应受到控制，如以菜单等方式限制操作	
			用户应按照操作规程使用业务应用系统，操作规程应指明具体作业的指令，处理和使用的信息，以及操作步骤	
			业务应用系统操作规程应形成正式文档或帮助文件，需要进行改动时应得到管理层授权	
			操作规程应说明处理错误或其他异常情况的指令，以及在出现意外的操作或技术问题时需要技术支持的联系方法	
			对重要的业务应用操作应根据特别许可的权限执行，关键的业务应用操作应有 2 人同时在场或同时操作，并对操作过程进行记录	
			业务应用操作应进行审计	
		★变更控制和重用管理	★信息系统的变更，应提出更改方案，**进行安全评估**并得到系统主管领导的审批才能进行	5.5.2.6 e)
			进行变更应进行记录，对重大变更应评估其潜在影响，考虑全面安全事务一致性，更改后将变更结果书面向所有相关人员通报	
			操作系统、数据库系统的变更控制与应用系统的更改控制应相互配合	
			通过审计日志和过程记录，记载更改中的所有有关信息，过程记录应妥善保存	
			对重要的变更控制应实施安全审计，并对全面安全事务一致性进行检查，防止因变更而开放危险端口或服务	
			明确中止变更并从失败变更中恢复的责任和处理方法	
			对变更执行情况、过程文档管理，进行定期或不定期的检查**和持续改进**	
			设备重用，应提出设备重用方案，**进行安全评估**并得到系统主管领导的审批才能进行，应清除重用设备中原有信息，过程记录应妥善保存	
			对设备重用执行情况、过程文档管理，进行定期或不定期的检查**和持续改进**	
		信息交换管理	★在信息系统中发布信息和用户交换信息，应符合国家有关政策法规的规定	5.5.2.7 d)
			应采取适当的安全措施保护信息系统中发布信息和用户交换信息的完整性	
			应保护业务应用中的信息交换的安全性，防止欺诈、合同纠纷以及泄露或修改信息事件的发生	
			在组织机构之间进行信息交换应建立安全条件的协议	
			明确业务信息交换管理责任及数据传输的最低安全要求	
			还对于信息系统内部不同安全区域之间的信息传输，应有明确的安全要求	
			对高安全等级信息向低安全域的传输应经过领导层的批准，明确部门和人员的责任，并采取的安全专控措施	

表 A.37（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	运行维护管理	日常运行安全管理	★应通过正式授权程序委派专人负责信息系统运行的安全管理和风险控制，**作为组织机构业务管理的组成部分**	5.5.3.1 e)
			应明确运行值班的日常处理工作和安全管理职责，建立和维护信息系统运行过程管理文档	
			应对运行安全进行监督检查，包括检测、监控、分析等措施，评估运行安全策略的落实情况和一致性	
			应明确各个岗位人员对信息系统各类资源的安全责任和目标，包括日常操作、备份及容错等，以及对责任履行情况的审计	
			应明确信息系统安全管理人员和系统用户、普通用户对信息系统资源的访问权限	
			对信息系统关键岗位人员采取最小授权和分权制衡措施，如关键安全操作双人共管	
			应检查和维护信息系统中业务应用数据完整性、可用性、保密性，可根据需要提出技术改进的建议	
			★应用软件的使用采取授权管理，未经验证的软件不得运行系统中安装，对应用软件的使用进行审计	
			不允许外部服务方对信息系统访问	
			执行信息系统的数据备份、病毒防范、安全事件处理、变更控制等安全管理规定的日常工作任务	
			进行应急响应和灾难恢复计划规定的实际演练和技术培训，明确专人负责执行情况检查和**组织评估**，如数据备份和备用设备的可用性	
			根据组织机构和信息系统出现的各种变化进行风险分析，及时修订、完善各种规章制度，保证各方面安全事务管理的一致性和有效性	
			接受本系统上级或国家指定专门部门、专门机构进行专门监督和检查	
		运行状况监控	★委派专人负责监视信息系统重要应用、网络系统、核心服务器等是否运行正常，监视系统性能及与安全机制相关的服务器、网络性能变化	5.5.3.2 e)
			信息系统应使用统一的时间，以确保记录日志和审计信息准确	
			信息系统审计日志应保留一定期限，有脱机保存的介质，不能被改变，只允许授权用户访问	
			定期分析信息系统日志并产生报告	
			应告知用户某些行为是会被审计的	
			安全机制集中管理机构负责信息系统安全管理、系统管理、审计管理的集中监控和分析	
			安全机制集中管理机构应对关键区域和关键业务应用系统运行的监视，并与主管部门共同制定具体的管理办法	
			安全机制集中管理机构对关键区域和关键业务应用系统核心数据进行监视，应与主管部门共同制定具体的管理办法，并经上一级负责人的批准执行	

表 A.37（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	运行维护管理	软件硬件维护管理	★应明确信息系统的软件、硬件维护的人员和责任，规定维护的时限	5.5.3.3 d)
			对涉及维修的重要区域的数据和软件系统采取保护措施，防止因维修造成破坏和泄漏	
			应明确信息系统的硬件设备维修、替换和更新的申报、审批和管理流程	
			应明确信息系统软件维护的申报、审批和管理流程	
			★对需要外出维修的设备，应经过审批，磁盘数据应进行删除	
			★一般不应允许外部维修人员进入关键区域，必须进入机房维修，应经过审批，并有专人负责陪同	
			应根据维修方案和风险评估的结果确定维修方式，可采用更新设备的方法解决	
			应对维修过程及有关故障现象记录备案	
		外部服务方访问管理	对外部服务方访问实施严格控制，采取对外部服务方访问实施监视等安全措施，必要时应外部服务方的访问进行限制	5.5.3.4 d)
			应对外部服务方访问的要求进行风险分析，并经过相应的申报和审批程序，在重要安全区域对外部服务方每次访问进行风险控制	
			★外部服务方访问应签署了相应的保密合同	
	★外包服务管理	★外包服务合同	★对由外部服务商承担完成的外包服务，应签署正式的书面合同	5.5.4.1 a)
			对符合法律要求的说明，如数据保护法规	
			对外包服务的风险的说明，包括风险的来源、具体风险描述和风险的影响，明确如何维护并检测组织机构的业务资产的完整性和保密性	
			对外包服务合同各方的安全责任界定，应确保外包合同中的参与方（包括转包商）都了解各自的安全责任	
			对控制安全风险应采用的控制措施的说明，包括物理和逻辑控制措施，限制授权用户对组织机构的敏感业务信息的访问，以及设备的物理安全保护	
			对外包服务风险发生时应采取措施的说明，如在发生灾难事故时，应如何维护服务的可用性	
			对外包服务的期限、中止的条件和善后处理的事宜以及由此产生责任问题的说明	
			对审计人员权限的说明	
		外包服务商	外包服务的限制，关键的或涉密的业务应用，一般不应采用业务应用系统外包服务方式	5.5.4.2 c)
			★在行业认可或者是经过上级主管部门批准的范围内，选择具有相应服务资质并信誉好的可信的外包服务商	
		★外包服务的运行管理	★外包服务的限制，关键的或涉密的业务应用，一般不应采用业务应用系统外包服务方式	5.5.4.3 b)
			★对外包服务的业务应用系统运行的安全状况应进行监控和检查，应定期进行评估	
			对外包服务出现问题应遵照合同规定及时处理和报告	
			★当出现重大安全问题或隐患时应进行重新评估，提出改进意见，直至停止外包服务	

表 A.37（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	有关安全机制保障	★身份鉴别机制管理要求	信息系统所有用户均应明确使用身份鉴别机制的责任，保护用户自己的身份鉴别信息的保密性和完整性	5.5.5.1 e)
			在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性	
			★在每次用户登录系统时和重新连接系统时，采用受安全管理中心控制的口令、令牌、基于生物特征、数字证书以及其他具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别，且其中一种鉴别技术产生的鉴别数据是不可替代的	
			应指定安全管理人员定期检查信息系统用户身份鉴别机制和身份鉴别信息的安全性，特别是跨网络的远程用户鉴别信息的安全性	
			必要时，采用身份鉴别信息分段由多人保管，输入时由多人进行操作，操作过程需要留有操作记录和审批记录	
			规定需要重新鉴别用户的事件，即在需要重新鉴别的条件成立时，对用户进行重新鉴别，如进行重要操作之前进行重新鉴别	
			必要时，对身份鉴别机制的管理，可与相关业务部门共同制定专项管理措施	
		★访问控制机制管理要求	应根据自主访问控制安全策略，允许授权用户对其创建的客体具有相应的访问操作权限，包括对客体的创建、读、写、修改和删除等	5.5.5.2 e)
			实施访问控制机制主体的粒度为用户，客体的粒度为文件或数据库表级和(或)记录或字段级，强制访问控制客体的粒度为**文件或数据库表级和（或）记录或字段级**，将自主和强制访问控制扩展到所有主体与客体	
			★能够阻止非授权用户读取敏感信息并能将这些权限的部分或全部授予其他用户	
			实现对自主访问控制过程的审计，告知访问者须为自己的行为负责	
			应由授权的安全管理员通过特定专用方式对主、客体进行安全标记；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制	
			应确保信息系统内的所有主、客体具有一致的标记信息，并实施同一安全策略的强制访问控制规则	
			对访问控制进行监控管理，对系统、用户或环境进行持续性检查，注意保护监控数据	
			对访问控制权限进行专项审批，安全管理人员对网络、系统和应用等方面的访问控制机制进行检查	
		系统安全管理要求	应通过正式授权程序委派专人负责系统安全管理，包括对操作系统和数据库管理系统管理(系统管理员、数据库管理员)	5.5.5.3 e)
			建立系统安全配置、备份等安全管理规章制度及操作规程	
			由授权的系统安全员通过系统提供的操作界面，根据访问控制安全策略设置、维护用户及主、客体的标记信息	

表 A.37（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	有关安全机制保障	系统安全管理要求	★按规章制度的要求进行正确的系统安全配置、备份等操作，及时进行补丁升级	5.5.5.3 e)
			对操作系统和数据库系统进行用户账号安全使用和授权管理，并进行审计	
			对授权用户登录系统和使用许可的资源，进行身份鉴别和审计	
			依据安全策略确定审计事件、审计内容、审计归档、审计报告	
			应对系统的安全弱点和漏洞进行控制，对可能危及系统安全的系统工具进行严格的控制	
			应依据变更控制规程对系统的变更进行控制，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	
			应及时对系统资源和系统文档进行备份和安全标识	
			制定操作系统和数据库管理系统应急计划	
			应按系统内置角色强制指定系统安全管理责任人	
			保证系统管理过程的可审计，对系统管理过程留有记录	
			定期对操作系统、数据库系统的安全性进行检查	
			使用经过验证的系统及应用软件，对操作人员的操作过程实施监控或审计	
			信息系统的安全维护和管理工作也应受到监控，如一人操作一人检查	
		网络安全管理要求	应通过正式授权程序指定网络管理人员对网络系统进行配置和安全管理	5.5.5.4 e)
			★应按网络区域边界安全控制策略，实施数据包过滤措施，采用常规校验机制检验数据传输的完整性等安全管理，能够发现数据完整性被破坏，并在发现完整性被破坏时进行恢复	
			信息系统网络安全区域边界按访问控制策略设置自主和强制访问控制机制，对进出安全区域边界的数据信息进行控制，阻止非授权访问	
			依据总体安全策略制定网络访问控制策略，并定期检查和完善网络安全策略	
			采取网络访问授权管理，保证经过授权的用户才能得到许可的网络服务	
			告知用户使用网络的安全责任和操作规程	
			用户在外部访问组织机构内部网络应经审批，可采用由密码技术支持的保密性、完整性保护机制或具有相应强度的其他安全机制，保护网络数据传输安全	
			定期对外部网络连接接口的安全进行评估，可采用由密码技术支持的保密性、完整性保护机制或具有相应强度的其他安全机制，保护网络数据传输安全	
			对外公共服务的信息系统，应采取严格访问控制，保证外部用户的访问得到控制和审计，不危及内部信息系统的安全	

表 A.37（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	有关安全机制保障	网络安全管理要求	对外传输的数据和信息要经过批准和审查，防止内部人员通过内外网的边界泄露敏感信息	5.5.5.4 e)
			对可能从内部网络向外发起的连接资源实施控制和检查，探测非法外联等行为，保护网络及区域边界完整性	
			信息系统的关键网络设备设施的备份进行管理，保证可用性	
			对网络安全日常管理、网络配置变更、网络故障及事件处理等，定期进行安全检查和评估，对网络服务、网络安全策略、安全控制措施进行有效性检查和监督，提交正式的网络安全报告	
			可采用由密码技术支持的可信网络连接机制，通过对连接到通信网络的设备进行可信检验，保证接入通信网络的设备真实可信，防止设备的非法接入，保证信息系统网络之间的连接应使用可信路径	
			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	
			要求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	
			信息系统网络之间的连接严格控制在可信的物理环境范围内	
		应用系统安全管理要求	应通过正式授权程序委派专人负责应用系统的安全管理（应用系统管理员）	5.5.5.5 e)
			★应用系统管理员根据安全策略和专门授权对应用系统的操作人员等用户及其权限进行管理，监控应用系统的运行	
			应明确管理范围、管理事务、管理规程，以及应用系统软件的安全配置、备份等安全工作	
			应结合业务需求制定相关规章制度，制定并落实应用系统的安全操作规程，并严格按照规章制度的要求实施应用系统安全管理	
			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，保证应用系统数据的保密性、完整性和可用性	
			应指定专人负责应用系统的审计工作，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	

表 A.37（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	有关安全机制保障	应用系统安全管理要求	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	5.5.5.5 e)
			对应用系统软件的使用采取授权管理，未授权用户不得在在运行系统中安装、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	
			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负责应用系统的安全配置管理和应用管理	
			定期对应用系统的总体安全策略、应用系统安全措施的落实情况和运行管理进行检查	
			采取独立的应用安全审计，审计人员仅实施审计工作，不参与系统的其他任务，防止应用系统信息的泄漏	
			要求至少有两名以上的应用安全管理人员实施应用安全管理事务，并保证应用安全管理本身的安全风险得到控制，应与应用系统主管部门共同制定专项安全措施	
			应对应用系统的安全状态实施周期更短的审计、检查和操作过程监督，并保证对应用系统的安全措施能适应安全环境的变化	
		病毒防护管理要求	安排专人负责计算机病毒防护，定期进行检查报告主机和网络的病毒安全状况	5.5.5.6 d)
			★在主机安装防病毒软件，在安全区域边界设置防恶意代码网关，并及时升级，检查病毒库的升级情况并进行记录	
			对非在线的内部计算机设备及其他移动存储设备，以及外来或新增计算机做到入网前进行杀毒和防病毒软件版本检测	
			从不信任网络上所接收的文件或邮件，在使用前应首先检查是否有病毒	
			在网络内部建立专门的防病毒软件升级服务，实行整体策略、定期升级、统一控制，紧急情况下增加升级次数	
			采取对系统所有终端防范病毒软件集中管理的措施	
			定期检查信息系统病毒防护执行和管理情况	
		密码管理要求	★应按国家密码主管部门的规定，对信息系统中使用的密码算法和密钥进行管理	5.5.5.7 b)
			应按国家有关法律法规要求，对信息系统中包含密码的软、硬件信息处理模块的进、出口进行管理	

表 A.37（续）

类	族	评估项	评估内容要点	标准依据
运行和维护管理	安全集中管理	★安全机制集中控管	★对信息系统所涉及的服务器、网络、安全设备以及应用系统等的安全管理、系统管理、审计管理机制实施集中的监控、配置和管理	5.5.6.1 b)
			建立一体化和开放性平台，提供标准的接口，具备对安全资源管理能力	
			对系统的资源和运行进行配置、控制和管理，包括用户身份管理、系统资源配置、系统加载和启动、系统运行的异常处理以及支持管理本地和(或)异地灾难备份与恢复等	
			对系统中的主体、客体进行统一标记，对主体进行授权，对服务器、网络设备、安全设备等配置一致的安全策略	
			对分布在系统各个组成部分的安全审计机制进行集中管理，对审计记录应进行分析，并根据分析结果进行处理	
			授权的安全、系统、审计管理员应以自己的账户和身份鉴别信息进行登录和操作	
			根据信息系统网络结构需要，可按照分布式多层次的管理结构，进行分层分级联合方式的集中安全管理	
		安全信息集中管理	★将信息系统安全管理信息、系统管理信息、审计管理信息实施集中管理、综合分析	5.5.6.2 c)
			提供可视化报表和安全事件分析过程，以及安全事件的管理与辅助分析机制	
			对关键区域安全信息的集中管理，应采用相应安全级别的访问控制和保护措施	
			核心区域安全信息的集中管理应根据的需要确定，与有关主管部门共同制定专项的安全控制和保护措施	
		安全机制整合要求	进行信息系统资产信息管理	5.5.6.3 a)
			进行信息系统网络异常流量监控	
			进行信息系统安全事件监控管理	
			进行信息系统脆弱性管理	
			进行信息系统安全策略管理	
			进行信息系统安全预警管理	
		安全机制整合的处理方式	主要工作方式可包括自动处理、人工干预处理、远程处理、辅助决策分析处理、记录和事后处理等	5.5.6.4 a)

A.6.6 业务连续性管理

表 A.38 业务连续性管理（第五级信息系统）

类	族	评估项	评估内容要点	标准依据
业务连续性管理	★备份与恢复	★数据备份和恢复	★应明确说明需定期备份重要业务信息、系统数据及软件等内容和备份周期，根据数据的重要程度和更新频率设定备份周期	5.6.1.1 d)
			确定重要业务信息的保存期以及其他需要保存的归档拷贝的保存期	
			采用离线备份或在线备份方案，定期进行数据增量备份和应用系统全备份，必要时应采用热备份方式保存数据	
			指定专人负责数据备份和恢复，可使用手工或软件产品进行备份和恢复，同时保存几个版本的备份	
			定期检查备份介质，保证在紧急情况时可以使用	
			定期检查及测试恢复程序，确保在预定的时间内正确恢复	
			应分别指定专人负责不同方式的数据备份和恢复，并保存必要的操作记录	
			根据数据实时性和其他安全要求，采用本地或远地备份方式，制定适当的备份和恢复方式以及操作程序	
			必要时对备份后的数据采取加密或数据隐藏处理，操作时要求两名工作人员在场并登记备案	
		设备和系统的备份与冗余	★实现信息系统的关键设备备份与容错，实现系统热备份与冗余	5.6.1.2 c)
			★指定专人定期维护和检查备份设备和冗余设备的状况，确保需要接入系统时能够正常运行	
			根据实际需求确定备份设备接入的工作流程和操作时间，根据实际需求限定系统热备份和冗余设备切换的时间	
			指定专人定期维护和检查热备份的运行状况，定期进行切换试验，确保需要时能正常运行	
			选择远离市区的地方或其他城市，建立系统远地备份中心，确保主系统在遭到破坏中断运行时，远地系统能替代主系统运行，保证信息系统所支持的业务系统能按照需要继续运行	
	安全事件处理	安全事件划分	安全事件的处置需要贯穿整个安全管理的全过程，建立信息安全事件分等级响应和处置的制度	5.6.2.1 c)
			安全事件包括不可抗拒的事件、设备故障事件、病毒爆发事件、外部网络入侵事件、内部信息安全事件、内部误用和误操作等事件等	
			应依据安全事件对信息系统的破坏程度、所造成的社会影响及涉及的范围，确定具体信息系统安全事件处置等级的划分原则	
			★对信息系统中发生的各类事件制定相应安全保护等级的处置预案，确定事件响应和处置的范围、程度及工作流程	
			信息安全事件发生后，按预案分等级进行响应和处置	
			在发现或怀疑系统或服务出现安全漏洞或受到威胁时，应按照安全事件处置要求处理	
			明确不同安全事件的管理责任，制定不同安全事件的管理流程，包括制定处理预案、分析原因、收集证据、处理过程控制、总结吸取教训、责任划分和追究等内容	

表 A.38（续）

类	族	评估项	评估内容要点	标准依据
业务连续性管理	安全事件处理	★安全事件报告和响应	信息安全事件实行分等级响应和处置	5.6.2.2 c)
			★安全事件应尽快通过适当的管理渠道报告，注意安全弱点和可疑事件的报告，制定正式的报告程序和事故响应程序	
			对于暂不能确定为事故或入侵等的可疑事件也应报告	
			对于所有安全事件的报告应记录在案归档留存	
			使所有员工知道报告安全事件程序和责任，告知员工未经许可测试弱点属于滥用系统	
			★信息安全事件发生后，根据其危害和发生的部位，迅速确定事件等级，并根据等级启动相应的响应和处置预案	
			要求安全管理机构或职能部门负责接报安全事件报告，并及时进行处理，注意记录事件处理过程	
			对于重要区域或业务应用发生的安全事件，应注意控制事件的影响	
			事件处理后应有相应的反馈程序，应追究安全事件发生的技术原因和管理责任，写出处理报告，并进行必要的评估	
	★应急处理	应急处理和灾难恢复	★信息安全领导小组应有人负责或指定专人负责应急计划和灾难恢复计划管理工作	5.6.3.1 e)
			信息系统安全机制集中管理机构应协助应急处理小组负责具体落实	
			检查或验证（演练）应急计划和灾难恢复计划，保证应急计划和灾难恢复计划能够有效执行	
			安全管理机构应制定总体应急计划和灾难恢复计划，应急处理小组负责落实	
			制定**所有**应用系统和支持系统的**全面的**应急预案和灾难恢复预案，并进行测试	
			对计划涉及人员进行培训，保证这些人员具有相应执行能力	
			与应急需要应急的外部支持单位，应签订合同	
			做好应急处理和灾难恢复的基础工作，包括安全事件处理，系统及数据备份的管理	
			针对应急计划和灾难恢复计划实施进行独立审计	
			针对应急计划和灾难恢复计划进行定期评估，不断改进和完善	
			基于应急计划和灾难恢复计划和安全策略，进行可验证的操作过程监督	
		★应急计划	★制定应急计划（应急计划框架内容包括）	5.6.3.2 a)
			制定应急计划策略，明确制定应急计划所需的职权和相应的管理部门	
			进行业务影响分析，识别关键信息系统和部件，确定优先次序	
			确定防御性控制，减小系统中断的影响，提高系统的可用性；注意采取措施，减少应急计划生存周期费用	
			制定恢复策略，确保系统可以在中断后快速和有效的恢复	
			制定信息系统应急计划，包括恢复受损系统所需的指导方针和规程	
			计划测试、培训和演练，发现计划的不足，培训技术人员	
			计划维护，有规律地更新适应系统发展	

表 A.38（续）

类	族	评估项	评估内容要点	标准依据
业务连续性管理	★应急处理	应急计划的实施保障	★应对明确应急计划的组织和实施人员，使其知道在应急计划实施过程中各自的责任	5.6.3.3 e)
			对系统相关的人员进行培训和组织演练，知道如何以及何时使用应急计划中的控制手段及恢复策略，保证执行应急计划应具有的能力	
			进行系统化管理用于实施和维护整个组织的应急计划体系，并记录计划实施过程	
			确保应急计划的执行有足够资源的保证	
			应对系统运行过程的风险进行评估，识别可能引起业务过程中断的事件，听取业务人员的建议，完善应急计划的实施	
			应针对计划的正确性和完整性进行定期检查，在计划发生重大变化时应立即检查	
			根据业务应用的重要程度的不同，不断对计划内容和规程进行评估和完善	

A.6.7 监督和检查管理

表 A.39 监督和检查管理（第五级信息系统）

类	族	评估项	评估内容要点	标准依据
监督和检查管理	符合法律要求	★知晓适用的法律	应认识对于信息系统应用范畴适用的所有法律法规	5.7.1.1 c)
			★对信息系统的设计、操作、使用和管理，以及信息管理方面，应认识和规避法律法规禁区，防止出现违法行为	
			保护组织机构的数据信息和个人信息隐私	
			对于详细而准确的法律要求应从组织机构的法律顾问，或者合格的法律从业人员处获得帮助	
			应知晓不允许滥用信息处理设备，以免危害组织机构和社会利益，并有措施防止滥用	
			★信息系统中采用的密码技术应使用国家主管部门批准的算法，符合国家有关法规的要求	
		知识产权管理	应建立关于尊重知识产权的策略，防止发生侵犯版权的行为，并形成书面文档	5.7.1.2 c)
			涉及软件开发的工作人员和承包商应做到符合和遵守相关的法律、法规	
			应明确规定外包开发的应用系统软件的有关软件版权问题	
			应防止外包开发的应用系统因软件升级或改造发生侵犯软件版权问题	
			★对关键业务应用，必要时应要求使用具有自主知识产权的软件，以保护关键业务应用的安全	

表 A.39（续）

类	族	评估项	评估内容要点	标准依据
监督和检查管理	符合法律要求	保护证据记录	规定组织机构的重要记录的内容范围，如财务记录、数据库记录、审计日志等	5.7.1.3 a)
			★应按照法律法规的要求保护组织机构的重要记录，防止丢失、毁坏和被篡改	
			被作为证据的记录，信息的内容和保留的时间应遵守国家法律法规的规定	
	依从性检查	检查和改进	要求组织机构定期对安全管理活动的各个方面进行检查和评估工作	5.7.2.1 b)
			建立检查和改进制度，做到定期检查实施的所有安全程序是否遵从了组织机构制定的安全方针和政策，检查信息系统在技术方面是否依从了安全标准，根据检查过程中发现的不足对安全管理体系进行不断改进	
			★对照组织机构的安全策略和管理制度做到自管、自查、自评，并应落实责任制，接受国家监管部门的监管	
		★安全策略依从性检查	定期检查信息系统的网络、操作系统、数据库系统等系统管理员，对安全策略的遵守情况，包括是否能正确执行安全制度，遵从安全策略	5.7.2.2 c)
			★定期检查信息系统各个岗位对操作规程和管理制度的执行情况，确保遵从组织机构的安全策略	
			检查范围应包括信息系统本身，以及系统供应商、信息和信息资产的所有者、用户和管理层，保证其符合安全策略和标准	
			检查有关系统使用情况和操作等监控过程，根据检查结果，对信息系统安全管理体系和安全管理执行过程存在的问题进行不断改进	
		★技术依从性检查	**★按照信息系统应达到安全保护等级第五级技术要求**定期进行检查，根据检查信息系统对安全实施标准的符合情况进行初步评价并形成意见	5.7.2.3 c)
			对硬件和软件的检验，以及技术依从检查应由有能力的、经过授权的人员来进行	
			对于技术检测应由有经验的系统工程师手工或使用软件包进行并生成检测结果，经技术专家解释并产生技术报告	
			应根据检查结果，对存在的缺陷进行不断改进	
			对关键区域或敏感系统的技术依从性检查应严格控制，并注意对有关检测过程和检测结果的安全进行保护	

表 A.39（续）

类	族	评估项	评估内容要点	标准依据
监督和检查管理	审计及监管控制	★审计控制	应有独立的审计机构或人员对组织机构的安全管理体系、信息系统的安全风险控制、管理过程的有效性和正确性进行审计	5.7.3.1 c)
			★对审计过程进行控制，应制定审计的工作程序和规范化工作流程，将审计活动周期化，同时加强安全事件发生后的审计	
			应对系统的审计活动进行规划，尽量减小中断业务流程的风险	
			系统审计过程控制要求，审计的范围必须经过授权并得到控制，审计所需的资源应明确定义并保证可用性，应审计和记录所有的访问，对所有的流程、需求和责任都应文档化	
			应对系统审计工具进行保护，防止误用造成危害	
			审计工具应与开发系统和运行系统分开管理	
			应明确审计工具的适用范围，使用过程应经过批准，应记录审计工具的所有使用过程，应明确审计工具的保存方式、责任人员等	
		监管控制	**依照国家有关法规和 GB 17859—1999 第五级的要求进行自主保护，国家指定专门部门、专门机构进行专门监督**	5.7.3.2 e)
	责任认定	审计结果的责任认定	对于审计及监管过程发现的问题应限期解决	5.7.4.1 c)
			★应认定技术责任和管理责任，明确责任当事人，提出问题解决办法和责任处理意见	
			应对审计及监管过程发现的问题认定相关领导者的责任，组织机构领导层应就此提出问题解决办法和责任处理意见，以及监督问题解决情况	
			应对审计及监管过程发现问题的处理结果进行必要的复查，并明确进行审计及监管复查的期限和责任	
		审计及监管者责任的认定	审计及监管者应按有关监督和检查的规定定期进行审计，逾期未进行审计及监管，使本应审计的问题因未审计而造成信息系统损失，应承担相应的责任	5.7.4.2 c)
			审计及监管者虽能够按有关监督和检查的规定进行审计，但因未能及时发现本应审计出问题而造成信息系统损失的，应承担相应的责任	
			审计及监管者应对审计及监管过程发现问题的处理结果进行必要的跟踪检查直至问题的解决，如因未进行跟踪检查而造成损失的，应承担相应的责任	

A.6.8 生存周期管理

表 A.40 生存周期管理(第五级信息系统)

类	族	评估项	评估内容要点	标准依据
生存周期管理	★规划和立项管理	系统规划要求	信息系统的管理者应对信息系统的建设和改造,以及近期和远期的发展制定工作计划,并应得到管理层的批准	5.8.1.1 c)
			应制定安全策略规划并得到管理层的批准	
			安全策略规划主要包括信息系统的总体安全策略、安全保障体系的安全技术框架和安全管理策略等	
			能够为信息系统安全保障体系的规划、建设和改造提供依据,使管理者和使用者都了解信息系统安全防护的基本原则和策略,知道应采用的各种技术和管理措施对抗各种威胁	
			依据安全策略规划,制定安全建设和安全改造的规划,并应得到组织机构管理层的批准	
		系统需求的提出	★信息系统应用部门或业务部门需要开发新的业务应用系统或更改已运行的业务应用系统时,以书面形式提出申请	5.8.1.2 c)
			★信息系统的安全管理职能部门应根据信息系统的安全状况和存在隐患的分析,以及信息安全评估结果等提出加强系统安全的具体需求,并以书面形式提出申请	
			安全需求的分析和说明,至少包括组织机构的业务特点和需求,威胁、脆弱性和风险的说明,安全的要求和保护目标	
			信息系统的管理者应根据信息系统安全建设规划的要求,提出当前应进行安全建设和安全改造的具体需求,并以书面形式提出申请	
		★系统开发的立项	接到系统需求的书面申请,必须组织有关部门负责人和有关安全技术专家进行可行性论证和安全性评价	5.8.1.3 c)
			★通过可行性论证和确认项目安全性符合要求后由主管领导审批,或者经过管理层的讨论批准,才能正式立项	
	★建设过程管理	★建设项目准备	★对信息系统建设和改造项目应明确指定项目负责人,监督和管理项目的全过程,明确信息系统建设和改造项目的管理流程	5.8.2.1 c)
			应制定详细的项目实施计划,作为项目管理过程的依据	
			建立工程实施监理管理制度,明确指定项目实施监理负责人	
		工程项目外包要求	对于安全保护等级较高的信息系统工程项目,一般不应采取工程项目外包方式	5.8.2.2 d)
			信息系统工程项目外包,应选择具有服务资质的信誉较好的厂商,要求其已获得国家规定的资质证书、有成功的实施案例	
			对重要的信息系统工程项目外包,应在主管部门指定或特定范围内选择具有服务资质的信誉较好的厂商,并应经实践证明是安全可靠的厂商	
			对外包中被废止和暂停的项目,要确保相关的系统设计、文档、代码等的安全	
			对代码的所有权和知识产权、软件开发过程质量控制、代码质量检测、上线前的安全测试等制定控制措施	

表 A.40（续）

类	族	评估项	评估内容要点	标准依据
生存周期管理	★建设过程管理	自行开发环境控制	★自行开发项目，要求开发环境与实际运行环境做到物理分开，建立完全独立的两个环境	5.8.2.3 d)
			开发及测试活动也应尽可能分开	
			系统开发文档应有专人负责保管，系统开发文档的使用须经管理层的批准	
			系统开发文档的变更应按照变更管理流程进行控制	
			一般不鼓励对非自行开发的软件包进行修改，必须改动时应注意内置的控制措施和整合过程被损害的风险，软件的改动对将来的维护带来影响，应保留原始软件并在完全一样的复制件上进行改动，所有的改动应经过充分的测试并形成文件，以便必要时用于将来的软件升级	
			应严格控制对源程序的访问，源程序不应被保存在运行系统中，技术开发人员不应具有对程序资源库不受限制的访问权，源程序库的更新和向程序员发布的程序源应经授权，应保留程序的所有版本，程序清单应被保存在一个安全的环境中，应保存对所有源程序库访问的审计记录	
			对于安全保护等级较高的信息系统建设项目及涉密项目，应对开发全过程采取相应的保密措施，对参与开发的有关人员进行保密教育和管理	
		★安全产品使用要求	信息安全产品包括构成信息系统安全保护功能的信息技术硬件、软件、固件设备，以及安全检查、检测验证工具等	5.8.2.4 a) 及公通字[2007]43 号文件第 21 条
			★信息系统使用的信息安全产品应按照相应的安全保护等级的要求选择相应等级的产品	
			★产品研制、生产单位是由中国公民、法人投资或者国家投资或者控股的，在中华人民共和国境内具有独立的法人资格	
			★产品的核心技术、关键部件具有我国自主知识产权	
			★产品研制、生产单位及其主要业务、技术人员无犯罪记录	
			★产品研制、生产单位声明没有故意留有或者设置漏洞、后门、木马等程序和功能	
			★对国家安全、社会秩序、公共利益不构成危害	
			★对已列入信息安全产品认证目录的，应当取得国家信息安全产品认证机构颁发的认证证书	
		★建设项目测试验收	★对信息系统建设和改造项目进行功能及性能测试，进行安全测试验收，保证信息系统建设项目的保密性、完整性、可用性	5.8.2.5 c)
			应指定项目测试（包括安全测试）验收负责人	
			应制订测试和接收标准，确保信息系统建设和改造项目的接收要求和标准被清晰定义并文档化	
			对安全系统的测试至少包括对组成系统的所有部件进行安全性测试，对系统进行集成性安全测试，对业务应用进行安全测试等	
			在信息系统建设和改造项目验收时至少还应考虑系统性能和容量的要求，错误恢复、重启程序及应急计划，制定并测试日常的操作程序以达到规定的标准，实施了设计方案规定的安全控制措施，提供了有效的用户指南，新系统对组织机构业务的安全影响，操作和使用新系统的培训	

表 A.40（续）

类	族	评估项	评估内容要点	标准依据
生存周期管理	系统启用和终止管理	★新系统启用管理	★在新的信息系统或子系统、信息系统设备在启用以前，应经过正式测试验收	5.8.3.1 d)
			由使用者或管理者提出申请，经过相应领导审批才能正式投入使用	
			应进行一定期限的试运行，并得到相应领导和技术负责人认可才能正式投入使用，并形成文档备案	
			组织有关管理者、技术负责人、用户和安全专家，对新的信息系统或子系统、信息系统设备的试运行进行专项安全评估，得到认可并形成文档备案才能正式投入使用	
			新系统正式投入使用的一定时间内，应进行审计跟踪，定期对审计结果做出风险评价，对安全进行确认以决定是否能够继续运行，并形成文档备案	
		★终止运行管理	终止运行包括现有信息系统或子系统、主要设备	5.8.3.2 c)
			应由使用者或管理者提出申请并说明原因	
			应由使用者或管理者提出采取的保护措施	
			★在任何新的信息系统或子系统、信息系统设备需要终止运行以前，应进行必要数据和软件备份，对终止运行的设备进行数据清除	
			得到相应领导和技术负责人认可才能正式终止运行，并形成文档备案	
			★应采取必要的安全措施，并进行数据和软件备份，对终止运行的设备进行不可恢复的数据清除，如果存储设备损坏则必须采取销毁措施，在得到相应领导和技术负责人认可才能正式终止运行，并形成文档备案	

参 考 文 献

[1] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求
[2] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求
[3] GA/T 713—2007 信息安全技术 信息系统安全管理测评
[4] 公通字[2007]43号 信息安全等级保护管理办法
[5] OCTAVE Method Implementation Guide v2.0(OCTAVE方法实施指南)

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
信息系统安全管理评估要求
GB/T 28453—2012
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100013)
北京市西城区三里河北街 16 号(100045)
网址:www.gb168.cn
服务热线:010-68522006
2012 年 10 月第一版
*
书号:155066·1-45468

GB/T 28453-2012