ICS 35.020
L09

GA

中华人民共和国公共安全行业标准

GA/T 713-2007

信息安全技术
信息系统安全管理测评

Information security technology -
Information system security management testing and evaluation

2007-08-13 发布　　2007-10-01 实施

中华人民共和国公安部　发布

目　　次

前　　言

（略）

引　　言

本标准用于在实施信息系统安全等级保护时，根据GB/T 20269-2006《信息安全技术 信息系统安全管理要求》对安全管理体系各等级安全管理要求的落实情况进行评估，规定了评估的主要内容和原则，明确了评估过程和方法。对于涉及国家秘密的信息和信息系统的保密管理，应按照国家有关保密管理规定和相关测评标准执行。

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、第三方评估机构、信息系统的管理者等，对应的评估可以是检查评估、第三方评估或自评估，本标准中统称评估。

本标准第 4 章（管理评估的基本原则）、第 5 章（评估方法）、第 6 章（评估实施）给出了每一安全保护等级的评估需要执行的统一要求和评估方法，在第 7 章分等级描述了 GB/T 20269-2006 规定的评估要求。本标准中有关信息系统安全管理评估项见附录 A。

信息安全技术

信息系统安全管理测评

1 范围

本标准规定了按照 GB17859-1999 等级划分的要求对信息系统实施安全管理评估的原则和方法。

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。

2 规范性引用文件

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

GB 17859-1999 计算机信息系统 安全保护等级划分准则

GB/T 20269-2006 信息安全技术 信息系统安全管理要求

3 术语和定义

GB 17859-1999、GB/T 20269-2006 确立的以及下列术语和定义适用于本标准。

3.1

安全审计 security audit

对信息系统记录与活动的独立的审查和检查，以测试系统控制的充分程度，确保符合已建立的安全策略和操作过程，检测出安全违规，并对在控制、安全策略和过程中指示的变化提出建议。

3.2

风险评估 risk assessment

风险识别、分析、估值的全过程，其目标是确定和估算风险值。

3.3

安全策略 security policy

一个组织为其运转而规定的一个或多个安全规则、规程、惯例和指南。

3.4

监测验证 validate by inspect and test

通过对与安全管理有关的监测信息（包括审计信息以及各种监测、监控机制收集的信息）的分析，对安全管理实施的有效性进行验证的过程。

4 管理评估的基本原则

对信息系统安全管理的评估应坚持科学性、有效性、公正性等基本原则，即评估的原理、方法、流程、具体要求是科学的，正确的；评估的方法、流程等是可操作的，成本和效率等方面可接受；评估结果是客观公正的，评估机构是中立权威的。还应遵循以下原则：

—— 有效性原则：根据 GB/T 20269-2006 充分考虑信息系统功能，信息资产的重要性，可能受到的威胁及面临的风险，评估整个安全管理体系的有效性；

—— 体系化原则：根据 GB/T 20269-2006 中 4.2 的信息系统安全管理原则，针对安全管理体系基本要素，评估安全管理体系是否完整。比较完整的安全管理体系应基本涵盖 GB/T 20269-2006 中 4.1 的各项；

—— 标准化原则：根据 GB/T 20269-2006 各保护等级的安全管理目标，重点检查、评估安全管理标准化工作情况；识别和理解信息安全保障相互关联的层面和过程，采用管理和技术结合的方法，提高实现安全保障目标的有效性和效率；

—— 一致性原则：根据 GB/T 20269-2006 各保护等级系统的安全管理应贯穿整个信息

系统的生存周期，评估时重点检查信息系统设计、开发、部署、运维各个阶段的安全管理措施是否都到位；

—— 风险可控性原则：信息安全管理工作是信息系统安全稳定运行的基础，安全管理的安全性直接决定了信息与信息系统的安全性，在评估管理体系时，应注意相关安全管理的可靠性、可控性，确保管理行为和风险得到控制；

—— 安全管理保证原则：根据 GB/T 20269-2006 各保护等级安全管理条款，要求评估时应根据信息系统安全管理工作的保证情况，实事求是地根据实际保证证据决定是否达到相应保护等级安全管理要求的标准；

—— 客观性和公正性原则：评估工作应摆脱自身偏见，避免主观臆断，坚持实事求是，按照评估工作相关各方相互认可的评估计划和方案，基于明确定义的评估要求，开展评估工作，给出可靠结论。

5 评估方法

5.1 调查性访谈

5.1.1 调查性访谈主要对象

调查性访谈的主要对象一般可以包括：

—— 组织的领导、信息化主管领导、信息部门领导；

—— 物理安全主管及资产管理、机房值守、机房维护人员；

—— 运行维护主管及网络管理、系统管理、数据库管理、应用软件维护、硬件维护、文档介质管理人员；

—— 信息安全主管及安全管理、审计管理人员；

—— 系统建设主管及建设管理、软件开发、系统集成人员；

—— 外包服务方主管及外包方运行、维护人员；

—— 业务部门主管，以及应用管理、业务应用、业务操作人员；

—— 人事部门主管，以及人事管理、应用培训人员等。

5.1.2 调查性访谈准备

调查性访谈前，应准备调查问卷，提高访谈效率。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保证结构清晰、系统、详细，确保问题的答案是“是/否/不确定”。对等级要求明确的内容应建立检查表，确保检查表结构清晰、提高数据取得的一致性。

5.1.3 调查性访谈阶段划分

调查性访谈是从被评估单位相关组织中的成员以及其他机构获得评估证据的一种方法。实施调查性访谈时，应明确评估不同阶段的目标和任务。调查性访谈应划分为以下阶段：

a) 初步访谈：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；

b) 实事收集访谈：实事收集访谈主要用于根据安全管理体系特定要求，针对特定对象的访谈；

c) 后续深入访谈：后续深入访谈主要是在对事实收集访谈收集到的信息进行分析并发现问题后进行的，目的是寻找解决问题的答案；

d) 结案性访谈：结案性访谈是指评估工作结束时的会议，通过与被评估单位进行会议讨论，保证评估结论、评估发现、建议的正确性。

5.1.4 调查性访谈质量控制

对调查性访谈的质量，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，调查性访谈的质量控制分为：

a) 一级控制，包括下列要求：

——访谈对象以负责人为主；

——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) 二级控制，包括下列要求：

——访谈对象以负责人、技术人员为主，必要时可选择操作人员；

——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) 三级控制，包括下列要求：

——访谈对象以负责人、技术人员、操作人员为主，必要时可选择其他相关人员；

——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) 四级控制，包括下列要求：

——访谈对象以负责人、技术人员、操作人员为主，并选择其他相关人员；

——进行全面访谈，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) 五级控制，包括下列要求：

——访谈对象以负责人、技术人员、操作人员为主，并选择保密部门及其他相关人员；

——进行全面访谈，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。

5.2 符合性检查

5.2.1 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，安全应急及复审和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／管理员指南；

g) 其他需要进行符合性检查的内容。

5.2.2 符合性检查方法

符合性检查可以采用以下方法：

a) 根据安全管理标准和被评估单位的安全管理体系相关文件的要求，检查安全管理运行过程或各个环节的文档的具体规定是否与有关要求相一致，必要时可以对相关的材料（如记录、日志、报告、检验／评估／审计结果等）进行评价；

b) 为了减少评估对象的工作量，评估人员应尽最大可能重复使用以前的安全管理控制评价的结果和证据（当有这样的结果可供使用的时候，信息系统应该没有发生过有可能造成结果无效的重大变更，而且应证明这些结果是可靠的）。

5.2.3 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) 一级控制，包括下列要求：

——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) 二级控制，包括下列要求：

——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) 三级控制，包括下列要求：

——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) 四级控制，包括下列要求：

——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) 五级控制，包括下列要求：

——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。

5.3 有效性验证

5.3.1 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) 针对访问控制策略、制度，采用验证工具进行功能性验证；

b) 针对标识与鉴别和审计机制的功能检验；

c) 针对安全配置设定的功能检验；

d) 针对物理访问控制的功能检验；

e) 针对信息系统备份操作的功能检验；

f) 针对事件响应和意外防范规划能力的检验。

5.3.2 有效性验证方法

针对被评估组织确立的安全管理目标，通过对管理活动的实际考查，验证安全管理体系的运行效果，以及能否获得预期的目标。有效性验证方法及评价主要包括：

a） 检查信息系统的管理者是否已经按GB/T 20269-2006的要求建立了文件化的安全管理体系，即过程已经被确定，过程程序已经恰当地形成了文件；

b） 检查被确定的过程是否已经得到了充分的展开，即按过程程序的要求得到了贯彻实施；

c） 检查过程程序的贯彻实施是否取得了预期期望的结果，并以此证明过程是有效的；

d） 有效性可从以下方面进行评价：

——管理控制措施：如方针策略、业务目标、安全意识等方面；

——业务流程：如风险评估和处理、选择控制措施等；

——运营措施：如操作程序、备份、防范恶意代码、存储介质等方面；

——技术控制措施：如防火墙、入侵检测、内容过滤、补丁管理等；

——审核、回顾和测试：如内审、外审、技术符合性等。

5.3.3 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) 一级控制，包括下列要求：
——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) 二级控制，包括下列要求：
——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) 三级控制，包括下列要求：
——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) 四级控制，包括下列要求：
——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) 五级控制，包括下列要求：
——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。

5.4 监测验证

5.4.1 监测验证的主要依据

安全管理监测验证的主要依据是与安全管理有关的审计信息和监测、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监测、监控信息，包括独立监测、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监测、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监测、监控信息；

d) 其他涉及信息系统安全管理方面的监测、监控信息。

5.4.2 监测验证方法

安全管理监测验证的方法包括：

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) 安全管理监测验证分为：
——简单的监测验证；
——充分的监测验证；
——全面的监测验证。

c） 安全管理监测验证的过程，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。

5.4.3 监测验证质量控制

对监测信息验证的质量，应从监测验证的广度和监测验证的深度进行控制。根据不同安全等级的不同要求，监测验证的质量控制分为：

a） 一级控制，包括下列要求：

——可进行简单的监测验证，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、数据库管理系统的审计信息为基本依据，进行监测验证；

——可通过对特定时段的审计信息的分析进行监测验证。

b） 二级控制，包括下列要求：

——应进行简单的监测验证，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监测验证；

——应通过对特定时段的监测信息的分析进行检测验证。

c） 三级控制，包括下列要求：

——应进行充分的监测验证，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监测验证；

——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。

d） 四级控制，包括下列要求：

——应进行较全面的监测验证，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监测验证；

——应通过对较长时段的连续监测信息的分析进行检测验证。

e） 五级控制，包括下列要求：

——应进行全面的监测验证，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，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期望的结果，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的监测验证；

——应通过对长期的连续监测信息的分析进行监测验证。

6 评估实施

6.1 确定评估目标

信息系统安全管理评估的目标是，根据已经确定的安全管理等级，按照 GB/T 20269-2006 相应等级的管理内容及管理水平进行符合性、有效性检查和验证，检验信息系统安全管理体系和管理水平是否满足确定等级的管理要求。

具体实施安全管理评估时，应明确描述所涉及的被评估对象，确定每一个具体的被评估对象的安全管理等级，以及需要达到的安全管理评估的具体目标。

6.2 控制评估过程

信息系统安全管理评估过程可从以下方面进行控制：

a) 确定安全管理评估的范围，包括：根据安全方针政策、安全工作计划、安全方案等相关文件中描述的安全管理控制，并依据系统的使命、业务、组织管理结构、技术平台、物理网络基础设施、以及相关政策、法律、法规等，确定评估的范围；

b) 建立安全管理控制措施的评估规程，包括：

——应在充分考虑信息系统的安全目标和安全要求的基础上，明确各种安全管理控制措施的各项评估规程，并编入评估计划；

——对于每种安全管理控制，评估人员都应逐项建立对应的评估规程，明确评估规程相关的目标、步骤；

——评估规程相关步骤的数量会因信息系统、信息系统安全不同等级要求不同，体现了评估过程精确度和强度；

——根据 GB/T 20269-2006 相应等级的安全管理要求，针对特定管理对象进行裁剪时，应对各种增减的措施进行标明，对新增的安全管理控制编制评估操作规程，确保评估的有效性；

——根据安全管理控制的变化，可能会对信息系统中其他管理控制产生影响，对影响评估这些控制措施的效果所需要的评估规程和规程步骤进行必要对调整。

c) 优化评估规程以确保评估质量，包括：

——在评估信息系统的安全管理控制时，为了节省时间、降低评估成本，应充分利用以往的评估结果；

——针对特定系统的安全管理控制措施的评估规程进行检查，在可能或可行的情况下结合或合并一些规程步骤，要充分考虑优化 GB/T 20269-2006 所列各个安全管理控制类别的可能性；

——应给评估人员在实施评估计划的过程中以很大的灵活性，确保评估工作的效率和效果。

d) 收集以往的评估结果，包括：

——根据前次评估的时间、评估的深度和广度，以及负责评估的评估人员或评估小组的能力和独立性等情况，评估人员可通过分析以前的评估结果，获得对信息系统安全管理控制情况的深入了解；

——有关安全评估计划是否使用或接受以往的评估结果，需要与单位相关负责人共同讨论、确认后决定，确保相关结果的采用不与国家或主管部门法律、法规、政策、标准冲突。

e) 形成安全管理评估计划并获准执行，包括：

——在完成评估规程的编制、优化后，形成安全管理评估计划的正式文件，其中要明确执行评估工作的各个时间节点和评估过程各项重要工作完成的时间表；

——安全管理评估计划应与被评估单位的安全目标、安全风险评估以及与评估工作资源配置相关的成本效益要求保持一致。评估计划文件完成编制后，需呈交相关管理部门审批，以确保计划的严肃性。如果属于自评估，评估计划的审批步骤可以省略；

——安全管理评估计划正式成文并得到批准后，评估人员或安全评估小组方可开始安全评估工作；评估人员或评估小组根据已经达成一致意见的重要事件时间表执行安全评估计划。

f） 评估实施过程中采取的调查性访谈、符合性检查、有效性验证以及监测验证，应根据安全管理评估计划有序进行，有关对象、方法和质量控制遵照第5章要求执行。

6.3 处理评估结果

信息系统安全管理评估应按下列要求对评估结果进行处理：

a） 评估结果应按照规定的报告格式记录在案，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） 应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下列判断：

——完全满足：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；

——部分满足：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；

——不满足：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单位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线路图；

——提供信息安全主管领导和相关信息系统支持单位可利用评估结果和有关信息系统残余脆弱性信息来确定本单位信息系统运行和相关资产面临的总体风险。

6.4 建立保障证据

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，并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：

—— 在评估过程中收集证据，以支持被评估机构信息安全决策责任人就信息系统做出采用的基于风险的安全控制行之有效的决定；

—— 收集从各种来源获得的保障证据，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、安全检察人员和机构的信息安全人员等提供的系统安全性评估结果；

—— 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，其中也会反映安全管理体系运行的总体效果；

—— 从不同详细程度和范围的评估中获取信息，包括使用全部评估方法和规程进行认证和认可的全面评估以及其他类型评估（如监管机构评估、自评估、审计和检查）提供有用的信息；

—— 了解并记录评估人员的资格。

7 分等级评估

7.1 第一级：用户自主保护级评估

7.1.1 管理目标和范围评估

依据GB/T 20269-2006中5.1.1.1 a）的描述，评估管理目标和范围是否达到基本的管理目标和范围的要求。

7.1.2 策略和制度评估

本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.1.1.2a）、5.1.1.3a）、5.1.1.4a）的描述，评估总体安全管理策略是否达到基本的安全管理策略的要求，以及制定和发布过程的要求；

b） 依据 GB/T 20269-2006 中 5.1.2.1a）、5.1.2.2a）的描述，评估安全管理规章制度是否达到基本的安全管理制度和操作规程，以及制定和发布过程的要求；

c） 依据 GB/T 20269-2006 中 5.1.3.1a）、5.1.3.2a）的描述，评估策略与制度文档管理是否达到基本的评审和修订，以及指定专人保管的要求。

7.1.3 机构和人员管理评估

本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.2.1.1a）的描述，评估组织机构是否达到配备安全管理人员，以及基本安全管理职能的要求；

b） 依据 GB/T 20269-2006 中 5.2.3.1a）、5.2.3.2a）、5.2.3.3a）、5.2.3.4a）、5.2.3.5a）、5.2.3.6a）的描述，评估人员管理是否达到安全管理人员配备、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、第三方人员管理的要求；

c） 依据 GB/T 20269-2006 中 5.2.4.1a）、5.2.4.2a）的描述，评估组织机构信息安全教育是否达到应知应会要求，以及听取信息安全专家建议的要求。

7.1.4 风险管理评估

本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.3.1.1a）的描述，评估风险管理是否达到基本风险管理，以及基本的风险管理策略的要求；

b） 依据 GB/T 20269-2006 中 5.3.2.1a）、5.3.2.2a）、5.3.2.3a）、5.3.2.4a）的描述，评估风险分析是否达到信息系统的资产统计和分类，威胁的基本分析，脆弱性工具扫描，以及经验的风险评估的要求；

c） 依据 GB/T 20269-2006 中 5.3.3.1a）的描述，评估风险控制是否达到基于安全等级标准选择控制的要求；

d） 依据 GB/T 20269-2006 中 5.3.4.1a）、5.3.4.2a）的描述，评估风险决策是否达到残余风险接受，以及信息系统运行的决定的要求；

e） 依据 GB/T 20269-2006 中 5.3.5.1a）、5.3.5.2a）、5.3.5.3a）、5.3.5.4a）的描述，评估风险评估的管理是否达到对评估机构按资质和信誉选择，对评估机构签署保密协议，对评估信息规定交接手续以及对技术测试应经过授权的要求。

7.1.5 环境和资源管理评估

本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.4.1.1a）、5.4.1.2a）的描述，评估环境安全管理是否达到环境安全的基本要求，以及机房安全管理的基本要求；

b） 依据 GB/T 20269-2006 中 5.4.2.1a）、5.4.2.2a）、5.4.2.3a）、5.4.2.4a）的描述，评估资源管理是否达到一般资产清单编制，资产标识，介质管理基本要求，以及对设备管理申报和审批的要求。

7.1.6 运行和维护管理评估

本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.5.1.1a）、5.5.1.2a）、5.5.1.3a）、5.5.1.4a）、5.5.1.5a）的描述，评估用户管理是否达到用户分类清单编制，系统用户最小授权，普通用户的基本要求，外部用户一般要求，以及临时用户的设置与删除要求；

b） 依据 GB/T 20269-2006 中 5.5.2.1a）、5.5.2.2a）、5.5.2.3a）、5.5.2.4a）、5.5.2.5a）、5.5.2.6a）、5.5.2.7a）的描述，评估运行操作管理是否达到服务器、终端计算机、

便携机操作管理的基本要求，网络及安全设备操作基本要求，业务应用操作程序和权限控制，变更控制的申报和审批，以及信息交换的基本管理的要求；

c） 依据 GB/T 20269-2006 中 5.5.3.1a）、5.5.3.2a）、5.5.3.3a）、5.5.3.4a）的描述，评估运行维护管理是否达到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，以及外部服务方访问的审批控制的要求；

d） 依据 GB/T 20269-2006 中 5.5.4.1a）、5.5.4.2a）、5.5.4.3a）的描述，评估对外包服务的管理是否达到外包服务合同基本要求，外包服务商的基本要求，以及外包服务的监控的要求；

e） 依据 GB/T 20269-2006 中 5.5.5.1a）、5.5.5.2a）、5.5.5.3a）、5.5.5.4a）、5.5.5.5a）、5.5.5.6a）的描述，评估有关安全机制的保障是否达到身份鉴别机制管理基本要求，自主访问控制机制的管理，系统安全管理基本要求，网络安全管理基本要求，应用系统安全管理基本要求，以及病毒防护管理基本要求。

7.1.7 业务连续性管理评估

本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.6.1.1a）的描述，评估业务连续性管理是否达到数据备份的内容和周期的要求；

b） 依据 GB/T 20269-2006 中 5.6.2.1a）、5.6.2.2a）的描述，评估安全事件处理是否达到安全事件内容和划分，以及安全事件报告和处理程序的要求；

c） 依据 GB/T 20269-2006 中 5.6.3.1a）、5.6.3.2a）、5.6.3.3a）的描述，评估应急处理是否达到应急处理的基本要求，应急计划框架，以及应急计划的责任的要求。

7.1.8 监督和检查管理评估

本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.7.1.1a）、5.7.1.2a）、5.7.1.3a）的描述，评估法律符合性是否达到知晓适用的法律并防止违法行为，知识产权保护的基本要求，以及保护机构的重要记录的要求；

b） 依据 GB/T 20269-2006 中 5.7.3.2a）的描述，评估监督控制是否达到接受监管并进行自主保护的要求。

7.1.9 生存周期管理评估

本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.8.1.1a）、5.8.1.2a）、5.8.1.3a）的描述，评估规划和立项管理是否达到系统建设和发展计划，业务应用的需求，以及系统开发立项的基本要求；

b） 依据 GB/T 20269-2006 中 5.8.2.1a）、5.8.2.2a）、5.8.2.3a）、5.8.2.4a）、5.8.2.5a）的描述，评估建设过程管理是否达到对建设项目准备确定项目负责人，对工程项目外包选择具有服务资质的厂商，开发环境与运行环境物理分开，信息安全产品使用分级管理，以及功能和性能测试的要求；

c） 依据 GB/T 20269-2006 中 5.8.3.1a）、5.8.3.2a）的描述，评估系统启用和终止管理是否达到新系统启用的申报和审批，以及终止运行的申报和审批的要求。

7.1.10 实施原则及方法

对第一级信息系统安全管理的评估，应遵从本标准第4章管理评估的基本原则、第5章评估方法和第6章评估实施的要求，其中，第5章对质量控制的具体要求如下：

a） 调查性访谈应按 5.1.4a)的要求进行质量控制；

b） 符合性检查应按 5.2.3a)的要求进行质量控制；

c） 有效性验证应按 5.3.3a)的要求进行质量控制；

d） 监测验证应按 5.4.3a)的要求进行质量控制。

7.2 第二级：系统审计保护级

7.2.1 管理目标和范围评估

依据GB/T 20269-2006中5.1.1.1 b）的描述，在满足第一级的评估要求的基础上，评估管理目标和范围是否达到具有基于操作规程的安全管理的要求。

7.2.2 策略和制度评估

在满足第一级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.1.1.2b）、5.1.1.3b）、5.1.1.4b）的描述，评估总体安全管理策略是否达到较完整的安全管理策略，以及制定和发布过程的要求；

b） 依据 GB/T 20269-2006 中 5.1.2.1b）、5.1.2.2b）的描述，评估安全管理规章制度是否达到较完整的安全管理制度和操作规程，以及制定和发布过程的要求；

c） 依据 GB/T 20269-2006 中 5.1.3.1b）、5.1.3.2b）的描述，评估策略与制度文档管理是否达到较完整的评审和修订，以及借阅审批和登记的要求。

7.2.3 机构和人员管理评估

在满足第一级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.2.1.1b）、5.2.1.3a）的描述，评估组织机构是否达到建立安全职能部门，以及安全管理领导职能的要求；

b） 依据 GB/T 20269-2006 中 5.2.3.1b）、5.2.3.2b）、5.2.3.3b）、5.2.3.4b）、5.2.3.5b）、5.2.3.6a）的描述，评估人员管理是否达到安全管理人员配备、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、第三方人员管理的要求；

c） 依据 GB/T 20269-2006 中 5.2.4.1b）、5.2.4.2a）的描述，评估组织机构信息安全教育是否达到有计划培训，以及听取信息安全专家建议的要求。

7.2.4 风险管理评估

在满足第一级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.3.1.1b）、5.3.1.2a）的描述，评估风险管理是否达到定期风险评估，以及基本的风险管理策略的要求；

b） 依据 GB/T 20269-2006 中 5.3.2.1a）、5.3.2.2b）、5.3.2.3b）、5.3.2.4b）的描述，评估评估风险分析是否达到信息系统的资产统计和分类，威胁列表，脆弱性分析和渗透测试，以及全面的风险评估的要求；

c） 依据 GB/T 20269-2006 中 5.3.3.1b）的描述，评估风险控制是否达到基于风险评估选择控制的要求；

d） 依据 GB/T 20269-2006 中 5.3.4.1b）、5.3.4.2b）的描述，评估风险决策是否达到残余风险监视，以及信息系统运行的决定的要求；

e） 依据 GB/T 20269-2006 中 5.3.5.1b）、5.3.5.2b）、5.3.5.3b）、5.3.5.4b）的描述，评估风险评估的管理是否达到对评估机构在上级认可的范围内选择，对评估机构签署保密协议，对评估信息替换敏感参数以及对技术测试在监督下进行的要求。

7.2.5 环境和资源管理评估

在满足第一级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.4.1.1b）、5.4.1.2b）、5.4.1.3a）的描述，评估环境安全管理是否达到较完整的制度化管理，对机房安全管理加强对来访人员的控制，以及办公环境安全管理基本要求；

b） 依据 GB/T 20269-2006 中 5.4.2.1b）、5.4.2.2b）、5.4.2.3b）、5.4.2.4b）的描述，评估资源管理是否达到详细的资产清单编制，资产分类管理，介质异地存放，以

及对设备系统化管理的要求。

7.2.6 运行和维护管理评估

在满足第一级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.5.1.1b）、5.5.1.2b）、5.5.1.3b）、5.5.1.4b）、5.5.1.5b）的描述，评估用户管理是否达到特权用户管理，系统用户责任到人，普通用户处理敏感信息的要求，外部特定用户要求，以及临时用户审计的要求；

b） 依据 GB/T 20269-2006 中 5.5.2.1b）、5.5.2.2a）、5.5.2.3b）、5.5.2.4b）、5.5.2.5b）、5.5.2.6b）、5.5.2.7b）的描述，评估运行操作管理是否达到服务器日志文件和监控管理，终端计算机操作管理，便携机远程操作的限制，网络及安全设备策略配置及检查，业务应用操作的限制，制度化的变更控制，以及信息交换的规范化管理的要求；

c） 依据 GB/T 20269-2006 中 5.5.3.1b）、5.5.3.2b）、5.5.3.3b）、5.5.3.4b）的描述，评估运行维护管理是否达到系统运行的制度化管理，监视服务器安全性能，送外维修的要求，以及外部服务方访问的制度化管理的要求；

d） 依据 GB/T 20269-2006 中 5.5.4.1a）、5.5.4.2b）、5.5.4.3b）的描述，评估外包服务管理是否达到外包服务合同基本要求，在既定的范围内选择外包服务商，以及外包服务的评估的要求；

e） 依据 GB/T 20269-2006 中 5.5.5.1b）、5.5.5.2b）、5.5.5.3b）、5.5.5.4b）、5.5.5.5b）、5.5.5.6b）、5.5.5.7a）的描述，评估有关安全机制的保障是否达到身份鉴别机制增强要求，自主访问控制审计管理，基于审计的系统安全管理，基于规程的网络安全管理，基于操作规程的应用系统安全管理，基于制度化的病毒防护管理，以及密码算法和密钥管理的要求。

7.2.7 业务连续性管理评估

在满足第一级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.6.1.1b）、5.6.1.2a）的描述，评估备份与恢复管理是否达到备份介质及其恢复的检查要求，以及设备备份的要求；

b） 依据 GB/T 20269-2006 中 5.6.2.1b）、5.6.2.2b）的描述，评估安全事件处理是否达到安全事件处置制度，以及安全隐患报告和防范的要求；

c） 依据 GB/T 20269-2006 中 5.6.3.1b）、5.6.3.2a）、5.6.3.3b）的描述，评估应急处理是否达到应急处理的制度化要求，应急计划框架，以及应急计划的能力的要求。

7.2.8 监督和检查管理评估

在满足第一级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.7.1.1b）、5.7.1.2b）、5.7.1.3a）的描述，评估法律符合性是否达到防止对信息处理设备的滥用，重要应用系统软件的保护，以及保护机构的重要记录的要求；

b） 依据 GB/T 20269-2006 中 5.7.2.1a）、5.7.2.2a）、5.7.2.3a）的描述，评估依从性检查是否达到检查和改进的基本要求，对系统管理员执行安全策略的检查，以及技术依从性检查的要求；

c） 依据 GB/T 20269-2006 中 5.7.3.1a）、5.7.3.2b）的描述，评估审计及监管是否达到审计机构及职能，以及接受监管并进行指导保护的要求；

d） 依据 GB/T 20269-2006 中 5.7.4.1a）、5.7.4.2a）的描述，评估责任认定是否达到明确审计结果的责任，以及按规定要求定期审计的责任的要求。

7.2.9 生存周期管理评估

在满足第一级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.8.1.1b）、5.8.1.2b）、5.8.1.3b）的描述，评估规划和立项管理是否达到信息系统安全策略规划，系统安全的需求，以及可行性论证的要求；

b） 依据 GB/T 20269-2006 中 5.8.2.1b）、5.8.2.2b）、5.8.2.3b）、5.8.2.4a）、5.8.2.5b）的描述，评估建设过程管理是否达到对建设项目制定项目实施计划，对工程项目外包选择可信的具有服务资质的厂商，系统开发文档和软件包的控制，信息安全产品使用分级管理，以及安全性测试的要求；

c） 依据 GB/T 20269-2006 中 5.8.3.1b）、5.8.3.2b）的描述，评估系统启用和终止管理是否达到新系统启用前的试运行，以及终止运行的信息保护的要求。

7.2.10 实施原则及方法

对第二级信息系统安全管理的评估，应遵从本标准第 4 章管理评估的基本原则、第 5 章描评估方法和第 6 章评估实施的要求，其中，第 5 章对质量控制的具体要求如下：

a） 调查性访谈应按 5.1.4b)的要求进行质量控制；

b） 符合性检查应按 5.2.3b)的要求进行质量控制；

c） 有效性验证应按 5.3.3b)的要求进行质量控制；

d） 监测验证应按 5.4.3b)的要求进行质量控制。

7.3 第三级：安全标记保护级

7.3.1 管理目标和范围评估

依据GB/T 20269-2006中5.1.1.1 c）的描述，在满足第二级的评估要求的基础上，评估管理目标和范围是否达到具有完好定义的安全管理的要求。

7.3.2 策略和制度评估

在满足第二级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.1.1.2c）、5.1.1.3c）、5.1.1.4c）的描述，评估总体安全管理策略是否达到体系化的安全管理策略，以及制定和发布过程的要求；

b） 依据 GB/T 20269-2006 中 5.1.2.1c）、5.1.2.2c）的描述，评估安全管理规章制度是否达到体系化的安全管理制度，以及制定和发布过程的要求；

c） 依据 GB/T 20269-2006 中 5.1.3.1c）、5.1.3.2c）的描述，评估策略与制度文档管理是否达到体系化的评审和修订，以及限定借阅范围的要求。

7.3.3 机构和人员管理评估

在满足第二级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.2.1.1c）、5.2.1.2a）、5.2.1.3b）的描述，评估安全管理机构是否达到成立安全领导小组，以及集中安全管理职能的要求；

b） 依据 GB/T 20269-2006 中 5.2.2.1a）、5.2.2.2a）的描述，评估安全机制集中管理机构是否达到集中管理机构人员和职责，以及信息系统安全运行统一管理的要求；

c） 依据 GB/T 20269-2006 中 5.2.3.1c）、5.2.3.2c）、5.2.3.3c）、5.2.3.4c）、5.2.3.5c）、5.2.3.6b）的描述，评估人员管理是否达到安全管理人员配备、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、第三方人员管理的要求；

d） 依据 GB/T 20269-2006 中 5.2.4.1c）、5.2.4.2b）的描述，评估组织机构信息安全教育是否达到针对不同岗位培训，以及对信息安全专家管理的要求。

7.3.4 风险管理评估

在满足第二级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.3.1.1c）、5.3.1.2b）的描述，评估风险管理是否达到规范风险评估，以及风险管理的监督机制的要求；

b） 依据 GB/T 20269-2006 中 5.3.2.1b）、5.3.2.2c）、5.3.2.3c）、5.3.2.4c）的描述，评估风险分析是否达到信息系统的体系特征描述，威胁的详细分析，制度化脆弱性评估，以及建立和维护风险信息库的要求；

c） 依据 GB/T 20269-2006 中 5.3.3.1c）的描述，评估风险控制是否达到基于风险评估形成防护控制系统的要求；

d） 依据 GB/T 20269-2006 中 5.3.4.1c）、5.3.4.2b）的描述，评估风险决策是否达到安全风险再评估，以及信息系统受控运行的要求；

e） 依据 GB/T 20269-2006 中 5.3.5.1b）、5.3.5.2b）、5.3.5.3c）、5.3.5.4c）的描述，评估风险评估的管理是否达到对评估机构在上级认可的范围内选择，对评估机构专人监督检查，对评估信息不得带出指定区域，以及对技术测试由被评估方操作的要求。

7.3.5 环境和资源管理评估

在满足第二级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.4.1.1c）、5.4.1.2c）、5.4.1.3b）的描述，评估环境安全管理是否达到安全区域标记管理，对机房安全管理增强门禁控制手段，以及办公环境安全加强管理的要求；

b） 依据 GB/T 20269-2006 中 5.4.2.1c）、5.4.2.2c）、5.4.2.3c）、5.4.2.4c）的描述，评估资源管理是否达到业务应用系统清单编制，资产体系架构，对介质完整性检查，以及建立资产管理信息登记机制的要求。

7.3.6 运行和维护管理评估

在满足第二级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.5.1.1c）、5.5.1.2c）、5.5.1.3c）、5.5.1.4c）、5.5.1.5c）的描述，评估用户管理是否达到重要业务用户管理，系统用户监督性保护，普通用户重要业务应用，外部用户的限制，以及临时用户限制的要求；

b） 依据 GB/T 20269-2006 中 5.5.2.1c）、5.5.2.2b）、5.5.2.3c）、5.5.2.4c）、5.5.2.5c）、5.5.2.6c）、5.5.2.7c）的描述，评估运行操作管理是否达到服务器配置文件管理，重要部位的终端计算机管理，重要应用的便携机的管理，网络及安全设备安全机制集中管理，业务应用操作的监督，变更控制的一致性管理，以及不同安全区域之间信息传输管理的要求；

c） 依据 GB/T 20269-2006 中 5.5.3.1c）、5.5.3.2c）、5.5.3.3c）、5.5.3.4c）的描述，评估运行维护管理是否达到系统运行的风险控制，监视网络安全性能，可监督的维修过程，以及外部服务方访问的风险评估的要求；

d） 依据 GB/T 20269-2006 中 5.5.4.2c）的描述，评估外包服务管理是否达到外包服务的限制的要求；

e） 依据 GB/T 20269-2006 中 5.5.5.1c）、5.5.5.2c）、5.5.5.3c）、5.5.5.4c）、5.5.5.5c）、5.5.5.6c）、5.5.5.7b）的描述，评估有关安全机制保障是否达到身份鉴别和认证系统的管理维护，强制访问控制的管理，基于标记的系统安全管理，基于标记的网络安全管理，基于标记的应用系统安全管理，基于集中实施的病毒防护管理，以及以密码为基础的安全管理的要求；

f） 依据 GB/T 20269-2006 中 5.5.6.1a）、5.5.6.2a）、5.5.6.3a）、5.5.6.4a）的描述，评估安全机制集中管理是否达到安全机制集中控管基本要求，安全信息集中管理的基本要求，安全机制整合的一般功能，以及安全机制整合的主要工作方式的要求。

7.3.7 业务连续性管理评估

在满足第二级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.6.1.1c）、5.6.1.2b）的描述，评估备份与恢复是否达到备份和恢复措施的强化管理，以及系统热备份与冗余的要求；

b） 依据 GB/T 20269-2006 中 5.6.2.1c）、5.6.2.2c）的描述，评估安全事件处理是否达到安全事件管理程序，以及强化安全事件处理责任的要求；

c） 依据 GB/T 20269-2006 中 5.6.3.1c）、5.6.3.2a）、5.6.3.3c）的描述，评估应急处理是否达到应急处理的检查要求，应急计划框架，以及应急计划的系统化管理的要求。

7.3.8 监督和检查管理评估

在满足第二级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.7.1.1c）、5.7.1.2c）、5.7.1.3a）的描述，评估法律符合性是否达到遵照法规要求使用密码技术，关键业务应用的软件版权，以及保护机构的重要记录的要求；

b） 依据 GB/T 20269-2006 中 5.7.2.1b）、5.7.2.2b）、5.7.2.3b）的描述，评估依从性检查是否达到制度化的检查和改进，全面和系统化的安全策略检查，以及技术依从性检查手段的要求；

c） 依据 GB/T 20269-2006 中 5.7.3.1b）、5.7.3.2c）的描述，评估审计及监管是否达到系统审计过程要求，以及接受监管并进行监督保护的要求；

d） 依据 GB/T 20269-2006 中 5.7.4.1b）、5.7.4.2b）的描述，评估责任认定是否达到明确审计结果中的领导责任，以及审计及监管不得力的责任的要求。

7.3.9 生存周期管理评估

在满足第二级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.8.1.1c）、5.8.1.2c）、5.8.1.3c）的描述，评估规划和立项管理是否达到信息系统安全建设规划，系统规划的需求，以及系统安全性评价的要求；

b） 依据 GB/T 20269-2006 中 5.8.2.1c）、5.8.2.2c）、5.8.2.3c）、5.8.2.4a）、5.8.2.5c）的描述，评估建设过程管理是否达到对建设项目制定监理管理制度，对项目的保护和控制程序，对程序资源库的控制，信息安全产品使用分级管理，以及进一步的验收的要求；

c） 依据 GB/T 20269-2006 中 5.8.3.1c）、5.8.3.2c）的描述，评估系统启用和终止管理是否达到新系统的安全评估，以及终止运行的安全保护的要求。

7.3.10 实施原则及方法

对第三级信息系统安全管理的评估，应遵从本标准第 4 章管理评估的基本原则、第 5 章评估方法和第 6 章评估实施的要求，其中，第 5 章对质量控制的具体要求如下：

a） 调查性访谈应按 5.1.4c)的要求进行质量控制；

b） 符合性检查应按 5.2.3c)的要求进行质量控制；

c） 有效性验证应按 5.3.3c)的要求进行质量控制；

d） 监测验证应按 5.4.3c)的要求进行质量控制。

7.4 第四级：结构化保护级

7.4.1 管理目标和范围评估

依据GB/T 20269-2006中5.1.1.1 d）的描述，在满足第三级的评估要求的基础上，评估管理目标和范围是否达到具有量化控制的安全管理的要求。

7.4.2 策略和制度评估

在满足第三级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.1.1.2d）、5.1.1.3d）、5.1.1.4d）的描述，评估总体安全管理策略是否达到强制保护的安全管理策略，以及制定和发布过程的要求；

b） 依据 GB/T 20269-2006 中 5.1.2.1d）、5.1.2.2d）安全管理规章制度是否达到强制保护的信息安全管理制度，以及制定和发布过程的要求；

c） 依据 GB/T 20269-2006 中 5.1.3.1d）、5.1.3.2d）的描述，评估策略与制度文档管理是否达到强制保护的评审和修订，以及全面严格保管的要求。

7.4.3 机构和人员管理评估

在满足第三级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.2.1.1d）、5.2.1.2a）、5.2.1.3b）的描述，评估安全管理机构是否达到主要负责人出任领导，以及集中的安全管理职能的要求；

b） 依据 GB/T 20269-2006 中 5.2.2.1a）、5.2.2.2b）的描述，评估安全机制集中管理机构是否达到集中管理机构人员和职责，以及关键区域安全运行管理的要求；

c） 依据 GB/T 20269-2006 中 5.2.3.1d）、5.2.3.2d）、5.2.3.3d）、5.2.3.4d）、5.2.3.5d）、5.2.3.6c）的描述，评估人员管理是否达到安全管理人员配备、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、第三方人员管理的要求；

d） 依据 GB/T 20269-2006 中 5.2.4.1d）、5.2.4.2b）的描述，评估组织机构信息安全教育是否达到按人员资质要求培训，以及对信息安全专家管理的要求。

7.4.4 风险管理评估

在满足第三级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.3.1.1d）、5.3.1.2c）的描述，评估风险管理是否达到独立审计的风险管理，以及风险评估的重新启动的要求；

b） 依据 GB/T 20269-2006 中 5.3.2.1b）、5.3.2.2d）、5.3.2.3c）、5.3.2.4c）的描述，评估是否达到信息系统的体系特征描述，使用检测工具捕捉攻击，制度化脆弱性评估，以及建立和维护风险信息库的要求；

c） 风险处理和减缓，同第三级评估要求[见 7.3.4c）]；

d） 基于风险的决策，同第三级评估要求[见 7.3.4d）]；

e） 依据 GB/T 20269-2006 中 5.3.5.1c）、5.3.5.2c）、5.3.5.3c）、5.3.5.4d）的描述，评估风险评估的管理是否达到组织专门机构的评估，对评估机构制定具体办法，对评估信息不得带出指定区域，以及对技术测试过滤测试结果的要求。

7.4.5 环境和资源管理评估

在满足第三级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.4.1.1d）、5.4.1.2d）、5.4.1.3c）的描述，评估环境安全管理是否达到安全区域隔离和监视，对机房安全管理使用视频监控和专职警卫，以及关键部位办公环境的要求；

b） 依据 GB/T 20269-2006 中 5.4.2.1c）、5.4.2.2c）、5.4.2.3d）、5.4.2.4c）的描述，评估资源管理是否达到业务应用系统清单编制，资产体系架构，介质加密存储，以及建立资产管理信息登记机制的要求。

7.4.6 运行和维护管理评估

在满足第三级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.5.1.1d）、5.5.1.2c）、5.5.1.3c）、5.5.1.4c）、5.5.1.5c）的描述，评估用户管理是否达到关键部位用户管理，系统用户监督性保护，普通用户重要业务应用，外部用户的限制，以及临时用户限制的要求；

b） 依据 GB/T 20269-2006 中 5.5.2.1c）、5.5.2.2c）、5.5.2.3d）、5.5.2.4c）、5.5.2.5c）、

5.5.2.6d）、5.5.2.7d）的描述，评估运行操作管理是否达到服务器配置文件管理，重要部位的终端计算机管理，有涉及国家秘密数据的便携机的管理，网络及安全设备安全机制集中管理，业务应用操作的监督，变更控制的安全审计，以及高安全信息向低安全域传输管理的要求；

c） 依据 GB/T 20269-2006 中 5.5.3.1d）、5.5.3.2d）、5.5.3.3d）、5.5.3.4d）的描述，评估运行维护管理是否达到系统运行的安全审计，对关键区域的监视，强制性的维修管理，以及外部服务方访问的强制管理的要求；

d） 外包服务管理，同第三级评估要求[见 7.3.6d）]；

e） 依据 GB/T 20269-2006 中 5.5.5.1d）、5.5.5.2d）、5.5.5.3d）、5.5.5.4d）、5.5.5.5d）、5.5.5.6d）、5.5.5.7b）的描述，评估有关安全机制保障是否达到身份鉴别和认证管理的强制保护，访问控制的监控管理，基于强制的系统安全管理，基于规程的网络安全管理，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，以及以密码为基础的安全管理的要求；

f） 依据 GB/T 20269-2006 中 5.5.6.1b）、5.5.6.2b）、5.5.6.3a）、5.5.6.4a）的描述，评估安全机制集中管理是否达到安全机制分层级联和控管，对关键区域安全信息的集中管理，安全机制整合的一般功能，以及安全机制整合的主要工作方式的要求。

7.4.7 业务连续性管理评估

在满足第三级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.6.1.1d）、5.6.1.2c）的描述，评估备份与恢复管理是否达到关键备份和恢复的操作过程监督，以及系统远地备份的要求；

b） 安全事件处理，同第三级评估要求[见 7.3.7b）]；

c） 依据 GB/T 20269-2006 中 5.6.3.1d）、5.6.3.2a）、5.6.3.3d）的描述，评估应急处理是否达到应急处理的强制保护要求，应急计划框架，以及应急计划监督的要求。

7.4.8 监督和检查管理评估

在满足第三级要求的基础上，本级评估要求如下：

a） 符合法律，同第三级评估要求[见 7.3.8a）]；

b） 依据 GB/T 20269-2006 中 5.7.2.1b）、5.7.2.2c）、5.7.2.3c）的描述，评估依从性检查是否达到制度化的检查和改进，操作过程监督和持续改进，以及技术依从性检查控制的要求；

c） 依据 GB/T 20269-2006 中 5.7.3.1c）、5.7.3.2d）的描述，评估审计及监管是否达到系统审计工具保护要求，以及接受监管并进行强制保护的要求；

d） 依据 GB/T 20269-2006 中 5.7.4.1c）、5.7.4.2c）的描述，评估责任认定是否达到明确审计结果处理的复查责任，以及审计结果处理的跟踪责任的要求。

7.4.9 生存周期管理评估

在满足第三级要求的基础上，本级评估要求如下：

a） 规划和立项管理，同第三级评估要求[见 7.3.9a）]；

b） 依据 GB/T 20269-2006 中 5.8.2.1c）、5.8.2.2d）、5.8.2.3d）、5.8.2.4a）、5.8.2.5c）的描述，评估建设过程管理是否达到对建设项目制定监理管理制度，工程项目外包的限制，系统开发保密性的控制，信息安全产品使用分级管理，以及进一步的验收的要求；

c） 依据 GB/T 20269-2006 中 5.8.3.1d）、5.8.3.2c）的描述，评估系统启用和终止管理是否达到新系统运行的审计跟踪，以及终止运行的安全保护的要求。

7.4.10 实施原则及方法

对第四级信息系统安全管理的评估，应遵从本标准第 4 章管理评估的基本原则、第 5 章评估方法和第 6 章评估实施的要求，其中，第 5 章对质量控制的具体要求如下：

a） 调查性访谈应按 5.1.4d)的要求进行质量控制；

b） 符合性检查应按 5.2.3d)的要求进行质量控制；

c） 有效性验证应按 5.3.3d)的要求进行质量控制；

d） 监测验证应按 5.4.3d)的要求进行质量控制。

7.5 第五级：访问验证保护级

7.5.1 管理目标和范围评估

依据GB/T 20269-2006中5.1.1.1e）的描述，在满足第四级的评估要求的基础上，评估管理目标和范围是否达到具有自我持续改进的安全管理的要求。

7.5.2 策略和制度评估

在满足第四级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.1.1.2e）、5.1.1.3e）、5.1.1.4e）的描述，评估总体安全管理策略是否达到专控保护的信息安全管理策略，以及制定和发布过程的要求；

b） 依据 GB/T 20269-2006 中 5.1.2.1e）、5.1.2.2e）的描述，评估安全管理规章制度是否达到专控保护的信息安全管理制度，以及制定和发布过程的要求；

c） 依据 GB/T 20269-2006 中 5.1.3.1e）、5.1.3.2e）的描述，评估策略与制度文档管理是否达到专控保护的评审和修订，以及专控保护管理的要求。

7.5.3 机构和人员管理评估

在满足第四级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.2.1.1e）、5.2.1.2b）、5.2.1.3b）的描述，评估安全管理机构是否是否达到建立信息安全保密管理部门，以及保密监督管理职能的要求；

b） 依据 GB/T 20269-2006 中 5.2.2.1a）、5.2.2.2c）的描述，评估安全机制集中管理机构是否达到集中管理机构人员和职责，以及核心系统安全运行管理的要求；

c） 依据 GB/T 20269-2006 中 5.2.3.1d）、5.2.3.2e）、5.2.3.3d）、5.2.3.4d）、5.2.3.5d）、5.2.3.6c）的描述，评估人员管理是否达到安全管理人员配备、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、第三方人员管理的要求；

d） 依据 GB/T 20269-2006 中 5.2.4.1e）、5.2.4.2b）的描述，评估组织机构信息安全教育是否达到培养安全意识自觉性，以及对信息安全专家管理的要求。

7.5.4 风险管理评估

在满足第四级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.3.1.1e）、5.3.1.2c）的描述，评估风险管理是否达到全面风险管理，以及风险评估的重新启动的要求；

b） 风险分析和评估，同第四级评估要求[见 7.4.4b）]；

c） 风险处理和减缓，同第四级评估要求[见 7.4.4c）]；

d） 基于风险的决策，同第四级评估要求[见 7.4.4d）]；

e） 风险评估的管理，同第四级评估要求[见 7.4.4e）]。

7.5.5 环境和资源管理评估

在满足第四级要求的基础上，本级评估要求如下：

a） 依据 GB/T 20269-2006 中 5.4.1.1e）、5.4.1.2e）、5.4.1.3c）的描述，评估环境安全管理是否达到安全保障的持续改善，对机房安全管理采取防止电磁泄漏保护，以及关键部位办公环境的要求；

b） 依据 GB/T 20269-2006 中 5.4.2.1c）、5.4.2.2c）、5.4.2.3e）、5.4.2.4c）的描述，

评估资源管理是否达到业务应用系统清单编制，资产体系架构，介质高强度加密存储，以及建立资产管理信息登记机制的要求。

7.5.6 运行和维护管理评估

在满足第四级要求的基础上，本级评估要求如下：

a） 用户管理，同第四级评估要求[见 7.4.5a）]；

b） 依据 GB/T 20269-2006 中 5.5.2.1c）、5.5.2.2c）、5.5.2.3d）、5.5.2.4c）、5.5.2.5c）、5.5.2.6e）、5.5.2.7d）的描述，评估运行操作管理是否达到服务器配置文件管理，重要部位的终端计算机管理，有涉及国家秘密数据的便携机的管理，网络及安全设备安全机制集中管理，业务应用操作的监督，变更的安全评估，以及高安全信息向低安全域传输管理的要求；

c） 依据 GB/T 20269-2006 中 5.5.3.1d）、5.5.3.2e）、5.5.3.3d）、5.5.3.4d）的描述，评估运行维护管理是否达到系统运行的全面安全管理，对核心数据的监视，强制性的维修管理，以及外部服务方访问的强制管理的要求；

d） 外包服务管理，同第四级评估要求[见 7.4.6d）]；

e） 依据 GB/T 20269-2006 中 5.5.5.1e）、5.5.5.2e）、5.5.5.3e）、5.5.5.4e）、5.5.5.5e）、5.5.5.6d）、5.5.5.7b）的描述，评估有关安全机制保障是否达到身份鉴别和认证管理的专项管理，访问控制的专项控制，基于专控的系统安全管理，基于专控的网络安全管理，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，以及以密码为基础的安全管理的要求；

f） 依据 GB/T 20269-2006 中 5.5.6.1b）、5.5.6.2c）、5.5.6.3a）、5.5.6.4a）的描述，评估安全机制集中管理是否达到安全机制分层级联和控管，对核心区域安全信息的集中管理，安全机制整合的一般功能，以及安全机制整合的主要工作方式的要求。

7.5.7 业务连续性管理评估

在满足第四级要求的基础上，本级评估要求如下：

a） 备份与恢复，同第四级评估要求[见 7.4.7a）]；

b） 安全事件处理，同第四级评估要求[见 7.4.7b）]；

c） 依据 GB/T 20269-2006 中 5.6.3.1e）、5.6.3.2a）、5.6.3.3e）的描述，评估应急处理是否达到应急处理管理，应急计划框架，以及应急计划的持续改进的要求。

7.5.8 监督和检查管理评估

在满足第四级要求的基础上，本级评估要求如下：

a） 符合法律，同第四级评估要求[见 7.4.8a）]；

b） 依从性检查，同第四级评估要求[见 7.4.8b）]；

c） 依据 GB/T 20269-2006 中 5.7.3.1c）、5.7.3.2e）的描述，评估审计及监管是否达到系统审计工具保护要求，以及接受监管并进行专控保护的要求；

d） 责任认定，同第四级评估要求[见 7.4.8d）]。

7.5.9 生存周期管理评估

在满足第四级要求的基础上，本级评估要求如下：

a） 规划和立项管理，同第四级评估要求[见 7.4.9a）]；

b） 建设过程管理，同第四级评估要求[见 7.4.9b）]；

c） 系统启用和终止管理，同第四级评估要求[见 7.4.9c）]。

7.5.10 实施原则及方法

对第五级信息系统安全管理的评估，应遵从本标准第 4 章管理评估的基本原则、第 5 章评估方法和第 6 章评估实施的要求，其中，第 5 章对质量控制的具体要求如下：

a） 调查性访谈应按 5.1.4e)的要求进行质量控制；
b） 符合性检查应按 5.2.3e)的要求进行质量控制；
c） 有效性验证应按 5.3.3e)的要求进行质量控制；
d） 监测验证应按 5.4.3e)的要求进行质量控制。

附 录 A
（资料性附录）
安全管理评估内容

根据 GB/T 20269-2006 第 5 章和第 6 章关于安全管理要求的规定，信息系统安全管理内容与分等级评估要求的对应关系见表 A.1。在该表中将安全管理要素的结构分为三个层次，为便于说明将第一层称为类，第二层称为族，第三层为具体的安全管理要素。所有章节标识与 GB/T 20269-2006 章节对应。

表 A.1 安全管理内容与分等级评估要求的对应关系

类	族	评估项	对应等级条款				
			一级	二级	三级	四级	五级
5.1 策略和制度	5.1.1 信息安全管理策略	5.1.1.1 安全管理目标与范围	a）	b）	c）	d）	e）
		5.1.1.2 总体安全管理策略	a）	b）	c）	d）	e）
		5.1.1.3 安全管理策略的制定	a）	b）	c）	d）	e）
		5.1.1.4 安全管理策略的发布	a）	b）	c）	d）	e）
	5.1.2 安全管理规章制度	5.1.2.1 安全管理规章制度内容	a）	b）	c）	d）	e）
		5.1.2.2 安全管理规章制度的制定	a）	b）	c）	d）	e）
	5.1.3 策略与制度文档管理	5.1.3.1 策略与制度文档的评审和修订	a）	b）	c）	d）	e）
		5.1.3.2 策略与制度文档的保管	a）	b）	c）	d）	e）
5.2 机构和人员管理	5.2.1 安全管理机构	5.2.1.1 建立安全管理机构	a）	b）	c）	d）	e）
		5.2.1.2 信息安全领导小组			a）	a）	b）
		5.2.1.3 信息安全职能部门		a）	b）	b）	b）
	5.2.2 安全机制集中管理机构	5.2.2.1 设置集中管理机构			a）	a）	a）
		5.2.2.2 集中管理机构职能			a）	b）	c）
	5.2.3 人员管理	5.2.3.1 安全管理人员配备	a）	b）	c）	d）	d）
		5.2.3.2 关键岗位人员管理	a）	b）	c）	d）	e）
		5.2.3.3 人员录用管理	a）	b）	c）	d）	d）
		5.2.3.4 人员离岗	a）	b）	c）	d）	d）
		5.2.3.5 人员考核与审查	a）	b）	c）	d）	d）
		5.2.3.6 第三方人员管理	a）	b）	c）	c）	c）
	5.2.4 教育和培训	5.2.4.1 信息安全教育	a）	b）	c）	d）	e）
		5.2.4.2 信息安全专家	a）	a）	b）	b）	b）
5.3 风险管理	5.3.1 风险管理要求和策略	5.3.1.1 风险管理要求	a）	b）	c）	d）	e）
		5.3.1.2 风险管理策略	a）	a）	b）	c）	c）
	5.3.2 风险分析和评估	5.3.2.1 资产识别和分析	a）	a）	b）	b）	b）
		5.3.2.2 威胁识别和分析	a）	b）	c）	d）	d）
		5.3.2.3 脆弱性识别和分析	a）	b）	c）	c）	c）
		5.3.2.4 风险分析和评估要求	a）	b）	c）	c）	c）
	5.3.3 风险控制	5.3.3.1 选择和实施风险控制措施	a）	b）	c）	c）	c）
	5.3.4 基于风险的决策	5.3.4.1 安全确认	a）	b）	c）	c）	c）
		5.3.4.2 信息系统运行的决策	a）	a）	b）	b）	b）

表 A.1 （续）

类	族	评估项	对应等级条款				
			一级	二级	三级	四级	五级

类	族	评估项	对应等级条款				
			一级	二级	三级	四级	五级
	5.3.5 评估安全管理	5.3.5.1 评估机构的选择	a）	b）	b）	c）	c）
		5.3.5.2 评估机构的保密要求	a）	a）	b）	c）	c）
		5.3.5.3 评估信息的管理	a）	b）	c）	c）	c）
		5.3.5.4 技术测试过程管理	a）	b）	c）	d）	d）
5.4 环境和资源管理	5.4.1 环境安全管理	5.4.1.1 环境安全管理要求	a）	b）	c）	d）	e）
		5.4.1.2 机房安全管理要求	a）	b）	c）	d）	e）
		5.4.1.3 办公环境安全管理要求		a）	b）	c）	c）
	5.4.2 资源管理	5.4.2.1 资产清单管理	a）	b）	c）	c）	c）
		5.4.2.2 资产的分类与标识要求	a）	b）	c）	c）	c）
		5.4.2.3 介质管理	a）	b）	c）	d）	e）
		5.4.2.4 设备管理要求	a）	b）	c）	c）	c）
5.5 运行和维护管理	5.5.1 用户管理	5.5.1.1 用户分类管理	a）	b）	c）	d）	d）
		5.5.1.2 系统用户要求	a）	b）	c）	c）	c）
		5.5.1.3 普通用户要求	a）	b）	c）	c）	c）
		5.5.1.4 机构外部用户要求	a）	b）	c）	c）	c）
		5.5.1.5 临时用户要求	a）	b）	c）	c）	c）
	5.5.2 运行操作管理	5.5.2.1 服务器操作管理	a）	b）	c）	c）	c）
		5.5.2.2 终端计算机操作管理	a）	a）	b）	c）	c）
		5.5.2.3 便携机操作管理	a）	b）	c）	d）	d）
		5.5.2.4 网络及安全设备操作管理	a）	b）	c）	c）	c）
		5.5.2.5 业务应用操作管理	a）	b）	c）	c）	c）
		5.5.2.6 变更控制和重用管理	a）	b）	c）	d）	e）
		5.5.2.7 信息交换管理	a）	b）	c）	d）	d）
	5.5.3 运行维护管理	5.5.3.1 日常运行安全管理	a）	b）	c）	d）	e）
		5.5.3.2 运行状况监控	a）	b）	c）	d）	e）
		5.5.3.3 软件硬件维护管理	a）	b）	c）	d）	d）
		5.5.3.4 外部服务方访问管理	a）	b）	c）	d）	d）
	5.5.4 外包服务管理	5.5.4.1 外包服务合同	a）	a）			
		5.5.4.2 外包服务商	a）	b）	c）	c）	c）
		5.5.4.3 外包服务的运行管理	a）	b）			
	5.5.5 有关安全机制保障	5.5.5.1 身份鉴别机制管理要求	a）	b）	c）	d）	e）
		5.5.5.2 访问控制机制管理要求	a）	b）	c）	d）	e）
		5.5.5.3 系统安全管理要求	a）	b）	c）	d）	e）
		5.5.5.4 网络安全管理要求	a）	b）	c）	d）	e）
		5.5.5.5 应用系统安全管理要求	a）	b）	c）	d）	e）
		5.5.5.6 病毒防护管理要求	a）	b）	c）	d）	d）
		5.5.5.7 密码管理要求		a）	b）	b）	b）
	5.5.6 安全集中管理	5.5.6.1 安全机制集中控管			a）	b）	b）
		5.5.6.2 安全信息集中管理			a）	b）	c）
		5.5.6.3 安全机制整合要求			a）	a）	a）
		5.5.6.4 安全机制整合的处理方式			a）	a）	a）
5.6 业务连续性管理	5.6.1 备份与恢复	5.6.1.1 数据备份和恢复	a）	b）	c）	d）	d）
		5.6.1.2 设备和系统备份与冗余		a）	b）	c）	c）
	5.6.2 安全事件处理	5.6.2.1 安全事件划分	a）	b）	c）	c）	c）
		5.6.2.2 安全事件报告和响应	a）	b）	c）	c）	c）
	5.6.3 应急处理	5.6.3.1 应急处理和灾难恢复	a）	b）	c）	d）	e）
		5.6.3.2 应急计划	a）	a）	a）	a）	a）
		5.6.3.3 应急计划的实施保障	a）	b）	c）	d）	e）

表 A.1 （续）

类	族	评估项	对应等级条款				
			一级	二级	三级	四级	五级
5.7 监督和检查管理	5.7.1 符合法律要求	5.7.1.1 知晓适用的法律	a）	b）	c）	c）	c）
		5.7.1.2 知识产权管理	a）	b）	c）	c）	c）
		5.7.1.3 保护证据记录	a）	a）	a）	a）	a）
	5.7.2 依从性检查	5.7.2.1 检查和改进		a）	b）	b）	b）
		5.7.2.2 安全策略依从性检查		a）	b）	c）	c）
		5.7.2.3 技术依从性检查		a）	b）	c）	c）
	5.7.3 审计及监管控制	5.7.3.1 审计控制		a）	b）	c）	c）
		5.7.3.2 监管控制	a）	b）	c）	d）	e）
	5.7.4 责任认定	5.7.4.1 审计结果中责任的认定	a）	b）	b）	c）	c）
		5.7.4.2 审计及监管者责任的认定	a）	b）	b）	c）	c）
5.8 生存周期管理	5.8.1 规划和立项管理	5.8.1.1 系统规划要求	a）	b）	c）	c）	c）
		5.8.1.2 系统需求的提出	a）	b）	c）	c）	c）
		5.8.1.3 系统开发的立项	a）	b）	c）	c）	c）
	5.8.2 建设过程管理	5.8.2.1 建设项目准备	a）	b）	c）	c）	c）
		5.8.2.2 工程项目外包要求	a）	b）	c）	d）	d）
		5.8.2.3 自行开发环境控制	a）	b）	c）	d）	d）
		5.8.2.4 安全产品使用要求	a）	a）	a）	a）	a）
		5.8.2.5 建设项目测试验收	a）	b）	c）	c）	c）
	5.8.3 系统启用和终止管理	5.8.3.1 新系统启用管理	a）	b）	c）	d）	d）
		5.8.3.2 终止运行管理	a）	b）	c）	c）	c）
注：表中“对应等级条款”一级、二级、三级、四级、五级列表项内的 a）、b）、c）、d）、e）表示 “管理要素”列表项内对应行的标题下的 a）、b）、c）、d）、e）列项内容。							

参　考　文　献

[1] GB/T 19715.1-2005　信息技术 信息技术安全管理指南 第1部分：信息技术安全概念和模型

[2] GB/T 19715.2-2005　信息技术 信息技术安全管理指南 第2部分：管理和规划信息技术安全

[3] GB/T 19716-2005 信息技术 信息安全管理实用规则