信息安全技术
信息系统安全等级保护基本要求

Information Security Technology-

Basic Requirements for Classified

Security Protection of Information System

（试用稿_修订版 V1.1）

目 录

信息安全技术

信息系统安全等级保护基本要求

1　范围

本文件规定了信息系统安全等级保护的基本要求，包括基本技术要求和基本管理要求，适用于不同安全等级的信息系统的安全保护。

2　规范性引用文件

下列文件中的条款通过在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使用这些文件的最新版本。凡是不注明日期的引用文件，其最新版本适用于本标准。

GB17859-1999《计算机信息系统安全保护等级划分准则》

GB/T XXXA-XXX《信息系统安全保护等级定级指南》

3　术语和定义

GB 17859-1999 和 GB/T XXX-XXXX《信息系统安全保护等级定级指南》确立的以及下列术语和定义适用于本标准。

3.1

安全威胁 security threat

可能对信息系统造成损害的不希望的事故或事件的潜在原因。

3.2

安全目标 security objective

意在对抗确定的威胁，使信息系统达到特定安全等级的安全要求的简要陈述。

3.3

安全保护能力 security protective ability

系统能够预防威胁并能够检测到威胁存在的能力和在遭到威胁破坏后，系统能够恢复之前各种状态（包括数据的各种属性、业务运行状态等）的能力。

4　标记说明

在第 6 章“安全目标”中对安全目标使用了标记，安全目标的标记包括三部分：标识、等级和序号，如下表所示。

安全目标标记	01-1

标识	安全目标（0）
等级	1
序号	1

O 为安全目标标识；等级代表该目标对应的信息系统安全等级；序号是指该目标在该等级安全目标列表中的顺序编号。

在第 5 章“基本概念”和后续的章节中对安全基本要求使用了标记，标记如下表所示。

安全标记	S1	A2	G3
关注方面	业务信息安全性	业务服务保证性	通用安全保护
安全等级	1	2	3

安全的关注方面包括业务信息安全性、业务服务保证性和通用安全保护等三个方面。其中业务信息安全性（简记为 S）关注的是保护业务信息在存储、传输、处理过程中不被泄漏、破坏或未授权的修改；业务服务保证性（简记为 A）关注的是保护系统连续正常的运行，免受对系统破坏或未授权的修改而导致系统不可用；通用安全保护（简记为 G）既关注保护业务信息的安全，同时也关注保护系统的可用。

标记中的等级对应于其所适用的信息系统的安全等级。

在附录 B“威胁描述”对安全威胁使用了标记，安全威胁的标记包括三部分：标识、等级和序号，如下表所示。

安全威胁标记	T1-1
标识	安全威胁（T）
等级	1
序号	1

T 为安全威胁标识；等级是指需要对抗该威胁的信息系统安全等级；序号是指该威胁在该类威胁列表中的顺序编号。

5　基本概念

5.1.　信息系统概述

信息系统是指基于计算机和计算机网络，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

信息系统是由软件、硬件、操作人员及系统所承载的信息等几部分组成。软件包括计算机系统软件、网络软件和应用软件等，这些软件对系统硬件进行管理并为按需求进行信息处理等应用提供必要的支持；硬件包括计算机硬件、网络硬件及其配套硬件设备等，它们是信息的载体，信息系统的基础；人是信息系统最终使用者，也是在信息系统整个生命周期中，如规划设计、建设实施、运行维护等过程中的参与者和管理者，人的因素是保证信息系统正常工作不可缺少的重要部分。

信息系统面临多种威胁，可能面临自然、环境和技术故障等非人为因素的威胁，也可能面临人员失误和恶意攻击等人为因素的威胁，威胁可能引起不希望的安全事件，对信息系统的业务信息安全性或业务服务保证性造成损害。不同的信息系统所承载的业务和处理的数据重要程度不同、不同的信息系统所处在位置和环境有所不同，对信息系统的保护要求也会不同。

5.2. 信息系统的五个安全等级

信息系统划分为以下五个安全等级：

第一级为自主保护级，主要对象为一般的信息系统，其受到破坏后，会对公民、法人和其他组织的权益有一定影响，但不危害国家安全、社会秩序和公共利益。

第二级为指导保护级，主要对象为一般的信息系统，其受到破坏后，会对社会秩序和公共利益造成轻微损害，但不损害国家安全。

第三级为监督保护级，主要对象为涉及国家安全、社会秩序和公共利益的重要信息系统，其受到破坏后，会对国家安全、社会秩序和公共利益造成损害。

第四级为强制保护级，主要对象为涉及国家安全、社会秩序和公共利益的重要信息系统，其受到破坏后，会对国家安全、社会秩序和公共利益造成严重损害。

第五级为专控保护级，主要对象为涉及国家安全、社会秩序和公共利益的重要信息系统的核心子系统，其受到破坏后，会对国家安全、社会秩序和公共利益造成特别严重损害。

一个组织机构内可能运行一个或多个信息系统，这些信息系统完成不同使命、承载不同业务、处理不同数据，不同的信息系统可能具有相同的安全等级或不同的安全等级；一个组织机构拥有的、由相同安全等级或不同安全等级的多个信息系统互联构成了组织机构等级化的大型信息系统。

5.3. 不同安全等级的安全保护能力

不同级别的信息系统应具备不同的安全保护能力。不同级别的信息系统应具备的基本安全保护能力要求如下：

1 级安全保护能力：应具有能够对抗来自个人的、拥有很少资源（如利用公开可获取的工具等）的威胁源发起的恶意攻击、一般的自然灾难（灾难发生的强度弱、持续时间很短、系统局部范围等）以及其他相当危害程度威胁的能力，并在威胁发生后，能够恢复部分功能。

2 级安全保护能力：应具有能够对抗来自小型组织的（如自发的三两人组成的黑客组织）、拥有少量资源（如个别人员能力、公开可获或特定开发的工具等）的威胁源发起的恶意攻击、一般的自然灾难（灾难发生的强度一般、持续时间短、覆盖范围小（局部性）等）

以及其他相当危害程度（无意失误、设备故障等）威胁的能力，并在威胁发生后，能够在一段时间内恢复部分功能。

3 级安全保护能力：应具有能够对抗来自大型的、有组织的团体（如一个商业情报组织或犯罪组织等），拥有较为丰富资源（包括人员能力、计算能力等）的威胁源发起的恶意攻击、较为严重的自然灾难（灾难发生的强度较大、持续时间较长、覆盖范围较广（地区性）等）以及其他相当危害程度（内部人员的恶意威胁、设备的较严重故障等）威胁的能力，并在威胁发生后，能够较快恢复绝大部分功能。

4 级安全保护能力：应具有能够对抗来自敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难（灾难发生的强度大、持续时间长、覆盖范围广（多地区性）等）以及其他相当危害程度（内部人员的恶意威胁、设备的严重故障等）威胁的能力，并在威胁发生后，能够迅速恢复所有功能。

上述对不同等级的信息系统的基本安全保护能力要求是一种整体和抽象的描述，本文件的其余大部分内容是对基本安全保护能力的具体化。每一级别的信息系统所应该具有的基本安全保护能力将通过体现基本安全保护能力的安全目标的提出以及实现安全目标的具体技术要求和管理要求的描述得到具体化。

5.4. 技术要求和管理要求

信息系统的安全等级保护是依据信息系统的安全等级情况保证它们具有相应等级的基本安全保护能力，不同安全等级的信息系统要求具有不同的安全保护能力。

实现基本安全保护能力将通过选用合适的安全措施或安全控制来保证，在本文件中可以使用的安全措施或安全控制表现为安全基本要求，依据实现方式的不同，信息系统等级保护的安全基本要求分为技术要求和管理要求两大类。

技术类安全要求通常与信息系统提供的技术安全机制有关，主要是通过在信息系统中部署软硬件并正确的配置其安全功能来实现；管理类安全要求通常与信息系统中各种角色参与的活动有关，主要是通过控制各种角色的活动，从政策、制度、规范、流程以及记录等方面做出规定来实现。

基本技术要求从物理安全、网络安全、主机系统安全、应用安全和数据安全几个层面提出安全要求；基本管理要求从安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理几个方面提出安全要求。

在本文件中，物理安全是指包括支撑设施、硬件设备、存储介质等在内的信息系统相关支持环境的安全；网络安全是指包括路由器、交换机、通信线路等在内的信息系统网络环境

的安全；主机系统安全是指包括服务器、终端/工作站以及安全设备/系统在内的计算机设备在操作系统及数据库系统层面的安全；应用安全是指支持业务处理的业务应用系统的安全；数据安全是指信息系统中数据的采集、传输、处理和存储过程中的安全。此外，在本文件的数据安全部分将包括在信息系统遭到破坏时能够恢复数据以及业务系统运行的内容。

技术要求与管理要求是确保信息系统安全不可分割的两个部分，两者之间既互相独立，又互相关联，在一些情况下，技术和管理能够发挥它们各自的作用；在另一些情况下，需要同时使用技术和管理两种手段，实现安全控制或更强的安全控制；大多数情况下，技术和管理要求互相提供支撑以确保各自功能的正确实现。

5.5. 技术要求的三种类型

技术类安全要求提出了信息系统应提供的技术安全机制，这些安全机制将通过在信息系统中部署软硬件并正确的配置其安全功能来实现。根据安全机制的保护侧重点，技术类安全要求又进一步细分为业务信息安全类（简记为 S）、业务服务保证类（简记为 A 类）和通用安全保护类（简记为 G 类）三类。

业务信息安全类（S 类）安全要求关注的是保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权的修改；业务服务保证类（A 类）安全要求关注的是保护系统连续正常的运行，免受对系统的未授权修改、破坏而导致系统不可用；通用安全保护类（G 类）安全要求是没有明显的侧重，既关注保护业务信息的安全性，同时也关注保护系统的连续可用性。

5.6. 基本要求的选择

信息系统由于承载的业务不同，对其的安全关注点会有所不同，有的更关注数据的安全性，即更关注对盗窃、搭线窃听、假冒用户等可能导致信息泄密、非法篡改等威胁的对抗；有的更关注业务的连续性，即更关注保证系统连续正常的运行，免受对系统未授权的修改、破坏而导致系统不可用引起业务中断。

不同安全等级的信息系统，其对业务信息的安全性要求和业务服务的连续性要求是有差异的；即使相同安全等级的信息系统，其对业务信息的安全性要求和业务服务的连续性要求也有差异。信息系统的安全等级由各个业务子系统的业务信息安全性等级和业务服务保证性等级较高者决定（参见《信息系统安全保护等级定级指南》），因此，对某一个定级后的信息系统的保护要求可以有多种组合。

不同安全等级的信息系统可以选择的保护要求组合如下表所示：

表 1：各等级信息系统保护要求组合

安全等级	信息系统保护要求的组合
第一级	S1A1G1
第二级	S1A2G2，S2A2G2，S2A1G2
第三级	S1A3G3，S2A3G3，S3A3G3，S3A2G3，S3A1G3
第四级	S1A4G4，S2A4G4，S3A4G4，S4A4G4，S4A3G4，S4A2G4，S4A1G4

本文件的每一个安全等级的基本要求按照业务信息安全性等级和业务服务保证性等级相同的情况组织，也就是每一个安全等级的基本要求针对 S1A1G1、S2A2G2、S3A3G3 和 S4A4G4 情况给出。

对基本要求进行选择的过程如下：

首先，基本要求的选择由信息系统的安全等级确定，基本要求包括技术要求和管理要求。一级系统应该选择第一级的基本要求，二级系统应该选择第二级的基本要求，三级系统应该选择第三级的基本要求，四级系统应该选择第四级的基本要求。

其次，可以根据信息系统保护要求的组合对技术要求进行调整。对业务信息安全性等级高于业务服务保证性等级的系统，业务服务保证类（A 类）技术要求可以根据业务服务保证性等级选择相应等级的业务服务保证类（A 类）技术要求；对业务服务保证性等级高于业务信息安全性等级的系统，业务信息安全类（S 类）技术要求可以根据业务信息安全性等级选择相应等级的业务信息安全类（S 类）技术要求。

最后，由于各种原因对基本要求项有调整需求的，应针对需要调整的基本要求项逐项进行风险分析，在保证不降低整体安全保护强度的前提下，对基本要求项进行调整，并形成书面的调整理由进行说明。

对于涉密的信息系统，在确定安全等级后，除应按照本文件规定的相应安全等级的基本要求进行保护外，还应按照国家保密工作部门和国家密码管理部门的相关规定进行要求和保护。

6　安全目标

6.1.　第1级安全目标

第一级信息系统应实现以下目标。

6.1.1.　技术目标

O1-1.　应具有防雷击的能力

O1-2. 应具有防水和防潮的能力

O1-3. 应具有灭火的能力

O1-4. 应具有温湿度检测和控制的能力

O1-5. 应具有防止电压波动的能力

O1-6. 应具有对传输和存储数据进行完整性检测的能力

O1-7. 应具有系统软件、应用软件容错的能力

O1-8. 应具有合理使用和控制系统资源的能力

O1-9. 应具有设计合理、安全网络结构的能力

O1-10. 应具有控制机房进出的能力

O1-11. 应具有防止设备、介质等丢失的能力

O1-12. 应具有控制接触重要设备、介质的能力

O1-13. 应具有发现网络协议、操作系统、应用系统等重要漏洞并及时修补的能力

O1-14. 应具有对网络、系统和应用的访问进行控制的能力

O1-15. 应具有对数据、文件或其他资源的访问进行控制的能力

O1-16. 应具有对用户进行标识和鉴别的能力

O1-17. 应具有保证鉴别数据传输和存储保密性的能力

O1-18. 应具有对恶意代码的检测、阻止和清除能力

O1-19. 应具有重要数据恢复的能力

6.1.2. 管理目标

O1-20. 应确保配备了足够数量的管理人员，支持信息系统的管理工作

O1-21. 应确保建立了基本的安全管理制度，并保证安全管理制度的有效性

O1-22. 应确保对信息系统进行合理定级

O1-23. 应确保能控制信息安全相关事件的授权与审批

O1-24. 应确保建立恰当可靠的联络渠道，以便安全事件发生时能得到支持

O1-25. 应确保对人员的行为进行控制

O1-26. 应确保安全产品的可信度和产品质量

O1-27. 应确保自行开发过程和工程实施过程中的安全

O1-28. 应确保能顺利地接管和维护信息系统

O1-29. 应确保安全工程的实施质量和安全功能的准确实现

O1-30. 应确保机房具有良好的运行环境

O1-31. 应确保对信息资产进行安全管理

O1-32. 应确保对各种软硬件设备的选型、采购、发放、使用和保管等过程进行控制

O1-33. 应确保对网络、操作系统、数据库管理系统和应用系统进行安全管理

O1-34. 应确保用户具有鉴别信息使用的安全意识

O1-35. 应确保定期地对通信线路进行检查和维护

O1-36. 应确保硬件设备、存储介质存放环境安全，并对其的使用进行控制和保护

O1-37. 应确保对支撑设施、硬件设备、存储介质进行日常维护和管理

O1-38. 应确保系统中使用的硬件、软件产品的质量

O1-39. 应确保各类人员具有与其岗位相适应的技术能力

O1-40. 应确保对各类人员进行相关的技术培训

O1-41. 应确保提供的足够的使用手册、维护指南等资料

O1-42. 应确保内部人员具有安全方面的常识和意识

O1-43. 应确保对信息安全事件进行报告和处置

6.2. 第2级安全目标

第二级信息系统应实现以下目标。

6.2.1. 技术目标

O2-1. 应具有抵抗一般强度地震、台风等自然灾难造成破坏的能力

O2-2. 应具有防止雷击事件导致重要设备被破坏的能力

O2-3. 应具有防水和防潮的能力

O2-4. 应具有灭火的能力

O2-5. 应具有检测火灾和报警的能力

O2-6. 应具有温湿度自动检测和控制的能力

O2-7. 应具有防止电压波动的能力

O2-8. 应具有对抗短时间断电的能力

O2-9. 应具有防止静电导致重要设备被破坏的能力

O2-10. 具有基本的抗电磁干扰能力

O2-11. 应具有对传输和存储数据进行完整性检测的能力

O2-12. 应具有对硬件故障产品进行替换的能力

O2-13. 应具有系统软件、应用软件容错的能力

O2-14. 应具有软件故障分析的能力

O2-15. 应具有合理使用和控制系统资源的能力

O2-16. 应具有记录用户操作行为的能力

O2-17. 应具有对用户的误操作行为进行检测和报警的能力

O2-18. 应具有控制机房进出的能力

O2-19. 应具有防止设备、介质等丢失的能力

O2-20. 应具有控制机房内人员活动的能力

O2-21. 应具有控制接触重要设备、介质的能力

O2-22. 应具有对传输和存储中的信息进行保密性保护的能力

O2-23. 应具有对通信线路进行物理保护的能力

O2-24. 应具有限制网络、操作系统和应用系统资源使用的能力

O2-25. 应具有能够检测对网络的各种攻击并记录其活动的能力

O2-26. 应具有发现所有已知漏洞并及时修补的能力

O2-27. 应具有对网络、系统和应用的访问进行控制的能力

O2-28. 应具有对数据、文件或其他资源的访问进行控制的能力

O2-29. 应具有对资源访问的行为进行记录的能力

O2-30. 应具有对用户进行唯一标识的能力

O2-31. 应具有对用户产生复杂鉴别信息并进行鉴别的能力

O2-32. 应具有对恶意代码的检测、阻止和清除能力

O2-33. 应具有防止恶意代码在网络中扩散的能力

O2-34. 应具有对恶意代码库和搜索引擎及时更新的能力

O2-35. 应具有保证鉴别数据传输和存储保密性的能力

O2-36. 应具有对存储介质中的残余信息进行删除的能力

O2-37. 应具有非活动状态一段时间后自动切断连接的能力

O2-38. 应具有网络边界完整性检测能力

O2-39. 应具有重要数据恢复的能力

6.2.2. 管理目标

O2-40. 应确保建立了安全职能部门，配备了安全管理人员，支持信息安全管理工作

O2-41. 应确保配备了足够数量的管理人员，对系统进行运行维护

O2-42. 应确保对主要的管理活动进行了制度化管理

O2-43. 应确保建立并不断完善、健全安全管理制度

O2-44. 应确保能协调信息安全工作在各功能部门的实施

O2-45. 应确保能控制信息安全相关事件的授权与审批

O2-46. 应确保建立恰当可靠的联络渠道，以便安全事件发生时能得到支持

O2-47. 应确保对人员的行为进行控制

O2-48. 应确保对人员的管理活动进行了指导

O2-49. 应确保安全策略的正确性和安全措施的合理性

O2-50. 应确保对信息系统进行合理定级

O2-51. 应确保安全产品的可信度和产品质量

O2-52. 应确保自行开发过程和工程实施过程中的安全

O2-53. 应确保能顺利地接管和维护信息系统

O2-54. 应确保安全工程的实施质量和安全功能的准确实现

O2-55. 应确保机房具有良好的运行环境

O2-56. 应确保对信息资产进行标识管理

O2-57. 应确保对各种软硬件设备的选型、采购、发放、使用和保管等过程进行控制

O2-58. 应确保各种网络设备、服务器正确使用和维护

O2-59. 应确保对网络、操作系统、数据库管理系统和应用系统进行安全管理

O2-60. 应确保用户具有鉴别信息使用的安全意识

O2-61. 应确保定期地对通信线路进行检查和维护

O2-62. 应确保硬件设备、存储介质存放环境安全，并对其的使用进行控制和保护

O2-63. 应确保对支撑设施、硬件设备、存储介质进行日常维护和管理

O2-64. 应确保系统中使用的硬件、软件产品的质量

O2-65. 应确保各类人员具有与其岗位相适应的技术能力

O2-66. 应确保对各类人员进行相关的技术培训

O2-67. 应确保提供的足够的使用手册、维护指南等资料

O2-68. 应确保内部人员具有安全方面的常识和意识

O2-69. 应确保具有设计合理、安全网络结构的能力

O2-70. 应确保密码算法和密钥的使用符合国家有关法律、法规的规定

O2-71. 应确保任何变更控制和设备重用要申报和审批，并对其实行制度化的管理

O2-72. 应确保在事件发生后能采取积极、有效的应急策略和措施

O2-73. 应确保信息安全事件实行分等级响应、处置

6.3. 第3级安全目标

第三级信息系统应实现以下目标。

6.3.1. 技术目标

O3-1. 应具有对抗中等强度地震、台风等自然灾难造成破坏的能力

O3-2. 应具有防止雷击事件导致大面积设备被破坏的能力

O3-3. 应具有防水和防潮的能力

O3-4. 应具有对水患检测和报警的能力

O3-5. 应具有自动灭火的能力

O3-6. 应具有检测火灾和报警的能力

O3-7. 应具有防止火灾蔓延的能力

O3-8. 应具有温湿度自动检测和控制的能力

O3-9. 应具有防止电压波动的能力

O3-10. 应具有对抗较长时间断电的能力

O3-11. 应具有防止静电导致大面积设备被破坏的能力

O3-12. 应具有对重要设备和介质进行电磁屏蔽的能力

O3-13. 应具有防止强电磁场、强震动源和强噪声源等污染影响系统正常运行的能力

O3-14. 应具有监测通信线路传输状况的能力

O3-15. 应具有及时恢复正常通信的能力

O3-16. 应具有对传输和存储数据进行完整性检测和纠错的能力

O3-17. 应具有系统软件、应用软件容错的能力

O3-18. 应具有软件故障分析的能力

O3-19. 应具有软件状态监测和报警的能力

O3-20. 应具有自动保护当前工作状态的能力

O3-21. 应具有合理使用和控制系统资源的能力

O3-22. 应具有按优先级自动分配系统资源的能力

O3-23. 应具有对软件缺陷进行检查的能力

O3-24. 应具有记录用户操作行为和分析记录结果的能力

O3-25. 应具有对用户的误操作行为进行检测、报警和恢复的能力

O3-26. 应具有严格控制机房进出的能力

O3-27. 应具有防止设备、介质等丢失的能力

O3-28. 应具有严格控制机房内人员活动的能力

O3-29. 应具有实时监控机房内部活动的能力

O3-30. 应具有对物理入侵事件进行报警的能力

O3-31. 应具有控制接触重要设备、介质的能力

O3-32. 应具有对通信线路进行物理保护的能力

O3-33. 应具有使重要通信线路及时恢复的能力

O3-34. 应具有限制网络、操作系统和应用系统资源使用的能力

O3-35. 应具有合理分配、控制网络、操作系统和应用系统资源的能力

O3-36. 应具有能够检测、分析、响应对网络和重要主机的各种攻击的能力

O3-37. 应具有发现所有已知漏洞并及时修补的能力

O3-38. 应具有对网络、系统和应用的访问进行严格控制的能力

O3-39. 应具有对数据、文件或其他资源的访问进行严格控制的能力

O3-40. 应具有对资源访问的行为进行记录、分析并响应的能力

O3-41. 应具有对恶意代码的检测、阻止和清除能力

O3-42. 应具有防止恶意代码等在网络中扩散的能力

O3-43. 应具有对恶意代码库和搜索引擎及时更新的能力

O3-44. 应具有保证鉴别数据传输和存储保密性的能力

O3-45. 应具有对用户进行唯一标识的能力

O3-46. 应具有对同一个用户产生多重鉴别信息并进行多重鉴别的能力

O3-47. 应具有对硬件设备进行唯一标识的能力

O3-48. 应具有对硬件设备进行合法身份确定的能力

O3-49. 应具有检测非法接入设备的能力

O3-50. 应具有对存储介质中的残余信息进行删除的能力

O3-51. 应具有对传输和存储中的信息进行保密性保护的能力

O3-52. 应具有防止加密数据被破解的能力

O3-53. 应具有路由选择和控制的能力

O3-54. 应具有信息源发的鉴别能力

O3-55. 应具有通信数据完整性检测和纠错能力

O3-56. 应具有对关键区域进行电磁屏蔽的能力

O3-57. 应具有持续非活动状态一段时间后自动切断连接的能力

O3-58. 应具有基于密码技术的抗抵赖能力

O3-59. 应具有防止未授权下载、拷贝软件或者文件的能力

O3-60. 应具有网络边界完整性检测能力

O3-61. 应具有切断非法连接的能力

O3-62. 应具有重要数据和程序进行完整性检测和纠错能力

O3-63. 应具有对敏感信息进行标识的能力

O3-64. 应具有对敏感信息的流向进行控制的能力

O3-65. 应具有及时恢复重要数据的能力

O3-66. 应具有保证重要业务系统及时恢复运行的能力

6.3.2. 管理目标

O3-67. 应确保建立了安全职能部门，配备了安全管理人员，支持信息安全管理工作

O3-68. 应确保配备了足够数量的管理人员，对系统进行运行维护

O3-69. 应确保对管理活动进行了制度化管理

O3-70. 应确保建立并不断完善、健全安全管理制度

O3-71. 应确保能协调信息安全工作在各功能部门的实施

O3-72. 应确保能控制信息安全相关事件的授权与审批

O3-73. 应确保建立恰当可靠的联络渠道，以便安全事件发生时能得到支持

O3-74. 应确保对人员的行为进行控制和规范

O3-75. 应确保对人员的管理活动进行了指导

O3-76. 应确保安全策略的正确性和安全措施的合理性

O3-77. 应确保对信息系统进行合理定级，，并进行备案管理

O3-78. 应确保安全产品的可信度和产品质量

O3-79. 应确保自行开发过程和工程实施过程中的安全

O3-80. 应确保能顺利地接管和维护信息系统

O3-81. 应确保安全工程的实施质量和安全功能的准确实现

O3-82. 应确保机房具有良好的运行环境

O3-83. 应确保对信息资产进行分类标识管理

O3-84. 应确保对各种软硬件设备的选型、采购、发放、使用和保管等过程进行控制

O3-85. 应确保各种网络设备、服务器正确使用和维护

O3-86. 应确保对网络、操作系统、数据库系统和应用系统进行安全管理

O3-87. 应确保用户具有鉴别信息使用的安全意识

O3-88. 应确保定期地对通信线路进行检查和维护

O3-89. 应确保硬件设备、存储介质存放环境安全，并对其进行控制和保护

O3-90. 应确保对支撑设施、硬件设备、存储介质进行日常维护和管理

O3-91. 应确保系统中使用的硬件、软件产品的质量

O3-92. 应确保各类人员具有与其岗位相适应的技术能力

O3-93. 应确保对各类人员进行相关的技术培训

O3-94. 应确保提供的足够的使用手册、维护指南等资料

O3-95. 应确保内部人员具有安全方面的常识和意识

O3-96. 应确保具有设计合理、安全网络结构的能力

O3-97. 应确保对软硬件的分发过程进行控制

O3-98. 应确保软硬件中没有后门程序

O3-99. 应确保密码算法和密钥的使用符合国家有关法律、法规的规定

O3-100. 应确保任何变更控制和设备重用要申报和审批，并对其实行制度化的管理

O3-101. 应确保在事件发生后能采取积极、有效的应急策略和措施

O3-102. 应确保信息安全事件实行分等级响应、处置

6.4. 第4级安全目标

第四级信息系统应实现以下目标。

6.4.1. 技术目标

O4-1. 应具有对抗中等强度地震、台风等自然灾难造成破坏的能力

O4-2. 应具有防止雷击事件导致大面积设备被破坏的能力

O4-3. 应具有防水和防潮的能力

O4-4. 应具有对水患检测和报警的能力

O4-5. 应具有自动灭火的能力

O4-6. 应具有检测火灾和报警的能力

O4-7. 应具有防止火灾蔓延的能力

O4-8. 应具有温湿度自动检测和控制的能力

O4-9. 应具有防止电压波动的能力

O4-10. 应具有对抗较长时间断电的能力

O4-11. 应具有防止静电导致大面积设备被破坏的能力

O4-12. 应具有检测静电和消除静电的能力

O4-13. 应具有对机房电磁屏蔽的能力

O4-14. 应具有防止强电磁场、强震动源和强噪声源等污染影响系统正常的能力

O4-15. 应具有监测通信线路传输状况的能力

O4-16. 应具有系统软件、应用软件容错的能力

O4-17. 应具有软件故障分析的能力

O4-18. 应具有软件状态监测和报警的能力

O4-19. 应具有自动保护当前工作状态的能力

O4-20. 应具有自动恢复到故障前工作状态的能力

O4-21. 应具有合理使用和控制系统资源的能力

O4-22. 应具有按优先级自动分配系统资源的能力

O4-23. 应具有对传输和存储数据进行完整性检测和纠错的能力

O4-24. 应具有对软件缺陷进行检查的能力

O4-25. 应具有记录用户操作行为和分析记录结果的能力

O4-26. 应具有对用户的误操作行为进行检测、报警和恢复的能力

O4-27. 应具有安全机制失效的自动检测和报警能力

O4-28. 应具有检测到安全机制失效后恢复安全机制的能力

O4-29. 应具有严格控制机房进出的能力

O4-30. 应具有防止设备、介质等丢失的能力

O4-31. 应具有严格控制机房内人员活动的能力

O4-32. 应具有实时监控机房内部活动的能力

O4-33. 应具有对物理入侵事件进行报警的能力

O4-34. 应具有控制接触重要设备、介质的能力

O4-35. 应具有对通信线路进行物理保护的能力

O4-36. 应具有使重要通信线路及时恢复的能力

O4-37. 应具有限制网络、操作系统和应用系统资源使用的能力

O4-38. 应具有能够检测、集中分析、响应、阻止对网络和所有主机的各种攻击的能力

O4-39. 应具有合理分配、控制网络、操作系统和应用系统资源的能力

O4-40. 应具有发现所有已知漏洞并及时修补的能力

O4-41. 应具有对网络、系统和应用的访问进行严格控制的能力

O4-42. 应具有对数据、文件或其他资源的访问进行严格控制的能力

O4-43. 应具有对资源访问的行为进行记录、集中分析并响应的能力

O4-44. 应具有对恶意代码的检测、集中分析、阻止和清除能力

O4-45. 应具有防止恶意代码在网络中扩散的能力

O4-46. 应具有对恶意代码库和搜索引擎及时更新的能力

O4-47. 应具有保证鉴别数据传输和存储保密性的能力

O4-48. 应具有对用户进行唯一标识的能力

O4-49. 应具有对同一个用户产生多重鉴别信息，其中一个是不可伪造的鉴别信息并进行多重鉴别的能力

O4-50. 应具有对硬件设备进行唯一标识的能力

O4-51. 应具有对硬件设备进行合法身份确定的能力

O4-52. 应具有检测非法接入设备的能力

O4-53. 应具有对传输和存储中的信息进行保密性保护的能力

O4-54. 应具有对存储介质中的残余信息进行删除的能力

O4-55. 应具有防止加密数据被破解的能力

O4-56. 应具有路由选择和控制的能力

O4-57. 应具有信息源发的鉴别能力

O4-58. 应具有对关键区域进行电磁屏蔽的能力

O4-59. 应具有持续非活动状态一段时间后自动切断连接的能力

O4-60. 应具有基于密码技术的抗抵赖能力

O4-61. 应具有防止未授权下载、拷贝软件或者文件的能力

O4-62. 应具有网络边界完整性检测能力

O4-63. 应具有切断非法连接的能力

O4-64. 应具有重要数据和程序进行完整性检测和纠错能力

O4-65. 应具有对敏感信息进行标识的能力

O4-66. 应具有对敏感信息的流向进行控制的能力

O4-67. 应具有迅速恢复重要数据的能力

O4-68. 应具有保证通信不中断的能力

O4-69. 应具有保证业务系统不中断的能力

6.4.2. 管理目标

O4-70. 应确保建立了安全职能部门，配备了安全管理人员，支持信息安全管理工作

O4-71. 应确保配备了足够数量的管理人员，对系统进行运行维护

O4-72. 应确保对管理活动进行了制度化管理

O4-73. 应确保建立并不断完善、健全安全管理制度

O4-74. 应确保能协调信息安全工作在各功能部门的实施

O4-75. 应确保能控制信息安全相关事件的授权与审批

O4-76. 应确保建立恰当可靠的联络渠道，以便安全事件发生时能得到支持

O4-77. 应确保对人员的行为进行控制和规范

O4-78. 应确保对人员的管理活动进行了指导

O4-79. 应确保安全策略的正确性和安全措施的合理性

O4-80. 应确保对信息系统进行合理定级，并进行备案管理

O4-81. 应确保安全产品的可信度和产品质量

O4-82. 应确保自行开发过程和工程实施过程中的安全

O4-83. 应确保能顺利地接管和维护信息系统

O4-84. 应确保安全工程的实施质量和安全功能的准确实现

O4-85. 应确保机房具有良好的运行环境

O4-86. 应确保对信息资产进行分类标识、分级管理

O4-87. 应确保对各种软硬件设备的选型、采购、发放、使用和保管等过程进行控制

O4-88. 应确保各种网络设备、服务器正确使用和维护

O4-89. 应确保对网络、操作系统、数据库系统和应用系统进行安全管理

O4-90. 应确保用户具有鉴别信息使用的安全意识

O4-91. 应确保定期地对通信线路进行检查和维护

O4-92. 应确保硬件设备、存储介质存放环境安全，并对其的使用进行控制和保护

O4-93. 应确保对支撑设施、硬件设备、存储介质进行日常维护和管理

O4-94. 应确保系统中使用的硬件、软件产品的质量

O4-95. 应确保各类人员具有与其岗位相适应的技术能力

O4-96. 应确保对各类人员进行相关的技术培训

O4-97. 应确保提供的足够的使用手册、维护指南等资料

O4-98. 应确保内部人员具有安全方面的常识和意识

O4-99. 应确保具有设计合理、安全网络结构的能力

O4-100. 应确保对软硬件的分发过程进行控制

O4-101. 应确保软硬件中没有后门程序和隐蔽信道

O4-102. 应确保密码算法和密钥的使用符合国家有关法律、法规的规定

O4-103. 应确保任何变更控制和设备重用要申报和审批，并对其实行制度化的管理

O4-104. 应确保在事件发生后能采取积极、有效的应急策略和措施

O4-105. 应确保信息安全事件实行分等级响应、处置

7 第 1 级基本要求

7.1. 技术要求

7.1.1. 物理安全

7.1.1.1. 物理访问控制（G1）

a) 机房出入应有专人负责，进入的人员登记在案。

7.1.1.2. 防盗窃和防破坏（G1）

a) 应将主要设备放置在物理受限的范围内；

b) 应对设备或主要部件进行固定，并设置明显的不易除去的标记。

7.1.1.3. 防雷击（G1）

a) 机房建筑应设置避雷装置。

7.1.1.4. 防火（G1）

a) 应设置灭火设备，并保持灭火设备的良好状态。

7.1.1.5. 防水和防潮（G1）

a) 应对穿过墙壁和楼板的水管增加必要的保护措施，如设置套管；

b) 应采取措施防止雨水通过屋顶和墙壁渗透。

7.1.1.6. 温湿度控制（G1）

a) 应设置必要的温、湿度控制设施，使机房温、湿度的变化在设备运行所允许的范围之内。

7.1.1.7. 电力供应（A1）

a) 计算机系统供电应与其他供电分开；

b) 应设置稳压器和过电压防护设备。

7.1.2. 网络安全

7.1.2.1. 结构安全与网段划分（G1）

a) 主要网络设备的业务处理能力应满足基本业务需要；

b) 根据机构业务的特点，在满足基本业务需要的基础上，应合理设计网络接入及核心网络的带宽；

c) 应在业务终端与业务服务器之间进行路由控制，并建立安全的访问路径；

d) 应设计和绘制与当前运行情况相符的网络拓扑结构图。

7.1.2.2. 网络访问控制（G1）

a) 应根据访问控制列表对源地址、目的地址、源端口、目的端口、协议等进行检查，以允许/拒绝数据包出入。

7.1.2.3. 拨号访问控制（G1）

a) 通过访问控制列表对系统资源实现允许或拒绝用户访问，控制粒度为用户组。

7.1.2.4. 网络设备防护（G1）

a) 应对登录网络设备的用户进行身份鉴别；

b) 应具有登录失败处理功能，如结束会话、限制非法登录次数。

7.1.3. 主机系统安全

7.1.3.1. 身份鉴别（S1）

a) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；

b) 应具有登录失败处理功能，如结束会话、限制非法登录次数。

7.1.3.2. 自主访问控制（S1）

a) 操作系统和数据库管理系统应依据安全策略控制用户对客体的访问；

b) 自主访问控制的覆盖范围应包括与信息安全直接相关的主体、客体及它们之间的操作；

c) 操作系统和数据库系统自主访问控制的粒度应达到主体为用户组/用户级，客体为文件、数据库表级；

d) 应由授权主体设置对客体访问和操作的权限；

e) 应严格限制默认用户的访问权限。

7.1.3.3. 恶意代码防范（G1）

a) 重要业务处理服务器应安装实时检测与查杀恶意代码的软件产品。

7.1.4. 应用安全

7.1.4.1. 身份鉴别（S1）

a) 应对登录应用系统的用户进行身份标识和鉴别；

b) 应具有登录失败处理的功能，如结束会话、限制非法登录次数。

7.1.4.2. 访问控制（S1）

a) 应控制应用系统用户对系统功能和用户数据的访问；

b) 应用系统自主访问控制的粒度应达到主体为用户组/用户级；

c) 应由授权主体设置用户对系统功能操作和对数据访问的权限；

d) 应严格限制默认用户的访问权限。

7.1.4.3. 通信完整性（S1）

a) 通信双方应约定通信会话的方式，在进行通信时，双方根据会话方式判断对方报文的有效性。

7.1.4.4. 软件容错（A1）

a) 应对通过人机接口输入或通过通信接口输入的数据进行有效性检验；

b) 在故障发生并中断退出时，提供故障类型和故障发生点的信息。

7.1.4.5. 资源控制（A1）

a) 应对应用系统的最大并发会话连接数进行限制。

7.1.4.6. 代码安全（G1）

a) 应对应用程序代码进行恶意代码扫描，确认不存在恶意代码。

7.1.5. 数据安全

7.1.5.1. 数据完整性（S1）

a) 应能够检测到系统管理数据、鉴别信息和用户数据在传输过程中完整性受到破坏；

b) 应能够检测到系统管理数据、鉴别信息和用户数据在存储过程中完整性受到破坏。

7.1.5.2. 数据保密性（S1）

a) 网络设备、操作系统、数据库系统和应用系统的鉴别信息应采用加密或其他保护措施实现存储保密性。

7.1.5.3. 数据备份和恢复（A1）

a) 应提供用户有选择的备份和恢复重要信息的功能。

7.2. 管理要求

7.2.1. 安全管理机构

7.2.1.1. 岗位设置

a) 应设立系统管理人员、网络管理人员、安全管理人员岗位，定义各个工作岗位的职责。

7.2.1.2. 人员配备

a) 应配备一定数量的系统管理人员、网络管理人员、安全管理人员，各个岗位的人员可以兼任。

7.2.1.3. 授权和审批

a) 应授权审批部门及批准人，对网络、应用、系统等重要资源的访问等关键活动进行审批。

7.2.1.4. 沟通和合作

a) 应加强各类管理人员和组织内部机构之间的合作与沟通，定期或不定期召开协调会议，共同协助处理信息安全问题。

7.2.2. 安全管理制度

7.2.2.1. 管理制度

a) 应制定信息安全工作的总体方针、政策性文件和安全策略等，说明机构安全工作的总体目标、范围、方针、原则、责任等；

b) 应建立日常管理活动中常用的安全管理制度，以规范安全管理活动，约束人员的行为。

7.2.2.2. 制定和发布

a) 应授权或指定专门的人员负责制定安全管理制度；

b) 应组织相关人员对制定的安全管理进行论证和审定；

c) 安全管理制度应以某种方式发布到相关人员手中。

7.2.3. 人员安全管理

7.2.3.1. 人员录用

a) 应保证被录用人具备基本的专业技术水平和安全管理知识；

b) 应对被录用人的身份和专业资格等进行审查；

c) 应对被录用人说明其角色和职责。

7.2.3.2. 人员离岗

a) 应立即终止由于各种原因即将离岗的员工的所有访问权限；

b） 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

7.2.3.3. 安全意识教育和培训

a） 应对各类人员进行安全意识教育；

b） 应告知人员相关的安全责任和惩戒措施。

7.2.3.4. 第三方人员访问管理

a） 第三方人员应在访问前与机构签署安全责任合同书或保密协议。

7.2.4. 系统建设管理

7.2.4.1. 系统定级

a） 应明确信息系统划分的方法；

b） 应确定信息系统的安全等级；

c） 应以书面的形式定义确定了安全等级的信息系统的属性，包括使命、业务、网络、硬件、软件、数据、边界、人员等；

d） 应确保信息系统的定级结果经过相关部门的批准。

7.2.4.2. 安全方案设计

a） 应根据系统的安全级别选择基本安全措施，依据风险分析的结果补充和调整安全措施；

b） 应以书面的形式描述对系统的安全保护要求和策略、安全措施等内容，形成系统的安全方案；

c） 应对安全方案进行细化，形成能指导安全系统建设和安全产品采购的详细设计方案。

7.2.4.3. 产品采购

a） 应确保安全产品的使用符合国家的有关规定。

7.2.4.4. 自行软件开发

a） 应确保开发环境与实际运行环境物理分开；

b） 应确保系统开发文档由专人负责保管，系统开发文档的使用受到控制。

7.2.4.5. 外包软件开发

a） 应与软件开发单位签订协议，明确知识产权的归属和安全方面的要求；

b） 应根据协议的要求检测软件质量；

c） 应在软件安装之前检测软件包中可能存在的恶意代码。

7.2.4.6. 工程实施

a) 应与工程实施单位签订与安全相关的协议，约束工程实施单位的行为。

7.2.4.7. 测试验收

a) 应对系统进行安全性测试验收；

b) 应在测试验收前根据设计方案或合同要求等制订测试验收方案，测试验收过程中详细记录测试验收结果，形成测试验收报告；

c) 应组织相关部门和相关人员对系统测试验收报告进行审定，没有疑问后由双方签字。

7.2.4.8. 系统交付

a) 应明确系统的交接手续，并按照交接手续完成交接工作；

b) 应由系统建设方完成对委托建设方的运维技术人员的培训；

c) 应由系统建设方提交系统建设过程中的文档和指导用户进行系统运行维护的文档。

7.2.4.9. 安全服务商选择

a) 应确保安全服务商的选择符合国家的有关规定。

7.2.5. 系统运维管理

7.2.5.1. 环境管理

a) 应对机房供配电、空调、温湿度控制等设施指定专人或专门的部门定期进行维护管理；

b) 应配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理；

c) 应建立机房出入管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定。

7.2.5.2. 资产管理

a) 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门；

b) 应编制并保存与信息系统相关的资产、资产所属关系、安全级别和所处位置等信息的资产清单。

7.2.5.3. 介质管理

a) 应确保介质存放在安全的环境中，并对各类介质进行控制和保护，以防止被盗、被毁、被未授权修改以及信息的非法泄漏；

b) 应有介质的存储、归档、登记和查询记录，并根据备份及存档介质的目录清单定期盘点。

7.2.5.4. 设备管理

a) 应对信息系统相关的各种设施、设备、线路等指定专人或专门的部门定期进行维护管理；

b) 应对信息系统的各种软硬件设备的选型、采购、发放或领用等过程建立基于申报、审批和专人负责的管理规定；

c) 应按操作规程实现服务器的启动/停止、加电/断电等操作，并根据业务系统的要求维护好系统配置和服务设定；

d) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用过程进行规范化管理。

7.2.5.5. 监控管理

a) 应了解服务器的CPU、内存、进程、磁盘使用情况。

7.2.5.6. 网络安全管理

a) 应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；

b) 应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；

c) 应进行网络系统漏洞扫描，对发现的网络系统安全漏洞进行及时的修补。

7.2.5.7. 系统安全管理

a) 应指定专人对系统进行管理，删除或者禁用不使用的系统缺省账户；

b) 应定期安装系统的最新补丁程序，并根据厂家提供的可能危害计算机的漏洞进行及时修补，并在安装系统补丁前对现有的重要文件进行备份；

c) 应根据业务需求和系统安全分析确定系统的访问控制策略，系统访问控制策略用于控制分配信息系统、文件及服务的访问权限。

7.2.5.8. 恶意代码防范管理

a) 应提高所用用户的防病毒意识，告知及时升级防病毒软件；

b) 应在读取移动存储设备（如软盘、移动硬盘、光盘）上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也要进行病毒检查。

7.2.5.9. 备份与恢复管理

a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b) 应规定备份信息的备份方式（如增量备份或全备份等）、备份频度（如每日或每周等）、存储介质、保存期等。

7.2.5.10. 安全事件处置

a) 所有用户均有责任报告自己发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；

b) 应制定安全事件报告和处置管理制度，规定安全事件的现场处理、事件报告和后期恢复的管理职责。

8 第 2 级基本要求

8.1. 技术要求

8.1.1. 物理安全

8.1.1.1. 物理位置的选择（G2）

a) 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内。

8.1.1.2. 物理访问控制（G2）

a) 机房出入口应有专人值守，鉴别进入的人员身份并登记在案；

b) 应批准进入机房的来访人员，限制和监控其活动范围。

8.1.1.3. 防盗窃和防破坏（G2）

a) 应将主要设备放置在物理受限的范围内；

b) 应对设备或主要部件进行固定，并设置明显的不易除去的标记；

c) 应将通信线缆铺设在隐蔽处，如铺设在地下或管道中等；

d) 应对介质分类标识，存储在介质库或档案室中；

e) 应安装必要的防盗报警设施，以防进入机房的盗窃和破坏行为。

8.1.1.4. 防雷击（G2）

a) 机房建筑应设置避雷装置；

b) 应设置交流电源地线。

8.1.1.5. 防火（G2）

a) 应设置灭火设备和火灾自动报警系统，并保持灭火设备和火灾自动报警系统的良好状态。

8.1.1.6. 防水和防潮（G2）

a) 水管安装，不得穿过屋顶和活动地板下；

b) 应对穿过墙壁和楼板的水管增加必要的保护措施，如设置套管；

c） 应采取措施防止雨水通过屋顶和墙壁渗透；

d） 应采取措施防止室内水蒸气结露和地下积水的转移与渗透。

8.1.1.7. 防静电（G2）

a） 应采用必要的接地防静电措施。

8.1.1.8. 温湿度控制（G2）

a） 应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。

8.1.1.9. 电力供应（A2）

a） 计算机系统供电应与其他供电分开；

b） 应设置稳压器和过电压防护设备；

c） 应提供短期的备用电力供应（如：UPS设备）。

8.1.1.10. 电磁防护（S2）

a） 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；

b） 电源线和通信线缆应隔离，避免互相干扰。

8.1.2. 网络安全

8.1.2.1. 结构安全与网段划分（G2）

a） 网络设备的业务处理能力应具备冗余空间，要求满足业务高峰期需要；

b） 应设计和绘制与当前运行情况相符的网络拓扑结构图；

c） 应根据机构业务的特点，在满足业务高峰期需要的基础上，合理设计网络带宽；

d） 应在业务终端与业务服务器之间进行路由控制，建立安全的访问路径；

e） 应根据各部门的工作职能、重要性、所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；

f） 重要网段应采取网络层地址与数据链路层地址绑定措施，防止地址欺骗。

8.1.2.2. 网络访问控制（G2）

a） 应能根据会话状态信息（包括数据包的源地址、目的地址、源端口号、目的端口号、协议、出入的接口、会话序列号、发出信息的主机名等信息，并应支持地址通配符的使用），为数据流提供明确的允许/拒绝访问的能力。

8.1.2.3. 拨号访问控制（G2）

a） 应在基于安全属性的允许远程用户对系统访问的规则的基础上，对系统所有资源允许或拒绝用户进行访问，控制粒度为单个用户；

b) 应限制具有拨号访问权限的用户数量。

8.1.2.4. 网络安全审计（G2）

a) 应对网络系统中的网络设备运行状况、网络流量、用户行为等事件进行日志记录；

b) 对于每一个事件，其审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功，及其他与审计相关的信息。

8.1.2.5. 边界完整性检查（S2）

a) 应能够检测内部网络中出现的内部用户未通过准许私自联到外部网络的行为（即“非法外联”行为）。

8.1.2.6. 网络入侵防范（G2）

a) 应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击、网络蠕虫攻击等入侵事件的发生。

8.1.2.7. 恶意代码防范（G2）

a) 应在网络边界及核心业务网段处对恶意代码进行检测和清除；

b) 应维护恶意代码库的升级和检测系统的更新；

c) 应支持恶意代码防范的统一管理。

8.1.2.8. 网络设备防护（G2）

a) 应对登录网络设备的用户进行身份鉴别；

b) 应对网络设备的管理员登录地址进行限制；

c) 网络设备用户的标识应唯一；

d) 身份鉴别信息应具有不易被冒用的特点，例如口令长度、复杂性和定期的更新等；

e) 应具有登录失败处理功能，如：结束会话、限制非法登录次数，当网络登录连接超时，自动退出。

8.1.3. 主机系统安全

8.1.3.1. 身份鉴别（S2）

a) 操作系统和数据库系统用户的身份标识应具有唯一性；

b) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；

c) 操作系统和数据库系统身份鉴别信息应具有不易被冒用的特点，例如口令长度、复杂性和定期的更新等；

d) 应具有登录失败处理功能，如：结束会话、限制非法登录次数，当登录连接超时，自动退出。

8.1.3.2. 自主访问控制（S2）

a) 应依据安全策略控制主体对客体的访问；

b) 自主访问控制的覆盖范围应包括与信息安全直接相关的主体、客体及它们之间的操作；

c) 自主访问控制的粒度应达到主体为用户级，客体为文件、数据库表级；

d) 应由授权主体设置对客体访问和操作的权限；

e) 应严格限制默认用户的访问权限。

8.1.3.3. 安全审计（G2）

a) 安全审计应覆盖到服务器上的每个操作系统用户和数据库用户；

b) 安全审计应记录系统内重要的安全相关事件，包括重要用户行为和重要系统命令的使用等；

c) 安全相关事件的记录应包括日期和时间、类型、主体标识、客体标识、事件的结果等；

d) 审计记录应受到保护避免受到未预期的删除、修改或覆盖等。

8.1.3.4. 系统保护（G2）

a) 系统应提供在管理维护状态中运行的能力，管理维护状态只能被系统管理员使用。

8.1.3.5. 剩余信息保护（S2）

a) 应保证操作系统和数据库管理系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

b) 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

8.1.3.6. 恶意代码防范（G2）

a) 服务器和重要终端设备（包括移动设备）应安装实时检测和查杀恶意代码的软件产品；

b) 主机系统防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；

8.1.3.7. 资源控制（A2）

a) 应限制单个用户的会话数量；

b) 应通过设定终端接入方式、网络地址范围等条件限制终端登录。

8.1.4. 应用安全

8.1.4.1. 身份鉴别（S2）

a) 应用系统用户的身份标识应具有唯一性；

b) 应对登录的用户进行身份标识和鉴别；

c) 系统用户身份鉴别信息应具有不易被冒用的特点，例如口令长度、复杂性和定期的更新等；

d) 应具有登录失败处理功能，如：结束会话、限制非法登录次数，当登录连接超时，自动退出。

8.1.4.2. 访问控制（S2）

a) 应依据安全策略控制用户对客体的访问；

b) 自主访问控制的覆盖范围应包括与信息安全直接相关的主体、客体及它们之间的操作；

c) 自主访问控制的粒度应达到主体为用户级，客体为文件、数据库表级；

d) 应由授权主体设置用户对系统功能操作和对数据访问的权限；

e) 应实现应用系统特权用户的权限分离，例如将管理与审计的权限分配给不同的应用系统用户；

f) 权限分离应采用最小授权原则，分别授予不同用户各自为完成自己承担任务所需的最小权限，并在它们之间形成相互制约的关系；

g) 应严格限制默认用户的访问权限。

8.1.4.3. 安全审计（G2）

a) 安全审计应覆盖到应用系统的每个用户；

b) 安全审计应记录应用系统重要的安全相关事件，包括重要用户行为和重要系统功能的执行等；

c) 安全相关事件的记录应包括日期和时间、类型、主体标识、客体标识、事件的结果等；

d) 审计记录应受到保护避免受到未预期的删除、修改或覆盖等。

8.1.4.4. 剩余信息保护（S2）

a) 应保证用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

b) 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

8.1.4.5. 通信完整性（S2）

a) 通信双方应约定单向的校验码算法，计算通信数据报文的校验码，在进行通信时，双方根据校验码判断对方报文的有效性。

8.1.4.6. 通信保密性（S2）

a) 当通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；

b) 在通信双方建立连接之前，利用密码技术进行会话初始化验证；

c) 在通信过程中，应对敏感信息字段进行加密。

8.1.4.7. 软件容错（A2）

a) 应对通过人机接口输入或通过通信接口输入的数据进行有效性检验；

b) 应对通过人机接口方式进行的操作提供“回退”功能，即允许按照操作的序列进行回退；

c) 在故障发生时，应继续提供一部分功能，确保能够实施必要的措施。

8.1.4.8. 资源控制（A2）

a) 应限制单个用户的多重并发会话；

b) 应对应用系统的最大并发会话连接数进行限制；

c) 应对一个时间段内可能的并发会话连接数进行限制。

8.1.4.9. 代码安全（G2）

a) 应对应用程序代码进行恶意代码扫描；

b) 应对应用程序代码进行安全脆弱性分析。

8.1.5. 数据安全

8.1.5.1. 数据完整性（S2）

a) 应能够检测到系统管理数据、鉴别信息和用户数据在传输过程中完整性受到破坏；

b) 应能够检测到系统管理数据、鉴别信息和用户数据在存储过程中完整性受到破坏。

8.1.5.2. 数据保密性（S2）

a) 网络设备、操作系统、数据库系统和应用系统的鉴别信息、敏感的系统管理数据和敏感的用户数据应采用加密或其他有效措施实现传输保密性；

b) 网络设备、操作系统、数据库系统和应用系统的鉴别信息、敏感的系统管理数据和敏感的用户数据应采用加密或其他保护措施实现存储保密性；

c） 当使用便携式和移动式设备时，应加密或者采用可移动磁盘存储敏感信息。

8.1.5.3. 数据备份和恢复（A2）

a） 应提供自动机制对重要信息进行有选择的数据备份；

b） 应提供恢复重要信息的功能；

c） 应提供重要网络设备、通信线路和服务器的硬件冗余。

8.2. 管理要求

8.2.1. 安全管理机构

8.2.1.1. 岗位设置

a） 应设立信息安全管理工作的职能部门，设立安全主管人、安全管理各个方面的负责人岗位，定义各负责人的职责；

b） 应设立系统管理人员、网络管理人员、安全管理人员岗位，定义各个工作岗位的职责；

c） 应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

8.2.1.2. 人员配备

a） 应配备一定数量的系统管理人员、网络管理人员、安全管理人员等；

b） 安全管理人员不能兼任网络管理员、系统管理员、数据库管理员等。

8.2.1.3. 授权和审批

a） 应授权审批部门及批准人，对关键活动进行审批；

b） 应列表说明须审批的事项、审批部门和可批准人。

8.2.1.4. 沟通和合作

a） 应加强各类管理人员和组织内部机构之间的合作与沟通，定期或不定期召开协调会议，共同协助处理信息安全问题；

b） 信息安全职能部门应定期或不定期召集相关部门和人员召开安全工作会议，协调安全工作的实施；

c） 应加强与兄弟单位、公安机关、电信公司的合作与沟通，以便在发生安全事件时能够得到及时的支持。

8.2.1.5. 审核和检查

a） 应由安全管理人员定期进行安全检查，检查内容包括用户账号情况、系统漏洞情况、系统审计情况等。

8.2.2. 安全管理制度

8.2.2.1. 管理制度

a) 应制定信息安全工作的总体方针、政策性文件和安全策略等，说明机构安全工作的总体目标、范围、方针、原则、责任等；

b) 应对安全管理活动中重要的管理内容建立安全管理制度，以规范安全管理活动，约束人员的行为方式；

c) 应对要求管理人员或操作人员执行的重要管理操作，建立操作规程，以规范操作行为，防止操作失误。

8.2.2.2. 制定和发布

a) 应在信息安全职能部门的总体负责下，组织相关人员制定；

b) 应保证安全管理制度具有统一的格式风格，并进行版本控制；

c) 应组织相关人员对制定的安全管理进行论证和审定；

d) 安全管理制度应经过管理层签发后按照一定的程序以文件形式发布。

8.2.2.3. 评审和修订

a) 应定期对安全管理制度进行评审和修订，对存在不足或需要改进的安全管理制度进行修订。

8.2.3. 人员安全管理

8.2.3.1. 人员录用

a) 应保证被录用人具备基本的专业技术水平和安全管理知识；

b) 应对被录用人的身份、背景、专业资格和资质等进行审查；

c) 应对被录用人所具备的技术技能进行考核；

d) 应对被录用人说明其角色和职责；

e) 应签署保密协议。

8.2.3.2. 人员离岗

a) 应立即终止由于各种原因即将离岗的员工的所有访问权限；

b) 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；

c) 应经机构人事部门办理严格的调离手续，并承诺调离后的保密义务后方可离开。

8.2.3.3. 人员考核

a) 应定期对各个岗位的人员进行安全技能及安全认知的考核；

b) 应对关键岗位的人员进行全面、严格的安全审查；

c） 应对违背安全策略和规定的人员进行惩戒。

8.2.3.4. 安全意识教育和培训

a） 应对各类人员进行安全意识教育；

b） 应告知人员相关的安全责任和惩戒措施；

c） 应制定安全教育和培训计划，对信息安全基础知识、岗位操作规程等进行培训；

d） 应对安全教育和培训的情况和结果进行记录并归档保存。

8.2.3.5. 第三方人员访问管理

a） 第三方人员应在访问前与机构签署安全责任合同书或保密协议；

b） 对重要区域的访问，必须经过有关负责人的批准，并由专人陪同或监督下进行，并记录备案。

8.2.4. 系统建设管理

8.2.4.1. 系统定级

a） 应明确信息系统划分的方法；

b） 应确定信息系统的安全等级；

c） 应以书面的形式定义确定了安全等级的信息系统的属性，包括使命、业务、网络、硬件、软件、数据、边界、人员等；

d） 应确保信息系统的定级结果经过相关部门的批准。

8.2.4.2. 安全方案设计

a） 应根据系统的安全级别选择基本安全措施，依据风险分析的结果补充和调整安全措施；

b） 应以书面的形式描述对系统的安全保护要求和策略、安全措施等内容，形成系统的安全方案；

c） 应对安全方案进行细化，形成能指导安全系统建设和安全产品采购的详细设计方案；

d） 应组织相关部门和有关安全技术专家对安全设计方案的合理性和正确性进行论证和审定；

e） 应确保安全设计方案必须经过批准，才能正式实施。

8.2.4.3. 产品采购

a） 应确保安全产品的使用符合国家的有关规定；

b） 应确保密码产品的使用符合国家密码主管部门的要求；

c） 应指定或授权专门的部门负责产品的采购。

8.2.4.4. 自行软件开发

a） 应确保开发环境与实际运行环境物理分开；

b） 应确保提供软件设计的相关文档和使用指南；

c） 应确保系统开发文档由专人负责保管，系统开发文档的使用受到控制。

8.2.4.5. 外包软件开发

a） 应与软件开发单位签订协议，明确知识产权的归属和安全方面的要求；

b） 应根据协议的要求检测软件质量；

c） 应在软件安装之前检测软件包中可能存在的恶意代码；

d） 应确保提供软件设计的相关文档和使用指南。

8.2.4.6. 工程实施

a） 应与工程实施单位签订与安全相关的协议，约束工程实施单位的行为；

b） 应指定或授权专门的人员或部门负责工程实施过程的管理；

c） 应制定详细的工程实施方案控制实施过程。

8.2.4.7. 测试验收

a） 应对系统进行安全性测试验收；

b） 应在测试验收前根据设计方案或合同要求等制订测试验收方案，测试验收过程中详细记录测试验收结果，形成测试验收报告；

c） 应组织相关部门和相关人员对系统测试验收报告进行审定，没有疑问后由双方签字。

8.2.4.8. 系统交付

a） 应明确系统的交接手续，并按照交接手续完成交接工作；

b） 应由系统建设方完成对委托建设方的运维技术人员的培训；

c） 应由系统建设方提交系统建设过程中的文档和指导用户进行系统运行维护的文档；

d） 应由系统建设方进行服务承诺，并提交服务承诺书，确保对系统运行维护的支持。

8.2.4.9. 安全服务商选择

a） 应确保安全服务商的选择符合国家的有关规定。

8.2.5. 系统运维管理

8.2.5.1. 环境管理

a) 应对机房供配电、空调、温湿度控制等设施指定专人或专门的部门定期进行维护管理；

b) 应配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理；

c) 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；

d) 应对机房来访人员实行登记、备案管理，同时限制来访人员的活动范围；

e) 加强对办公环境的保密性管理，包括如工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等。

8.2.5.2. 资产管理

a) 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门；

b) 应编制并保存与信息系统相关的资产、资产所属关系、安全级别和所处位置等信息的资产清单；

c) 应根据资产的重要程度对资产进行定性赋值和标识管理，根据资产的价值选择相应的管理措施。

8.2.5.3. 介质管理

a) 应确保介质存放在安全的环境中，并对各类介质进行控制和保护，以防止被盗、被毁、被未授权的修改以及信息的非法泄漏；

b) 应有介质的存储、归档、登记和查询记录，并根据备份及存档介质的目录清单定期盘点；

c) 对于需要送出维修或销毁的介质，应首先清除介质中的敏感数据，防止信息的非法泄漏；

d) 应根据所承载数据和软件的重要程度对介质进行分类和标识管理，并实行存储环境专人管理。

8.2.5.4. 设备管理

a) 应对信息系统相关的各种设施、设备、线路等指定专人或专门的部门定期进行维护管理；

b) 应对信息系统的各种软硬件设备的选型、采购、发放或领用等过程建立基于申报、审批和专人负责的管理规定；

c) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理；

d) 应对带离机房或办公地点的信息处理设备进行控制；

e) 应按操作规程实现服务器的启动/停止、加电/断电等操作，加强对服务器操作的日志文件管理和监控管理，应按安全策略的要求对网络及设备进行配置，并对其定期进行检查。

8.2.5.5. 监控管理

a) 应了解服务器的CPU、内存、进程、磁盘使用情况。

8.2.5.6. 网络安全管理

a) 应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；

b) 应建立网络安全管理制度，对网络安全配置和日志等方面作出规定；

c) 应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；

d) 应进行网络系统漏洞扫描，对发现的网络系统安全漏洞进行及时的修补；

e) 应保证所有与外部系统的连接均应得到授权和批准；

f) 应对网络设备的安全策略、授权访问、最小服务、升级与打补丁、维护记录、日志等方面做出具体要求；

g) 应规定网络审计日志的保存时间以便为可能的安全事件调查提供支持。

8.2.5.7. 系统安全管理

a) 应指定专人对系统进行管理，删除或者禁用不使用的系统缺省账户；

b) 应制度系统安全管理制度，对系统安全配置、系统账户以及审计日志等方面作出规定；

c) 应定期安装系统的最新补丁程序，并根据厂家提供的可能危害计算机的漏洞进行及时修补，并在安装系统补丁前对现有的重要文件进行备份；

d) 应根据业务需求和系统安全分析确定系统的访问控制策略，系统访问控制策略用于控制分配信息系统、文件及服务的访问权限；

e) 应对系统账户进行分类管理，权限设定应当遵循最小授权要求；

f) 应对系统的安全策略、授权访问、最小服务、升级与打补丁、维护记录、日志等方面做出具体要求；

g) 应规定系统审计日志的保存时间以便为可能的安全事件调查提供支持；

h) 应进行系统漏洞扫描，对发现的系统安全漏洞进行及时的修补。

8.2.5.8. 恶意代码防范管理

a) 应提高所用用户的防病毒意识，告知及时升级防病毒软件；

b) 应在读取移动存储设备（如软盘、移动硬盘、光盘）上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也要进行病毒检查；

c) 应指定专人对网络和主机的进行恶意代码检测并保存检测记录；

d) 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确管理规定。

8.2.5.9. 密码管理

a) 密码算法和密钥的使用应符合国家密码管理规定。

8.2.5.10. 变更管理

a) 确认系统中要发生的变更，并制定变更方案；

b) 建立变更管理制度，重要系统变更前，应向主管领导申请，审批后方可实施变更；

c) 系统变更情况应向所有相关人员通告。

8.2.5.11. 备份与恢复管理

a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b) 应规定备份信息的备份方式（如增量备份或全备份等）、备份频度（如每日或每周等）、存储介质、保存期等；

c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略应指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；

d) 应指定相应的负责人定期维护和检查备份及冗余设备的状况，确保需要接入系统时能够正常运行；

e) 根据备份方式，规定相应设备的安装、配置和启动的流程。

8.2.5.12. 安全事件处置

a) 所有用户均有责任报告自己发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；

b) 应制定安全事件报告和处置管理制度，规定安全事件的现场处理、事件报告和后期恢复的管理职责；

c) 应分析信息系统的类型、网络连接特点和信息系统用户特点，了解本系统和同类系统已发生的安全事件，识别本系统需要防止发生的安全事件，事件可能来自攻击、错误、故障、事故或灾难；

d) 应根据国家相关管理部门对计算机安全事件等级划分方法，根据安全事件在本系统产生的影响，将本系统计算机安全事件进行等级划分；

e) 应记录并保存所有报告的安全弱点和可疑事件，分析事件原因，监督事态发展，采取措施避免安全事件发生。

8.2.5.13. 应急预案管理

a) 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程和事后教育和培训等内容；

b) 应对系统相关的人员进行培训使之了解如何及何时使用应急预案中的控制手段及恢复策略，对应急预案的培训至少每年举办一次。

9 第 3 级基本要求

9.1. 技术要求

9.1.1. 物理安全

9.1.1.1. 物理位置的选择（G3）

a) 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；

b) 机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁；

c) 机房场地应当避开强电场、强磁场、强震动源、强噪声源、重度环境污染、易发生火灾、水灾、易遭受雷击的地区。

9.1.1.2. 物理访问控制（G3）

a) 机房出入口应有专人值守，鉴别进入的人员身份并登记在案；

b) 应批准进入机房的来访人员，限制和监控其活动范围；

c) 应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过度区域；

d) 应对重要区域配置电子门禁系统，鉴别和记录进入的人员身份并监控其活动。

9.1.1.3. 防盗窃和防破坏（G3）

a) 应将主要设备放置在物理受限的范围内；

b) 应对设备或主要部件进行固定，并设置明显的不易除去的标记；

c) 应将通信线缆铺设在隐蔽处，如铺设在地下或管道中等；

d) 应对介质分类标识，存储在介质库或档案室中；

e) 设备或存储介质携带出工作环境时，应受到监控和内容加密；

f) 应利用光、电等技术设置机房的防盗报警系统，以防进入机房的盗窃和破坏行为；

g) 应对机房设置监控报警系统。

9.1.1.4. 防雷击（G3）

a) 机房建筑应设置避雷装置；

b) 应设置防雷保安器，防止感应雷；

c) 应设置交流电源地线。

9.1.1.5. 防火（G3）

a) 应设置火灾自动消防系统，自动检测火情、自动报警，并自动灭火；

b) 机房及相关的工作房间和辅助房，其建筑材料应具有耐火等级；

c) 机房采取区域隔离防火措施，将重要设备与其他设备隔离开。

9.1.1.6. 防水和防潮（G3）

a) 水管安装，不得穿过屋顶和活动地板下；

b) 应对穿过墙壁和楼板的水管增加必要的保护措施，如设置套管；

c) 应采取措施防止雨水通过屋顶和墙壁渗透；

d) 应采取措施防止室内水蒸气结露和地下积水的转移与渗透。

9.1.1.7. 防静电（G3）

a) 应采用必要的接地防静电措施；

b) 应采用防静电地板。

9.1.1.8. 温湿度控制（G2）

a) 应设置恒温恒湿系统，使机房温、湿度的变化在设备运行所允许的范围之内。

9.1.1.9. 电力供应（A3）

a) 计算机系统供电应与其他供电分开；

b) 应设置稳压器和过电压防护设备；

c) 应提供短期的备用电力供应（如：UPS设备）；

d) 应设置冗余或并行的电力电缆线路；

e) 应建立备用供电系统（如备用发电机），以备常用供电系统停电时启用。

9.1.1.10. 电磁防护（S3）

a) 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；

b) 电源线和通信线缆应隔离，避免互相干扰；

c) 对重要设备和磁介质实施电磁屏蔽。

9.1.2. 网络安全

9.1.2.1. 结构安全与网段划分（G3）

a) 网络设备的业务处理能力应具备冗余空间，要求满足业务高峰期需要；

b) 应设计和绘制与当前运行情况相符的网络拓扑结构图；

c) 应根据机构业务的特点，在满足业务高峰期需要的基础上，合理设计网络带宽；

d) 应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；

e) 应根据各部门的工作职能、重要性、所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；

f) 重要网段应采取网络层地址与数据链路层地址绑定措施，防止地址欺骗；

g) 应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要信息资产主机。

9.1.2.2. 网络访问控制（G3）

a) 应能根据会话状态信息（包括数据包的源地址、目的地址、源端口号、目的端口号、协议、出入的接口、会话序列号、发出信息的主机名等信息，并应支持地址通配符的使用），为数据流提供明确的允许/拒绝访问的能力；

b) 应对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制；

c) 应依据安全策略允许或者拒绝便携式和移动式设备的网络接入；

d) 应在会话处于非活跃一定时间或会话结束后终止网络连接；

e) 应限制网络最大流量数及网络连接数。

9.1.2.3. 拨号访问控制（G3）

a) 应在基于安全属性的允许远程用户对系统访问的规则的基础上，对系统所有资源允许或拒绝用户进行访问，控制粒度为单个用户；

b) 应限制具有拨号访问权限的用户数量；

c) 应按用户和系统之间的允许访问规则，决定允许用户对受控系统进行资源访问。

9.1.2.4. 网络安全审计（G3）

a) 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行全面的监测、记录；

b) 对于每一个事件，其审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功，及其他与审计相关的信息；

c) 安全审计应可以根据记录数据进行分析，并生成审计报表；

d) 安全审计应可以对特定事件，提供指定方式的实时报警；

e) 审计记录应受到保护避免受到未预期的删除、修改或覆盖等。

9.1.2.5. 边界完整性检查（S3）

a) 应能够检测内部网络中出现的内部用户未通过准许私自联到外部网络的行为（即“非法外联”行为）；

b) 应能够对非授权设备私自联到网络的行为进行检查，并准确定出位置，对其进行有效阻断；

c) 应能够对内部网络用户私自联到外部网络的行为进行检测后准确定出位置，并对其进行有效阻断。

9.1.2.6. 网络入侵防范（G3）

a) 应在网络边界处应监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击、网络蠕虫攻击等入侵事件的发生；

b) 当检测到入侵事件时，应记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。

9.1.2.7. 恶意代码防范（G3）

a) 应在网络边界及核心业务网段处对恶意代码进行检测和清除；

b) 应维护恶意代码库的升级和检测系统的更新；

c) 应支持恶意代码防范的统一管理。

9.1.2.8. 网络设备防护（G3）

a) 应对登录网络设备的用户进行身份鉴别；

b) 应对网络上的对等实体进行身份鉴别；

c) 应对网络设备的管理员登录地址进行限制；

d) 网络设备用户的标识应唯一；

e) 身份鉴别信息应具有不易被冒用的特点，例如口令长度、复杂性和定期的更新等；

f) 应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；

g) 应具有登录失败处理功能，如：结束会话、限制非法登录次数，当网络登录连接超时，自动退出；

h) 应实现设备特权用户的权限分离，例如将管理与审计的权限分配给不同的网络设备用户。

9.1.3. 主机系统安全

9.1.3.1. 身份鉴别（S3）

a) 操作系统和数据库系统用户的身份标识应具有唯一性；

b) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；

c) 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；

d) 操作系统和数据库系统用户的身份鉴别信息应具有不易被冒用的特点，例如口令长度、复杂性和定期的更新等；

e) 应具有登录失败处理功能，如：结束会话、限制非法登录次数，当登录连接超时，自动退出；

f) 应具有鉴别警示功能；

g) 重要的主机系统应对与之相连的服务器或终端设备进行身份标识和鉴别。

9.1.3.2. 自主访问控制（S3）

a) 应依据安全策略控制主体对客体的访问；

b) 自主访问控制的覆盖范围应包括与信息安全直接相关的主体、客体及它们之间的操作；

c) 自主访问控制的粒度应达到主体为用户级，客体为文件、数据库表级；

d) 应由授权主体设置对客体访问和操作的权限；

e) 权限分离应采用最小授权原则，分别授予不同用户各自为完成自己承担任务所需的最小权限，并在他们之间形成相互制约的关系；

f) 应实现操作系统和数据库系统特权用户的权限分离；

g) 应严格限制默认用户的访问权限。

9.1.3.3. 强制访问控制（S3）

a) 应对重要信息资源和访问重要信息资源的所有主体设置敏感标记；

b) 强制访问控制的覆盖范围应包括与重要信息资源直接相关的所有主体、客体及它们之间的操作；

c) 强制访问控制的粒度应达到主体为用户级，客体为文件、数据库表级。

9.1.3.4. 安全审计（G3）

a) 安全审计应覆盖到服务器和客户端上的每个操作系统用户和数据库用户；

b) 安全审计应记录系统内重要的安全相关事件，包括重要用户行为、系统资源的异常使用和重要系统命令的使用；

c) 安全相关事件的记录应包括日期和时间、类型、主体标识、客体标识、事件的结果等；

d) 安全审计应可以根据记录数据进行分析，并生成审计报表；

e) 安全审计应可以对特定事件，提供指定方式的实时报警；

f) 审计进程应受到保护避免受到未预期的中断；

g) 审计记录应受到保护避免受到未预期的删除、修改或覆盖等。

9.1.3.5. 系统保护（G3）

a) 系统因故障或其他原因中断后，应能够以手动或自动方式恢复运行。

9.1.3.6. 剩余信息保护（S3）

a) 应保证操作系统和数据库管理系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

b) 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

9.1.3.7. 入侵防范（G3）

a) 应进行主机运行监视，包括监视主机的CPU、硬盘、内存、网络等资源的使用情况；

b) 应设定资源报警域值，以便在资源使用超过规定数值时发出报警；

c) 应进行特定进程监控，限制操作人员运行非法进程；

d) 应进行主机账户监控，限制对重要账户的添加和更改；

e) 应检测各种已知的入侵行为，记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；

f) 应能够检测重要程序完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

9.1.3.8. 恶意代码防范（G3）

a) 服务器和终端设备(包括移动设备)均应安装实时检测和查杀恶意代码的软件产品；

b) 主机系统防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；

c) 应支持恶意代码防范的统一管理。

9.1.3.9. 资源控制（A3）

a) 应限制单个用户的多重并发会话；

b) 应对最大并发会话连接数进行限制；

c) 应对一个时间段内可能的并发会话连接数进行限制；

d) 应通过设定终端接入方式、网络地址范围等条件限制终端登录；

e) 应根据安全策略设置登录终端的操作超时锁定和鉴别失败锁定，并规定解锁或终止方式；

f) 应禁止同一用户账号在同一时间内并发登录；

g) 应限制单个用户对系统资源的最大或最小使用限度；

h) 当系统的服务水平降低到预先规定的最小值时，应能检测和报警；

i) 应根据安全策略设定主体的服务优先级，根据优先级分配系统资源，保证优先级低的主体处理能力不会影响到优先级高的主体的处理能力。

9.1.4. 应用安全

9.1.4.1. 身份鉴别（S3）

a) 系统用户的身份标识应具有唯一性；

b) 应对登录的用户进行身份标识和鉴别；

c) 系统用户的身份鉴别信息应具有不易被冒用的特点，例如口令长度、复杂性和定期的更新等；

d) 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；

e) 应具有登录失败处理功能，如：结束会话、限制非法登录次数，当登录连接超时，自动退出；

f) 应具有鉴别警示功能；

g) 应用系统应及时清除存储空间中动态使用的鉴别信息。

9.1.4.2. 访问控制（S3）

a) 应依据安全策略控制用户对客体的访问；

b) 自主访问控制的覆盖范围应包括与信息安全直接相关的主体、客体及它们之间的操作；

c) 自主访问控制的粒度应达到主体为用户级，客体为文件、数据库表级；

d) 应由授权主体设置用户对系统功能操作和对数据访问的权限；

e) 应实现应用系统特权用户的权限分离，例如将管理与审计的权限分配给不同的应用系统用户；

f) 权限分离应采用最小授权原则，分别授予不同用户各自为完成自己承担任务所需的最小权限，并在它们之间形成相互制约的关系；

g) 应严格限制默认用户的访问权限。

9.1.4.3. 安全审计（G3）

a) 安全审计应覆盖到应用系统的每个用户；

b) 安全审计应记录应用系统重要的安全相关事件，包括重要用户行为、系统资源的异常使用和重要系统功能的执行等；

c) 安全相关事件的记录应包括日期和时间、类型、主体标识、客体标识、事件的结果等；

d) 安全审计应可以根据记录数据进行分析，并生成审计报表；

e) 安全审计应可以对特定事件，提供指定方式的实时报警；

f) 审计进程应受到保护避免受到未预期的中断；

g) 审计记录应受到保护避免受到未预期的删除、修改或覆盖等。

9.1.4.4. 剩余信息保护（S3）

a) 应保证用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

b) 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

9.1.4.5. 通信完整性（S3）

a) 通信双方应约定密码算法，计算通信数据报文的报文验证码，在进行通信时，双方根据校验码判断对方报文的有效性。

9.1.4.6. 通信保密性（S3）

a) 当通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；

b) 在通信双方建立连接之前，利用密码技术进行会话初始化验证；

c) 在通信过程中，应对整个报文或会话过程进行加密；

d) 应选用符合国家有关部门要求的密码算法。

9.1.4.7. 抗抵赖（G3）

a) 应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；

b) 应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

9.1.4.8. 软件容错（A3）

a) 应对通过人机接口输入或通过通信接口输入的数据进行有效性检验；

b) 应对通过人机接口方式进行的操作提供“回退”功能，即允许按照操作的序列进行回退；

c) 应有状态监测能力，当故障发生时，能实时检测到故障状态并报警；

d) 应有自动保护能力，当故障发生时，自动保护当前所有状态。

9.1.4.9. 资源控制（A3）

a) 应限制单个用户的多重并发会话；

b) 应对应用系统的最大并发会话连接数进行限制；

c) 应对一个时间段内可能的并发会话连接数进行限制；

d) 应根据安全策略设置登录终端的操作超时锁定和鉴别失败锁定，并规定解锁或终止方式；

e) 应禁止同一用户账号在同一时间内并发登录；

f) 应对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额；

g) 应根据安全属性（用户身份、访问地址、时间范围等）允许或拒绝用户建立会话连接；

h) 当系统的服务水平降低到预先规定的最小值时，应能检测和报警；

i) 应根据安全策略设定主体的服务优先级，根据优先级分配系统资源，保证优先级低的主体处理能力不会影响到优先级高的主体的处理能力。

9.1.4.10. 代码安全（G3）

a) 应制定应用程序代码编写安全规范，要求开发人员参照规范编写代码；

b) 应对应用程序代码进行代码复审，识别可能存在的恶意代码；

c) 应对应用程序代码进行安全脆弱性分析；

d) 应对应用程序代码进行穿透性测试。

9.1.5. 数据安全

9.1.5.1. 数据完整性（S3）

a) 应能够检测到系统管理数据、鉴别信息和用户数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；

b) 应能够检测到系统管理数据、鉴别信息和用户数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；

c） 应能够检测到重要程序的完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

9.1.5.2. 数据保密性（S3）

a） 网络设备、操作系统、数据库系统和应用系统的鉴别信息、敏感的系统管理数据和敏感的用户数据应采用加密或其他有效措施实现传输保密性；

b） 网络设备、操作系统、数据库系统和应用系统的鉴别信息、敏感的系统管理数据和敏感的用户数据应采用加密或其他保护措施实现存储保密性；

c） 当使用便携式和移动式设备时，应加密或者采用可移动磁盘存储敏感信息；

d） 用于特定业务通信的通信信道应符合相关的国家规定。

9.1.5.3. 数据备份和恢复（A3）

a） 应提供自动机制对重要信息进行本地和异地备份；

b） 应提供恢复重要信息的功能；

c） 应提供重要网络设备、通信线路和服务器的硬件冗余；

d） 应提供重要业务系统的本地系统级热备份。

9.2. 管理要求

9.2.1. 安全管理机构

9.2.1.1. 岗位设置

a） 应设立信息安全管理工作的职能部门，设立安全主管人、安全管理各个方面的负责人岗位，定义各负责人的职责；

b） 应设立系统管理人员、网络管理人员、安全管理人员岗位，定义各个工作岗位的职责；

c） 应成立指导和管理信息安全工作的委员会或领导小组，其最高领导应由单位主管领导委任或授权；

d） 应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

9.2.1.2. 人员配备

a） 应配备一定数量的系统管理人员、网络管理人员、安全管理人员等；

b） 应配备专职安全管理人员，不可兼任；

c） 关键岗位应定期轮岗。

9.2.1.3. 授权和审批

a） 应授权审批部门及批准人，对关键活动进行审批；

b) 应列表说明须审批的事项、审批部门和可批准人；

c) 应建立各审批事项的审批程序，按照审批程序执行审批过程；

d) 应建立关键活动的双重审批制度；

e) 不再适用的权限应及时取消授权；

f) 应定期审查、更新需授权和审批的项目；

g) 应记录授权过程并保存授权文档。

9.2.1.4. 沟通和合作

a) 应加强各类管理人员和组织内部机构之间的合作与沟通，定期或不定期召开协调会议，共同协助处理信息安全问题；

b) 信息安全职能部门应定期或不定期召集相关部门和人员召开安全工作会议，协调安全工作的实施；

c) 信息安全领导小组或者安全管理委员会定期召开例会，对信息安全工作进行指导、决策；

d) 应加强与兄弟单位、公安机关、电信公司的合作与沟通，以便在发生安全事件时能够得到及时的支持；

e) 应加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通，获取信息安全的最新发展动态，当发生紧急事件的时候能够及时得到支持和帮助；

f) 应文件说明外联单位、合作内容和联系方式；

g) 聘请信息安全专家，作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。

9.2.1.5. 审核和检查

a) 应由安全管理人员定期进行安全检查，检查内容包括用户账号情况、系统漏洞情况、系统审计情况等；

b) 应由安全管理部门组织相关人员定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；

c) 应由安全管理部门组织相关人员定期分析、评审异常行为的审计记录，发现可疑行为，形成审计分析报告，并采取必要的应对措施；

d) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；

e) 应制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。

9.2.2. 安全管理制度

9.2.2.1. 管理制度

a) 应制定信息安全工作的总体方针、政策性文件和安全策略等，说明机构安全工作的总体目标、范围、方针、原则、责任等；

b) 应对安全管理活动中的各类管理内容建立安全管理制度，以规范安全管理活动，约束人员的行为方式；

c) 应对要求管理人员或操作人员执行的日常管理操作，建立操作规程，以规范操作行为，防止操作失误；

d) 应形成由安全政策、安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系；

e) 应由安全管理职能部门定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定。

9.2.2.2. 制定和发布

a) 应在信息安全领导小组的负责下，组织相关人员制定；

b) 应保证安全管理制度具有统一的格式风格，并进行版本控制；

c) 应组织相关人员对制定的安全管理进行论证和审定；

d) 安全管理制度应经过管理层签发后按照一定的程序以文件形式发布；

e) 安全管理制度应注明发布范围，并对收发文进行登记。

9.2.2.3. 评审和修订

a) 应定期对安全管理制度进行评审和修订，对存在不足或需要改进的安全管理制度进行修订；

b) 当发生重大安全事故、出现新的安全漏洞以及技术基础结构发生变更时，应对安全管理制度进行检查、审定和修订；

c) 每个制度文档应有相应负责人或负责部门，负责对明确需要修订的制度文档的维护。

9.2.3. 人员安全管理

9.2.3.1. 人员录用

a) 应保证被录用人具备基本的专业技术水平和安全管理知识；

b) 应对被录用人的身份、背景、专业资格和资质等进行审查；

c) 应对被录用人所具备的技术技能进行考核；

d) 应对被录用人说明其角色和职责；

e) 应签署保密协议；

f) 从事关键岗位的人员应从内部人员选拔，并定期进行信用审查；

g) 从事关键岗位的人员应签署岗位安全协议。

9.2.3.2. 人员离岗

a) 应立即终止由于各种原因即将离岗的员工的所有访问权限；

b) 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；

c) 应经机构人事部门办理严格的调离手续，并承诺调离后的保密义务后方可离开。

9.2.3.3. 人员考核

a) 应对所有人员进行全面、严格的安全审查；

b) 应定期对各个岗位的人员进行安全技能及安全认知的考核；

c) 应对考核结果进行记录并保存；

d) 应对违背安全策略和规定的人员进行惩戒。

9.2.3.4. 安全意识教育和培训

a) 应对各类人员进行安全意识教育；

b) 应告知人员相关的安全责任和惩戒措施；

c) 应制定安全教育和培训计划，对信息安全基础知识、岗位操作规程等进行培训；

d) 应针对不同岗位制定不同培训计划；

e) 应对安全教育和培训的情况和结果进行记录并归档保存。

9.2.3.5. 第三方人员访问管理

a) 第三方人员应在访问前与机构签署安全责任合同书或保密协议；

b) 对重要区域的访问，须提出书面申请，批准后由专人全程陪同或监督，并记录备案；

c) 对第三方人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行。

9.2.4. 系统建设管理

9.2.4.1. 系统定级

a) 应明确信息系统划分的方法；

b) 应确定信息系统的安全等级；

c) 应以书面的形式定义确定了安全等级的信息系统的属性，包括使命、业务、网络、硬件、软件、数据、边界、人员等；

d) 应以书面的形式说明确定一个信息系统为某个安全等级的方法和理由；

e) 应组织相关部门和有关安全技术专家对信息系统的定级结果的合理性和正确性进行论证和审定；

f) 应确保信息系统的定级结果经过相关部门的批准。

9.2.4.2. 安全方案设计

a) 应根据系统的安全级别选择基本安全措施，依据风险分析的结果补充和调整安全措施；

b) 应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；

c) 应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件；

d) 应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定；

e) 应确保总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等文件必须经过批准，才能正式实施；

f) 应根据安全测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。

9.2.4.3. 产品采购

a) 应确保安全产品的使用符合国家的有关规定；

b) 应确保密码产品的使用符合国家密码主管部门的要求；

c) 应指定或授权专门的部门负责产品的采购；

d) 应制定产品采购方面的管理制度明确说明采购过程的控制方法和人员行为准则；

e) 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。

9.2.4.4. 自行软件开发

a) 应确保开发环境与实际运行环境物理分开；

b) 应确保系统开发文档由专人负责保管，系统开发文档的使用受到控制；

c） 应制定开发方面的管理制度明确说明开发过程的控制方法和人员行为准则；

d） 应确保开发人员和测试人员的分离，测试数据和测试结果受到控制；

e） 应确保提供软件设计的相关文档和使用指南；

f） 应确保对程序资源库的修改、更新、发布进行授权和批准。

9.2.4.5. 外包软件开发

a） 应与软件开发单位签订协议，明确知识产权的归属和安全方面的要求；

b） 应根据协议的要求检测软件质量；

c） 应在软件安装之前检测软件包中可能存在的恶意代码；

d） 应要求开发单位提供技术培训和服务承诺；

e） 应要求开发单位提供软件设计的相关文档和使用指南。

9.2.4.6. 工程实施

a） 应与工程实施单位签订与安全相关的协议，约束工程实施单位的行为；

b） 应指定或授权专门的人员或部门负责工程实施过程的管理；

c） 应制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程；

d） 应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则。

9.2.4.7. 测试验收

a） 应对系统进行安全性测试验收；

b） 应在测试验收前根据设计方案或合同要求等制订测试验收方案，测试验收过程中详细记录测试验收结果，形成测试验收报告；

c） 应委托公正的第三方测试单位对系统进行测试，并出具测试报告；

d） 应制定系统测试验收方面的管理制度明确说明系统测试验收的控制方法和人员行为准则；

e） 应指定或授权专门的部门负责系统测试验收的管理，并按照管理制度的要求完成系统测试验收工作；

f） 应组织相关部门和相关人员对系统测试验收报告进行审定，没有疑问后由双方签字。

9.2.4.8. 系统交付

a） 应明确系统的交接手续，并按照交接手续完成交接工作；

b） 应由系统建设方完成对委托建设方的运维技术人员的培训；

c） 应由系统建设方提交系统建设过程中的文档和指导用户进行系统运行维护的文档；

d） 应由系统建设方进行服务承诺，并提交服务承诺书，确保对系统运行维护的支持；

e） 应制定系统交付方面的管理制度明确说明系统交付的控制方法和人员行为准则；

f） 应指定或授权专门的部门负责系统交付的管理工作，并按照管理制度的要求完成系统交付工作。

9.2.4.9. 系统备案

a） 应将系统定级、系统属性等材料指定专门的人员或部门负责管理，并控制这些材料的使用；

b） 应将系统等级和系统属性等资料报系统主管部门备案；

c） 应将系统等级、系统属性、等级划分理由及其他要求的备案材料报相应公安机关备案。

9.2.4.10. 安全测评

a） 应在系统投入运行前进行安全测评，测评后符合相应等级保护标准要求的才能投入使用；

b） 应在系统运行过程中定期对系统进行安全测评，发现不符合相应等级保护标准要求的及时整改；

c） 应在系统发生变更时及时对系统进行安全测评，发现级别发生变化的及时调整级别并进行安全改造；发现不符合相应等级保护标准要求的及时整改；

d） 应选择具有国家相关技术资质和安全资质的测评单位进行安全测评；

e） 应与测评单位签订与安全相关的协议，约束测评单位的行为；

f） 应指定或授权专门的人员或部门负责安全测评的管理。

9.2.4.11. 安全服务商选择

a） 应确保安全服务商的选择符合国家的有关规定。

9.2.5. 系统运维管理

9.2.5.1. 环境管理

a） 应对机房供配电、空调、温湿度控制等设施指定专人或专门的部门定期进行维护管理；

b） 应配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理；

c） 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；

d) 加强对办公环境的保密性管理，包括如工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等；

e) 应有指定的部门负责机房安全，并配置电子门禁系统，对机房来访人员实行登记记录和电子记录双重备案管理；

f) 应对办公环境的人员行为，如工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等作出规定。

9.2.5.2. 资产管理

a) 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为；

b) 应编制并保存与信息系统相关的资产、资产所属关系、安全级别和所处位置等信息的资产清单；

c) 应根据资产的重要程度对资产进行定性赋值和标识管理，根据资产的价值选择相应的管理措施；

d) 应确定信息分类与标识的原则和方法，并对信息的使用、传输和存储作出规定。

9.2.5.3. 介质管理

a) 应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定；

b) 应有介质的归档和查询记录，并对存档介质的目录清单定期盘点；

c) 对于需要送出维修或销毁的介质，应首先清除介质中的敏感数据，防止信息的非法泄漏；

d) 应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同；

e) 应根据所承载数据和软件的重要程度对介质进行分类和标识管理，并实行存储环境专人管理；

f) 应对介质的物理传输过程中人员选择、打包、交付等情况进行控制；

g) 应对存储介质的使用过程、送出维修以及销毁进行严格的管理，保密性较高的信息存储介质未经批准不得自行销毁；

h) 必要时应对重要介质的数据和软件采取加密存储，对带出工作环境的存储介质进行内容加密和监控管理；

i) 应对存放在介质库中的介质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。

9.2.5.4. 设备管理

a) 应对信息系统相关的各种设备、线路等指定专人或专门的部门定期进行维护管理；

b) 应对信息系统的各种软硬件设备的选型、采购、发放或领用等过程建立基于申报、审批和专人负责的管理规定；

c) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理；

d) 应对带离机房或办公地点的信息处理设备进行控制；

e) 应按操作规程实现服务器的启动/停止、加电/断电等操作，加强对服务器操作的日志文件管理和监控管理，并对其定期进行检查；

f) 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等；

g) 应在安全管理机构统一安全策略下对服务器进行系统配置和服务设定，并实施配置管理。

9.2.5.5. 监控管理

a) 应进行主机运行监视，包括监视主机的CPU、硬盘、内存、网络等资源的使用情况；

b) 应对分散或集中的安全管理系统的访问授权、操作记录、日志等方面进行有效管理；

c) 应严格管理运行过程文档，其中包括责任书、授权书、许可证、各类策略文档、事故报告处理文档、安全配置文档、系统各类日志等，并确保文档的完整性和一致性。

9.2.5.6. 网络安全管理

a) 应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；

b) 应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；

c) 应进行网络系统漏洞扫描，对发现的网络系统安全漏洞进行及时的修补；

d) 应保证所有与外部系统的连接均应得到授权和批准；

e) 应建立网络安全管理制度，对网络安全配置、网络用户以及日志等方面作出规定；

f) 应对网络设备的安全策略、授权访问、最小服务、升级与打补丁、维护记录、日志以及配置文件的生成、备份、变更审批、符合性检查等方面做出具体规定；

g) 应规定网络审计日志的保存时间以便为可能的安全事件调查提供支持；

h) 应明确各类用户的责任、义务和风险，并按照机构制定的审查和批准程序建立用户和分配权限，定期检查用户实际权限与分配权限的符合性；

i) 应对日志的备份、授权访问、处理、保留时间等方面做出具体规定，使用统一的网络时间，以确保日志记录的准确；

j) 应通过身份鉴别、访问控制等严格的规定限制远程管理账户的操作权限和登录行为；

k) 应定期检查违反规定拨号上网或其他违反网络安全策略的行为。

9.2.5.7. 系统安全管理

a) 应指定专人对系统进行管理，删除或者禁用不使用的系统缺省账户；

b) 应制定系统安全管理制度，对系统安全配置、系统账户以及审计日志等方面作出规定；

c) 应对能够使用系统工具的人员及数量进行限制和控制；

d) 应定期安装系统的最新补丁程序，并根据厂家提供的可能危害计算机的漏洞进行及时修补，并在安装系统补丁前对现有的重要文件进行备份；

e) 应根据业务需求和系统安全分析确定系统的访问控制策略，系统访问控制策略用于控制分配信息系统、文件及服务的访问权限；

f) 应对系统账户进行分类管理，权限设定应当遵循最小授权要求；

g) 应对系统的安全策略、授权访问、最小服务、升级与打补丁、维护记录、日志以及配置文件的生成、备份、变更审批、符合性检查等方面做出具体规定；

h) 应规定系统审计日志的保存时间以便为可能的安全事件调查提供支持；

i) 应进行系统漏洞扫描，对发现的系统安全漏洞进行及时的修补；

j) 应明确各类用户的责任、义务和风险，对系统账户的登记造册、用户名分配、初始口令分配、用户权限及其审批程序、系统资源分配、注销等作出规定；

k) 应对于账户安全管理的执行情况进行检查和监督，定期审计和分析用户账户的使用情况，对发现的问题和异常情况进行相关处理。

9.2.5.8. 恶意代码防范管理

a) 应提高所有用户的防病毒意识，告知及时升级防病毒软件；

b) 应在读取移动存储设备（如软盘、移动硬盘、光盘）上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也要进行病毒检查；

c） 应指定专人对网络和主机的进行恶意代码检测并保存检测记录；

d） 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确管理规定；

e） 应建立恶意代码集中防护的安全管理中心，确保整个网络统一配置、统一升级、统一控制；

f） 应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。

9.2.5.9. 密码管理

a） 应建立密码使用管理制度，密码算法和密钥的使用应符合国家密码管理规定。

9.2.5.10. 变更管理

a） 确认系统中要发生的变更，并制定变更方案；

b） 建立变更管理制度，重要系统变更前，应向主管领导申请，变更和变更方案经过评审、审批后方可实施变更；

c） 系统变更情况应向所有相关人员通告；

d） 应建立变更控制的申报和审批文件化程序，变更影响分析应文档化，变更实施过程应记录，所有文档记录应妥善保存；

e） 中止变更并从失败变更中恢复程序应文档化，应明确过程控制方法和人员职责，必要时恢复过程应经过演练。

9.2.5.11. 备份与恢复管理

a） 应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b） 应规定备份信息的备份方式（如增量备份或全备份等）、备份频度（如每日或每周等）、存储介质、保存期等；

c） 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略应指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；

d） 应指定相应的负责人定期维护和检查备份及冗余设备的状况，确保需要接入系统时能够正常运行；

e） 应建立控制数据备份和恢复过程的程序，备份过程应记录，所有文件和记录应妥善保存；

f) 应根据系统级备份所采用的方式和产品，建立备份及冗余设备的安装、配置、启动、操作及维护过程控制的程序，记录设备运行过程状况，所有文件和记录应妥善保存；

g) 应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

9.2.5.12. 安全事件处置

a) 所有用户均有责任报告自己发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；

b) 应制定安全事件报告和处置管理制度，规定安全事件的现场处理、事件报告和后期恢复的管理职责；

c) 应分析信息系统的类型、网络连接特点和信息系统用户特点，了解本系统和同类系统已发生的安全事件，识别本系统需要防止发生的安全事件，事件可能来自攻击、错误、故障、事故或灾难；

d) 应根据国家相关管理部门对计算机安全事件等级划分方法，根据安全事件在本系统产生的影响，将本系统计算机安全事件进行等级划分；

e) 应制定的安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；

f) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存；

g) 对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。

9.2.5.13. 应急预案管理

a) 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程和事后教育和培训等内容；

b) 应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；

c) 应对系统相关的人员进行培训使之了解如何及何时使用应急预案中的控制手段及恢复策略，对应急预案的培训至少每年举办一次；

d) 应急预案应定期演练，根据不同的应急恢复内容，确定演练的周期；

e) 应规定应急预案需要定期审查和根据实际情况更新内容，并按照执行。

10 第 4 级基本要求

10.1. 技术要求

10.1.1. 物理安全

10.1.1.1. 物理位置的选择（G4）

a) 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；

b) 机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁；

c) 机房场地应当避开强电场、强磁场、强震动源、强噪声源、重度环境污染、易发生火灾、水灾、易遭受雷击的地区。

10.1.1.2. 物理访问控制（G4）

a) 机房出入口应有专人值守并配置电子门禁系统，鉴别进入的人员身份并登记在案；

b) 应批准进入机房的来访人员，限制和监控其活动范围；

c) 应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过度区域；

d) 应对重要区域配置第二道电子门禁系统，控制、鉴别和记录进入的人员身份并监控其活动。

10.1.1.3. 防盗窃和防破坏（G4）

a) 应将主要设备放置在物理受限的范围内；

b) 应对设备或主要部件进行固定，并设置明显的不易除去的标记；

c) 应将通信线缆铺设在隐蔽处，如铺设在地下或管道中等；

d) 应对介质分类标识，存储在介质库或档案室中；

e) 设备或存储介质携带出工作环境时，应受到监控和内容加密；

f) 应利用光、电等技术设置机房的防盗报警系统，以防进入机房的盗窃和破坏行为；

g) 应对机房设置监控报警系统。

10.1.1.4. 防雷击（G4）

a) 机房建筑应设置避雷装置；

b) 应设置防雷保安器，防止感应雷；

c) 应设置交流电源地线。

10.1.1.5. 防火（G4）

a) 应设置火灾自动消防系统，自动检测火情、自动报警，并自动灭火；

b) 机房及相关的工作房间和辅助房，其建筑材料应具有耐火等级；

c) 机房采取区域隔离防火措施，将重要设备与其他设备隔离开。

10.1.1.6. 防水和防潮（G4）

a) 水管安装，不得穿过屋顶和活动地板下；

b) 应对穿过墙壁和楼板的水管增加必要的保护措施，如设置套管；

c) 应采取措施防止雨水通过屋顶和墙壁渗透；

d) 应采取措施防止室内水蒸气结露和地下积水的转移与渗透；

e) 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

10.1.1.7. 防静电（G4）

a) 应采用必要的接地防静电措施；

b) 应采用防静电地板；

c) 应采用静电消除器等装置，减少静电的产生。

10.1.1.8. 温湿度控制（G4）

a) 应设置恒温恒湿系统，使机房温、湿度的变化在设备运行所允许的范围之内。

10.1.1.9. 电力供应（A4）

a) 计算机系统供电应与其他供电分开；

b) 应设置稳压器和过电压防护设备；

c) 应提供短期的备用电力供应（如：UPS设备）；

d) 应设置冗余或并行的电力电缆线路；

e) 应建立备用供电系统（如备用发电机），以备常用供电系统停电时启用。

10.1.1.10. 电磁防护（S4）

a) 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；

b) 电源线和通信线缆应隔离，避免互相干扰；

c) 对重要设备和磁介质实施电磁屏蔽；

d) 对机房实施电磁屏蔽。

10.1.2. 网络安全

10.1.2.1. 结构安全与网段划分（G4）

a) 网络设备的业务处理能力应具备冗余空间，要求满足业务高峰期需要；

b) 应设计和绘制与当前运行情况相符的网络拓扑结构图；

c) 应根据机构业务的特点，在满足业务高峰期需要的基础上，合理设计网络带宽；

d) 应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；

e) 应根据各部门的工作职能、重要性、所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配IP地址段；

f) 重要网段应采取网络层地址与数据链路层地址绑定措施，防止地址欺骗；

g) 应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要信息资产主机。

10.1.2.2. 网络访问控制（G4）

a) 应不允许数据带通用协议通过；

b) 应禁止便携式和移动式设备接入网络。

10.1.2.3. 拨号访问控制（G4）

a) 应不开放远程拨号访问功能（如远程拨号用户或移动VPN用户）。

10.1.2.4. 网络安全审计（G4）

a) 对网络系统中的网络设备运行状况、网络流量、用户行为等进行全面的监测、记录；

b) 对于每一个事件，其审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功，及其他与审计相关的信息；

c) 安全审计应可以根据记录数据进行分析，并生成审计报表；

d) 安全审计应可以对特定事件，提供指定方式的实时报警；

e) 审计记录应受到保护避免受到未预期的删除、修改或覆盖等；

f) 安全审计应能跟踪监测到可能的安全侵害事件，并终止违规进程；

g) 审计员应能够定义审计跟踪极限的阈值，当存储空间接近极限时，能采取必要的措施（如报警并导出），当存储空间被耗尽时，终止可审计事件的发生；

h) 安全审计应根据信息系统的统一安全策略，实现集中审计；

i) 网络设备时钟应与时钟服务器时钟保持同步。

10.1.2.5. 边界完整性检查（S4）

a) 应能够检测内部网络中出现的内部用户未通过准许私自联到外部网络的行为（即“非法外联”行为）；

b) 应能够对非授权设备私自联到网络的行为进行检查，并准确定位、有效阻断；

c) 应能够对内部网络用户私自联到外部网络的行为进行检查后准确定出位置，并对其进行有效阻断；

d) 应能够根据信息流控制策略和信息流的敏感标记，阻止重要信息的流出。

10.1.2.6. 网络入侵防范（G4）

a) 在网络边界处应监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击、网络蠕虫攻击等入侵事件的发生；

b) 当检测到入侵事件时，应记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间等，并发出安全警告（如可采取屏幕实时提示、E-mail告警、声音告警等几种方式）及自动采取相应动作。

10.1.2.7. 恶意代码防范（G4）

a) 应在网络边界及核心业务网段处对恶意代码进行检测和清除；

b) 应维护恶意代码库的升级和检测系统的更新；

c) 应支持恶意代码防范的统一管理。

10.1.2.8. 网络设备防护（G4）

a) 应对登录网络设备的用户进行身份鉴别；

b) 应对网络上的对等实体进行身份鉴别；

c) 应对网络设备的管理员登录地址进行限制；

d) 网络设备用户的标识应唯一；

e) 身份鉴别信息应具有不易被冒用的特点，例如口令长度、复杂性和定期的更新等；

f) 应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；

g) 网络设备用户的身份鉴别信息至少有一种应是不可伪造的，例如以公私钥对、生物特征等作为身份鉴别信息；

h) 应具有登录失败处理功能，如：结束会话、限制非法登录次数，当网络登录连接超时，自动退出；

i) 应实现设备特权用户的权限分离，例如将管理与审计的权限分配给不同的网络设备用户。

10.1.3. 主机系统安全

10.1.3.1. 身份鉴别（S4）

a) 操作系统和数据库系统用户的身份标识应具有唯一性；

b) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；

c) 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；

d) 操作系统和数据库系统用户的身份鉴别信息应具有不易被冒用的特点，例如口令长度、复杂性和定期的更新等；

e) 操作系统和数据库系统用户的身份鉴别信息至少有一种应是不可伪造的，例如以公私钥对、生物特征等作为身份鉴别信息；

f) 应具有登录失败处理功能，如：结束会话、限制非法登录次数，当登录连接超时，自动退出；

g) 应具有鉴别警示功能；

h) 重要的主机系统应对与之相连的服务器或终端设备进行身份标识和鉴别。

10.1.3.2. 自主访问控制（S4）

a) 应依据安全策略控制用户对客体的访问；

b) 自主访问控制的覆盖范围应包括与信息安全直接相关的主体、客体及它们之间的操作；

c) 自主访问控制的粒度应达到主体为用户级，客体为文件、数据库表/记录、字段级；

d) 应由授权主体设置对客体访问和操作的权限；

e) 应实现操作系统和数据库系统特权用户的权限分离；

f) 权限分离应采用最小授权原则，分别授予不同用户各自为完成自己承担任务所需的最小权限，并在他们之间形成相互制约的关系；

g) 应禁止默认用户访问。

10.1.3.3. 强制访问控制（S4）

a) 应对重要信息资源和访问重要信息资源的所有主体设置敏感标记；

b) 强制访问控制的覆盖范围应包括与重要信息资源直接相关的所有主体、客体及它们之间的操作；

c) 强制访问控制的粒度应达到主体为用户级，客体为文件、数据库表/记录、字段级。

10.1.3.4. 可信路径（S4）

a) 在用户进行初始登录和/或鉴别时，系统应在它与用户之间建立一条安全的信息传输通路。

10.1.3.5. 安全审计（G4）

a) 安全审计应覆盖到服务器和客户端上的所有用户；

b) 安全审计应记录系统内重要的安全相关事件，包括重要用户行为、系统资源的异常使用和重要系统命令的使用；

c) 安全相关事件的记录应包括日期和时间、类型、主体标识、客体标识、客体敏感标记、事件的结果等；

d) 安全审计应可以根据记录数据进行分析，并生成审计报表；

e) 安全审计应可以对特定事件，提供指定方式的实时报警；

f) 审计进程应受到保护避免受到未预期的中断；

g) 审计记录应受到保护避免受到未预期的删除、修改或覆盖等；

h) 安全审计应能跟踪监测到可能的安全侵害事件，并终止违规进程；

i) 审计员应能够定义审计跟踪极限的阈值，当存储空间接近极限时，能采取必要的措施（如报警并导出），当存储空间被耗尽时，终止可审计事件的发生；

j) 安全审计应根据信息系统的统一安全策略，实现集中审计；

k) 系统设备时钟应与时钟服务器时钟保持同步。

10.1.3.6. 系统保护（G4）

a) 系统因故障或其他原因中断后，应能够以手动或自动方式恢复运行；

b) 应对被保护存储单元的访问和操作权限加以控制，当发生对存储单元的未授权执行行为时，系统应能及时报警或者中断执行行为。

10.1.3.7. 剩余信息保护（S4）

a) 应保证操作系统和数据库管理系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

b) 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

10.1.3.8. 入侵防范（G4）

a) 应进行主机运行监视，包括监视主机的CPU、硬盘、内存、网络等资源的使用情况；

b) 应设定资源报警域值，以便在资源使用超过规定数值时发出报警；

c) 应进行特定进程监控，限制操作人员运行非法进程；

d) 应进行主机账户监控，限制对重要账户的添加和更改；

e) 应检测各种已知的入侵行为，记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；

f) 主机系统应根据安全策略阻止某些指定的入侵事件；

g) 应能够检测重要程序完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

10.1.3.9. 恶意代码防范（G4）

a) 服务器和终端设备(包括移动设备)均应安装实时检测和查杀恶意代码的软件产品；

b) 主机系统防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；

c) 应支持恶意代码防范的统一管理。

10.1.3.10. 资源控制（A4）

a) 应限制单个用户的多重并发会话；

b) 应对最大并发会话连接数进行限制；

c) 应对一个时间段内可能的并发会话连接数进行限制；

d) 应通过设定终端接入方式、网络地址范围等条件限制终端登录；

e) 应根据安全策略设置登录终端的操作超时锁定和鉴别失败锁定，并规定解锁或终止方式；

f) 应禁止同一用户 在同一时间内并发登录；

g) 应限制单个用户对系统资源的最大或最小使用限度；

h) 当系统的服务水平降低到预先规定的最小值时，应能检测和报警；

i) 应根据安全策略设定主体的服务优先级，根据优先级分配系统资源，保证优先级低的主体处理能力不会影响到优先级高的主体的处理能力。

10.1.4. 应用安全

10.1.4.1. 身份鉴别（S4）

a) 系统用户的身份标识应具有唯一性；

b) 应对登录的用户进行身份标识和鉴别；

c) 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；

d) 系统用户的身份鉴别信息应具有不易被冒用的特点，例如口令长度、复杂性和定期的更新等；

e) 系统用户的身份鉴别信息至少有一种应是不可伪造的，例如以公私钥对、生物特征等作为身份鉴别信息；

f) 应具有登录失败处理功能，如：结束会话、限制非法登录次数，当登录连接超时自动退出；

g) 应具有鉴别警示功能；

h) 应用系统应及时清除存储空间中动态使用的鉴别信息。

10.1.4.2. 访问控制（S4）

a) 应依据安全策略控制用户对客体的访问；

b) 自主访问控制的覆盖范围应包括与信息安全直接相关的主体、客体及它们之间的操作；

c) 自主访问控制的粒度应达到主体为用户级，客体为文件、数据库表级；

d) 应由授权主体设置用户对应用系统功能操作和对数据访问的权限；

e) 应实现应用系统特权用户的权限分离，例如将管理与审计的权限分配给不同的应用系统用户；

f) 权限分离应采用最小授权原则，分别授予不同用户各自为完成自己承担任务所需的最小权限，并在它们之间形成相互制约的关系；

g) 应禁止默认用户访问；

h) 主体和客体具有安全标记，通过比较安全标签来确定是授予还是拒绝主体对客体的访问。

10.1.4.3. 安全审计（G4）

a) 安全审计应覆盖到应用系统的每个用户；

b) 安全审计应记录应用系统重要的安全相关事件，包括重要用户行为、系统资源的异常使用和重要系统功能的执行等；

c) 安全相关事件的记录应包括日期和时间、类型、主体标识、客体标识、客体敏感标记、事件的结果等；

d) 安全审计应可以根据记录数据进行分析，并生成审计报表；

e) 安全审计应可以对特定事件，提供指定方式的实时报警；

f) 审计进程应受到保护避免受到未预期的中断；

g) 审计记录应受到保护避免受到未预期的删除、修改或覆盖等；

h) 安全审计应能跟踪监测到可能的安全侵害事件，并终止违规进程；

i) 安全审计应根据系统的统一安全策略，实现集中审计。

10.1.4.4. 剩余信息保护（S4）

a) 应保证用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

b) 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

10.1.4.5. 通信完整性（S4）

a) 通信双方应约定密码算法，计算通信数据报文的报文验证码，在进行通信时，双方根据校验码判断对方报文的有效性。

10.1.4.6. 通信保密性（S4）

a) 当通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；

b) 在通信双方建立连接之前，利用密码技术进行会话初始化验证；

c) 在通信过程中，应对整个报文或会话过程进行加密；

d) 应选用符合国家有关部门要求的密码算法；

e) 应基于硬件化的设备，产生密钥，进行加解密运算。

10.1.4.7. 抗抵赖（G4）

a) 应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；

b) 应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能；

10.1.4.8. 软件容错（A4）

a) 应对通过人机接口输入或通过通信接口输入的数据进行有效性检验；

b) 应对通过人机接口方式进行的操作提供“回退”功能，即允许按照操作的序列进行回退；

c) 应有状态监测能力，当故障发生时，能实时检测到故障状态并报警；

d) 应有自动保护能力，当故障发生时，自动保护当前所有状态；

e) 应有自动恢复能力，当故障发生时，立即启动新的进程，恢复原来的工作状态。

10.1.4.9. 资源控制（A4）

a) 应限制单个用户的多重并发会话；

b) 应对最大并发会话连接数进行限制；

c) 应对一个时间段内可能的并发会话连接数进行限制；

d) 应根据安全策略设置登录终端的操作超时锁定和鉴别失败锁定，并规定解锁或终止方式；

e) 应禁止同一用户账号在同一时间内并发登录；

f) 应对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额；

g) 应根据安全属性（用户身份、访问地址、时间范围等）允许或拒绝用户建立会话连接；

h) 当系统的服务水平降低到预先规定的最小值时，应能检测和报警；

i） 应确定访问用户或请求进程的优先级，对全部资源采用优先服务机制。

10.1.4.10. 代码安全（G4）

a） 应制定应用程序代码编写安全规范，要求开发人员参照规范编写代码；

b） 应对应用程序代码进行代码复审，识别可能存在的恶意代码；

c） 应对应用程序代码进行安全脆弱性分析；

d） 应对应用程序代码进行穿透性测试；

e） 应对应用程序代码进行严格的代码复审，识别可能存在的隐蔽信道。

10.1.5. 数据安全

10.1.5.1. 数据完整性（S4）

a） 应能够检测到系统管理数据、鉴别信息和用户数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；

b） 应能够检测到系统管理数据、鉴别信息和用户数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；

c） 应能够检测到重要程序的完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；

d） 应为重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用通信协议的攻击，破坏数据的完整性。

10.1.5.2. 数据保密性（S4）

a） 网络设备、操作系统、数据库系统和应用系统的鉴别信息、敏感的系统管理数据和敏感的用户数据应采用加密或其他有效措施实现传输保密性；

b） 网络设备、操作系统、数据库系统和应用系统的鉴别信息、敏感的系统管理数据和敏感的用户数据应采用加密或其他保护措施实现存储保密性；

c） 当使用便携式和移动式设备时，应加密或者采用可移动磁盘存储敏感信息；

d） 用于特定业务通信的通信信道应符合相关的国家规定；

e） 网络设备、操作系统、数据库管理系统和应用系统应为重要通信提供专用协议或安全通信协议服务，避免来自基于通用协议的攻击，破坏数据保密性。

10.1.5.3. 数据备份和恢复（A4）

a） 应提供自动机制实现数据实时本地和异地备份；

b） 应提供恢复数据的功能；

c） 应提供重要网络设备、通信线路和服务器的硬件冗余；

d) 应提供重要业务系统的本地和异地系统级热备份；

e) 应提供自动机制在灾难发生时实现自动业务切换和恢复。

10.2. 管理要求

10.2.1. 安全管理机构

10.2.1.1. 岗位设置

a) 应设立信息安全管理工作的职能部门，设立安全主管人、安全管理各个方面的负责人岗位，定义各负责人的职责；

b) 应设立系统管理人员、网络管理人员、安全管理人员岗位，定义各个工作岗位的职责；

c) 应成立指导和管理信息安全工作的委员会或领导小组，其最高领导应由单位主管领导委任或授权；

d) 应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

10.2.1.2. 人员配备

a) 应配备一定数量的系统管理人员、网络管理人员、安全管理人员等；

b) 应配备专职安全管理人员，不可兼任；

c) 关键区域或部位的安全管理人员应按照机要人员条件配备；

d) 关键岗位应定期轮岗；

e) 关键事务应配备多人共同管理。

10.2.1.3. 授权和审批

a) 应授权审批部门及批准人，对关键活动进行审批；

b) 应列表说明须审批的事项、审批部门和可批准人；

c) 应建立各审批事项的审批程序，按照审批程序执行审批过程；

d) 应建立关键活动的双重审批制度；

e) 不再适用的权限应及时取消授权；

f) 应定期审查、更新需授权和审批的项目；

g) 应记录授权过程并保存授权文档。

10.2.1.4. 沟通和合作

a) 应加强各类管理人员和组织内部机构之间的合作与沟通，定期或不定期召开协调会议，共同协助处理信息安全问题；

b) 信息安全职能部门应定期或不定期召集相关部门和人员召开安全工作会议，协调安全工作的实施；

c) 信息安全领导小组或者安全管理委员会定期召开例会，对信息安全工作进行指导、决策；

d) 应加强与兄弟单位、公安机关、电信公司的合作与沟通，以便在发生安全事件时能够得到及时的支持；

e) 应加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通，获取信息安全的最新发展动态，当发生紧急事件的时候能够及时得到支持和帮助；

f) 应文件说明外联单位、合作内容和联系方式；

g) 聘请信息安全专家，作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。

10.2.1.5. 审核和检查

a) 应由安全管理人员定期进行安全检查，检查内容包括用户账号情况、系统漏洞情况、系统审计情况等；

b) 应由安全管理部门组织相关人员定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；

c) 应由安全管理部门组织相关人员定期分析、评审异常行为的审计记录，发现可疑行为，形成审计分析报告，并采取必要的应对措施；

d) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；

e) 应制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。

10.2.2. 安全管理制度

10.2.2.1. 管理制度

a) 应制定信息安全工作的总体方针、政策性文件和安全策略等，说明机构安全工作的总体目标、范围、方针、原则、责任等；

b) 应对安全管理活动中的各类管理内容建立安全管理制度，以规范安全管理活动，约束人员的行为方式；

c) 应对要求管理人员或操作人员执行的日常管理操作，建立操作规程，以规范操作行为，防止操作失误；

d) 应形成由安全政策、安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系；

e) 应由安全管理职能部门定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定。

10.2.2.2. 制定和发布

a) 应在信息安全领导小组的负责下，组织相关人员制定；

b) 应保证安全管理制度具有统一的格式风格，并进行版本控制；

c) 应组织相关人员对制定的安全管理进行论证和审定；

d) 安全管理制度应经过管理层签发后按照一定的程序以文件形式发布；

e) 安全管理制度应注明发布范围，并对收发文进行登记；

f) 安全管理制度应注明密级，进行密级管理。

10.2.2.3. 评审和修订

a) 应定期对安全管理制度进行评审和修订，对存在不足或需要改进的安全管理制度进行修订；

b) 当发生重大安全事故、出现新的安全漏洞以及技术基础结构发生变更时，应对安全管理制度进行检查、审定和修订；

c) 每个制度文档应有相应负责人或负责部门，负责对明确需要修订的制度文档的维护；

d) 评审和修订的操作范围应考虑安全管理制度的相应密级。

10.2.3. 人员安全管理

10.2.3.1. 人员录用

a) 应保证被录用人具备基本的专业技术水平和安全管理知识；

b) 应对被录用人的身份、背景、专业资格和资质等进行审查；

c) 应对被录用人所具备的技术技能进行考核；

d) 应对被录用人说明其角色和职责；

e) 应签署保密协议；

f) 从事关键岗位的人员应从内部人员选拔，并定期进行信用审查；

g) 对从事关键岗位的人员应签署岗位安全协议。

10.2.3.2. 人员离岗

a) 应立即终止由于各种原因即将离岗的员工的所有访问权限；

b) 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；

c) 应经机构人事部门办理严格的调离手续，并承诺调离后的保密义务后方可离开；

d) 关键岗位的人员调离应按照机要人员的有关管理办法进行。

10.2.3.3. 人员考核

a) 应对所有人员实施全面、严格的安全审查；

b) 应定期对各个岗位的人员进行安全技能及安全认知的考核；

c) 应对考核结果进行记录并保存；

d) 应对违背安全策略和规定的人员进行惩戒。

10.2.3.4. 安全意识教育和培训

a) 应对各类人员进行安全意识教育；

b) 应告知人员相关的安全责任和惩戒措施；

c) 应制定安全教育和培训计划，对信息安全基础知识、岗位操作规程等进行培训；

d) 应针对不同岗位制定不同培训计划；

e) 应对安全教育和培训的情况和结果进行记录并归档保存。

10.2.3.5. 第三方人员访问管理

a) 第三方人员应在访问前与机构签署安全责任合同书或保密协议；

b) 对重要区域的访问，须提出书面申请，批准后由专人全程陪同或监督，并记录备案；

c) 对第三方人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行；

d) 对关键区域不允许第三方人员访问。

10.2.4. 系统建设管理

10.2.4.1. 系统定级

a) 应明确信息系统划分的方法；

b) 应确定信息系统的安全等级；

c) 应以书面的形式定义确定了安全等级的信息系统的属性，包括使命、业务、网络、硬件、软件、数据、边界、人员等；

d) 应以书面的形式说明确定一个信息系统为某个安全等级的方法和理由；

e) 应组织相关部门和有关安全技术专家对信息系统的定级结果的合理性和正确性进行论证和审定；

f) 应确保信息系统的定级结果经过相关部门的批准。

10.2.4.2. 安全方案设计

a) 应根据系统的安全级别选择基本安全措施，依据风险分析的结果补充和调整安全措施；

b) 应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；

c) 应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件；

d) 应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定；

e) 应确保总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等文件必须经过批准，才能正式实施；

f) 应根据安全测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。

10.2.4.3. 产品采购

a) 应确保安全产品的使用符合国家的有关规定；

b) 应确保密码产品的使用符合国家密码主管部门的要求；

c) 应指定或授权专门的部门负责产品的采购；

d) 应制定产品采购方面的管理制度明确说明采购过程的控制方法和人员行为准则；

e) 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单；

f) 应对重要部位的产品委托专业测评单位进行专项测试，根据测试结果选用产品。

10.2.4.4. 自行软件开发

a) 应确保开发环境与实际运行环境物理分开；

b) 应确保系统开发文档由专人负责保管，系统开发文档的使用受到控制；

c) 应制定开发方面的管理制度明确说明开发过程的控制方法和人员行为准则；

d) 应确保开发人员和测试人员的分离，测试数据和测试结果受到控制；

e) 应确保提供软件设计的相关文档和使用指南；

f) 应确保对程序资源库的修改、更新、发布进行授权和批准；

g) 应确保开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。

10.2.4.5. 外包软件开发

a) 应与软件开发单位签订协议，明确知识产权的归属和安全方面的要求；

b) 应根据协议的要求检测软件质量；

c) 应在软件安装之前检测软件包中可能存在的恶意代码；

d) 应要求开发单位提供技术培训和服务承诺；

e) 应要求开发单位提供软件设计的相关文档和使用指南；

f) 应要求开发单位提供软件源代码，并审查软件中可能存在的后门。

10.2.4.6. 工程实施

a) 应与工程实施单位签订与安全相关的协议，约束工程实施单位的行为；

b) 应指定或授权专门的人员或部门负责工程实施过程的管理；

c) 应制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程；

d) 应制定工程实施方面的管理制度明确说明实施过程的控制方法和人员行为准则；

e) 应通过工程监理控制项目的实施过程。

10.2.4.7. 测试验收

a) 应对系统进行安全性测试验收；

b) 应在测试验收前根据设计方案或合同要求等制订测试验收方案，测试验收过程中详细记录测试验收结果，形成测试验收报告；

c) 应委托公正的第三方测试单位对系统进行测试，并出具测试报告；

d) 应制定系统测试验收方面的管理制度明确说明系统测试验收的控制方法和人员行为准则；

e) 应指定或授权专门的部门负责系统测试验收的管理，并按照管理制度的要求完成系统测试验收工作；

f) 应组织相关部门和相关人员对系统测试验收报告进行审定，没有疑问后由双方签字。

10.2.4.8. 系统交付

a) 应明确系统的交接手续，并按照交接手续完成交接工作；

b) 应由系统建设方完成对委托建设方的运维技术人员的培训；

c) 应由系统建设方提交系统建设过程中的文档和指导用户进行系统运行维护的文档；

d) 应由系统建设方进行服务承诺，并提交服务承诺书，确保对系统运行维护的支持；

e) 应制定系统交付方面的管理制度明确说明系统交付的控制方法和人员行为准则；

f) 应指定或授权专门的部门负责系统交付的管理工作，并按照管理制度的要求完成系统交付工作。

10.2.4.9. 系统备案

a) 应将系统定级、系统属性等材料指定专门的人员或部门负责管理，并控制这些材料的使用；

b) 应将系统等级和系统属性等资料报系统主管部门备案；

c) 应将系统等级、系统属性、等级划分理由及其他要求的备案材料报相应公安机关备案。

10.2.4.10. 安全测评

a) 应在系统投入运行前进行安全测评，测评后符合相应等级保护标准要求的才能投入使用；

b) 应在系统运行过程中定期对系统进行安全测评，发现不符合相应等级保护标准要求的及时整改；

c) 应在系统发生变更时及时对系统进行安全测评，发现级别发生变化的及时调整级别并进行安全改造；发现不符合相应等级保护标准要求的及时整改；

d) 应选择具有国家相关技术资质和安全资质的测评单位进行安全测评；

e) 应与测评单位签订与安全相关的协议，约束测评单位的行为；

f) 应指定或授权专门的人员或部门负责安全测评的管理。

10.2.4.11. 安全服务商选择

a) 应确保安全服务商的选择符合国家的有关规定。

10.2.5. 系统运维管理

10.2.5.1. 环境管理

a) 应对机房供配电、空调、温湿度控制等设施指定专人或专门的部门定期进行维护管理；

b) 应配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理；

c) 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；

d) 加强对办公环境的保密性管理，包括如工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等；

e) 应对办公环境的人员行为，如工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等作出规定；

f) 应有指定的部门负责机房安全，并配置电子门禁系统和专职警卫，对机房来访人员实行登记记录、电子记录和监控录像三重备案管理；

g) 应对机房和办公环境实行统一策略的安全管理，出入人员应经过相应级别授权，对进入重要安全区域的活动行为应实时监视和记录。

10.2.5.2. 资产管理

a) 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为；

b) 应编制并保存与信息系统相关的资产、资产所属关系、安全级别和所处位置等信息的资产清单；

c) 应根据资产的重要程度对资产进行定性赋值和标识管理，根据资产的价值选择相应的管理措施；

d) 应确定信息分类与标识的原则和方法，并对信息的使用、传输和存储作出规定；

e) 应根据信息分类与标识的原则和方法，在信息的存储、传输等过程中对信息进行标识。

10.2.5.3. 介质管理

a) 应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定；

b) 应有介质的归档和查询记录，并对存档介质的目录清单定期盘点；

c) 对于需要送出维修或销毁的介质，应采用多次读写覆盖，清除介质中的敏感或秘密数据，防止信息的非法泄漏，对无法执行删除操作的受损介质必须销毁；

d) 应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同；

e) 应根据所承载数据和软件的重要程度对介质进行分类和标识管理，并实行存储环境专人管理；

f) 应对介质的物理传输过程中人员选择、打包、交付等情况进行控制；

g) 应对存储介质的使用过程、送出维修以及销毁等进行严格的管理，保密性较高的信息存储介质未经批准不得自行销毁，销毁时必须做到双人监销，销毁记录应妥善保存；

h) 重要数据存储在本地或带出工作环境必须采取加密方式存储，并进行监控管理；

i） 应对存放在介质库中的介质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。

10.2.5.4. 设备管理

a） 应对信息系统相关的各种设备、线路等指定专人或专门的部门定期进行维护管理；

b） 应对信息系统的各种软硬件设备的选型、采购、发放或领用等过程建立基于申报、审批和专人负责的管理规定；

c） 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用建进行规范化管理；

d） 应对带离机房或办公地点的信息处理设备进行控制；

e） 应按操作规程实现服务器的启动/停止、加电/断电等操作，加强对服务器操作的日志文件管理和监控管理，并对其定期进行检查；

f） 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等；

g） 应在安全管理机构统一安全策略下对服务器进行系统配置和服务设定，并实施配置管理。

10.2.5.5. 监控管理

a） 应进行主机运行监视，包括监视主机的CPU、硬盘、内存、网络等资源的使用情况；

b） 应对分散或集中的安全管理系统的访问授权、操作记录、日志等方面进行有效管理；

c） 应严格管理运行过程文档，其中包括责任书、授权书、许可证、各类策略文档、事故报告处理文档、安全配置文档、系统各类日志等，并确保文档的完整性和一致性；

d） 应定期或不定期的对保密制度执行情况进行监督检查；

e） 应建立安全管理中心，对恶意代码、补丁、审计等进行集中管理。

10.2.5.6. 网络安全管理

a） 应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；

b） 应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；

c） 应进行网络系统漏洞扫描，对发现的网络系统安全漏洞进行及时的修补；

d） 应保证所有与外部系统的连接均应得到授权和批准；

e） 应建立网络安全管理制度，对网络安全配置、网络用户以及日志等方面作出规定；

f) 应对网络设备的安全策略、授权访问、最小服务、升级与打补丁、维护记录、日志以及配置文件的生成、备份、变更审批、符合性检查等方面做出具体规定；

g) 应规定网络审计日志的保存时间以便为可能的安全事件调查提供支持；

h) 应明确各类用户的责任、义务和风险，并按照机构制定的审查和批准程序建立用户和分配权限，定期检查用户实际权限与分配权限的符合性；

i) 应对日志的备份、授权访问、处理、保留时间等方面做出具体规定，使用统一的网络时间，以确保日志记录的准确；

j) 应通过身份鉴别、访问控制等严格的规定限制远程管理账户的操作权限和登录行为；

k) 应定期检查违反规定拨号上网或其他违反网络安全策略的行为；

l) 应严格控制网络管理用户的授权，授权程序中要求必须有两人在场，并经双重认可后方可操作，操作过程应当有不可更改的审计日志。

10.2.5.7. 系统安全管理

a) 应指定专人对系统进行管理，删除或者禁用不使用的系统缺省账户；

b) 应制度系统安全管理制度，对系统安全配置、系统账户以及审计日志等方面作出规定；

c) 应对能够使用系统工具的人员及数量进行限制和控制；

d) 应定期安装系统的最新补丁程序，并根据厂家提供的可能危害计算机的漏洞进行及时修补，并在安装系统补丁前对现有的重要文件进行备份；

e) 应根据业务需求和系统安全分析确定系统的访问控制策略，系统访问控制策略用于控制分配信息系统、文件及服务的访问权限；

f) 应对系统账户进行分类管理，权限设定应当遵循最小授权要求；

g) 应对系统的安全策略、授权访问、最小服务、升级与打补丁、维护记录、日志以及配置文件的生成、备份、变更审批、符合性检查等方面做出具体规定；

h) 应规定系统审计日志的保存时间以便为可能的安全事件调查提供支持；

i) 应进行系统漏洞扫描，对发现的系统安全漏洞进行及时的修补；

j) 应明确各类用户的责任、义务和风险，对系统账户的登记造册、用户名分配、初始口令分配、用户权限及其审批程序、系统资源分配、注销等作出规定；

k) 应对于账户安全管理的执行情况进行检查和监督，定期审计和分析用户账户的使用情况，对发现的问题和异常情况进行相关处理。

10.2.5.8. 恶意代码防范管理

a) 应提高所用用户的防病毒意识，告知及时升级防病毒软件；

b) 应在读取移动存储设备（如软盘、移动硬盘、光盘）上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也要进行病毒检查；

c) 应指定专人对网络和主机的进行恶意代码检测并保存检测记录；

d) 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确管理规定；

e) 应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。

10.2.5.9. 密码管理

a) 应建立密码使用管理制度，密码算法和密钥的使用应符合国家密码管理规定。

10.2.5.10. 变更管理

a) 确认系统中要发生的变更，并制定变更方案；

b) 建立变更管理制度，重要系统变更前，管理人员应向主管领导申请，变更和变更方案经过评审、审批后方可实施变更；

c) 系统变更情况应向所有相关人员通告；

d) 应建立变更控制的申报和审批文件化程序，变更影响分析应文档化，变更实施过程应记录，所有文档记录应妥善保存；

e) 中止变更并从失败变更中恢复程序应文档化，应明确过程控制方法和人员职责，必要时恢复过程应经过演练；

f) 变更控制的申报和审批程序应控制所有系统变更情况；

g) 应定期检查变更控制的申报和审批程序的执行情况，评估系统现有状况与文档记录的一致性。

10.2.5.11. 备份与恢复管理

a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b) 应规定备份信息的备份方式（如增量备份或全备份等）、备份频度（如每日或每周等）、存储介质、保存期等；

c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略应指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；

d) 应指定相应的负责人定期维护和检查备份及冗余设备的状况，确保需要接入系统时能够正常运行；

e) 应建立控制数据备份和恢复过程的程序，备份过程应记录，所有文件和记录应妥善保存；

f) 应根据系统级备份所采用的方式和产品，建立备份及冗余设备的安装、配置、启动、操作及维护过程控制的程序，记录设备运行过程状况，所有文件和记录应妥善保存；

g) 应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复；

h) 对需要采取加密或数据隐藏处理的备份数据，进行备份和加密操作时要求两名工作人员在场并登记备案。

10.2.5.12. 安全事件处置

a) 所有用户均有责任报告自己发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；

b) 应制定安全事件报告和处置管理制度，规定安全事件的现场处理、事件报告和后期恢复的管理职责；

c) 应分析信息系统的类型、网络连接特点和信息系统用户特点，了解本系统和同类系统已发生的安全事件，识别本系统需要防止发生的安全事件，事件可能来自攻击、错误、故障、事故或灾难；

d) 应根据国家相关管理部门对计算机安全事件等级划分方法，根据安全事件在本系统产生的影响，将本系统计算机安全事件进行等级划分；

e) 应制定的安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；

f) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存；

g) 对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序；

h) 可能涉及国家秘密的重大失、泄密事件应按照有关规定向公安、安全、保密等部门汇报；

i) 严格控制参与涉密事件处理和恢复的人员，重要操作要求至少两名工作人员在场并登记备案。

10.2.5.13. 应急预案管理

a) 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程和事后教育和培训等内容；

b) 应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；

c) 应对系统相关的人员进行培训使之了解如何及何时使用应急预案中的控制手段及恢复策略，对应急预案的培训至少每年举办一次；

d) 应急预案应定期演练，根据不同的应急恢复内容，确定演练的周期；

e) 应规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行；

f) 应根据信息系统的备份技术措施，制定相应的灾难恢复计划；

g) 应急预案和灾难恢复计划应得到测试以确保各个恢复规程的正确性和计划整体的有效性，测试内容包括运行系统恢复、人员协调、备用系统性能测试、通信连接等，根据测试结果，对不适用的规定进行修改或更新；

h) 应随着信息系统的变更，定期对原有的应急预案重新评估，修订完善。

11 第 5 级基本要求

第五级信息系统是涉及国家安全、社会秩序和公共利益的重要信息系统的核心子系统，国家将指定专门部门或者专门机构对其信息安全等级保护工作进行强制监督、检查，对第五级信息系统的基本要求将由国家指定的专门部门或者专门机构参照第四级的基本要求另行制定。

附录 A 威胁描述

A1. 第1级对抗威胁

第一级信息系统应考虑对抗以下威胁：

T1-1. 雷击、水患和火灾等灾害

T1-2. 高温、低温、多雨等原因导致温度、湿度异常

T1-3. 电压波动

T1-4. 通信线路因线缆老化等原因导致损坏或传输质量下降

T1-5. 存储介质老化或质量问题等导致不可用

T1-6. 网络设备、系统设备及其他设备使用时间过长或质量问题等导致硬件故障

T1-7. 系统软件、应用软件运行故障

T1-8. 系统软件、应用软件过度使用内存、CPU 等系统资源

T1-9. 通信过程中受到干扰等原因发生数据传输错误

T1-10. 应用软件、系统软件缺陷导致数据丢失或系统运行中断

T1-11. 网络结构设计不合理

T1-12. 设施、通信线路、设备或存储介质因使用、维护或保养不当等原因导致故障

T1-13. 授权用户操作失误导致系统文件被覆盖、数据丢失或不能使用

T1-14. 攻击者利用非法手段进入机房内部盗窃、破坏等

T1-15. 攻击者非法物理访问系统设备、网络设备或存储介质等

T1-16. 攻击者利用网络协议、操作系统、应用系统漏洞，越权访问文件、数据或其他资源

T1-17. 攻击者利用各种工具获取身份鉴别数据，并对鉴别数据进行分析和解剖，获得鉴别信息，未授权访问网络、系统，或非法使用应用软件、文件和数据

T1-18. 攻击者利用非法手段获得授权用户的鉴别信息或密码介质，访问网络、系统，或使用应用软件、文件和数据

T1-19. 攻击者盗用授权用户的会话连接

T1-20. 攻击者利用网络扩散病毒

T1-21. 内部人员下载、拷贝软件或文件以及打开可疑邮件时引入病毒

A2. 第2级对抗威胁

第二级信息系统应考虑对抗以下威胁：

T2-1. 雷击、地震和台风等自然灾难

T2-2. 水患和火灾等灾害

T2-3. 高温、低温、多雨等原因导致温度、湿度异常

T2-4. 电压波动

T2-5. 供电系统故障

T2-6. 静电、设备寄生耦合干扰和外界电磁干扰

T2-7. 通信线路因线缆老化等原因导致损坏或传输质量下降

T2-8. 存储介质老化或质量问题等导致不可用

T2-9. 网络设备、系统设备及其他设备使用时间过长或质量问题等导致硬件故障

T2-10. 系统软件、应用软件运行故障

T2-11. 系统软件、应用软件过度使用内存、CPU 等系统资源

T2-12. 通信过程中受到干扰等原因发生数据传输错误

T2-13. 应用软件、系统软件缺陷导致数据丢失或系统运行中断

T2-14. 网络结构设计不合理

T2-15. 设施、通信线路、设备或存储介质因使用、维护或保养不当等原因导致故障

T2-16. 授权用户操作失误导致系统文件被覆盖、数据丢失或不能使用

T2-17. 授权用户对系统错误配置或更改

T2-18. 攻击者利用非法手段进入机房内部盗窃、破坏等

T2-19. 攻击者非法物理访问系统设备、网络设备或存储介质等

T2-20. 攻击者采用在通信线缆上搭接或切断等导致线路不可用

T2-21. 攻击者利用分布式拒绝服务攻击等拒绝服务攻击工具，恶意地消耗网络、操作系统和应用系统资源，导致拒绝服务

T2-22. 攻击者利用网络协议、操作或应用系统漏洞，越权访问文件、数据或其他资源

T2-23. 攻击者利用网络协议存在的漏洞进行可躲避检测的攻击（如碎片重组，协议端口重定位等）

T2-24. 攻击者利用通过恶意代码或木马程序，对网络、操作系统或应用系统进行攻击

T2-25. 攻击者利用网络结构设计缺陷旁路安全策略，未授权访问网络

T2-26. 攻击者利用各种工具获取身份鉴别数据，并对鉴别数据进行分析和解剖，获得鉴别信息，未授权访问网络、系统，或非法使用应用软件、文件和数据

T2-27. 攻击者利用非法手段获得授权用户的鉴别信息或密码介质，访问网络、系统，或使用应用软件、文件和数据

T2-28. 攻击者截获、读取、破解介质的信息或剩余信息，进行信息的窃取

T2-29. 攻击者截获、读取、破解通信线路中的信息

T2-30. 攻击者利用通信干扰工具，故意导致通信数据错误

T2-31. 攻击者利用通用安全协议/算法/软件等缺陷，获取信息、解密密钥或破坏通信完整性

T2-32. 攻击者盗用授权用户的会话连接

T2-33. 攻击者否认自己的操作行为

T2-34. 攻击者利用网络扩散病毒

T2-35. 内部人员下载、拷贝软件或文件，打开可疑邮件时引入病毒

T2-36. 内部人员未授权接入外部网络

A3. 第3级对抗威胁

第三级信息系统应考虑对抗以下威胁：

T3-1. 雷击、地震和台风等自然灾难

T3-2. 水患和火灾等灾害

T3-3. 高温、低温、多雨等原因引起温度、湿度异常

T3-4. 电压波动

T3-5. 供电系统故障

T3-6. 静电、设备寄生耦合干扰和外界电磁干扰

T3-7. 强电磁场、强震动源、强噪声源等污染

T3-8. 线路老化等原因导致通信线路损坏或传输质量下降

T3-9. 存储介质使用时间过长或质量问题等导致不可用

T3-10. 网络设备、系统设备及其他设备使用时间过长或质量问题等导致硬件故障

T3-11. 系统软件、应用软件运行故障

T3-12. 系统软件、应用软件过度使用内存、CPU 等系统资源

T3-13. 通信过程中受到干扰等原因发生数据传输错误

T3-14. 应用软件、系统软件缺陷导致数据丢失或运行中断

T3-15. 网络设计不合理

T3-16. 设施、通信线路、设备或存储介质因使用、维护或保养不当等原因导致故障

T3-17. 授权用户操作失误导致系统文件被覆盖、数据丢失或不能使用

T3-18. 授权用户对系统错误配置或更改

T3-19. 由于授权用户的不正确启动和恢复导致安全机制失效

T3-20. 攻击者利用非法手段进入机房内部盗窃、破坏等

T3-21. 攻击者非法物理访问系统设备、网络设备或存储介质等

T3-22. 攻击者采用在通信线缆上搭接或切断等导致线路不可用

T3-23. 攻击者利用分布式拒绝服务攻击等拒绝服务攻击工具，恶意地消耗网络、操作系统和应用系统资源，导致拒绝服务

T3-24. 攻击者利用网络协议、操作系统、应用系统漏洞，越权访问文件、数据或其他资源

T3-25. 攻击者利用网络协议存在的漏洞进行可躲避检测的攻击（如碎片重组，协议端口重定位等）

T3-26. 攻击者利用通过恶意代码或木马程序，对网络、操作系统或应用系统进行攻击

T3-27. 攻击者利用网络结构设计缺陷旁路安全策略，未授权访问网络

T3-28. 攻击者利用应用系统、操作系统中的后门程序攻击系统

T3-29. 攻击者利用各种工具获取身份鉴别数据，并对鉴别数据进行分析和解剖，获得鉴别信息，未授权访问网络、系统，或非法使用应用软件、文件和数据

T3-30. 攻击者利用非法手段获得授权用户的鉴别信息或密码介质，访问网络、系统，或使用应用软件、文件和数据

T3-31. 攻击者利用伪造客户端进入系统，进行非法访问

T3-32. 攻击者提供伪造的应用系统服务进行信息的窃取

T3-33. 攻击者截获、读取、破解介质的信息或剩余信息，进行信息的窃取

T3-34. 攻击者截获、读取、破解通信线路中的信息

T3-35. 攻击者利用通信干扰工具，故意导致通信数据错误

T3-36. 攻击者利用通用安全协议/算法/软件等缺陷，获取信息、解密密钥或破坏通信完整性

T3-37. 攻击者截获数据，进行篡改、插入，并重发，造成数据的完整性、真实性丧失

T3-38. 攻击者利用工具捕捉电磁泄漏的信号，导致信息泄露

T3-39. 攻击者盗用授权用户的会话连接

T3-40. 攻击者否认自己的操作行为

T3-41. 攻击者在软硬件分发环节（生产、运输等）中恶意更改软硬件

T3-42. 攻击者利用网络扩散病毒

T3-43. 内部人员下载、拷贝软件或文件，打开可疑邮件时引入病毒

T3-44. 内部人员未授权接入外部网络

T3-45. 内部人员利用技术或管理漏洞，未授权修改重要系统数据或修改系统程序

T3-46. 内部人员未授权访问敏感信息，将信息带出或通过网络传出，导致信息泄露

A4. 第4级对抗威胁

第四级信息系统应考虑对抗以下威胁：

T4-1. 雷击、地震和台风等自然灾难

T4-2. 水患和火灾等灾害

T4-3. 高温、低温、多雨等原因引起温度、湿度异常

T4-4. 电压波动

T4-5. 供电系统故障

T4-6. 静电、设备寄生耦合干扰和外界电磁干扰

T4-7. 强电磁场、强震动源、强噪声源等污染

T4-8. 线路老化等原因导致通信线路损坏或传输质量下降

T4-9. 存储介质使用时间过长或质量问题等导致不可用

T4-10. 网络设备、系统设备及其他设备使用时间过长或质量问题等导致硬件故障

T4-11. 系统软件、应用软件运行故障

T4-12. 系统软件、应用软件过度使用内存、CPU 等系统资源

T4-13. 通信过程中受到干扰等原因发生数据传输错误

T4-14. 应用软件、系统软件缺陷导致数据丢失或运行中断

T4-15. 网络设计不合理

T4-16. 设施、通信线路、设备或存储介质因使用、维护或保养不当等原因导致故障

T4-17. 授权用户操作失误导致系统文件被覆盖、数据丢失或不能使用

T4-18. 授权用户对系统错误配置或更改

T4-19. 由于授权用户的不正确启动和恢复导致安全机制失效

T4-20. 攻击者采取武力形式攻击系统的物理环境

T4-21. 攻击者利用非法手段进入机房内部盗窃、破坏等

T4-22. 攻击者非法物理访问系统设备、网络设备或存储介质等

T4-23. 攻击者采用在通信线缆上搭接或切断等导致线路不可用

T4-24. 攻击者利用分布式拒绝服务攻击等拒绝服务攻击工具，恶意地消耗网络、操作

系统和应用系统资源，导致拒绝服务

T4-25. 攻击者利用网络协议、操作系统、应用系统漏洞，越权访问文件、数据或其他资源

T4-26. 攻击者利用网络协议存在的漏洞进行可躲避检测的攻击（如碎片重组，协议端口重定位等）

T4-27. 攻击者利用通过恶意代码或木马程序，对网络、操作系统或应用系统进行攻击

T4-28. 攻击者利用网络结构设计缺陷旁路安全策略，未授权访问网络

T4-29. 攻击者利用应用系统、操作系统中的后门程序攻击系统

T4-30. 攻击者利用应用系统、操作系统中的隐蔽信道攻击系统

T4-31. 攻击者利用各种工具获取身份鉴别数据，并对鉴别数据进行分析和解剖，获得鉴别信息，未授权访问网络、系统，或非法使用应用软件、文件和数据

T4-32. 攻击者利用非法手段获得授权用户的鉴别信息或密码介质，访问网络、系统，或使用应用软件、文件和数据

T4-33. 攻击者利用伪造客户端进入系统，进行非法访问

T4-34. 攻击者提供伪造的应用系统服务进行信息的窃取

T4-35. 攻击者截获、读取、破解介质的信息或剩余信息，进行信息的窃取

T4-36. 攻击者截获、读取、破解通信线路中的信息

T4-37. 攻击者利用通信干扰工具，故意导致通信数据错误

T4-38. 攻击者利用通用安全协议/算法/软件等缺陷，获取信息、解密密钥或破坏通信完整性

T4-39. 攻击者截获数据，进行篡改、插入，并重发，造成数据的完整性、真实性丧失

T4-40. 攻击者利用工具捕捉电磁泄漏的信号，导致信息泄露

T4-41. 攻击者盗用授权用户的会话连接

T4-42. 攻击者否认自己的操作行为

T4-43. 攻击者在软硬件分发环节（生产、运输等）中恶意更改软硬件

T4-44. 攻击者利用网络扩散病毒

T4-45. 内部人员下载、拷贝软件或文件，打开可疑邮件时引入病毒

T4-46. 内部人员未授权接入外部网络

T4-47. 内部人员利用技术或管理漏洞，未授权修改重要系统数据或修改系统程序

T4-48. 内部人员未授权访问敏感信息，将信息带出或通过网络传出，导致信息泄露

附录 B 安全威胁与安全目标的关系

B1. 一级

安全威胁	安全目标
T1-1. 雷击、水患和火灾等灾害	O1-1；O1-2；O1-3；O1-19
T1-2. 高温、低温、多雨等原因导致温度、湿度异常	O1-4；O1-19
T1-3. 电压波动	O1-5；O1-19
T1-4. 通信线路因线缆老化等原因导致损坏或传输质量下降	O1-35
T1-5. 存储介质老化或质量问题等导致不可用	O1-6；O1-19；O1-37
T1-6. 网络设备、系统设备及其他设备使用时间过长或质量问题等导致硬件故障	O1-19；O1-36 ；O1-37 ；O1-38
T1-7. 系统软件、应用软件运行故障	O1-7；O1-19；O1-38
T1-8. 系统软件、应用软件过度使用内存、CPU 等系统资源	O1-8
T1-9. 通信过程中受到干扰等原因发生数据传输错误	O1-6
T1-10.应用软件、系统软件缺陷导致数据丢失或系统运行中断	O1-19；O1-38
T1-11.网络结构设计不合理	O1-9
T1-12.设施、通信线路、设备或存储介质因使用、维护或保养不当等原因导致故障	O1-19；O1-39 ；O1-40
T1-13.授权用户操作失误导致系统文件被覆盖、数据丢失或不能使用	O1-19； O1-39 ；O1-40 ；O1-41
T1-14.攻击者利用非法手段进入机房内部盗窃、破坏等	O1-10；O1-11；O1-19
T1-15.攻击者非法物理访问系统设备、网络设备或存储介质等	O1-12
T1-16. 攻击者利用操作系统、应用系统漏洞，越权访问文件、数据或其他资源	O1-13；O1-14；O1-15；O1-16
T1-17. 攻击者利用各种工具获取身份鉴别数据，并对鉴别数据进行分析和解剖，获得鉴别信息，未授权访问网络、系统，或非法使用应用软件、文件和数据	O1-16；O1-17；O1-14；O1-15

安全威胁	安全目标
T1-18.攻击者利用非法手段获得授权用户的鉴别信息或密码介质，访问网络、系统，或使用应用软件、文件和数据	O1-16；O1-17；O1-14；O1-15；O1-34
T1-19.攻击者盗用授权用户的会话连接	O1-17；O1-14；O1-15；O1-42
T1-20.攻击者利用网络扩散病毒	O1-18
T1-21. 内部人员下载、拷贝软件或文件以及执行可疑邮件时引入病毒	O1-18；O1-42

B2. 二级

安全威胁	安全目标
T2-1. 雷击、地震和台风等自然灾难	O2-1；O2-2；O2-39
T2-2. 水患和火灾等灾害	O2-3；O2-4；O2-5；O2-39
T2-3. 高温、低温、多雨等原因导致温度、湿度异常	O2-6；O2-39
T2-4. 电压波动	O2-7；O2-39
T2-5. 供电系统故障	O2-8；O2-39
T2-6. 静电、设备寄生耦合干扰和外界电磁干扰	O2-9；O2-10
T2-7.通信线路因线缆老化等原因导致损坏或传输质量下降	O2-61
T2-8. 存储介质老化或质量问题等导致不可用	O2-11；O2-39；O2-62；O2-63
T2-9. 网络设备、系统设备及其他设备使用时间过长或质量问题等导致硬件故障	O2-12；O2-39； O2-62；O2-63；O2-64
T2-10.系统软件、应用软件运行故障	O2-13；O2-14；O2-39；O2-64
T2-11.系统软件、应用软件过度使用内存、CPU 等系统资源	O2-15
T2-12.通信过程中受到干扰等原因发生数据传输错误	O2-11
T2-13.应用软件、系统软件缺陷导致数据丢失或系统运行中断	O2-40；O2-64
T2-14.网络结构设计不合理	O2-69
T2-15.设施、通信线路、设备或存储介质因使用、维护或保养不当等原因导致故障	O2-12；O2-39；O2-65；O2-66；O2-67；O2-47
T2-16.授权用户操作失误导致系统文件被覆盖、数据丢失或不能使用	O2-16；O2-17；O2-39； O2-65；O2-66；O2-67；O2-47

安全威胁	安全目标
T2-17.授权用户对系统错误配置或更改	O2-16；O2-17；O2-39； O2-47
T2-18.攻击者利用非法手段进入机房内部盗窃、破坏等	O2-18；O2-19；O2-20；O2-39
T2-19.攻击者非法物理访问系统设备、网络设备或存储介质等	O2-21；O2-22
T2-20.攻击者采用在通信线缆上搭接或切断等导致线路不可用	O2-23
T2-21.攻击者利用分布式拒绝服务攻击等拒绝服务攻击工具，恶意地消耗网络、操作系统和应用系统资源，导致拒绝服务	O2-24；O2-25
T2-22.攻击者利用网络协议、操作系统、应用系统漏洞，越权访问文件、数据或其他资源	O2-26；O2-27；O2-28；O2-29；O2-30；O2-31
T2-23.攻击者利用网络协议存在的漏洞进行可躲避检测的攻击（如碎片重组，协议端口重定位等）	O2-26；O2-25；O2-27；O2-28
T2-24.攻击者利用通过恶意代码或木马程序，对网络、操作系统或应用系统进行攻击	O2-32；O2-33；O2-34；O2-25；O2-27；O2-28
T2-25.攻击者利用网络结构设计缺陷旁路安全策略，未授权访问网络	O2-25；O2-27；O2-28；O2-67
T2-26.攻击者利用各种工具获取身份鉴别数据，并对鉴别数据进行分析和解剖，获得鉴别信息，未授权访问网络、系统，或非法使用应用软件、文件和数据	O2-30；O2-31；O2-27；O2-28
T2-27.攻击者利用非法手段获得授权用户的鉴别信息或密码介质，访问网络、系统，或使用应用软件、文件和数据	O2-30；O2-31；O2-35；O2-27；O2-28；O2-60
T2-28.攻击者截获、读取、破解介质的信息或剩余信息，进行信息的窃取	O2-36；O2-37；O2-28
T2-29.攻击者截获、读取、破解通信线路中的信息	O2-37
T2-30.攻击者利用通信干扰工具，故意导致通信数据错误	O2-11
T2-31.攻击者利用通用安全协议/算法/软件等缺陷，获取信息、解密密钥或破坏通信完整性	O2-26；O2-37；O2-11
T2-32.攻击者盗用授权用户的会话连接	O2-37；O2-30；O2-31；O2-27；O2-28；O2-69

安全威胁	安全目标
T2-33.攻击者否认自己的操作行为	02-16
T2-34.攻击者利用网络扩散病毒	02-32；02-33；02-34；02-11
T2-35.内部人员下载、拷贝软件或文件，执行可疑邮件时引入病毒	02-32；02-33；02-34；02-11；02-68
T2-36.内部人员未授权接入外部网络	02-39；02-16；02-48；02-68

B3. 三级

安全威胁	安全目标
T3-1. 雷击、地震和台风等自然灾难	03-1，03-2，03-65，03-66
T3-2. 水患和火灾等灾害	03-3，03-4，03-5，03-6，03-7，03-65，03-66
T3-3. 高温、低温、多雨等原因引起温度、湿度异常	03-8，03-65，03-66
T3-4. 电压波动	03-9，03-65，03-66
T3-5. 供电系统故障	03-10，03-65，03-66
T3-6. 静电、设备寄生耦合干扰和外界电磁干扰	03-11，03-12
T3-7. 强电磁场、强震动源、强噪声源等污染	03-13，03-65，03-66
T3-8. 线路老化等原因导致通信线路损坏或传输质量下降	03-14，03-15，03-86
T3-9. 存储介质使用时间过长或质量问题等导致不可用	03-16，03-65，03-33，03-89，03-90
T3-10.网络设备、系统设备及其他设备使用时间过长或质量问题等导致硬件故障	03-65，03-66， 03-89，03-90，03-91
T3-11.系统软件、应用软件运行故障	03-17，03-18，03-19，03-20，03-65，03-66， 03-91
T3-12.系统软件、应用软件过度使用内存、CPU 等系统资源	03-21，03-19，03-22
T3-13.通信过程中受到干扰等原因发生数据传输错误	03-16
T3-14.应用软件、系统软件缺陷导致数据丢失或运行中断	03-16，03-23，03-65，03-66， 03-91
T3-15.网络设计不合理	03-96

安全威胁	安全目标
T3-16.设施、通信线路、设备或存储介质因使用、维护或保养不当等原因导致故障	O3-66，O3-65，O3-92，O3-93，O3-94
T3-17.授权用户操作失误导致系统文件被覆盖、数据丢失或不能使用	O3-24，O3-25，O3-65，O3-66， O3-92，O3-93，O3-94，O3-74
T3-18.授权用户对系统错误配置或更改	O3-24，O3-25，O3-65，O3-66， O3-74
T3-19.由于授权用户的不正确启动和恢复导致安全机制失效	O3-24，O3-25，O3-74
T3-20.攻击者利用非法手段进入机房内部盗窃、破坏等	O3-26，O3-27，O3-28，O3-29，O3-30，O3-65，O3-66
T3-21.攻击者非法物理访问系统设备、网络设备或存储介质等	O3-31；O3-44；O3-52
T3-22.攻击者采用在通信线缆上搭接或切断等导致线路不可用	O3-32；O3-33
T3-23.攻击者利用分布式拒绝服务攻击等拒绝服务攻击工具，恶意地消耗网络、操作系统和应用系统资源，导致拒绝服务	O3-34；O3-36；O3-35；O3-65
T3-24.攻击者利用网络协议、操作系统、应用系统漏洞，越权访问文件、数据或其他资源	O3-37；O3-38；O3-39；O3-40；O3-45；O3-46
T3-25.攻击者利用网络协议存在的漏洞进行可躲避检测的攻击（如碎片重组，协议端口重定位等）	O3-37；O3-36；O3-38；O3-39
T3-26.攻击者利用通过恶意代码或木马程序，对网络、操作系统或应用系统进行攻击	O3-41；O3-42；O3-43；O3-36；O3-38；O3-39
T3-27.攻击者利用网络结构设计缺陷旁路安全策略，未授权访问网络	O3-36；O3-38；O3-39；O3-96
T3-28.攻击者利用应用系统、操作系统中的后门程序攻击系统	O3-36；O3-38；O3-39；O3-98
T3-29.攻击者利用各种工具获取身份鉴别数据，并对鉴别数据进行分析和解剖，获得鉴别信息，未授权访问网络、系统，或非法使用应用软件、文件和数据	O3-44；O3-52；O3-45；O3-46；O3-38；O3-39
T3-30.攻击者利用非法手段获得授权用户的鉴别信息或密码介质，访问网络、系统，或使用应用软件、文件和数据	O3-45；O3-46；O3-44；O3-52；O3-38；O3-39；O3-85
T3-31.攻击者利用伪造客户端进入系统，进行非法访问	O3-47；O3-48；O3-49；O3-45；O3-46；O3-38；O3-39

安全威胁	安全目标
T3-32.攻击者提供伪造的应用系统服务进行信息的窃取	03-47；03-48；03-49；03-44
T3-33.攻击者截获、读取、破解介质的信息或剩余信息，进行信息的窃取	03-50；03-51；03-52；03-39
T3-34.攻击者截获、读取、破解通信线路中的信息	03-44；03-52
T3-35.攻击者利用通信干扰工具，故意导致通信数据错误	03-16；03-53
T3-36.攻击者利用通用安全协议/算法/软件等缺陷，获取信息、解密密钥或破坏通信完整性	03-37；03-44；03-52；03-16
T3-37.攻击者截获数据，进行篡改、插入，并重发，造成数据的完整性、真实性丧失	03-54；03-44；03-52；03-16
T3-38.攻击者利用工具捕捉电磁泄漏的信号，导致信息泄露	03-56；03-44；03-52
T3-39.攻击者盗用授权用户的会话连接	03-57；03-44；03-52；03-45；03-46；03-38；03-39；03-95
T3-40.攻击者否认自己的操作行为	03-58；03-24
T3-41.攻击者在软硬件分发环节（生产、运输等）中恶意更改软硬件	03-37；03-97
T3-42.攻击者利用网络扩散病毒	03-41；03-42；03-43；03-16
T3-43.内部人员下载、拷贝软件或文件，执行可疑邮件时引入病毒	03-41；03-42；03-43；03-16；03-95
T3-44.内部人员未授权接入外部网络	03-60；03-61；03-24；03-95
T3-45.内部人员利用技术或管理漏洞，未授权修改重要系统数据或修改系统程序	03-37；03-39；03-24；03-62；03-45；03-46；03-38；03-39；03-24
T3-46.内部人员未授权访问敏感信息，将信息带出或通过网络传出，导致信息泄露	03-63；03-64；03-44；03-52；03-45；03-46；03-38；03-39；03-24

B4. 四级

安全威胁	安全目标
T4-1. 雷击、地震和台风等自然灾难	04-1；04-2；04-67；04-69
T4-2. 水患和火灾等灾害	04-3；04-4；04-5；04-6；04-7；04-67；04-69

安全威胁	安全目标
T4-3. 高温、低温、多雨等原因引起温度、湿度异常	04-8；04-67；04-69
T4-4. 电压波动	04-9；04-67；04-69
T4-5. 供电系统故障	04-10；04-67；04-69
T4-6. 静电、设备寄生耦合干扰和外界电磁干扰	04-11；04-12；04-13
T4-7. 强电磁场、强震动源、强噪声源等污染	04-14；04-67；04-69
T4-8. 线路老化等原因导致通信线路损坏或传输质量下降	04-15；04-68；04-90
T4-9. 存储介质使用时间过长或质量问题等导致不可用	04-23；04-67；04-69；04-91；04-92
T4-10.网络设备、系统设备及其他设备使用时间过长或质量问题等导致硬件故障	04-67；04-69；04-91；04-92；04-93
T4-11.系统软件、应用软件运行故障	04-16；04-17；04-18；04-19；04-20；04-67；04-69； 04-94
T4-12.系统软件、应用软件过度使用内存、CPU 等系统资源	04-21；04-18；04-22
T4-13.通信过程中受到干扰等原因发生数据传输错误	04-23
T4-14.应用软件、系统软件缺陷导致数据丢失或运行中断	04-24；04-67；04-69；04-94
T4-15.网络设计不合理	04-99
T4-16.设施、通信线路、设备或存储介质因使用、维护或保养不当等原因导致故障	04-69；04-67；04-95；04-96；04-98；04-77
T4-17.授权用户操作失误导致系统文件被覆盖、数据丢失或不能使用	04-25；04-26；04-67；04-69； 04-95；04-96；04-98；04-77
T4-18.授权用户对系统错误配置或更改	04-25；04-26；04-67；04-69； 04-77
T4-19.由于授权用户的不正确启动和恢复导致安全机制失效	04-27；04-28；04-25；04-26；04-77
T4-20.攻击者采取武力形式攻击系统的物理环境	04-67；04-69
T4-21.攻击者利用非法手段进入机房内部盗窃、破坏等	04-29；04-30；04-31；04-32；04-33；04-67；04-69
T4-22.攻击者非法物理访问系统设备、网络设备或存储介质等	04-47；04-55
T4-23.攻击者采用在通信线缆上搭接或切断等导致线路不可用	04-35；04-36
T4-24.攻击者利用分布式拒绝服务攻击等拒绝服务攻击工具，恶意地消耗网络、操作系统和应用系统资源，导致拒绝服务	04-37；04-38；04-39；04-69

安全威胁	安全目标
T4-25.攻击者利用网络协议、操作系统、应用系统漏洞，越权访问文件、数据或其他资源	O4-40；O4-41；O4-42；O4-43；O4-48；O4-49
T4-26.攻击者利用网络协议存在的漏洞进行可躲避检测的攻击（如碎片重组，协议端口重定位等）	O4-40；O4-38；O4-41；O4-42
T4-27.攻击者利用通过恶意代码或木马程序，对网络、操作系统或应用系统进行攻击	O4-44；O4-45；O4-46；O4-38；O4-41；O4-42
T4-28.攻击者利用网络结构设计缺陷旁路安全策略，未授权访问网络	O4-38；O4-41；O4-42；O4-99
T4-29.攻击者利用应用系统、操作系统中的后门程序攻击系统	O4-38；O4-41；O4-42；O4-101
T4-30.攻击者利用应用系统、操作系统中的隐蔽信道攻击系统	O4-38；O4-41；O4-42； O4-101
T4-31.攻击者利用各种工具获取身份鉴别数据，并对鉴别数据进行分析和解剖，获得鉴别信息，未授权访问网络、系统，或非法使用应用软件、文件和数据	O4-47；O4-55；O4-49；O4-41；O4-42
T4-32.攻击者利用非法手段获得授权用户的鉴别信息或密码介质，访问网络、系统，或使用应用软件、文件和数据	O4-48；O4-49；O4-47；O4-55；O4-41；O4-42；O4-90
T4-33.攻击者利用伪造客户端进入系统，进行非法访问	O4-50；O4-51；O4-52；O4-48；O4-49；O4-41；O4-41；O4-42
T4-34.攻击者提供伪造的应用系统服务进行信息的窃取	O4-50；O4-51；O4-52；O4-47
T4-35.攻击者截获、读取、破解介质的信息或剩余信息，进行信息的窃取	O4-54；O4-53；O4-55；O4-42
T4-36.攻击者截获、读取、破解通信线路中的信息	O4-47；O4-55
T4-37.攻击者利用通信干扰工具，故意导致通信数据错误	O4-23；O4-56
T4-38.攻击者利用通用安全协议/算法/软件等缺陷，获取信息、解密密钥或破坏通信完整性	O4-40；O4-47；O4-55；O4-23
T4-39.攻击者截获数据，进行篡改、插入，并重发，造成数据的完整性、真实性丧失	O4-57；O4-47；O4-55；O4-23
T4-40.攻击者利用工具捕捉电磁泄漏的信号，导致信息泄露	O4-58；O4-47；O4-55
T4-41.攻击者盗用授权用户的会话连接	O4-59；O4-47；O4-55；O4-48；O4-49；O4-41；O4-42；O4-98
T4-42.攻击者否认自己的操作行为	O4-60；O4-25

安全威胁	安全目标
T4-43.攻击者在软硬件分发环节（生产、运输等）中恶意更改软硬件	04-40；04-100
T4-44.攻击者利用网络扩散病毒	04-40；04-45；04-46；04-23
T4-45.内部人员下载、拷贝软件或文件，执行可疑邮件时引入病毒	04-44；04-61；04-45；04-46；04-23；04-77；04-98
T4-46.内部人员未授权接入外部网络	04-62；04-63；04-25； 04-77；04-98
T4-47.内部人员利用技术或管理漏洞，未授权修改重要系统数据或修改系统程序	04-40；04-42；04-25；04-64；04-48；04-49；04-41；04-42；04-25
T4-48.内部人员未授权访问敏感信息，将信息带出或通过网络传出，导致信息泄露	04-66；04-47；04-55；04-48；04-49；04-41；04-42；04-25

附录 C 安全目标与基本要求的关系

C1.一级

安全目标	基本要求
O1-1.应具有防雷击的能力	7.1.1.3 防雷击
O1-2.应具有防水和防潮的能力	7.1.1.5 防水和防潮
O1-3.应具有灭火的能力	7.1.1.4 防火
O1-4.应具有温湿度检测和控制的能力	7.1.1.6 温湿度控制
O1-5.应具有防止电压波动的能力	7.1.1.7 电力供应
O1-6.应具有对传输和存储数据进行完整性检测的能力	7.1.4.3 通信完整性；7.1.5.1 数据完整性
O1-7.应具有系统软件、应用软件容错的能力	7.1.4.4 软件容错
O1-8.应具有合理使用和控制系统资源的能力	7.1.4.5 资源控制
O1-9.应具有设计合理、安全网络结构的能力	7.1.2.1 结构安全和网段划分；7.2.4.2 安全方案设计
O1-10.应具有控制机房进出的能力	7.1.1.1 物理访问控制；7.2.5.1 环境管理
O1-11.应具有防止设备、介质等丢失的能力	7.1.1.2 防盗窃和防破坏;7.1.1.1 物理访问控制;7.2.5.1 环境管理;7.2.5.3 介质管理；7.2.5.4 设备管理
O1-12.应具有控制接触重要设备、介质的能力	7.1.1.1 物理访问控制；7.1.1.2 防盗窃和防破坏
O1-13.应具有发现操作系统、应用系统等重要漏洞并及时修补的能力	7.1.3.3 恶意代码防范；7.2.5.6 网络安全管理；7.2.5.7 系统安全管理
O1-14.应具有对网络、系统和应用的访问进行控制的能力	7.1.2.4 网络设备防护；7.1.2.2 网络访问控制；7.1.3.1 身份鉴别；7.1.3.2 自主访问控制；7.1.4.1 身份鉴别；7.1.4.2 访问控制
O1-15.应具有对数据、文件或其他资源的访问进行控制的能力	7.1.2.2 网络访问控制；7.1.2.3 拨号访问控制；7.1.3.2 自主访问控制；7.1.4.2 访问控制
O1-16.应具有对用户进行标识和鉴别的能力	7.1.2.4 网络设备防护；7.1.3.1 身份鉴别；7.1.4.1 身份鉴别
O1-17.应具有保证鉴别数据传输和存储保密性的能力	7.1.5.2 数据保密性
O1-18.应具有对病毒的检测、阻止和清除能力	7.1.3.3 恶意代码防范；7.2.5.8 恶意代码防范管理

安全目标	基本要求
O1-19.应具有重要数据恢复的能力	7.1.5.3 数据备份和恢复；7.2.5.9 备份与恢复管理
O1-20.应确保配备了足够数量的管理人员，支持信息系统的管理工作	7.2.1.1 岗位设置；7.2.1.2 人员配备
O1-21.应确保建立了基本的安全管理制度，并保证安全管理制度的有效性	7.2.2.2 制定和发布
O1-22.应确保对信息系统进行合理定级	7.2.4.1 系统定级
O1-23.应确保能控制信息安全相关事件的授权与审批	7.2.1.3 授权和审批
O1-24.应确保建立恰当可靠的联络渠道，以便安全事件发生时能得到支持	7.2.1.4 沟通和合作；7.2.5.10 安全事件处置
O1-25.应确保对人员的行为进行控制	7.2.2.1 管理制度；7.2.3.1 人员录用；7.2.3.2 人员离岗；7.2.3.4 第三方人员访问管理
O1-26.应确保安全产品的可信度和产品质量	7.2.4.3 产品采购；
O1-27.应确保自行开发过程和工程实施过程中的安全	7.2.4.4 自行软件开发；7.2.4.6 工程实施
O1-28.应确保能顺利地接管和维护信息系统	7.2.4.8 系统交付
O1-29.应确保安全工程的实施质量和安全功能的准确实现	7.2.4.2 安全方案设计；7.2.4.7 测试验收；7.2.4.9 安全服务商选择
O1-30.应确保机房具有良好的运行环境	7.2.5.1 环境管理
O1-31.应确保对信息系统资产进行安全管理	7.2.5.2 资产管理
O1-32.应确保对各种软硬件设备的选型、采购、发放、使用和保管等过程进行控制	7.2.5.4 设备管理
O1-33.应确保对网络、操作系统、数据库管理系统和应用系统进行安全管理	7.2.5.6 网络安全管理；7.2.5.7 系统安全管理
O1-34.应确保用户具有鉴别信息使用的安全意识	7.2.3.3 安全意识教育和培训；7.2.5.7 系统安全管理
O1-35.应确保定期地对通信线路进行检查和维护	7.2.5.4 设备管理
O1-36.应确保硬件设备、存储介质存放环境安全，并对其的使用进行控制和保护	7.2.5.1 环境管理；7.2.5.3 介质管理；7.2.5.4 设备管理

安全目标	基本要求
O1-37.应确保对支撑设施、硬件设备、存储介质进行日常维护和管理	7.2.5.5 监控管理；7.2.5.3 介质管理；7.2.5.4 设备管理
O1-38.应确保系统中使用的硬件、软件产品的质量	7.2.4.3 产品采购；7.2.4.4 自行软件开发；7.2.4.5 外包软件开发；7.2.4.7 测试验收；7.1.4.6 代码安全
O1-39.应确保各类人员具有与其岗位相适应的技术能力	7.2.3.1 人员录用；7.2.3.3 安全意识教育和培训
O1-40.应确保对各类人员进行相关的技术培训	7.2.3.3 安全意识教育和培训
O1-41.应确保提供的足够的使用手册、维护指南等资料	7.2.4.5 外包软件开发；7.2.4.3 产品采购；7.2.2.1 管理制度；7.2.5.5 监控管理
O1-42.应确保内部人员具有安全方面的常识和意识	7.2.3.3 安全意识教育和培训
O1-43.应确保对信息安全事件进行报告和处置	7.2.5.10 安全事件处置

C2.二级

安全目标	基本要求
O2-1. 应具有抵抗一般强度地震、台风等自然灾难造成破坏的能力	8.1.1.1 物理位置的选择；8.1.5.3 数据备份和恢复；8.2.5.11 备份与恢复管理
O2-2. 应具有防止雷击事件导致重要设备被破坏的能力	8.1.1.1 物理位置的选择；8.1.1.4 防雷击；8.1.5.3 数据备份和恢复；8.2.5.11 备份与恢复管理
O2-3. 应具有防水和防潮的能力	8.1.1.6 防水和防潮
O2-4. 应具有灭火的能力	8.1.1.5 防火
O2-5. 应具有检测火灾和报警的能力	8.1.1.5 防火
O2-6. 应具有温湿度自动检测和控制的能力	8.1.1.8 温湿度控制
O2-7. 应具有防止电压波动的能力	8.1.1.9 电力供应
O2-8. 应具有对抗短时间断电的能力	8.1.1.9 电力供应
O2-9. 应具有防止静电导致重要设备被破坏的能力	8.1.1.7 防静电
O2-10.具有基本的抗电磁干扰能力	8.1.1.10 电磁防护

安全目标	基本要求
O2-11.应具有对传输和存储数据进行完整性检测的能力	8.1.4.5 通信完整性；8.1.5.1 数据完整性
O2-12.应具有对硬件故障产品进行替换的能力	8.1.5.3 数据备份和恢复；8.2.5.11 备份与恢复管理
O2-13.应具有系统软件、应用软件容错的能力	8.1.4.7 软件容错；8.1.3.4 系统保护
O2-14.应具有软件故障分析的能力	8.1.4.7 软件容错；8.2.5.5 监控管理
O2-15.应具有合理使用和控制系统资源的能力	8.1.3.7 系统资源控制；8.1.4.8 资源控制
O2-16.应具有记录用户操作行为的能力	8.1.2.4 网络安全审计；8.1.3.3 安全审计；8.1.4.3 安全审计
O2-17.应具有对用户的误操作行为进行检测和报警的能力	8.1.4.7 软件容错；8.1.5.3 数据备份和恢复；8.2.5.11 备份与恢复管理
O2-18.应具有控制机房进出的能力	8.1.1.2 物理访问控制；8.2.5.1 环境管理
O2-19.应具有防止设备、介质等丢失的能力	8.1.1.3 防盗窃和防破坏；8.1.1.2 物理访问控制；8.2.5.1 环境管理 8.2.5.3 介质管理
O2-20.应具有控制机房内人员活动的能力	8.1.1.2 物理访问控制；8.2.5.1 环境管理；8.1.1.3 防盗窃和防破坏
O2-21.应具有控制接触重要设备、介质的能力	8.1.1.2 物理访问控制；8.1.1.3 防盗窃和防破坏
O2-22.应具有对传输和存储中的信息进行保密性保护的能力	8.1.4.6 通信保密性；8.1.5.2 数据保密性
O2-23.应具有对通信线路进行物理保护的能力	8.1.1.2 物理访问控制；8.1.1.3 防盗窃和防破坏
O2-24.应具有限制网络、操作系统和应用系统资源使用的能力	8.1.3.7 系统资源控制；8.1.4.8 资源控制
O2-25.应具有能够检测对网络的各种攻击并记录其活动的能力	8.1.2.6 网络入侵防范
O2-26.应具有发现所有已知漏洞并及时修补的能力	8.1.2.7 恶意代码防范；8.1.3.6 恶意代码防范；8.2.1.5 审核和检查； 8.2.5.6 网络安全管理；8.2.5.7 系统安全管理；
O2-27.应具有对网络、系统和应用的访问进行控制的能力	8.1.2.8 网络设备防护;8.1.2.2 网络访问控制;8.1.3.1 身份鉴别;8.1.3.2 自主访问控制；8.1.4.1 身份鉴别；8.1.4.2 访问控制
O2-28.应具有对数据、文件或其他资源的访问进行控制的能力	8.1.2.2 网络访问控制；8.1.2.3 拨号访问控制；8.1.3.2 自主访问控制；

安全目标	基本要求
	8.1.4.2 访问控制
O2-29.应具有对资源访问的行为进行记录的能力	8.1.2.4 网络安全审计；8.1.3.3 安全审计；8.1.4.3 安全审计
O2-30.应具有对用户进行唯一标识的能力	8.1.2.8 网络设备防护；8.1.3.1 身份鉴别；8.1.4.1 系统身份鉴别
O2-31.应具有对用户产生复杂鉴别信息并进行鉴别的能力	8.1.2.8 网络设备防护；8.1.3.1 身份鉴别；8.1.4.1 系统身份鉴别
O2-32.应具有对恶意代码的检测、阻止和清除能力	8.1.2.7 恶意代码防范；8.1.3.6 恶意代码防范；8.2.5.8 恶意代码防范管理
O2-33.应具有防止恶意代码在网络中扩散的能力	8.1.2.7 网络恶意代码安全；8.1.3.6 恶意代码防范；8.2.5.8 恶意代码防范管理
O2-34.应具有对恶意代码库和搜索引擎及时更新的能力	8.1.2.7 网络恶意代码安全；8.1.3.6 恶意代码防范；8.2.5.8 恶意代码防范管理
O2-35.应具有保证鉴别数据传输和存储保密性的能力	8.1.5.2 数据保密性
O2-36.应具有对存储介质中的残余信息进行删除的能力	8.1.3.5 剩余信息保护；8.1.4.4 剩余信息保护；8.2.5.3 介质管理
O2-37.应具有非活动状态一段时间后自动切断连接的能力	8.1.2.8 网络设备防护；8.1.3.1 身份鉴别；8.1.3.2 身份鉴别；8.1.3.7 系统资源控制；8.1.4.8 资源控制；8.2.5.1 环境管理
O2-38.应具有网络边界完整性检测能力	8.1.2.5 边界完整性检查
O2-39.应具有重要数据恢复的能力	8.1.5.3 数据备份和恢复；8.2.5.11 备份与恢复管理
O2-40.应确保建立了安全职能部门，配备了安全管理人员，支持信息安全管理工作	8.2.1.1 岗位设置；8.2.1.2 人员配备
O2-41.应确保配备了足够数量的管理人员，对系统进行运行维护	8.2.1.2 人员配备；8.2.5.5 监控管理
O2-42.应确保对主要的管理活动进行了制度化管理	8.2.2.1 管理制度；8.2.2.2 制定和发布
O2-43.应确保不断完善、健全安全管理制度	8.2.2.3 评审和修订

安全目标	基本要求
O2-44.应确保能协调信息安全工作在各功能部门的实施	8.2.1.4 沟通和合作
O2-45.应确保能控制信息安全相关事件的授权与审批	8.2.1.3 授权和审批
O2-46.应确保建立恰当可靠的联络渠道，以便安全事件发生时能得到支持	8.2.1.4 沟通和合作；8.2.5.12 安全事件处置
O2-47.应确保对人员的行为进行控制	8.2.2.1 管理制度；8.2.3.1 人员录用；8.2.3.2 人员离岗；8.2.3.3 人员考核；8.2.3.5 第三方人员访问管理
O2-48.应确保对人员的管理活动进行了指导	8.2.2.1 管理制度；8.2.3.4 安全意识教育和培训
O2-49.应确保安全策略的正确性和安全措施的合理性	8.2.1.5 审核和检查
O2-50.应确保对信息系统进行合理定级	8.2.4.3 系统定级
O2-51.应确保安全产品的可信度和产品质量	8.2.4.3 产品采购
O2-52.应确保自行开发过程和工程实施过程中的安全	8.2.4.4 自行软件开发；8.2.4.6 工程实施
O2-53.应确保能顺利地接管和维护信息系统	8.2.4.8 系统交付
O2-54.应确保安全工程的实施质量和安全功能的准确实现	8.2.4.2 安全方案设计；8.2.4.7 测试验收；8.2.4.9 安全服务商选择
O2-55.应确保机房具有良好的运行环境	8.2.5.1 环境管理
O2-56.应确保对信息系统资产进行标识管理	8.2.5.2 资产管理
O2-57.应确保对各种软硬件设备的选型、采购、发放、使用和保管等过程进行控制	8.2.5.3 介质管理；8.2.5.4 设备管理
O2-58.应确保各种网络设备、服务器正确使用和维护	8.2.2.1 管理制度；8.2.5.5 监控管理
O2-59.应确保对网络、操作系统、数据库管理系统和应用系统进行安全管理	8.2.5.6 网络安全管理；8.2.5.7 系统安全管理
O2-60.应确保用户具有鉴别信息使用的安全意识	8.2.3.4 安全意识教育和培训；8.2.5.7 系统安全管理
O2-61.应确保定期地对通信线路进行检查和维护	8.2.5.4 介质管理；8.2.5.4 设备管理
O2-62.应确保硬件设备、存储介质存放环境安全，并对其的使用进行控制和保护	8.2.5.1 环境管理；8.2.5.3 介质管理；8.2.5.4 设备管理

安全目标	基本要求
O2-63.应确保对支撑设施、硬件设备、存储介质进行日常维护和管理	8.2.5.5 监控管理；8.2.5.3 介质管理；8.2.5.4 设备管理
O2-64.应确保系统中使用的硬件、软件产品的质量	8.2.4.3 产品采购;8.2.4.4 自行软件开发;8.2.4.5 外包软件开发;8.2.4.7 测试验收；8.1.4.9 代码安全
O2-65.应确保各类人员具有与其岗位相适应的技术能力	8.2.3.1 人员录用；8.2.3.4 安全意识教育和培训
O2-66.应确保对各类人员进行相关的技术培训	8.2.3.4 安全意识教育和培训
O2-67.应确保提供的足够的使用手册、维护指南等资料	8.2.4.5 外包软件开发；8.2.4.3 产品采购；8.2.2.1 管理制度；8.2.5.5 监控管理
O2-68.应确保内部人员具有安全方面的常识和意识	8.2.3.4 安全意识培训和教育
O2-69.应确保具有设计合理、安全网络结构的能力	8.2.4.2 安全方案设计；8.1.2.1 结构安全和网段划分
O2-70.应确保密码算法和密钥的使用符合国家有关法律、法规的规定	8.2.5.9 密码管理
O2-71.应确保任何变更控制和设备重用要申报和审批，并对其实行制度化的管理	8.2.1.3 授权和审批；8.2.5.10 变更管理
O2-72.应确保在事件发生后能采取积极、有效的应急策略和措施	8.2.5.12 安全事件处置；8.2.5.13 应急预案管理；8.2.5.11 备份和恢复管理
O2-73.应确保信息安全事件实行分等级响应、处置	8.2.5.12 安全事件处置

C3.三级

安全目标	基本要求
O3-1.应具有对抗中等强度地震、台风等自然灾难造成破坏的能力	9.1.1.1 物理位置的选择；9.1.5.3 数据备份和恢复；9.2.5.11 备份与恢复管理
O3-2.应具有防止雷击事件导致大面积设备被破坏的能力	9.1.1.1 物理位置的选择；9.1.1.4 防雷击；9.1.5.3 数据备份和恢复；9.2.5.11 备份与恢复管理
O3-3.应具有防水和防潮的能力	9.1.1.6 防水和防潮
O3-4.应具有对水患检测和报警的能力	9.1.1.6 防水和防潮

安全目标	基本要求
O3-5.应具有自动灭火的能力	9.1.1.5 防火
O3-6.应具有检测火灾和报警的能力	9.1.1.5 防火
O3-7.应具有防止火灾蔓延的能力	9.1.1.5 防火；
O3-8.应具有温湿度自动检测和控制的能力	9.1.1.8 温湿度控制
O3-9.应具有防止电压波动的能力	9.1.1.9 电力供应
O3-10.应具有对抗长时间断电的能力	9.1.1.9 电力供应
O3-11.应具有防止静电导致大面积设备被破坏的能力	9.1.1.7 防静电
O3-12.应具有对重要设备和介质进行电磁屏蔽的能力	9.1.1.10 电磁防护
O3-13.应具有防止强电磁场、强震动源和强噪声源等污染影响系统正常的能力	9.1.1.1 物理位置的选择；9.1.1.10 电磁防护
O3-14.应具有监测通信线路传输状况的能力	9.2.5.6 网络安全管理；9.2.5.5 监控管理
O3-15.应具有及时恢复正常通信的能力	9.1.5.3 数据备份和恢复；9.2.5.11 备份与恢复管理
O3-16.应具有对传输和存储数据进行完整性检测和纠错的能力	9.1.4.5 通信完整性；9.1.5.1 数据完整性
O3-17.应具有系统软件、应用软件容错的能力	9.1.4.8 软件容错；9.1.3.5 系统保护
O3-18.应具有软件故障分析的能力	9.1.4.8 软件容错；9.2.5.5 监控管理
O3-19.应具有软件状态监测和报警的能力	9.1.3.7 入侵防范；9.2.5.5 监控管理
O3-20.应具有自动保护当前工作状态的能力	9.1.3.5 系统保护；9.1.4.8 软件容错
O3-21.应具有合理使用和控制系统资源的能力	9.1.3.9 系统资源控制；9.1.4.9 资源控制
O3-22.应具有按优先级自动分配系统资源的能力	9.1.3.9 系统资源控制；9.1.4.9 资源控制
O3-23.应具有对软件缺陷进行检查的能力	9.1.4.10 代码安全；9.2.4.4 产品采购；9.2.4.5 自行软件开发；9.2.4.6 外包软件开发
O3-24.应具有记录用户操作行为和分析记录结果的能力	9.1.2.4 网络安全审计；9.1.3.4 安全审计；9.1.4.3 安全审计
O3-25.应具有对用户的误操作行为进行检测、报警和恢复的能力	9.1.4.8 软件容错；9.1.5.3 数据备份和恢复；9.2.5.11 备份与恢复管理

安全目标	基本要求
O3-26.应具有严格控制机房进出的能力	9.1.1.2 物理访问控制；9.2.5.1 环境管理
O3-27.应具有防止设备、介质等丢失的能力	9.1.1.3 防盗窃和防破坏；9.1.1.2 物理访问控制；9.2.5.1 环境管理；9.2.5.3 介质管理
O3-28.应具有严格控制机房内人员活动的能力	9.1.1.2 物理访问控制；9.2.5.1 环境管理；9.1.1.3 防盗窃和防破坏
O3-29.应具有实时监控机房内部活动的能力	9.1.1.2 物理访问控制；9.1.1.3 防盗窃和防破坏
O3-30.应具有对物理入侵事件进行报警的能力	9.1.1.2 物理访问控制；9.1.1.3 防盗窃和防破坏
O3-31.应具有控制接触重要设备、介质的能力	9.1.1.2 物理访问控制；9.1.1.3 防盗窃和防破坏
O3-32.应具有对通信线路进行物理保护的能力	9.1.1.2 物理访问控制；9.1.1.3 防盗窃和防破坏
O3-33.应具有使重要通信线路及时恢复的能力	9.1.5.3 数据备份和恢复；9.2.5.11 备份与恢复管理
O3-34.应具有限制网络、操作系统和应用系统资源使用的能力	9.1.3.9 系统资源控制；9.1.4.9 资源控制
O3-35.应具有合理分配、控制网络、操作系统和应用系统资源的能力	9.1.2.1 结构安全和网段划分；9.1.3.9 系统资源控制；9.1.4.9 资源控制
O3-36.应具有能够检测、分析、响应对网络和重要主机的各种攻击的能力	9.1.2.6 网络入侵防范；9.1.3.7 入侵防范
O3-37.应具有发现所有已知漏洞并及时修补的能力	9.1.2.7 恶意代码防范；9.1.3.8 恶意代码防范；9.2.1.5 审核和检查；9.2.5.6 网络安全管理；9.2.5.7 系统安全管理
O3-38.应具有对网络、系统和应用的访问进行严格控制的能力	9.1.2.8 网络设备防护；9.1.2.2 网络访问控制；9.1.3.1 身份鉴别；9.1.3.2 自主访问控制；9.1.3.3 强制访问控制；9.1.4.1 身份鉴别；9.1.4.2 访问控制
O3-39.应具有对数据、文件或其他资源的访问进行严格控制的能力	9.1.2.2 网络访问控制;9.1.2.3 拨号访问控制;9.1.3.2 自主访问控制;9.1.3.3 强制访问控制；9.1.4.2 访问控制
O3-40.应具有对资源访问的行为进行记录、分析并响应的能力	9.1.2.4 网络安全审计；9.1.3.4 安全审计；9.1.4.3 安全审计
O3-41.应具有对恶意代码的检测、阻止和清除能力	9.1.2.7 恶意代码防范；9.1.3.8 恶意代码防范；9.2.5.8 恶意代码防范管理
O3-42.应具有防止恶意代码在网络中扩散的能力	9.1.2.7 网络恶意代码安全；9.1.3.8 恶意代码防范；9.2.5.8 恶意代码防范管

安全目标	基本要求
	理
O3-43.应具有对恶意代码库和搜索引擎及时更新的能力	9.1.2.7 恶意代码防范；9.1.3.8 恶意代码防范；9.2.5.8 恶意代码防范管理
O3-44.应具有保证鉴别数据传输和存储保密性的能力	9.1.5.2 数据保密性
O3-45.应具有对用户进行唯一标识的能力	9.1.2.8 网络设备防护；9.1.3.1 身份鉴别；9.1.4.1 应用系统身份鉴别
O3-46.应具有对同一个用户产生多重鉴别信息并进行多重鉴别的能力	9.1.2.8 网络设备防护；9.1.3.1 身份鉴别；9.1.4.1 应用系统身份鉴别
O3-47.应具有对硬件设备进行唯一标识的能力	9.1.2.8 网络设备防护；9.1.3.1 身份鉴别
O3-48.应具有对硬件设备进行合法身份确定的能力	9.1.2.8 网络设备防护；9.1.3.1 身份鉴别
O3-49.应具有检测非法接入设备的能力	9.1.2.5 边界完整性检查
O3-50.应具有对存储介质中的残余信息进行删除的能力	9.1.3.6 剩余信息保护；9.1.4.4 剩余信息保护；9.2.5.3 介质管理
O3-51.应具有对传输和存储中的信息进行保密性保护的能力	9.1.4.6 通信保密性；9.1.5.2 数据保密性
O3-52.应具有防止加密数据被破解的能力	9.1.4.6 通信保密性；9.1.5.2 数据保密性；9.2.4.4 产品采购；9.2.5.9 密码管理
O3-53.应具有路由选择和控制的能力	9.1.2.1 结构安全和网段划分
O3-54.应具有信息源发的鉴别能力	9.1.4.7 抗抵赖
O3-55.应具有通信数据完整性检测和纠错能力	9.1.4.5 通信完整性
O3-56.应具有对关键区域进行电磁屏蔽的能力	9.1.1.10 电磁防护
O3-57.应具有持续非活动状态一段时间后自动切断连接的能力	9.1.2.8 网络设备防护；9.1.3.1 身份鉴别；9.1.4.1 身份鉴别；9.1.3.9 系统资源控制；9.1.4.9 资源控制；9.2.5.1 环境管理
O3-58.应具有基于密码技术的抗抵赖能力	9.1.4.7 抗抵赖
O3-59.应具有防止未授权下载、拷贝软件或者文件的能力	9.1.2.7 恶意代码防范；9.1.3.8 恶意代码防范；9.2.5.8 恶意代码防范管理
O3-60.应具有网络边界完整性检测能力	9.1.2.5 边界完整性检查
O3-61.应具有切断非法连接的能力	9.1.2.5 边界完整性检查

安全目标	基本要求
O3-62.应具有重要数据和程序进行完整性检测和纠错能力	9.1.4.5 通信完整性；9.1.5.1 数据完整性；9.1.3.7 入侵防范
O3-63.应具有对敏感信息进行标识的能力	9.1.3.3 强制访问控制；9.1.4.2 访问控制；9.2.5.2 资产管理；9.2.5.3 介质管理
O3-64.应具有对敏感信息的流向进行控制的能力	9.1.3.3 强制访问控制；9.2.5.2 资产管理；9.2.5.3 介质管理
O3-65.应具有及时恢复重要数据的能力	9.1.5.3 数据备份和恢复；9.2.5.11 备份与恢复管理
O3-66.应具有保证重要业务系统及时恢复运行的能力	9.1.5.3 数据备份和恢复；9.2.5.11 备份与恢复管理
O3-67.应确保建立了安全职能部门，配备了安全管理人员，支持信息安全管理工作	9.2.1.1 岗位设置；9.2.1.2 人员配备
O3-68.应确保配备了足够数量的管理人员，对系统进行运行维护	9.2.1.2 人员配备；9.2.5.5 监控管理；
O3-69.应确保对管理活动进行了制度化管理	9.2.2.1 管理制度；9.2.2.2 制定和发布
O3-70.应确保建立并不断完善、健全安全管理制度	9.2.2.2 制定和发布；9.2.2.3 评审和修订
O3-71.应确保能协调信息安全工作在各功能部门的实施	9.2.1.4 沟通和合作
O3-72.应确保能控制信息安全相关事件的授权与审批	9.2.1.3 授权和审批
O3-73.应确保建立恰当可靠的联络渠道，以便安全事件发生时能得到支持	9.2.1.4 沟通和合作；9.2.5.12 安全事件处置
O3-74.应确保对人员的行为进行控制和规范	9.2.2.1 管理制度；9.2.3.1 人员录用；9.2.3.2 人员离岗；9.2.3.3 人员考核；9.2.3.5 第三方人员访问管理
O3-75.应确保对人员的管理活动进行了指导	9.2.2.1 管理制度；9.2.3.4 安全意识教育和培训
O3-76.应确保安全策略的正确性和安全措施的合理性	9.2.1.5 审核和检查
O3-77.应确保对信息系统进行合理定级，并进行备案管理	9.2.4.1 系统定级
O3-78.应确保安全产品的可信度和产品质量	9.2.4.4 产品采购
O3-79.应确保自行开发过程和工程实施过程中的安全	9.2.4.5 自行软件开发；9.2.4.7 工程实施
O3-80.应确保能顺利地接管和维护信息系统	9.2.4.9 系统交付
O3-81.应确保安全工程的实施质量和安全功能的准确实现	9.2.4.3 安全方案设计；9.2.4.8 测试验收；9.2.4.10 安全测评；9.2.4.11 安

安全目标	基本要求
	全服务商选择
O3-82.应确保机房具有良好的运行环境	9.2.5.1 环境管理
O3-83.应确保对各种软硬件设备的选型、采购、发放、使用和保管等过程进行控制	9.2.5.3 介质管理；9.2.5.4 设备管理
O3-84.应确保对信息资产进行分类标识管理	9.2.5.2 资产管理
O3-85.应确保各种网络设备、服务器正确使用和维护	9.2.2.1 管理制度；9.2.5.5 监控管理
O3-86.应确保对网络、操作系统、数据库系统和应用系统进行安全管理	9.2.5.6 网络安全管理；9.2.5.7 系统安全管理
O3-87.应确保用户具有鉴别信息使用的安全意识	9.2.3.4 安全意识教育和培训；9.2.5.7 系统安全管理
O3-88.应确保定期地对通信线路进行检查和维护	9.2.5.3 介质管理；9.2.5.4 设备管理
O3-89.应确保硬件设备、存储介质存放环境安全，并对其进行控制和保护	9.2.5.1 环境管理；9.2.5.3 介质管理；9.2.5.4 设备管理
O3-90.应确保对支撑设施、硬件设备、存储介质进行日常维护和管理	9.2.5.5 监控管理；9.2.5.3 介质管理；9.2.5.4 设备管理
O3-91.应确保系统中使用的硬件、软件产品的质量	9.2.4.4 产品采购；9.2.4.5 自行软件开发；9.2.4.6 外包软件开发；9.2.4.8 测试验收
O3-92.应确保各类人员具有与其岗位相适应的技术能力	9.2.3.1 人员录用；9.2.3.4 安全意识教育和培训
O3-93.应确保对各类人员进行相关的技术培训	9.2.3.4 安全意识教育和培训
O3-94.应确保提供的足够的使用手册、维护指南等资料	9.2.4.6 外包软件开发；9.2.4.4 产品采购；9.2.2.1 管理制度；9.2.5.5 监控管理
O3-95.应确保内部人员具有安全方面的常识和意识	9.2.3.4 安全意识培训和教育
O3-96.应确保具有设计合理、安全网络结构的能力	9.2.4.3 安全方案设计
O3-97.应确保对软硬件的分发过程进行控制	9.2.5.3 介质管理；9.2.5.4 设备管理；9.2.5.8 恶意代码防范管理
O3-98.应确保软硬件中没有后门程序	9.2.4.6 外包软件开发；9.2.4.4 产品采购；9.2.4.8 测试验收；9.2.5.8 恶意代码防范管理

安全目标	基本要求
O3-99.应确保密码算法和密钥的使用符合国家有关法律、法规的规定	9.2.5.9 密码管理
O3-100.应确保任何变更控制和设备重用要申报和审批，并对其实行制度化的管理	9.2.1.3 授权和审批；9.2.5.10 变更管理
O3-101.应确保在事件发生后能采取积极、有效的应急策略和措施	9.2.5.12 安全事件处置；9.2.5.13 应急预案管理；9.2.5.11 备份和恢复管理
O3-102. 应确保信息安全事件实行分等级响应、处置	9.2.5.12 安全事件处置

C4.四级

安全目标	基本要求
O4-1.应具有对抗中等强度地震、台风等自然灾难造成破坏的能力	10.1.1.1 物理位置的选择；10.1.5.3 数据备份和恢复；10.2.5.11 备份与恢复管理
O4-2.应具有防止雷击事件导致大面积设备被破坏的能力	10.1.1.1 物理位置的选择；10.1.1.4 防雷击；10.1.5.3 数据备份和恢复；10.2.5.11 备份与恢复管理
O4-3.应具有防水和防潮的能力	10.1.1.6 防水和防潮
O4-4.应具有对水患检测和报警的能力	10.1.1.6 防水和防潮
O4-5.应具有自动灭火的能力	10.1.1.5 防火
O4-6.应具有检测火灾和报警的能力	10.1.1.5 防火
O4-7.应具有防止火灾蔓延的能力	10.1.1.5 防火
O4-8.应具有温湿度自动检测和控制的能力	10.1.1.8 温湿度控制
O4-9.应具有防止电压波动的能力	10.1.1.9 电力供应
O4-10.应具有对抗长时间断电的能力	10.1.1.9 电力供应
O4-11.应具有防止静电导致大面积设备被破坏的能力	10.1.1.7 防静电
O4-12.应具有检测静电和消除静电的能力	10.1.1.7 防静电
O4-13.应具有对机房电磁屏蔽的能力	10.1.1.10 电磁防护

安全目标	基本要求
O4-14.应具有防止强电磁场、强震动源和强噪声源等污染影响系统正常的能力	10.1.1.1 物理位置的选择；10.1.1.10 电磁防护
O4-15.应具有监测通信线路传输状况的能力	10.2.5.6 网络安全管理；10.2.5.5 监控管理
O4-16.应具有系统软件、应用软件容错的能力	10.1.4.8 软件容错；10.1.3.6 系统保护
O4-17.应具有软件故障分析的能力	10.1.4.8 软件容错；10.2.5.5 监控管理
O4-18.应具有软件状态监测和报警的能力	10.1.3.8 入侵防范；10.2.5.5 监控管理
O4-19.应具有自动保护当前工作状态的能力	10.1.3.6 系统保护；10.1.4.8 软件容错；10.1.5.3 数据备份和恢复
O4-20.应具有自动恢复到故障前工作状态的能力	10.1.4.8 软件容错；10.1.5.3 数据备份和恢复；10.2.5.11 备份与恢复管理
O4-21.应具有合理使用和控制系统资源的能力	10.1.3.10 系统资源控制；10.1.4.9 资源控制
O4-22.应具有按优先级自动分配系统资源的能力	10.1.3.10 系统资源控制；10.1.4.9 资源控制
O4-23.应具有对传输和存储数据进行完整性检测和纠错的能力	10.1.4.5 通信完整性；10.1.5.1 数据完整性
O4-24.应具有对软件缺陷进行检查的能力	10.1.4.10 代码安全;10.2.4.5 产品采购;10.2.4.6 自行软件开发;10.2.4.7 外包软件开发
O4-25.应具有记录用户操作行为和分析记录结果的能力	10.1.2.4 网络安全审计；10.1.3.5 安全审计；10.1.4.3 安全审计
O4-26.应具有对用户的误操作行为进行检测、报警和恢复的能力	10.1.4.8 软件容错；10.1.5.3 数据备份和恢复；10.2.5.11 备份与恢复管理
O4-27.应具有安全机制失效的自动检测和报警能力	10.1.3.6 系统保护;10.1.2.4 网络安全审计;10.1.3.5 安全审计;10.1.4.3 安全审计；10.2.5.5 监控管理
O4-28.应具有检测到安全机制失效后恢复安全机制的能力	10.1.3.6 系统保护；10.1.4.8 软件容错；10.1.5.3 数据备份和恢复；10.2.5.11 备份与恢复管理
O4-29.应具有严格控制机房进出的能力	10.1.1.2 物理访问控制；10.2.5.1 环境管理
O4-30.应具有防止设备、介质等丢失的能力	10.1.1.3 防盗窃和防破坏；10.1.1.2 物理访问控制；10.2.5.1 环境管理；

安全目标	基本要求
	10.2.5.3 介质管理
O4-31.应具有严格控制机房内人员活动的能力	10.1.1.2 物理访问控制；10.2.5.1 环境管理；10.1.1.3 防盗窃和防破坏
O4-32.应具有实时监控机房内部活动的能力	10.1.1.2 物理访问控制；10.1.1.3 防盗窃和防破坏
O4-33.应具有对物理入侵事件进行报警的能力	10.1.1.2 物理访问控制；10.1.1.3 防盗窃和防破坏
O4-34.应具有控制接触重要设备、介质的能力	10.1.1.2 物理访问控制；10.1.1.3 防盗窃和防破坏
O4-35.应具有对通信线路进行物理保护的能力	10.1.1.2 物理访问控制；10.1.1.3 防盗窃和防破坏
O4-36.应具有使重要通信线路及时恢复的能力	10.1.5.3 数据备份和恢复；10.2.5.11 备份与恢复管理
O4-37.应具有限制网络、操作系统和应用系统资源使用的能力	10.1.3.10 系统资源控制；10.1.4.9 资源控制
O4-38.应具有能够检测、集中分析、响应、阻止对网络和所有主机的各种攻击的能力	10.1.2.6 网络入侵防范；10.1.3.8 入侵防范
O4-39.应具有合理分配、控制网络、操作系统和应用系统资源的能力	10.1.2.1 结构安全和网段划分；10.1.3.10 系统资源控制；10.1.4.9 资源控制
O4-40.应具有发现所有已知漏洞并及时修补的能力	10.1.2.7 恶意代码防范；10.1.3.9 恶意代码防范；10.2.1.5 审核和检查；10.2.5.6 网络安全管理；10.2.5.7 系统安全管理
O4-41.应具有对网络、系统和应用的访问进行严格控制的能力	10.1.2.8 网络设备防护；10.1.2.2 网络访问控制；10.1.3.1 身份鉴别；10.1.4.1 身份鉴别；10.1.3.2 自主访问控制；10.1.3.3 强制访问控制；10.1.4.2 访问控制
O4-42.应具有对数据、文件或其他资源的访问进行严格控制的能力	10.1.2.2 网络访问控制；拨号访问控制；10.1.3.2 自主访问控制；10.1.3.3 强制访问控制；10.1.4.2 访问控制
O4-43.应具有对资源访问的行为进行记录、集中分析并响应的能力	10.1.2.4 网络安全审计；10.1.3.5 安全审计；10.1.4.3 安全审计
O4-44.应具有对恶意代码的检测、集中分析、阻止和清除能力	网络 10.1.2.7 恶意代码防范；主机 10.1.2.7 恶意代码防范；10.1.2.7 恶意代码防范管理

安全目标	基本要求
O4-45.应具有防止恶意代码在网络中扩散的能力	10.1.2.7 网络恶意代码安全；10.1.3.9 恶意代码防范；10.2.5.8 恶意代码防范管理
O4-46.应具有对恶意代码库和搜索引擎及时更新的能力	10.1.2.7 恶意代码防范；10.1.3.9 恶意代码防范；10.2.5.8 恶意代码防范管理
O4-47.应具有保证鉴别数据传输和存储保密性的能力	10.1.5.2 数据保密性
O4-48.应具有对用户进行唯一标识的能力	10.1.2.8 网络设备防护；10.1.3.1 身份鉴别；10.1.4.1 身份鉴别
O4-49.应具有对同一个用户产生多重鉴别信息，其中一个是不可伪造的鉴别信息并进行多重鉴别的能力	10.1.2.8 网络设备防护；10.1.3.1 身份鉴别；10.1.4.1 身份鉴别
O4-50.应具有对硬件设备进行唯一标识的能力	10.1.2.8 网络设备防护；10.1.3.1 身份鉴别
O4-51.应具有对硬件设备进行合法身份确定的能力	10.1.2.8 网络设备防护；10.1.3.1 身份鉴别
O4-52.应具有检测非法接入设备的能力	10.1.2.5 边界完整性检查
O4-53.应具有对传输和存储中的信息进行保密性保护的能力	10.1.4.6 通信保密性；10.1.5.2 数据保密性；10.1.3.4 可信路径
O4-54.应具有对存储介质中的残余信息进行删除的能力	10.1.3.7 剩余信息保护；10.1.4.4 剩余信息保护；10.2.5.3 介质管理
O4-55.应具有防止加密数据被破解的能力	10.1.4.6 通信保密性;10.1.5.2 数据保密性;10.2.4.4 产品采购;10.2.5.9 密码管理
O4-56.应具有路由选择和控制的能力	10.1.2.1 结构安全和网段划分
O4-57.应具有信息源发的鉴别能力	10.1.4.7 抗抵赖
O4-58.应具有对关键区域进行电磁屏蔽的能力	10.1.1.10 电磁防护
O4-59.应具有持续非活动状态一段时间后自动切断连接的能力	10.1.2.8 网络设备防护;10.1.3.1 身份鉴别;10.1.4.1 身份鉴别;10.1.3.10 系统资源控制；10.1.4.9 资源控制；10.2.5.1 环境管理
O4-60.应具有基于密码技术的抗抵赖能力	10.1.4.7 抗抵赖
O4-61.应具有防止未授权下载、拷贝软件或者文件的能力	10.1.2.7 恶意代码防范；10.1.3.9 恶意代码防范；10.2.5.8 恶意代码防范管理

安全目标	基本要求
O4-62.应具有网络边界完整性检测能力	10.1.2.5 边界完整性检查
O4-63.应具有切断非法连接的能力	10.1.2.5 边界完整性检查
O4-64.应具有重要数据和程序进行完整性检测和纠错能力	10.1.4.5 通信完整性；10.1.5.1 数据完整性；10.1.3.8 入侵防范
O4-65.应具有对敏感信息进行标识的能力	10.1.3.3 强制访问控制；10.1.4.2 访问控制；10.2.5.2 资产管理；1.2.5.3 介质管理
O4-66.应具有对敏感信息的流向进行控制的能力	10.1.3.3 强制访问控制；资产管理；1.2.5.3 介质管理
O4-67.应具有迅速恢复重要数据的能力	10.1.5.3 数据备份和恢复；10.2.5.10 备份与恢复管理
O4-68.应具有保证通信不中断的能力	10.1.5.3 数据备份和恢复；10.2.5.10 备份与恢复管理
O4-69.应具有保证业务系统不中断的能力	10.1.5.3 数据备份和恢复；10.2.5.10 备份与恢复管理
O4-70.应确保建立了安全职能部门，配备了安全管理人员，支持信息安全管理工作	10.2.1.1 岗位设置；10.2.1.2 人员配备
O4-71.应确保配备了足够数量的管理人员，对系统进行运行维护	10.2.1.2 人员配备；10.2.5.5 监控管理；
O4-72.应确保对管理活动进行了制度化管理	10.2.2.1 管理制度；10.2.2.1 制定和发布
O4-73.应确保不断完善、健全安全管理制度	10.2.2.3 评审和修订
O4-74.应确保能协调信息安全工作在各功能部门的实施	10.2.1.4 沟通和合作
O4-75.应确保能控制信息安全相关事件的授权与审批	10.2.1.3 授权和审批
O4-76.应确保建立恰当可靠的联络渠道，以便安全事件发生时能得到支持	10.2.1.4 沟通和合作；10.2.5.12 安全事件处置
O4-77.应确保对人员的行为进行控制和规范	10.2.2.1 管理制度；10.2.3.1 人员录用；10.2.3.2 人员离岗；10.2.3.3 人员考核；10.2.3.5 第三方人员访问管理
O4-78.应确保对人员的管理活动进行了指导	10.2.2.1 管理制度；10.2.3.4 安全意识教育和培训
O4-79.应确保安全策略的正确性和安全措施的合理性	10.2.1.5 审核和检查
O4-80.应确保对信息系统进行合理定级，并进行备案管理	10.2.4.1 系统定级；10.2.4.2 系统备案
O4-81.应确保安全产品的可信度和产品质量	10.2.4.4 产品采购；10.2.4.8 测试验收

安全目标	基本要求
O4-82.应确保自行开发过程和工程实施过程中的安全	10.2.4.3 自行软件开发；10.2.4.7 工程实施
O4-83.应确保能顺利地接管和维护信息系统	10.2.4.9 系统交付
O4-84.应确保安全工程的实施质量和安全功能的准确实现	10.2.4.3 安全方案设计；10.2.4.8 测试验收；10.2.4.10 安全测评；10.2.4.11 安全服务商选择
O4-85.应确保机房具有良好的运行环境	10.2.5.1 环境管理
O4-86.应确保对信息资产进行分类标识、分级管理	10.2.5.1 资产管理
O4-87.应确保对各种软硬件设备的选型、采购、发放、使用和保管等过程进行控制	10.2.5.3 介质管理；10.2.5.4 设备管理
O4-88.应确保各种网络设备、服务器正确使用和维护	10.2.2.1 管理制度；10.2.5.5 监控管理
O4-89.应确保对网络、操作系统、数据库系统和应用系统进行安全管理	10.2.5.7 系统安全管理；10.2.5.6 网络安全管理
O4-90.应确保用户具有鉴别信息使用的安全意识	10.2.3.4 安全意识教育和培训；10.2.5.7 系统安全管理
O4-91.应确保定期地对通信线路进行检查和维护	10.2.5.3 介质管理；10.2.5.4 设备管理
O4-92.应确保硬件设备、存储介质存放环境安全，并对其的使用进行控制和保护	10.2.5.1 环境管理；10.2.5.3 介质管理；10.2.5.4 设备管理
O4-93.应确保对支撑设施、硬件设备、存储介质进行日常维护和管理	10.2.5.5 监控管理；1.2.5.3 介质管理；10.2.5.4 设备管理
O4-94.应确保系统中使用的硬件、软件产品的质量	10.2.4.4 产品采购；10.2.4.6 外包软件开发；10.2.4.5 自行软件开发；10.2.4.8 测试验收
O4-95.应确保各类人员具有与其岗位相适应的技术能力	10.2.3.1 人员录用；10.2.3.4 安全意识教育和培训
O4-96.应确保对各类人员进行相关的技术培训	10.2.3.4 安全意识教育和培训
O4-97.应确保提供的足够的使用手册、维护指南等资料	10.2.4.6 外包软件开发;10.2.4.4 产品采购;10.2.2.1 管理制度;10.2.5.5 监控管理；
O4-98.应确保内部人员具有安全方面的常识和意识	10.2.3.4 安全意识培训和教育
O4-99.应确保具有设计合理、安全网络结构的能力	10.2.4.3 安全方案设计

安全目标	基本要求
O4-100.应确保对软硬件的分发过程进行控制	1.2.5.3 介质管理；10.2.5.4 设备管理；10.2.5.8 恶意代码防范管理
O4-101. 应确保软硬件中没有后门程序和隐蔽信道	10.2.4.6 外包软件开发;10.2.4.4 产品采购;10.2.4.8 测试验收;10.2.5.8 恶意代码防范管理
O4-102. 应确保密码算法和密钥的使用符合国家有关法律、法规的规定	10.2.5.9 密码管理
O4-103. 应确保任何变更控制和设备重用要申报和审批，并对其实行制度化的管理	10.2.1.3 授权和审批；10.2.5.10 变更管理
O4-104. 应确保在事件发生后能采取积极、有效的应急策略和措施	10.2.5.12 安全事件处置；10.2.5.13 应急预案管理；10.2.5.10 备份和恢复管理
O4-105. 应确保信息安全事件实行分等级响应、处置	10.2.5.12 安全事件处置

附录 D 基本要求与安全目标的关系

D1.一级

基本要求	安全目标
7.1.1.1 物理访问控制	O1-10；O1-11；O1-12
7.1.1.2 防盗窃和防破坏	O1-11；O1-12
7.1.1.3 防雷击	O1-1
7.1.1.4 防火	O1-3
7.1.1.5 防水和防潮	O1-2
7.1.1.6 温湿度控制	O1-4
7.1.1.7 电力供应	O1-5
7.1.2.1 结构安全和网段划分	O1-9
7.1.2.2 网络访问控制	O1-14；O1-15
7.1.2.3 拨号访问控制	O1-15
7.1.2.4 网络设备防护	O1-14；O1-16
7.1.3.1 身份鉴别	O1-14；O1-16
7.1.3.2 自主访问控制	O1-14；O1-15
7.1.3.3 恶意代码防范	O1-13；O1-18
7.1.4.1 身份鉴别	O1-14；O1-16
7.1.4.2 访问控制	O1-14；O1-15
7.1.4.3 通信完整性	O1-6
7.1.4.4 软件容错	O1-7
7.1.4.5 资源控制	O1-8
7.1.4.6 代码安全	O1-35
7.1.5.1 数据完整性	O1-6

7.1.5.2 数据保密性	O1-17
7.1.5.3 数据备份和恢复	O1-19
7.2.1.1 岗位设置	O1-20
7.2.1.2 人员配备	O1-20
7.2.1.3 授权和审批	O1-23
7.2.1.4 沟通和合作	O1-24
7.2.2.1 管理制度	O1-25；O1-41
7.2.2.2 制定和发布	O1-21
7.2.3.1 人员录用	O1-25；O1-39
7.2.3.2 人员离岗	O1-25
7.2.3.3 安全意识教育和培训	O1-34；O1-39；O1-40；O1-42
7.2.3.4 第三方人员访问管理	O1-25
7.2.4.1 系统定级	O1-22
7.2.4.2 安全方案设计	O1-9；O1-29
7.2.4.3 产品采购	O1-26；O1-38；O1-41
7.2.4.4 自行软件开发	O1-27；O1-38
7.2.4.5 外包软件开发	O1-38；O1-41
7.2.4.6 工程实施	O1-27
7.2.4.7 测试验收	O1-29；O1-38
7.2.4.8 系统交付	O1-28
7.2.4.9 安全服务商选择	O1-29
7.2.5.1 环境管理	O1-10；O1-11；O1-30；O1-36
7.2.5.2 资产管理	O1-31
7.2.5.3 介质管理	O1-11；O1-36；O1-37
7.2.5.4 设备管理	O1-11；O1-32；O1-35；O1-36；O1-37

7.2.5.5 监控管理	O1-37；O1-41
7.2.5.6 网络安全管理	O1-13；O1-33
7.2.5.7 系统安全管理	O1-13；O1-33；O1-34
7.2.5.8 恶意代码防范管理	O1-18
7.2.5.9 备份与恢复管理	O1-19
7.2.5.10 安全事件处置	O1-24；O1-43

D2.二级

基本要求	安全目标
8.1.1.1 物理位置的选择	O2-1；O2-2
8.1.1.2 物理访问控制	O2-18；O2-19；O2-20；O2-21；O2-23
8.1.1.3 防盗窃和防破坏	O2-19；O2-20；O2-21；O2-23；
8.1.1.4 防雷击	O2-2
8.1.1.5 防火	O2-4；O2-5
8.1.1.6 防水和防潮	O2-3
8.1.1.7 防静电；	O2-9
8.1.1.8 温湿度控制	O2-6
8.1.1.8 电力供应	O2-7；O2-8
8.1.1.10 电磁防护	O2-10
8.1.2.1 结构安全和网段划分	O2-67
8.1.2.2 网络访问控制	O2-27；O2-28；
8.1.2.3 拨号访问控制	O2-28
8.1.2.4 网络安全审计	O2-16；O2-29
8.1.2.5 边界完整性检查	O2-38
8.1.2.6 网络入侵防范	O2-25

8.1.2.7 恶意代码防范	O2-26；O2-32；O2-33；O2-34；O2-43
8.1.2.8 网络设备防护	O2-27；O2-30；O2-31；O2-37
8.1.3.1 身份鉴别	O2-27；O2-30；O2-31；O2-37
8.1.3.2 自主访问控制	O2-27；O2-28；O2-37
8.1.3.3 安全审计	O2-16；O2-29
8.1.3.4 系统保护	O2-13
8.1.3.5 剩余信息保护	O2-36
8.1.3.6 恶意代码防范	O2-26；O2-32；O2-33；O2-34
8.1.3.7 系统资源控制	O2-15；O2-24；O2-37
8.1.4.1 身份鉴别	O2-27；O2-30；O2-31
8.1.4.2 访问控制	O2-27；O2-28
8.1.4.3 安全审计	O2-16；O2-29
8.1.4.4 剩余信息保护	O2-36
8.1.4.5 通信完整性	O2-11
8.1.4.6 通信保密性	O2-22
8.1.4.7 软件容错	O2-13；O2-14；O2-17
8.1.4.8 资源控制	O2-15；O2-24；O2-37
8.1.4.8 代码安全	O2-62
8.1.5.1 数据完整性	O2-11
8.1.5.2 数据保密性	O2-22；O2-35
8.1.5.3 数据备份和恢复	O2-1；O2-2；O2-12；O2-17；O2-39
8.2.1.1 岗位设置	O2-40
8.2.1.2 人员配备	O2-40；O2-41
8.2.1.3 授权和审批	O2-45；O2-71
8.2.1.4 沟通和合作	O2-44；O2-46

8.2.1.5 审核和检查	O2-26；O2-49
8.2.2.1 管理制度	O2-42；O2-47；O2-48；O2-58；O2-67
8.2.2.2 制定和发布	O2-42
8.2.2.3 评审和修订	O2-43
8.2.3.1 人员录用	O2-47；O2-65
8.2.3.2 人员离岗	O2-47
8.2.3.3 人员考核	O2-47
8.2.3.4 安全意识教育和培训	O2-48；O2-60；O2-65；O2-66；O2-68
8.2.3.5 第三方人员访问管理	O2-47
8.2.4.1 系统定级	O2-50
8.2.4.2 安全方案设计	O2-54；O2-69
8.2.4.3 产品采购	O2-51；O2-64；O2-67
8.2.4.4 自行软件开发	O2-52；O2-64
8.2.4.5 外包软件开发	O2-64；O2-67
8.2.4.6 工程实施	O2-52
8.2.4.7 测试验收	O2-54；O2-64
8.2.4.8 系统交付	O2-53
8.2.4.9 安全服务商选择	O2-54
8.2.5.1 环境管理	O2-18；O2-19；O2-20；O2-37；O2-55；O2-62
8.2.5.2 资产管理	O2-56
8.2.5.3 介质管理	O2-19；O2-36；O2-57；O2-61；O2-62；O2-63
8.2.5.4 设备管理	O2-57；O2-61；O2-62；O2-63
8.2.5.5 监控管理	O2-14；O2-41；O2-58；O2-63；O2-67
8.2.5.6 网络安全管理	O2-26；O2-59
8.2.5.7 系统安全管理	O2-26；O2-59；O2-60

8.2.5.8 恶意代码防范管理	O2-32；O2-33；O2-34
8.2.5.9 密码管理	O2-70
8.2.5.10 变更管理	O2-71
8.2.5.11 备份与恢复管理	O2-1；O2-2；O2-12；O2-17；O2-39；O2-72
8.2.5.12 安全事件处置	O2-46；O2-72；O2-73
8.2.5.13. 应急预案管理	O2-72

D3.三级

基本要求	安全目标
9.1.1.1 物理位置的选择	O3-1；O3-2；O3-13
9.1.1.2 物理访问控制	O3-26；O3-27；O3-28；O3-29；O3-30；O3-31；O3-32
9.1.1.3 防盗窃和防破坏	O3-27；O3-28；O3-29；O3-30；O3-31；O3-32
9.1.1.4 防雷击	O3-2
9.1.1.5 防火	O3-5；O3-6；O3-7
9.1.1.6 防水和防潮	O3-3；O3-4
9.1.1.7 防静电；	O3-11
9.1.1.8 温湿度控制	O3-8
9.1.1.9 电力供应	O3-9；O3-10
9.1.1.9 电磁防护	O3-12；O3-13；O3-56
9.1.2.1 结构安全和网段划分	O3-35；O3-53
9.1.2.2 网络访问控制	O3-38；O3-39
9.1.2.3 拨号访问控制	O3-39
9.1.2.4 网络安全审计	O3-24；O3-40
9.1.2.5 边界完整性检查	O3-49；O3-60；O3-61
9.1.2.6 网络入侵防范	O3-36
9.1.2.7 恶意代码防范	O3-37；O3-41；O3-42；O3-43；O3-59

9.1.2.8 网络设备防护	O3-38；O3-45；O3-46；O3-47；O3-48；O3-57
9.1.3.1 身份鉴别	O3-38；O3-45；O3-46；O3-47；O3-48；O3-57
9.1.3.2 自主访问控制	O3-38；O3-39
9.1.3.3 强制访问控制	O3-38；O3-39；O3-63；O3-64
9.1.3.4 安全审计	O3-24；O3-40
9.1.3.5 系统保护	O3-17；O3-20
9.1.3.6 剩余信息保护	O3-50
9.1.3.7 入侵防范	O3-19；O3-36；O3-62
9.1.3.8 恶意代码防范	O3-37；O3-41；O3-42；O3-43；O3-59
9.1.3.9 系统资源控制	O3-21；O3-22；O3-34；O3-35；O3-57
9.1.4.1 身份鉴别	O3-38；O3-45；O3-46；O3-57
9.1.4.2 访问控制	O3-38；O3-39；O3-63
9.1.4.3 安全审计	O3-24；O3-40
9.1.4.4 剩余信息保护	O3-50
9.1.4.5 通信完整性	O3-16；O3-55；O3-62
9.1.4.6 通信保密性	O3-51；O3-52
9.1.4.7 抗抵赖	O3-54；O3-58
9.1.4.8 软件容错	O3-17；O3-18；O3-20；O3-25
9.1.4.9 资源控制	O3-21；O3-22；O3-34；O3-35；O3-57
9.1.4.9 代码安全	O3-23
9.1.5.1 数据完整性	O3-16；O3-62
9.1.5.2 数据保密性	O3-44；O3-51；O3-52
9.1.5.3 数据备份和恢复	O3-1；O3-2；O3-15；O3-25；O3-33；O3-65；O3-66
9.2.1.1 岗位设置	O3-67
9.2.1.2 人员配备	O3-67；O3-68

9.2.1.3 授权和审批	O3-72；O3-100
9.2.1.4 沟通和合作	O3-71；O3-73
9.2.1.5 审核和检查	O3-37；O3-76
9.2.2.1 管理制度	O3-69；O3-74；O3-75；O3-85；O3-94
9.2.2.2 制定和发布	O3-69
9.2.2.3 评审和修订	O3-70
9.2.3.1 人员录用	O3-74；O3-90
9.2.3.2 人员离岗	O3-74
9.2.3.3 人员考核	O3-74
9.2.3.4 安全意识教育和培训	O3-75
9.2.3.5 第三方人员访问管理	O3-74
9.2.4.1 系统定级	O3-77
9.2.4.2 系统备案	O3-77
9.2.4.3 安全方案设计	O3-81；O3-96
9.2.4.4 产品采购	O3-23；O3-52；O3-77；O3-91；O3-94；O3-98
9.2.4.5 自行软件开发	O3-23；O3-79；O3-91
9.2.4.6 外包软件开发	O3-23；O3-91；O3-94；O3-98
9.2.4.7 工程实施	O3-79
9.2.4.8 测试验收	O3-81；O3-91；O3-98
9.2.4.9 系统交付	O3-80
9.2.4.10 安全测评	O3-81
9.2.4.11 安全服务商选择	O3-81
9.2.5.1 环境管理	O3-26；O3-27；O3-28；O3-57；O3-82；O3-89
9.2.5.2 资产管理	O3-63；O3-64

9.2.5.3 介质管理	O3-27；O3-50；O3-63；O3-64；O3-83；O3-88；O3-89；O3-90；O3-97
9.2.5.4 设备管理	O3-83；O3-88；O3-89；O3-90；O3-97
9.2.5.5 监控管理	O3-14；O3-18；O3-19；O3-27；O3-68；O3-85；O3-90；O3-94
9.2.5.6 网络安全管理	O3-14；O3-37；O3-86
9.2.5.7 系统安全管理	O3-37；O3-86；O3-87
9.2.5.8 恶意代码防范管理	O3-41；O3-42；O3-43；O3-59；O3-97；O3-98
9.2.5.9 密码管理	O3-52；O3-99
9.2.5.10 变更管理	O3-100
9.2.5.11 备份与恢复管理	O3-1；O3-2；O3-15；O3-25；O3-33；O3-65；O3-66；O3-101
9.2.5.12 安全事件处置	O3-73；O3-101；O3-102
9.2.5.13. 应急预案管理	O3-101

D4.四级

基本要求	安全目标
10.1.1.1 物理位置的选择	O4-1；O4-2；O4-14
10.1.1.2 物理访问控制	O4-29；O4-30；O4-31；O4-32；O4-33；O4-34；O4-35
10.1.1.3 防盗窃和防破坏	O4-30；O4-31；O4-32；O4-33；O4-34；O4-35
10.1.1.4 防雷击	O4-2
10.1.1.5 防火	O4-5；O4-6；O4-7
10.1.1.6 防水和防潮	O4-3；O4-4
10.1.1.7 防静电；	O4-11；O4-12
10.1.1.8 温湿度控制	O4-8
10.1.1.9 电力供应	O4-9；O4-10

10.1.1.10 电磁防护	O4-13；O4-14；O4-58
10.1.2.1 结构安全和网段划分	O4-39；O4-56
10.1.2.2 网络访问控制	O4-41；O4-42；
10.1.2.3 拨号访问控制	O4-42
10.1.2.4 网络安全审计	O4-25；O4-27；O4-43
10.1.2.5 边界完整性检查	O4-52；O4-62；O4-63
10.1.2.6 网络入侵防范	O4-38
10.1.2.7 恶意代码防范	O4-40；O4-44；O4-45；O4-46；O4-61
10.1.2.8 网络设备防护	O4-41；O4-48；O4-49；O4-50；O4-51；O4-59
10.1.3.1 身份鉴别	O4-41；O4-48；O4-49；O4-50；O4-51；O4-59
10.1.3.2 自主访问控制	O4-41；O4-42
10.1.3.3 强制访问控制	O4-41；O4-42；O4-65；O4-66
10.1.3.4 可信路径	O4-53
10.1.3.5 安全审计	O4-25；O4-27；O4-43
10.1.3.6 系统保护	O4-16；O4-19；O4-27；O4-28
10.1.3.7 剩余信息保护	O4-25
10.1.3.8 入侵防范	O4-18；O4-38；O4-64
10.1.3.9 恶意代码防范	O4-40；O4-45；O4-46；O4-61
10.1.3.10 系统资源控制	O4-21；O4-22；O4-37；O4-39；O4-59
10.1.4.1 身份鉴别	O4-41；O4-48；O4-49；O4-59
10.1.4.2 访问控制	O4-41；O4-42；O4-65
10.1.4.3 安全审计	O4-25；O4-27；O4-43
10.1.4.4 剩余信息保护	O4-54
10.1.4.5 通信完整性	O4-23；O4-64
10.1.4.6 通信保密性	O4-53；O4-55

10.1.4.7 抗抵赖	O4-57；O4-60
10.1.4.8 软件容错	O4-16；O4-17；O4-19；O4-20；O4-26；O4-28
10.1.4.9 资源控制	O4-21；O4-22；O4-37；O4-39；O4-59
10.1.4.10 代码安全	O4-24
10.1.5.1 数据完整性	O4-23；O4-64
10.1.5.2 数据保密性	O4-47；O4-53；O4-55
10.1.5.3 数据备份和恢复	O4-1；O4-2；O4-19；O4-20；O4-26；O4-28；O4-36；O4-67；O4-68；O4-69
10.2.1.1 岗位设置	O4-70
10.2.1.2 人员配备	O4-70；O4-71
10.2.1.3 授权和审批	O4-75；O4-103
10.2.1.4 沟通和合作	O4-74；O4-76
10.2.1.5 审核和检查	O4-40；O4-79
10.2.2.1 管理制度	O4-72；O4-77；O4-78；O4-88；O4-97
10.2.2.2 制定和发布	O4-72
10.2.2.3 评审和修订	O4-73
10.2.3.1 人员录用	O4-77；O4-95
10.2.3.2 人员离岗	O4-77
10.2.3.3 人员考核	O4-77
10.2.3.4 安全意识教育和培训	O4-78；O4-90；O4-95；O4-96；O4-98
10.2.3.5 第三方人员访问管理	O4-77
10.2.4.1 系统定级	O4-80
10.2.4.2 系统备案	O4-80
10.2.4.3 安全方案设计	O4-84；O4-99
10.2.4.4 产品采购	O4-24；O4-55；O4-80；O4-94；O4-97；O4-101
10.2.4.5 自行软件开发	O4-24；O4-82

10.2.4.6 外包软件开发	O4-24；O4-97；O4-101
10.2.4.7 工程实施	O4-82
10.2.4.8 测试验收	O4-81；O4-84；O4-94；O4-101
10.2.4.9 系统交付	O4-83
10.2.4.10 安全测评	O4-84
10.2.4.11 安全服务商选择	O4-84
10.2.5.1 环境管理	O4-29；O4-30；O4-31；O4-59；O4-85；O4-92
10.2.5.2 资产管理	O4-65；O4-66
10.2.5.3 介质管理	O4-30；O4-54；O4-66；O4-87；O4-91；O4-92；O4-93
10.2.5.4 设备管理	O4-87；O4-91；O4-92；O4-93；O4-100
10.2.5.5 监控管理	O4-15；O4-17；O4-18；O4-27；O4-71；O4-88；O4-93；O4-97
10.2.5.6 网络安全管理	O4-15；O4-40；O4-89
10.2.5.7 系统安全管理	O4-40；O4-89；O4-90
10.2.5.8 恶意代码防范管理	O4-45；O4-46；O4-61；O4-100；O4-101
10.2.5.9 密码管理	O4-55；O4-102
10.2.5.10 变更管理	O4-103
10.2.5.11 备份与恢复管理	O4-1；O4-2；O4-19；O4-20；O4-26；O4-28；O4-36；O4-67；O4-68；O4-69；O4-104
10.2.5.12 安全事件处置	O4-104；O4-105
10.2.5.13. 应急预案管理	O4-104

参考文献

1 GB17859-1999 计算机信息系统安全等级划分准则

2 GB/T 18336-2000 信息技术 信息技术安全性评估准则

3 GB/T 19716-2005 信息技术 信息安全管理实用规则

4 GB/T 19715.2-2005 信息技术 信息安全管理指南 第 2 部分

5 GB/T XXXX — XXXX 信息安全技术 信息系统安全通用技术要求（送审稿）

6 GB/T XXXX — XXXX 信息安全技术 信息系统安全管理要求（送审稿）

7 GB/T XXXX — XXXX 信息安全技术 操作系统安全技术要求（送审稿）

8 GB/T XXXX — XXXX 信息安全技术 数据库管理系统安全技术要求（送审稿）

9 GB/T XXXX — XXXX 信息安全技术 物理安全技术要求（送审稿）

10 GB/T XXXX — XXXX 信息安全技术 信息安全风险评估指南（送审稿）

11 GA/T 390-2002 计算机信息系统安全等级保护通用技术要求

12 GA/T 391-2002 计算机信息系统安全等级保护安全管理要求

13 GA/T 388-2002 计算机信息系统安全等级保护操作系统技术要求

14 GA/T 389-2002 计算机信息系统安全等级保护数据库管理系统技术要求

15 NIST Special Publication 800-53 联邦信息系统推荐性安全控制措施

16 DoD Directive & Instruction 8500-1，2 信息保障 & 信息保障实施