ICS35.040
L80

中华人民共和国国家标准

GB/T ××××—××××

信息安全技术
信息系统安全等级保护实施指南

Information Security Technology-

Guide of Implementation for Classified

Security Protection of Information System

（送审稿_修订版 v1.1）

200×-××-××发布　　200×-××-××实施

国家质量监督检验检疫总局 发布

目　次

前　言

信息系统安全等级保护是信息安全等级保护工作的一个重要组成部分。为指导和规范信息系统安全等级保护工作的实施，特制定本标准。

本标准分为两部分：

第一部分：正文部分。介绍了信息系统的安全等级和保护要求等相关概念；说明了信息系统安全等级保护实施过程中涉及的角色；信息系统安全等级保护实施的基本原则；信息系统安全等级保护实施的基本过程；信息系统安全等级保护实施的主要阶段和主要活动以及与信息系统生命周期之间的关系；提出了信息系统安全等级保护在信息系统生命周期不同阶段的实施要点、实施流程、具体的活动内容以及活动的输入输出等，并对其进行了详细的描述。

第二部分：附录部分。列表说明了各个主要阶段的主要活动，以及各个活动的输入、输出产品和主要参考的相关标准，并对各阶段的主要输出产品进行了标注。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：公安部信息安全等级保护评估中心 。

引　言

1994 年国务院颁布的《中华人民共和国计算机信息系统安全保护条例》规定计算机信息系统实行信息系统安全等级保护。2003 年中央办公厅、国务院办公厅转发的《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）中明确指出：“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息系统安全等级保护制度，制定信息系统安全等级保护的管理办法和技术指南”。2004 年公安部等四部委《关于信息系统安全等级保护工作的实施意见》（公通字[2004]66 号）也指出：“信息系统安全等级保护制度是国家在国民经济和社会信息化的发展过程中，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设健康发展的一项基本制度”。

为配合我国信息系统安全等级保护制度的实施，以 GB17859-1999《计算机信息系统安全保护等级划分准则》为首的相关配套系列标准正在陆续发布或正在开发之中，本标准是这些相关配套系列标准之一。

本标准以信息系统安全等级保护建设为主要线索，结合信息系统的生命周期定义了信息系统安全等级保护实施的主要阶段，介绍了每个阶段实施的主要活动，针对每个活动说明了实施的主体、活动目标、主要活动内容、主要输入和输出以及需要参考的主要标准等。

信息系统安全等级保护
实施指南

1　范围

本标准规定了信息系统安全等级保护实施的方法和过程，适用于各类机构或组织对某个具体信息系统实施安全等级保护工作。

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。

GB/T 5271.8-2001　信息技术 词汇 第 8 部分：安全

GB17859-1999　计算机信息系统安全保护等级划分准则

3　术语和定义

GB/T 5271.8-2001 和 GB 17859-1999 确立的以及下列术语和定义适用于本标准。

3.1

信息系统安全等级 security classifications of information system

信息系统重要程度的表征。重要程度从信息系统受到破坏后，对国家安全、社会秩序、经济建设和公共利益造成的损害来衡量。

3.2

信息系统安全等级保护 Classified Security Protection of Information System

对信息系统分等级实施安全保护。

3.3

业务子系统 business subsystem

由信息系统的一部分组件构成，能够完成某项业务工作的系统。

3.4

业务信息安全性 security of business information

保证业务信息机密性、完整性和可用性程度的表征。

3.5

业务服务保证性　business assurance

保证业务系统完成使命程度的表征，业务使命可能因系统无法提供服务或无法提供有效服务而不能完成。

3.6

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。

3.7

基本保护要求 basic protection requirements

为确保信息系统具有与其安全等级相对应的安全保护能力应该满足的最低要求。

3.8

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。

3.9

安全域 security domains

具有相同安全保护策略的区域。

3.10

安全测评 security testing and evaluating

对信息系统的安全保护能力是否达到相应保护要求的衡量。

3.11

系统终止 system expiration

信息系统完成了自己的使命，被终止不用。

3.12

监督检查 supervision and inspection

对信息系统安全保护制度和措施的落实情况的检查。

4 等级保护概述

4.1. 等级保护目标

实行等级保护的总体目标是为了统一信息安全保护工作，推进规范化、法制化建设，保障安全，促进发展，完善我国信息安全法规和标准体系，提高我国信息安全和信息系统安全建设的整体水平；通过充分调动国家、法人和其他组织及公民的积极性，发挥各方面的作用，达到对信息和信息系统重点保护和有效保护的目的，增强安全保护的整体性、针对性和实效性，使信息安全和信息系统安全建设更加突出重点、统一规范、科学合理。

4.2. 等级保护对象

等级保护的对象是信息和信息系统，等级保护工作涉及到三个方面，即对信息系统分等级实施安全保护、对信息系统中使用的信息安全产品实行分等级管理、对信息系统中发生的信息安全事件分等级响应、处置。

本标准主要提供对信息系统分等级实施安全保护的指导，关于国家对信息安全产品的使用实行分等级管理以及信息安全事件实行分等级响应、处置的管理参见其他的相关标准。在本标准后续的条款中所指的“等级保护”，其含义均为“信息系统分等级实施安全保护”。

4.3. 系统安全等级

信息系统可以分为五个安全等级，国家对不同级别的信息系统实行不同强度的监管政策：

a) 第一级为自主保护级

主要对象为一般的信息系统，其业务信息安全性或业务服务保证性受到破坏后，会对公民、法人和其他组织的合法权益产生损害，但不损害国家安全、社会秩序和公共利益；本级系统依照国家管理规范和技术标准进行自主保护。

b) 第二级为指导保护级

主要对象为一般的信息系统，其业务信息安全性或业务服务保证性受到破坏后，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；本级系统依照国家管理规范和技术标准进行自主保护，必要时，信息安全监管职能部门对其进行指导。

c) 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，其业务信息安全性或业务服务保证性受到破坏后，会对国家安全、社会秩序和公共利益造成严重损害；本级系统依照国家管理规范和技术标准进行自主保护，信息安全监管职能部门对其进行监督、检查。

d) 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，其业务信息安全性或业务服务保证性受到破坏后，会对国家安全、社会秩序和公共利益造成严重损害；本级系统依照国家管理规范和技术标准进行自主保护，信息安全监管职能部门对其进行强制监督、检查。

e) 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，其业务信息安全性或业务服务保证性受到破坏后，会对国家安全、社会秩序和公共利益造成特别严重损害；本级系统依照国家管理规范和技术标准进行自主保护，国家指定专门部门、专门机构进行专门监督、检查。

信息系统的类型千差万别、错综复杂，大型、复杂的信息系统通常由完成不同使命、承载不同业务、处理不同数据的多个信息系统构成，应根据信息系统的重要程度，分别确定每个信息系统的安全等级。大型、复杂的信息系统应该考虑是由不同安全等级的几个小型信息系统构成，从而达到对整个信息系统区分保护和重点保护的目的。

4.4. 基本保护要求

信息系统在被确定了安全等级后，需要根据国家对不同安全等级的信息系统应达到的安全保护能力要求进行保护。国家对信息系统的安全保护能力要求为基本保护要求，对不同安全等级的信息系统有不同的基本保护要求，国家按照基本保护要求对信息系统实行不同强度的监管。

国家对不同安全等级的信息系统提出的基本保护要求，是对不同信息系统相同保护要求的共性的抽取，是保障各等级信息系统安全的最基本要求。对特定信息系统的安全保护，应以其相应等级的基本保护要求为基础，然后结合自身的特点进行安全需求分析，对基本保护要求进行调整和定制。对不同安全等级信息系统的基本保护要求参见相关的国家标准。

5 等级保护实施过程

5.1. 基本原则

等级保护的核心是对信息系统分等级、按标准进行建设、管理和监督。等级保护在实施过程中应遵循以下基本原则：

a) 自主保护原则

由各主管部门和运营使用单位按照国家相关法规和标准，自主确定信息系统的安全等级，自行组织实施安全保护。

b) 同步建设原则

信息系统在新建、改建、扩建时应当同步规划和设计安全方案，投入一定比例的资金建设信息安全设施，保障信息安全与信息化建设相适应。

c) 重点保护原则

根据信息系统的重要程度、业务特点，通过划分不同安全等级的信息系统，实现不同强度的安全保护，集中资源优先保护涉及核心业务或关键信息资产的信息系统。

d) 适当调整原则

要跟踪信息系统的变化情况，调整安全保护措施。因为信息系统的应用类型、范围等条件的变化及其他原因，安全等级需要变更的，应当根据等级保护的管理规范和技术标准的要求，重新确定信息系统的安全等级，根据信息系统安全等级的调整情况，重新实施安全保护。

5.2. 角色和职责

对一个信息系统实施等级保护的过程中涉及到各类组织和人员，他们将会参与不同的或相同的活动，比如信息系统的主管单位和信息系统的运营单位将参与系统定级活动，如果委托安全服务商进行定级，则安全服务商也会参与定级活动；又如信息系统的运营、使用单位可以自己完成风险分析活动，也可以委托安全服务商完成风险分析活动。

本标准中将参与等级保护过程的各类组织和人员划分为主要角色和次要角色。其中主要角色将参与等级保护实施过程的所有活动，次要角色将参与等级保护实施过程的某一个或多个活动。主要角色是指信息系统主管部门和信息系统运营、使用单位；次要角色是指信息系统安全服务商、信息安全监管机构、安全测评机构和安全产品提供商。

等级保护实施过程中各类角色的职责如下：

a) 信息系统主管部门

信息系统主管部门的主要责任是做好下属单位的等级保护监督管理工作；组织、协调和督促下属单位按照等级保护的管理规范和技术标准对信息系统进行等级保护；对下属单位确定的信息系统安全等级进行审批；督促下属单位定期进行安全状况检测评估，及时消除安全隐患和漏洞等。

b) 信息系统运营、使用单位

信息系统运营、使用单位的主要责任是按照等级保护的管理规范和技术标准，确定其信息系统的安全等级，并报其主管部门审批同意；对安全等级在三级以上的信息系统，报送本地区地市级公安机关备案；根据已经确定的安全等级，按照等级保护的管理规范和技术标准，进行信息系统的规划设计、建设施工；采购和使用相应等级的信息安全产品，建设安全设施，落实安全技术措施；对已经完成等级保护建设的信息系统进行检查评估，发现问题及时整改，；加强和完善自身等级保护制度的建设，加强自我保护；定期进行安全状况检测评估，及时消除安全隐患和漏洞，建立安全制度，制定不同等级信息安全事件的响应、处置预案，加强信息系统的安全管理。

c) 信息系统安全服务商

信息系统安全服务商的主要责任是根据信息系统运营、使用单位的委托，按照等级保护的管理规范和技术标准，协助信息系统运营、使用单位完成等级保护的相关工作，可能包括确定其信息系统的安全等级、进行安全需求分析、进行信息系统的规划设计、建设施工等。

d) 信息安全监管机构

信息安全监管机构的主要责任是对不同重要程度的信息系统的等级保护工作给予相应的指导，确保等级保护工作顺利开展；按照等级保护的管理规范和技术标准的要求，重点对第三、第四级信息系统的等级保护状况进行监督检查；发现存在安全隐患或未达到等级保护的管理规范和技术标准要求的，要限期整改，使信息系统的安全保护措施更加完善；对信息系统中使用的信息安全产品的等级进行监督检查。

e) 安全测评机构

安全测评机构的主要责任是根据信息系统运营、使用单位的委托或根据信息安全监管机构的委托，协助信息系统运营、使用单位或信息安全监管职能部门，按照等级保护的管理规范和技术标准，对已经完成等级保护建设的信息系统进行检查评估；对安全产品供应商提供的安全产品进行检查评估。

f) 安全产品供应商

安全产品供应商的主要责任是按照等级保护的管理规范和技术标准，开发符合等级保护要求的安全产品；提交安全产品进行安全等级测评并按照等级保护要求销售安全产品。

5.3. 实施的基本过程

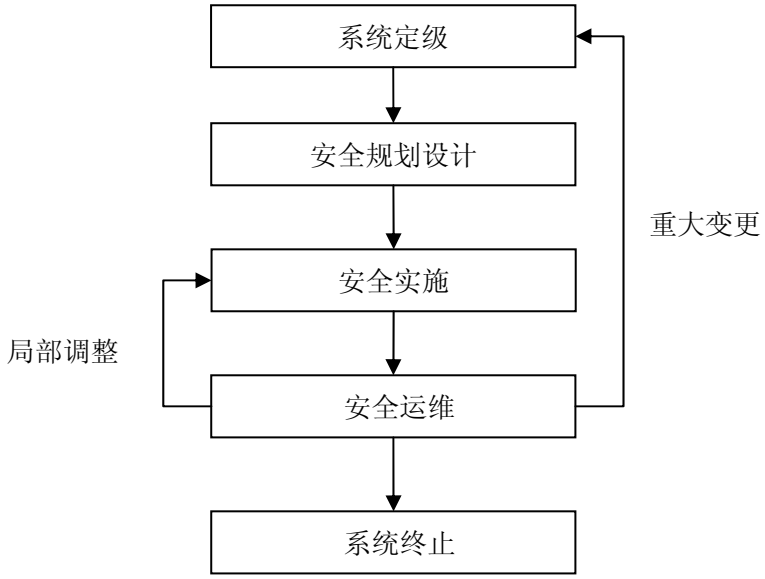

图 5-1 信息系统安全等级保护实施的基本过程

对一个信息系统实施等级保护的过程中涉及的活动很多，根据安全的动态性理论，很多活动需要重复执行，从而保证安全保护的有效性，虽然安全保护是一个不断循环和不断提高的过程，但是实施等级保护的一次完整过程是可以区分清楚的，比如从系统定级、系统安全运维，最终到系统终止，为了便于清晰划分等级保护的一次实施过程，有必要根据信息系统的一个生命周期确定等级保护实施的过程。

对一个信息系统实施等级保护的过程如图 5-1 所示：

对信息系统实施等级保护的过程包括五个主要阶段，系统定级阶段、安全规划设计阶段、安全实施阶段、安全运维阶段、系统终止阶段。在安全运维阶段，当局部调整等原因导致安全措施的变化时，如果不影响系统的安全等级，应从安全运维阶段进入安全实施阶段，重新调整和实施安全措施，确保满足等级保护的要求；在安全运维阶段，当系统发生重大变更导

致影响系统的安全等级时，应从安全运维阶段进入系统定级阶段，重新开始一次等级保护的实施过程。

5.4. 主要阶段和主要活动

对信息系统实施等级保护的过程划分为五个阶段，即系统定级阶段、安全规划设计阶段、安全实施阶段、安全运维阶段和系统终止阶段。

a) 系统定级阶段

系统定级阶段通过对信息系统调查和分析，进行信息系统划分，确定包括的相对独立的信息系统的个数，选择合适的信息系统安全等级定级方法，科学、准确地确定每个信息系统的安全等级。

通常情况下，系统定级阶段包括系统识别和描述、信息系统划分和安全等级确定等几个主要安全活动。

b) 安全规划设计阶段

安全规划设计阶段通过安全需求分析判断信息系统的安全保护现状与国家等级保护基本要求之间的差距，确定安全需求，然后根据信息系统的划分情况、信息系统定级情况、信息系统承载业务情况和安全需求等，设计合理的、满足等级保护要求的总体安全方案，并制定出安全实施规划等，以指导后续的信息系统安全建设工程实施。

通常情况下，安全规划设计阶段包括安全需求分析、安全总体设计、安全建设规划等几个主要活动。

c) 安全实施阶段

安全实施阶段通过安全方案详细设计、安全产品的采购、安全控制的开发、安全控制集成、机构和人员的配置、安全管理制度的建设、人员的安全技能培训等环节，将规划阶段的安全方针和策略，具体落实到信息系统中去，其最终的成果是提交满足用户安全需求的信息系统以及配套的安全管理体系。

通常情况下，安全实施阶段包括安全方案详细设计、等级保护技术实施和等级保护管理实施等几个主要活动。

安全管理体系的建设应该贯穿信息系统的整个生命周期，涉及等级保护实施过程的各个阶段。本标准中为了便于叙述，只在安全实施阶段强调了等级保护管理实施过程。

d) 安全运维阶段

安全运维阶段将介绍运行管理和控制、变更管理和控制、安全状态监控以及安全事件处置和应急预案等过程；通过运行管理和控制、变更管理和控制、对安全状态进行监控，对发生的安全事件及时响应，确保信息系统正常运行；通过安全检查和持续改进不断跟踪信息系统的变化，并依据变化进行调整，确保信息系统满足相应等级的安全要求，处于良好安全状态。

安全运维阶段需要进行的安全控制活动很多，本标准描述一些重要的安全控制活动，如运行管理和控制、变更管理和控制、安全状态监控以及安全事件处置和应急预案等。

e) 系统终止阶段

系统终止阶段是对信息系统的过时或无用部分进行报废处理的过程，主要涉及对信息、设备、存储介质或整个信息系统的废弃处理。系统终止阶段的主要活动可能包括对信息的转

移、暂存或清除，对设备迁移或废弃，对存储介质的清除或销毁；系统终止阶段当要迁移或废弃系统组件时，核心关注点是防止敏感信息泄漏。

等级保护实施过程的主要活动如图 5-2 所示。等级保护实施过程中的各类角色应在从事各类活动时不断提高自己的活动能力；对于专门从事等级保护工作的信息系统安全服务商和安全测评机构，应在等级保护实施过程中不断完善自己的质量体系，使自己的等级保护实施能力不断提高、逐渐成熟。

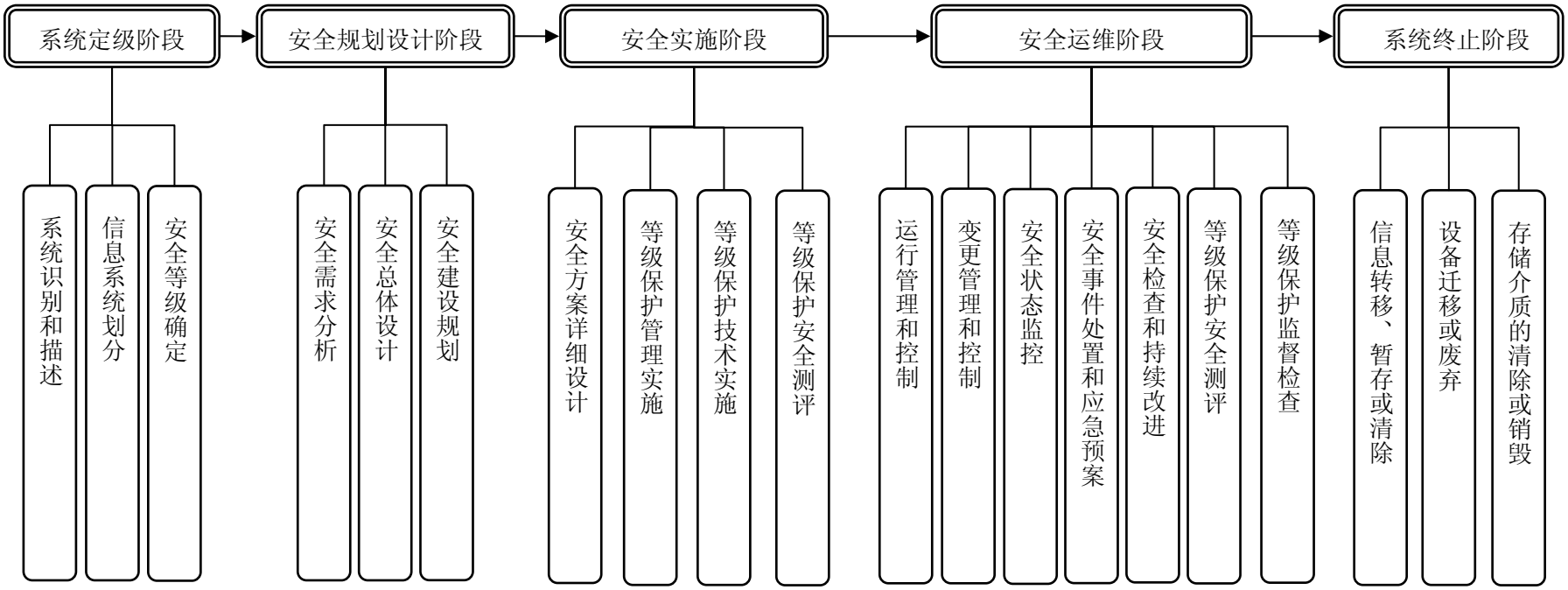

图 5-2　等级保护实施过程的主要活动

5.5. 与信息系统生命周期的关系

信息系统存在生命周期，关于信息系统的生命周期不同的方法论有不同的描述方法，最常见的观点认为信息系统生命周期包括五个阶段，即启动准备阶段、设计/开发阶段、实施/实现阶段、运行维护阶段和系统终止阶段。等级保护的实施活动与信息系统生命周期中的其他活动有着不可分割的关系，同时等级保护实施活动又有自己的特点，等级保护工作将贯穿信息系统生命周期的各个阶段。

等级保护实施的过程与信息系统生命周期的关系如图 5-4 所示。

等级保护的实施分为新建信息系统等级保护的实施和已建信息系统等级保护的实施，两者在信息系统生命周期中的切入点是不同的。

新建信息系统在生命周期中的各个阶段应同步考虑等级保护实施的主要活动。在启动准备阶段，应该仔细分析和合理划分各个信息系统，确定各个信息系统的安全等级，定级过程也可能在设计/开发阶段实施；在设计/开发阶段，应该根据各个信息系统的安全等级，进行安全需求分析，合理规划设计网络结构、应用系统、安全保护措施等，确保各个信息系统按照国家等级保护的要求进行规划设计；在实施/实现阶段，应在系统建设的同时，同步进行安全措施的落实和实现；在系统运行维护阶段，应按照国家等级保护的要求进行安全维护和安全管理；在系统终止阶段，应对系统的废弃过程进行有效安全管理。

已建信息系统通常处于系统运行维护阶段，由于在启动准备阶段、设计/开发阶段和实施/实现阶段可能没有同步考虑国家等级保护的要求，因此，应在信息系统运行维护阶段开始启动等级保护工作，等级保护实施过程中的系统定级阶段、安全规划设计阶段、安全实施阶段的主要活动都将在信息系统生命周期的系统运行维护阶段完成。由于是已经存在的信息系统，工作的重点应放在系统定级阶段如何划分信息系统并确定安全等级、在安全规划设计阶段如何规划设计出符合国家等级保护要求的安全改造方案、在安全实施阶段如何保证在不影响现有业务应用的情况下使各类安全措施可以顺利落实等方面。

无论是新建的信息系统或已建的信息系统，虽然等级保护实施的切入点在信息系统生命周期的不同阶段，但是对信息系统实施等级保护的主要活动基本相同，当然，本标准的读者可以针对两类信息系统的特点在安全活动上进行必要的调整和裁减。

图 5-3 等级保护过程与信息系统生命周期对应关系

6 系统定级

6.1. 定级方法

系统定级是实施等级保护的前提和基础。信息系统安全等级的确定是否准确直接关系到是否对信息系统采取了足够的安全保护措施，是否能够将信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度降到最低。

信息系统定级可以选择但不局限于以下方法：

a) 根据经验直接定级

信息系统的主管单位、信息系统的运营、使用单位将本机构拥有的各个信息系统按照其在国家安全、经济建设、社会生活中的重要程度进行排序，并形成信息系统重要程度列表，通过与信息系统的五个安全等级的定义进行对比，确定每个信息系统的安全等级。

b) 自行制定定级方法

信息系统运营、使用单位根据本行业或自身信息系统的特点，参照国家发布的有关确定信息系统安全等级的定级方面标准和方法，制定适合本行业或自身信息系统的定级方法，对所管辖范围内或所拥有的信息系统进行科学、准确地定级。

c) 按照定级标准定级

信息系统运营、使用单位根据国家发布的有关确定信息系统安全等级的定级方面标准和方法，对所拥有的信息系统进行科学、准确地定级。

在这里要强调的是，信息系统的安全等级确定可能不是一个过程就可以完成的，可能要经过信息系统划分、定级要素赋值、信息系统定级、定级结果调整、定级要素重新赋值、信息系统再定级、定级结果再调整的循环过程，最终才能确定出较为准确的信息系统安全等级。

6.2. 定级活动流程

系统定级主要包括以下几个步骤：

第一步 系统识别和描述

系统识别过程充分利用查询相关文档、编制调查表、与有关人员访谈、现场实地观察等多种方式尽可能多的收集信息系统相关信息，对收集到的信息系统相关信息进行综合分析和整理，在此基础上针对所有信息系统形成准确的信息系统描述文件。

第二步 信息系统划分

信息系统划分过程为拥有多个信息系统的组织部门提供了将复杂的信息系统分解为多个相对独立的信息系统的方法和步骤，并且明确了如果一个信息系统包含多个业务，为了方便定级则可以进行业务子系统划分，并形成信息系统/业务子系统列表和每个业务子系统的描述性文件。

第三步 安全等级确定

安全等级确定是在系统识别和描述、信息系统划分和业务子系统划分活动结束后，依据确定的定级方法确定信息系统的安全等级，并形成信息系统定级结果的统一描述性文件。

系统定级阶段的活动流程如图 6-1 所示。

通常情况下，系统定级阶段包括系统识别和描述、信息系统划分、安全等级确定等几个主要安全活动，但读者可根据目标系统的实际情况对活动的内容进行裁减。

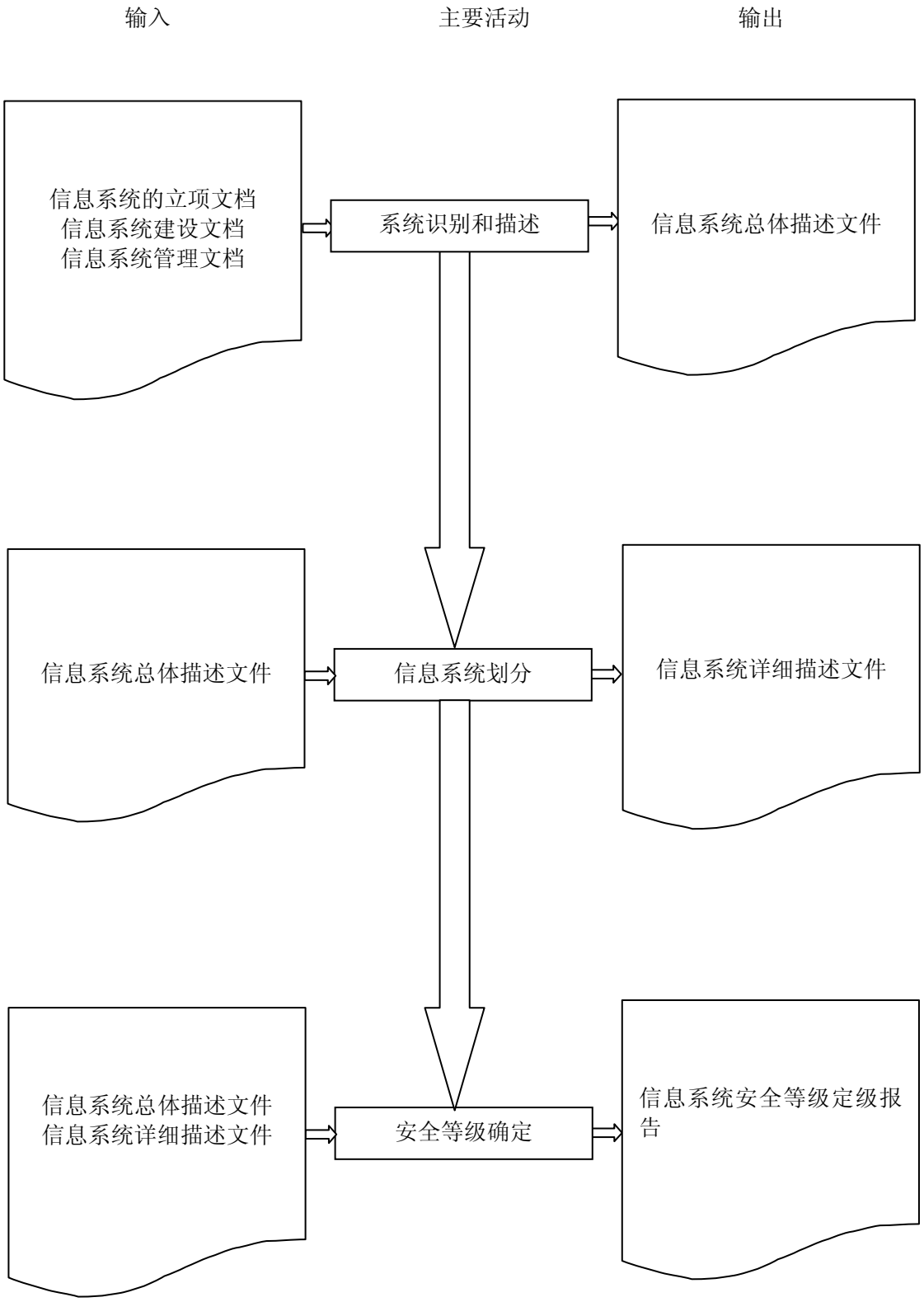

图 6-1 系统定级阶段基本流程

6.3. 系统识别和描述

活动目标：

本活动的目标是通过从信息系统运营、使用单位相关人员处收集有关信息系统的信息，并对信息进行综合分析和整理，依据分析和整理的内容准确描述，形成组织机构内所有信息系统的总体描述性文档。

参与角色：信息系统运营、使用单位，安全服务商。

活动输入：信息系统的立项、建设、管理文档

活动描述：

系统识别和描述过程主要包括以下活动内容：

a) 识别信息系统的基本信息

调查了解信息系统的行业特征、主管机构、业务范围、地理位置以及信息系统基本情况，获得信息系统的背景信息和联络方式。

b) 识别信息系统的管理框架

了解信息系统的组织管理结构、管理策略、部门设置和部门在业务运行中的作用、岗位职责、，获得支持信息系统业务运营的管理特征和管理框架方面的信息。管理框架是将信息系统划分为不同的业务子系统时首要的参考因素。

c) 识别信息系统的网络及设备部署

具有相同的或相似的运行环境意味着系统所面临的威胁相似，有利于采取统一策略的安全保护。因此，系统调查很重要的一个活动就是了解信息系统的物理环境、网络拓扑结构和硬件设备的部署情况，在此基础上明确信息系统的边界，即确定等级保护的对象和范围。

d) 识别信息系统的业务种类和特性

了解机构内主要依靠信息系统处理的有多少种业务，这些业务各自的社会属性，业务内容和业务流程等，从中明确支持机构业务运营的信息系统的业务特性，相同的业务特征和安全需求可能遵循同样的安全策略，有助于将处理相同类型数据或相似类型数据业务构成的信息系统划分成一个独立的信息系统。

e) 识别业务系统处理的信息资产

了解业务系统处理的信息资产的类型，这些信息资产在保密性、完整性和可用性方面的重要性程度。

f) 识别用户范围和用户类型

根据用户或用户群的分布范围了解业务系统的服务范围、作用以及业务连续性方面的要求等。

g) 信息系统描述

对收集的信息进行整理、分析，形成对信息系统的总体描述文件。一个典型的信息系统的总体描述文件应包含但不限于以下内容：

1)系统概述；

2)系统边界描述；

3)网络拓扑；

4)设备部署；

5)支撑的业务应用的种类和特性；

6)处理的信息资产；

7)用户的范围和用户类型；

8)信息系统的管理框架。

活动输出： 信息系统总体描述文件

6.4. 信息系统划分

活动目标：

本活动的目标是依据信息系统的描述文件，在综合分析的基础上将组织机构内运行的信息系统进行合理分解，确定所包含信息系统的个数，如果某一个信息系统中包含多个业务子系统，对业务子系统进行划分，并对每个业务子系统进行描述。

参与角色：信息系统运营、使用单位，安全服务商。

活动输入：信息系统总体描述文件

活动描述：

信息系统划分包括以下主要的活动内容：

a) 划分方法的选择

一个组织机构可能会运行一个或多个信息系统，信息系统是接受相应等级保护管理的最小单元，进行信息系统划分的方法可以有多种，信息系统的运营、使用单位可以根据本单位的具体情况确定分解原则，按照既定的原则对信息系统进行分解。以下提供的划分方法，各单位可以根据需要选择其中的一种方法或几种方法的组合：

1) 从组织管理角度划分

根据组织机构的管理框架和管理范围划分信息系统。同一个管理机构的管理控制保证了遵循同样的管理策略。例如，对于一个大型机构来讲，不同管理部门负责管理的信息系统可以划分为一个单独的信息系统。

2) 从业务类型角度划分

根据业务类型和安全需求划分信息系统。相同的业务特征和安全需求保证了遵循同样的安全策略。例如，处理相同类型数据或相似类型数据业务构成的信息系统可以作为一个独立的信息系统；以信息处理为主的业务构成的信息系统可以划分为一个独立的信息系统；以业务处理为主的业务构成的信息系统可以划分为一个独立的系统。

3) 从物理区域角度划分

根据所处的运行环境划分信息系统。具有相同的或相似的运行环境意味着系统所面临的威胁相似，有利于采取统一策略的安全保护。例如，不同物理位置或区域的系统可以作为一个独立的信息系统。

b) 信息系统划分

依据选择的系统划分原则，将一个组织机构内拥有的多个信息系统进行划分，成为相对独立的信息系统。在信息系统划分的过程中，应该首先考虑组织管理的要素，然后考虑业务类型、物理区域等要素。

c) 业务子系统划分

信息系统是接受相应等级保护管理的最小单元，然而一个信息系统中也可能处理多种业

务，即包含多个业务子系统，业务子系统是被定级分析的最小单元。

为确定信息系统的安全等级，进行业务子系统划分是必要的。在业务子系统划分过程中，应保证业务子系统具有信息系统的全部特点，应该是由计算机硬件、计算机网络硬件以及安装于这些硬件上的软件构成的一个有形实体，并且应当承载确定的业务。

d) 信息系统和业务子系统描述

在对信息系统进行划分以及某些信息系统中的业务子系统进行划分后，应在信息系统总体描述文件的基础上，进一步增加信息系统划分信息的描述，准确描述一个大型信息系统中包括的分解的信息系统个数，每个信息系统包含的业务子系统信息等，进一步的信息系统详细描述文件应包含但不限于以下内容：

1) 信息系统列表；

2）每个信息系统的概述；

3) 每个信息系统的边界；

4) 每个信息系统的设备部署；

5) 每个信息系统支撑的业务应用的列表；

6）每个业务应用处理的信息资产类型；

7) 每个业务应用的服务范围和用户类型；

8) 每个业务应用的其他特性；

9) 等等。

活动输出： 信息系统详细描述文件

6.5. 安全等级确定

活动目标：

本活动的目标是确定每个信息系统的安全等级，信息系统的安全等级由所包括的各业务子系统的最高等级决定；并对定级过程文档进行整理，形成文件化的信息系统定级结果报告。

参与角色：信息系统运营、使用单位，信息系统主管部门，安全服务商

活动输入：信息系统总体描述文件、信息系统详细描述文件

活动描述：

信息系统安全等级的确定包括以下主要活动内容：

a) 各个业务子系统安全等级确定

依次确定每个业务子系统的安全等级，包括业务信息安全性等级和业务服务保证性等级，业务子系统的安全等级由业务信息安全性等级和业务服务保证性等级较高者决定。

b) 信息系统安全等级确定

根据每个信息系统所包含的业务子系统的个数、业务子系统的安全等级，确定每个信息系统的安全等级，每个信息系统的安全等级由其包含的各个业务子系统的最高安全等级决定，每个信息系统的业务信息安全性等级由各个业务子系统的业务信息安全性等级的最高等级决定，每个信息系统的业务服务保证性等级由各个业务子系统的业务服务保证性等级的最高等级决定。

c) 定级结果文档化

对信息系统的总体描述文档、信息系统的详细描述描述文件、信息系统安全等级确定结

果等内容进行整理，形成文件化的信息系统定级结果报告。

信息系统定级结果报告可以包括但不局限于以下内容：

1）单位信息化现状概述；

2) 管理模式；

3) 信息系统列表；

4）每个信息系统的概述；

5) 每个信息系统的边界；

6) 每个信息系统的设备部署；

7) 每个信息系统支撑的业务应用的列表和等级；

8) 信息系统列表、安全等级以及保护要求组合；

9) 等等。

活动输出：信息系统安全等级定级报告

7 安全规划设计

7.1. 安全规划设计阶段的活动流程

安全规划设计是等级保护实施过程中的一个重要阶段，安全规划设计阶段的目标是通过安全需求分析判断信息系统的安全保护现状与等级保护基本要求之间的差距，确定安全需求，然后根据信息系统的划分情况、信息系统的定级情况、信息系统承载业务情况和安全需求等，设计合理的、满足等级保护要求的总体安全方案，并制定出安全实施计划等，以指导后续的信息系统安全建设工程实施。

通常情况下，安全规划设计阶段包括安全需求分析、安全总体设计、安全建设规划几个主要活动，但使用者可根据自身系统的复杂程度对活动的内容进行裁减。对于大型的信息系统，比如包含多个不同等级的信息系统、涉及的地理范围较大、安全建设周期较长，则建议执行所有的活动。对于小型信息系统，比如只有一个安全等级且涉及范围不大的信息系统，可以执行部分活动。安全规划设计的活动流程如图 7-1 所示。

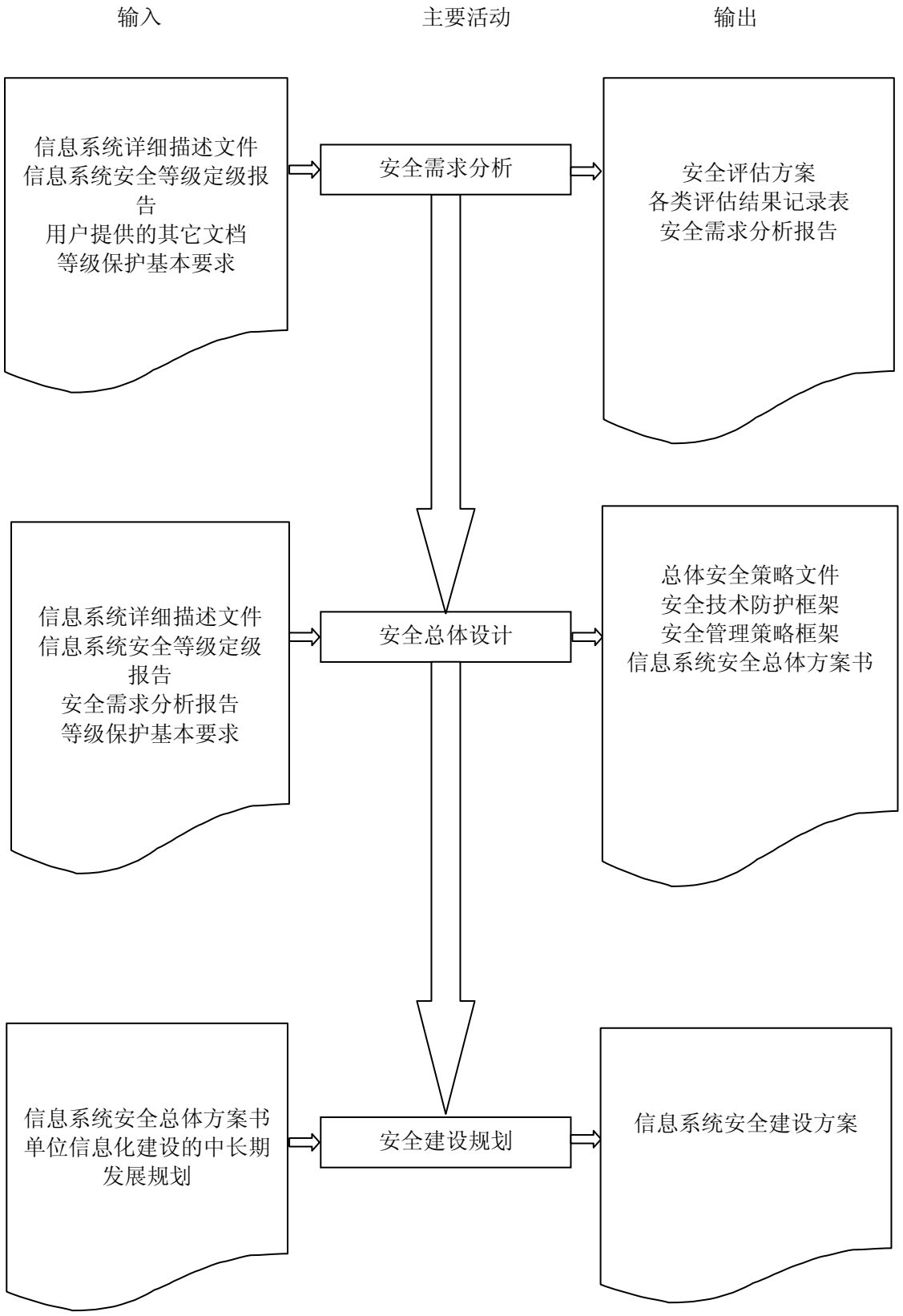

图 7-1 安全规划设计基本流程

信息系统安全规划设计阶段的主要活动内容如图 7-1 包括：

第一步 安全需求分析

安全需求分析首先应判断信息系统的安全保护现状与国家等级保护基本要求之间的差距，这种差距作为初步的安全需求；除上述安全需求外，还要通过风险分析的方法确定系统额外的安全需求，这种需求反映在对特殊环境和威胁的安全保护要求，或对系统重要对象的较高保护要求方面。通过现状差距的分析和特殊要求的分析，明确系统的完整安全需求。

安全需求分析的主要活动内容包括：

1) 评估对象和评估方法的明确；

2) 评估指标体系的选择和确定；

3) 安全现状和评估指标的对比；

4) 除与基本安全要求之间的差距外，额外安全需求的确定；

5) 评估结果的综合分析，形成安全需求分析报告。

第二步 安全总体设计

安全总体设计首先根据系统安全需求分析报告制定系统总体的安全策略，然后依据总体安全策略和等级保护相关要求，设计系统的安全技术框架和安全管理框架，形成系统符合等级保护要求，同时满足系统特定安全保护需求的安全总体方案。

安全总体设计并非等级保护实施过程中必须的执行过程，对于规模较小、构成内容简单的信息系统，在通过安全需求分析确定了信息系统的安全需求之后，可以直接进入安全实施阶段，参见本标准第 8 章。

安全总体设计的主要活动包括但不局限于以下内容：

1) 系统等级化模型处理；

2) 总体安全策略设计；

3) 各级系统安全技术措施设计；

4) 系统整体安全管理策略设计；

5) 设计结果文档化。

第三步 安全建设规划

安全建设规划首先根据系统的安全总体方案选择安全建设的策略，然后依据安全建设策略，规划中、长期的安全建设内容，制定安全建设的实施计划，形成指导今后一段时间内安全建设工作的安全建设规划方案。

安全建设规划也并非等级保护实施过程中必须的执行过程，在完成安全总体设计后，如果信息系统安全总体方案书中的大部分内容已经完成，剩余的建设内容少，建设周期短，则可以直接进入安全实施阶段，参见本标准第 8 章。

对于安全总体设计书中的大部分内容尚未建设，涉及内容多，建设周期长的信息系统，为了保证安全总体方案书中的内容获得有效实现，应实施安全建设规划过程，即结合机构信息化建设的总体规划、安全建设内容的缓急程度以及安全建设资金状况等规划未来一段时间内的安全建设项目。

安全建设规划的主要活动包括但不局限于以下内容：

a) 建设策略选择和建设目标确定；

b) 安全建设内容规划；

c) 安全建设方案设计；

d) 规划结果文档化。

7.2. 安全需求分析

7.2.1. 评估对象和评估方法的明确

活动目标：

本活动的目标是通过收集和了解被评估信息系统的网络结构、业务流程、设备信息和数据信息等，明确被评估信息系统的具体评估对象；通过分析被评估信息系统和具体评估对象的特性选择和确定具体的评估方法。

参与角色： 信息系统运营、使用单位，安全服务商

活动输入： 信息系统详细描述文件、信息系统安全等级定级报告、用户提供的其它文档

活动描述：

a) 确定评估范围

明确本次被评估系统的范围，包括每个信息系统的范围、各个等级信息系统的范围，信息系统的边界等。

b) 获得信息系统的信息

通过调查或查阅资料的方式，了解被评估信息系统的构成，包括网络拓扑、业务应用、业务流程、设备信息、安全措施状况等。

c) 确定具体的评估对象

初步确定每个等级信息系统的被评估对象，包括整体对象，如机房、办公环境、网络等，也包括具体对象，如边界设备、网关设备、服务器设备、工作站、应用系统等。

d) 确定评估工作的方法

根据信息系统安全等级情况、系统规模大小等，明确本次评估的方法，如所有对象的评估还是抽样方式的评估；询问、检查、测试的组合方式等。

e) 制定评估工作计划

制定评估工作计划或方案，说明评估范围、评估对象、工作方法、人员组成、角色职责、时间计划等。

活动输出：评估工作方案

7.2.2. 评估指标选择和组合

活动目标：

本活动的目标是根据被评估信息系统的安全等级，从等级保护基本要求的指标中选择和组合评估用的安全指标，形成一套信息系统的评估指标，作为评估的依据；将具体评估对象和评估指标进行结合，形成评估使用的评估方案。

参与角色： 信息系统运营、使用单位，安全服务商

活动输入： 信息系统详细描述文件、信息系统安全等级定级报告、评估工作方案、等级保护基本要求

活动描述：

a) 形成评估指标

根据各个信息系统的安全等级从基本要求中选择相应等级的通用指标，然后根据系统信息资产安全性等级选择信息资产安全性指标，根据系统连续性等级选择业务连续性指标，之后进行三类指标的组合，形成评估指标。

b) 制定评估方案

根据评估指标，结合确定的具体评估对象制定可以操作的评估方案，评估方案可以包括但不局限于以下内容：

1) 管理状况评估表格；
2) 网络状况评估表格；
3) 网络设备（含安全设备）评估表格；
4) 主机设备评估表格；
5) 主要设备安全测试方案；
6) 重要操作的作业指导书。

活动输出： 安全评估方案

7.2.3. 现状与评估指标对比

活动目标：

本活动的目标是根据所确定的安全评估指标和安全评估方案，通过询问、检查和测试等多种手段，将系统现状与安全评估指标进行逐一对比，记录当前的现状情况，找到与评估指标之间的差距。

参与角色： 信息系统运营、使用单位，安全服务商

活动输入：信息系统详细描述文件、信息系统安全等级定级报告、评估工作方案、安全评估方案

活动描述：

a) 判断安全管理方面与评估指标的符合程度

通过观察现场、询问人员、查询资料、检查记录等方式进行安全管理方面的评估，准确记录评估结果，判断安全管理的各个方面与评估指标的符合程度，给出判断结论。评估工作原始记录表应由相关人员确认签字。

b) 判断安全技术方面与评估指标的符合程度

通过观察现场、询问人员、查询资料、检查记录、检查配置、技术测试、渗透攻击等方式进行安全技术方面的评估，准确记录评估结果，判断安全技术的各个方面与评估指标的符合程度，给出判断结论。评估工作原始记录表应由相关人员确认签字。

活动输出： 各类评估结果记录表

7.2.4. 额外/特殊安全需求的确定

活动目标：

本活动的目标是通过对信息系统重要资产特殊保护要求的分析，确定超出相应等级保护要求的部分或具有独特安全保护要求的部分，采用需求分析/风险分析的方法，确定可能的安全风险，判断超出等级保护要求部分安全措施的必要性。

参与角色： 信息系统运营、使用单位，安全服务商

活动输入：信息系统详细描述文件、信息系统安全等级定级报告、评估工作方案、安全评估方案

活动描述：

在安全现状和评估指标对比后确定基本安全需求的基础上，通过需求分析/风险分析的手段可以确定额外或特殊的安全需求。确定额外安全需求可以采用目前成熟或流行的需求分析/风险分析方法，也可以采用但不局限于下面介绍的活动：

a) 重要资产的分析

明确信息系统中的重要部件，如边界设备、网关设备、核心网络设备、重要服务器设备、重要应用系统等。

b) 重要资产安全弱点评估

检查或判断上述重要部件可能存在的弱点，包括技术上和管理上的；分析安全弱点被利用的可能性。

c) 重要资产面临威胁评估

分析和判断上述重要部件可能面临的威胁，包括外部的威胁和内部的威胁，威胁发生的可能性或概率。

d) 综合风险分析

分析威胁利用弱点可能产生的安全事件，安全事件发生的可能性或概率，安全事件造成的损害或产生的影响大小，防止此种风险的必要性。按照重要资产的排序和风险的排序确定安全保护的要求。

活动输出： 重要资产的特殊保护要求

7.2.5. 形成安全需求分析报告

活动目标：

本活动的目标是总结安全指标对比结果和传统需求分析/风险分析的结果，获得系统安全现状的汇总、与等级保护基本要求的差距汇总和系统特殊安全保护要求的汇总，形成安全需求分析报告和等级化安全措施建议报告/安全需求分析报告。

参与角色： 信息系统运营、使用单位，安全服务商

活动输入：信息系统详细描述文件、信息系统安全等级定级报告、评估工作方案、安全评估方案、各类评估结果记录表、重要资产的特殊保护要求

活动描述：

a) 完成安全需求分析报告

根据各类评估结果记录表，分析和汇总各类评估数据，说明现有安全状况、现在存在的不足和可能的风险，特殊的安全保护需求等形成安全需求分析报告。

安全需求分析报告可以包括但不局限于以下内容：

1) 评估范围；
2) 评估方法；
3) 评估对象；
4) 评估过程；
5) 安全管理状况；

6) 安全技术状况；

7) 统计和汇总结果；

8) 存在的不足和可能的风险；

9) 等级化评估结论。

活动输出： 安全需求分析报告

7.3. 安全总体设计

7.3.1. 系统等级化模型处理

活动目标：

本活动的目标是对一个大型、复杂信息系统的构成内容进行抽象处理，提取共性形成模型，以便于针对模型要素提出统一的安全策略和安全措施要求，以指导等级保护工作的具体落实。

对于小规模信息系统可以不进行此活动。

参与角色： 信息系统运营、使用单位，安全服务商

活动输入： 信息系统详细描述文件、信息系统安全等级定级报告

活动描述：

a) 信息系统构成抽象处理

对于通过骨干网或城域网连接分布在多个不同物理地区的局域网构成，并且每个物理地区的局域网内划分为多个不同级别的业务子系统的情况，为了便于分析和处理，首先用模型表示信息系统的构成，将信息系统抽象为骨干网、城域网、局域网这些分析要素，通过抽象处理后，信息系统可以认为是由骨干网/城域网连接的多个局域网形成。当然，只由局域网构成的信息系统可以直接进行活动 C）。

b) 骨干网/城域网抽象处理

通常将骨干网/城域网分解为通信线路、网络设备和骨干网/城域网管理中心三个要素，暂不考虑骨干网/城域网内部的实现细节，认为骨干网/城域网是由通信线路连接网络设备构成的模型。通过对骨干网/城域网模型化处理后，关注点将放在通信线路、网络设备和骨干网/城域网的网络管理上，通过对通信线路、网络设备和网络管理提出安全策略要求和安全措施要求，实现骨干网/城域网的安全保护。

c) 局域网抽象处理

对于每个局域网可能是由多个不同级别的业务子系统构成的情况，无论局域网内部业务子系统有多少，可以将同级的或处理同类信息的业务子系统抽象为一个模型要素，我们称之为安全域，将域中业务子系统的最高级别定为安全域的级别。通过抽象处理后，局域网模型可能是由多个级别的安全域互联构成的模型，关注点将放在不同级别安全域互联和不同级别安全域的边界上，通过对不同级别的安全域互联、安全域边界提出安全策略要求和安全措施要求，实现对安全域边界的安全保护。

d) 安全域内部抽象处理

局域网中不同级别的安全域的规模和复杂程度可能不同，但是每个级别的安全域的构成要素基本一致，即是由服务器、工作站和连接它们构成网络的网络设备构成。为了便于分析和处理，将安全域内部抽象为服务器设备（包括存贮设备）、工作站设备和网络设备这些要

素，通过对安全域内部的模型化处理后，对每个安全域内部的关注点将放在服务器设备、工作站设备和网络设备上，通过对不同级别的安全域中的服务器设备、工作站设备和网络设备提出安全策略要求和安全措施要求，实现安全域内部的安全保护。

e) 形成信息系统抽象模型

通过对信息系统的分析和抽象处理，最终应形成被分析的信息系统的抽象模型。信息系统抽象模型的表达应包括以下内容：

1) 信息系统如何由骨干网、城域网、局域网构成，骨干网、城域网、局域网之间如何互联；

2) 局域网最多包含几个不同级别的安全域；

3) 局域网内部不同级别的安全域之间如何连接；

4) 不同局域网之间的安全域之间如何连接；

5) 局域网内部安全域是否与外部机构/单位或国际互联网有互联；

6) 等等。

活动输出： 信息系统等级化抽象模型

7.3.2. 总体安全策略设计

活动目标：

本活动的目标是形成机构纲领性的安全策略文件，包括确定安全方针，规定安全策略，以便结合等级保护基本要求和安全保护特定需求，构建机构信息系统的技术保护框架和安全管理体系。

参与角色： 信息系统运营、使用单位，安全服务商

活动输入： 信息系统详细描述文件、信息系统安全等级定级报告、安全需求分析报告、信息系统等级化抽象模型

活动描述：

a) 制定安全方针

形成机构最高层次的安全方针文件，阐明安全工作的使命和意愿，定义信息安全的总体目标，规定信息安全责任机构和职责，建立安全工作运行模式等；

b) 说明安全策略

形成机构高层次的安全策略文件，说明安全工作的主要策略，包括安全组织机构划分策略、业务系统分级策略、数据信息分级策略、安全域互连策略、信息流控制策略等；

活动输出： 总体安全策略文件

7.3.3. 各级系统安全技术措施设计

活动目标：

本活动的目标是根据等级保护基本要求、安全需求分析报告、机构总体安全策略文件等，针对信息系统的抽象模型，提出模型要素需要实现的安全技术措施，形成机构特定的系统安全技术保护框架，用以指导信息系统分等级保护的具体实现。

参与角色： 信息系统运营、使用单位，安全服务商

活动输入：安全需求分析报告、信息系统等级化抽象模型、等级保护基本要求

活动描述：

a) 选择和规定骨干网/城域网的安全保护技术措施

针对信息系统等级化抽象模型，根据机构总体安全策略文件、等级保护基本要求和安全需求，提出骨干网/城域网的安全保护策略和安全技术措施。骨干网/城域网的安全保护策略和安全技术措施提出时应考虑网络线路和网络设备共享的情况，如果不同级别的安全域通过骨干网/城域网的同一线路和设备传输数据，线路和设备的安全保护策略和安全技术措施应满足最高级别安全域的等级保护基本要求。

b) 选择和规定安全域之间互联的安全技术措施

针对信息系统等级化抽象模型，根据机构总体安全策略文件、等级保护基本要求和安全需求，提出跨局域网互联的安全域之间的信息传输保护策略要求和具体的安全技术措施，包括同级互联的策略、不同级别互联的策略等；提出局域网内部互联的安全域之间的信息传输保护策略要求和具体的安全技术措施，包括同级互联的策略、不同级别互联的策略等。

c) 选择和规定不同级别安全域的边界保护技术措施

针对信息系统等级化抽象模型，根据机构总体安全策略文件、等级保护基本要求和安全需求，提出不同级别安全域边界的安全保护策略和安全技术措施。安全域边界安全保护策略和安全技术措施提出时应考虑边界设备共享的情况，如果不同级别的安全域通过同一设备进行边界保护，这个边界设备的安全保护策略和安全技术措施应满足最高级别安全域的等级保护基本要求。

d) 选择和规定不同级别安全域内部系统平台和业务应用的安全保护技术措施

针对信息系统等级化抽象模型，根据机构总体安全策略文件、等级保护基本要求和安全需求，提出不同级别安全域内部网络平台、系统平台和业务应用的安全保护策略和安全技术措施。

e) 选择和规定不同级别信息系统机房的安全保护技术措施

针对信息系统等级化抽象模型，根据机构总体安全策略文件、等级保护基本要求和安全需求，提出不同级别信息系统机房的安全保护策略和安全技术措施。信息系统机房安全保护策略和安全技术措施提出时应考虑不同级别的信息系统共享机房的情况，如果不同级别的信息系统共享同一机房，机房的安全保护策略和安全技术措施应满足最高级别信息系统的等级保护基本要求。

f) 形成信息系统技术防护框架

将骨干网/城域网、通过骨干网/城域网的安全域互联、局域网内部的安全域互联、安全域的边界、安全域内部各类平台、机房以及其他方面的安全保护策略和安全技术措施进行整理、汇总，形成信息系统的安全技术防护框架。

活动输出： 信息系统安全技术防护框架

7.3.4. 系统整体安全管理策略设计

活动目标：

本活动的目标是根据等级保护基本要求、安全需求分析报告、机构总体安全策略文件等，调整原有管理模式和管理策略，既从全局高度考虑为每个等级信息系统制定统一的安全管理策略，又从每个信息系统的实际需求出发，选择和调整具体的安全管理措施，最后形成统一的系统整体安全管理体系。

参与角色： 信息系统运营、使用单位，安全服务商

活动输入： 信息系统抽象模型、等级保护基本要求、安全需求分析报告

活动描述：

a) 选择和规定信息安全的组织管理体系和对各信息系统的安全管理职责

根据机构总体安全策略文件、等级保护基本要求和安全需求，提出机构的安全组织管理机构框架，分配各个级别信息系统的安全管理职责、规定各个级别信息系统的安全管理制度框架等。

b) 选择和规定各等级信息系统的人员安全管理策略

根据机构总体安全策略文件、等级保护基本要求和安全需求，提出各个不同级别信息系统的管理人员框架，分配各个级别信息系统的管理人员职责、规定各个级别信息系统的人员安全管理策略等。

c) 选择和规定各等级信息系统机房及办公区等物理环境的安全管理策略

根据机构总体安全策略文件、等级保护基本要求和安全需求，提出各个不同级别信息系统的机房和办公环境的安全策略。

d) 选择和规定各等级信息系统介质、设备等的安全管理策略

根据机构总体安全策略文件、等级保护基本要求和安全需求，提出各个不同级别信息系统的介质、设备等的安全策略。

e) 选择和规定各等级信息系统运行安全管理策略

根据机构总体安全策略文件、等级保护基本要求和安全需求，提出各个不同级别信息系统的安全运维框架和运维安全策略等。

f) 选择和规定各等级信息系统安全事件处置和应急管理策略

根据机构总体安全策略文件、等级保护基本要求和安全需求，提出各个不同级别信息系统的安全事件处置和应急管理策略等。

g) 形成信息系统安全管理策略框架

将上述各个方面的安全管理策略进行整理、汇总，形成信息系统的整体安全管理策略框架。

活动输出：信息系统安全管理策略框架

7.3.5. 设计结果文档化

活动目标：

本活动的目标是将安全总体设计工作的结果文档化，最后形成一套指导机构信息安全工作的指导性文件。

参与角色： 信息系统运营、使用单位，安全服务商

活动输入： 安全需求分析报告、信息系统抽象模型、信息系统安全技术防护框架、信息系统安全管理策略框架

活动描述：

对安全需求分析报告、信息系统的分级保护模型以及为信息系统设计的技术防护策略和安全管理策略等文档进行整理，形成文件化的信息系统安全总体方案书。

信息系统安全总体方案书包括但不限于以下内容：

a) 信息系统概述；

b) 总体安全策略；

c) 信息系统等级化分析；

d) 信息系统分级保护模型；

e) 信息系统技术防护策略；

f) 信息系统安全管理与安全保障策略。

活动输出：信息系统安全总体方案书

7.4. 安全建设规划

7.4.1. 安全建设目标确定

活动目标：

本活动的目标是依据信息系统安全策略规划书或称信息系统安全总体方案书（一个或多个文件构成）、机构当前面临的机遇和挑战以及机构的安全建设资金状况确定各个时期的安全建设目标。

参与角色： 信息系统运营单位，安全服务商

活动输入：信息系统安全总体方案书、单位信息化建设的中长期发展规划

活动描述：

根据信息系统安全总体方案书，结合安全需求分析结果，根据现有系统与安全策略规划之间的差距，分析这些差距对信息系统的影响，同时考虑到信息系统运营使用单位自身信息化建设的中长期发展规划，提出分期分批的系统建设目标。

a) 信息化建设中长期发展规划和安全需求调查

了解和调查单位信息化建设的现况、中长期信息化建设的目标、主管部门对信息化的投入，对比信息化建设过程中阶段状态与安全策略规划之间的差距，分析急迫和关键的安全问题，考虑可以同步进行的安全建设内容等。

b) 提出信息系统安全建设分阶段目标

制定系统在规划期内（一般安全规划期为 3 年）所要实现的总体安全目标；制定系统短期（1 年以内）要实现的安全目标，主要解决目前急迫和关键的问题，争取在短期内安全状况有大幅度提高。

活动输出： 信息系统分阶段安全建设目标

7.4.2. 安全建设内容规划

活动目标：

本活动的目标是根据安全建设目标和信息系统安全总体方案书的要求，设计分期分批的主要建设内容，并将建设内容组合成不同的项目，阐明项目之间的依赖或促进关系等。

参与角色： 信息系统运营单位，安全服务商

活动输入：信息系统安全总体方案书、信息系统分阶段安全建设目标

活动描述：

a） 确定主要安全建设内容

根据信息系统安全总体方案书明确主要的安全建设内容，对主要安全建设内容进行适当的分解。主要建设内容可能分解但不限于以下内容：

1) 安全基础设施建设；
2) 网络安全建设；
3) 系统平台和应用平台安全建设；
4) 数据系统安全建设；
5) 安全标准体系建设；
6) 人才培养体系建设；
7) 安全管理体系建设。

b） 确定主要安全建设项目

组合安全建设内容为不同的安全建设项目，描述项目所解决的主要安全问题及所要达到的安全目标，对项目进行支持或依赖等相关性分析，对项目进行紧迫性分析，对项目进行实施难易程度分析，对项目进行预期效果分析，描述项目的具体工作内容、建设方案，形成安全项目列表。

活动输出： 安全建设内容

7.4.3. 安全建设方案设计

活动目标：

本活动的目标是根据建设目标和建设内容，在时间和经费上对安全建设项目列表进行总体考虑，分到不同的时期和阶段，设计建设顺序，进行投资估算，形成安全建设方案或安全建设计划，重点是形成近期或明年的可行的安全建设方案或安全建设计划。

参与角色： 信息系统运营单位，安全服务商

活动输入：信息系统安全总体方案书、信息系统分阶段安全建设目标、安全建设内容等

活动描述：

对信息系统的分期分批建设目标、安全建设总体方案和安全建设实施计划等文档进行整理，形成信息系统安全建设方案。

安全建设方案可包括但不限于以下内容：

1） 规划建设的依据和原则；
2） 规划建设的目标和范围；
3） 信息系统安全现状；
4） 信息化的中长期发展规划；
5） 信息系统安全建设的总体框架；
6） 安全技术体系建设规划；
7） 安全管理与安全保障体系建设规划；
8） 安全建设投资估算；
9） 信息系统安全建设的实施保障等内容。

活动输出： 信息系统安全建设方案

8 安全实施

8.1. 安全实施阶段的实施活动流程

安全实施的目标是按照信息系统安全总体方案书的总体要求，结合信息系统安全建设方案，分期分步落实安全措施。

为确保安全保护能够平滑地纳入到整个信息系统，必须在信息系统建设的各个阶段，同时考虑和进行安全的建设与实施。信息系统安全建设和信息系统建设过程存在相似性，我们只需对信息系统建设过程进行适当的调整就可以把信息系统安全建设与信息系统建设过程很好地结合起来，参见 5.5 节。

信息系统安全实施/实现阶段的主要活动内容包括依据安全建设规划的安全详细方案设计，根据安全详细设计方案的安全技术措施实施/实现、安全管理措施实施/实现以及安全实施实现后的等级保护安全测评。等级保护技术实施和等级保护管理实施是可以并行建设的，安全实施/实现阶段的流程如图 8-1 所示。

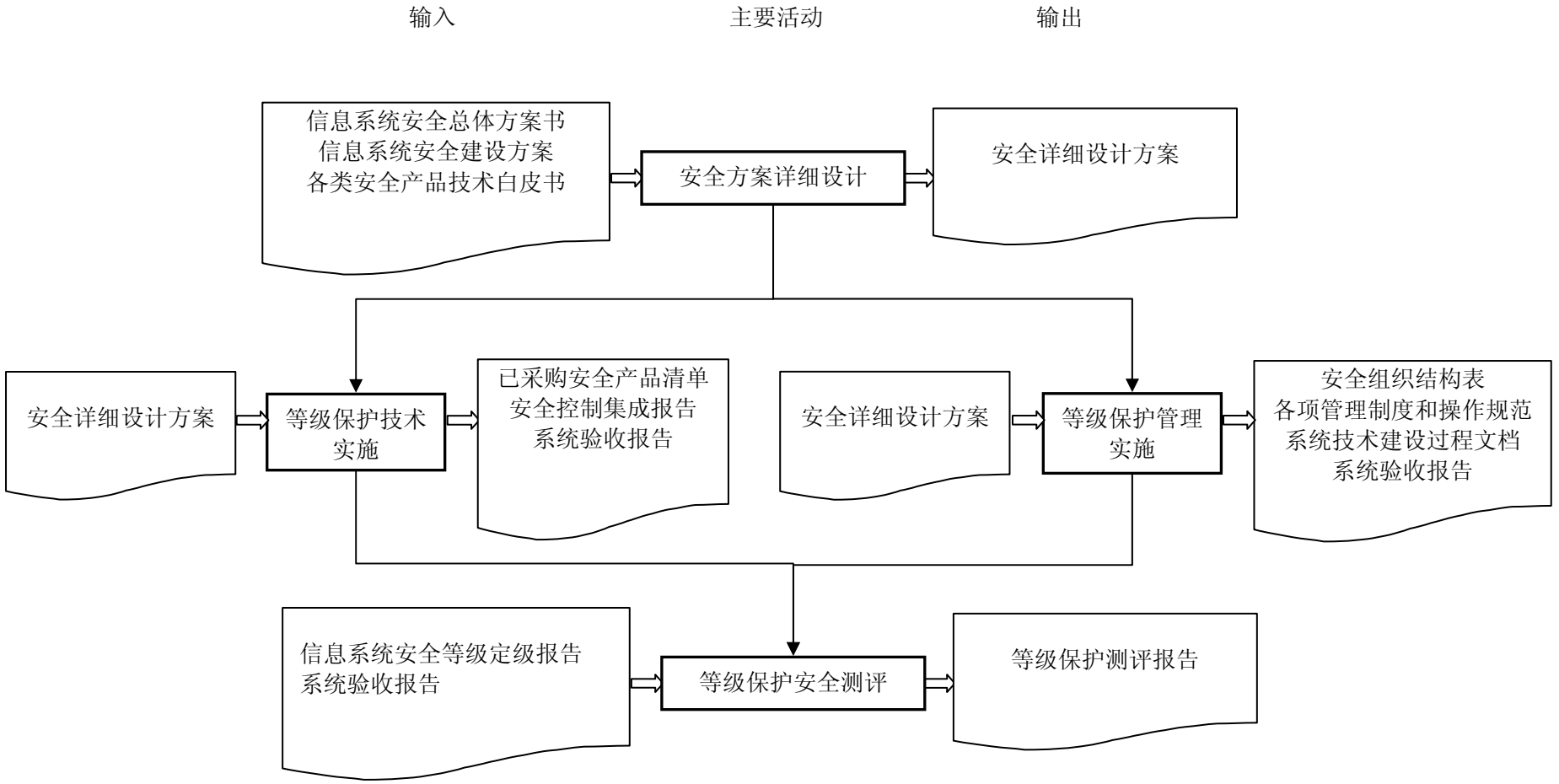
输入
主要活动
输出
信息系统安全总体方案书
信息系统安全建设方案
各类安全产品技术白皮书
安全方案详细设计
安全详细设计方案
安全详细设计方案
等级保护技术实施
已采购安全产品清单
安全控制集成报告
系统验收报告
安全详细设计方案
等级保护管理实施
安全组织结构表
各项管理制度和操作规范
系统技术建设过程文档
系统验收报告
信息系统安全等级定级报告
系统验收报告
等级保护安全测评
等级保护测评报告

图 8-1 安全实施流程图

信息系统安全实施阶段的主要活动内容如图 8-1 包括：

第一 安全方案详细设计

安全方案详细设计主要是依据信息系统安全建设方案，提出本期实施项目的具体实施方案，包括等级保护技术实施内容、等级保护管理实施内容、项目实施计划以及项目经费投入等，以便进行本次项目的实施。

安全方案详细设计的主要内容是等级保护技术实施内容的设计和等级保护管理实施内容的设计。

第二 等级保护管理实施

等级保护管理实施主要是建立与信息系统安全技术和安全运行相适应的安全管理机制。在本期安全详细设计方案的指导下，建立配套的安全管理机构和人员，建立配套的安全管理制度和操作规程，进行人员的安全技能培训等，保证本期安全实施完成后，安全运维有配套的机制。

等级保护管理实施过程中，主要的活动内容包括配套的安全管理机构和人员设置、配套的安全管理制度建立或修订、安全管理人员的技能培训以及安全实施过程的控制。

在系统定级阶段和安全规划设计阶段都需要建立与其相适应的安全管理机制，包括安全管理机构和人员的设置以及安全管理制度的建立等。但也应该保证等级保护管理实施过程和等级保护技术实施过程同步进行。等级保护管理实施的活动之间没有顺序的关系，因此本标准只对等级保护管理实施的主要活动进行了表述。

第三 等级保护技术实施

等级保护技术实施的目标是保证按照安全详细设计方案实现各项安全技术措施，并确保安全技术措施的有效性。

等级保护技术实施包括安全产品采购、安全控制开发、安全控制集成、测试与验收等主要活动环节。

第四 等级保护安全测评

等级保护安全测评是根据等级保护的管理规范和技术标准要求，针对已经实施了等级保护的信息系统，进行信息系统的安全保护措施是否符合相应等级的基本安全要求的评测。

等级保护安全测评活动可以在信息系统安全建设完成后进行，也可以在信息系统的运行维护过程中进行。等级保护安全测评活动可以针对一个信息系统多次进行，在测评过程中可以对已往测评结果进行复用，通过对已往测评结果进行分析与审核，判断已往结果是否适用或准确反映系统目前的安全状态，如果已往结果已经不适用于系统现在的安全状态，就需要重新进行测评。

8.2. 安全方案详细设计

8.2.1. 等级保护技术实施内容设计

活动目标：

本活动的目标是根据本期建设目标和建设内容将信息系统安全总体方案书中要求实现的安全策略、安全技术体系架构、安全措施和要求落实到产品功能或物理形态上，提出指定的产品或组件及其具体规范，并将产品功能特征整理成文档。使得在安全产品采购和安全控制开发阶段具有依据。

参与角色：信息系统运营、使用单位，信息系统安全服务提供商

活动输入：信息系统安全总体方案书、信息系统安全建设方案、各类安全产品技术白皮书

活动描述：

a) 结构框架设计

依据本次实施项目的建设内容和信息系统的实际情况，给出与规划设计阶段的安全框架一致的安全实现技术框架，内容可能包括安全防护的层次、安全产品的使用、网络安全域划分、IP 地址规划等等。

b) 功能要求设计

对安全实现技术框架中使用到的相关安全产品，如防火墙、VPN、网闸、认证网关、代理服务器、网络防病毒、PKI 等提出功能指标要求。对需要开发的安全控制组件，提出功能指标要求。

c) 性能要求设计

对安全实现技术框架中对使用到的相关安全产品，如防火墙、VPN、网闸、认证网关、代理服务器、网络防病毒、PKI 等提出性能指标要求。对需要开发的安全控制组件，提出性能指标要求。

d) 部署方案设计

结合目前信息系统网络拓扑，以图示的方式给出安全技术实现框架的实现方式，包括安全产品或安全组件的部署位置、连线方式、IP 地址分配等。对于需对原有网络进行调整的，给出网络调整的图示方案等。

e) 制定安全策略实现计划

依据信息系统安全总体方案书中提出的安全策略的要求，制定设计和设置安全产品或安全组件的安全策略实现计划。

活动输出：等级保护技术实施方案

8.2.2. 等级保护管理实施内容设计

活动目标：

本活动的目标是根据机构当前安全管理需要和安全技术保障需要提出与信息系统安全总体方案书中管理部分相适应的本期安全实施内容，以保证安全技术建设的同时，安全管理的同步建设。

参与角色：信息系统运营、使用单位，信息系统安全服务提供商

活动输入：信息系统安全总体方案书、信息系统安全建设方案

活动描述：

结合系统实际安全管理需要和本次技术建设内容，确定本次安全管理建设的范围和内容，同时注意与信息系统安全总体方案书的一致性。安全管理设计的内容主要考虑：安全管理机构和人员的配套、安全管理制度的配套、人员安全管理技能的配套等。

活动输出：等级保护管理实施方案

8.2.3. 设计结果文档化

活动目标：

本活动的目标是将等级保护技术实施内容、等级保护管理实施内容汇总，同时考虑工时和费用，最后形成指导安全实施的指导性文件。

参与角色：信息系统运营、使用单位，信息系统安全服务提供商

活动输入：等级保护技术实施方案、等级保护管理实施方案

活动描述：

对技术实施内容、管理实施内容等文档进行整理，形成信息系统安全建设详细设计方案。

安全详细设计方案包括但不限于以下内容：

a) 本期建设目标和建设内容；

b) 技术实现框架；

c) 安全产品或组件功能及性能；

d) 安全产品或组件部署；

e) 安全策略和配置；

f) 配套的安全管理建设内容；

g) 工程实施计划；

h) 项目投资估算。

活动输出：安全详细设计方案

8.3. 等级保护管理实施

8.3.1. 管理机构和人员的设置

活动目标：

本活动的目标是建立配套的安全管理职能部门，通过管理机构的岗位设置、人员的分工以及各种资源的配备，为信息系统的安全管理提供组织上的保障。

参与角色： 信息系统运营、使用单位，信息系统安全服务提供商

活动输入：机构现有相关管理制度和政策、安全详细设计方案

活动描述：

a) 安全组织

识别与信息安全管理有关的组织成员及其角色，例如：操作人员、文档管理员、系统管理员、安全管理员等，形成安全组织结构表。

b) 角色说明

以书面的形式详细描述每个角色与职责，确保有人对所有的风险负责。

活动输出：机构、角色与职责说明书

8.3.2. 管理制度的建设和修订

活动目标：

本活动的目标是建设或修订与信息系统安全管理相配套的、包括所有信息系统的建设、开发、运维、升级和改造等各个阶段和环节所应当遵循的行为规范和操作规程。

参与角色： 信息系统主管部门，信息系统运营、使用单位，安全服务提供商

活动输入：安全组织结构表、安全成员及角色说明书、安全详细设计方案

活动描述：

a) 应用范围

管理制度建立首先要明确制度的应用范围，如机房管理、帐户管理、远程访问管理、特殊权限管理、设备管理、变更管理等方面的内容。

b) 人员职责

管理制度的建立要明确相关岗位人员的责任和权利范围，并要征求相关人员的意见，要保证责任明确。

c) 行为规范

管理制度是通过制度化、规范化的流程和行为，来保证各项管理工作的一致性。

d) 评估与完善

制度在发布、执行过程中，要定期对其进行评估，根据实际环境和情况的变化，对制度进行修改和完善，必要时考虑管理制度的重新制定。

活动输出： 各项管理制度和操作规范

8.3.3. 人员安全技能培训

活动目标：

本活动的目标是对人员的职责、素质、技能等方面进行培训，保证人员具有与其岗位职责相适应的技术能力和管理能力，以减少人为因素给系统带来的安全风险。

参与角色： 信息系统主管部门，信息系统运营、使用单位，安全服务提供商

活动输入：系统/产品使用说明书、各项管理制度和操作规范

活动描述：

针对普通员工、管理员、开发人员、主管人员以及安全人员的特定技能培训和安全意识培训，培训后进行考核，合格者发给上岗资格证书等。

活动输出：培训记录及上岗资格证书等

8.3.4. 安全实施过程管理

活动目标：

本活动的目标是在系统定级、规划设计、实施过程中，对工程的质量、进度、文档和变更等方面的工作进行监督控制和科学管理。

参与角色：信息系统运营、使用单位，安全服务提供商，安全产品供应商

活动输入：安全技术建设各阶段相关文档

活动描述：

a) 质量管理

质量管理首先要控制系统建设的质量，保证系统建设始终处于等级保护制度所要求的框架内进行。同时，还要保证用于创建系统的过程的质量，在系统建设的过程中，要建立一个

不断测试和改进质量的过程，在整个系统的生命周期中，通过测量、分析和修正活动，保证所完成目标和过程的质量。

b) 风险管理

为了识别、评估和减低风险，以保证系统工程活动和全部技术工作项目都成功实施。在整个系统建设过程中，风险管理要贯穿始终。

c) 变更管理

在系统建设的过程中，由于各种条件的变化，会导致变更的出现，变更发生在工程的范围、进度、质量、费用、人力资源、沟通、合同等多方面。每一次的变更处理，必须遵循同样的程序，即相同的文字报告、相同的管理办法、相同的监控过程。必须确定每一次变更对系统成本、进度、风险和技术要求的影响。一旦批准变更，必须设定一个程序来执行变更。

d) 进度管理

系统建设的实施必须要有一组明确的可交付成果，同时也要求有结束的日期。因此在建设系统的过程中，必须制订项目进度计划，绘制网络图，将系统分解为不同的子任务，并进行时间控制确保项目的如期完成。

e) 文档管理

文档是记录项目整个过程的书面资料，在系统建设的过程中，针对每个环节都有大量的文档输出，文档管理涉及系统建设的各个环节，主要包括：系统定级、规划设计、方案设计、安全实施、系统验收、人员培训等方面。

活动输出：各阶段管理过程文档

8.4. 等级保护技术实施

8.4.1. 安全产品采购

活动目标：

本活动的目标是按照安全详细设计方案中对于产品的具体指标要求进行产品采购，根据产品或产品组合实现的功能满足安全设计要求的情况来选购所需的安全产品。

参与角色：安全产品提供商，信息系统运营、使用单位

活动输入：安全详细设计方案、相关产品信息

活动描述：

a) 制定产品采购说明书

安全产品选型过程首先依据安全设计方案的设计要求，制定产品采购说明书，对产品的采购原则、采购范围、指标要求、采购方式、采购流程等方面进行说明，然后依据产品采购说明书对现有产品进行比对和筛选。对于产品的功能和性能指标，可以依据国家认可的测试机构所出具的产品测试报告，也可以依据用户自行组织的安全产品功能和性能选型测试所出具的报告。

b) 产品选择

在依据产品采购说明书对现有产品进行选择时，不仅要考虑产品的使用环境、安全功能、成本（包括采购和维护成本）、易用性、可扩展性、与其他产品的互动和兼容性等因素，还

要考虑产品质量和可信性。产品可信性是保证系统安全的基础，用户在选择安全产品时应确保符合国家关于安全产品使用的有关规定。

国家对信息安全产品实行等级化管理，国家将颁布关于安全专用产品的分级标准，以满足不同等级系统对安全产品的需求。

对于一些信息产品比如操作系统和数据库，虽然不属于安全专用产品，但是，信息系统的一些重要安全控制机制是由他们完成和实现的，因此，国家发布了操作系统和数据库的等级划分标准，不同等级的产品体现了不同的安全保护能力和可信度。

对于密码产品的使用，应当按照国家商用密码管理局的相关规定进行选择和使用。

活动输出：已采购安全产品清单

8.4.2. 安全控制开发

活动目标：

本活动的目标是对于一些不能通过采购现有安全产品来实现的安全措施和安全功能，通过专门进行的设计、开发来实现。安全控制的开发应当与系统的应用开发同步设计、同步实施，而应用系统一旦开发完成后，再增加安全措施会造成很大的成本投入。因此，在应用系统开发的同时，要依据安全详细设计方案进行安全控制的开发设计，保证系统应用与安全同步建设。

参与角色：信息系统运营、使用单位，信息安全服务提供商

活动输入：安全详细设计方案

活动描述：

a) 安全措施需求分析

安全措施需求分析的主要内容是采用规范的形式准确表达安全方案设计中的安全措施的指标要求，确定软件设计的约束和软件同其他系统元素的接口细节。

b) 概要设计

概要设计要考虑安全方案中关于身份鉴别、访问控制、安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖等方面的指标要求，设计安全措施模块的体系结构，定义开发安全措施的模块组成，定义每个模块的主要功能和模块之间的接口。

c) 详细设计

依据概要设计说明书，将安全控制开发进一步细化，对每个安全功能模块的接口，函数要求，各接口之间的关系，各部分的内在实现机理都要进行详细的分析和细化设计。

按照功能的需求和模块划分进行各个部分的详细设计，包含接口设计和管理方式设计等。详细设计是设计人员根据概要设计书进行模块设计，将总体设计所获得的模块按照单元、程序、过程的顺序逐步细化，详细定义各个单元的数据结构、程序的实现算法以及程序、单元、模块之间的接口等，作为以后编码工作的依据。

d) 编码实现

按照设计进行硬件调试和软件的编码，在编码和开发过程中，要关注硬件组合的安全性和编码的安全性，并通过论证。编码须忠实于设计。项目组自己进行的单元测试过程是检验编码质量的首要环节，错误发现的越早，改正的代价就越小。因此提交测试组进行系统测试之前，项目组要进行单元测试。

e) 测试

开发基本完成要进行测试，保证功能的实现和安全性的实现。测试分为单元测试、集成测试、系统测试和以用户试用为主的用户测试四个阶段。只有通过最后得系统测试和用户测试的产品，才可以通过验收测试。

f) 安全控制开发过程文档化

安全控制开发过程需要将概要设计说明书、详细设计说明书、开发测试报告以及开发说明书等整理归档。

活动输出：安全控制开发过程相关文档

8.4.3. 安全控制集成

活动目标：

本活动的目标是将不同的软硬件产品集成起来，依据安全详细设计方案，将安全产品、系统软件平台和开发的安全控制模块与各种应用系统综合、整合成为一个系统。安全控制集成的过程需要把安全实施、风险控制、质量控制在实施和集成的过程中有机结合起来，遵循运营、使用单位与信息系统安全服务提供商共同参与相互配合的实施的原则。

参与角色：信息系统主管部门，信息系统运营、使用单位，信息系统安全服务商

活动输入：安全详细设计方案

活动描述：

a) 集成实施方案制定

本阶段主要工作内容是制定集成实施方案，集成实施方案的目标是具体指导工程的建设内容、方法和规范等，实施方案有别于安全设计方案的一个显著特征之处就是它的可操作性很强，要具体落实到产品的安装、部署和配置中，实施方案是工程建设的具体指导文件。

b) 集成准备阶段

实施准备阶段主要工作需要对实施环境进行准备，包括硬件设备准备、软件系统准备、环境准备。为了保证系统实施的质量，信息系统安全服务提供商应该依据系统设计方案，制定一套可行的系统质量控制方案，以便有效地指导系统实施过程。该质量控制方案应该确定系统实施各个阶段的质量控制目标、控制措施、工程质量问题的处理流程、系统实施人员的职责要求等，并提供详细的安全控制集成进度表。

c) 集成实施阶段

实施阶段主要工作内容是将配置好策略的安全产品和开发控制模块部署到实际的应用环境中，并调整相关策略。实施阶段应严格按照集成进度安排进行，出现问题各方应及时沟通。系统实施的各个阶段应该遵照质量控制方案的要求，分阶段地进行系统测试，逐步地实现质量控制目标。例如：综合布线系统施工过程中，应该及时利用网络测试仪测定线路质量，及早发现并解决质量问题。

d) 培训阶段

信息系统建设完成后，安全服务提供商应当向运营和使用单位提供信息系统使用说明书及建设过程文档，同时需要对系统维护人员进行必要培训，培训效果的好坏将直接影响到今后系统能否安全运行。

e) 形成安全控制集成报告

应将安全控制集成过程相关内容文档化，并形成安全控制集成报告，其包括但不局限于集成实施方案、质量控制方案、集成实施报告以及培训考核记录等内容。

活动输出： 安全控制集成报告

8.4.4. 测试与验收

活动目标：

本活动的目标是检验系统是否严格按照安全详细设计方案进行建设，是否实现了设计的功能和性能。在安全控制集成工作完成后，系统验收及测试是从总体出发，对整个系统进行集成性安全测试，包括对系统运行效率和可靠性的测试，也包括等级保护管理实施内容的验收。

参与角色：信息系统主管部门，信息系统运营、使用单位，信息系统安全服务商

活动输入：安全详细设计方案、安全控制集成报告

活动描述：

a) 验收准备

安全控制开发、集成完成后，要根据安全设计方案中需要达到的安全目标，标识验收测试对象，对每个测试对象设计测试方案，包括测试过程和预期结果。测试方案应当立足于合同条款、需求说明书和安全设计方案，充分体现用户的安全的需求。

成立验收测试工作组对验收方案进行审核，组织制定验收计划、定义验收的方法和严格程度。

b) 组织验收

这一阶段由验收测试工作组按照验收计划负责组织实施，组织测试人员根据已通过评审的验收测试方案对系统进行测试，该阶段要形成一些测试报告，验收测试工作组要对测试报告进行综合分析和评估。

c) 验收报告

在验收测试完成后要形成验收报告，验收报告需要用户与建设方进行确认。验收报告将明确给出验收的评审结论，结论分为“通过”和“不通过”两种。如果结论是“不通过”，安全服务提供商应当根据验收评审意见尽快修正有关问题，重新进行验收或者转入合同争议处理程序。

d) 系统交付

在验收测试通过以后，要进行系统的交付，需要安全服务提供商提交系统建设过程中的文档、指导用户进行系统运行维护的文档、服务承诺书等。

活动输出：系统验收报告

8.5. 等级保护安全测评

活动目标：

本活动的目标是通过安全测评机构对已经完成等级保护建设的信息系统进行测评，确保信息系统的安全保护措施符合相应等级的安全要求。

参与角色：信息系统主管部门，信息系统运营、使用单位，安全测评机构

活动输入：信息系统安全等级定级报告，系统验收报告

活动描述：

参见附录 B 中本活动的的主要参考标准。

活动输出：等级保护测评报告

9　安全运维

9.1.　实施的主要活动

安全运维是等级保护实施过程中确保信息系统正常运行的必要环节。安全运维涉及的内容较多，包括安全运行维护机构和安全运行维护机制的建立，环境、资产、设备、介质的管理，网络、系统的管理，密码、密钥的管理，运行、变更的管理，安全状态的监控和安全事件的处置，安全审计和安全检查等等。本标准并不对上述所有的管理活动进行描述，希望全面了解和控制安全运维中各类活动的读者可以参见其它标准或指南。

本标准关注安全运维阶段的运行管理和控制、变更管理和控制、安全状态监控、安全事件处置和应急预案、安全检查和持续改进以及监督检查等活动，重点描述各个活动的活动内容，使用者可根据自身系统的安全等级、复杂程度和实际需求等考虑对其它安全运维活动的添加或对描述的活动内容进行删减。

安全运维的活动之间没有顺序的关系，因此本标准只对安全运维的主要活动进行了表述，如图 9-1 所示。

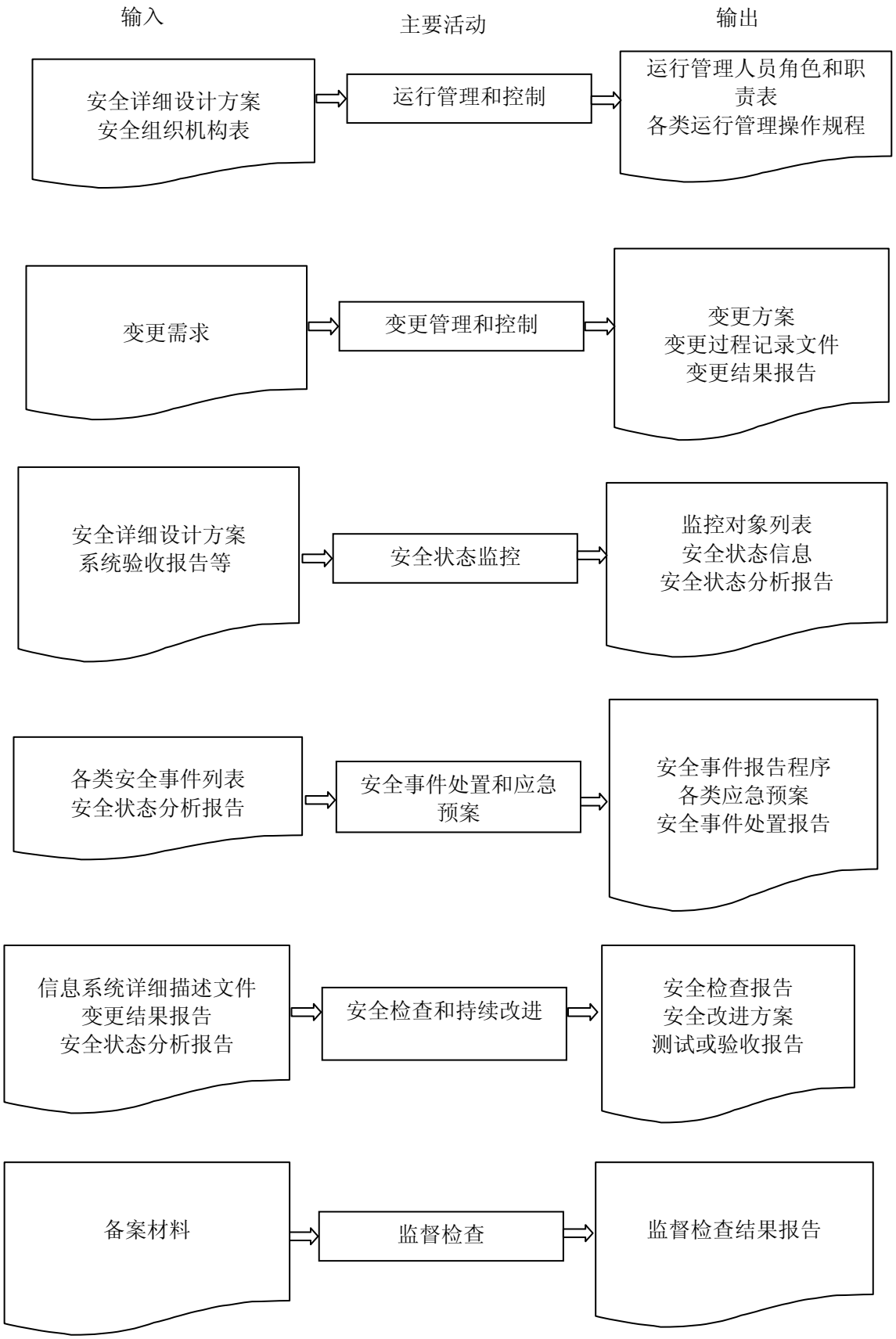

图 9-1 安全运维阶段的主要活动

信息系统安全运维阶段的主要活动内容如图 9-1 包括：

第一 运行管理和控制

运行管理和控制的目标是确保信息系统的安全运行，操作人员应对信息系统实行正确和安全的操作，并且保证系统不断变化和种类繁多的运行管理活动得到控制。应重视对运行活动的安全管理，安全等级越高的信息系统，需要控制的运行活动就越多。本标准中，安全运行管理和控制包括安全配置管理，关注的方面主要是操作人员的职责和操作过程的控制等，更详细的运行管理和控制内容参见其它相关标准。

第二 变更管理和控制

变更管理和控制的目标是确保在发生安全配置、安全设施、系统结构和业务应用等变化的时候，使用标准的方法和步骤，尽快的实施变更，并确保变更所导致的信息资产安全性降低、业务中断或业务影响减小到最低。关于变更管理和控制的更详细内容参见相关的标准，本标准在变更管理和控制方面更加关注使系统的安全等级发生变化的处理活动。

第三 安全状态监控

不同安全等级的信息系统在安全状态监控方面要求采用的手段和要求监控的内容会不同，具体要求可以参见相关的标准。本标准只对安全状态监控管理通常进行的活动内容进行描述，对活动的控制粒度要求也可以参见相关标准。

第四 安全事件处置和应急预案

安全事件采取分级响应与处置的机制，信息系统运营使用单位应根据安全事件相关标准中规定的安全事件分级原则和划分结果，结合自身具体的情况酌情划分本单位安全事件级别，并建立合适的应急响应机制，充分体现自主保护的原则，保障业务系统的持续运行。

第五 安全检查和持续改进

在信息系统安全运行维护过程中，会发生信息系统变更、安全状态改变等情况，因此必须定期对信息系统的状况进行安全检查。并依据检查的结果对信息系统进行持续改进。安全检查可以采用定期的监督检查、安全测评、自我检查等手段实现，风险评估可以作为安全检查的一种辅助手段。持续改进通过判断检查的结果对信息系统的安全措施进行局部补充或局部调整，或者重新确定信息系统的安全等级，进入信息系统安全等级保护的一个新的循环过程。

第六 等级保护安全测评

在运行维护过程中应按照等级保护的相关法规和标准定期对信息系统进行安全测评，使信息系统的安全状态能够达到相应等级的安全保护能力。

第七 等级保护监督检查

国家信息安全监督管理职能部门按照等级保护的管理规范和技术标准的要求，重点对第三、第四级信息和信息系统安全保护制度和措施的落实情况，以及安全现状的达标情况进行监督检查。安全监督管理职能部门对信息系统安全等级监督检查遵循“公平、公正、权威、有效”原则，采用例行检查和专项检查相结合的方法。

9.2. 运行管理和控制

9.2.1. 运行管理职责确定

活动目标：

本活动的目标是通过对运行管理活动或任务的角色划分，并授予相应的管理权限，来确定安全运行管理的具体人员和职责。

参与角色：信息系统运营、使用单位

活动输入：安全详细设计方案、安全组织机构表

活动描述：

a) 划分运行管理角色

根据管理制度和实际运行管理需求，划分运行管理需要的角色。越高安全等级的运行管理角色划分越细。

b) 授予管理权限

根据管理制度和实际运行管理需要，授予每一个运行管理角色不同的管理权限。安全等级越高的系统管理权限的划分也越细。

c) 定义人员职责

根据不同的安全等级要求的控制粒度，分析所需要运行管理控制内容，并以此定义不同运行管理角色的职责。

活动输出：运行管理人员角色和职责表

9.2.2. 运行管理过程控制

活动目标：

本活动的主要目标是通过制定运行管理操作规程，确定运行管理人员的操作目的、操作内容、操作时间和地点、操作方法和流程等，并进行操作过程记录，确保对操作过程进行控制。

参与角色：信息系统运营、使用单位

活动输入：运行管理需求、运行管理人员角色和职责表

活动描述：

a) 建立操作规程

将操作过程或流程规范化，并形成指导运行管理人员工作的操作规程，操作规程作为正式文件处理。安全等级越高的系统，对更多的操作要形成操作规程文件。

b) 操作过程记录

对运行管理人员按照操作规程执行的操作过程形成相关的记录文件，可能是日志文件，记录操作的时间和人员、正常或异常等信息。

活动输出：各类运行管理操作规程

9.3. 变更管理和控制

9.3.1. 变更需求和影响分析

活动目标：

本活动的主要目标是通过对变更需求和变更影响的分析，来确定变更的类别，计划后续的活动内容。

参与角色：信息系统运营、使用单位

活动输入：变更需求

活动描述：

a) 变更需求分析

对变更需求进行分析，确定变更的内容、变更资源需求和变更范围等，判断变更的必要性和可行性。

b) 变更影响分析

对变更可能引起的后果进行判断和分析，确定可能产生的影响大小，进行变更的先决条件和后续活动等。

c) 明确变更的类别

确定信息系统是局部调整还是重大变更。如果是由信息系统类型发生变化、承载的信息资产类型发生变化、信息系统服务范围发生变化和业务处理自动化程度发生变化等原因引起信息系统安全等级发生变化的重大变更，则需要重新确定信息系统安全等级，返回到等级保护实施过程的系统定级阶段。如果是局部调整，则确定需要配套进行的其它工作内容。

d) 制定变更方案

根据 a）、b）、c）的结果制定变更方案。

活动输出：变更方案

9.3.2. 变更过程控制

活动目标：

本活动的目标是确保变更实施过程受到控制，各项变化内容进行记录，保证变更对业务的影响最小。

参与角色：信息系统运营、使用单位

活动输入：变更方案

活动描述：

a) 变更内容审核和审批

对变更目的、内容、影响、时间和地点以及人员权限进行审核，以确保变更合理、科学的实施。按照机构建立的审批流程对变更方案进行审批。

b) 建立变更过程日志

按照批准的变更方案实施变更，对变更过程各类系统状态、各种操作活动等建立操作记录或日志。

c) 形成变更结果报告

收集变更过程的各类相关文档，整理、分析和总结各类数据，形成变更结果报告，并归档保存。

活动输出：变更结果报告

9.4. 安全状态监控

9.4.1. 监控对象确定

活动目标：

本活动的目标是确定可能会对信息系统安全造成影响的因素，即确定安全状态监控的对象。

参与角色：信息系统运营、使用单位

活动输入：安全详细设计方案、系统验收报告等

活动描述：

a) 安全关键点分析

对影响系统、业务安全性的关键要素进行分析，确定安全状态监控的对象，这些对象可能包括防火墙、入侵检测、防病毒、核心路由器、核心交换机、主要通信线路、关键服务器或客户端等系统范围内的对象；也可能包括安全标准和法律法规等外部对象。

b) 形成监控对象列表

根据确定的监控对象，分析监控的必要性和可行性、监控的开销和成本等因素，形成监控对象列表。

活动输出：监控对象列表

9.4.2. 监控对象状态信息收集

活动目标：

本活动的目标是选择状态监控工具，收集安全状态监控的信息，识别和记录入侵行为，对信息系统的安全状态进行监控。

参与角色：信息系统运营、使用单位

活动输入：监控对象列表

活动描述：

a) 选择监控工具

根据监控对象的特点、监控管理的具体要求、监控工具的功能、性能特点等，选择合适的监控工具。监控工具也可能不是自动化的工具，而只是由各类人员构成的，遵循一定规则进行操作的组织，或者是两者的综合。

b) 状态信息收集

收集来自监控对象的各类状态信息，可能包括网络流量、日志信息、安全报警和性能状况等；或者是来自外部环境的安全标准和法律法规的变更信息。

活动输出：安全状态信息

9.4.3. 监控状态分析和报告

活动目标：

本活动的目标通过是对安全状态信息进行分析，及时发现安全事件或安全变更需求，并对其影响程度和范围进行分析，形成安全状态结果分析报告。

参与角色：信息系统运营、使用单位

活动输入：安全状态信息

活动描述：

a) 状态分析

对安全状态信息进行分析，及时发现险情、隐患或安全事件，并记录这些安全事件，分析其发展趋势。

b) 影响分析

根据对安全状况变化的分析，分析这些变化对安全的影响，通过判断他们的影响决定是否有必要作出响应。

c) 形成安全状态分析报告

根据安全状态分析和影响分析的结果，形成安全状态分析报告，上报安全事件或提出变更需求。

活动输出：安全状态分析报告

9.5. 安全事件处置和应急预案

9.5.1. 安全事件分级

活动目标：

本活动的目标是按照安全事件相关标准，结合本信息系统的实际情况，通过预测、评估和分析事件对信息系统的破坏程度，所造成后果严重程度，将安全事件依次进行等级划分。

参与角色：信息系统运营、使用单位

活动输入：各类安全事件列表

活动描述：

a) 安全事件调查和分析

针对各类安全事件列表，根据安全事件相关标准，调查本系统内安全事件的类型、安全事件对业务的影响范围和程度以及安全事件的敏感程度等信息，分析对安全事件进行响应恢复所需要的时间。

b) 安全事件等级划分

根据以上调查和分析结果，参考安全事件相关标准，规定本系统内安全事件的级别，制定安全事件的报告程序。安全事件的报告程序可以包括安全事件的类型、等级、报告程序等。

活动输出：安全事件报告程序

9.5.2. 应急预案制定

活动目标：

本活动的目标是通过对安全事件的等级分析，在统一的应急预案框架下制定不同安全事件的应急预案。

参与角色：信息系统运营、使用单位

活动输入：安全事件报告程序

活动描述：

a) 确定应急预案对象

针对安全事件等级，考虑其可能性和对系统和业务产生的影响，确定需制定应急预案的安全事件对象。

b) 确定和认可各项职责

在统一的应急预案框架下，明确和认可应急预案中各部门的职责，并协调各部门间的合作和分工。

c) 制定应急预案程序及其执行条件

针对不同等级、不同优先级的安全事件制定相应的应急预案程序，说明应急预案启动的条件，发生安全事件后要采取的流程和措施等。

活动输出：各类应急预案

9.5.3. 安全事件处置

活动目标：

本活动的目标是对监控到的安全事件采取适当的方法进行处置，对安全事件的影响程度和等级进行分析，确定是否启动应急响应。

参与角色：信息系统运营、使用单位

活动输入：安全状态分析报告、安全事件报告程序、各类应急预案

活动描述：

a) 安全事件上报

根据安全状态分析报告分析可能的安全事件，如果明确为安全事件的，按照安全事件报告程序上报安全事件。

b) 安全事件处置

对接报的安全事件进行分析，明确安全事件等级、影响程度以及优先级等，确定是否应对安全事件启动应急预案。对于应该启动应急预案的安全事件按照应急预案响应机制进行安全事件处置。对未知安全事件的处置，应根据安全事件的等级，制定安全事件处置方案，包括安全事件处置方法以及应采取的措施等；并按照安全事件处置流程和方案对安全事件进行处置。

c) 安全事件总结和报告

一旦安全事件得到解决，对于未知的安全事件进行事件记录，分析记录信息并补充所需信息，使安全事件成为已知事件，并文档化；对安全事件处置过程进行总结，制定安全事件处置报告，并保存。

活动输出：安全事件处置报告

9.6. 安全检查和持续改进

9.6.1. 安全状态检查

活动目标：

本活动的主要目标是通过对信息系统的安全状态进行检查，为信息系统的持续改进过程提供依据和建议，确保信息系统的安全保护能力满足相应等级安全要求和自身特殊的安全需求。

关于监督检查参见 9.8 节，关于安全测评参见 9.7 节，本节描述自我检查过程。

参与角色：信息系统运营、使用单位

活动输入：信息系统详细描述文件、变更结果报告，安全状态分析报告

活动描述：

a) 确定检查对象和检查方法

确定检查的目标和意义，确定本次安全检查活动是自己组织的检查还是其他方组织的安全检查，如果是其他方组织的安全检查，则需要与其他方实施检查的单位进行沟通、洽谈和配合。

b) 制定检查计划和检查方案

确定检查工作的角色和职责，确定检查工作的方法，成立安全检查工作组。制定安全检查工作计划和安全检查方案，说明安全检查的范围、对象、工作方法等，准备安全检查需要的各类表单和工具。

c) 安全检查实施

根据安全检查计划，通过询问、检查和测试等多种手段，进行安全状况检查，记录各种检查活动的结果数据，分析安全措施的有效性、安全事件产生的可能性和信息系统的实际改进需求等。

d) 安全检查结果和报告

总结安全检查的结果，提出改进的的建议，并产生安全检查报告。将安全检查过程的各类文档、资料归档保存。

活动输出：安全检查报告

9.6.2. 改进方案制定

活动目标：

本活动的主要目标是依据安全检查的结果，调整信息系统的安全状态，保证信息系统安全防护的有效性。

参与角色：信息系统运营、使用单位

活动输入：安全检查报告

活动描述：

a) 安全改进的立项

根据安全检查结果确定安全改进的策略，如果涉及安全等级的变化，则应进入安全等级保护实施的一个新的循环过程；如果安全等级不变，但是调整内容较多、涉及范围较大，则应对安全改进项目进行立项，重新开始安全实施/实现过程，参见第 8 章；如果调整内容较小，则可以直接进行安全改进实施。

b) 制定安全改进方案

确定安全改进的工作方法、工作内容、人员分工、时间计划等，制定安全改进方案。安全改进方案只适用于小范围内的安全改进，如安全加固、配置加强、系统补丁等。

活动输出：安全改进方案

9.6.3. 安全改进实施

活动目标：

本活动的目标是保证按照安全改进方案实现各项补充安全措施，并确保原有的技术措施和管理措施与各项补充的安全措施一致有效地工作。

参与角色：信息系统运营、使用单位

活动输入：安全改进方案

活动描述：

a) 安全方案实施控制

参见 8.3.4 节。

b) 安全措施测试与验收

参见 8.4.4。

c) 配套技术文件和管理制度的修订

按照安全改进方案实施和落实各项补充的安全措施后，要调整和修订各类相关的技术文件和管理制度，保证原有体系完整性和一致性。

活动输出：测试或验收报告

9.7. 等级保护安全测评

活动目标：

本活动的目标是通过安全测评机构对已经完成等级保护建设，并投入运行的信息系统进行测评，确保信息系统的安全保护措施符合相应等级的安全要求。

参与角色：信息系统主管部门，信息系统运营、使用单位，安全测评机构

活动输入：信息系统安全等级定级报告，系统验收报告，测试或验收报告

活动描述：

具体活动过程参加 8.5 节。

活动输出：等级保护测评报告

9.8. 等级保护监督检查

活动目标：

本过程的目标是通过信息安全监管职能部门对信息系统定级、规划设计、建设实施和运行管理等过程进行监督检查，确保其符合信息系统安全保护相应等级的要求。

参与角色：信息安全监管职能部门

活动输入：备案材料

活动描述：

参见附录 B 中本活动的的主要参考标准。

活动输出：监督检查结果报告

10 系统终止

10.1. 实施的主要活动

系统终止阶段是等级保护实施过程中的最后环节。当信息系统被转移、终止或废弃时，正确处理系统内的敏感信息对于确保组织信息资产的安全是至关重要的。在信息系统生命周期中，有些系统并不是真正意义上的废弃，而是改进技术或转变业务到新的信息系统，对于这些信息系统在终止处理过程中应确保信息转移、设备迁移和介质销毁等方面的安全。

本标准在系统终止阶段关注信息转移、暂存和清除、设备迁移或废弃、存储介质的清除或销毁等活动，重点描述各个活动的活动内容，使用者可根据自身系统的安全等级、复杂程度和实际需求等考虑对系统终止阶段具体活动的添加或对描述活动内容的删减。

系统终止阶段的各个活动之间没有顺序的关系，因此本标准只对系统终止阶段的主要活动进行了表述，如图 10-1 所示。

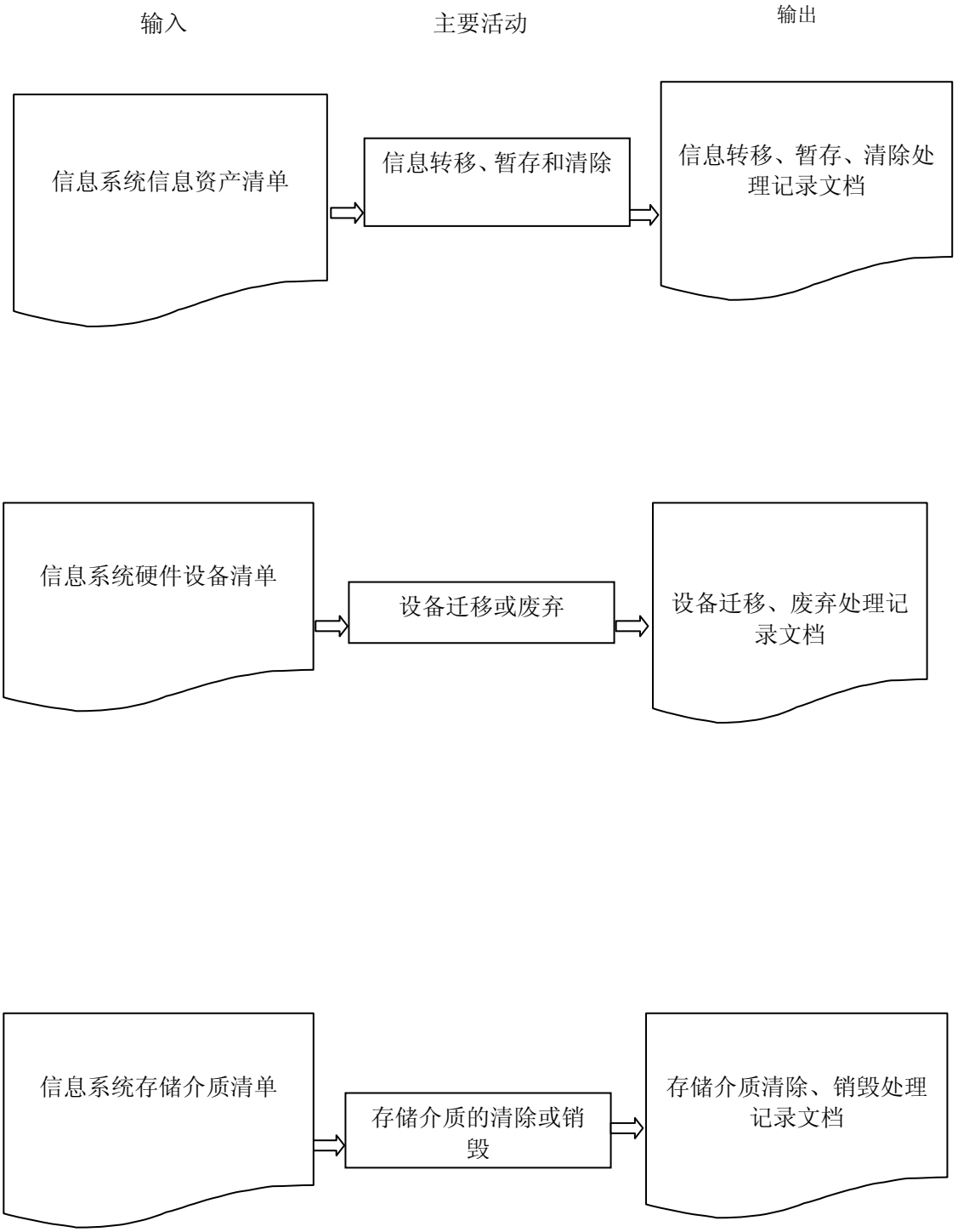

图 10-1 系统终止阶段的主要活动

10.2. 信息转移、暂存和清除

活动目标：

本活动的目标是在信息系统终止处理过程中，对于可能会在另外的信息系统中使用的信息采取适当的方法将其安全地转移或暂存到可以恢复的介质中，确保将来可以继续使用，同时采用安全的方法清除要终止的信息系统中的信息。

参与角色：信息系统主管部门，信息系统运营、使用单位

活动输入：信息系统信息资产清单

活动描述：

a) 识别要转移、暂存和清除的信息资产

根据要终止的信息系统的信息资产清单，识别重要信息资产、所处的位置以及当前状态等，列出需转移、暂存和清除的信息资产的清单。

b) 信息资产转移、暂存和清除

根据信息资产的重要程度制定信息资产的转移、暂存、清除的方法和过程，如果是涉密信息，应该按照国家相关部门的规定进行转移、暂存和清除。

c) 处理过程记录

记录信息转移、暂存和清除的过程，包括参与的人员、转移、暂存和清除的方式以及目前信息所处的位置等。

活动输出：信息转移、暂存、清除处理记录文档

10.3. 设备迁移或废弃

活动目标：

本活动的目标是确保信息系统终止后，迁移或废弃的设备内不包括敏感信息，对设备的处理方式应符合国家相关部门的要求。

参与角色：信息系统主管部门，信息系统运营、使用单位

活动输入：设备迁移或废弃清单等

活动描述：

c) 软硬件设备识别

根据要终止的信息系统的设备清单，识别要被迁移或废弃的硬件设备、所处的位置以及当前状态等，列出需迁移、废弃的设备的清单。

d) 制定硬件设备处理方案

根据规定和实际情况制定设备处理方案，包括重用设备、废弃设备、敏感信息的清除方法等。

e) 处理方案审批

包括重用设备、废弃设备、敏感信息的清除方法等的设备处理方案应该经过主管领导审查和批准。

f) 设备处理和记录

根据设备处理方案对设备进行处理，如果是涉密信息的设备，其处理过程应符合国家相关部门的规定；记录设备处理过程，包括参与的人员、处理的方式、是否有残余信息的检查结果等。

活动输出：设备迁移、废弃处理报告

10.4. 存储介质的清除或销毁

活动目标：

本活动的目标是通过采用合理的方式对计算机介质（包括磁带、磁盘、打印结果和文档）进行信息清除或销毁处理，防止介质内的敏感信息泄露。

参与角色：信息系统主管部门，信息系统运营、使用单位

活动输入：存储介质清单等

活动描述：

a) 识别要清除或销毁的介质

根据要终止的信息系统的存储介质清单，识别载有重要信息的存储介质、所处的位置以及当前状态等，列出需清除或销毁的存储介质清单。

b) 确定存储介质处理方法和流程

根据存储介质所承载信息的敏感程度确定对存储介质的处理方式和处理流程。存储介质的处理包括数据清除和存储介质销毁等。对于存储涉密信息的介质应按照国家相关部门的规定进行处理。

c) 处理方案审批

包括存储介质的处理方式和处理流程等的处理方案应该经过主管领导审查和批准。

d) 存储介质处理和记录

根据存储介质处理方案对存储介质进行处理，记录处理过程，包括参与的人员、处理的方式、是否有残余信息的检查结果等。

活动输出：存储介质的清除或销毁记录文档

附录 A

（规范性附录）

主要活动及其活动输出

主要阶段	主要活动	子活动	活动输入	活动输出
系统定级	系统识别和描述		信息系统的立项、建设、管理文档	信息系统总体描述文件
	信息系统划分		信息系统总体描述文件	* 信息系统详细描述文件
	安全等级确定		信息系统总体描述文件 信息系统详细描述文件	* 信息系统安全等级定级报告
安全规划设计	安全需求分析	评估对象和评估方法的明确	信息系统详细描述文件 信息系统安全等级定级报告 用户提供的其它文档	评估工作方案
		评估指标选择和组合	信息系统详细描述文件 信息系统安全等级定级报告 评估工作方案 等级保护基本要求	安全评估方案
		现状与评估指标对比	信息系统详细描述文件 信息系统安全等级定级报告 评估工作方案 安全评估方案	各类评估结果记录表

主要阶段	主要活动	子活动	活动输入	活动输出
		额外/特殊安全需求的确定	信息系统详细描述文件 信息系统安全等级定级报告 评估工作方案 安全评估方案	重要资产的特殊保护要求
		形成安全需求分析报告	信息系统详细描述文件 信息系统安全等级定级报告 评估工作方案 安全评估方案 各类评估结果记录表 重要资产的特殊保护要求	* 安全需求分析报告
	安全总体设计	系统等级化模型处理	信息系统详细描述文件 信息系统安全等级定级报告	信息系统等级化抽象模型
		总体安全策略设计	信息系统详细描述文件 信息系统安全等级定级报告 安全需求分析报告 信息系统等级化抽象模型	总体安全策略文件
		各级系统安全技术措施设计	安全需求分析报告 信息系统等级化抽象模型 等级保护基本要求	信息系统安全技术防护框架

主要阶段	主要活动	子活动	活动输入	活动输出
		系统整体安全管理策略设计	信息系统抽象模型 等级保护基本要求 安全需求分析报告	信息系统安全管理策略框架
		设计结果文档化	安全需求分析报告 信息系统抽象模型 信息系统安全技术防护框架 信息系统安全管理策略框架	* 信息系统安全总体方案书
	安全建设规划	安全建设目标确定	信息系统安全总体方案书 单位信息化建设的中长期发展规划	信息系统分阶段安全建设目标
		安全建设内容规划	信息系统安全总体方案书 信息系统分阶段安全建设目标	安全建设内容
		安全建设方案设计	信息系统安全总体方案书 信息系统分阶段安全建设目标 安全建设内容	* 信息系统安全建设方案
安全实施/实现	安全方案详细设计	等级保护技术实施内容设计	信息系统安全总体方案书 信息系统安全建设方案 各类安全产品技术白皮书	等级保护技术实施方案
		等级保护管理实施内容设计	信息系统安全总体方案书 信息系统安全建设方案	等级保护管理实施方案

主要阶段	主要活动	子活动	活动输入	活动输出
		设计结果文档化	等级保护技术实施方案 等级保护管理实施方案	* 安全详细设计方案
	等级保护管理实施	管理机构和人员的设置	机构现有相关管理制度和政策 安全详细设计方案	* 角色与职责说明书
		管理制度的建设和修订	安全组织结构表 角色与职责说明书 安全详细设计方案	* 各项管理制度和操作规范
		人员安全技能培训	系统/产品使用说明书 各项管理制度和操作规范	培训记录及上岗资格证等
		安全实施过程管理	安全技术建设各阶段相关文档	各阶段管理过程文档
	等级保护技术实施	安全产品采购	安全详细设计方案、相关产品信息	已采购安全产品清单
		安全控制开发	安全详细设计方案	安全控制开发过程相关文档
		安全控制集成	安全详细设计方案	安全控制集成报告
		测试与验收	安全详细设计方案 安全控制集成报告	* 系统验收报告
	等级保护安全测评		信息系统安全等级定级报告 系统验收报告	* 等级保护测评报告
安全运维管理	运行管理和控制	运维管理职责确定	安全详细设计方案 安全组织机构表	* 运行管理人员角色和职责表

主要阶段	主要活动	子活动	活动输入	活动输出
		运维管理过程控制	运行管理需求 运行管理人员角色和职责表	* 各类运行管理操作规程
	变更管理和控制	变更需求和影响分析	变更需求	变更方案
		变更过程控制	变更方案	* 变更结果报告
	安全状态监控	监控对象确定	安全详细设计方案 系统验收报告等	监控对象列表
		监控对象状态信息收集	监控对象列表	安全状态信息
		监控状态分析和报告	安全状态信息	* 安全状态分析报告
	安全事件处置和应急预案	安全事件分级	各类安全事件列表	* 安全事件报告程序
		应急预案制定	安全事件报告程序	* 各类应急预案
		安全事件处置	安全状态分析报告 安全事件报告程序 各类应急预案	* 安全事件处置报告
	安全检查和持续改进	安全状态检查	信息系统详细描述文件 变更结果报告 安全状态分析报告	* 安全检查报告
		改进方案制定	安全检查报告	* 安全改进方案
		安全改进实施	安全改进方案	* 测试或验收报告

主要阶段	主要活动	子活动	活动输入	活动输出
	等级保护安全测评		信息系统安全等级定级报告 系统验收报告 测试或验收报告	* 等级保护测评报告
	监督检查		备案材料	* 监督检查结果报告
系统终止	信息转移、暂存和清除		信息系统信息资产清单	信息转移、暂存、清除处理记录文档
	设备迁移或废弃		信息系统硬件设备清单	设备迁移、废弃处理记录文档
	存储介质的清除或销毁		信息系统存储介质清单	存储介质清除、销毁处理记录文档

注： * 标注的输出文件为比较重要的文件。

附录 B

（资料性附录）

主要活动及其主要参考标准

主要阶段	主要活动	子活动	主要参考标准
系统定级	系统识别和描述		GB/T XXXA-XXXX 等。
	信息系统划分		GB/T XXXA-XXXX 等。
	安全等级确定		GB17859-1999、GB/T XXXA-XXXX、FIPS 199 等。
安全规划设计	安全需求分析	评估对象和评估方法的明确	GB/T XXXB-XXXX、GB/T XXXD-XXXX、GB/T XXXJ-XXXX 等。
		评估指标选择和组合	GB17859-1999、GB/T XXXB-XXXX、GB/T XXXD-XXXX、GB/T XXXE-XXXX、GB/T XXXF-XXXX、GB/T 20008-2005、GB/T 20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/T XXXI-XXXX、GB/T 19715.2-2005、GB/T 19716-2005、GB/T XXXJ-XXXX 等。
		现状与评估指标对比	GB17859-1999、GB/T XXXB-XXXX、GB/T XXXD-XXXX、GB/T XXXE-XXXX、GB/T XXXF-XXXX、GB/T 20008-2005、GB/T 20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/T XXXI-XXXX、GB/T 19715.2-2005、GB/T XXXJ-XXXX、GB/T 19716-2005 等。
		额外/特殊安全需求的确定	GB17859-1999、GB/T XXXB-XXXX、GB/T XXXD-XXXX、GB/T XXXE-XXXX、GB/T XXXF-XXXX、GB/T 20008-2005、GB/T 20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/T XXXI-XXXX、GB/T XXXJ-XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
		形成安全需求分析报告	GB17859-1999、GB/T XXXB-XXXX、GB/T XXXD-XXXX、GB/T XXXE-XXXX、GB/T XXXF-XXXX、GB/T 20008-2005、GB/T 20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/T XXXI-XXXX、GB/T XXXC-XXXX、GB/T XXXJ-XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。

主要阶段	主要活动	子活动	主要参考标准
	安全总体设计	系统等级化模型处理	GB17859-1999、GB/T XXXB-XXXX、GB/T XXXE-XXXX、GB/T XXXF-XXXX、GB/T 20008-2005、GB/T 20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/T XXXI-XXXX、GB/T XXXC-XXXX、GB/T XXXJ-XXXX、IATF3.0、GB/T 19715.2-2005、GB/T 19716-2005 等。
		总体安全策略设计	GB17859-1999、GB/T XXXB-XXXX、GB/T XXXE-XXXX、GB/T XXXF-XXXX、GB/T 20008-2005、GB/T 20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/T XXXI-XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
		各级系统安全技术措施设计	GB17859-1999、GB/T XXXB-XXXX、GB/T XXXE-XXXX、GB/T XXXF-XXXX、GB/T 20008-2005、GB/T 20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/T XXXI-XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
		系统整体安全管理策略设计	GB17859-1999、GB/T XXXB-XXXX、GB/T XXXE-XXXX、GB/T XXXF-XXXX、GB/T 20008-2005、GB/T 20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/T XXXI-XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
		设计结果文档化	GB17859-1999、GB/T XXXB-XXXX、GB/T XXXE-XXXX、GB/T XXXF-XXXX、GB/T 20008-2005、GB/T 20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/T XXXI-XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
	安全建设规划	安全建设目标确定	GB17859-1999、GB/T XXXB-XXXX、GB/T XXXE-XXXX、GB/T XXXF-XXXX、GB/T 20008-2005、GB/T 20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/T XXXI-XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
		安全建设内容规划	GB17859-1999、GB/T XXXB-XXXX、GB/T XXXE-XXXX、GB/T XXXF-XXXX、GB/T 20008-2005、GB/T 20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/T XXXI-XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。

主要阶段	主要活动	子活动	主要参考标准
		安全建设方案设计	GB17859-1999、GB/T XXXB-XXXX、GB/T XXXE-XXXX、GB/T XXXF-XXXX、GB/T 20008-2005、GB/T 20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/T XXXI-XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
安全实施	安全方案详细设计	等级保护技术实施内容设计	GB17859-1999、GB/T XXXB-XXXX、GB/T XXXE-XXXX、GB/T XXXF-XXXX、GB/T 20008-2005、GB/T 20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/T XXXI-XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
		等级保护管理实施内容设计	GB17859-1999、GB/T XXXB-XXXX、GB/T XXXE-XXXX、GB/T XXXF-XXXX、GB/T 20008-2005、GB/T 20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/T XXXI-XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
		设计结果文档化	GB17859-1999、GB/T XXXB-XXXX、GB/T XXXE-XXXX、GB/T XXXF-XXXX、GB/T 20008-2005、GB/T 20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/T XXXI-XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
	等级保护管理实施	管理机构和人员的设置	GB17859-1999、GB/T XXXB-XXXX、GB/T XXXE-XXXX、GB/T XXXF-XXXX、GB/T 20008-2005、GB/T 20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/T XXXI-XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
		管理制度的建设和修订	GB17859-1999、GB/T XXXB-XXXX、GB/T XXXE-XXXX、GB/T XXXF-XXXX、GB/T 20008-2005、GB/T 20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/T XXXI-XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
		人员安全技能培训	GB17859-1999、GB/T XXXB-XXXX、GB/T XXXE-XXXX、GB/T XXXF-XXXX、GB/T 20008-2005、GB/T 20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/T XXXI-XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。

主要阶段	主要活动	子活动	主要参考标准
		安全实施过程管理	GB17859-1999、GB/T XXXB-XXXX、GB/T XXXE-XXXX、GB/T XXXF-XXXX、GB/T 20008-2005、GB/T 20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/T XXXI-XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
	等级保护技术实施	安全产品采购	GB/T XXXB-XXXX、GB/T XXXE-XXXX、GB/T XXXF-XXXX、GB/T 20008-2005、GB/T 20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/T XXXI-XXXX 等。
		安全控制开发	GB17859-1999、GB/T XXXB -XXXX、GB/T XXXE -XXXX、GB/T XXXE -XXXX、GB/T20008-2005、GB/T 20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/T XXXI -XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
		安全控制集成	GB17859-1999、GB/T XXXB -XXXX、GB/T XXXE -XXXX、GB/T XXXE -XXXX、GB/T20008-2005、GB/T20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/TXXXI -XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
		测试与验收	GB17859-1999、GB/T XXXB -XXXX、GB/T XXXE -XXXX、GB/T XXXE -XXXX、GB/T20008-2005、GB/T20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/TXXXI -XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
	等级保护安全测评		GB/T XXXC－XXXX、GB/T XXXD－XXXX 等。
安全运维	运行管理和控制	运维管理职责确定	GB17859-1999、GB/T XXXB -XXXX、GB/T XXXE -XXXX、GB/T XXXE -XXXX、GB/T20008-2005、GB/T20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/TXXXI -XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
		运维管理过程控制	GB17859-1999、GB/T XXXB -XXXX、GB/T XXXE -XXXX、GB/T XXXE -XXXX、GB/T20008-2005、GB/T20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/TXXXI -XXXX、GB/T

主要阶段	主要活动	子活动	主要参考标准
			19715.2-2005、GB/T 19716-2005 等。
	变更管理和控制	变更需求和影响分析	GB17859-1999、GB/T XXXB -XXXX、GB/T XXXE -XXXX、GB/T XXXE -XXXX、GB/T20008-2005、GB/T20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/TXXXI -XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
		变更过程控制	GB17859-1999、GB/T XXXB -XXXX、GB/T XXXE -XXXX、GB/T XXXE -XXXX、GB/T20008-2005、GB/T20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/TXXXI -XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
	安全状态监控	监控对象确定	GB17859-1999、GB/T XXXB -XXXX、GB/T XXXE -XXXX、GB/T XXXE -XXXX、GB/T20008-2005、GB/T20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/TXXXI -XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
		监控对象状态信息收集	GB17859-1999、GB/T XXXB -XXXX、GB/T XXXE -XXXX、GB/T XXXE -XXXX、GB/T20008-2005、GB/T20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/TXXXI -XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
		监控状态分析和报告	GB17859-1999、GB/T XXXB -XXXX、GB/T XXXE -XXXX、GB/T XXXE -XXXX、GB/T20008-2005、GB/T20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/TXXXI -XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
	安全事件处置和应急预案	安全事件分级	GB17859-1999、GB/T XXXB -XXXX、GB/T XXXE -XXXX、GB/T XXXE -XXXX、GB/T20008-2005、GB/T20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/TXXXI -XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
		应急预案制定	GB17859-1999、GB/T XXXB -XXXX、GB/T XXXE -XXXX、GB/T XXXE -XXXX、GB/T20008-2005、

主要阶段	主要活动	子活动	主要参考标准
			GB/T20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/TXXXI -XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
		安全事件处置	GB17859-1999、GB/T XXXB -XXXX、GB/T XXXE -XXXX、GB/T XXXE -XXXX、GB/T20008-2005、GB/T20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/TXXXI -XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
	安全检查和持续改进	安全状态检查	GB17859-1999、GB/T XXXB -XXXX、GB/T XXXE -XXXX、GB/T XXXE -XXXX、GB/T20008-2005、GB/T20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/TXXXI -XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
		改进方案制定	GB17859-1999、GB/T XXXB -XXXX、GB/T XXXE -XXXX、GB/T XXXE -XXXX、GB/T20008-2005、GB/T20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/TXXXI -XXXX、GB/T 19715.2-2005、GB/T 19716-2005、GB/T XXXJ -XXXX 等。
		安全改进实施	GB17859-1999、GB/T XXXB -XXXX、GB/T XXXE -XXXX、GB/T XXXE -XXXX、GB/T20008-2005、GB/T20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/TXXXI -XXXX、GB/T 19715.2-2005、GB/T 19716-2005、GB/T XXXJ -XXXX 等。
	等级保护安全测评		GB/T XXXC －XXXX、GB/T XXXD－XXXX 等。
	监督检查		GB/T XXXL －XXXX 等。
系统终止	信息转移、暂存和清除		GB17859-1999、GB/T XXXB -XXXX、GB/T XXXE -XXXX、GB/T XXXE -XXXX、GB/T20008-2005、GB/T20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/TXXXI -XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。
	设备迁移或废弃		

GB17859-1999、GB/T XXXB -XXXX、GB/T XXXE -XXXX、GB/T XXXE -XXXX、GB/T20008-2005、GB/T20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/TXXXI -XXXX、GB/T 19715.2-2005、

主要阶段	主要活动	子活动	主要参考标准
			GB/T 19716-2005 等。
	存储介质的清除或销毁		GB17859-1999、GB/T XXXB -XXXX、GB/T XXXE -XXXX、GB/T XXXE -XXXX、GB/T20008-2005、GB/T20009-2005、GB/T 20010-2005、GB/T 20011-2005、GB/TXXXI -XXXX、GB/T 19715.2-2005、GB/T 19716-2005 等。

参考文献

1 GB/T 5271.8-2001 信息技术 词汇 第8部分：安全

2 GB17859-1999 计算机信息系统安全保护等级划分准则

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 XXXA -XXXX 信息系统安全保护等级定级指南（征求意见稿）

6 GB/T XXXB -XXXX 信息系统安全等级保护基本要求（征求意见稿）

7 GB/T XXXC -XXXX 信息系统安全等级保护测评准则（征求意见稿）

8 GB/T XXXD -XXXX 信息系统安全等级保护评估指南（征求意见稿）

9 GB/T XXXE -XXXX 信息安全技术 信息系统安全通用技术要求（报批稿）

10 GB/T XXXF -XXXX 信息安全技术 信息系统安全管理要求（报批稿）

11 GB/T 20008-2005 信息安全技术 操作系统安全评估准则

12 GB/T 20009-2005 信息安全技术 数据库管理系统安全评估准则

13 GB/T 20010-2005 信息安全技术 过滤包防火墙安全评估准则

14 GB/T 20011-2005 信息安全技术 路由器安全评估准则

15 GB/T XXXI -XXXX 信息安全技术 物理安全技术要求（征求意见稿）

16 GB/T XXXJ -XXXX 信息安全技术 信息安全风险评估指南（征求意见稿）

17 GB/T XXXK -XXXX 网络脆弱性扫描产品技术要求（送审稿）

18 GB/T XXXL －XXXX 信息系统安全等级保护监督检查管理办法（征求意见稿）

19 GA/T 390-2002 计算机信息系统安全等级保护通用技术要求

20 GA/T 391-2002 计算机信息系统安全等级保护安全管理要求

21 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

22 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

23 GA /T 387-2002 计算机信息系统安全等级保护网络技术要求

24 GA /T 370-2001 端设备隔离部件安全技术要求

25 FIPS 199 -2003 联邦信息和信息系统安全分类标准

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

27 IATF 信息保障技术框架3.0版，美国国家安全局发布