ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25058—2010

信息安全技术
信息系统安全等级保护实施指南

Information security technology—
Implementation guide for classified protection of information system

2010-09-02 发布　　2011-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准的附录 A 是规范性附录。

本标准由公安部和全国信息安全标准化技术委员会提出。

本标准由全国信息安全标准化技术委员会归口。

本标准起草单位：公安部信息安全等级保护评估中心。

本标准主要起草人：毕马宁、马力、陈雪秀、李明、朱建平、任卫红、谢朝海、曲洁、袁静、李升、刘静、罗峥。

引　言

依据《中华人民共和国计算机信息系统安全保护条例》(国务院147号令)、《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)、《关于信息安全等级保护工作的实施意见》(公通字[2004]66号)和《信息安全等级保护管理办法》(公通字[2007]43号),制定本标准。

本标准是信息安全等级保护相关系列标准之一。

与本标准相关的系列标准包括:

——GB/T 22240—2008　信息安全技术　信息系统安全等级保护定级指南;

——GB/T 22239—2008　信息安全技术　信息系统安全等级保护基本要求。

在对信息系统实施信息安全等级保护的过程中,除使用本标准外,在不同的阶段,还应参照其他有关信息安全等级保护的标准开展工作。

在信息系统定级阶段,应按照GB/T 22240—2008介绍的方法,确定信息系统安全保护等级。

在信息系统总体安全规划,安全设计与实施,安全运行与维护和信息系统终止等阶段,应按照GB 17859—1999、GB/T 22239—2008、GB/T 20269—2006、GB/T 20270—2006和GB/T 20271—2006等技术标准,设计、建设符合信息安全等级保护要求的信息系统,开展信息系统的运行维护管理工作。

GB 17859—1999、GB/T 22239—2008、GB/T 20269—2006、GB/T 20270—2006和GB/T 20271—2006等技术标准是信息系统安全等级保护的系列相关配套标准,其中GB 17859—1999是基础性标准,GB/T 20269—2006、GB/T 20270—2006和GB/T 20271—2006等是对GB 17859—1999的进一步细化和扩展,GB/T 22239—2008是以GB 17859—1999为基础,根据现有技术发展水平提出的对不同安全保护等级信息系统的最基本安全要求,是其他标准的一个底线子集。

对信息系统的安全等级保护应从GB/T 22239—2008出发,在保证信息系统满足基本安全要求的基础上,逐步提高对信息系统的保护水平,最终满足GB 17859—1999、GB/T 20269—2006、GB/T 20270—2006和GB/T 20271—2006等标准的要求。

除本标准和上述提到的标准外,在信息系统安全等级保护实施过程中,还可参照和使用GB/T 20272—2006和GB/T 20273—2006等其他等级保护相关技术标准。

信息安全技术
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过程，适用于指导信息系统安全等级保护的实施。

2 规范性引用文件

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

GB/T 5271.8 信息技术 词汇 第8部分：安全

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南

3 术语和定义

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

3.1

等级测评 classified security testing and evaluation

确定信息系统安全保护能力是否达到相应等级基本要求的过程。

4 等级保护实施概述

4.1 基本原则

信息系统安全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。信息系统安全等级保护实施过程中应遵循以下基本原则：

a) 自主保护原则

信息系统运营、使用单位及其主管部门按照国家相关法规和标准，自主确定信息系统的安全保护等级，自行组织实施安全保护。

b) 重点保护原则

根据信息系统的重要程度、业务特点，通过划分不同安全保护等级的信息系统，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。

c) 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。

d) 动态调整原则

要跟踪信息系统的变化情况，调整安全保护措施。由于信息系统的应用类型、范围等条件的变化及其他原因，安全保护等级需要变更的，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保护等级，根据信息系统安全保护等级的调整情况，重新实施安全保护。

4.2 角色和职责

信息系统安全等级保护实施过程中涉及的各类角色和职责如下：

a) 国家管理部门

公安机关负责信息安全等级保护工作的监督、检查、指导；国家保密工作部门负责等级保护工作中有关保密工作的监督、检查、指导；国家密码管理部门负责等级保护工作中有关密码工作的监督、检查、指导；涉及其他职能部门管辖范围的事项，由有关职能部门依照国家法律法规的规定进行管理；国务院信息化工作办公室及地方信息化领导小组办事机构负责等级保护工作的部门间协调。

b) 信息系统主管部门

负责依照国家信息安全等级保护的管理规范和技术标准，督促、检查和指导本行业、本部门或者本地区信息系统运营、使用单位的信息安全等级保护工作。

c) 信息系统运营、使用单位

负责依照国家信息安全等级保护的管理规范和技术标准，确定其信息系统的安全保护等级，有主管部门的，应当报其主管部门审核批准；根据已经确定的安全保护等级，到公安机关办理备案手续；按照国家信息安全等级保护管理规范和技术标准，进行信息系统安全保护的规划设计；使用符合国家有关规定，满足信息系统安全保护等级需求的信息技术产品和信息安全产品，开展信息系统安全建设或者改建工作；制定、落实各项安全管理制度，定期对信息系统的安全状况、安全保护制度及措施的落实情况进行自查，选择符合国家相关规定的等级测评机构，定期进行等级测评；制定不同等级信息安全事件的响应、处置预案，对信息系统的信息安全事件分等级进行应急处置。

d) 信息安全服务机构

负责根据信息系统运营、使用单位的委托，依照国家信息安全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，包括确定其信息系统的安全保护等级、进行安全需求分析、安全总体规划、实施安全建设和安全改造等。

e) 信息安全等级测评机构

负责根据信息系统运营、使用单位的委托或根据国家管理部门的授权，协助信息系统运营、使用单位或国家管理部门，按照国家信息安全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等级测评；对信息安全产品供应商提供的信息安全产品进行安全测评。

f) 信息安全产品供应商

负责按照国家信息安全等级保护的管理规范和技术标准，开发符合等级保护相关要求的信息安全产品，接受安全测评；按照等级保护相关要求销售信息安全产品并提供相关服务。

4.3 实施的基本流程

对信息系统实施等级保护的基本流程见图 1。

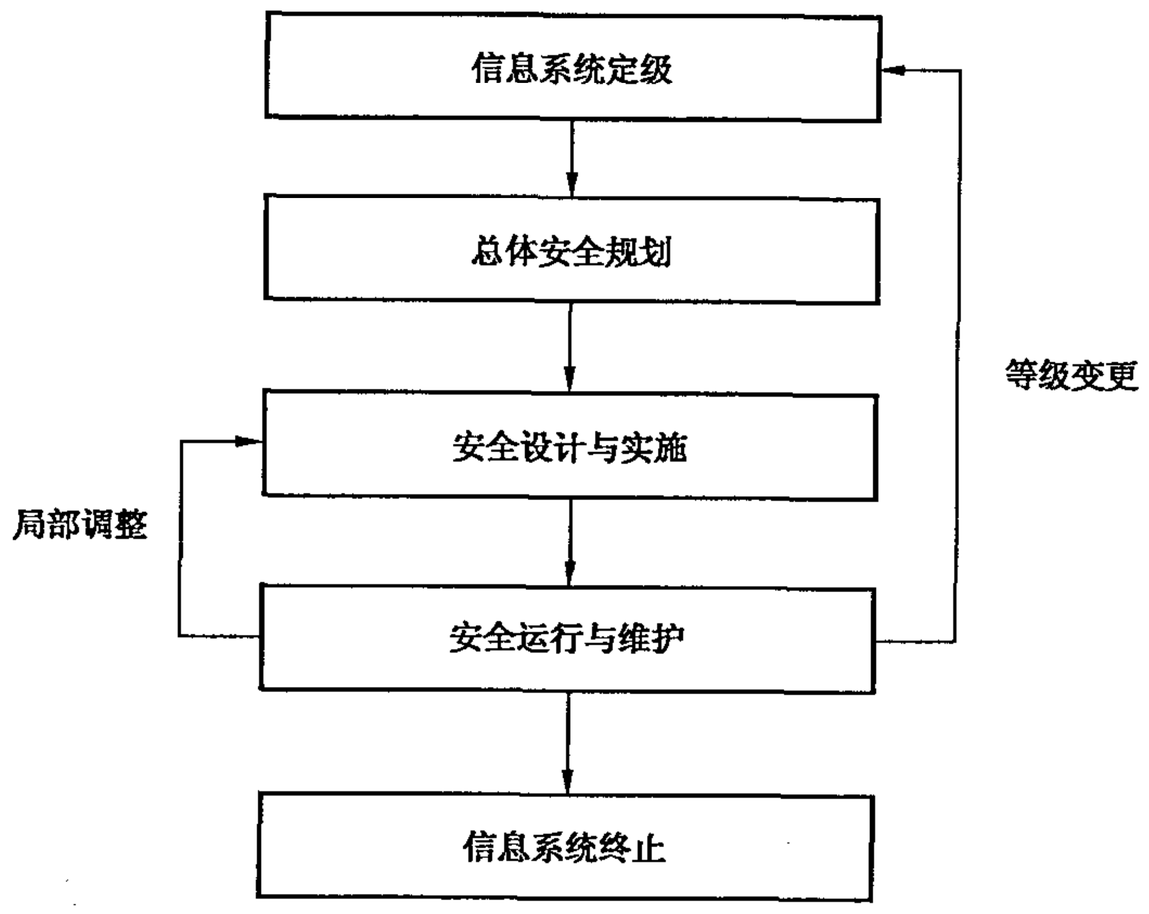

图 1 信息系统安全等级保护实施的基本流程

在安全运行与维护阶段，信息系统因需求变化等原因导致局部调整，而系统的安全保护等级并未改变，应从安全运行与维护阶段进入安全设计与实施阶段，重新设计、调整和实施安全措施，确保满足等级保护的要求；但信息系统发生重大变更导致系统安全保护等级变化时，应从安全运行与维护阶段进入信息系统定级阶段，重新开始一轮信息安全等级保护的实施过程。

信息系统安全等级保护实施基本流程中各个阶段的主要过程、活动、输入和输出见附录 A。

5 信息系统定级

5.1 信息系统定级阶段的工作流程

信息系统定级阶段的目标是信息系统运营、使用单位按照国家有关管理规范和 GB/T 22240—2008，确定信息系统的安全保护等级，信息系统运营、使用单位有主管部门的，应当经主管部门审核批准。

信息系统定级阶段的工作流程见图 2。

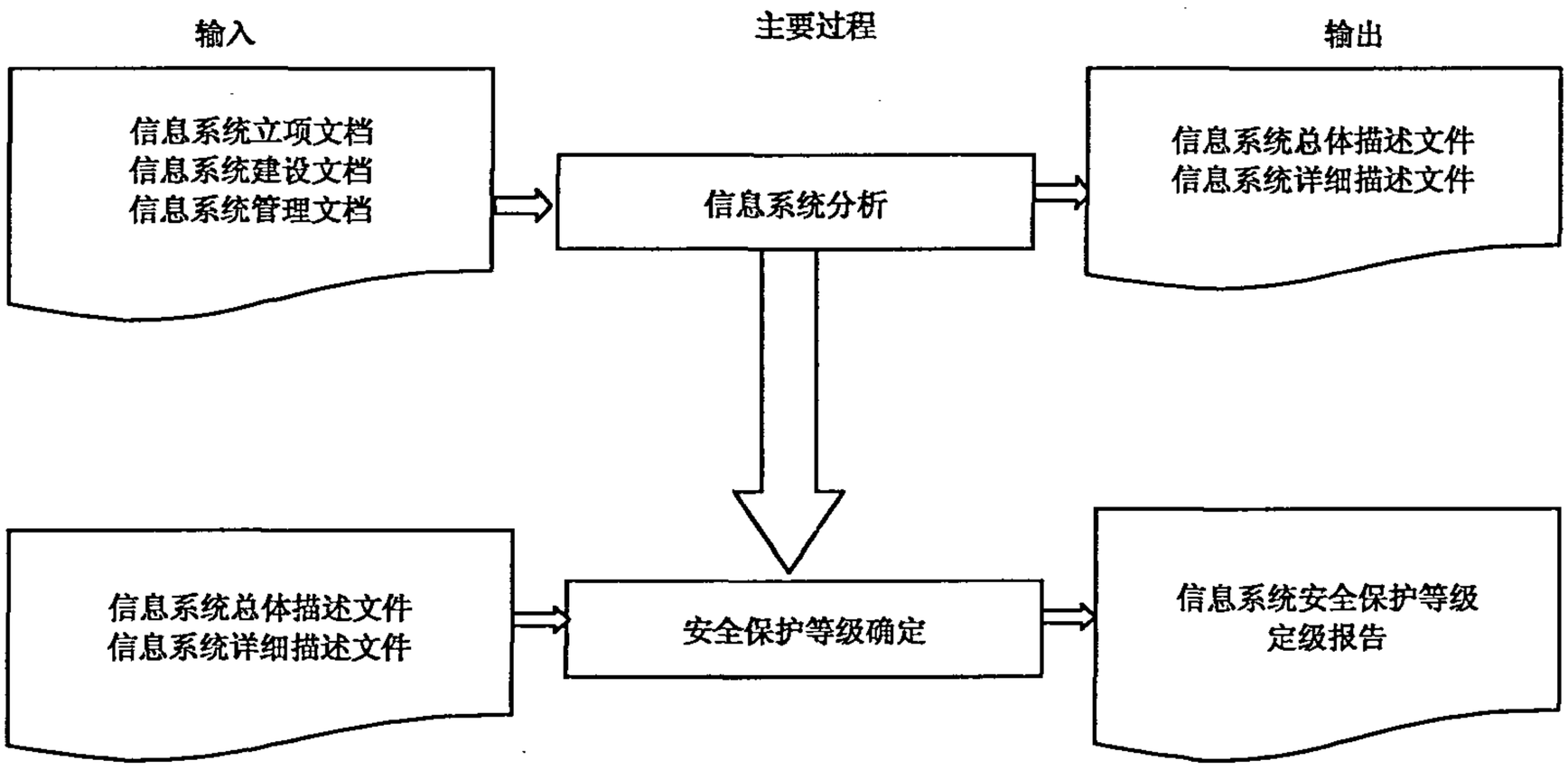

图 2 信息系统定级阶段工作流程

5.2 信息系统分析

5.2.1 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形成组织机构内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，信息安全服务机构。

活动输入：信息系统的立项、建设和管理文档。

活动描述：

本活动主要包括以下子活动内容：

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，从而明确信息系统的安全责任主体。

c) 识别信息系统的网络及设备部署

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，即确定定级对象及其范围。

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业务种类和数量，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，将承载比较单一的业务应用或者承载相对独立的业务应用的信息系统作为单独的定级对象。

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、完整性和可用性等方面的重要性程度。

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。

5.2.2 信息系统划分

活动目标：

本活动的目标是依据信息系统的总体描述文件，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，确定所包含可以作为定级对象的信息系统的个数。

参与角色：信息系统运营、使用单位，信息安全服务机构。

活动输入：信息系统总体描述文件。

活动描述：

本活动主要包括以下子活动内容：

a） 划分方法的选择

一个组织机构可能运行一个大型信息系统，为了突出重点保护的等级保护原则，应对大型信息系统进行划分，进行信息系统划分的方法可以有多种，可以考虑管理机构、业务类型、物理位置等因素，信息系统的运营、使用单位应该根据本单位的具体情况确定一个系统的分解原则。

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大型信息系统进行划分，划分出相对独立的信息系统并作为定级对象，应保证每个相对独立的信息系统具备定级对象的基本特征。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） 信息系统详细描述

在对信息系统进行划分并确定定级对象后，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定级对象的个数。

进一步的信息系统详细描述文件应包含以下内容：

1） 相对独立信息系统列表；

2) 每个定级对象的概述；

3) 每个定级对象的边界；

4) 每个定级对象的设备部署；

5) 每个定级对象支撑的业务应用及其处理的信息资产类型；

6) 每个定级对象的服务范围和用户类型；

7) 其他内容。

活动输出：信息系统详细描述文件。

5.3 安全保护等级确定

5.3.1 定级、审核和批准

活动目标：

本活动的目标是按照国家有关管理规范和 GB/T 22240—2008，确定信息系统的安全保护等级，并对定级结果进行审核和批准，保证定级结果的准确性。

参与角色：信息系统主管部门，信息系统运营、使用单位，信息安全服务机构。

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：

本活动主要包括以下子活动内容：

a) 信息系统安全保护等级初步确定

根据国家有关管理规范和 GB/T 22240—2008 确定的定级方法，信息系统运营、使用单位对每个定级对象确定初步的安全保护等级。

b) 定级结果审核和批准

信息系统运营、使用单位初步确定了安全保护等级后，有主管部门的，应当经主管部门审核批准。跨省或者全国统一联网运行的信息系统可以由主管部门统一确定安全保护等级。对拟确定为第四级以上信息系统的，运营使用单位或者主管部门应当邀请国家信息安全保护等级专家评审委员会评审。

活动输出：信息系统定级评审意见。

5.3.2 形成定级报告

活动目标：

本活动的目标是对定级过程中产生的文档进行整理，形成信息系统定级结果报告。

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：信息系统总体描述文件，信息系统详细描述文件，信息系统定级结果。

活动描述：

对信息系统的总体描述文档、信息系统的详细描述文件、信息系统安全保护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含以下内容：

a) 单位信息化现状概述；

b) 管理模式；

c) 信息系统列表；

d) 每个信息系统的概述；

e) 每个信息系统的边界；

f) 每个信息系统的设备部署；

g) 每个信息系统支撑的业务应用；

h) 信息系统列表、安全保护等级以及保护要求组合；

i) 其他内容。

活动输出：信息系统安全保护等级定级报告。

6 总体安全规划

6.1 总体安全规划阶段的工作流程

总体安全规划阶段的目标是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，通过分析明确信息系统安全需求，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，以指导后续的信息系统安全建设工程实施。对于已运营(运行)的信息系统，需求分析应当首先分析判断信息系统的安全保护现状与等级保护要求之间的差距。

总体安全规划阶段的工作流程见图 3。

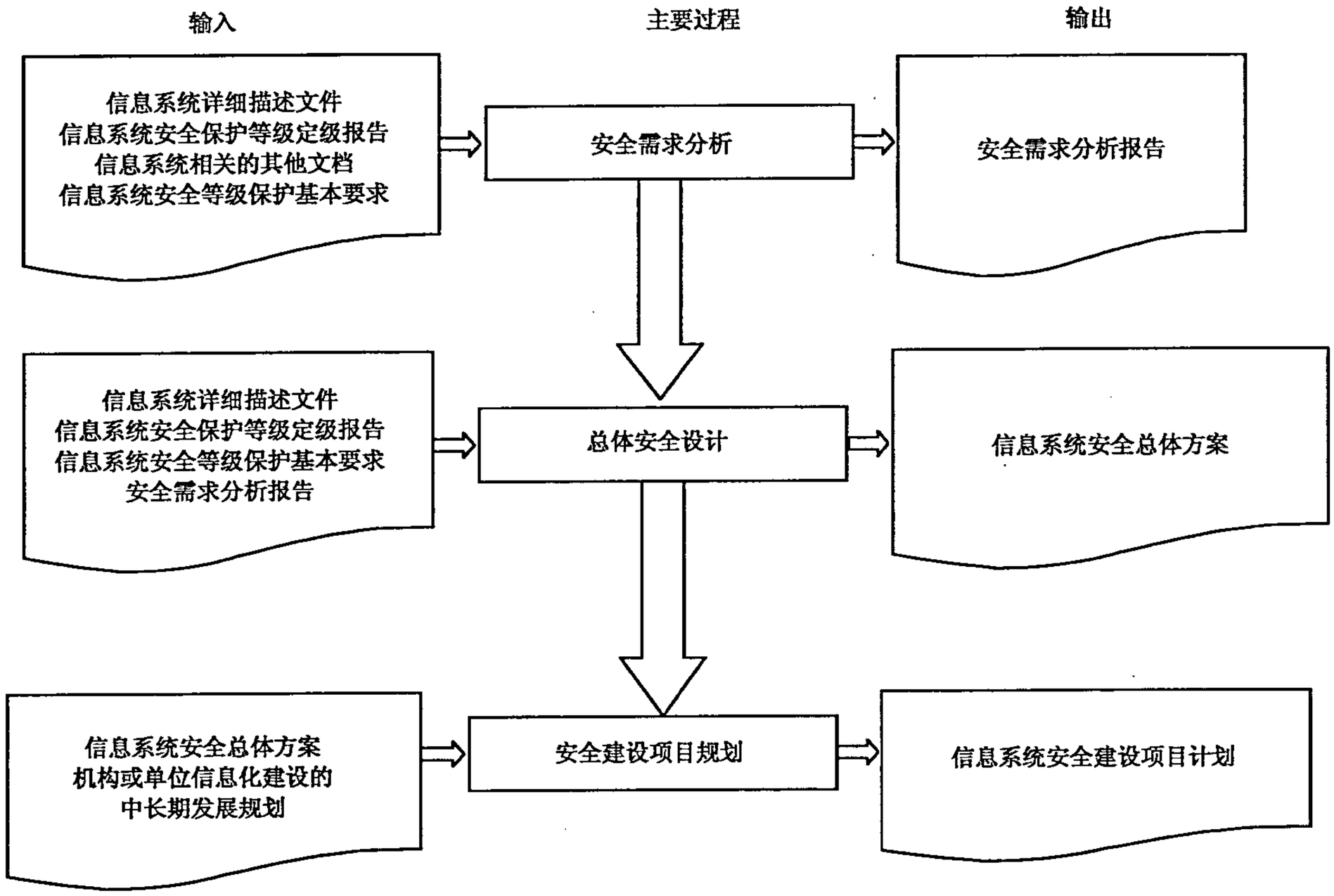

图 3 总体安全规划工作流程

6.2 安全需求分析

6.2.1 基本安全需求的确定

活动目标：

本活动的目标是根据信息系统的安全保护等级，判断信息系统现有的安全保护水平与国家等级保护管理规范和技术标准之间的差距，提出信息系统的基本安全保护需求。

参与角色：信息系统运营、使用单位，信息安全服务机构，信息安全等级测评机构。

活动输入：信息系统详细描述文件，信息系统安全保护等级定级报告，信息系统相关的其他文档，信息系统安全等级保护基本要求。

活动描述：

本活动主要包括以下子活动内容：

a) 确定系统范围和分析对象

明确不同等级信息系统的范围和边界，通过调查或查阅资料的方式，了解信息系统的构成，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。初步确定每个等级信息系统的分析对象，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。

b) 形成评价指标和评估方案

根据各个信息系统的安全保护等级从信息系统安全等级保护基本要求中选择相应等级的指标，形成评价指标。根据评价指标，结合确定的具体对象制定可以操作的评估方案，评估方案可以包含以下内容：

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。

c) 现状与评价指标对比

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和安全管理方面的评估，判断安全技术和安全管理的各个方面与评价指标的符合程度，给出判断结论。整理和分析不符合的评价指标，确定信息系统安全保护的基本需求。

活动输出：基本安全需求。

6.2.2 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基本要求的部分或具有特殊安全保护要求的部分，采用需求分析或风险分析的方法，确定可能的安全风险，判断对超出等级保护基本要求部分实施特殊安全措施的必要性，提出信息系统的特殊安全保护需求。

参与角色：信息系统运营、使用单位，信息安全服务机构。

活动输入：信息系统详细描述文件，信息系统安全保护等级定级报告，信息系统相关的其他文档。

活动描述：

确定特殊安全需求可以采用目前成熟或流行的需求分析或风险分析方法，或者采用下面介绍的活动：

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结果，结果产生的可能性或概率，结果造成的损害或影响的大小，以及避免上述结果产生的可能性、必要性和经济性。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。

6.2.3 形成安全需求分析报告

活动目标：

本活动的目标是总结基本安全需求和特殊安全需求，形成安全需求分析报告。

参与角色：信息系统运营、使用单位，信息安全服务机构。

活动输入:信息系统详细描述文件,信息系统安全保护等级定级报告,基本安全需求,重要资产的特殊保护要求。

活动描述:

本活动主要的子活动是完成安全需求分析报告。

根据基本安全需求和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含以下内容:

1) 信息系统描述;

2) 安全管理状况;

3) 安全技术状况;

4) 存在的不足和可能的风险;

5) 安全需求描述。

活动输出:安全需求分析报告。

6.3 总体安全设计

6.3.1 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,制定安全策略,以便结合等级保护基本要求和安全保护特殊要求,构建机构信息系统的安全技术体系结构和安全管理体系结构。

参与角色:信息系统运营、使用单位,信息安全服务机构。

活动输入:信息系统详细描述文件,信息系统安全保护等级定级报告,安全需求分析报告。

活动描述:

本活动主要包括以下子活动内容:

a) 确定安全方针

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) 制定安全策略

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、子系统互连策略、信息流控制策略等。

活动输出:总体安全策略文件。

6.3.2 安全技术体系结构设计

活动目标:

本活动的目标是根据信息系统安全等级保护基本要求、安全需求分析报告、机构总体安全策略文件等,提出系统需要实现的安全技术措施,形成机构特定的系统安全技术体系结构,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,信息安全服务机构。

活动输入:信息系统详细描述文件,信息系统安全保护等级定级报告,安全需求分析报告,信息系统安全等级保护基本要求。

活动描述:

本活动主要包括以下子活动内容:

a) 规定骨干网或城域网的安全保护技术措施

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,提出骨干网或城域网的安全保护策略和安全技术措施。骨干网或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,如果不同级别的子系统通过骨干网或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子系统的等级保护基本要求。

b) 规定子系统之间互联的安全技术措施

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子系统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子系统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) 规定不同级别子系统的边界保护技术措施

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，提出不同级别子系统边界的安全保护策略和安全技术措施。子系统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，如果不同级别的子系统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子系统的等级保护基本要求。

d) 规定不同级别子系统内部系统平台和业务应用的安全保护技术措施

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，提出不同级别子系统内部网络平台、系统平台和业务应用的安全保护策略和安全技术措施。

e) 规定不同级别信息系统机房的安全保护技术措施

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) 形成信息系统安全技术体系结构

将骨干网或城域网、通过骨干网或城域网的子系统互联、局域网内部的子系统互联、子系统的边界、子系统内部各类平台、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体系结构。

活动输出：信息系统安全技术体系结构。

6.3.3 整体安全管理体系结构设计

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，最后形成统一的整体安全管理体系结构。

参与角色：信息系统运营、使用单位，信息安全服务机构。

活动输入：信息系统详细描述文件，信息系统安全保护等级定级报告，安全需求分析报告，信息系统安全等级保护基本要求。

活动描述：

本活动主要包括以下子活动内容：

a) 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策略等。

b) 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) 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) 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) 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行与维护框架和运维安全策略等。

f) 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体系结构。

活动输出：信息系统安全管理体系结构。

6.3.4 设计结果文档化

活动目标：

本活动的目标是将总体安全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，信息安全服务机构。

活动输入：安全需求分析报告，信息系统安全技术体系结构，信息系统安全管理体系结构。

活动描述：

对安全需求分析报告、信息系统安全技术体系结构和安全管理体系结构等文档进行整理，形成信息系统总体安全方案。

信息系统总体安全方案包含以下内容：

a) 信息系统概述；

b) 总体安全策略；

c) 信息系统安全技术体系结构；

d) 信息系统安全管理体系结构。

活动输出：信息系统安全总体方案。

6.4 安全建设项目规划

6.4.1 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总体方案(一个或多个文件构成)、机构或单位信息化建设的中长期发展规划和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、使用单位，信息安全服务机构。

活动输入：信息系统安全总体方案、机构或单位信息化建设的中长期发展规划。

活动描述：

本活动主要包括以下子活动内容：

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。

6.4.2 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、使用单位，信息安全服务机构。

活动输入：信息系统安全总体方案，信息系统分阶段安全建设目标。

活动描述：

本活动主要包括以下子活动内容：

a) 确定主要安全建设内容

根据信息系统安全总体方案明确主要的安全建设内容，并将其适当的分解。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，形成安全建设项目列表。

活动输出：安全建设项目列表(含安全建设内容)。

6.4.3 形成安全建设项目计划

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，形成安全建设项目计划。

参与角色：信息系统运营、使用单位，信息安全服务机构。

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

活动描述：

对信息系统分阶段安全建设目标、安全总体方案和安全建设内容等文档进行整理，形成信息系统安全建设项目计划。

安全建设项目计划可包含以下内容：

a) 规划建设的依据和原则；
b) 规划建设的目标和范围；
c) 信息系统安全现状；
d) 信息化的中长期发展规划；
e) 信息系统安全建设的总体框架；
f) 安全技术体系建设规划；
g) 安全管理与安全保障体系建设规划；
h) 安全建设投资估算；
i) 信息系统安全建设的实施保障等内容。

活动输出：信息系统安全建设项目计划。

7 安全设计与实施

7.1 安全设计与实施阶段的工作流程

安全设计与实施阶段的目标是按照信息系统安全总体方案的要求，结合信息系统安全建设项目计划，分期分步落实安全措施。

安全设计与实施阶段的工作流程见图 4。

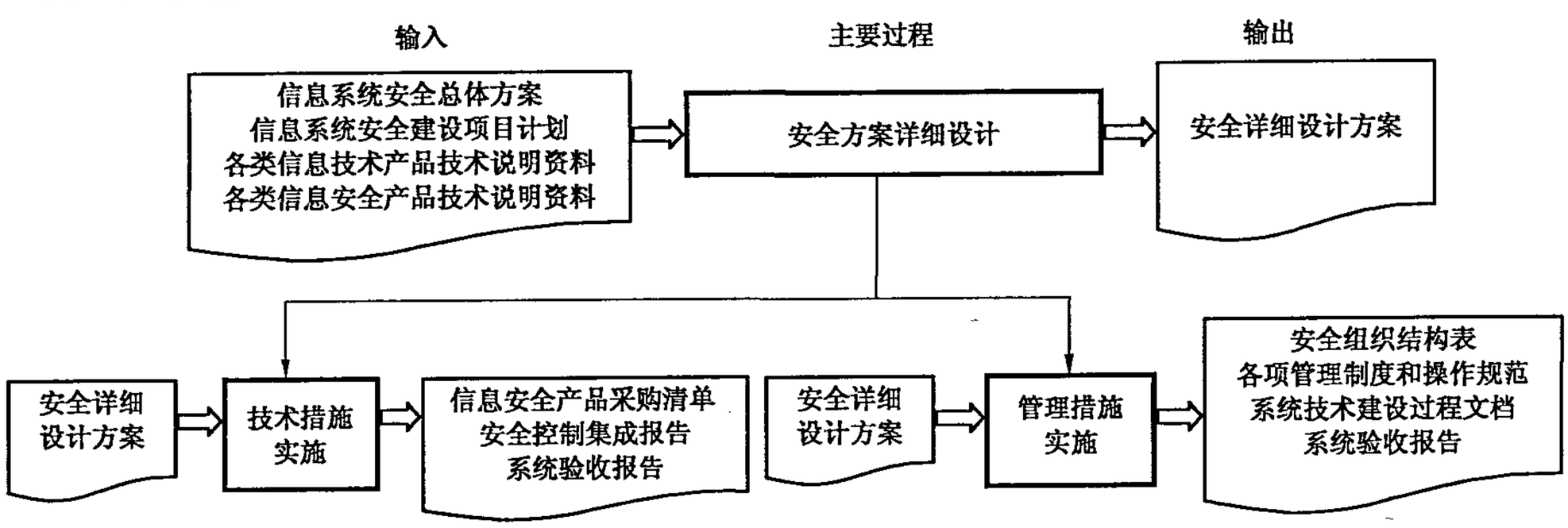

图 4 安全设计与实施流程图

7.2 安全方案详细设计

7.2.1 技术措施实现内容设计

活动目标：

本活动的目标是根据建设目标和建设内容将信息系统安全总体方案中要求实现的安全策略、安全技术体系结构、安全措施和要求落实到产品功能或物理形态上，提出能够实现的产品或组件及其具体规范，并将产品功能特征整理成文档。使得在信息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，信息安全服务机构，信息安全产品供应商。

活动输入：信息系统安全总体方案，信息系统安全建设项目计划，各类信息技术产品和信息安全产品技术说明资料。

活动描述：

本活动主要包括以下子活动内容：

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，给出与总体安全规划阶段的安全体系结构一致的安全实现技术框架，内容可能包括安全防护的层次、信息安全产品的使用、网络子系统划分、IP 地址规划等内容。

b) 功能要求设计

对安全实现技术框架中使用到的相关信息安全产品，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使用到的相关信息安全产品，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，包括信息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中提出的安全策略的要求，制定设计和设置信息安全产品或安全组件

的安全策略实现计划。

活动输出:技术措施落实方案。

7.2.2 管理措施实现内容设计

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中管理部分相适应的本期安全实施内容,以保证在安全技术建设的同时,安全管理得以同步建设。

参与角色:信息系统运营、使用单位,信息安全服务机构。

活动输入:信息系统安全总体方案,信息系统安全建设项目计划。

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:管理措施落实方案。

7.2.3 设计结果文档化

活动目标:

本活动的目标是将技术措施落实方案、管理措施落实方案汇总,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,信息安全服务机构。

活动输入:技术措施落实方案,管理措施落实方案。

活动描述:

对技术措施落实方案中技术实施内容和管理措施落实方案中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含以下内容:

a) 本期建设目标和建设内容;

b) 技术实现框架;

c) 信息安全产品或组件功能及性能;

d) 信息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) 项目投资概算。

活动输出:安全详细设计方案。

7.3 管理措施实施

7.3.1 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,信息安全服务机构。

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:

本活动主要包括以下子活动内容:

a) 安全组织确定

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,确保所有的风险都有人负责应对。

活动输出:机构、角色与职责说明书。

7.3.2 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、运行维护、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,信息安全服务机构。

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:

本活动主要包括以下子活动内容:

a) 应用范围明确

管理制度建立首先要明确制度的应用范围,如机房管理、账户管理、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) 人员职责定义

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) 行为规范规定

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。

7.3.3 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,信息安全服务机构。

活动输入:系统或产品使用说明书,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。

7.3.4 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,信息安全服务机构,信息安全产品供应商。

活动输入:安全设计与实施阶段参与各方相关进度控制和质量监督要求文档。

活动描述:

本活动主要包括以下子活动内容:

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。

7.4 技术措施实施

7.4.1 信息安全产品采购

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信息安全产品。

参与角色：信息安全产品供应商，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：

本活动主要包括以下子活动内容：

a) 制定产品采购说明书

信息安全产品选型过程首先依据安全详细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信息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，用户在选择信息安全产品时应确保符合国家关于信息安全产品使用的有关规定。对于密码产品的使用，应当按照国家密码管理的相关规定进行选择和使用。

活动输出：需采购信息安全产品清单。

7.4.2 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信息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控制同步建设。

参与角色：信息系统运营、使用单位，信息安全服务机构。

活动输入：安全详细设计方案。

活动描述：

本活动主要包括以下子活动内容：

a) 安全措施需求分析

以规范的形式准确表达安全方案设计中的指标要求，确定软件设计的约束和软件同其他系统相关的接口细节。

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，并通过论证和测试。

e) 测试

开发基本完成后要进行测试，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步骤。

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。

7.4.3 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，将信息安全产品、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、质量控制等有机结合起来，遵循运营使用单位与信息安全服务机构共同参与相互配合的实施原则。

参与角色：信息系统运营、使用单位，信息安全服务机构。

活动输入：安全详细设计方案。

活动描述：

本活动主要包括以下子活动内容：

a) 集成实施方案制定

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

主要工作内容是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，信息安全服务机构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

主要工作内容是将配置好策略的信息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。集成实施应严格按照集成进度安排进行，出现问题各方应及时沟通。系统实施的各个环节应该遵照质量控制方案的要求，分别进行系统测试，逐步实现质量控制目标。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

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，其包含集成实施方案、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。

7.4.4 系统验收

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，系统测试及验收是从总体出发，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，也包括对管理措施落实内容的验收。

参与角色：信息系统主管部门，信息系统运营、使用单位，信息安全服务机构。

活动输入：安全详细设计方案，安全控制集成报告。

活动描述：

本活动主要包括以下子活动内容：

a) 系统验收准备

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，准备系统验收方案。系统验收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需求。

成立系统验收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) 组织系统验收

由系统验收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系统验收方案对系统进行测试。

c) 验收报告

在测试完成后形成验收报告，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结论，安全服务提供商应当根据验收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

在系统验收通过以后，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 安全运行与维护

8.1 安全运行与维护阶段的工作流程

安全运行与维护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，涉及的内容较多，包括安全运行与维护机构和安全运行与维护机制的建立，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，安全状态监控和安全事件处置，安全审计和安全检查等内容。本标准并不对上述所有的管理过程进行描述，希望全面了解和控制安全运行与维护阶段各类过程的本标准使用者可以参见其他标准或指南。

本标准关注安全运行与维护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、等级测评、系统备案以及监督检查等过程。

安全运行与维护阶段的工作流程见图 5。

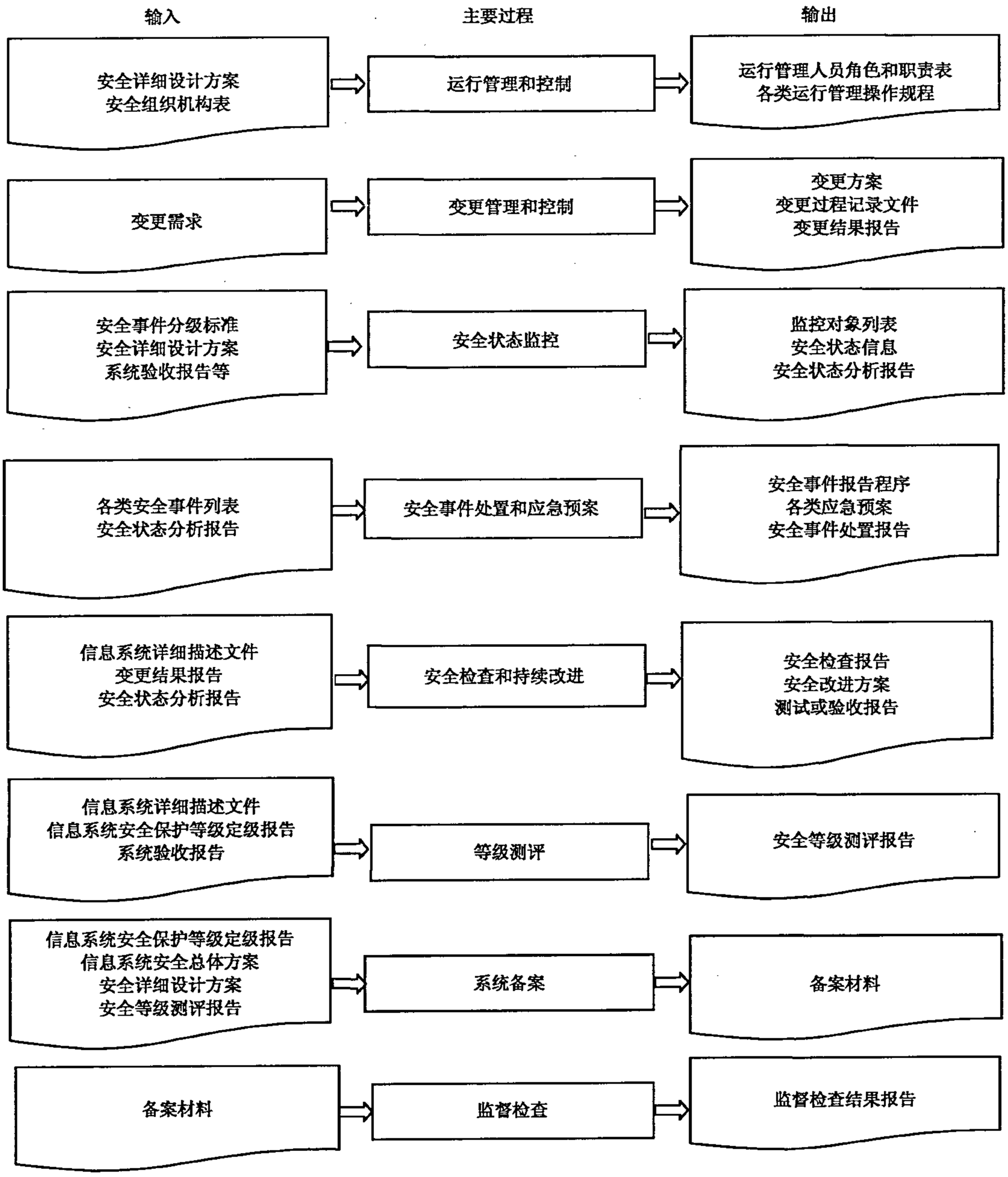

图 5 安全运行与维护阶段的主要过程

8.2 运行管理和控制

8.2.1 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：

本活动主要包括以下子活动内容：

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。越高安全保护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。安全保护等级越高的系统管理权限的划分也越细。

c) 定义人员职责

根据不同的安全保护等级要求的控制粒度，分析所需要运行管理控制的内容，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。

8.2.2 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：

本活动主要包括以下子活动内容：

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。

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。

8.3 变更管理和控制

8.3.1 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：

本活动主要包括以下子活动内容：

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保护等级发生变化的重大变更，则需要重新确定信息系统安全保护等级，返回到等级保护实施过程的信息系统定级阶段。如果是局部调整，则需要确定配套进行的其他工作内容。

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。

8.3.2 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：

本活动主要包括以下子活动内容：

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。

8.4 安全状态监控

8.4.1 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：

本活动主要包括以下子活动内容：

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。

8.4.2 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:

本活动主要包括以下子活动内容:

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、监控工具的功能和性能特点等,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。

8.4.3 监控状态分析和报告

活动目标:

本活动的目标是通过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:

本活动主要包括以下子活动内容:

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。

8.5 安全事件处置和应急预案

8.5.1 安全事件分级

活动目标:

本活动的目标是结合信息系统的实际情况,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分级。

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:

本活动主要包括以下子活动内容:

a) 安全事件调查和分析

针对各类安全事件列表，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，并根据信息安全事件造成的损失程度，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等因素，确定事件等级，制定安全事件的报告程序。

活动输出：安全事件报告程序。

8.5.2 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：

本活动主要包括以下子活动内容：

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，确定不同等级事件的响应和处置范围、程度以及适用的管理制度，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，并按照预案定期开展演练。

活动输出：各类应急预案。

8.5.3 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：

本活动主要包括以下子活动内容：

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，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，按照安全事件报告程序上报安全事件，确定是否应对安全事件启动应急预案。

b) 安全事件处置

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，应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。

8.6 安全检查和持续改进

8.6.1 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。

关于等级测评见 8.7,关于监督检查见 8.9,本条描述自我检查过程。

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:信息系统详细描述文件,变更结果报告,安全状态分析报告。

活动描述:

本活动主要包括以下子活动内容:

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。

8.6.2 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:

本活动主要包括以下子活动内容:

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,如果涉及安全保护等级的变化,则应进入安全保护等级保护实施的一个新的循环过程;如果安全保护等级不变,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,重新开始安全设计和实施过程,见第 7 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。

8.6.3 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：

本活动主要包括以下子活动内容：

a) 安全方案实施控制

见 7.3.4。

b) 安全措施测试与验收

见 7.4.4。

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。

8.7 等级测评

活动目标：

本活动的目标是通过信息安全等级测评机构对已经完成等级保护建设的信息系统定期进行等级测评，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，信息安全等级测评机构。

活动输入：信息系统详细描述文件，信息系统安全保护等级定级报告，系统验收报告。

活动描述：

参见有关信息系统安全保护等级测评的规范或标准。

活动输出：安全等级测评报告。

8.8 系统备案

活动目标：

本活动的目标是根据国家管理部门对备案的要求，整理相关备案材料，并向受理备案的单位提交备案材料。

参与角色：信息系统主管部门，信息系统运营、使用单位，国家管理部门。

活动输入：信息系统安全保护等级定级报告，信息系统安全总体方案，安全详细设计方案，安全等级测评报告。

活动描述：

本活动主要包括以下子活动内容：

a) 备案材料整理

信息系统运营、使用单位针对备案材料的要求，整理、填写备案材料。

b) 备案材料提交

信息系统运营、使用单位根据国家管理部门的要求办理定级备案手续，提交备案材料；国家管理部门接收备案材料。

活动输出：备案材料。

8.9 监督检查

活动目标：

本活动的目标是通过国家管理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:信息系统主管部门,信息系统运营、使用单位,国家管理部门。

活动输入:备案材料。

活动描述:

参见信息安全等级保护监督检查的规范或标准。

活动输出:监督检查结果报告。

9 信息系统终止

9.1 信息系统终止阶段的工作流程

信息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机构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。

本标准在信息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。

信息系统终止阶段的工作流程见图 6。

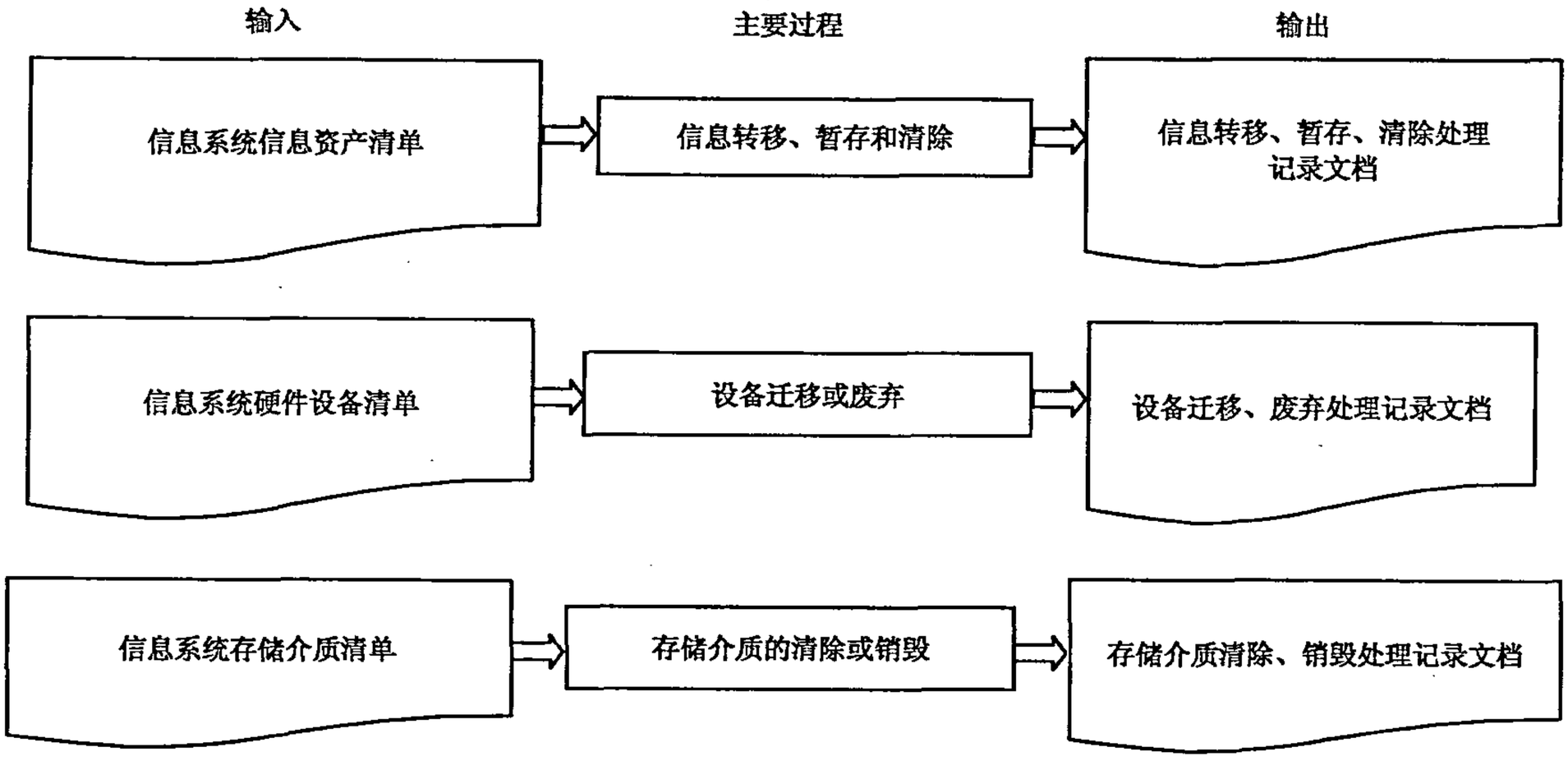

图 6 信息系统终止阶段的工作流程

9.2 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:信息系统运营、使用单位。

活动输入:信息系统信息资产清单。

活动描述:

本活动主要包括以下子活动内容:

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。

9.3 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：信息系统运营、使用单位。

活动输入：设备迁移或废弃清单等。

活动描述：

本活动主要包括以下子活动内容：

a) 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。

b) 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。

c) 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。

d) 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。

9.4 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：信息系统运营、使用单位。

活动输入：存储介质清单等。

活动描述：

本活动主要包括以下子活动内容：

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）
主要过程及其活动输出

主要阶段	主要过程	活 动	活动输入	活动输出
信息系统定级	信息系统分析	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
	安全保护等级确定	定级、审核和批准	信息系统总体描述文件 信息系统详细描述文件	定级结果
		形成定级报告	信息系统总体描述文件 信息系统详细描述文件 定级结果	* 信息系统安全保护等级定级报告
总体安全规划	安全需求分析	基本安全需求确定	信息系统详细描述文件 信息系统安全保护等级定级报告 信息系统安全等级保护基本要求 信息系统相关的其他文档	基本安全需求
		特殊安全需求的确定	信息系统详细描述文件 信息系统安全保护等级定级报告 信息系统相关的其他文档	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 信息系统安全保护等级定级报告 信息系统安全等级保护基本要求 基本安全需求 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	总体安全策略设计	信息系统详细描述文件 信息系统安全保护等级定级报告 安全需求分析报告	总体安全策略文件
		各级系统安全技术措施设计	总体安全策略文件 安全需求分析报告 信息系统安全等级保护基本要求	信息系统安全技术体系结构
		系统整体安全管理策略设计	总体安全策略文件 安全需求分析报告 信息系统安全等级保护基本要求	信息系统安全管理体系结构
		设计结果文档化	安全需求分析报告 信息系统安全技术体系结构 信息系统安全管理体系结构	* 信息系统安全总体方案
	安全建设项目规划	安全建设目标确定	信息系统安全总体方案 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 信息系统分阶段安全建设目标	安全建设内容

主要阶段	主要过程	活　　动	活动输入	活动输出
总体安全规划	安全建设项目规划	安全建设项目计划设计	信息系统安全总体方案 信息系统分阶段安全建设目标 安全建设内容	* 信息系统安全建设项目计划
安全设计与实施	安全方案详细设计	技术措施实现内容设计	信息系统安全总体方案 信息系统安全建设项目计划 各类信息技术产品技术说明资料 各类信息安全产品技术说明资料	技术措施实现方案
		管理措施实现内容设计	信息系统安全总体方案 信息系统安全建设项目计划	管理措施实现方案
		设计结果文档化	技术措施落实方案 管理措施落实方案	* 安全详细设计方案
	管理措施落实	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	系统或产品使用说明书 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
	技术措施落实	信息安全产品采购	安全详细设计方案、相关产品信息	已采购信息安全产品清单
		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
		系统验收	安全详细设计方案 安全控制集成报告	* 系统验收报告
安全运行与维护	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
		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

主要阶段	主要过程	活　　动	活动输入	活动输出
安全运行与维护	安全事件处置和应急预案	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
	等级测评		信息系统安全保护等级定级报告 系统验收报告 测试或验收报告	* 安全等级测评报告
	系统备案		信息系统安全保护等级定级报告 信息系统安全总体方案 安全详细设计方案 安全等级测评报告	* 备案材料
	监督检查		备案材料	* 监督检查结果报告
信息系统终止	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。				

中华人民共和国
国家标准
信息安全技术
信息系统安全等级保护实施指南
GB/T 25058—2010
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 2.25 字数 60 千字
2010年11月第一版 2010年11月第一次印刷
*
书号:155066·1-40462

GB/T 25058-2010