ICS 35.040
L 80

信息安全技术 网络安全等级保护实施指南

Information security technology—Implementation guide for classified protection of cybersecurity

GB/T 25058—2019
代替 GB/T 25058—2010

2020-03-01 实施

2019-08-30 发布

国家市场监督管理总局
中国国家标准化管理委员会 发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 25058—2010《信息安全技术 信息系统安全等级保护实施指南》，与 GB/T 25058—2010 相比，主要变化如下：

——标准名称变更为《信息安全技术 网络安全等级保护实施指南》；

[illegible]

——在总体安全规划阶段中增加了"设计等级保护对象的安全管理体系框架"内容，要求根据 GB/T 22239、安全需求分析报告等设计安全管理体系框架，并提出了安全管理体系框架（见 6.3.3，2010 年版的 6.3.3）；

——在安全设计与实施阶段，将"安全措施实现"与"管理措施实现"调换顺序（见 7.3，2010 年版的 7.3、7.4）；将"人员安全技能培训"合并到"安全管理机构和人员的设置"中（见 7.4.2，2010 年版的 7.5.1、7.5.3）；将"安全管理制度的建设和修订"与"安全管理机构和人员的设置"调换顺序（见 7.4.1、7.4.2，2010 年版的 7.5.1、7.5.2）；

[illegible]

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:公安部第三研究所(公安部信息安全等级保护评估中心)、中国电子科技集团公司第十五研究所(信息产业信息安全测评中心)、北京安信天行科技有限公司。

本标准主要起草人:袁静、任卫红、毕马宁、黎水林、刘健、翟建军、王然、张益、江雷、赵泰、李明、马力、于东升、陈广勇、沙淼淼、朱建平、曲洁、李升、刘静、罗峥、彭海龙、徐爽亮。

本标准所代替标准的历次版本发布情况为:

——GB/T 25058—2010。

信息安全技术
网络安全等级保护实施指南

1 范围

本标准规定了等级保护对象实施网络安全等级保护工作的过程。

本标准适用于指导网络安全等级保护工作的实施。

2 规范性引用文件

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

GB 17859 计算机信息系统 安全保护等级划分准则

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 22240 信息安全技术 信息系统安全等级保护定级指南

GB/T 25069 信息安全技术 术语

GB/T 28448 信息安全技术 网络安全等级保护测评要求

3 术语和定义

GB 17859、GB/T 22239、GB/T 25069 和 GB/T 28448 界定的术语和定义适用于本文件。

4 等级保护实施概述

4.1 基本原则

安全等级保护的核心是将等级保护对象划分等级，按标准进行建设、管理和监督。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

等级保护对象运营、使用单位及其主管部门按照国家相关法规和标准，自主确定等级保护对象的安全保护等级，自行组织实施安全保护。

b) 重点保护原则

[redacted]

c) 同步建设原则

[redacted]

d) 动态调整原则

[redacted]

其他原因，安全保护等级需要变更的，应根据等级保护的管理规范和技术标准的要求，重新确定定级对象的安全保护等级，根据其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

等级保护对象实施网络安全等级保护过程中涉及的各类角色和职责如下：

a） 等级保护管理部门

等级保护管理部门依照等级保护相关法律、行政法规的规定，在各自职责范围内负责网络安全保护监督管理工作。

b） 主管部门

负责依照国家网络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、本部门或者本区等级保护对象运营、使用单位的网络安全等级保护工作。

c） 运营、使用单位

负责等级保护对象的安全保护工作。

d） 网络安全服务机构

负责根据运营、使用单位的委托，协助运营、使用单位或等级保护对象的主管部门完成等级保护的相关工作。

e） 网络安全等级测评机构

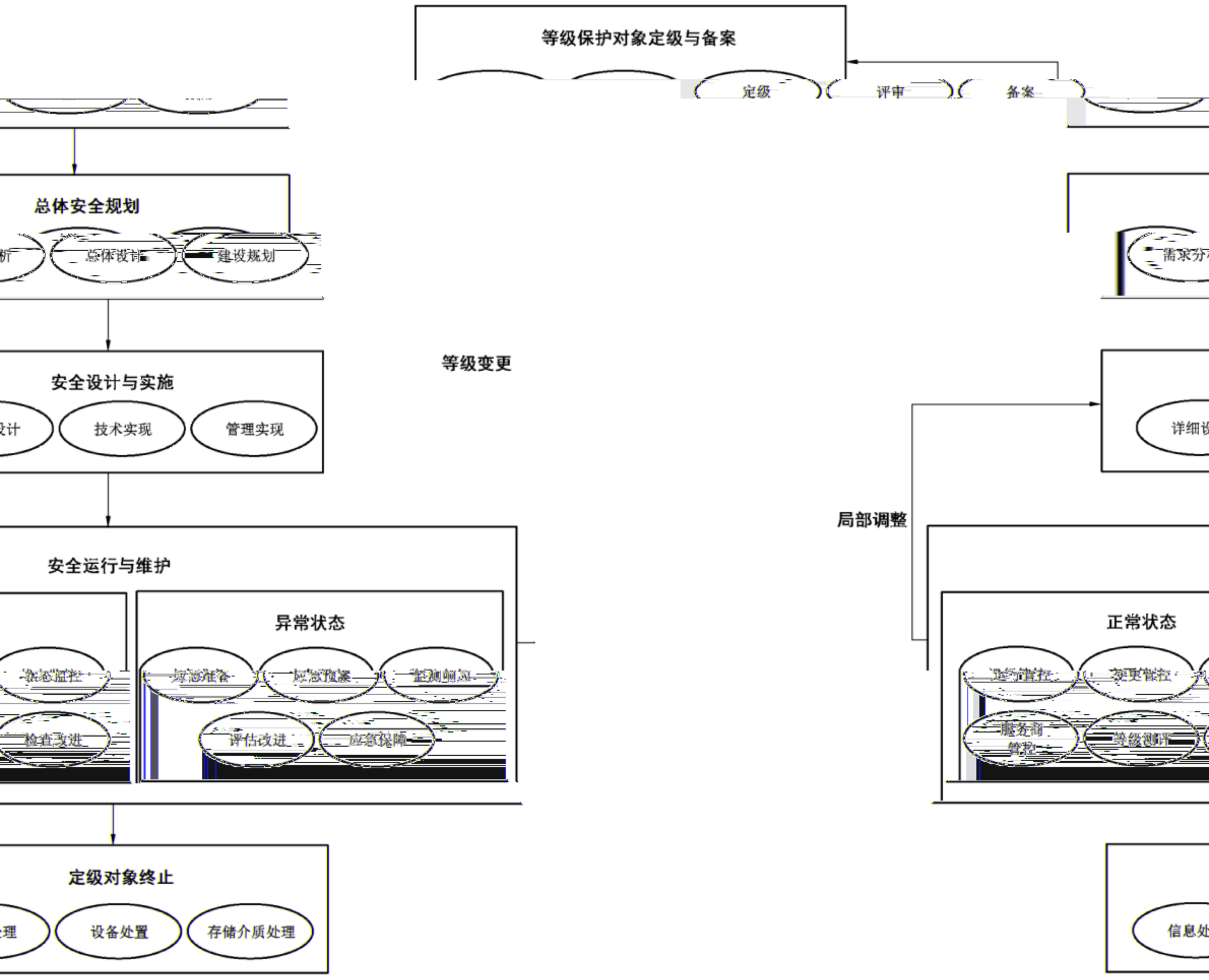
负责根据运营、使用单位的委托，依据网络安全等级保护管理规范和技术标准，对等级保护对象的安全保护状况进行等级测评。

f） 网络安全产品供应商

负责按照国家网络安全等级保护的管理规范和技术标准，为等级保护对象提供符合其相关要求的网络安全产品或相关服务。

4.3 实施的基本流程

对等级保护对象实施等级保护的基本流程包括等级保护对象定级与备案阶段、总体安全规划阶段、安全设计与实施阶段、安全运行与维护阶段和定级对象终止阶段，见图1。



等级保护工作实施的基本流程

图 1　安全

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

发生重大变更导致安全保护等级变化时，应从安全运行与维护阶段进入等

变，应从安全运行与维护阶段

保护的要求，当等级保护对象

护过程中，发生安全事件时可能会发生应急响应与保障。

等级保护对象安全等级保护实施的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 等级保护对象定级与备案

5.1 定级与备案阶段的工作流程

等级保护对象定级阶段的目标是运营、使用单位按照国家有关管理规范和定级标准，确定等级保护对象及其安全保护等级，并经过专家评审。运营、使用单位有主管部门的，应经主管部门审核、批准，并报公安机关备案审查。

等级保护对象定级与备案阶段的工作流程见图 2。

图 2 定级与备案阶段工作流程

活动目标：

行业/领域主管部门在必要时可组织梳理行业/领域的主要社会功能/职能及作用，分析履行主要社会功能/职能所依赖的主要业务及服务范围，最后依据分析和整理的内容形成行业/领域的业务总体描述性文档。

参与角色：主管部门，网络安全服务机构。

活动输入：行业介绍文档，GB/T 22240。

活动描述：

本活动主要包括以下子活动内容：

a） 识别、分析行业/领域重要性

主管部门组织梳理本行业/领域的行业特征、业务类型等内容，分析履行主要社会功能/职能和业务连续性等重要因素，分析主要社会功能/职能在保障国家安全、经济发展、社会秩序、公共服务等方面发挥的重要作用。

b） 识别行业/领域的主要业务

主管部门可组织梳理本行业/领域中主要依靠信息化处理的业务情况，并按照业务承载的社会功

定级指导

务重要性分析各

主管部门可组织分析本行业/领域内的主要业务，并根据业务信息重要性和业务

定级指导意见，

主要业务的安全保护等级和本系统自身情况确定主要业务的行业/领域

业定级工作部署

域的定级指导意见，统一部署全行业/领域的定级工作；行业/领域主

主管部门可制定本行业

结果进行审核、批准

管部门应对下属单位的定级

5.3 等级保护对象分析

5.3.1 对象重要性分析

活动目标：

通过收集了解有关等级保护对象的信息，并对信息进行综合分析和整理，分析单位的主要社会功能/职能及作用，确定履行主要社会功能/职能所依赖的等级保护对象，整理等级保护对象处理的业务及服务范围，最后依据分析和整理的内容，有行业/领域定级指导意见的还应依据行业/领域定级指导意

指导意见，行业/领域定级指导意见。

和生产产值等信息，分析主要社

挥的重要作用。

属性和业务内容，确定单位的等

情况，获得等级保护对象的背景

业务运行中的作用、岗位职责，获

确等级保护对象的安全责任

参与角色：至少一位使用单位、网络安全服务机构。

活动输入：单位情况说明文档、等级保护对象的立项、建设和管理文

活动描述：

本活动主要包括以下子活动内容：

a) 识别单位的基本信息

调查了解等级保护对象所属单位的业务范围、主要社会功能/职能

会功能/职能在保障国家安全、经济发展、社会秩序、公共服务等方面发

b) 识别单位的等级保护对象基本信息

了解单位内主要依靠信息化处理的业务情况，这些业务各自的社会

级保护对象。并确定等级保护对象的业务范围、地理位置以及其他基本

信息和联络方式。

c) 识别等级保护对象的管理框架

了解等级保护对象的组织管理结构、管理策略、部门设置和部门在

得支撑等级保护对象业务运营的管理特征和管理框架方面的信息，从

主管。

d) 识别等级保护对象的网络及设备部署

了解等级保护对象的物理环境、网络拓扑结构和硬件设备的部署情

象的边界，即确定等级保护对象及其范围。

e) 识别等级保护对象的业务特性

了解单位内主要依靠信息化处理的各种业务及业务流程，从中明确

对象的业务特性。

f) 识别等级保护对象处理的信息资产

了解等级保护对象处理的信息资产的类型，这些信息资产在保密性

在此基础上明确等级保护对

支撑单位业务运营的等级保护

、完整性和可用性等方面的重要

性程度。

g) 识别用户范围和用户类型

[illegible]

h) 等级保护对象描述

对收集的信息进行整理、分析，形成对等级保护对象的总体描述文件。一个典型的等级保护对象的总体描述文件应包含以下内容：

1) 等级保护对象概述；

2) 等级保护对象重要性分析；

3) 等级保护对象边界描述；

4) 网络拓扑；

5) 设备部署；

6) 支撑的业务应用的种类和特性；

7) 处理的信息资产；

8) 用户的范围和用户类型；

9) 等级保护对象的管理框架。

活动输出，等级保护对象总体描述文件。

5.3.2 定级对象确定

活动目标：

依据单位的等级保护对象总体描述文件(有行业/领域定级指导意见的还应依据行业/领域定级指导意见)，在综合分析的基础上将单位内运行的等级保护对象进行合理分解，确定所包含的定级对象及其个数。

参与角色：运营、使用单位，网络安全服务机构。

活动输入：行业/领域定级指导意见，行业/领域定级工作部署文件，等级保护对象总体描述文件，GB/T 22240。

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

为了突出重点保护的等级保护原则，运营、使用单位应对大型等级保护对象进行划分，划分的方法

[illegible]

b) [illegible]

[illegible]

物联网主要包括感知、网络传输和处理应用等特征要素，应将以上要素作为一个整体对象定级，各要素不单独定级。

对于工业控制系统，其一般包含现场采集/执行、现场控制、过程控制和生产管理等特征要素。其中，现场采集/执行、现场控制、过程控制等要素应作为一个整体对象定级，各要素不单独定级；生产管理要素宜单独定级。对于大型工业控制系统，可以根据系统功能、责任主体、控制对象和生产厂商等因素

[redacted]

5.4 安全保护等级确定

5.4.1 定级、审核和批准

活动目标：

[redacted]

活动输出：定级结果，主管部门审批意见。

5.4.2 形成定级报告

活动目标：

对定级过程中产生的文档进行整理，形成等级保护对象定级结果报告。

参与角色：主管部门，运营、使用单位。

活动输入：定级对象详细描述文件，定级结果。

活动描述：

对等级保护对象的总体描述文档、详细描述文件、定级结果等内容进行整理，形成文件化的定级结果报告。

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) 定级对象列表；

d) 每个定级对象的概述；

e) 每个定级对象的边界；

f) 每个定级对象的设备部署；

g) 每个定级对象支撑的业务应用；

h) 定级对象列表、安全保护等级以及保护要求组合；

i) 其他内容。

活动输出：安全保护等级定级报告。

5.5 定级结果备案

活动目标：

明确等级保护管理部门对备案的要求，整理相关备案材料，递交受理备案的单位提交备案材料。

参与角色：主管部门，运营、使用单位，等级保护管理部门。

活动输入：定级报告，主管部门审核意见，等级保护对象安全总体方案，安全详细设计方案，安全等级测评报告，第三级及以上等级系统需要提供。

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

运营、使用单位在等级保护对象建设之初根据其将要承载的业务信息及系统服务的重要性确定等级保护对象的安全保护等级，并针对备案材料的要求，整理、填写备案材料。

b) 备案材料提交

根据等级保护管理部门的要求办理定级备案手续，提交备案材料（新建等级保护对象可在等级测评实施完毕补充提交等级测评报告）。等级保护管理部门接收备案材料，出具备案证明。

活动输出：备案材料，备案证明。

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等级保护对象的划分情况、等级保护对象的定级情况、等级保护对象承载业务情况，通过分析明确等级保护对象安全需求，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，以指导后续的等级保护对象安全建设工程实施。

总体安全规划阶段的工作流程见图3。

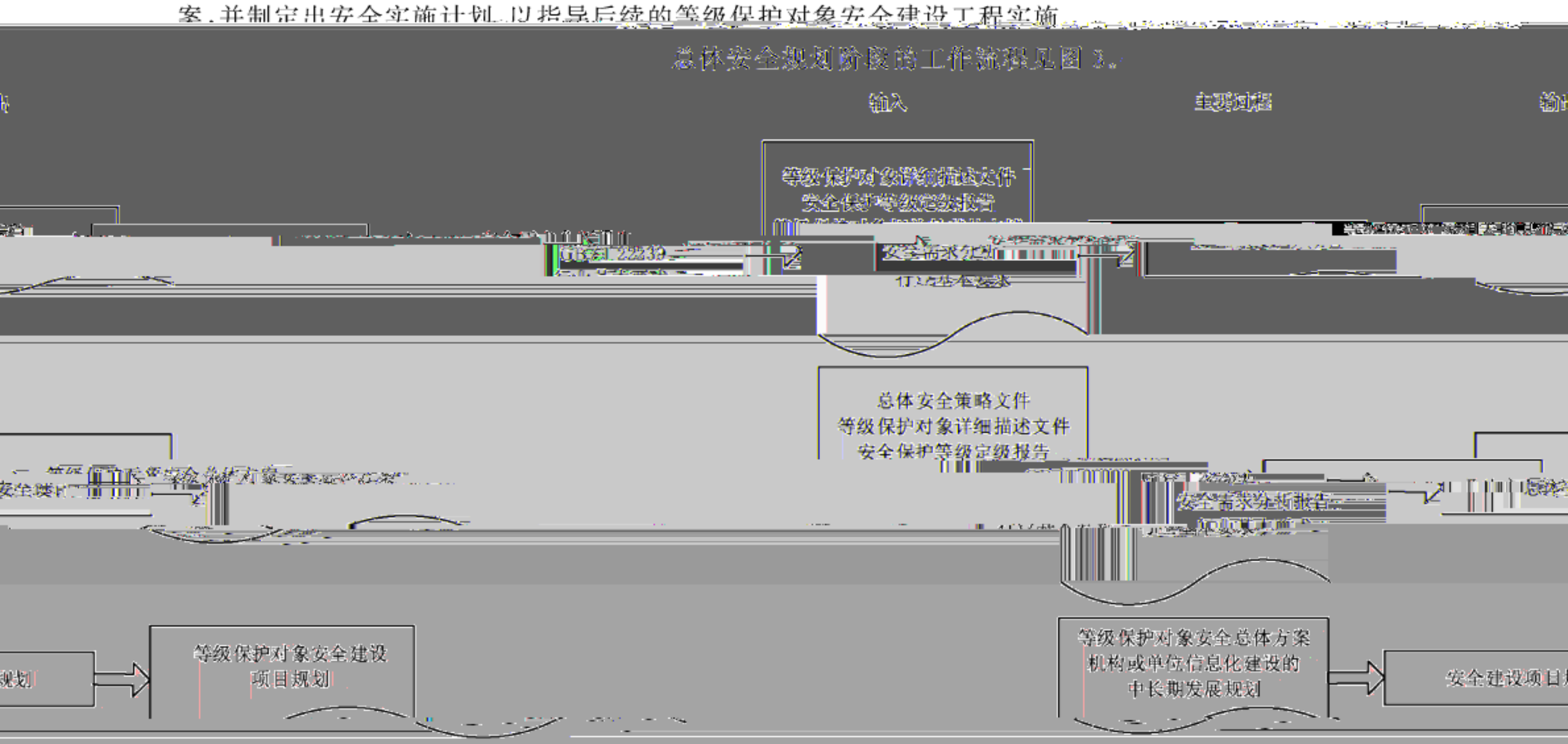


图3 总体安全规划阶段工作流程

6.2 安全需求分析

6.2.1 基本安全需求的确定

活动目标：

根据等级保护对象的安全保护等级，提出等级保护对象的基本安全保护需求。

参与角色：运营、使用单位，网络安全服务机构。

活动输入：等级保护对象详细描述文件，安全保护等级定级报告，等级保护对象相关的其他文档，GB/T 22239，行业基本要求。

活动描述：

本活动主要包括以下子活动内容：

a) 确定等级保护对象范围和分析对象

明确不同等级的等级保护对象的范围和边界，通过调查或查阅资料的方式，了解等级保护对象的业务应用、业务流程等情况。

b) 形成基本安全需求

根据各个等级保护对象的安全保护等级从GB/T 22239、行业基本要求中选择相应等级的要求，形成等级保护对象的基本安全需求。对于已开展等级保护测评的对象，应根据等评测结果合理修改需求，形成基本安全需求。

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：

通过分析重要资产的特殊保护要求、受威胁需求分析或风险分析的方法，确定了解等级保护对象实施特殊安全措施的必要性，提出等级保护对象的特殊安全保护需求。

参与角色：运营、使用单位，网络安全服务机构。

活动输入：等级保护对象详细描述文件，安全保护等级定级报告，等级保护对象相关的其他文档。

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） 重要资产分析

明确等级保护对象中的重要部件，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

，分析安全弱点被利用的可

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（包括技术和管理两方面）

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、内部的威胁，威胁

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

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

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：

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：运营、使用单位，网络安全服务机构。

活动输入：等级保护对象详细描述文件，安全保护等级定级报告，基

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

安全需求分析报告。

安全需求分析报告可以包含以下内容：

a） 等级保护对象描述；

b） 基本安全需求描述；

c） 特殊安全需求描述。

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：

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，定义网络安全的总体目标，规定网络安全责任机构和职责，建立安全工作运行模式等。

b） 确定安全策略

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 [illegible]

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：

[illegible]

分等级保护的具体实现。

[illegible]

报告、GB/T 22239、行业基本要求。

活动描述：

本活动主要包括以下子活动内容：

a） 设计安全技术体系架构

[illegible]

等级保护对象的安全技术体系架构见图4。

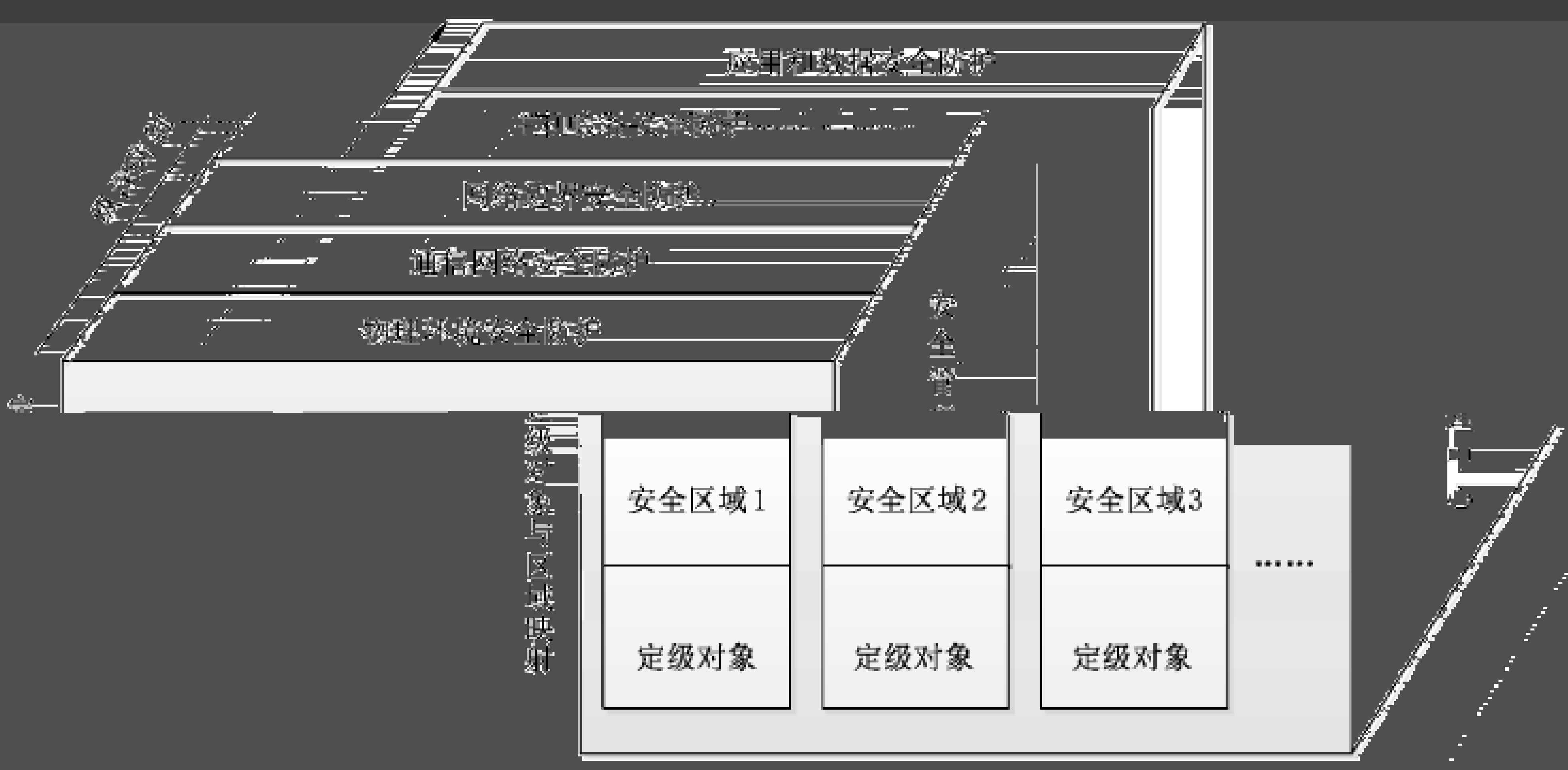


图4 等级保护对象的安全技术体系架构

b) 规定不同级别定级对象物理环境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，提出不同级别定级对象物理环境的安全保护策略和安全技术措施。定级对象物理环境安全保护策略和安全技术措施提出时应考虑不同级别的定级对象共享物理环境的情况，如果不同级别的定级对象共享同一物理环境，物理环境的安全保护策略和安全技术措施应满足最高级别定级对象的等级保护基本要求。

c) 规定通信网络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，提出通信网络的安全保护策略和安全技术措施。[illegible]

[illegible]

[illegible]

[illegible]

h) 形成等级保护对象安全技术体系结构

将骨干网或城域网、通过骨干网或城域网的定级对象互联、局域网内部的定级对象互联[illegible]

[illegible]

活动输出：等级保护对象安全技术体系结构。

6.3.3 整体安全管理体系结构设计

活动目标：

根据等级保护基本要求系列标准、行业基本要求、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的定级对象制定统一的安全管理策略，又从每个定级对象的实际需求出发，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：运营、使用单位，网络安全服务机构。

[illegible]

活动描述：

本活动主要包括以下子活动内容：

a） 设计等级保护对象的安全管理体系框架

根据等级保护基本要求系列标准、行业基本要求、安全需求分析报告等，设计等级保护对象安全管理体系框架。等级保护对象安全管理体系框架分为四层。第一层为总体方针、安全策略，通过网络安全总体方针、安全策略明确机构网络安全工作的总体目标、范围、原则等。第二层为网络安全管理制度，通过对网络安全活动中的各类内容建立管理制度，约束网络安全相关行为。第三层为安全技术标准、操作规程，通过对管理人员或操作人员执行的日常管理行为建立操作规程，就落网络安全管理制度的具体技

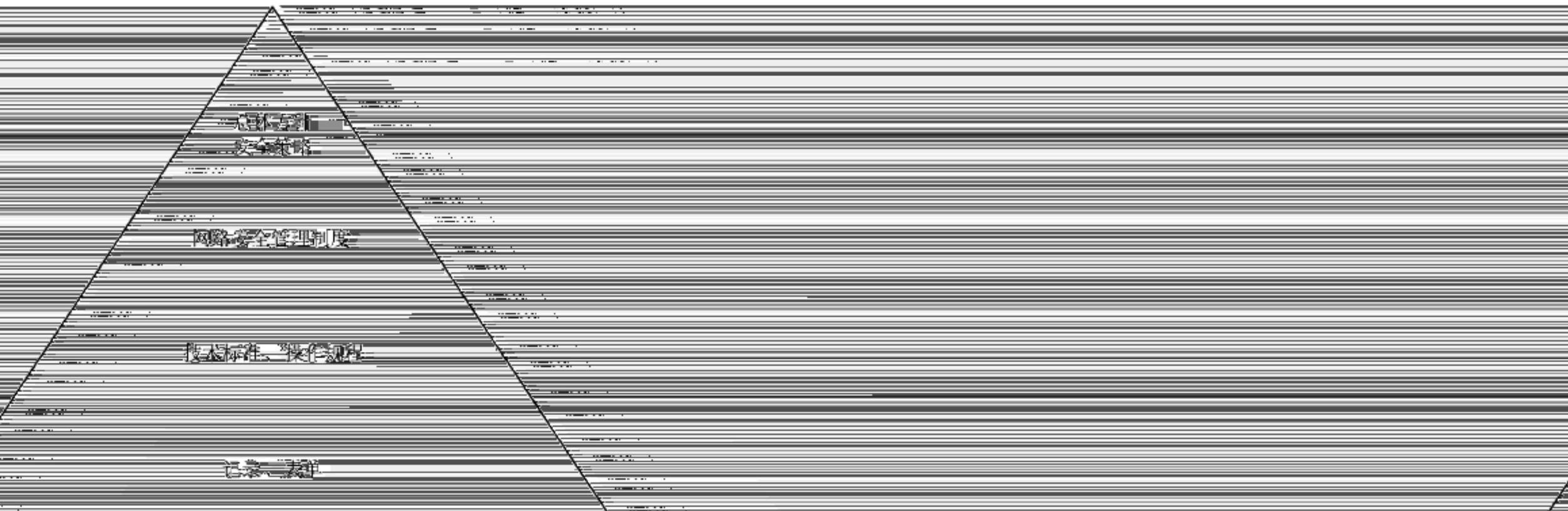


图5 等级保护对象的安全管理体系框架

识管理体系和对不同级别定级对象的安全管理职责

文件、等级保护基本要求系列标准、行业基本要求和安全需求，提出机构的

定级对象的人员安全管理策略

b） 规定网络安全的组

根据机构总体安全策略

略等。

c） 规定不同级别

个管理策略等。

d） 规定不同级别定级对象机房及办公区等物理环境的

全管理策略

根据机构总体安全策略文件、等级保护基本要求系列标准、行

同级别定级对象的安全运行与维护框架和运维安全策略等。

g) 规定不同级别定级对象安全事件外置和应急管理策略

求系列标准、行业标准要求安全需求，提出各个不

等。

档化

计工作的结果文档化，最后形成一套指导机构网络安全工作的指导性文件。

、使用单位，网络安全服务机构。

需求分析报告，等级保护对象安全技术体系结构，等级保护对象安全管理体系结构。

析报告、等级保护对象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

安全方案。

总体安全方案包含以下内容：

对象概述；

策略；

对象安全技术体系结构；

对象安全管理体系结构；

保护对象安全总体方案。

规划

标确定

对象安全总体方案(一个或多个文件构成)、单位信息化建设的中长期发展规划和机

况确定各个时期的安全建设目标。

、使用单位，网络安全服务机构。

保护对象安全总体方案、机构或单位信息化建设的中长期发展规划。

包括以下子活动内容：

6.3.4 设计结果文档

活动目标：

将总体安全设计

参与角色：运营

活动输入：安全

活动描述：

对安全需求分析

等级保护对象总体安

a)

b) 总体安全策

c)

d)

活动输出：等级

6.4 安全建设项目规

6.4.1 安全建设目标确

活动目标：

依据等级保护对

构的安全建设资金状

参与角色：运营

活动输入：等级

本活动主要

6.4.2 安全建设内容规划

活动目标：

根据安全建设目标和等级保护对象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：运营、使用单位，网络安全服务机构。

活动输入：等级保护对象安全总体方案，等级保护对象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

根据等级保护对象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为但不限于以下内容：

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

将安全建设内容组合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；[illegible]

活动输出：安全建设项目列表（含安全建设内容）。

6.4.3 形成安全建设项目规划

活动目标：

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，形成安全建设项目规划。

参与角色：运营、使用单位，网络安全服务机构。

活动输入：等级保护对象安全总体方案，等级保护对象分阶段安全建设目标，安全建设内容等。

活动描述：

对等级保护对象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，形成等级保护对象安全建设项目规划。

安全建设项目规划包括但不限于以下内容：

a) 规划建设的依据和原则；
b) 规划建设的目标和范围；
c) 等级保护对象安全现状；
d) 信息化的中长期发展规划；
e) 等级保护对象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、检测及运维估算等内容；
i) 等级保护对象安全建设的实施保障等内容。

活动输出：等级保护对象安全建设项目规划。

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等级保护对象安全总体方案的要求，结合等级保护对象安全建设项目规划，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6。

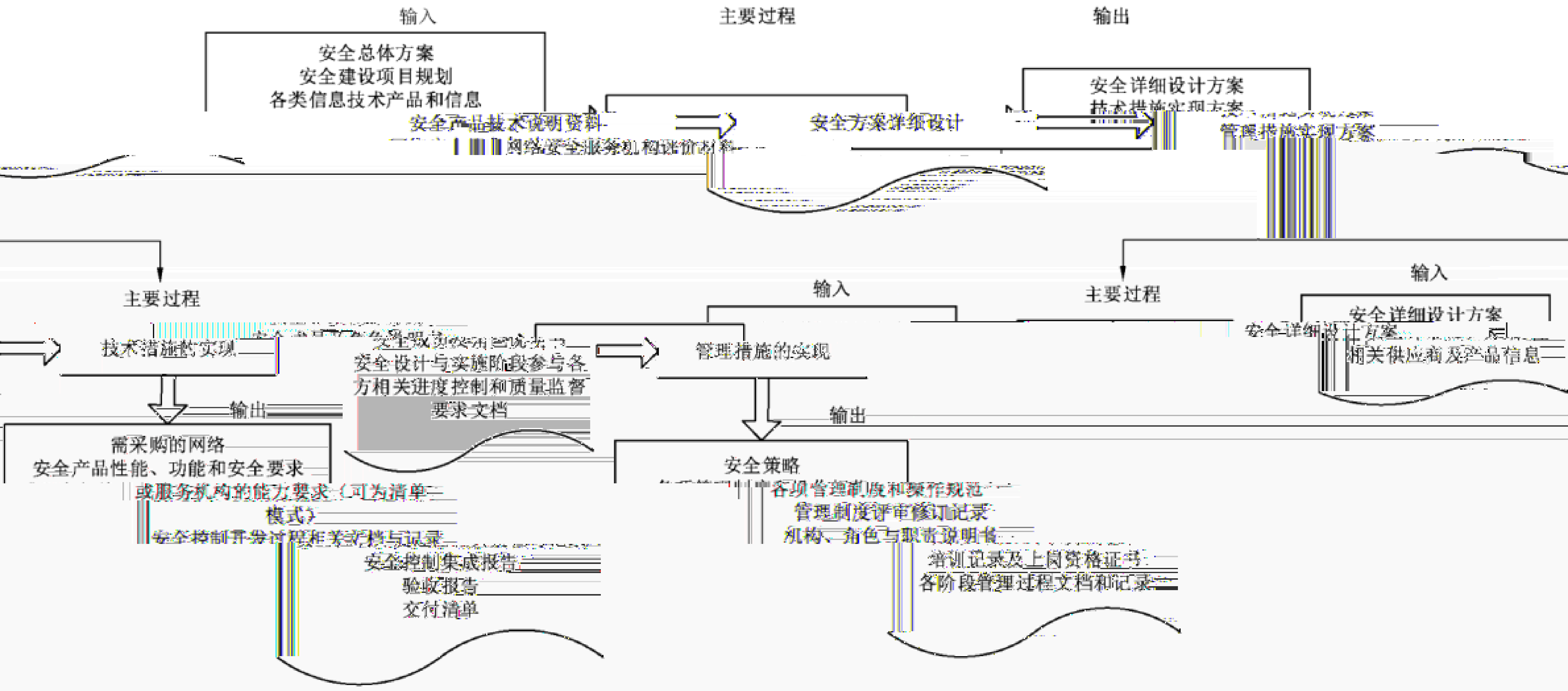


图6 安全设计与实施阶段工作流程

7.2 安全方案详细设计

7.2.1 技术措施实现内容的设计

活动目标：

根据建设目标和建设内容将等级保护对象安全总体方案中要求实现的安全策略、安全技术体系[illegible]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，使得在网络安全产品采购和安全控制的开发阶段具有依据。

参与角色：运营、使用单位，网络安全服务机构，网络安全产品供应商。

活动输入：安全总体方案，安全建设项目规划，各类信息技术产品和网络安全产品技术说明资料、网络安全服务机构评价材料。

活动描述：

本活动主要包括以下子活动内容：

a) 结构框架的设计

依据本次实施项目的建设内容和等级保护对象的实际情况，给出与总体安全规划阶段的安全策略、[illegible]结构、[illegible]网络安全产品的使用、网络子域划分、IP地址规划、云计算模式的选取（如有）、移动互联的接入方式（如有）等。

b） 安全功能要求的设计

对安全实现技术框架中使用到的相关网络安全产品，如防火墙、VPN、网闸、认证网关、代理服务器、网络防病毒、PKI、云安全防护产品、移动终端应用软件与防护产品等提出安全功能指标要求。对需要开发的安全控制组件，提出安全功能指标要求。

c） 部署方案的设计

结合目前等级保护对象网络拓扑，以图示的方式给出安全技术实现框架的实现方式，包括网络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。

d） 制定安全策略的实现计划

依据等级保护对象安全总体方案中提出的安全策略要求，制定设备和设备网络安全技术安全

制定安全管理机构和人员的配备安全建设过程管理等。

活动输出：管理措施实施方案。

7.2.3 设计结果的文档化

活动目标：

将技术措施实施方案、管理措施实施方案汇总，同时考虑工时和成本，最后形成指导安全实施的指导性文件。

参与角色：运营、使用单位，网络安全服务机构。

活动输入：技术措施实施方案，管理措施实施方案。

活动描述：

对技术措施实施方案和管理措施实施方案等文档进行编辑整理，形成等级保护对象安全建设详细设计方案。

详细设计方案应包括：

a） 建设目标和建设内容；

b） 技术实现方案；

c） 网络安全产品或组件安全功能及性能要求；

d） 网络安全产品或组件部署；

e） 安全控制策略和配置；

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 技术措施的实现

7.3.1 网络安全产品或服务采购

活动目标：

按照安全详细设计方案中对于产品或服务的具体指标要求进行采购，根据产品、产品组合或服务实现的功能、性能和安全性满足安全设计要求的情况来选购所需的网络安全产品或服务。

参与角色：网络安全产品供应商，网络安全服务机构，运营、使用单位，测试机构。

活动输入：安全详细设计方案，相关供应商及产品信息。

活动描述：

本活动主要包括以下子活动内容：

a） 制定产品或服务采购说明书

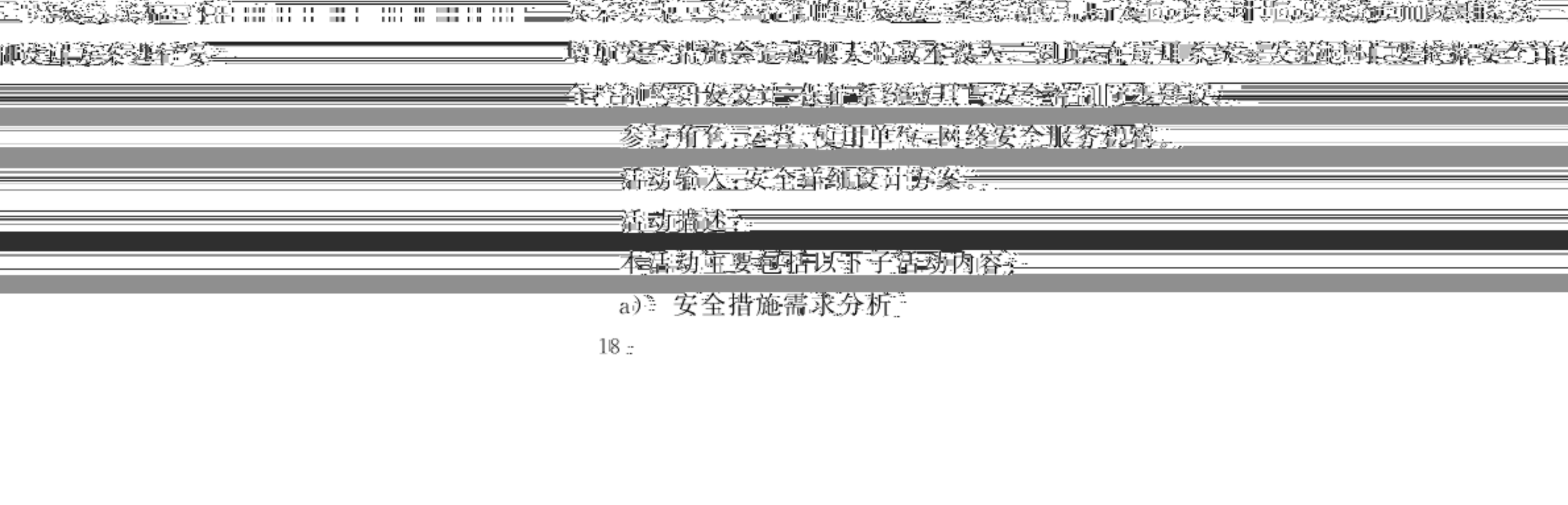
网络安全产品或服务选型过程首先依据安全详细设计方案的设计要求，制定产品或服务采购说明

控制的开发

7.3.2 安全

示：

些不能通过采购现有网络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



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

[illegible]

d) 编码实现

[illegible]

e) 测试

[illegible]

3) 安全控制的开发过程[illegible]理文档；

活动输出：安全控制开发过程相关文档与记录。

7.3.3 安全控制集成

活动目标：

将不同的软硬件产品进行集成，依据安全详细设计方案，将网络安全产品、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可以运营、使用单位与网络安全服务机构共同参与，相互配合，把安全实施、风险控制、质量控制等有机结合起来，实现安全态势[illegible]

参与角色：运营、使用单位，网络安全服务机构。

活动输入：安全详细设计方案[illegible]

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给出工程的建设内容、方法和规范[illegible]

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[illegible]

地指导系统实施过程。该质量控制方案应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[illegible]

c) 集成实施

主要工作内容是将配置好策略的网络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[illegible]质量[illegible]问题。

d) [illegible]

等级保护对象建设完成后，安全服务[illegible]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。

7.3.4 系统验收

活动目标：

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、性能和安全性。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[illegible]。

参与角色：[illegible]网络安全服务机构，测试机构。

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

安全控制的开发、集成完成后，要根据安全设计方案中需要达到的安全目标，准备验收方案。验收[illegible]

b) [illegible]

由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等级保护对象进行验收测试。验收测试[illegible]功能、性能和安全性进行测试。其中功能测试[illegible]可靠性、易用性[illegible]性能测试[illegible]安全性测试[illegible]网络的安全[illegible]验证。

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等。如果[illegible]文档。

d) 系统交付

在等级保护对象验收通过以后，要进行等级保护对象的交付，需要安全服务机构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：验收报告、交付清单。

实与等级保护对象安全管理相配套的、包
阶段和环节所应遵循的行为规范和操作

长户管理、远程访问管理、特殊权限管理、

正各项管理工作的规范性。

审记录。根据实际环境和情况的变化，对
操作规程、安全运维记录和表单四层体系
修订记录。
评审修订记录。

、人员的分工和岗位培训以及各种资源的

7.4 管理措施的实现

7.4.1 安全管理制度的建设和修订

活动目标：

依据国家网络安全相关政策、标准、规范，制定、修订并落实
括等级保护对象的建设、开发、运行、维护、升级和改造等各个阶
规程。

参与角色：运营、使用单位，网络安全服务机构。

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） 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
设备管理、变更管理、资源管理等方面。

b） 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约束，来保证

c） 评估与完善

制度在发布、执行过程中，要定期进行评估，保留评估或评
制度进行修改和完善，规范总体安全方针、安全管理制度、安全
文件的一致性，必要时考虑管理制度的重新制定，并保留版本修

活动输出：安全策略、各项管理制度和操作规范、管理制度

7.4.2 安全管理机构和人员的设置

活动目标：

建立配套的安全管理职能部门，通过管理机构的岗位设置

7.4.3 安全实施过程管理

活动目标：

在等级保护对象定级、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：运营、使用单位，网络安全服务机构，网络安全产品供应商。

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。

本活动主要包括以下子活动内容：

a) 整体管理

整体管理需要在等级保护对象建设的整个生命周期内，围绕等级保护对象安全级别的确定、整体计划制定、执行和控制，通过资源的整合，协调等级保护对象建设过程中所有的组成要素在恰当的时间、正确的位置，保证各要素以适度成本、质量和资源管理上协调。

b) 质量管理

在创建等级保护对象的过程中，要建立一个不断测试和改进质量的过程，在整个等级保护对象的生命周期中，通过测量、分析和修正活动，保证所完成目标和过程的质量。

c) 风险管理

为了识别、评估和减低风险，以保证工程活动和全部技术工作项目均得到成功实施。在整个等级保护对象建设过程中，风险管理要贯穿始终。

d) 变更管理

[illegible]

e) 进度管理

等级保护对象建设的实施必须要有一个明确的时间表和一个可行的计划，计划中应明确等级保护对象建设的各个环节、各个项目的起始时间和预期完成时间，保证各个项目的如期完成。

f) 文档管理

文档是记录项目整个过程的书面资料，在等级保护对象建设的过程中，每个环节都有大量的文档输出，文档管理贯穿等级保护对象建设的各个环节，主要包括系统定级、规划设计、方案设计、安全实施过程中确保等级保护对象正常运行的必要环节，涉及的内容较多，[illegible]

[illegible]

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等级保护对象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、安全自查和持续改进、服务商管理和监控、等级测评以及监督检查等过程，安全运行与维护阶段的主要过程见图7。

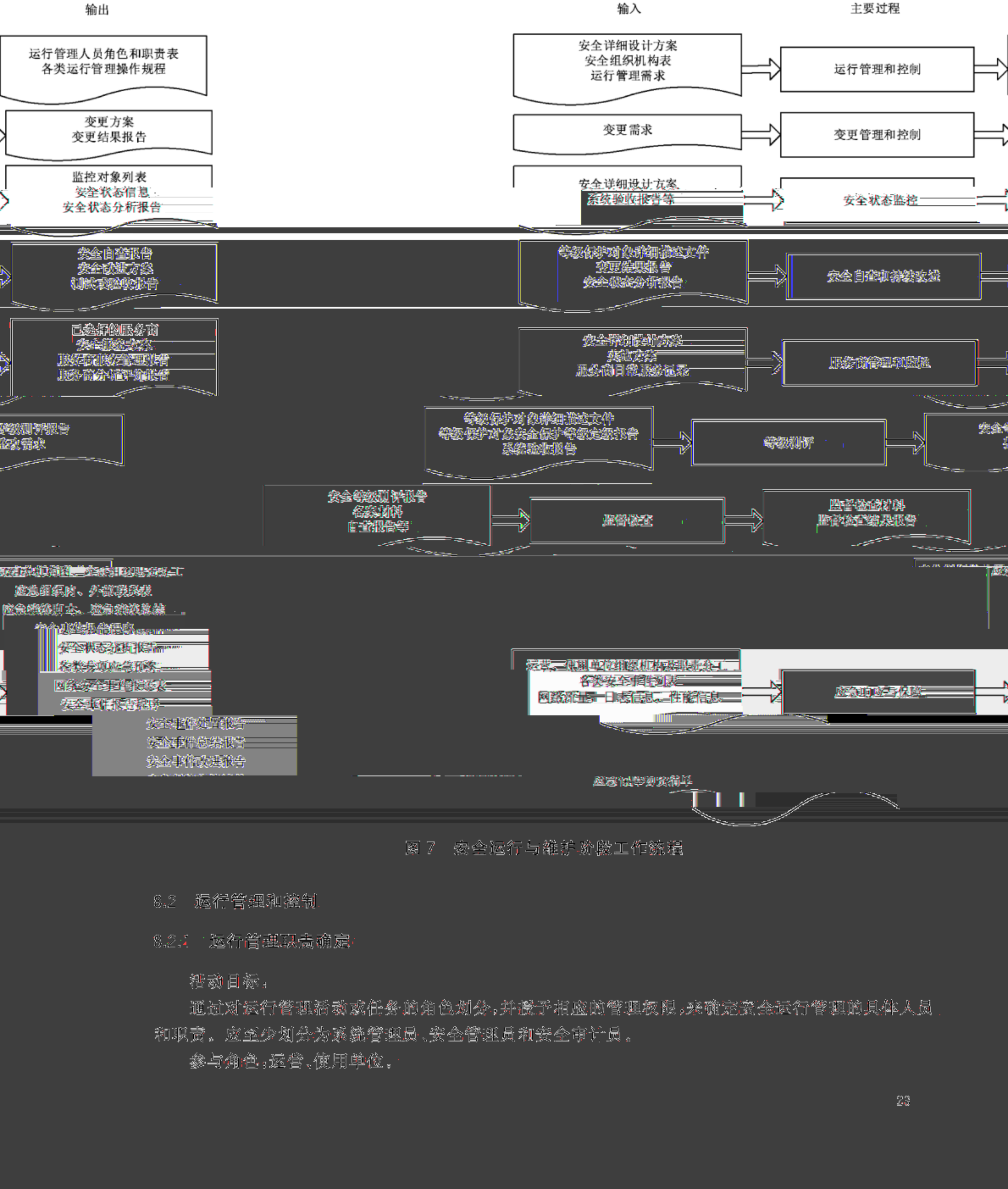


图7 安全运行与维护阶段工作流程

8.2 运行管理和控制

8.2.1 运行管理职责确定

活动目标：

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。应至少划分为系统管理员、安全管理员和安全审计员。

参与角色：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及用户，并由系统管理员创建角色及用户。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

[illegible]限。安全保护等级越高的系统管理权限的划分越细。

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，分析所需要的运行管理控制内容，并以此定义不同运行管理角色的职责。由安全审计员对系统管理员、安全管理员操作日志进行审计。

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：

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[illegible]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：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。操作规程应至少覆盖运维人员、使用用户等的各类操作，[illegible]、移动介质使用规程、终端使用规程、数[illegible]

[illegible]

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，[illegible]时间和人员、正常或异常等情况。

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：

通过对运行与维护过程中的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。

[illegible]

参与角色：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

[illegible]

更的必要性和可行性。

b) 变更影响分析

对运行与维护过程中的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、确定进行变更的先决条件和后续活动等。

c) 明确变更的类别

如果是由等级保护对象类型发生变化、承载的信息 [illegible] 确定等级保护对象是局部调整还是重大变更。如 [illegible]

[illegible]

活动输出:变更方案。

8.3.2 变更过程控制

活动目标:

确保运行与维护过程中的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: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:

确定可能会对等级保护对象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: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 [illegible]

[illegible]

b） 形成监控对象列表

[illegible]控对象列表。[illegible]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[illegible]

[illegible]

8.4.2 监控对象状态信息收集

活动目标：

全状态 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，对等级保护对象的安进行监控。

参与角色：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

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

者是两 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

[illegible]

[illegible]

b） 状态信息收集

[illegible]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 [illegible]收集关于监控对象的

[illegible]和法律法规的要求信息。 [illegible]来自外部环境的安全标准

[illegible]信息。 [illegible]活动输出：安全状态

报告

8.4.3 监控状态分析和报

活动目标：

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：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。

[illegible]活动输出：安全状态分析报告 [illegible]

8.5 安全自查和持续改进

8.5.1 安全状态自查

活动目标：

通过对等级保护对象的安全状态进行自查，为等级保护对象的持续改进过程提供依据和建议，确保等级保护对象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8.8。

参与角色：运营、使用单位。

活动输入：等级保护对象详细描述文件，变更结果报告，安全状态分析报告。

活动描述：

[illegible]

对象和自查方法

象和方法，确定本次安全自查的范围及安全自查工具、调研表格等。

的复审检查方案

的角色和职责，确定自查工作的方法、成立安全自查工作组、制定安全自查工作计划。

[illegible]

查实施。

[illegible]

全工作结果和记录。

[illegible]

8.5.2 改进方案制定

活动目标：

依据安全检查的结果，调整等级保护对象的安全状态，保证等级保护对象安全防护的有效性。

参与角色：运营、使用单位。

活动输入：安全自查报告。

[illegible]

本活动主要包括以下活动内容：

a) 安全改进的立项

[illegible]

b) 制定安全改进方案

[illegible]

8.5.3 安全改进实施

活动目标：

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措施一致有效地工作。

参与角色：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 7.4.3。

b） 安全措施测试与验收

见 7.5.3。

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。

8.6 服务商管理和监控

8.6.1 服务商选择

活动目标：

确定符合国家规定或行业规定的设计、测评、建设资质的服务商，为后续的管理和监控奠定基础。

参与角色：运营、使用单位，网络安全服务机构。

活动输入：安全详细设计方案，实施方案等。

活动描述：

本活动主要包括以下子活动内容：

a） 服务能力分析

从影响系统、业务安全性等关键要素层面分析服务商服务能力，根据国家招投标相关要求，选择最佳服务商，这些要素可能包括服务商的基本情况、企业资质和人员资质、信誉、技术力量和行业经验、内部控制和管理能力、持续经营状况、服务水平及人员配备情况等。

b） 网络安全风险分析

[illegible]

在选择服务商时，需要识别服务商的网络安全风险，防止高风险、不合格服务商承担安全运行维护工作。项目网络安全风险点包括但不限于以下观点：

——服务商可能的泄密行为；

——服务商服务能力及行业经验；

——物理访问、信息资料丢失、系统越权访问、误操作等；

——服务商企业资质、人员资质及网络安全口碑、业绩；

——服务商以往服务过程案例。

c） 服务内容适用分析

[illegible]络等级保护测评资质等。

活动输出：已选择的服务商，安全服务方案。

8.6.2 服务商管理

活动目标：

[illegible]

参与角色：运营、使用单位，网络安全服务机构。

活动输入：已选择的服务商，安全服务方案。

活动描述：

本活动主要包括以下子活动内容：

a） 人员管理

为确保服务商服务工作符合约定要求，使用单位对服务人员的管理措施应至少包括但不限于：

——使用单位需制定服务商人员管理规定，包含但不限于上岗资质审核机制、保密协议、品行管理、服务技能考核、行为管理、系统权限管理、口令管理等。

——使用单位负责对服务商核心人员的确定和变更进行备案。

[illegible]

8.6.3 服务商监控

活动目标：

[illegible]

e) 服务过程中，服务商如因正当理由需要调整、变更人员的，应提前通知使用单位，做好工作交接，并获得使用单位同意后方可进行。

活动输出：服务商分析评价报告。

8.7 等级测评

活动目标：

通过网络安全等级测评机构对已经完成等级保护建设的等级保护对象定期进行等级测评，确保等级保护对象的安全保护措施符合相应等级的安全要求。

参与角色：主管部门，运营、使用单位，网络安全等级测评机构。

活动输入：等级保护对象详细描述文件，等级保护对象安全保护等级定级报告，系统验收报告。

活动描述：

a) 网络安全等级测评机构依据有关等级保护对象安全保护等级测评的规范或标准对等级保护对

b) 运营、使用单位参考等级测评报告的安全等级测评报告，分

8.8 监督检查

活动目标：

根据等级保护管理部门对等级保护对象定级、规划设计、建设实施和运行管理等过程的监督检查要

参与角色：

活动输入：

活动描述：

等级保护管理部门依据国家网络安

8.9 应急响应与保障

8.9.1 应急准备

活动目标：

建立完善的应急组织体系，保证应急指挥工作反应迅速，协调有序，通过分析安全事

有效验证网络安全应急

系统完整性，应急预案的

从而有助于提高整体

参与角色：主管部门

活动输入：运营、使

活动描述：

本活动主要包括以

a) 建立应急组织

按照应急救援的需要，建立应急组织。应急组织一般分为五个核心应急功能机构，即指挥、行动、策划、后勤和财务。

b) 明确应急工作职责

[illegible]员、职责和权限。

c) 安全事件分类分级

参考《国家网络安全事件应急预案》和 GB/Z 20986—2007，根据安全事件的类型、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，对等级保护对象可能发生的安全事件进行分类分级，针对不同类别和等级制定相应的安全事件报告程序。

d) 确定应急预案对象

针对安全事件的不同类别和等级，考虑其发生的可能性及其对系统和业务产生的影响，确定需制定应急预案的对象。

e) 确定职责和应急协调方式

在统一的应急预案框架下明确应急预案中各部门的职责以及各部门间的合作和分工协调方式。

f) 制定应急预案程序及其执行条件

针对不同等级、不同类别的安全事件制定相应的应急预案程序，确定不同等级、不同类别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。

[illegible]

8.3.2 应急监测与响应

[illegible]

c) 安全事件上报和共享

根据安全状态分析和影响分析的结果，分析可能发生的安全事件，明确安全事件等级、影响程度以及告知对象等，形成安全状态分析报告和网络安全事件报送表，按照安全事件等级以及安全事件报告程序，上报主管部门，并按照规定向相关对象共享安全事件。

d) 安全事件处置

[illegible]

8.9.3 后期评估与改进

活动目标：

对安全事件原因、处置过程进行调查分析，并根据分析结果进行责任认定及制定改进预防措施。

参与角色：运营、使用单位。

活动输入：安全事件报告程序，各类专项应急预案，安全事件处置报告。

活动描述：

本活动主要包括以下子活动内容：

a) 调查评估

对于应急响应过程进行调查，评估应急过程合规性、处置及时性等。通过事件重现调查网络安全事件原因，追溯安全责任，并形成网络安全调查评估报告。

b) 改进预防

根据网络安全事件调查评估报告，制定改进预防措施，修改和完善应急预案，结合实际情况进行落实。开展应急预案培训。

活动输出：安全事件总结报告，安全事件改进报告，应急预案。

8.9.4 应急保障

活动目标：

建立健全应急保障体系，实现应急预案保障工作科学化。

参与角色：运营、使用单位。

活动输入：总体应急预案，各类专项应急预案。

活动描述：

针对各类专项应急预案进行分析，制定应急预案执行所需通信、装备、数据、队伍、交通运输、经费和治安保障内容。

活动输出：应急保障物资清单。

9 定级对象终止

9.1 定级对象终止阶段的工作流程

定级对象终止阶段是等级保护实施过程中的最后环节。当定级对象被转移、终止或废弃时，正确处[illegible]

级对象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定级对象，对于这些定级对象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。

本标准在定级对象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。

定级对象终止阶段的工作流程见图8。

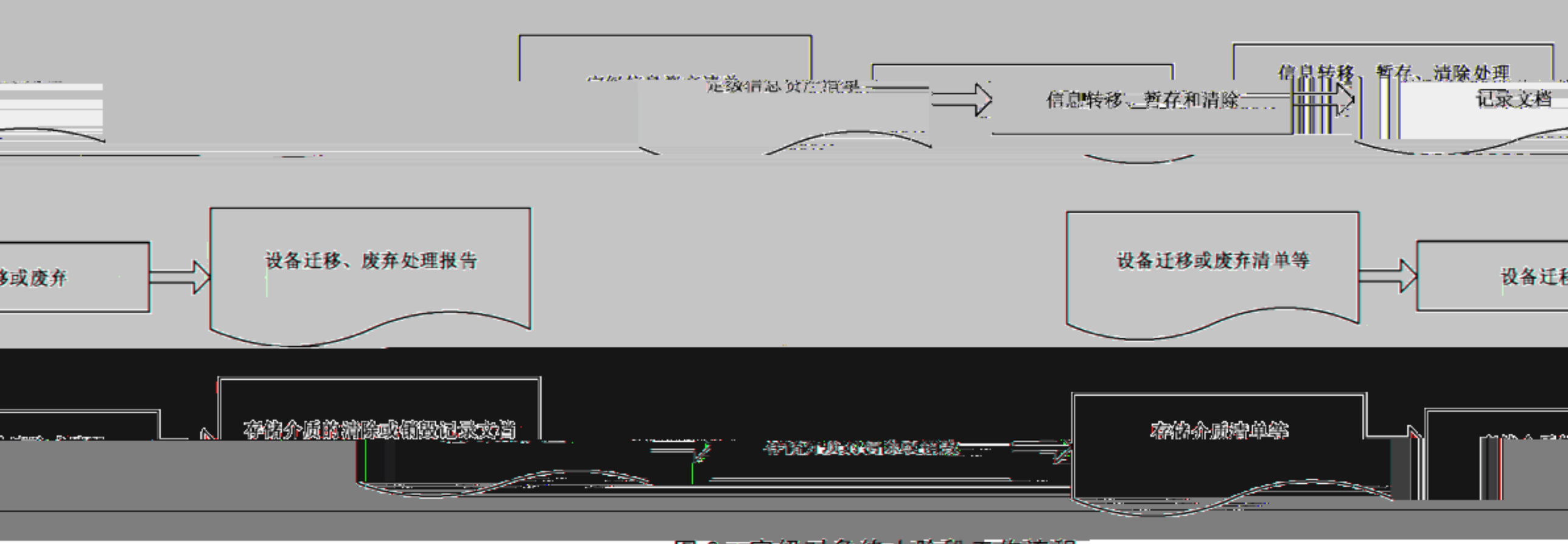


图8 定级对象终止阶段工作流程

9.2 信息转移、暂存和清除

活动目标：

在定级对象终止处理过程中，对于可能会在另外的定级对象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定级对象中的信息。

参与角色：运营、使用单位。

活动输入：定级对象信息资产清单。

活动描述：

本活动主要包括以下子活动内容：

a) 识别重要信息资产、所处的位置以及当前状态等，列出需要转移、暂存和清除的信息资产的清单。

根据要终止的定级对象的信息资产清单，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、清除的过程和结果，形成信息转移、暂存、清除处理记录文档。

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：

确保定级对象终止后，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：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

根据要终止的定级对象的设备清单，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） 确定被迁移设备处理方案

[illegible]

c） 处理方案审批

[illegible]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[illegible]

[illegible]

[illegible]

[illegible]

9.4 存储介质的清除或销毁

活动目标：

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[illegible]

[illegible]

参与角色：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

识别载有重要信息的存储介质、所处的位置以及当前状态

根据要终止的定级对象的存储介质清单，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

对存储介质的处理方式和处理流程。存储介质的处理包[illegible]

根据存储介质所承载信息的敏感程度确定[illegible]

[illegible]

c） 处理方案审批

[illegible]

[illegible]

[illegible]

d） 存储介质处理和记录

[illegible]

[illegible]

活动输出：存储介质清除或销毁记录文档。

附　录　A
（规范性附录）
主要过程及其活动和输入输出

等级保护对象实施网络安全等级保护工作的主要过程及其活动和输入输出见表 A.1。

表 A.1　等级保护对象实施网络安全等级保护工作的主要过程及其活动和输入输出

主要阶段	主要过程	活动	活动输入	活动输出
	行业/领域定级工作		行业介绍文档 GB/T 22240	行业/领域的业务总体描述文件 行业/领域定级指导意见 行业/领域定级工作部署文件
			单位情况说明文档 等级保护对象的立项、建	等级保护对象总体描述

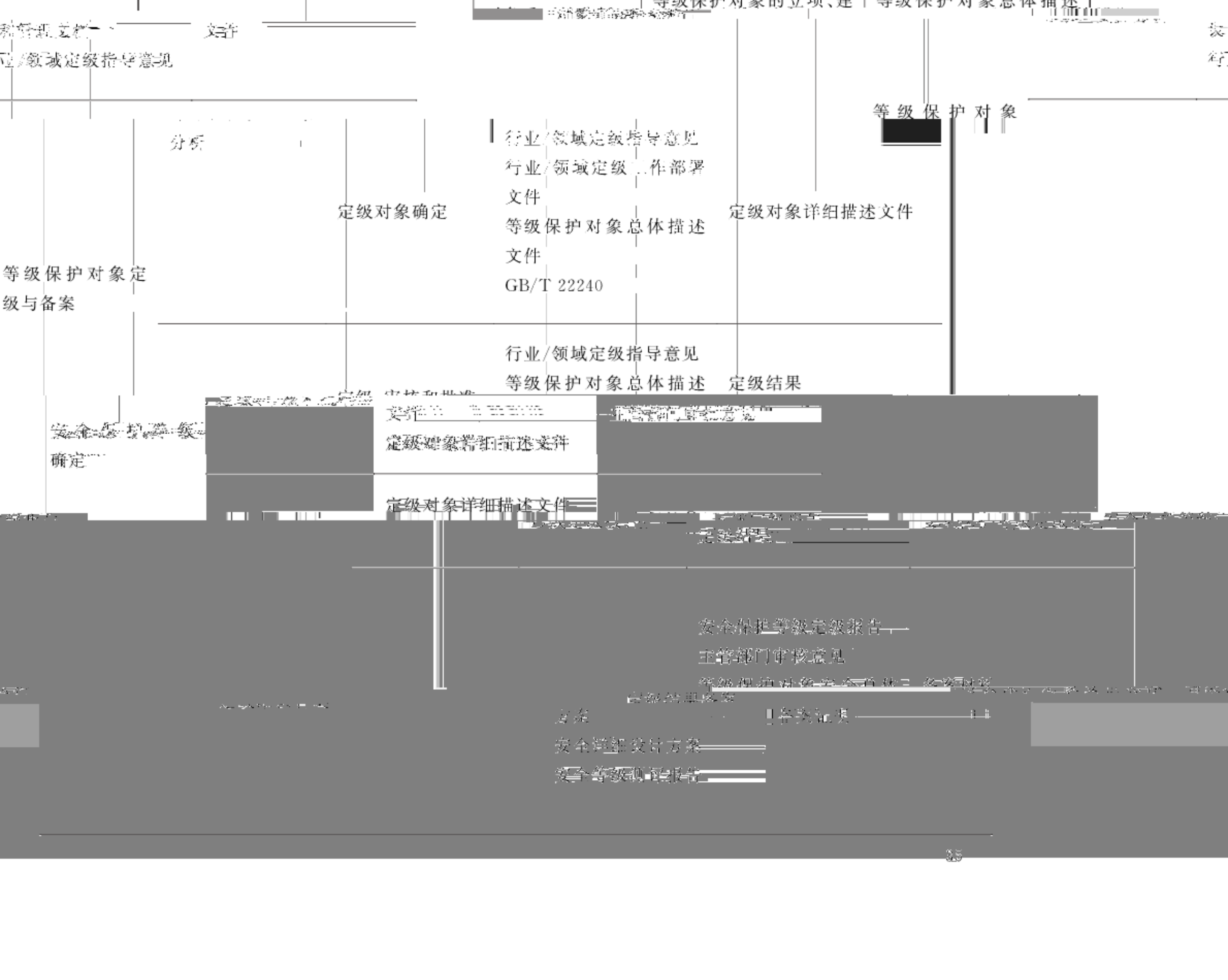


表 A.1（续）

主要阶段	主要过程	活动	活动输入	活动输出
确定				等级保护对象详细描述文件 安全保护等级定级报告
三析	特殊安全需求的确定		基本安全需求的 GB/T 22239 行业基本要求 等级保护对象详细描述文件 安全保护等级定级报告 等级保护对象相关的其他文档	重要资产的特殊保护要求
	形成安全需求分析报告		等级保护对象详细描述文件 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	安全需求分析报告
	总体安全策略设计		等级保护对象详细描述文件 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
	安全技术体系结构设计		总体安全策略文件 等级保护对象详细描述文件 安全保护等级定级报告 安全需求分析报告 GB/T 22239 行业基本要求	等级保护对象安全技术体系结构
设计	整体安全管理体系结构设计		总体安全策略文件 等级保护对象详细描述文件 安全保护等级定级报告 安全需求分析报告 GB/T 22239 行业基本要求	等级保护对象安全管理体系结构
	设计结果文档化		安全需求分析报告 等级保护对象安全技术体系结构 等级保护对象安全管理体系结构	等级保护对象安全总体方案
安全总体设				总体安全规划

表 A.1（续）

主要阶段	主要过程	活动	活动输入	活动输出
		安全建设目标确定	等级保护对象安全总体方案 机构或单位信息化建设的	等级保护对象分阶段安全建设目标
		总体安全规划	安全建设项目规定	形成安全建设项目规划
		安全建设项目规划	等级保护对象安全总体方案 等级保护对象分阶段安全建设目标 安全建设内容等	等级保护对象安全建设项目规划
		安全建设内容规划	等级保护对象安全总体方案 等级保护对象分阶段安全建设目标	安全建设内
				安全总体方案
				安全建设项目规划
				技术措施实现入口
				备类信息技术产品和网络
				技术措施实施
				安全方案详细
				设计
				安全详细设计方案
				安全控制的开
				关文档与记录
				安全控制集成报
				验收报告
				交付清单
				安全策略
				各项管理制度
				规范
				管理制度评审修
				管理措施实现
				管理措施实施
				安全详细设计方案
				安全控制的开发
				安全控制集成
				系统验收
				安全管理制度的建设和修订
				安全管理制度和操作规范
				安全设计与实施阶段参与
				各方相关进度控制和质量
				验收要求文档

表 A.1（续）

主要阶段	主要过程	活动	活动输入	活动输出
	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
	安全自查和持续改进	安全状态自查	等级保护对象详细描述文件 变更结果报告 安全状态分析报告	安全自查报告
		改进方案制定	安全自查报告	安全改进方案
安全运行与维护				

表 A.1（续）

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	应急响应与保障	应急监测与响应	网络流量，日志信息，性能信息等 安全事件报告程序 各类专项应急预案 网络安全事件报送表 安全事件报告程序等	网络安全事件报送表 安全状态分析报告 安全事件处置报告
		后期评估与改进	安全事件报告程序 各类专项应急预案 安全事件处置报告	安全事件总结报告 安全事件改进报告 应急预案
		应急保障	总体应急预案 各类专项应急预案	应急保障物资清单
定级对象终止	信息转移、暂存和清除		定级对象信息资产清单	信息转移、暂存、清除处理记录文档
	设备迁移或废弃		设备迁移或废弃清单等	设备迁移、废弃处理报告
	存储介质的清除或销毁		存储介质清单等	存储介质的清除或销毁记录文档

中华人民共和国
国家标准
信息安全技术
网络安全等级保护实施指南
GB/T 25058—2019
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2019年7月第一版
*
书号:155066·1-63192

GB/T 25058-2019