ICS 35.040
L 80

GB/T 25058—2019
代替 GB/T 25058—2010

信息安全技术

信息安全等级保护实施指南

Information security technology—Implementation guide for classified protection of cybersecurity

2019-08-30发布　　2020-03-01实施

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

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

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

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。

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

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

全保护等级，自行组织实施安全保护。

b) 重点保护原则

c) 动态保护原则

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

角色和职责 4.2

4.3 实施的基本流程

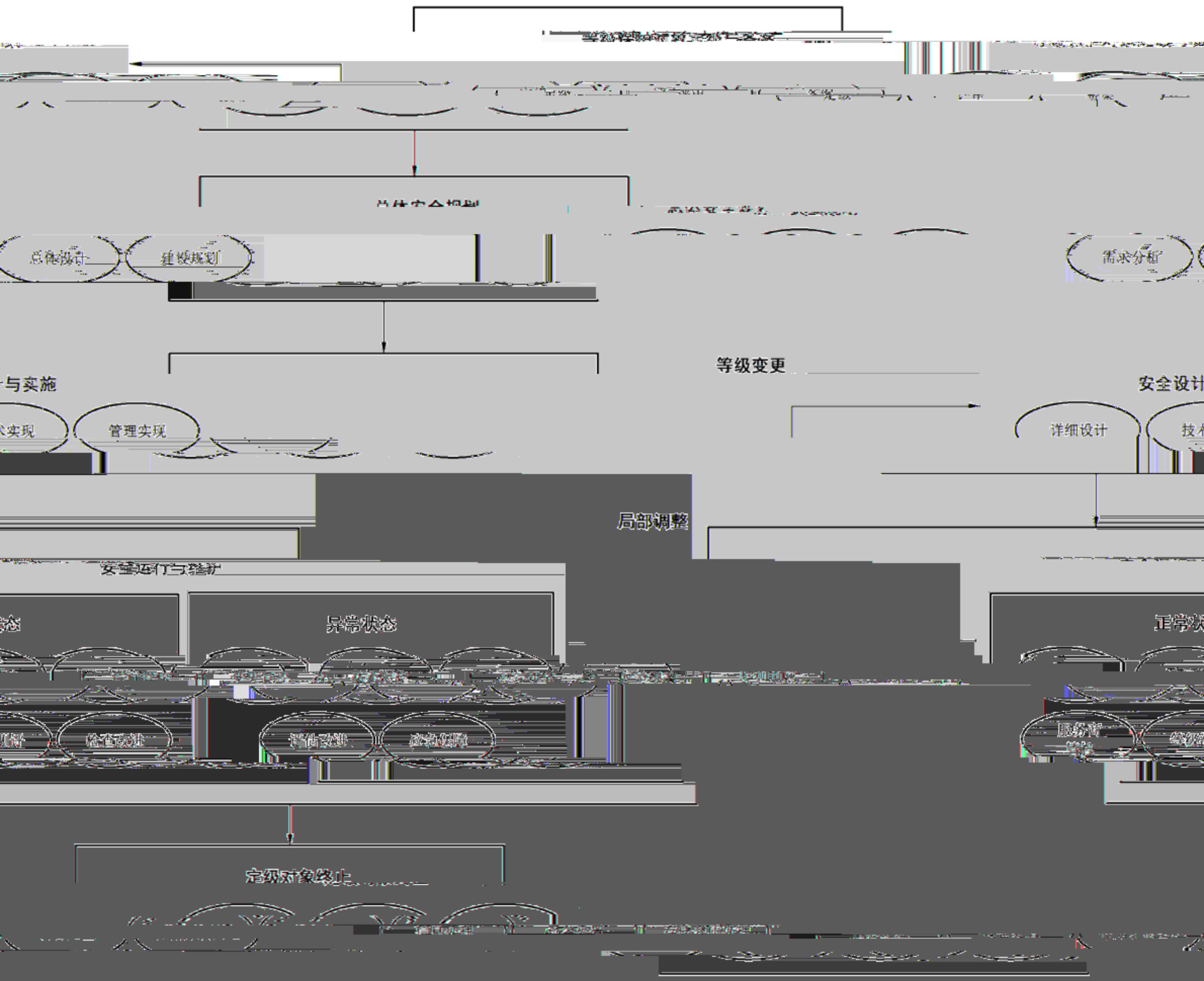


图 1　安全等级保护工作实施的基本流程

实、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，直至满足等级保护的要求。当等级保护对象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级变更过程。

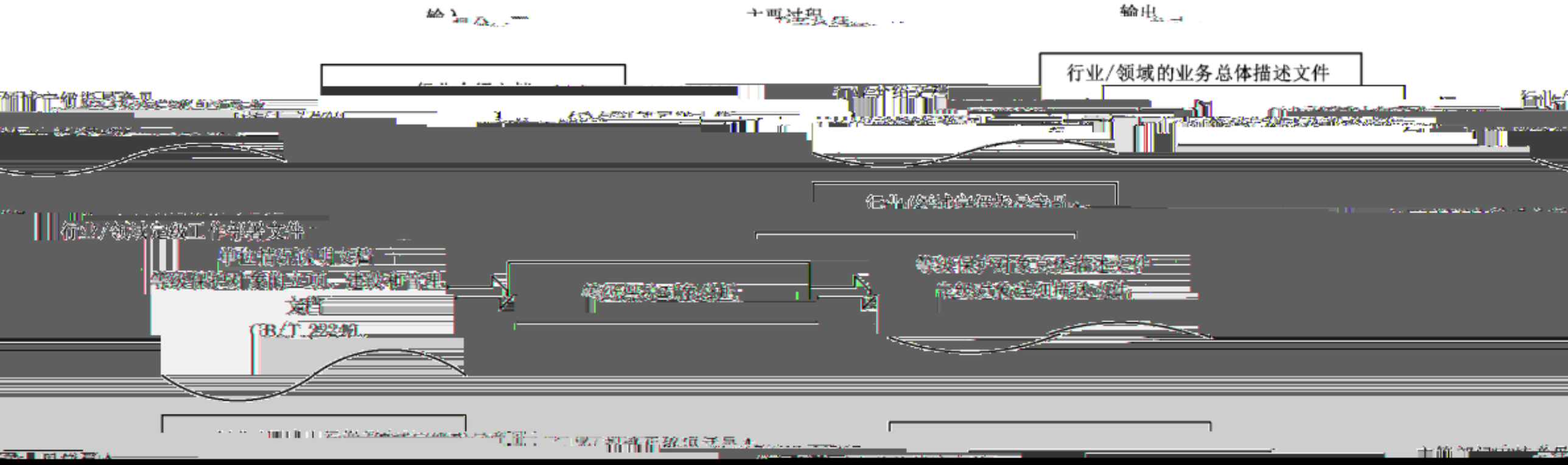
等级保护对象在定级与备案阶段、重大变更过程中，若定级对象等级变化，则在安全运行与维护过程中，发生安全事件时可能会发生应急响应与保障。

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

[redacted]

等级保护对象定级与备案阶段的工作流程见图 2。



主管部门可组织梳理本行业/领域内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

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所依赖的等级保护对象，整理等级保护对象处理的业务及

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，能/职能及作用，确定履行主要社会功能/职能

性程度。

) 识别用户范围和用户类型

g

为二等级保护对象描述

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

等级保护对象概念

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

参与数：

参与部门

方法描述

本活动主要包括以下活动内容：

a) 划分方法的选择

等级保护定级划分可以参考以下方法进行：

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。

[illegible]

c) 定级对象详细描述

在对等级保护对象进行划分并确定定级对象后，应在等级保护对象总体描述文件的基础上，进一步增加定级对象的描述，准确描述一个大型等级保护对象中包括的定级对象的个数。

[illegible]

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：定级对象详细描述文件。

5.4 安全保护等级确定

5.4.1 定级、审核和批准

活动目标：

[illegible]

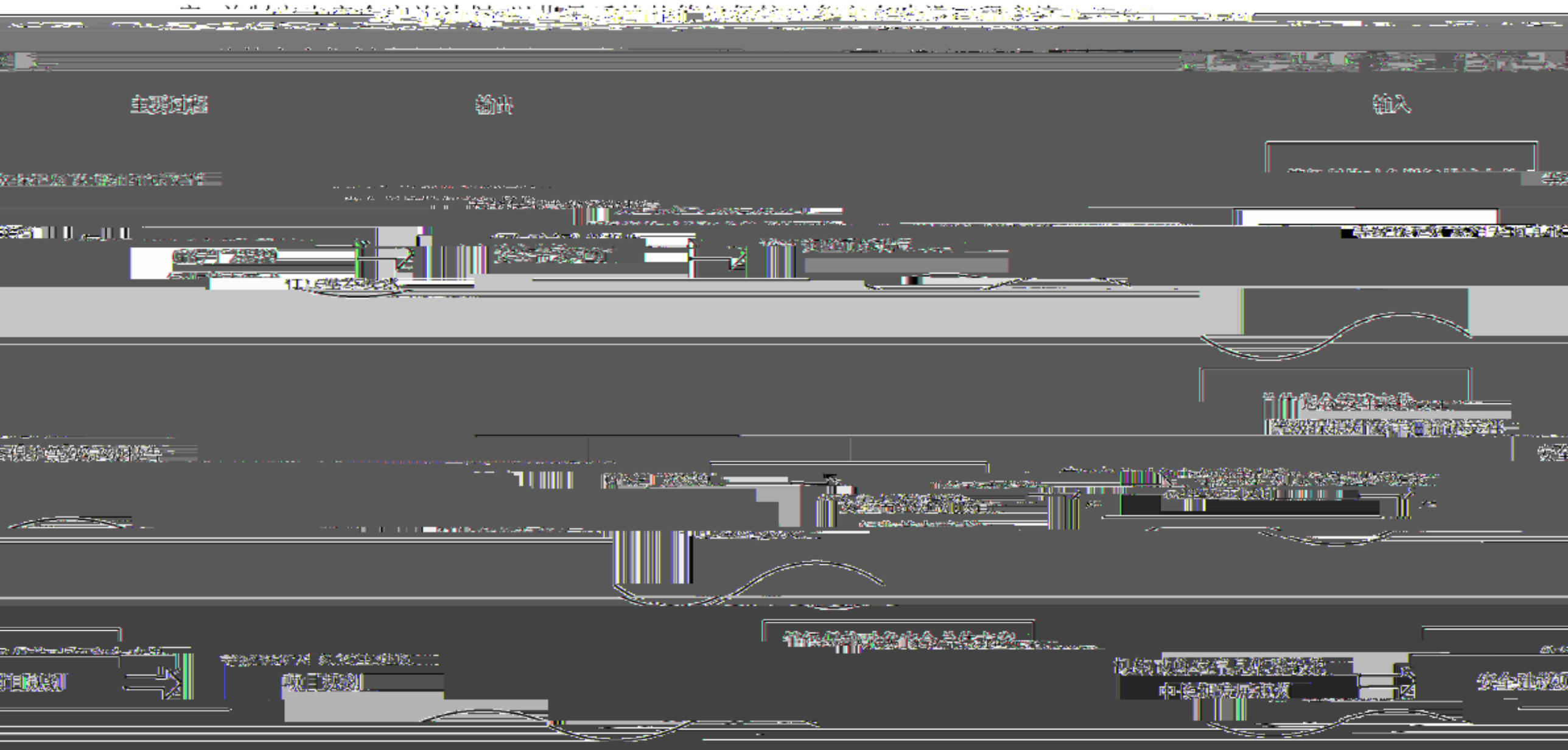
活动输入：[illegible]等级保护对象总体描述文件，定级对象详细描述文件。

[illegible]

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：



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。

活动描述：

本活动主要包括以下子活动内容：

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，包括外部与内部的威胁，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

发生的可能性或概率。

成的损害或影响的大小，以

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

基本安全需求，重要资产的特殊保护要求

活动输入：等级保护对象详细设计文件、安全保护等级定级报告、

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

要求。

活动描述：

本活动主要的子活动是完成安全需求

安全需求分析报告可以包含以

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：

参与角色：运营、使用单位，网络安全服务机构

活动描述：

本活动主要包括以下主要内容：

a)　确定安全方针

[illegible]

5.1　确定安全方针

[illegible]

6.3.2　安全技术体系结构设计

活动目标：

根据 GB/T 22239 《信息安全技术　网络安全等级保护基本要求》、安全需求分析报告、

[illegible]

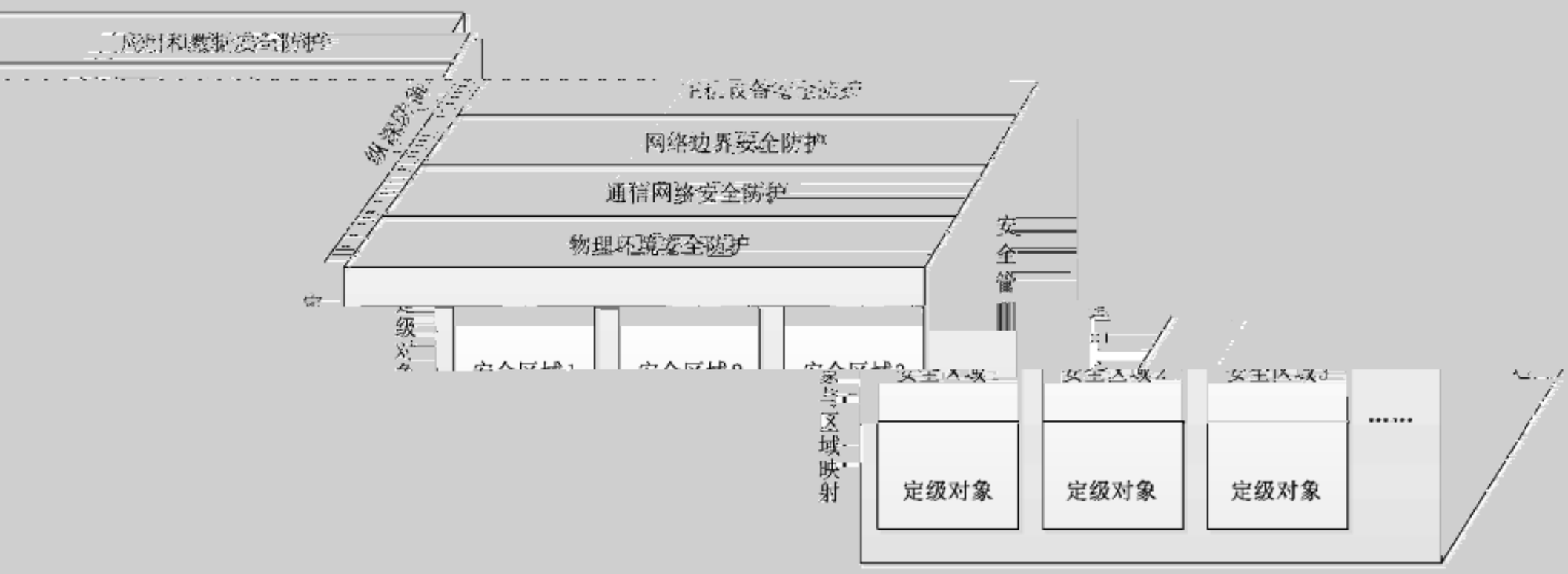


图 A　等级保护对象的安全技术体系架构

b） 规定不同级别定级对象物理环境的安全保护技术措施

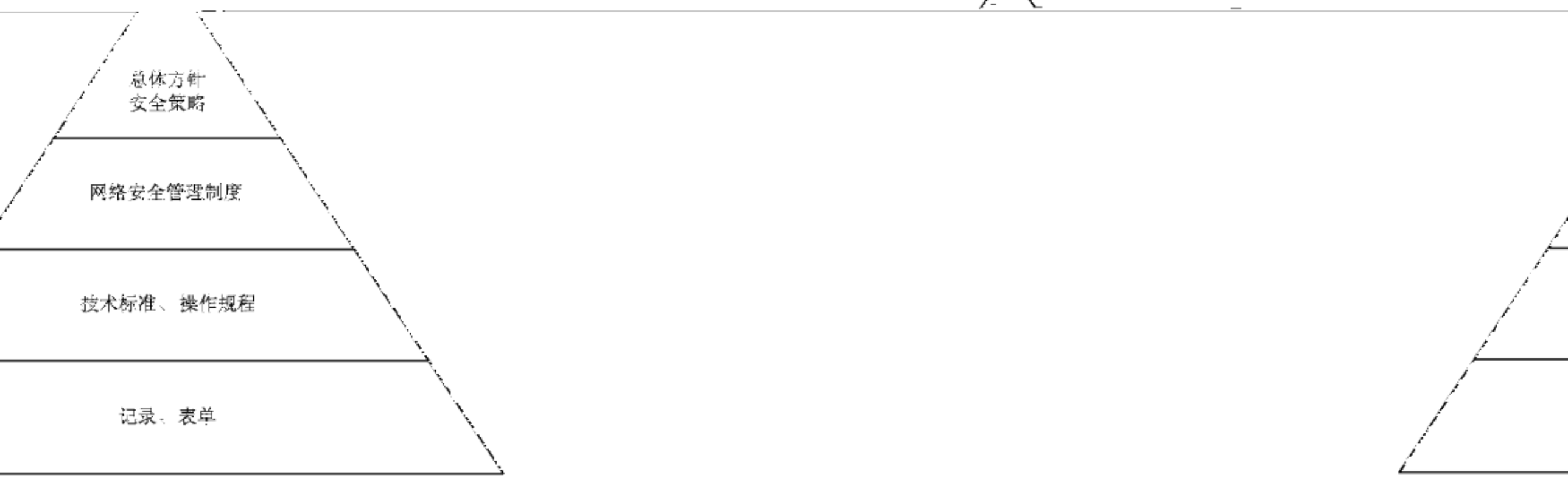
活动描述：

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

[redacted]



等级保护对象的安全管理体系框架

图 5

系和对不同级别定级对象的安全管理职责

b） 规定网络安全的组织管理体

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

根据机构总体安全策略文件、等级

略等。

[redacted]

全管理策略等。

d） 规定不同级别定级对象机房及办公区等物理环境的安全管理策略

g) 规定不同级别定级对象安全事件处置和应急管理策略

[redacted]

6.3.4 设计结果文档化

活动目标：

[redacted]

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：

[redacted]

6.4.2 安全建设内容规划

活动目标：

[redacted]

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 [illegible]

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，[illegible] 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：[illegible]

[illegible]

6.4.3 形成安全建设项目规划

活动目标：[illegible]

[illegible]

活动输入：[illegible]

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。[illegible]

a) 规划建设内容和[illegible]；

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内容规划；

f) 安全技术体系建设规划；

g) 安全管理与安全运维体系建设规划；

[illegible]

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：

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

b） 安全功能要求的设计

7.2.3 设计结果的文档化

活动目标：

a） 建设目标和

b） 技术实现方

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：

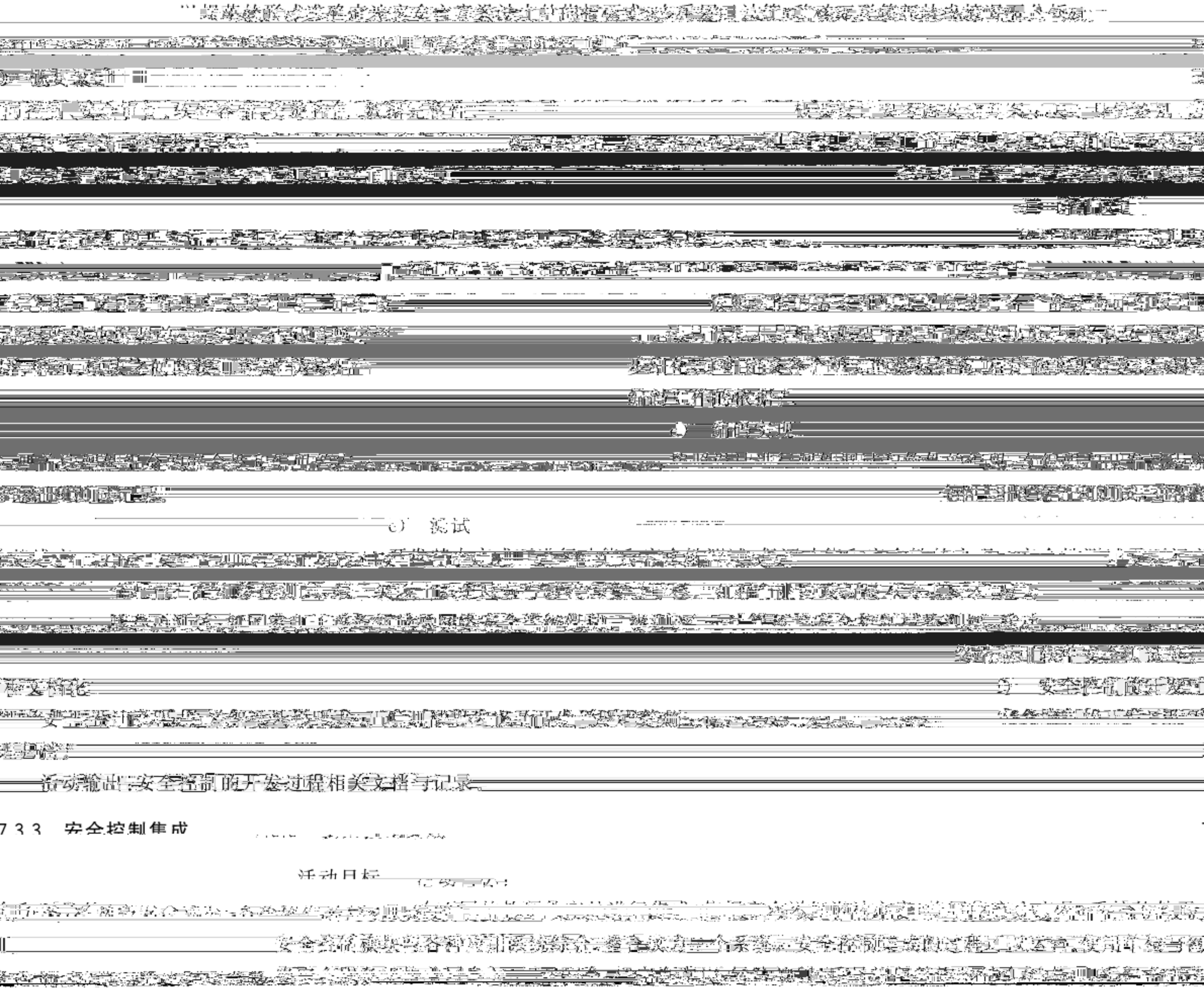
按照安全详细设计方案中对于产品或服务的具体指标要求进行采购，根据产品、产品组合或服务实

[redacted]

7.3.2 安全控制的开发

活动目标：

[redacted]



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：

7.4.3 安全实施过程管理

活动目标：

[illegible]

a) [illegible]

[illegible]

b) [illegible]

[illegible]

c) 风险管理

为了识别、评估和减低风险，以保[illegible]

[illegible]

d) [illegible]

[illegible]

e) 文档管理

[illegible]

活动输出：各阶段管理过程文档和记录。

8 安全运行与维护

8.1 安全运行与维护阶段的工作流程

[illegible]

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

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为系统管理员、安全管理员和安全审计员。

活动描述：

参与角色：

活动输入：安全管理设计方案、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) 建立运行管理组织

[illegible]

[illegible]

b) 授予管理权限

[illegible]

[illegible]

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]

[illegible]

参与角色：运营、使用单位。

[illegible]

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[illegible]

[illegible]

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，进而后续的活动[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]

要性和可行性。

变更影响分析

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、确定进行先决条件和后续活动等。

明确变更的类别

更的必

b)

对

变更的

c)

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，各项变化均实施记录，保证变更对业务的影响

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。

8.4 安全状态监控

8.4.1 监控对象确定

活动目标：

确定能够对等级保护对象安全造成影响的因素，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

b) 形成监控对象列表

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，

监控对象状态信息收集 8.4.2

活动目标：

活

参与角色：运营、使用单位。

活动输入：监控对象列表。

8.4.3 监控状态分析和报告

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。

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

b) 影响分析

根据对安全状况变化的分析，分

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。

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

8.5 安全自查和持续改进

8.5.1 安全状态自查

活动目标：

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安全措施一致有效地工作。

本活动主要包括以下子活动内容：

a) 实施安全方案实施控制

见 7.4.3。

b) 安全措施测试与验收

见 7.4.4。

c) 变更版本关键组件控制要求修订

根据安全改造方案实施落实各项补充的安全措施后，

到业务运行环境之前，

8.8 服务商管理和监控

8.8.1 服务商选择

活动目标：

8.8.2 服务商管理

活动目标：

服务商安全服务方案。

本活动主要包括以下子活动内容：

a) 人员管理

[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。

8.8 监督检查

8.9 应急响应与保障

8.9.1 应急准备

活动目标：

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

c） 安全事件分类分级

8.9.2 应急监测与响应

活动目标：

本活动主要包括以下活动内容：

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

[redacted]

8.9.3 后期评估与改进

[redacted]

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、

[redacted]

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、非电、物

[redacted]

5 定级对象变更

5.1 定级对象发生隶属单位变化的处理

附 录 A
（资料性附录）
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

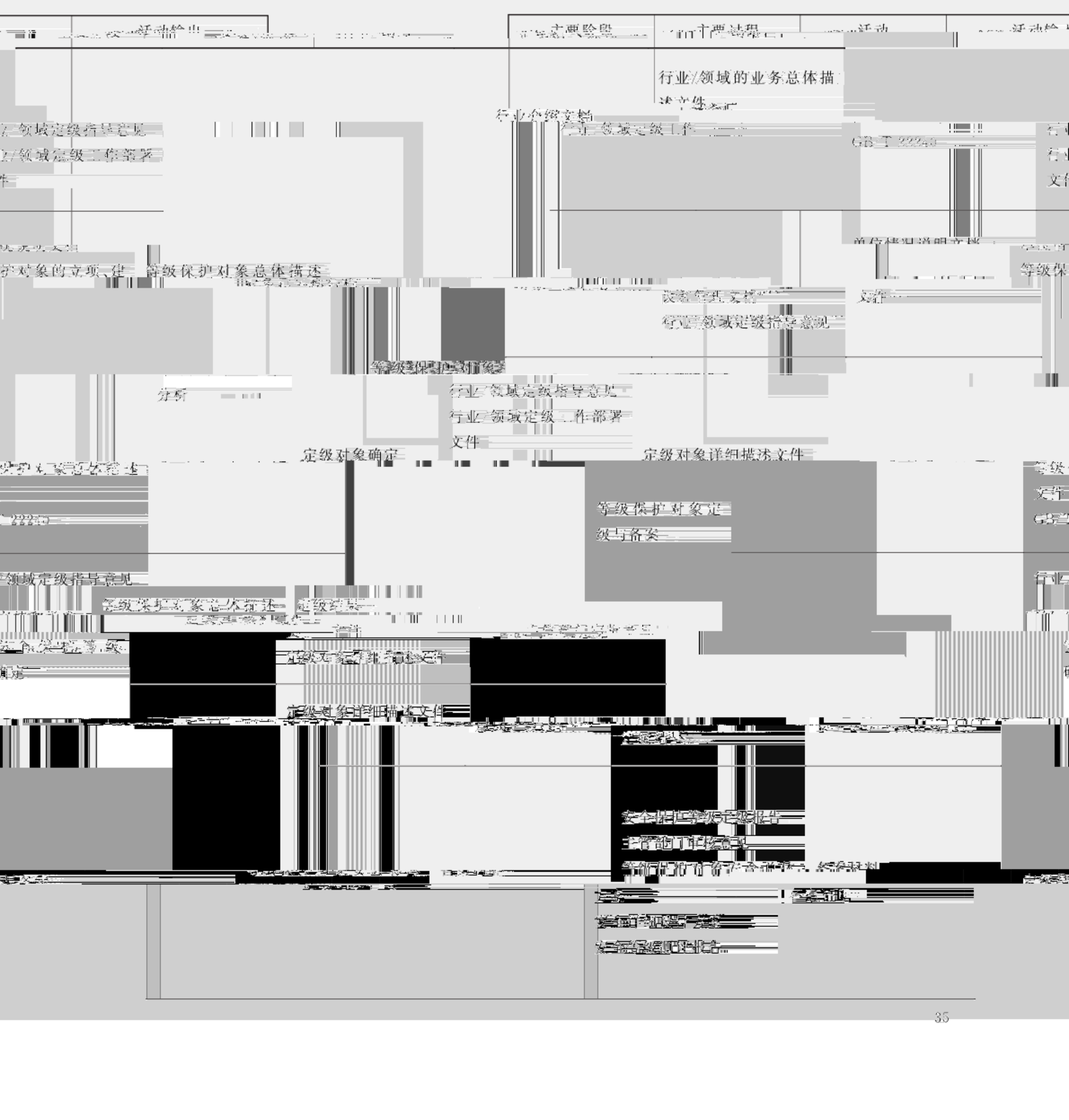


表 A.1（续）

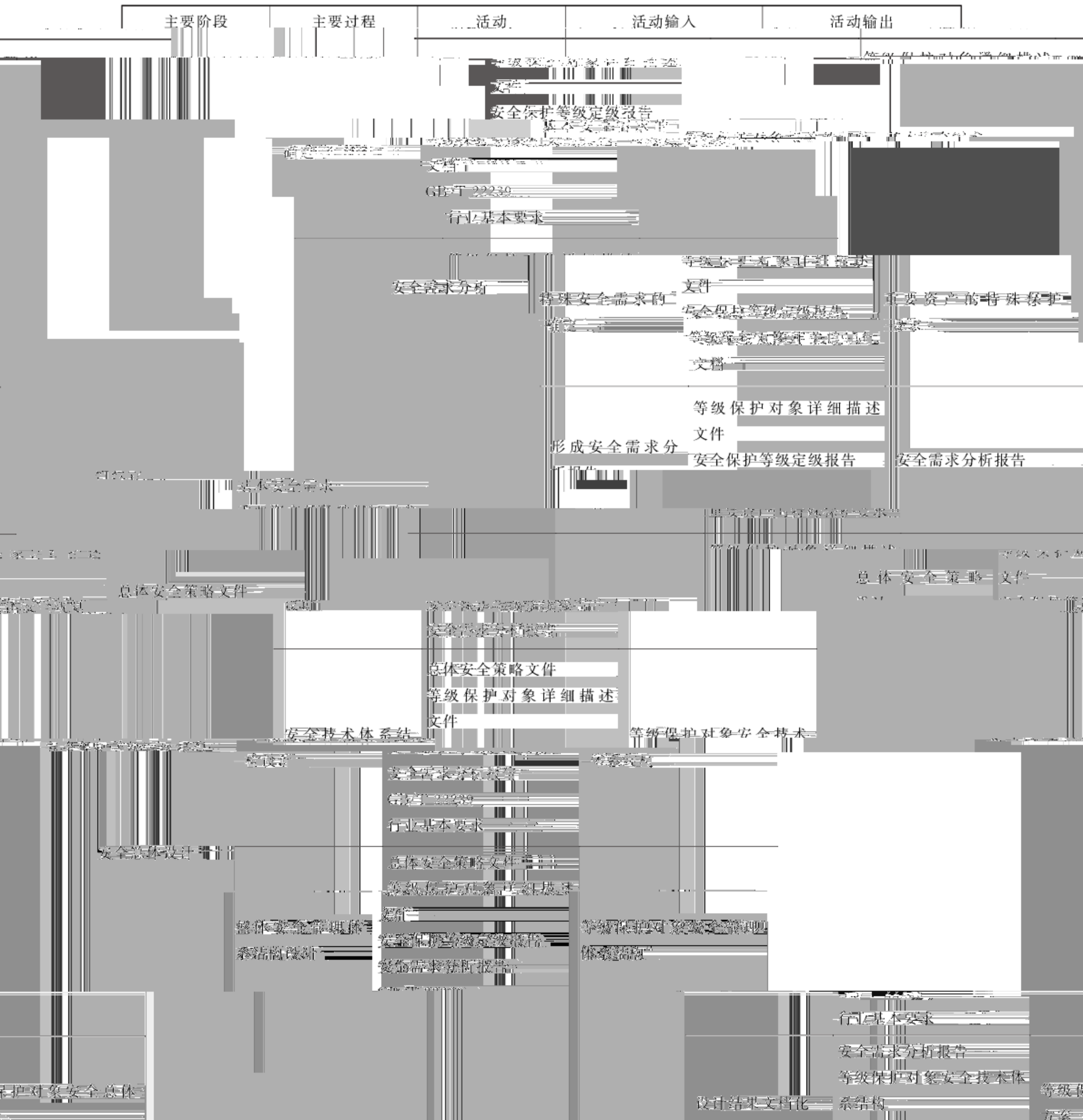

主要阶段
主要过程
活动
活动输入
活动输出
安全保护等级定级报告
文档
GB/T 22239
行业基本要求
安全需求分析
特殊安全需求的
文件
安全保护等级定级报告
文档
等级保护对象详细描述
文件
形成安全需求分
安全保护等级定级报告
安全需求分析报告
总体安全策略文件
安全技术体系结
总体安全策略文件
等级保护对象详细描述
文件
安全需求分析报告
GB/T 22239
行业基本要求
安全技术设计
总体安全策略文件
等级保护对象详细描述
文件
安全保护等级定级报告
安全需求分析报告
行业基本要求
安全需求分析报告
等级保护对象安全技术体
系结构
等级保护对象安全管理体
系结构
保护对象安全总体
设计结果文档化

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中长期发展规划	等级保护对象分阶段安全建设目标
		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	安全建设项目列表（含安全建设内容）
	总体安全规划	形成安全建设项目规划	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、安全建设项目列表（含安全建设内容）	安全建设项目规划
		技术措施实现内容设计	安全总体方案、安全建设项目规划、等级保护对象安全需求和风险评估、网络安全产品或服务	技术措施实现方案
	安全方案详细设计	管理措施实现内容设计	安全总体方案、安全建设项目规划	管理措施实现方案
		设计结果文档化	技术措施实现方案、管理措施实现方案	安全详细设计方案
		网络安全产品或服务采购	安全详细设计方案、相关供应商的产品信息	需采购的网络安全产品性能、功能和安全要求或服务机构的能力要求
		安全控制的开发	安全详细设计方案	安全控制的开发过程相关文档
	技术措施实现	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	测试报告、验收报告
	管理措施实现	安全管理制度的建设和修订	安全详细设计方案	安全策略、各项管理制度和操作规范、管理制度评审修订记录
		安全实施过程管理	各阶段管理过程文档和记录	安全设计与实施阶段各环节的文档及控制过程性文档

表 A.1（续）

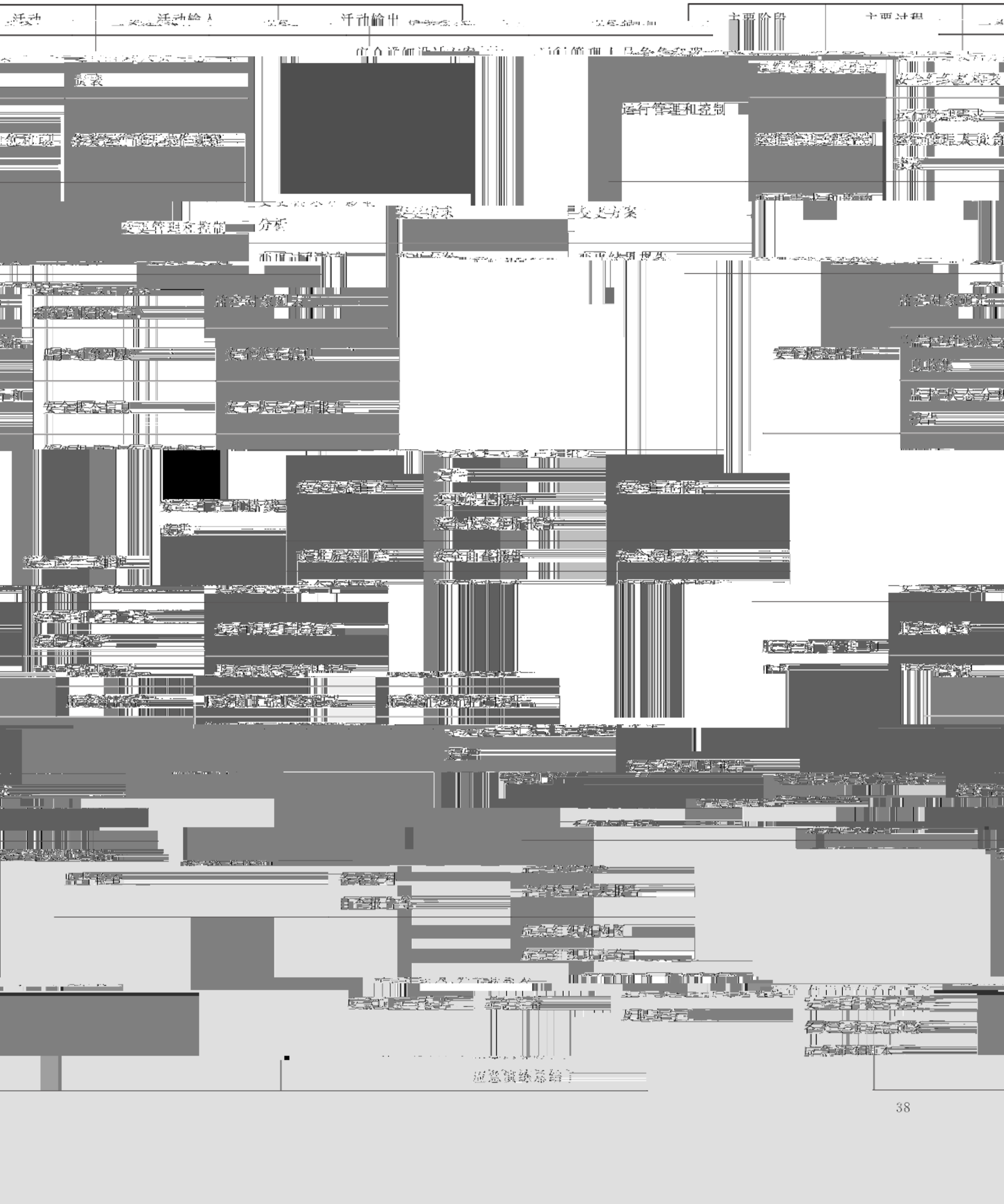


表 A.1（续）

主要阶段	主要过程	活动	活动输入	活动输出
			网络流量，日志信息，性能信息等	
			总体应急预案	
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	

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

中国标准出版社出版发行

北京市西城区三里河北街

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