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]

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

[illegible]

c) 同步建设原则

[illegible]

d) 动态调整原则

[illegible]

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和监督管理工作。

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、本部门或者本地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

[illegible]

d) 网络安全服务机构

负责根据运营、使用单位的委托,依照国家网络安全等级保护的管理规范和技术标准,协助运营、使用单位完成等级保护的相关工作,包括确定其等级保护对象的安全保护等级、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、提供服务支撑平台等。

e) 网络安全等级测评机构

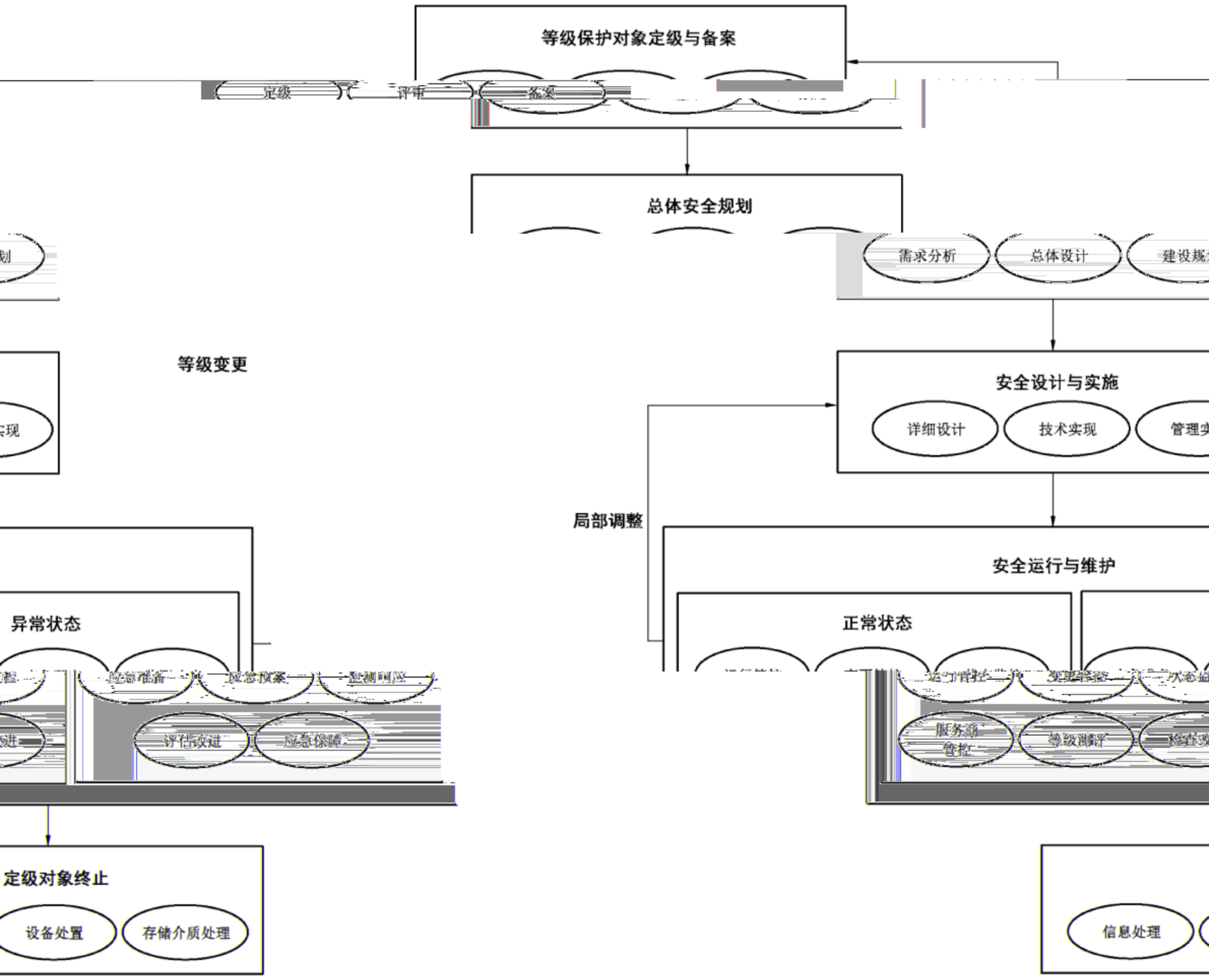
负责根据运营、使用单位的委托或根据等级保护管理部门的授权,协助运营、使用单位或等级保护管理部门,[illegible]对等级保护对象进行等级测评;对网络安全产品供应商提供的网络安全产品进行安全测评。

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,开发符合等级保护相关要求的网络安全产品,接受安全测评;按照等级保护相关要求销售网络安全产品并提供相关服务。

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。



护工作实施的基本流程

图 1　安全等级保

与实施阶段，重新设计、调整和实施安全措施，确保满足等级

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进入安全设计

保护的要求；当等级保护对象发生重大变更

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。

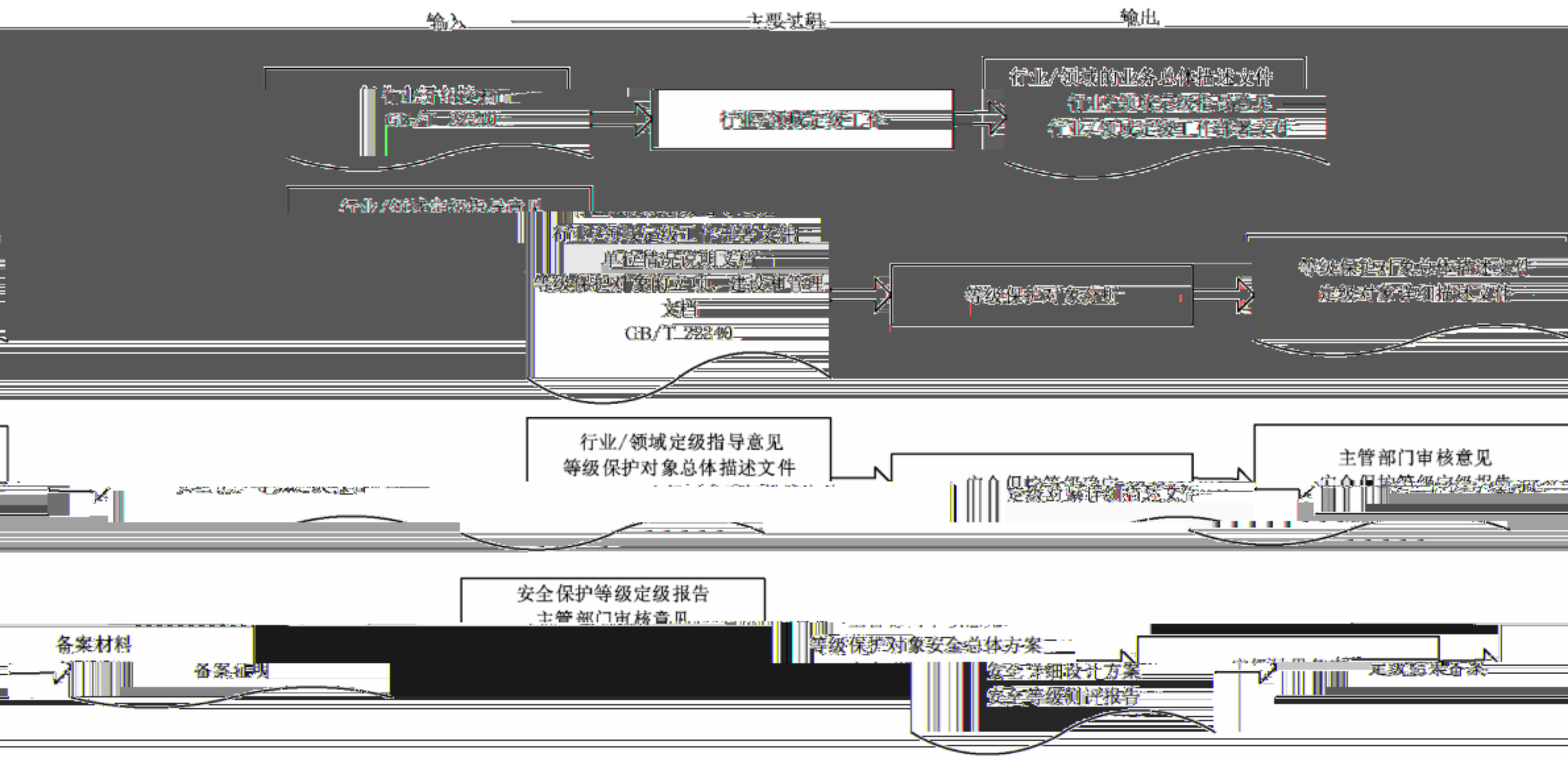


图 2 定级与备案阶段工作流程

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

主管部门可组织梳理本行业/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，并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。

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能[illegible]

[illegible]

d) [illegible]

主管部门可制定本行业/领域的定级指导意见，并统一部署本行业/领域的定级工作[illegible]管部门应对下属单位的定级结果进行审核、批准。

[illegible]

活动输出：[illegible]

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[illegible]

参与角色：[illegible]

活动输入：[illegible]建设和管理文档、行业/领域定级指导意见。

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/职能和生产产值等信息，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属性和业务内容，确定单位的等级保护对象，并确定等级保护对象的业务范围、地理位置以及其他基本情况，获得等级保护对象的背景信息和联络方式。

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、部门设置和部门在业务运行中的作用、岗位职责，获[illegible]

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况，在此基础上明确等级保护对象的边界，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种类

了解单位内主要依靠信息化处理的各种业务及业务流程，从中明确支撑单位业务运营的等级保护对象的业务特性。

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、完整性和可用性等方面的重要[illegible]

性程度。

[illegible] g) 识别用户范围和用户类

[illegible]

ii) 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档。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]

[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划分为多个定级对象。

[illegible]

[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。

进一步的定级对象详细描述文件应包含以下内容：

1) 相对独立的定级对象列表；

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：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]管理规范和定级标准，确定定级对象的安全保护等级[illegible]

[illegible]

参与角色：主管部门，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，等级保护对象总体描述文件，定级对象详细描述文件。

活动描述：

本活动主要包括以下子活动内容：

a) 定级对象安全保护等级初步确定

根据国家有关管理规范、行业/领域定级指导意见(若有则作为依据)以及定级方法，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) 定级结果评审

运营、使用单位初步确定了安全保护等级后，必要时可以组织网络安全专家和业务专家对初步定级结果的合理性进行评审，出具专家评审意见。

c) 定级结果审核批准

运营、使用单位初步确定了安全保护等级后，有上级主管部门的，应将初步定级结果上报行业/领域主管部门或上级主管部门进行审核、批准。行业/领域主管部门或上级主管部门应对初步定级结果的合理性进行审核，出具审核意见。

[illegible]进行审核、批准。

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[illegible]

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：

[illegible]

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，等级保护对象安全设计方案，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：

[illegible]

活动输出：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。

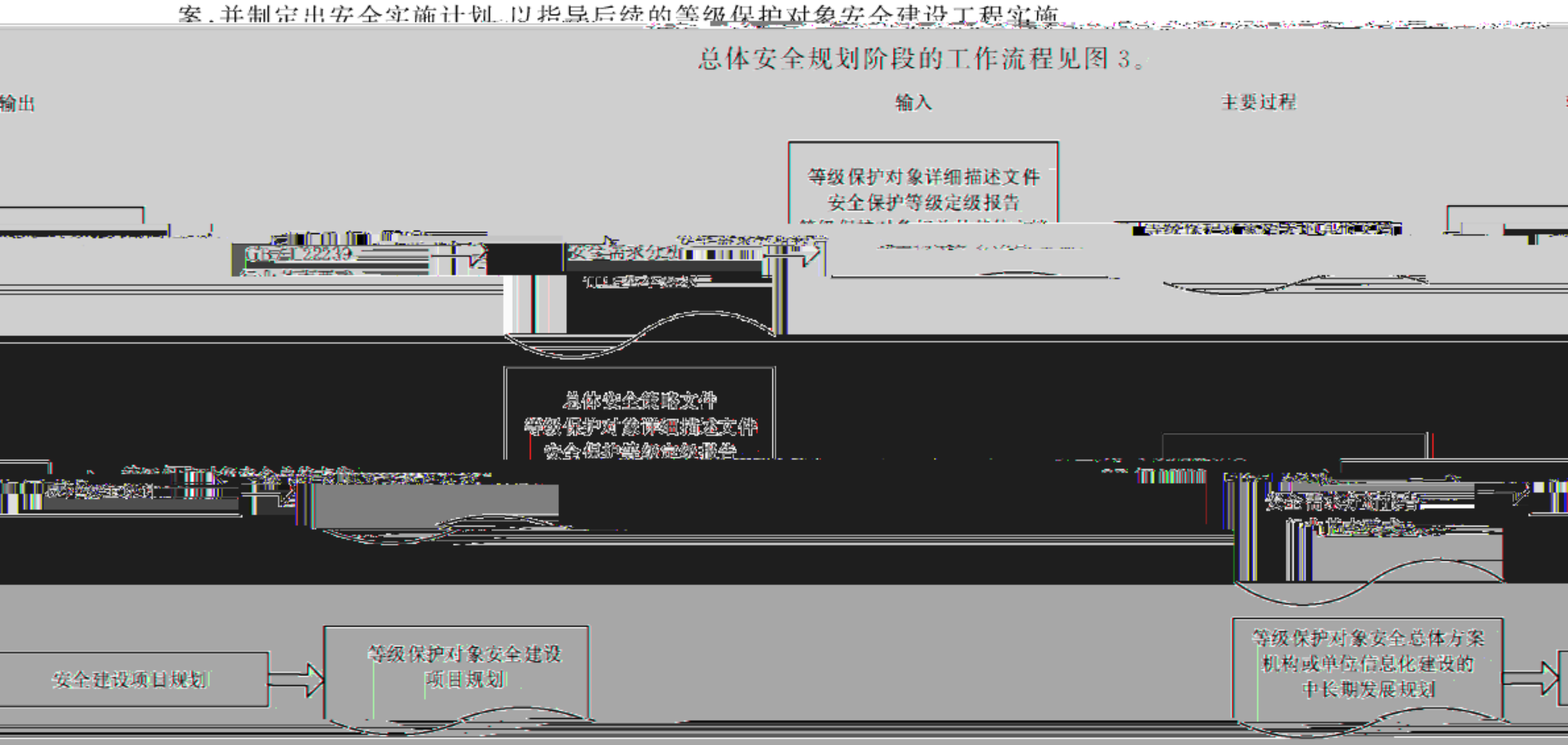


图3 总体安全规划阶段工作流程

析

6.2 安全需求分

需求的确定

6.2.1 基本安全需

活动目标：

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。

营、使用单位，网络安全服务机构。

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，

业基本要求。

包括以下子活动内容：

级保护对象范围和分析对象

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。

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

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：

出等级保护对象的特殊安全保护需求。

网络安全服务机构。

实施特殊安全措施的必要性，提

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，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，包括技术上和管理两方面）；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：

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：

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：

[illegible]

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

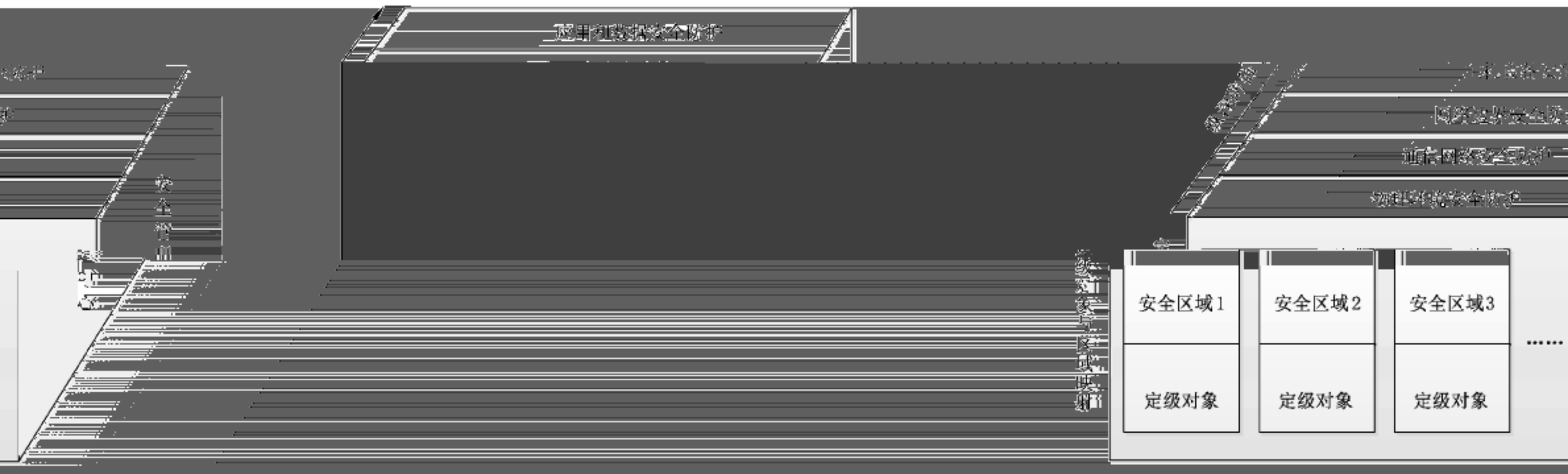
形成机构最高层次的安全方针文件，阐明安全工作的使命和意愿，定义网络安全的总体目标，规定网络安全责任机构和职责，建立安全工作运行模式等。

[redacted]

6.3.2 安全技术体系结构设计

活动目标：

[redacted]



[redacted]

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。通信网络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，[illegible]如果不同级别定级对象通过通信网络的同一线路和设备传输数据，[illegible]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。

d) [illegible]区域边界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区域边界的安全保护策略和安全技术措施。如果不同级别的定级对象共享同一设备进行边界保护，则该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定级对象的等级保护基本要求。

e) 规定定级对象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定级对象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定级对象之间的信息传输保护策略要求和具体的安全技术保护措施，包括同级互联的策略、不同级别互联的策略等。

f) 规定不同级别定级对象内部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内部网络平台、系统平台、业务应用和数据的安全保护策略和安全技术措施。[illegible]应满足最高级别定级对象的等级保护基本要求。

g) 规定云计算、移动互联等新技术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、行业基本要求和安全需求，提出云计算、移动互联[illegible]等新技术的安全保护策略和安全技术措施，[illegible]保护基本要求。

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、定级对象[illegible]，形成等级保护对象的安全技术体系结构。

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。

活动输入：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，[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

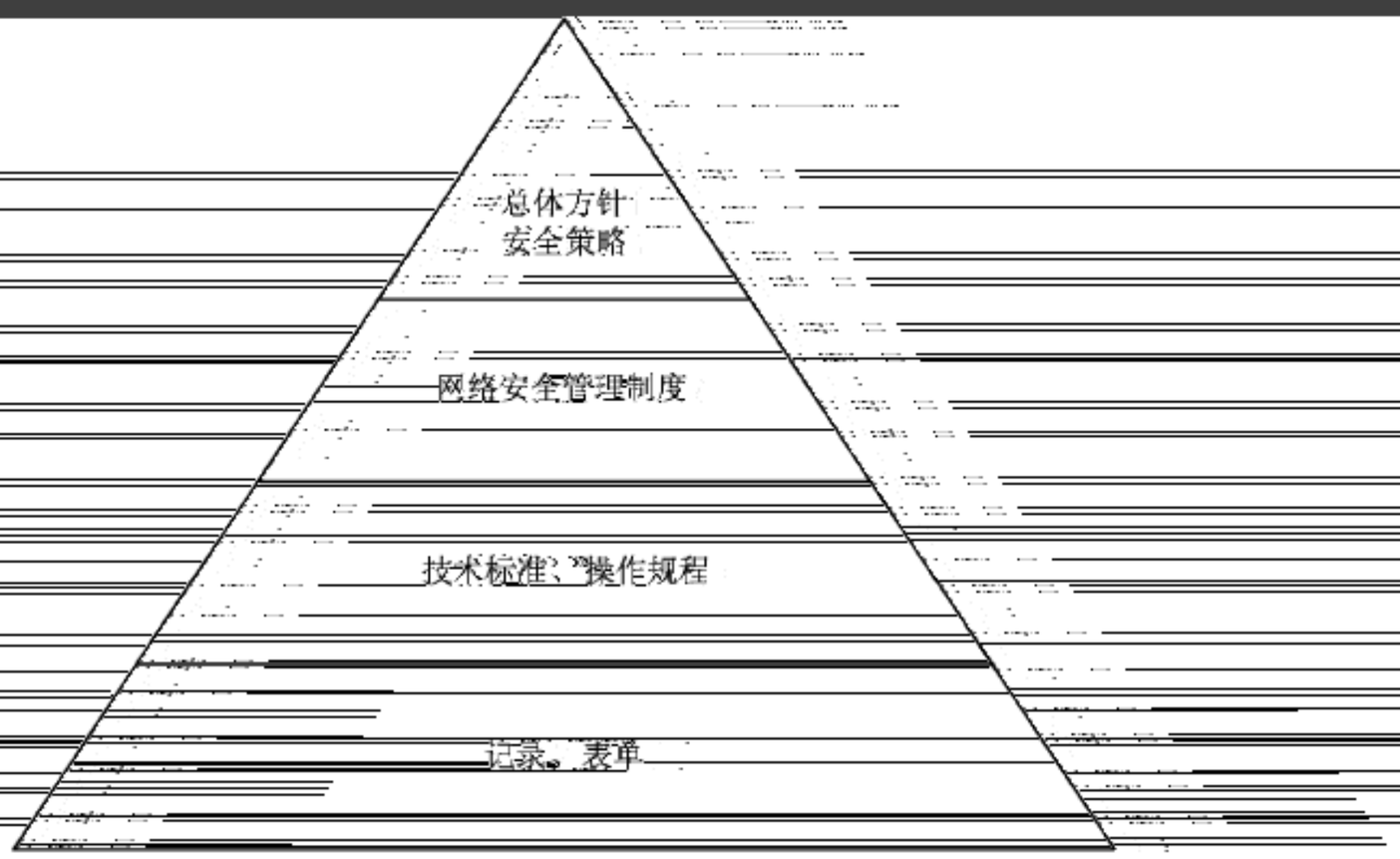


图 5 等级保护对象的安全管理体系框架

b） 规定网络安全的组织管理体系和对不同级别定级对象的安全管理职责

根据机构总体安全策略文件、等级保护基本要求系列标准、行业基本要求和安全需求，提出机构的

略等。

c） 规定不同级别定级对象的人员安全管理策略

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

g） 规定不同级别定级对象安全事件处置和应急管理策略。

根据总体安全策略文件、等级保护基本要求系列标准，针对

定级对象的安全事件处置和应急管理策略等。

h） 形成等级保护对象安全管理策略框架。

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。

单位，网络安全服务机构。

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。

等级保护对象安全技术体系结构和安全管理体系结构等文档进行整理，形成

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。

6.3.4 设计结果文档化

活动目标：

将总体安全设计工作的

参与角色：运营、使用单

活动输入：安全需求分

活动描述：

对安全需求分析报告、

等级保护对象总体安全方案

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：等级保

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

分解。主要建设内容可

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

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；

[illegible] 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

主要安全问题所要达到的安全

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

设项目规划

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

，进行投资估算，形成安全建设项目规划。

[illegible]

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。

动描述：

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

安全建设项目规划。

安全建设项目规划包含但不限于：

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) 安全建设资源保障（含测试及运维保障等）；

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。

6.4.3 形成安全建设

活动目标：

根据建设目标和

阶段，设计建设顺序

参

活

活

对

护对象等

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。

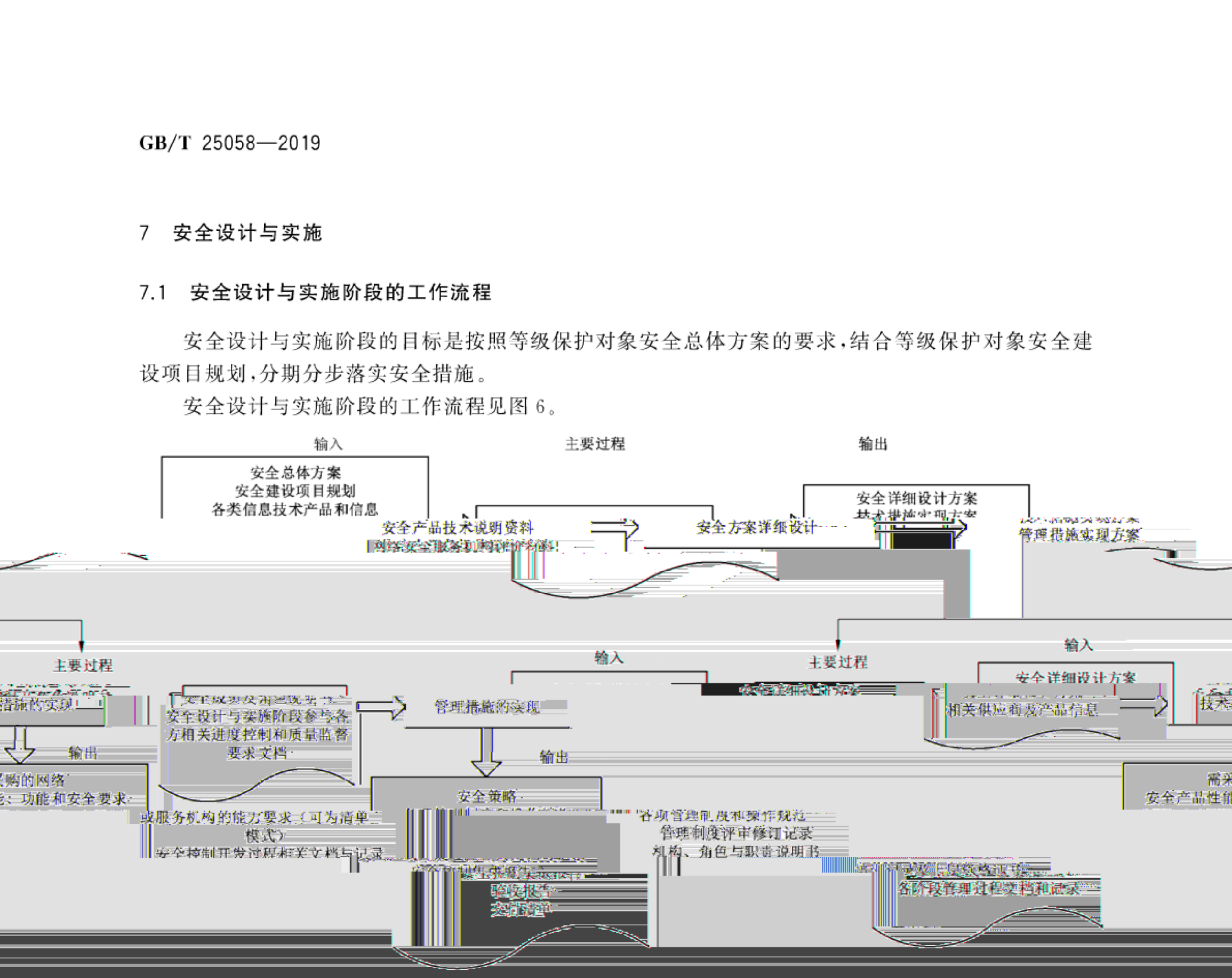


图 6 安全设计与实施阶段工作流程

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：

[illegible]

和安全控制的开发阶段具有依据；

品功能特征整理成文档，使得在网络安全产品采购

网络安全产品供应商。

参与角色：运营、使用单位，网络安全服务机构；

[illegible]

络安全服务机构评价材料。

活动描述：

活动内容：

本活动主要包括以下子

a） 结构框架的设计

[illegible]

[illegible]

。

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) 性能要求的设计

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) 部署方案的设计

结合目前等级保护对象网络拓扑结构与不同的方式路径安全技术实现框架的实现方式，包括安全设备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，给出调整的图示方案等。

e) 制定安全策略的实现计划

依据管理部分对等级保护对象安全总体方案中技术层面的安全管理要求，制定满足相关要求的安全策略和管理制度的实现计划。

7.2.2 管理措施实施内容的设计

活动目标：

根据等级保护对象运营、使用单位当前安全管理需要和安全技术保障需要提出与等级保护对象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：运营、使用单位，网络安全服务机构。

活动输入：安全总体方案，安全建设项目规划。

活动描述：

结合等级保护对象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，同时注意与等级保护对象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策略和管理制度制定、安全管理机构和人员的配套、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中技术实施内容和管理措施实施方案中管理实施内容进行汇总，形成等级保护对象安全建设整体设计方案。

方案主要包括安全总体设计：

a) 工程概述；

b) 设计依据；

c) 设计原则；

d) 总体设计；

e) 技术实现方案；

f) 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 [illegible]

[illegible]

7.3.2 安全控制的开发

活动目标：

对于一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 [illegible]

[illegible]

参与角色：运营、使用单位，网络安全 [illegible]

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

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

全管理相配套的、包
循的行为规范和操作

管理、特殊权限管理、

范性。

环境和情况的变化，对

构的岗位设置、人员的分工和岗位培训以及各种资源的

员、安全管

求相关人员

安全意识培训和培训

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、修订并落实与等级保护对象安
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段和环节所应遵
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、账户管理、远程访问
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，来保证各项管理工作的规

c） 评估与完善

制度在发布、执行过程中，要定期进行评估，保留评估或评审记录，根据实际

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

参与角色：使用单位、网络安全服务机构。

活动输入：安全详细设计方案、岗位职责和操作规范。

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

识别与网络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
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，明确相关岗位人员的责任和权限范围，并要征

c） 人员安全管理

针对普通员工、管理员、开发人员、运维人员以及安全人员开展特定技能培训和
试进行考核，合格者颁发上岗资格证书等。

活动输出：机构、角色与职责说明书、培训记录及上岗资格证书等。

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。

[illegible]

[illegible]

a) 资金管理

资金管理贯穿于等级保护对象建设的整个生命周期中，等级保护对象安全级别的确定、基本[illegible]

[illegible]

b) 成本管理

在创建等级保护对象的过程中，发生变更[illegible]

[illegible]

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，风险管理贯穿[illegible]

[illegible]

d) 变更管理

[illegible]

[illegible]

[illegible]

[illegible]

e) 进度管理

等级保护对象建设的实施必须要有一组明确的可[illegible]

[illegible]

交付成果，同时也要求有结束的日期，因此在建[illegible]

[illegible]

设等级保护对象的过程中，应制订项目进度计划，绘制[illegible]

进度网络图，将系统分解为不同的工作任务，并进行[illegible]

[illegible]

时间控制，确保项目的如期完成。

f) 文档管理

文档是记录项目整个过程的书面资料，在等级[illegible]

[illegible]

保护对象建设的过程中，针对每个环节都有大量的文[illegible]

[illegible]

档输出，文档管理涉及等级保护对象建设的各个环[illegible]

[illegible]

节，主要包括：系统定级、规划设计、方案设计、安全实[illegible]

[illegible]

施、测试验收等方面[illegible]

[illegible]

各阶段管理过程文档的记录[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

[illegible]

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。

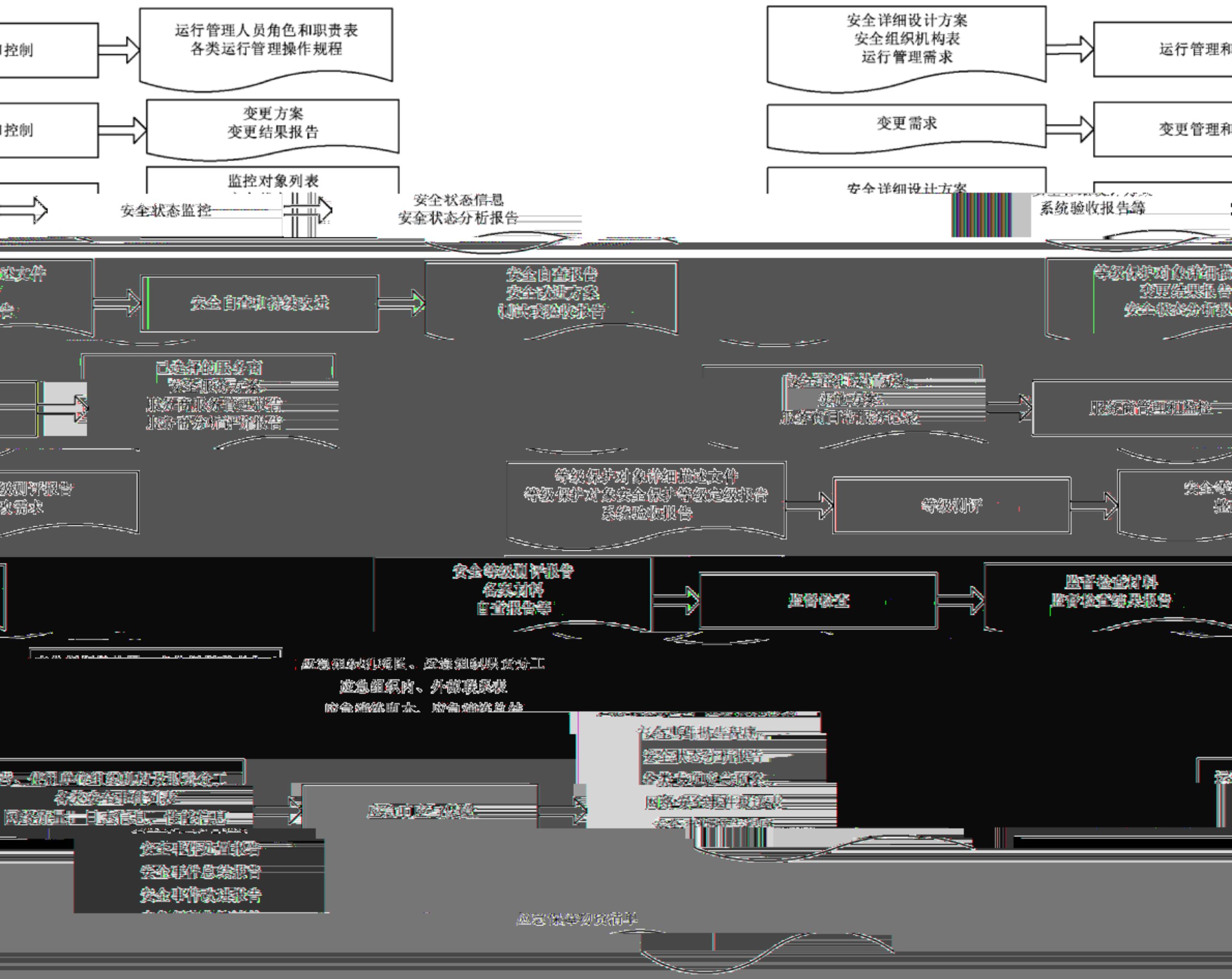


图7　安全运行与维护阶段工作流程

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[illegible]

[illegible]

根据不同的安全保护等级要求的控制粒度，分析需要运行管理控制内容，并明确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]

[illegible]

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，如：移动介质使用规程、终端使用规程、数[illegible]

[illegible]

b) 操作记录

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：

通过对运行与维护过程中的变更需求和变更影响的分析，来确定变更的类型，计划后续的活动。

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

对运行与维护过程中的变更需求进行分析[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

大变更。如果是由等级保护对象关键发生变化、承载的信息

确定等级保护对象是局部调整还是重

根据(一)

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

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

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

e) 形成变更结果报告

收集变更过程的各类相关文档,整理、

活动输出:变更结果报告。

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

及人员权限进行审核,以确保变更合理、科学的实施。按照

过程各类系统状态、各种操作活动等建立操作记录或日志。

分析和总结各类数据,形成变更结果报告,并归档保存。

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

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

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

影响的因素,即确定安全状态监控的对象。

收报告等。

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

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：

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全状态进行监控。

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

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结合。

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，或者来自外部环境的安全性威胁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：

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。

活动输出：安全状态分析报告。

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：

本活动主要包括以下子活动内容：

a) 确定自查对象和自查方法

确定检查的对象和方法，确定本次安全自查的范围及安全自查工具、调研表格等。

b) 制定自查方案

确定自查工作的角色和职责，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]

[illegible]

c) 安全自查实施

根据安全[illegible]通过访谈、检查和测试等多种手段，进行安全状况检查，记录各种自查活动的结果。[illegible]

[illegible]

d) 安全自查结果和报告

总结安全自查的结果，提出改进的建议，产生安全自查报告，将安全自查过程的各类文档、资料[illegible]

活动输出：安全自查报告。

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。

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[illegible]

[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安全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 7.4.3。

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。

选择服务商时，应要求测服务商的网络安全风险，评估其风险大小，考察服务商的安全运行能力，网络安全风险点包括但不限于以下情况：

——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。

服务商以往服务项目案例。

c） 服务内容互斥分析

[illegible]

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

8.6.2

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。

——服务商人员在向使用单位提供服务的过程中，要按遵守使用单位的各项规定、管理要求，服从使用单位安排。

——如因服务商人员原因给使用单位造成经济损失或人身伤害或对信誉造成影响的，服务商应承担相应责任。

——使用单位督促服务商对服务人员开展培训及安全教育工作。

b) 服务管理

[illegible]

——服务商基本信息发生变更（如法人、单位名称、银行账户等）应提前通知使用单位。

——按照约定要求服务商提供各项服务，保质保量完成服务目标；如因服务商未完成服务目标给使用单位造成损失的，应予赔偿。

——服务商确保所提供服务不存在任何侵犯第三方著作权、商标权、专利权等合法权益的情形；服务商提供服务过程中产生的研究成果及知识产权未经使用单位许可，服务商不得以任何形式向任何第三方转让权利义务。

——服务商提供项目验收和考核的相关材料，配合使用单位组织开展项目结题验收和考核工作。

——使用单位根据约定的售后服务内容及标准，定期跟踪服务商售后服务考核情况，作为后续服务 [illegible]

活动输出：服务商服务管理报告。

8.6.3 服务商监控

活动目标：

通过对服务商及其人员在服务过程中的行为进行有效监控，若发现不合规行为，限时督促整改，确保服务商服务工作安全、高效。

参与角色：运营、使用单位、网络安全服务机构。

活动输入：服务商日常服务记录、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) [illegible] 服务商及其人员及时按照使用单位要求对所提供的服务 [illegible] 进行改进或调整，使服务质量符合使用单位要求。

b) [illegible]

c) 使用单位 [illegible] 服务商 [illegible]

d) 使用单位应对服务商人员定期进行考核评价，考核方式可采用日常考核、季度考核和年度考核。

e) [illegible] 考核也可采用适合使用单位的考核方式，如发生违反合作原则、危害使用单位利益等事项，使用单位有权随时向服务商提出人员更换要求。

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象开展等级测评。

b) 运营、使用单位参考等级测评机构的安全等级测评报告，分析确定整改需求。

c) 运营、使用单位根据等级测评报告提出的整改需求，开展安全整改工作。

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求，等级保护管理部门实施对同安全、行业相关等级保护监督检查要求及标准的执行情况，开展监督检查工作。

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：安全等级保护相关文件，等级测评报告，各级主管部门监督检查要求等。

活动描述：

a) 主管部门依据国家网络安全等级保护工作监管要求等制定监督检查方案及表单。

b) 等级保护管理部门实施监督检查，形成监督检查记录，并将检查结果报告主管部门。

c) 运营、使用单位根据监督检查结果进行整改，并将整改结果报告主管部门。

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

[illegible]责、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。

g) [illegible]

针对应急预案涉及的部门和人员制定专项培训计划，培训宣贯内容包括应急职责、合作和分工、应急预案启动条件和流程等。

h) 应急演练

[illegible]

8.9.2 应急监测与响应

活动目标：

[illegible]

活动描述：

本活动主要包括以下子活动内容：

a) 异常状态信息收集

[illegible]

b) 异常状态分析

[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、影响程度以及优先级等，形成安全状态分析报告和网络安全事件报送表，按照安全事件管理以及安全事件报告程序，[illegible]

d) 安全事件处置

对于应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方案对安全事件进行处置。

e) 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；对安全事件的处置过程进行总结，制定安全事件处置报告，并保存。

活动输出：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。

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) 改进实施

根据网络安全事件调查评估报告，制定改进预防措施，修改相应应急预案，结合实际情况进行落实，并组织开展应急预案相关培训。

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。

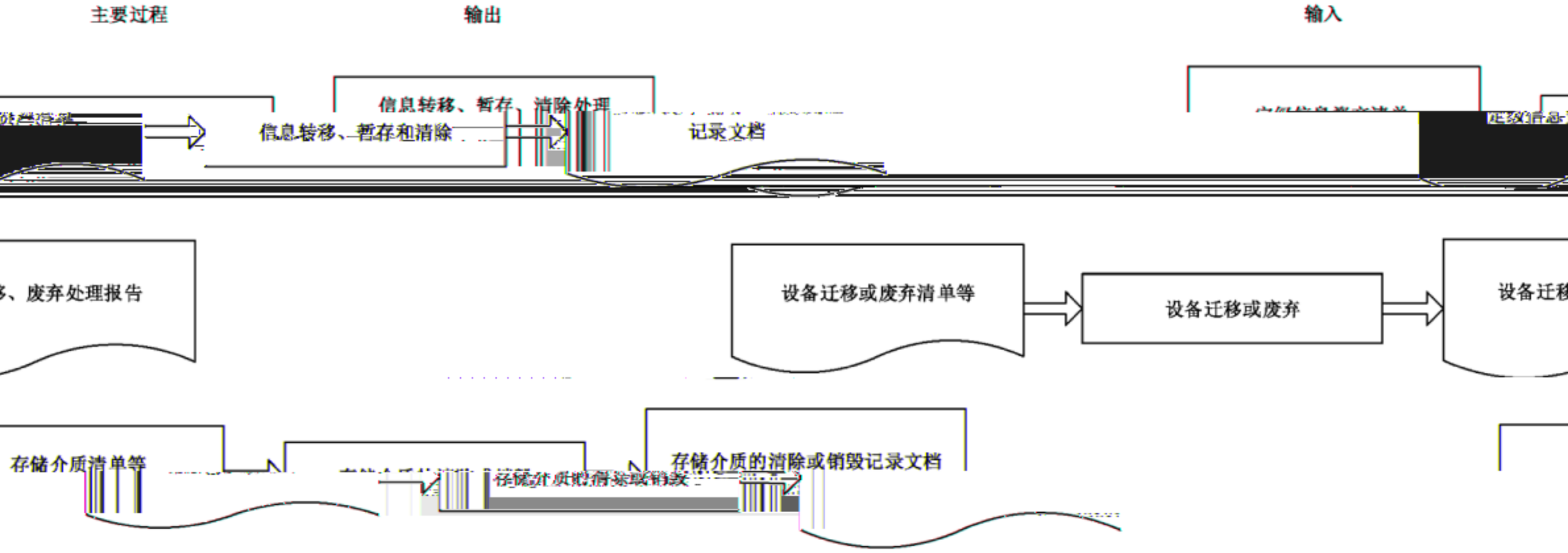


图 8　定级对象终止阶段工作流程

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）　识别要转移、暂存和清除的信息资产

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

输出：信息转移、暂存、清除处理记录文档，

活动输出：信息转移、暂存、清除处理记录文档，位置等。

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） 确定硬件设备处理方案

根据敏感信息的清除要求，确定设备处理方案，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

设备处理方案应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。

9.1.4 存储介质的清除或销毁

活动目标：

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，防止存储敏感信息的介质被未授权的用户获取和恢复敏感信息，确保定级对象终止后，存储介质中不包含敏感信息。

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

根据要终止的定级对象的存储介质清单，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，对于存储敏感信息的介质需按照国家相关部门的规定进行处理，并记录处理过程和相关责任人签字。

c） 处理方案审批

包括存储介质处理方案等应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，记录处理过程和相关责任人签字。

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
基本安全需求的确定	安全需求分析	特殊安全需求的确定	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
总体安全规划	总体安全规划	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
安全总体设计	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 等级保护对象安全管理体系结构
	设计结果文档化		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	等级保护对象安全设计方案

表 A.1（续）

主要阶段	主要过程	活动	活动输入	活动输出
安全设计与实施	总体安全规划	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	安全建设内容
		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 安全建设内容	等级保护对象安全建设项目规划
	安全方案详细设计	技术措施实现内容设计	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 [redacted] 网络安全服务机构材料	技术措施实施方案
		管理措施实现内容设计	安全总体方案 安全建设项目规划	管理措施实施方案
		设计结果文档化	技术措施实施方案 管理措施实施方案	安全详细设计方案
	技术措施的实现	网络安全产品或服务采购	安全详细设计方案 相关供应商及产品信息	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（可清单形式）
		安全控制的开发	安全详细设计方案	安全控制的开发过程和相关文档与记录
		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	验收报告 交付清单
	管理措施的实现	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
		安全管理机构和人员的设置	安全详细设计方案 安全策略 各项管理制度和操作规范	机构、角色与职责说明书
		安全实施过程管理	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	各阶段管理过程文档和记录

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
		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
		等级保护对象详细描述文件		
		安全状态审查	安全状态分析报告	安全审查报告
		变更结果报告		
		安全状态分析报告		
		改进方案制定	安全自查报告	安全改进方案
		安全改进方案		

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