ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25058—2019
代替 GB/T 25058—2010

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

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

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》。

——全文将“信息系统”调整为“等级保护对象”或“定级对象”，将国家标准“信息系统安全等级保护基本要求”调整为“网络安全等级保护基本要求”。

——考虑到云计算等新技术新应用在实施过程中的特殊处理，根据需要，相关章条增加云计算、移动互联、大数据等相关内容(见 5.3.2、6.3.2、7.2.1、7.3.2)。

——将各部分已有内容进一步细化，使其能够指导单位针对新建等级保护对象的等级保护工作(见 6.3.2、7.4.3)。

——在等级保护对象定级阶段，增加了行业/领域主管单位的工作过程(见 5.2)；增加了云计算、移动互联、物联网、工控、大数据定级的特殊关注点(见 5.3，2010 年版的 5.2)。

——在总体安全规划阶段，增加了行业等级保护管理规范和技术标准相关内容，即明确了基本安全需求既包括国家等级保护管理规范和技术标准提出的要求，也包括行业等级保护管理规范和技术标准提出的要求(见 6.2.1，2010 年版的 6.2.1)。

——在总体安全规划阶段，增加了“设计等级保护对象的安全技术体系架构”内容，要求根据机构总体安全策略文件、GB/T 22239 和机构安全需求，设计安全技术体系架构，并提供了安全技术体系架构图。此外，增加了云计算、移动互联等新技术的安全保护技术措施(见 6.3.2，2010 年版的 6.3.2)。

——在总体安全规划阶段，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，并提供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“技术措施实现”与“管理措施实现”调换顺序(见 7.3、7.4，2010 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 7.3.1、7.3.3)；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 7.4.1、7.4.2)。

——在安全设计与实施阶段，在技术措施实现中增加了对于云计算、移动互联等新技术的风险分析、技术防护措施实现等要求(见 7.2.1，2010 年版的 7.2.1)；在测试环节中，更侧重安全漏洞扫描、渗透测试等安全测试内容(见 7.3.2，2010 年版的 7.3.2)。

——在安全设计与实施阶段，在原有信息安全产品供应商的基础上，增加网络安全服务机构的评价和选择要求(见 7.3.1)；安全控制集成中，增加安全态势感知、监测通报预警、应急处置追踪溯源等安全措施的集成(见 7.3.3)；安全管理制度的建设和修订要求中，增加要求总体安全方针、安全管理制度、安全操作规程、安全运维记录和表单四层体系文件的一致性(见 7.4.1)；安全实施过程管理中，增加整体管理过程的活动内容描述(见 7.4.3)。

——在安全运行与维护阶段，增加“服务商管理和监控”(见 8.6)；删除了“安全事件处置和应急预案”(2010 年版的 8.5)；删除了“系统备案”(2010 年版的 8.8)；修改了“监督检查”的内容(8.8，2012 年版的 8.9)，增加了“应急响应与保障”(见 8.9)。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

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

根据等级保护对象的重要程度、业务特点，通过划分不同安全保护等级的等级保护对象，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等级保护对象。

c) 同步建设原则

等级保护对象在新建、改建、扩建时应同步规划和设计安全方案，投入一定比例的资金建设网络安全设施，保障网络安全与信息化建设相适应。

d) 动态调整原则

应跟踪定级对象的变化情况，调整安全保护措施。由于定级对象的应用类型、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

负责依照国家网络安全等级保护的管理规范和技术标准，确定其等级保护对象的安全保护等级，有主管部门的，应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；按照国家网络安全等级保护管理规范和技术标准，进行等级保护对象安全保护的规划设计；使用符合国家有关规定，满足等级保护对象安全保护等级需求的信息技术产品和网络安全产品，开展安全建设或者改建工作；制定、落实各项安全管理制度，定期对等级保护对象的安全状况、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；制定不同等级网络安全事件的响应、处置预案，对网络安全事件分等级进行应急处置。

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，按照国家网络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。

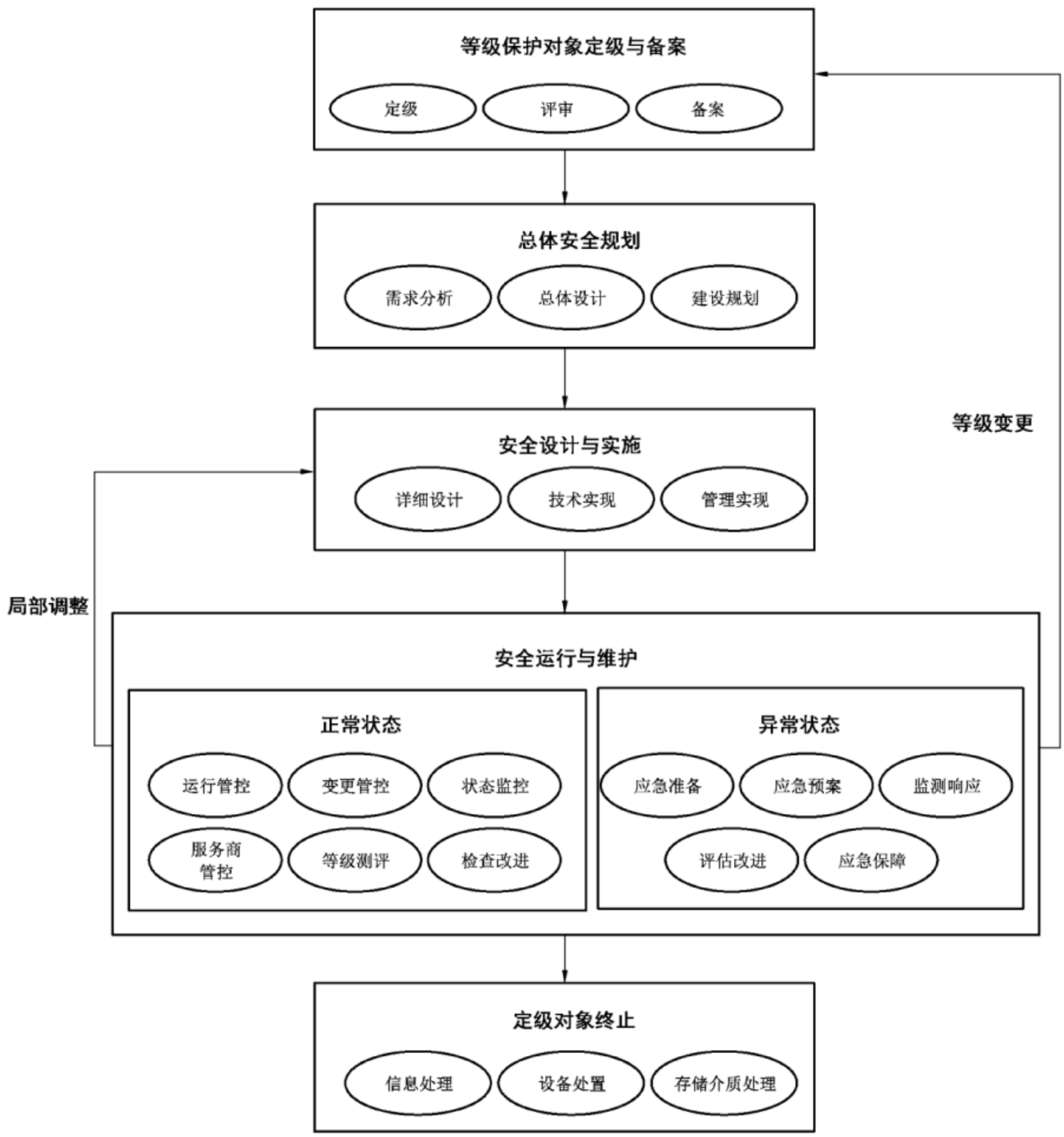

图 1　安全等级保护工作实施的基本流程

在安全运行与维护阶段，等级保护对象因需求变化等原因导致局部调整，而其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；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保护对象定级与备案阶段，重新开始一轮网络安全等级保护的实施过程。等级保护对象在运行与维护过程中，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

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。

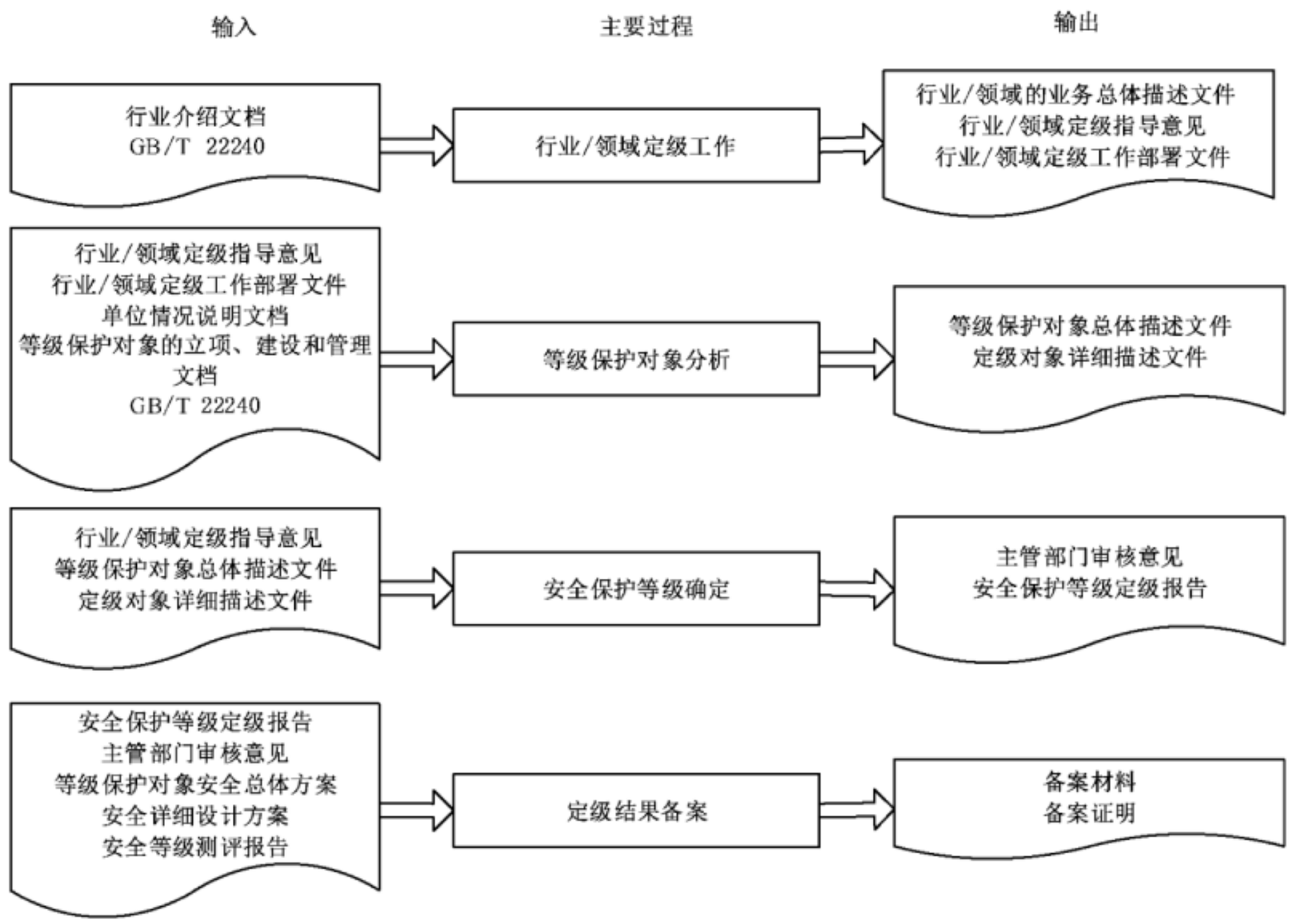

图 2 定级与备案阶段工作流程

5.2 行业/领域定级工作

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/领域的行业特征、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） 识别行业/领域的主要业务