

ICS 35.040
L 80



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 cy-

bersecurity

2019-08-30 发布

2020-03-01 实施

国家标准 网络安全等级保护实施指南 发布日期：2019-08-30 实施日期：2020-03-01 发布
中国网络安全和信息化委员会

目 次

前言 V

1 范围 1

2 规范性引用文件 1

3 术语和缩略语 2

4 定级对象 3

5 定级过程 4

6 定级结果 5

7 定级报告 6

8 定级工作实施 8

9 定级工作实施 8

10 定级工作实施 8

11 定级工作实施 8

12 定级工作实施 8

13 定级工作实施 8

14 定级工作实施 8

15 定级工作实施 8

16 定级工作实施 8

17 定级工作实施 8

18 定级工作实施 8

19 定级工作实施 8

20 定级工作实施 8

21 定级工作实施 8

22 定级工作实施 8

23 定级工作实施 8

24 定级工作实施 8

25 定级工作实施 8

26 定级工作实施 8

27 定级工作实施 8

28 定级工作实施 8

29 定级工作实施 8

30 定级工作实施 8

31 定级工作实施 8

32 定级工作实施 8

33 定级工作实施 8

34 定级工作实施 8

35 定级工作实施 8

36 定级工作实施 8

37 定级工作实施 8

38 定级工作实施 8

39 定级工作实施 8

40 定级工作实施 8

41 定级工作实施 8

42 定级工作实施 8

43 定级工作实施 8

44 定级工作实施 8

45 定级工作实施 8

46 定级工作实施 8

47 定级工作实施 8

48 定级工作实施 8

49 定级工作实施 8

50 定级工作实施 8

51 定级工作实施 8

52 定级工作实施 8

53 定级工作实施 8

54 定级工作实施 8

55 定级工作实施 8

56 定级工作实施 8

57 定级工作实施 8

58 定级工作实施 8

59 定级工作实施 8

60 定级工作实施 8

61 定级工作实施 8

62 定级工作实施 8

63 定级工作实施 8

64 定级工作实施 8

65 定级工作实施 8

66 定级工作实施 8

67 定级工作实施 8

68 定级工作实施 8

69 定级工作实施 8

70 定级工作实施 8

71 定级工作实施 8

72 定级工作实施 8

73 定级工作实施 8

74 定级工作实施 8

75 定级工作实施 8

76 定级工作实施 8

77 定级工作实施 8

78 定级工作实施 8

79 定级工作实施 8

80 定级工作实施 8

81 定级工作实施 8

82 定级工作实施 8

83 定级工作实施 8

84 定级工作实施 8

85 定级工作实施 8

86 定级工作实施 8

87 定级工作实施 8

88 定级工作实施 8

89 定级工作实施 8

90 定级工作实施 8

91 定级工作实施 8

92 定级工作实施 8

93 定级工作实施 8

94 定级工作实施 8

95 定级工作实施 8

96 定级工作实施 8

97 定级工作实施 8

98 定级工作实施 8

99 定级工作实施 8

100 定级工作实施 8

7.2.1 技术措施实现内容的设计 16

7.2.2 管理措施实现内容的设计 17

7.2.3 技术措施实现的文档化 17

7.3 技术措施的实现 18

7.3.1 网络安全 18

7.3.2 安全控制 18

7.3.3 安全控制集 19

7.3.4 系统验收 20

7.4 管理措施的实现 21

7.4.1 安全管理 21

7.4.2 安全培训 21

7.4.3 安全实施 21

7.4.4 安全运行 22

7.4.5 安全维护 22

7.4.6 安全改进 22

7.4.7 安全退出 22

7.4.8 安全记录 24

7.4.9 安全评估 24

7.4.10 安全改进 24

7.4.11 安全记录 24

7.4.12 安全改进 24

7.4.13 安全记录 24

7.4.14 安全改进 24

7.4.15 安全记录 24

7.4.16 安全改进 24

7.4.17 安全记录 24

7.4.18 安全改进 24

7.4.19 安全记录 24

7.4.20 安全改进 24

7.4.21 安全记录 24

7.4.22 安全改进 24

7.4.23 安全记录 24

7.4.24 安全改进 24

7.4.25 安全记录 24

7.4.26 安全改进 24

7.4.27 安全记录 24

7.4.28 安全改进 24

7.4.29 安全记录 24

7.4.30 安全改进 24

7.4.31 安全记录 24

7.4.32 安全改进 24

7.4.33 安全记录 24

7.4.34 安全改进 24

7.4.35 安全记录 24

7.4.36 安全改进 24

7.4.37 安全记录 24

7.4.38 安全改进 24

9 定级对象终止 32

9.1 定级对象终止 32

9.2 定级对象终止 32

9.3 定级对象终止 32

9.4 定级对象终止 32

9.5 定级对象终止 32

9.6 定级对象终止 32

9.7 定级对象终止 32

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定级、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

2 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，自主确定安全保护等级，自行组织实施安全保护。

b) 重点保护原则

c) 同步建设原则

其他原因, 安全防护等级需要变更的, 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

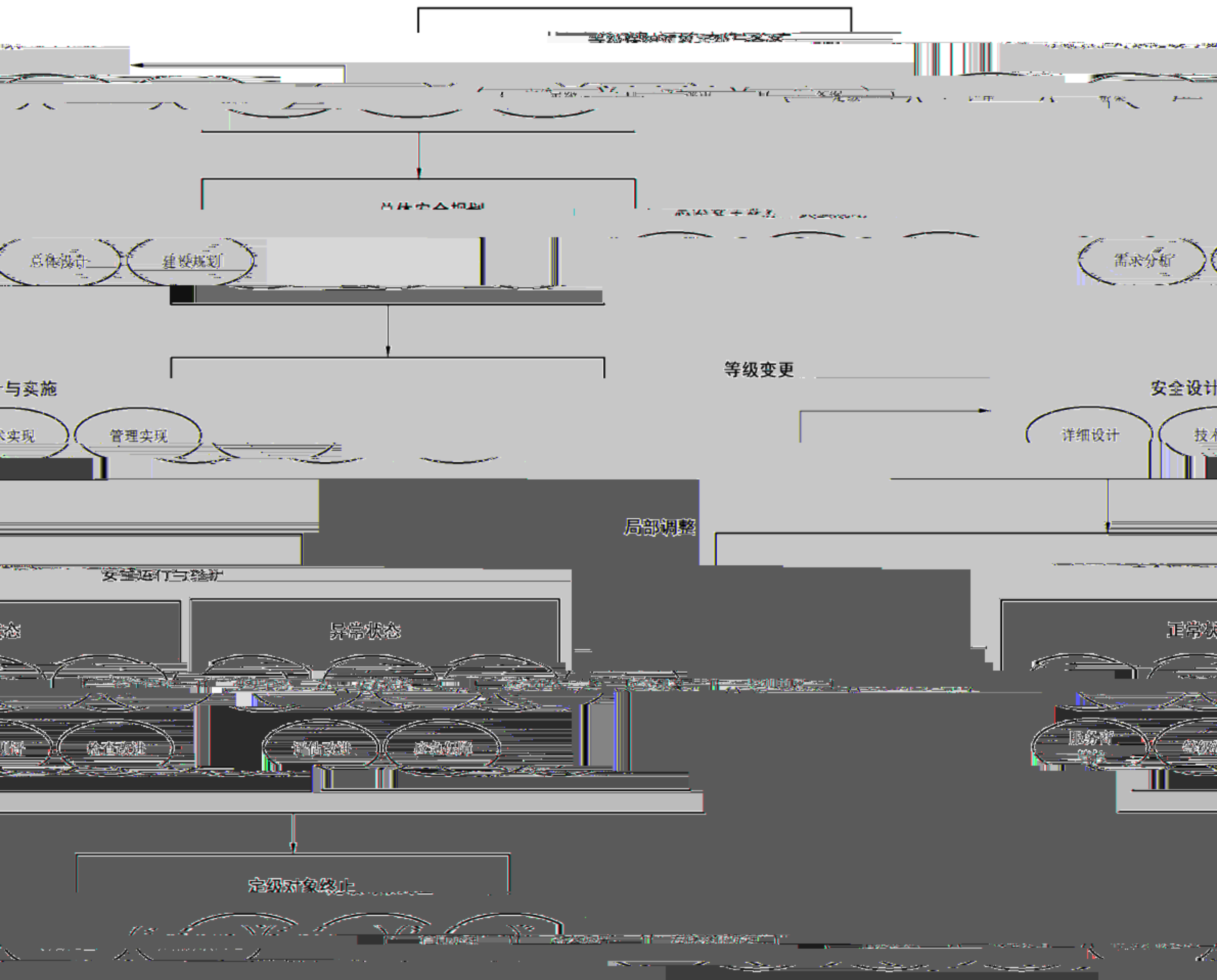


图 1 安全等级保护工作实施的基本流程

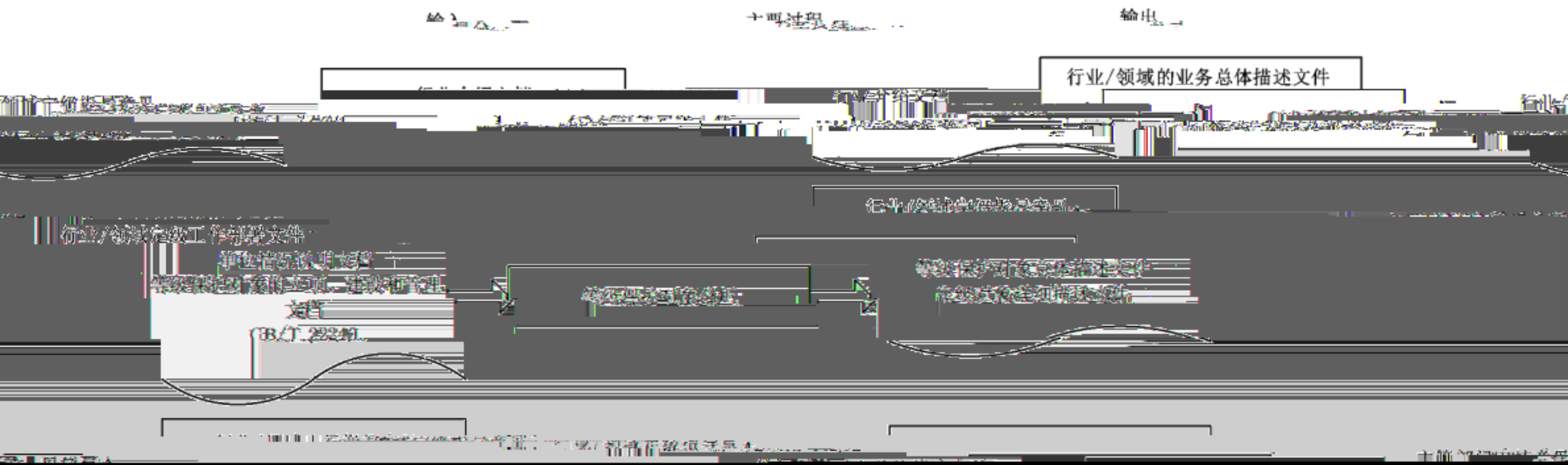
在安全等级保护实施过程中,应定期或不定期对安全等级保护对象的安全等级进行重新评估,并根据评估结果调整安全等级保护等级。当安全等级保护对象发生安全等级变化时,应从安全运行与维护阶段进入安全设计阶段,重新设计、建设和实施安全防护,并进行安全等级保护的要求。当安全等级保护对象发生安全等级变化时,应从安全运行与维护阶段进入安全运行与维护阶段,重新设计、建设和实施安全防护,并进行安全等级保护的要求。当安全等级保护对象发生安全等级变化时,应从安全运行与维护阶段进入安全运行与维护阶段,重新设计、建设和实施安全防护,并进行安全等级保护的要求。

在安全等级保护实施过程中,应定期或不定期对安全等级保护对象的安全等级进行重新评估,并根据评估结果调整安全等级保护等级。当安全等级保护对象发生安全等级变化时,应从安全运行与维护阶段进入安全设计阶段,重新设计、建设和实施安全防护,并进行安全等级保护的要求。当安全等级保护对象发生安全等级变化时,应从安全运行与维护阶段进入安全运行与维护阶段,重新设计、建设和实施安全防护,并进行安全等级保护的要求。

在安全等级保护实施过程中,应定期或不定期对安全等级保护对象的安全等级进行重新评估,并根据评估结果调整安全等级保护等级。当安全等级保护对象发生安全等级变化时,应从安全运行与维护阶段进入安全设计阶段,重新设计、建设和实施安全防护,并进行安全等级保护的要求。当安全等级保护对象发生安全等级变化时,应从安全运行与维护阶段进入安全运行与维护阶段,重新设计、建设和实施安全防护,并进行安全等级保护的要求。

5 等级保护对象定级与备案

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

5.3 等级保护实施

主管部门可制定本行业/领域的定级指导意见,统一部署全行业/领域定级

主管部门应对本部门/单位定级结果进行审核、批准

5.3.2 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/职能/作用,确定履行主要社会功能/职
服务范围,最后依据分析和整理的内容,有

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
行业/领域定级指导意见的还应依据行业/领域定级意见

本行业/领域
本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

本行业/领域

GB/T 25058—2019

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：

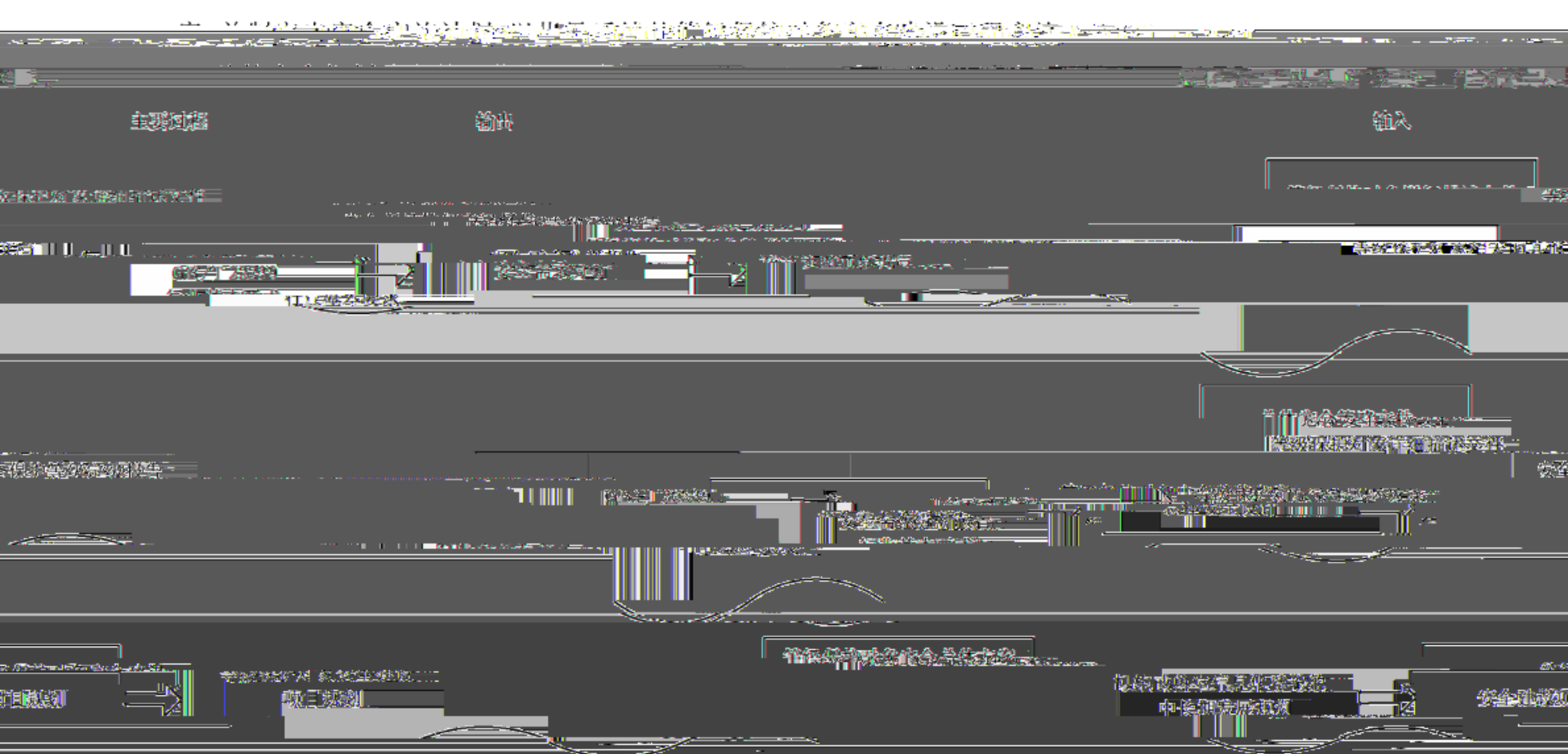


图3 识别安全风险与安全需求工作描述

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

全需求，并作为安全需求分析的基础。

活动描述：

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

全需求，并作为安全需求分析的基础。

活动描述：

本活动主要包括以下子活动内容：

- 1) 确定等级保护对象的安全保护等级；

能力。

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,结果造成

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: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

活动描述: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。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。根据基本安全需求和特殊的安全保护需求等形成

a) 等级保护对象描述

b) 基本安全需求描述

c) 安全保护等级描述。

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:

运营、使用单位,网络安全服务机构

参与角色

活动描述: ...

本活动主要内容包括如下系统内容:

a) 确定安全方针

政策和程序,且宜包括组织中人员职责,阐明安全工作职责和职责,宜以网络安全的总体目标,制定

5.1 制定安全策略

制定策略是系统安全工作的基础,制定安全策略是系统安全工作的首要任务,制定策略

制定策略和策略实施是制定策略的重要组成部分,制定策略和策略实施是制定策略的重要组成部分

活动输出是制定安全策略文件。

6.3.2 安全技术体系结构设计

活动目标:

根据 GB/T 25058 行业基本要求,安全需求分析报告

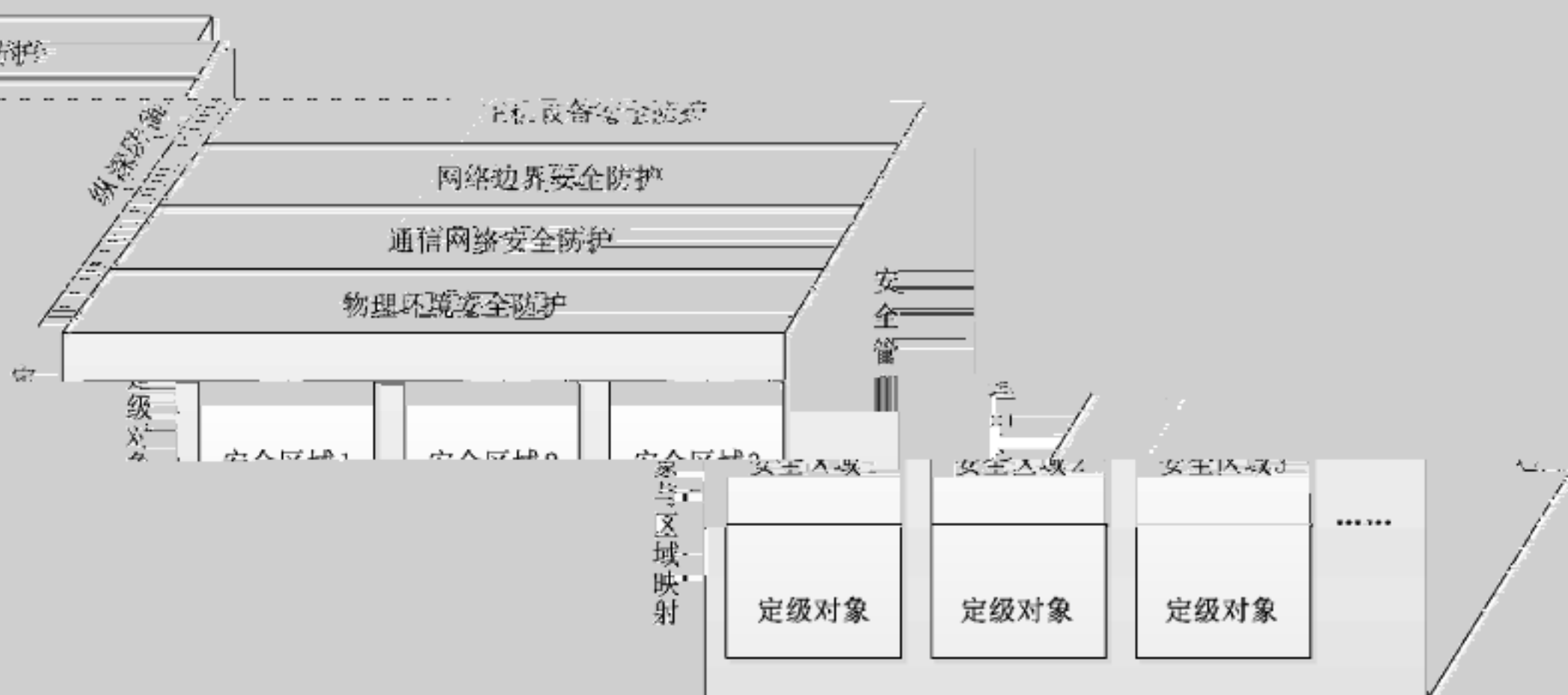


图 1 等级保护对象的安全技术体系架构

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、行业基本要求和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

等级保护对象的安全管理体系框架图

等级保护对象的安全管理体系框架图



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

及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

等级保护对象的安全管理体系框架图

等级保护对象的安全管理体系框架图

等级保护对象的安全管理体系框架图

等级保护对象的安全管理体系框架图

等级保护对象的安全管理体系框架图

安全管理策略等。

- 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

根据保护对象安全策略文件、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

- b) 规定网络安全的组织管理体制

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

网络安全策略等。

当安全策略级别定级对象

g) 规定不同级别定级对象安全事件处置和应急管理策略。

根据机构总体安全策略文档,等级保护基本要求系列标准,制定不同级别定级对象的安全事件处置和应急管理策略等。

B) 制定等级保护对象安全事件处置策略。

6.3.4 设计结果文档化

活动目标:

将等级保护建设产生的边界标识、资产清单、风险评估报告、安全策略、安全策略实施计划、等级保护对象安全管理策略等文档化。

参与角色:运营、使用单位、网络安全服务机构。

输出物:等级保护对象安全管理策略、等级保护对象安全管理策略实施计划。

输入物:等级保护对象安全管理策略、等级保护对象安全管理策略实施计划。

输出物:等级保护对象安全管理策略、等级保护对象安全管理策略实施计划。

输出物:等级保护对象安全管理策略、等级保护对象安全管理策略实施计划。

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:

根据等级保护对象安全建设总体规划,制定安全建设资金状况,确定各个时期的安全建设目标。

参与角色:运营、使用单位、网络安全服务机构。

输出物:等级保护对象安全建设总体规划、安全建设资金状况。

输入物:等级保护对象安全建设总体规划、安全建设资金状况。

输出物:等级保护对象安全建设总体规划、安全建设资金状况。

输出物:等级保护对象安全建设总体规划、安全建设资金状况。

输出物:等级保护对象安全建设总体规划、安全建设资金状况。

输出物:等级保护对象安全建设总体规划、安全建设资金状况。

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

参与角色:运营、使用单位;网络安全服务结构。

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;

将其适当分解为

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

能分解为和不限以下内容:

1) 网络安全建设;

2) 安全管理制度建设;

3) 安全管理平台建设;

4) 人员安全教育培训;

5) 安全风险评估与整改;

6) 安全应急响应与处置;

7) 安全监测与预警;

8) 安全审计与取证;

9) 安全加固与漏洞修复;

10) 安全培训与演练;

11) 安全评估与验收;

12) 安全运维与持续改进。

安全建设项目规划

6.4.3 形成安

活动目的

安全建设内容

活动输入

活动输出

活动描述

保护对象安全建设

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

护项目规划。

等级保护项目规划应包含以下要素:

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总体规划;

f) 安全建设目标和建设路线图;

g) 安全建设实施策略和保障措施等。

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

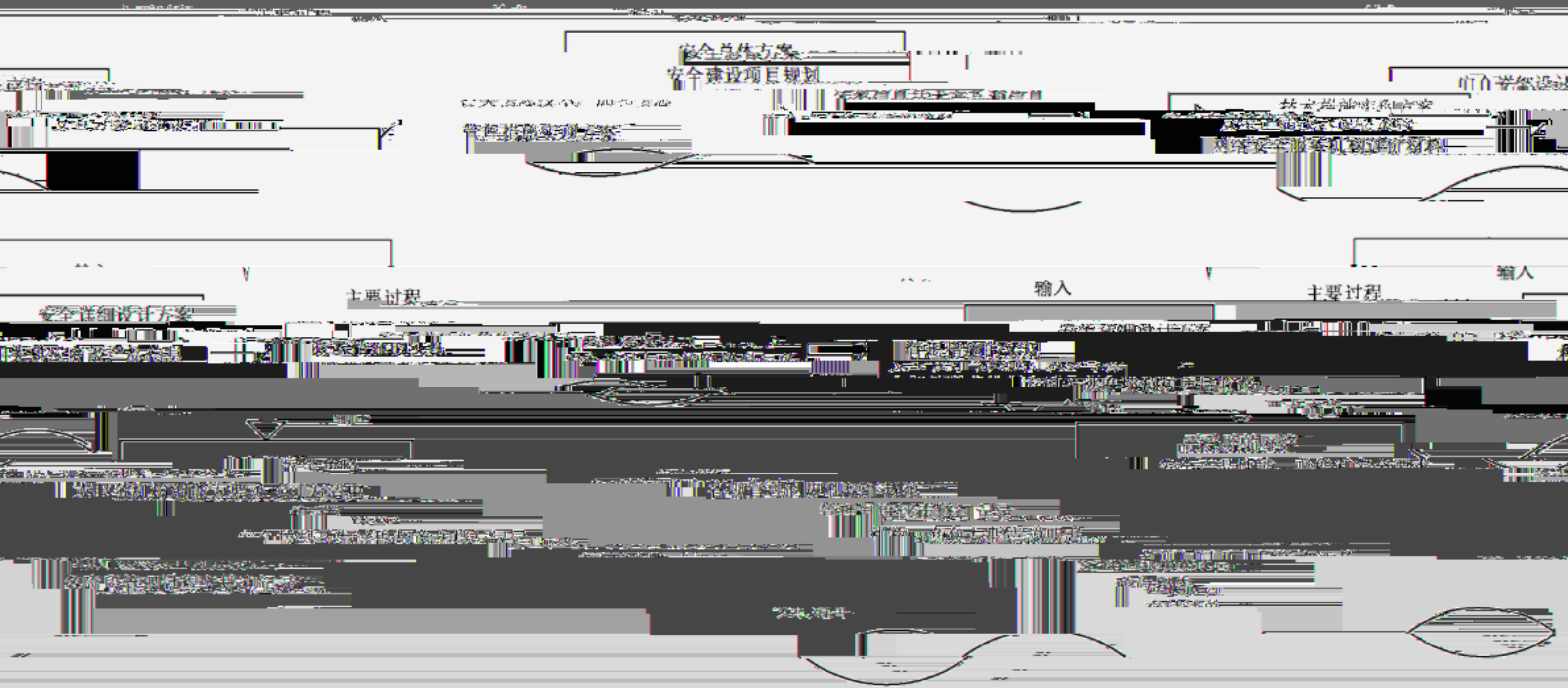


图 6 安全设计与实施阶段工作流程

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:

将产品需求整理成安全策略,安全策略体系结构,安全策略体系结构,安全措施和要
求落实到产品功能或物理形态上,相应能够实现的产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

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

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

b) 安全功能要求的设计

d) 部署方案的设计

部署方案

制定安全策略的实现计划

详细的安全策略实现计划

网络安全接入措施实施方案

网络安全接入措施实施方案内容摘要

活动目标

建设内容

参与角色(运营、使用单位、网络安全运营机构)

网络安全接入措施实施方案建设详细设计

建设内容

7.2.3 设计结果的文档化

活动目标

建设内容

参与角色(运营、使用单位、网络安全运营机构)

网络安全接入措施实施方案建设详细设计

建设内容

对技术措施实施方案中技术实施内容和管理措施实施等级保护对象安全建设详细设计方案

安全接入措施实施方案内容摘要

建设内容

建设内容

a) 建设目标和

b) 技术实现方

、网络接入方

网络安全接入措施实施方案建设详细设计

- 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

本活动的主要输出如下：

- a) 制定产品或服务采购说明。

网络安全产品或服务采购说明应详细描述安全详细设计方案中对于产品或服务采购的要求，制定产品或服务采购说明。

在依据产品或服务采购说明对现有产品或服务进行选择时，不仅要

在依据产品或服务采购说明对现有产品或服务进行选择时，不仅要

7.3.2 安全控制的开发

活动目标：

制定网络安全产品或服务的安全控制策略和配置，制定安全控制策略和配置。

制定安全控制策略和配置，制定安全控制策略和配置。

制定安全控制策略和配置，制定安全控制策略和配置。

制定安全控制策略和配置，制定安全控制策略和配置。

制定安全控制策略和配置，制定安全控制策略和配置。

制定安全控制策略和配置，制定安全控制策略和配置。

制定安全控制策略和配置，制定安全控制策略和配置。

制定安全控制策略和配置，制定安全控制策略和配置。

制定安全控制策略和配置，制定安全控制策略和配置。

制定安全控制策略和配置，制定安全控制策略和配置。

“煤炭行业安全生产标准化管理体系”的推广实施，为煤矿安全生产管理提供了有力支撑。

c) 调试

参考文献

1 GB 28181-2016 公共安全视频监控数字视音频编解码技术规范

附录A

活动输出：安全控制器的开发过程相关文档与记录

7.3.3 安全控制件成

活动日期：2019-01-01

安全控制件成：将各种应用系统综合、整合成一个系统，安全控制件成：将各种应用系统综合、整合成一个系统。

1. 安全控制件成：将各种应用系统综合、整合成一个系统。

2. 安全控制件成：将各种应用系统综合、整合成一个系统。

3. 安全控制件成：将各种应用系统综合、整合成一个系统。

4. 安全控制件成：将各种应用系统综合、整合成一个系统。

5. 安全控制件成：将各种应用系统综合、整合成一个系统。

6. 安全控制件成：将各种应用系统综合、整合成一个系统。

7. 安全控制件成：将各种应用系统综合、整合成一个系统。

8. 安全控制件成：将各种应用系统综合、整合成一个系统。

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

6.3 集成实施

6.3.1 集成实施过程应遵循“先集成、后实施”的原则，在集成过程中应充分考虑各子系统的兼容性、互操作性、可扩展性和可维护性，确保集成后的系统能够满足业务需求。

6.3.2 集成实施过程中应建立完善的沟通机制，定期召开集成实施会议，及时通报集成进度、存在的问题及解决方案，确保集成工作顺利进行。

- 6.3.2.1 形成安全控制集成报告。
- 6.3.2.2 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，其内容集成过程记录、变更控制、测试报告、验收报告、集成报告等。
- 6.3.2.3 活动输出包含安全控制集成报告。

6.4 总结验收

6.4.1 总结验收应在系统实施完成后进行，旨在验证系统是否满足业务需求，并评估系统的质量和性能。总结验收应包括系统验收测试、用户验收测试、性能测试、安全测试等。

6.4.2 总结验收过程中应建立完善的验收机制，明确验收标准、验收流程、验收责任和验收记录，确保验收工作规范、透明、公正。

- 6.4.2.1 制定验收计划。
- 6.4.2.2 按照验收计划在验收过程中进行验收。
- 6.4.2.3 记录验收过程。

6.4.3 总结验收完成后，应编制总结验收报告，详细记录验收过程、验收结果、存在的问题及改进措施，为后续系统运维提供依据。

6.4.4 总结验收过程中应建立完善的沟通机制，及时通报验收进度、存在的问题及解决方案，确保验收工作顺利进行。

6.4.5 总结验收完成后，应组织相关人员对系统实施过程进行回顾和总结，提炼经验教训，为后续项目实施提供参考。

6.4.6 总结验收过程中应建立完善的文档管理机制，确保验收过程文档的完整性、准确性和可追溯性。

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、行业、地方、企业等标准、规范和制度，结合企业实际情况，制定并完善与安全生产管理相适应的制度。

7.4.3 安全实施过程管理

活动目标：

在等级保护对象应用、规划设计、实施过程中，对工程的重要、关键、高风险等级的工作进行

遵循规范和科学管理

参与重点工程、重大项目、重要

1. 项目启动

2. 项目计划

3. 项目执行

4. 项目监控

5. 项目收尾

6. 项目评估

7. 项目总结

8. 项目归档

9. 项目移交

10. 项目验收

11. 项目报告

12. 项目反馈

13. 项目改进

14. 项目优化

15. 项目维护

16. 项目更新

17. 项目升级

18. 项目扩容

19. 项目迁移

20. 项目备份

21. 项目恢复

22. 项目灾难

23. 项目安全

24. 项目合规

25. 项目审计

26. 项目测试

27. 项目部署

28. 项目运行

29. 项目维护

30. 项目优化

31. 项目升级

32. 项目扩容

33. 项目迁移

34. 项目备份

35. 项目恢复

36. 项目灾难

37. 项目安全

38. 项目合规

39. 项目审计

40. 项目测试

41. 项目部署

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

包括安全运行工作机制和安全运行维护机制的建立、完善、运行、评估、改进、网络系

本标准关注安全运行与维护阶段的运行管理和控制,亦即管理和控制、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

8.2.1 运行管理职责确定

活动目的:

通过对运行管理活动或任务的角色划分,明确和职责,应至少划分参与角色与这些

授予相应的权限,来确定安全运行管理的具体人员

项目单位

活动输入: 安全策略、网络安全策略、安全组织架构表。

活动描述:

本活动主要包括以下子活动内容:

a) 识别运行管理控制:

识别: 识别安全保护等级的运行管理控制划分级别。

b) 授予管理权限:

根据: 安全保护等级和系统运行管

理: 安全保护等级要求的系统管

理: 安全保护等级要求的系统管

理: 安全保护等级要求的系统管

理: 安全保护等级要求的系统管

理: 安全保护等级要求的系统管

理: 安全保护等级要求的系统管

8.2.7 运行管理控制程序

8.2.7 运行管理控制程序

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。

运行管理控制程序应能识别运行管理控制。

运行管理控制程序应能识别运行管理控制。

运行、使用单位。

运行、使用单位。

识别运行管理控制: 识别运行管理控制。

识别运行管理控制: 识别运行管理控制。

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

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, 并制定后续的活动。

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:

识别: 识别变更需求。

要性和可行性。

更的必

变更影响分析

b)

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。

对
变更的

明确变更的类别

c)

8.3.1 制定变更方案

根据 a)、b) 或 c) 确定变更方案

活动输出: 变更方案

8.3.2 变更过程控制

活动目标:

确保运行与维护过程中的变更实施过程受到控制, 各项变化内容记录完整, 及时发现变更带来的影响

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。

b) 变更实施过程控制

按照批准的变更方案实施变更, 在变更过程中各类系统版本、各种操作活动等建立详细记录

c) 变更实施结果报告

整理、分析和总结各类数据, 形成变更结果报告, 并归档保存

收集变更过程中的各类相关文档

活动输出: 变更结果报告

4 安全状态监控

8.

4.1 监控对象确定

8.

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, 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。根据确定为监控对象,分析监控的必要性及可行性,监控的开销和成本等因素,

根据确定为监控对象,分析监控的必要性及可行性,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

运行监控

参与角色:运营、使用单位

活动输入:监控对象列表

活动输出:

本活动主要包含以下子活动内容:

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) 安全事件识别

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

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

根据对安全状况变化的分析,分

析响应。

c) 形成安全状态分析报告

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。

根据安全状态分析和影响分析的

活动输出:安全状态分析报告

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:

活动日期：_____

活动目标：

活动描述：

8.5.2 改进方案制定

活动日期：_____

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
安全措施一致有效地工作。

管理措施与各项补充的

本活动至少应包含以下子活动内容：

a) 安全方案实施控制

见7.4.3。

b) 安全措施测试与验收

见7.4.4。

c) 网络安全技术更新和系统漏洞修复

应制定网络安全更新和系统漏洞修复的安全策略，并定期更新和修复系统漏洞，确保安全策略和系统漏洞修复的安全策略得到落实。

8.3 服务商管理和监控

8.3.1 服务商选择

活动目标：

制定符合国家和行业规定的行业

参与制定行业安全标准

制定和发布安全策略

定期更新

本活动至少应包含以下子活动：

1) 制定安全策略

制定符合国家和行业规定的行业

参与制定行业安全标准

制定和发布安全策略

定期更新

本活动至少应包含以下子活动：

制定符合国家和行业规定的行业

参与制定行业安全标准

制定和发布安全策略

定期更新

本活动至少应包含以下子活动：

制定符合国家和行业规定的行业

参与制定行业安全标准

制定和发布安全策略

定期更新

本活动至少应包含以下子活动：

制定符合国家和行业规定的行业

参与制定行业安全标准

制定和发布安全策略

定期更新

本活动至少应包含以下子活动：

制定符合国家和行业规定的行业

参与制定行业安全标准

制定和发布安全策略

定期更新

8.3.2 服务商管理

活动目标：

制定符合国家和行业规定的行业

参与制定行业安全标准

制定和发布安全策略

定期更新

本活动至少应包含以下子活动：

本活动主要包括以下子活动内容：

a) 人员管理

人员的管理措施至少应包括但不限于：
——上岗资质审核、保密教育、品行管理、
——使用单位识别、服务规范及管理制度、信息安全、
——使用单位负责人签字、
——使用单位盖章对服务人员

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

- 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: 服务商公托评价报告

服务商公托评价报告应包含以下信息:

9.7 等级测评

活动目标:

8.8 监督检查

活动目标:

按照《信息安全等级保护管理办法》

规定,对信息系统的安全等级进行划分

并实施相应的

保护等级,确保信息系统的安全

8.9 应急响应与保障

8.9.1 应急准备

活动目标:

建立完善的应急响应组织体系,保障应急响应工作有序开展,通过公托安全事件的等级,在应急响应过程中,按照《信息安全等级保护管理办法》

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

明确应急组织内各成员的职责和权限,明确应急组织内各成员的职责和权限,明确应急组织内各成员的职责和权限。

c) 安全事件分类分级

根据安全事件的危害程度、影响范围、可控性、可预测性等因素,将安全事件分为不同的等级,并明确各等级安全事件的应急响应流程。

制定安全事件应急预案,明确安全事件发生时的应急响应流程,包括信息报告、应急处置、后期处置等各个环节。

定期开展应急演练,提高应急组织的应急处置能力和协同配合能力。

测与响应

8.9.2 应急监测

活动目标:

收集监测数据

活动描述:

本活动主要包含以下活动内容:

一是常态信息收集

二是应急响应信息收集

三是常态信息分析

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

及危害等级,形成安全状态分析报告和网络安全事件报告表,按照安全事件等级以及安全事件报告要求

8.9.3 后期评估与改进

活动目标:

对安全事件原因、处置过程进行复盘分析,并根据

参与角色进行复盘和改进。

活动输出:安全事件报告总结报告、复盘和改进

活动描述:

对安全事件处置过程进行复盘,总结经验教训。

改进措施

根据网络安全事件调查评估报告,制定改进措施,修改应急预案,结合复盘结果

8.9.4 应急保障

活动目标:

健全健全应急保障体系,实现应急预案保障工作科学化。

参与角色:运营、技术、安全。

活动输出:应急预案、各专项应急预案。

活动描述:

针对各专项应急预案进行分析,制定应急预案,并定期更新。

5 定级对象类

5.1 定级对象类去除段的工作流程

识别并记录设备清单，包括设备名称、设备编号、设备位置、设备状态、设备所属部门、设备负责人等。

3.1.1 设备清单

参与角色：系统管理员、操作人员。

活动输入：设备迁移或废弃清单等。

活动描述：

本活动主要包含以下子活动内容：

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，并记录设备名称、设备编号、设备位置、设备状态、设备所属部门、设备负责人等。

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，并记录设备名称、设备编号、设备位置、设备状态、设备所属部门、设备负责人等。

c) 处理方案审批

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，并记录设备名称、设备编号、设备位置、设备状态、设备所属部门、设备负责人等。

d) 设备迁移和记录

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，并记录设备名称、设备编号、设备位置、设备状态、设备所属部门、设备负责人等。

9.1 存储介质的清除或销毁

活动目标

清除或销毁

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。

清除或销毁的计算机介质清单，包括设备名称、设备编号、设备位置、设备状态、设备所属部门、设备负责人等。

参与角色：系统管理员、操作人员。

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，识别要被清除或销毁的存储介质，并记录设备名称、设备编号、设备位置、设备状态、设备所属部门、设备负责人等。

根据要终止的定级对象的存储介质清单，识别要被清除或销毁的存储介质，并记录设备名称、设备编号、设备位置、设备状态、设备所属部门、设备负责人等。

根据要终止的定级对象的存储介质清单，识别要被清除或销毁的存储介质，并记录设备名称、设备编号、设备位置、设备状态、设备所属部门、设备负责人等。

根据要终止的定级对象的存储介质清单，识别要被清除或销毁的存储介质，并记录设备名称、设备编号、设备位置、设备状态、设备所属部门、设备负责人等。

附录 A

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

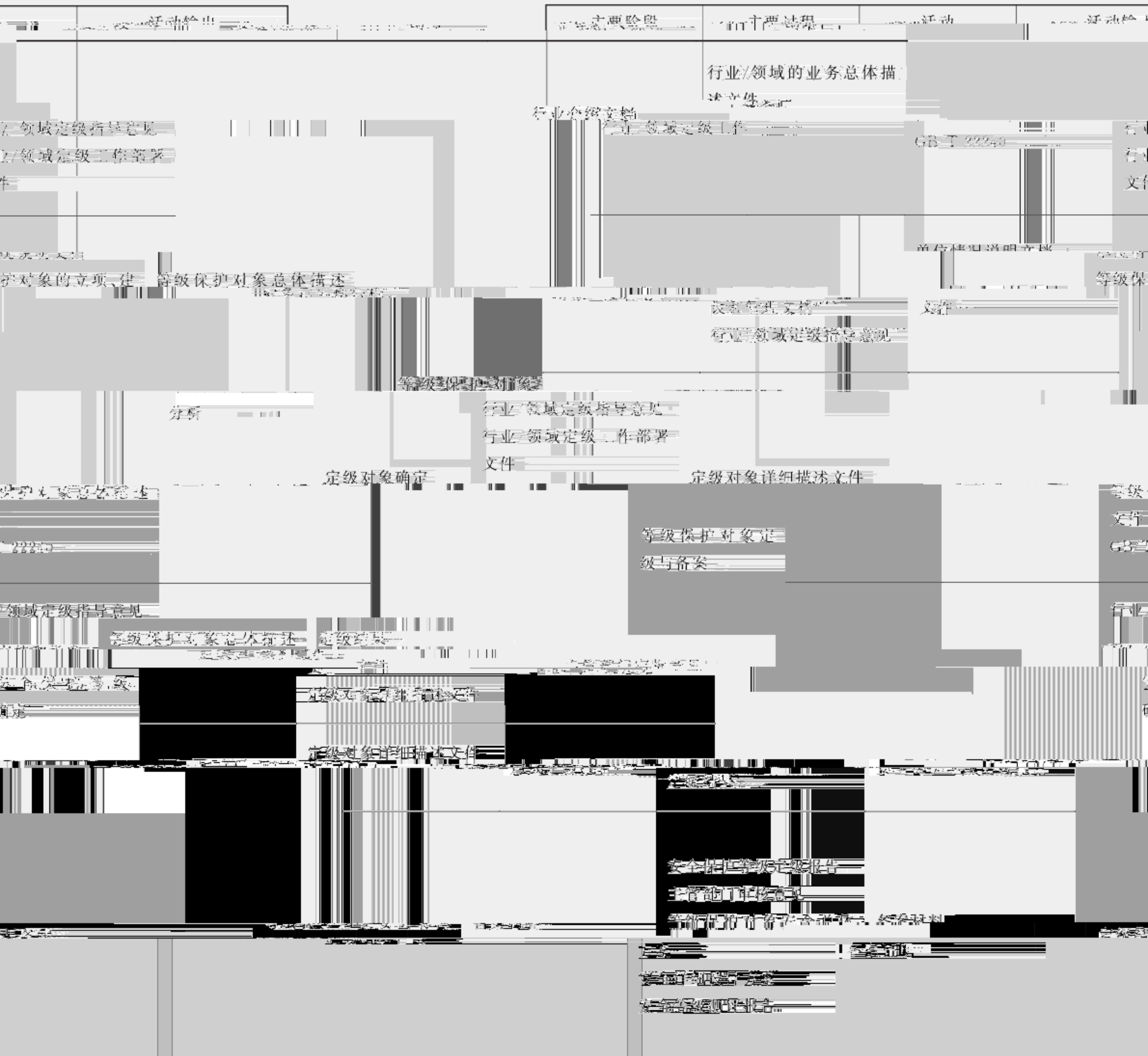


表 A.1 (续)

| 主要阶段 | 主要过程 | 活动 | 活动输入 | 活动输出 |
|------|----------------|--|--|--------------|
| | | 等级保护对象安全描述文件 | | 等级保护对象安全描述文件 |
| | | 安全保护等级定级报告 | | 安全保护等级定级报告 |
| | | GB/T 22239 | | |
| | | 行业基本要求 | | |
| | 安全需求分析 | 特殊安全需求的需求 | 等级保护对象详细描述文件 安全保护等级定级报告 等级保护对象安全描述文件 文档 | 重要资产的特殊保护需求 |
| | | 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 | 安全需求分析报告 |
| | 技术和安全需求 | | 重要资产的特殊保护需求 | |
| | 总体安全策略文件 | 安全需求分析概要 总体安全策略文件 等级保护对象详细描述文件 | 等级保护对象安全技术 | 总体安全策略文件 |
| | 安全技术体系结构 | 安全技术体系结构 | 等级保护对象安全技术 | |
| | 安全总体设计 | GB/T 22239 行业基本要求 总体安全策略文件 等级保护对象安全技术 | | |
| | 等级保护对象安全技术体系结构 | 安全保护等级定级报告 安全需求分析报告 | 等级保护对象安全技术体系结构 | |
| | 设计结果文档化 | | 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 等级保护对象安全技术体系结构 | 等级保护方案 |

表 A.1 (续)

| 主要阶段 | 主要过程 | 活动 | 活动输入 | 活动输出 |
|------------|------------|------------|------------------|------------------|
| 安全建设 确定 | 安全建设 确定 | 安全建设 确定 | 等级保护对象安全建设 规划 | 等级保护对象安全建设 规划 |
| | | 安全建设 确定 | 等级保护对象安全建设 规划 | 等级保护对象安全建设 规划 |
| 安全建设 实施 | 安全建设 实施 | 安全建设 实施 | 安全建设 实施 | 安全建设 实施 |
| 安全建设 验收 | 安全建设 验收 | 安全建设 验收 | 安全建设 验收 | 安全建设 验收 |
| 安全建设 维护 | 安全建设 维护 | 安全建设 维护 | 安全建设 维护 | 安全建设 维护 |
| 安全建设 改进 | 安全建设 改进 | 安全建设 改进 | 安全建设 改进 | 安全建设 改进 |
| 安全建设 总结 | 安全建设 总结 | 安全建设 总结 | 安全建设 总结 | 安全建设 总结 |
| 安全建设 评估 | 安全建设 评估 | 安全建设 评估 | 安全建设 评估 | 安全建设 评估 |
| 安全建设 培训 | 安全建设 培训 | 安全建设 培训 | 安全建设 培训 | 安全建设 培训 |
| 安全建设 宣传 | 安全建设 宣传 | 安全建设 宣传 | 安全建设 宣传 | 安全建设 宣传 |
| 安全建设 考核 | 安全建设 考核 | 安全建设 考核 | 安全建设 考核 | 安全建设 考核 |
| 安全建设 奖惩 | 安全建设 奖惩 | 安全建设 奖惩 | 安全建设 奖惩 | 安全建设 奖惩 |
| 安全建设 其他 | 安全建设 其他 | 安全建设 其他 | 安全建设 其他 | 安全建设 其他 |

表 A.1 (续)

| 活动 | 活动输入 | 活动输出 | 主要阶段 | 主要过程 |
|--------|----------|-----------|--------|--------|
| 变更管理 | 变更申请表 | 变更审批单 | 变更管理 | 变更管理 |
| 运行管理 | 运行规程 | 运行记录 | 运行管理 | 运行管理 |
| 安全状态分析 | 安全状态信息 | 安全状态分析报告 | 安全状态分析 | 安全状态分析 |
| 应急预案 | 应急预案编制指南 | 应急预案 | 应急预案编制 | 应急预案编制 |
| 应急演练 | 应急演练计划 | 应急演练报告 | 应急演练 | 应急演练 |
| 事故调查 | 事故调查报告 | 事故调查报告 | 事故调查 | 事故调查 |
| 安全培训 | 安全培训计划 | 安全培训记录 | 安全培训 | 安全培训 |
| 安全考核 | 安全考核试卷 | 安全考核成绩单 | 安全考核 | 安全考核 |
| 安全奖惩 | 安全奖惩制度 | 安全奖惩记录 | 安全奖惩 | 安全奖惩 |
| 安全文化建设 | 安全文化理念 | 安全文化成果 | 安全文化建设 | 安全文化建设 |
| 安全标准化 | 安全标准化规范 | 安全标准化自评报告 | 安全标准化 | 安全标准化 |
| 安全风险评估 | 安全风险评估表 | 安全风险评估报告 | 安全风险评估 | 安全风险评估 |
| 安全隐患排查 | 安全隐患排查表 | 安全隐患排查报告 | 安全隐患排查 | 安全隐患排查 |
| 安全整改 | 安全整改通知单 | 安全整改报告 | 安全整改 | 安全整改 |
| 安全验收 | 安全验收表 | 安全验收报告 | 安全验收 | 安全验收 |
| 安全总结 | 安全工作总结 | 安全工作总结报告 | 安全总结 | 安全总结 |

表 A.1 (续)

| 活动输入 | 活动输出 | 主要阶段 | 主要过程 | 活动 | 输出 |
|-----------|------------|------------|------------------|--------|----------|
| , 日志信息, 性 | 网络流量能信息等 | | | | |
| 定级对象终止 | 信息转移、留存和清除 | 定级对象信息资产清单 | 信息转移、留存、清除处理记录文档 | 定级对象终止 | 网络流量能信息等 |
| | 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 | 定级对象终止 | 网络流量能信息等 |
| | 存储介质的清除或销毁 | 存储介质的清除或销毁 | 存储介质的清除或销毁 | 定级对象终止 | 网络流量能信息等 |
| | 总体应急预案 | 总体应急预案 | 总体应急预案 | 定级对象终止 | 网络流量能信息等 |

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

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 2 号(100029)
16 号(100045)

北京海淀区中关村西街
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

版权专有 侵权必究



58-2019



GB/T 250