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 7.3.4。

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

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项目，网络安全风险点包括但不限于以下几点：

——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。

——服务商以往服务项目案例。

c） 服务内容互斥分析

在选择服务商时，需要识别服务商提供的服务与之前或后续提供的服务之间没有互斥性。承担等级保护对象安全建设服务的机构应具备等级保护安全建设服务机构资质。承担等级测评服务的机构具备等级测评机构资质。

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：

对服务商从多维度进行切实有效管理，使得服务商在约定范围内开展服务工作。

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。

——服务商人员在为使用单位提供服务的过程中，严格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，给使用单位或第三方造成人员人身伤害或财产损失的，服务商应承担赔偿责任。

——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

为确保服务商服务工作符合约定要求，服务商应满足但不限于：

——服务商提供齐全进场相关资料（如企业资质、人员资质、人员名单、物资资料等），并接受使用单位的审核。

——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；服务商保护好对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，实时跟踪服务商售后服务考核情况，作为后续服务商选择参考。

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，限时保质整改，确保服务商服务工作持续、规范、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） 使用单位负责组织制定服务评审标准及办法，并依据办法对服务质量进行评审；服务商应接受使用单位对其提供服务情况进行的监督和检查，并应及时按照使用单位要求对所提供的服务进行改进或调整，使服务质量符合使用单位要求。

b） 使用单位对服务商日常工作进行指导，当发现服务商工作中存在问题时，要求服务商及时纠正，因服务商原因（故意或过失）给使用单位造成损失的，服务商应承担全部赔偿责任。

c） 使用单位监管项目进展情况期间，对于重大情况服务商应及时主动报告。

d） 使用单位负责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，也可采用适合使用单位的考核方式；如发生严重违反合作原则、伤害使用单位利益、影响服务质量等行为，使用单位有权随时向服务商提出人员撤换要求。

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出具的安全等级测评报告，分析确定整改需求。

活动输出：安全等级测评报告，整改需求。

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，等级保护管理部门应按照国家、行业相关等级保护监督检查要求及标准，开展监督检查工作。

主管部门，运营、使用单位准备相应的监督检查材料，配合等级保护管理部门检查，确保等级保护对象符合安全保护相应等级的要求。

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：安全等级测评报告，备案材料，自查报告等。

活动描述：

等级保护管理部门、主管部门依据国家网络安全等级保护、行业监管要求等制定监督检查方案及表格；运营、使用单位根据网络安全保护等级保护监督检查、行业监管的规范或标准，准备相应的监督检查所需材料。

活动输出：监督检查材料，监督检查结果报告。

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，保证应急救援工作反应迅速、协调有序。通过分析安全事件的等级，在统一的应急预案框架下制定不同安全事件的应急预案。通过组织针对等级保护对象的应急演练，可以有效检验网络安全应急能力，并为消除或减小这些隐患与问题提供有价值的参考信息，检验应急预案体系的完整性、应急预案的可操作性、机构和应急人员的执行、协调能力以及应急保障资源的准备情况等，从而有助于提高整体应急能力。

参与角色：主管部门，运营、使用单位。

活动输入：运营、使用单位组织机构及职责分工，各类安全事件列表。

活动描述：

本活动主要包括以下子活动内容：

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

明确应急管理的领导机构、办事机构、专项应急指挥机构、基层应急机构、应急专家组组成部门或人员、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。

g） 培训宣贯

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

明确应急预案演练的规模、方式、范围、内容、组织、评估、总结等内容，并按照预案定期开展演练。

活动输出：应急组织机构图，应急组织职责分工，应急组织内、外部联系表，安全事件报告程序，各类专项应急预案，应急演练脚本，应急演练总结。

8.9.2 应急监测与响应

活动目标：

收集异常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，并根据应急预案启动条件研判是否启动应急程序。对监控到的安全事件采取适当的方法进行预处置，分析安全事件的影响程度和等级，启动相应级别的应急预案，开展应急响应处置工作。

参与角色：运营、使用单位。

活动输入：网络流量，日志信息，性能信息，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。

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

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标准和法律法规的变更信息。

b） 异常状态分析

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，分析其发展趋势及这些变化对安全状态的影响，通过判断他们的影响决定是否有必要作出响应。

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，按照安全事件等级以及安全事件报告程序上报，需要共享的按照规定向特定对象共享安全事件。

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流程和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，正确处理其中的敏感信息对于确保机构信息资产的安全是至关重要的。在等级保护对象生命周期中，有些定

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。

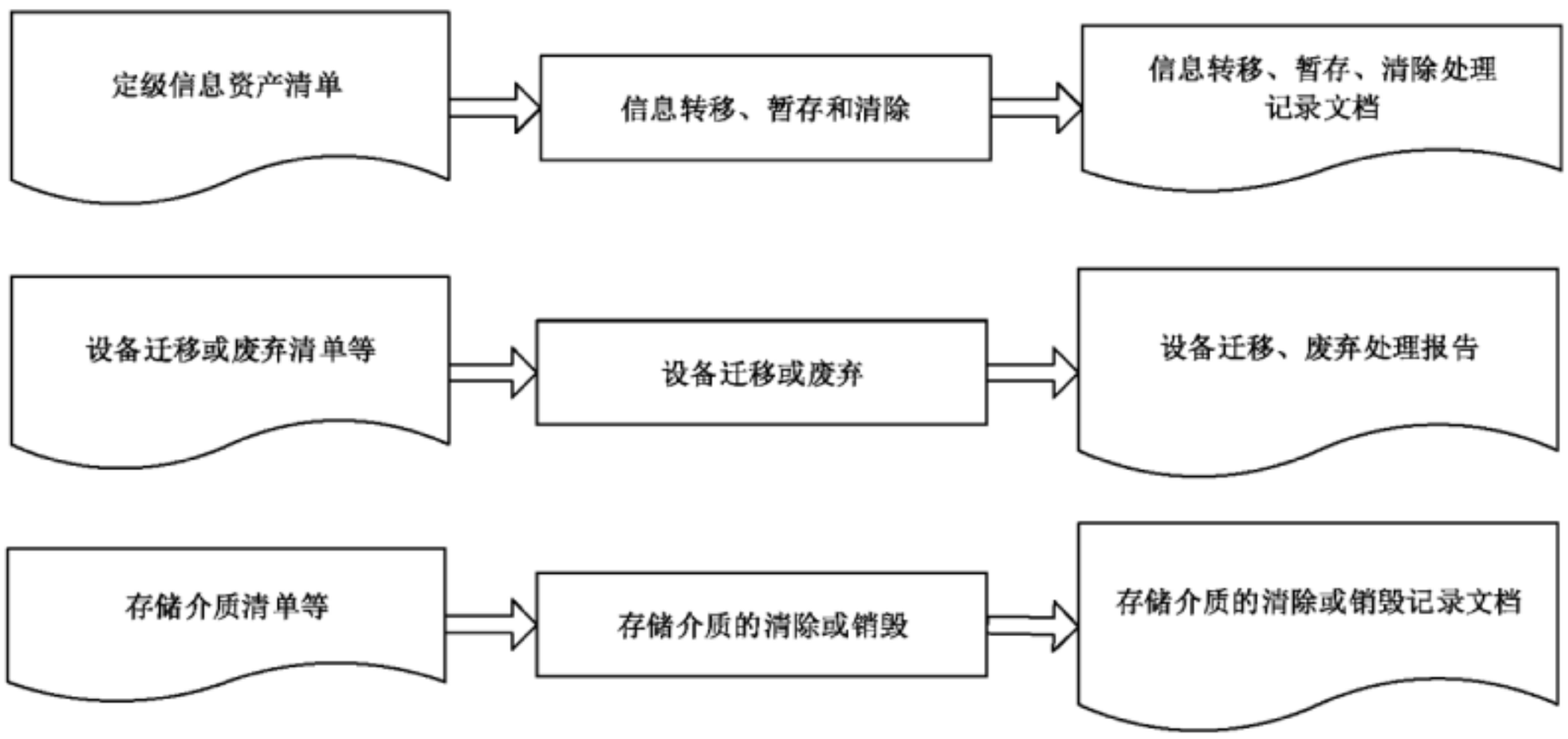

图 8　定级对象终止阶段工作流程

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

记录信息转移、暂存和清除的过程，包括参与的人员，转移、暂存和清除的方式以及目前信息所处的位置等。

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） 制定硬件设备处理方案

根据规定和实际情况制定设备处理方案，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

包括重用设备、废弃设备、敏感信息的清除方法等的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；记录设备处理过程，包括参与的人员、处理的方式、是否有残余信息的检查结果等。

活动输出：设备迁移、废弃处理报告。

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，防止介质内的敏感信息泄露。

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。对于存储涉密信息的介质应按照国家相关部门的规定进行处理。

c） 处理方案审批

包括存储介质的处理方式和处理流程等的处理方案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，包括参与的人员、处理的方式、是否有残余信息的检查结果等。

活动输出：存储介质的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
等级保护对象定级与备案	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
	等级保护对象分析	对象重要性分析	单位情况说明文档 等级保护对象的立项、建设和管理文档 行业/领域定级指导意见	等级保护对象总体描述文件
		定级对象确定	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	定级对象详细描述文件
	安全保护等级确定	定级、审核和批准	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	定级结果 主管部门审批意见
		形成定级报告	定级对象详细描述文件 定级结果	安全保护等级定级报告
	定级结果备案		安全保护等级定级报告 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	备案材料 备案证明

表 A.1（续）

主要阶段	主要过程	活动	活动输入	活动输出
总体安全规划	安全需求分析	基本安全需求的确定	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 GB/T 22239 行业基本要求	基本安全需求
		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
	安全总体设计	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
		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