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，通过网络安全总体方针、安全策略明确机构网络安全工作的总体目标、范围、原则等。第二层为网络安全管理制度，通过对网络安全活动中的各类内容建立管理制度，约束网络安全相关行为。第三层为安全技术标准、操作规程，通过对管理人员或操作人员执行的日常管理行为建立操作规程，规范网络安全管理制度的具体技术实现细节。第四层为记录、表单，网络安全管理制度、操作规程实施时需填写和需保留的表单、操作记录。

等级保护对象的安全管理体系框架见图 5。

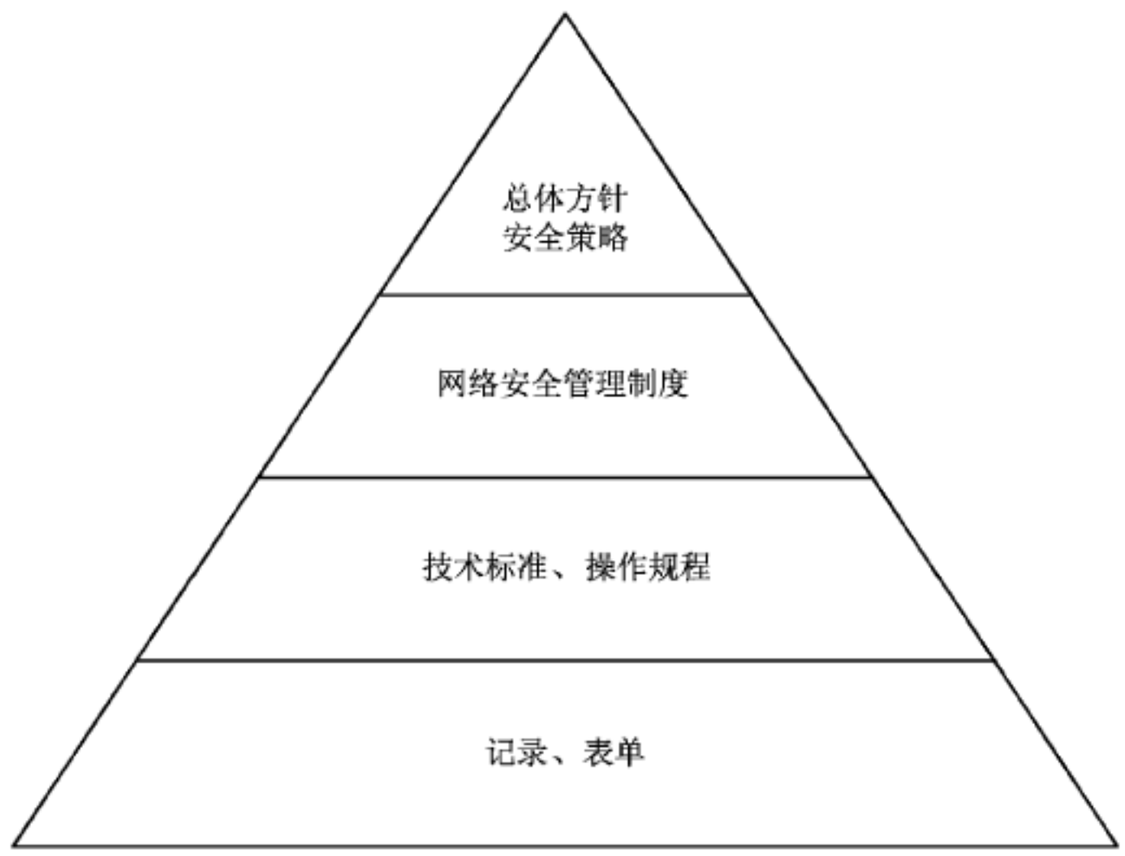

图 5 等级保护对象的安全管理体系框架

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，提出机构的安全组织管理机构框架，分配不同级别定级对象的安全管理职责、规定不同级别定级对象的安全管理策略等。

c） 规定不同级别定级对象的人员安全管理策略

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，提出不同级别定级对象的管理人员框架，分配不同级别定级对象的管理人员职责、规定不同级别定级对象的人员安全管理策略等。

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，提出各个不同级别定级对象的机房和办公环境的安全策略。

e） 规定不同级别定级对象介质、设备等的安全管理策略

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，提出各个不同级别定级对象的介质、设备等的安全策略。

f） 规定不同级别定级对象运行安全管理策略

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，提出各个不同级别定级对象的安全运行与维护框架和运维安全策略等。

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，提出各个不同级别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

将上述各个方面的安全管理策略进行整理、汇总，形成等级保护对象的整体安全管理体系结构。

活动输出：等级保护对象安全管理体系结构。

6.3.4 设计结果文档化

活动目标：

将总体安全设计工作的结果文档化，最后形成一套指导机构网络安全工作的指导性文件。

参与角色：运营、使用单位，网络安全服务机构。

活动输入：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。

活动描述：

对安全需求分析报告、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，形成等级保护对象总体安全方案。

等级保护对象总体安全方案包含以下内容：

a） 等级保护对象概述；

b） 总体安全策略；

c） 等级保护对象安全技术体系结构；

d） 等级保护对象安全管理体系结构。

活动输出：等级保护对象安全总体方案。

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：

依据等级保护对象安全总体方案（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构的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。

活动输入：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。

活动描述：

本活动主要包括以下子活动内容：

a） 信息化建设中长期发展规划和安全需求调查

了解和调查单位信息化建设的现况、中长期信息化建设的目标、主管部门对信息化的投入，对比信息化建设过程中阶段状态与安全策略规划之间的差距，分析急迫和关键的安全问题，考虑可以同步进行的安全建设内容等。

b） 提出等级保护对象安全建设分阶段目标

制定等级保护对象在规划期内（一般安全规划期为 3 年）所要实现的总体安全目标；制定等级保护对象短期（1 年以内）要实现的安全目标，主要解决目前急迫和关键的问题，争取在短期内安全状况有大幅度提高。

活动输出：等级保护对象分阶段安全建设目标。

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

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，并将其适当的分解。主要建设内容可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；

5） 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

将安全建设内容组合为不同的安全建设项目，描述项目所解决的主要安全问题及所要达到的安全目标，对项目进行支持或依赖等相关性分析，对项目进行紧迫性分析，对项目进行实施难易程度分析，对项目进行预期效果分析，描述项目的具体工作内容、建设方案，形成安全建设项目列表。

活动输出：安全建设项目列表（含安全建设内容）。

6.4.3 形成安全建设项目规划

活动目标：

根据建设目标和建设内容，在时间和经费上对安全建设项目列表进行总体考虑，分到不同的时期和阶段，设计建设顺序，进行投资估算，形成安全建设项目规划。

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，安全建设内容等。

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。

安全建设项目规划可包含以下内容：

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） 安全建设投资估算（含测试及运维估算等内容）；

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。

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。

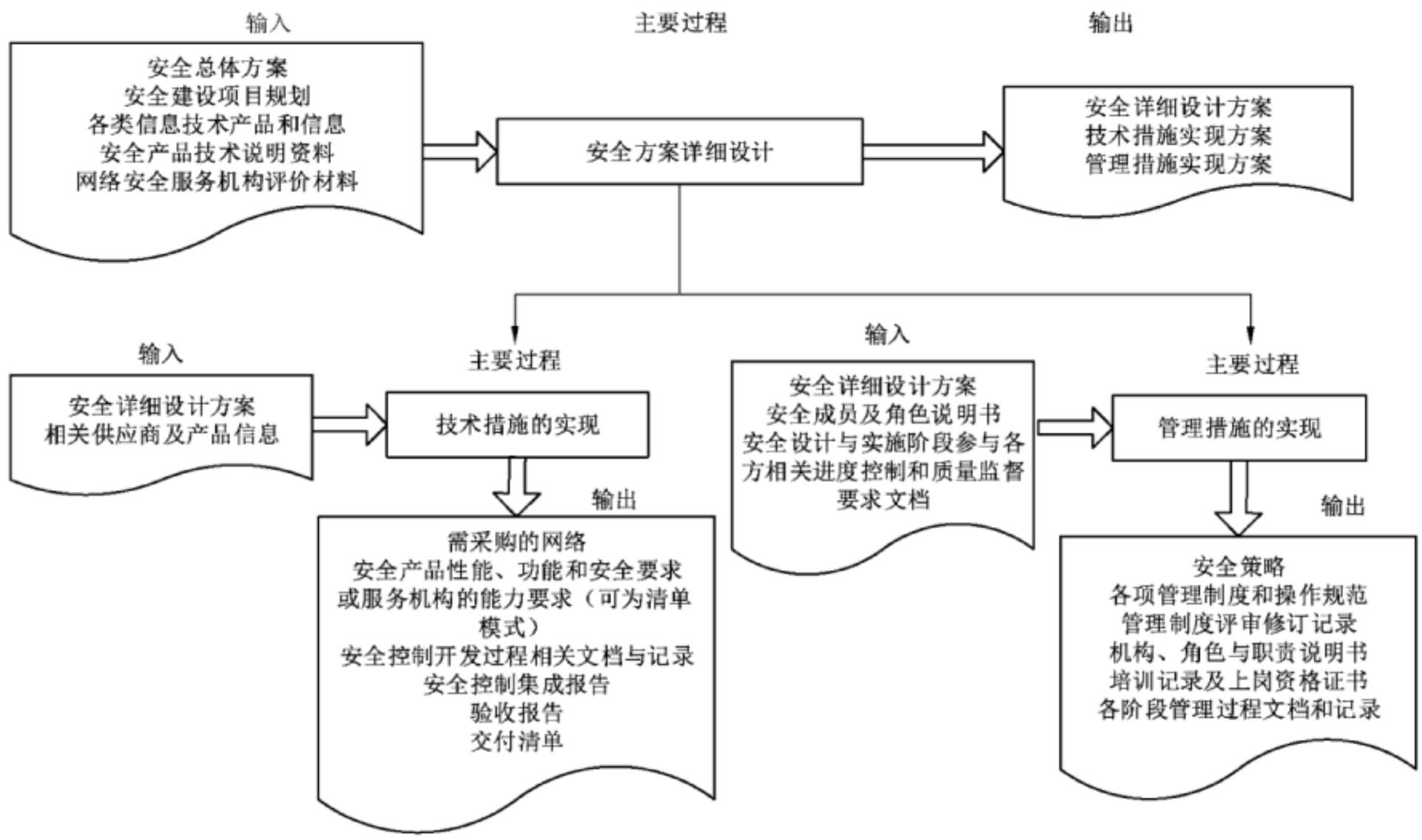

图 6 安全设计与实施阶段工作流程

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：

根据建设目标和建设内容将等级保护对象安全总体方案中要求实现的安全策略、安全技术体系结构、安全措施和要求落实到产品功能或物理形态上，提出能够实现的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阶段具有依据。

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技术说明资料、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

依据本次实施项目的建设内容和等级保护对象的实际情况，给出与总体安全规划阶段的安全体系结构一致的安全实现技术框架，内容至少包括安全防护的层次、网络安全产品的使用、网络子系统划分、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，以图示的方式给出安全技术实现框架的实现方式，包括网络安全产品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，给出网络调整的图示方案等。

e） 制定安全策略的实现计划

依据等级保护对象安全总体方案中提出的安全策略的要求，制定设计和设置网络安全产品或安全组件的安全策略实现计划。

活动输出：技术措施实施方案。

7.2.2 管理措施实现内容的设计

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等文档进行整理，形成等级保护对象安全建设详细设计方案。

安全详细设计方案包含以下内容：

a） 建设目标和建设内容；

b） 技术实现方案；

c） 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书，对产品或服务的采购原则、采购范围、技术指标要求、采购方式等方面进行说明。对于产品的功能、性能和安全性指标，可以依据第三方测试机构所出具的产品测试报告，也可以依据用户自行组织的网络安全产品功能、性能和安全性选型测试结果。对于安全服务的采购需求，应具有内部或外部针对网络安全服务机构的评价结果作为参考。

b) 选择产品或服务

在依据产品或服务采购说明书对现有产品或服务进行选择时，不仅要考虑产品或服务的使用环境、安全功能、成本(包括采购和维护成本)、易用性、可扩展性、与其他产品或服务的互动和兼容性等因素，还要考虑产品或服务的质量和可信性。产品或服务可信性是保证系统安全的基础，用户在选择网络安全产品时应确保符合国家关于网络安全产品使用的有关规定。对于密码产品的使用，应按照国家密码管理的相关规定进行选择和使用。对于网络安全服务，应选取有相关领域资质的网络安全服务机构。

活动输出：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(可为清单模式)。

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、开发来实现。安全控制的开发应与系统的应用开发同步设计、同步实施，而应用系统一旦开发完成后，再增加安全措施会造成很大的成本投入。因此，在应用系统开发的同时，要依据安全详细设计方案进行安全控制的开发设计，保证系统应用与安全控制同步建设。

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

以规范的形式准确表达安全方案设计中的指标要求，在采用云计算、移动互联等新技术情况下分析特有的安全威胁，确定对应的安全措施及其同其他系统相关的接口细节。

b） 概要设计

概要设计要考虑安全方案中关于身份鉴别、访问控制、安全审计、软件容错、资源控制、数据完整性、数据保密性、数据备份恢复、剩余信息保护和个人信息保护等方面的指标要求，设计安全措施模块的体系结构，定义开发安全措施的模块组成，定义每个模块的主要功能和模块之间的接口。

c） 详细设计

依据概要设计说明书，将安全控制的开发进一步细化，对每个安全功能模块的接口，函数要求，各接口之间的关系，各部分的内在实现机理都要进行详细的分析和细化设计。

按照功能的需求和模块划分进行各个部分的详细设计，包含接口设计和管理方式设计等。详细设计是设计人员根据概要设计书进行模块设计，将总体设计所获得的模块按照单元、程序、过程的顺序逐步细化，详细定义各个单元的数据结构、程序的实现算法以及程序、单元、模块之间的接口等，作为以后编码工作的依据。

d） 编码实现

按照设计进行硬件调试和软件的编码，在编码和开发过程中，要关注硬件组合的安全性和编码的安全性，开展论证和测试，并保留论证和测试记录。

e） 测试

开发基本完成要进行功能和安全性测试，保证功能和安全性的实现。安全性测试需要涵盖基线安全配置扫描和渗透测试，第三级以上系统应进行源代码安全审核。如有行业内或新技术专项要求，应开展专项测试，如国家电子政务领域的网络安全等级保护三级测评、云计算环境安全控制措施测评、移动终端应用软件安全测试等。

f） 安全控制的开发过程文档化

安全控制的开发过程需要将概要设计说明书、详细设计说明书、开发测试报告以及开发说明书等整理归档。

活动输出：安全控制的开发过程相关文档与记录。

7.3.3 安全控制集成

活动目标：

将不同的软硬件产品进行集成，依据安全详细设计方案，将网络安全产品、系统软件平台和开发的安全控制模块与各种应用系统综合、整合成为一个系统。安全控制集成的过程可以运营、使用单位与网络安全服务机构共同参与、相互配合，把安全实施、风险控制、质量控制等有机结合起来，实现安全态势感知、监测通报预警、应急处置追踪溯源等安全措施，构建统一安全管理平台。

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） 集成实施方案制定

主要工作内容是制定集成实施方案，集成实施方案的目标是具体指导工程的建设内容、方法和规范等，实施方案有别于安全设计方案的一个显著特征是其可操作性很强，要具体落实到产品的安装、部署和配置中，实施方案是工程建设的具体指导文件。

b） 集成准备

主要工作内容是对实施环境进行准备，包括硬件设备准备、软件系统准备、环境准备。为了保证系统实施的质量，网络安全服务机构应依据系统设计方案，制定一套可行的系统质量控制方案，以便有效