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、工程质量问题的处理流程、系统实施人员的职责要求等，并提供详细的安全控制集成进度表。

c） 集成实施

主要工作内容是将配置好策略的网络安全产品和开发控制模块部署到实际的应用环境中，并调整相关策略。集成实施应严格按照集成进度安排进行，出现问题各方应及时沟通。系统实施的各个环节应遵照质量控制方案的要求，分别进行系统集成测试，逐步实现质量控制目标。例如：综合布线系统施工过程中，应及时利用网络测试仪测定线路质量，及早发现并解决质量问题。

d） 培训

等级保护对象建设完成后，安全服务提供商应向运营、使用单位提供等级保护对象使用说明书及建设过程文档，同时需要对系统维护人员进行必要培训，培训效果的好坏将直接影响到今后系统能否安全运行。

e） 形成安全控制集成报告

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，其包含集成实施方案、质量控制方案、集成实施报告以及培训考核记录等内容。

活动输出：安全控制集成报告。

### 7.3.4 系统验收

活动目标：

检验系统是否严格按照安全详细设计方案进行建设，是否实现了设计的功能、性能和安全性。在安全控制集成工作完成后，系统测试及验收是从总体出发，对整个系统进行集成性安全测试，包括对系统运行效率和可靠性的测试，也包括管理措施落实内容的验收。

参与角色：运营、使用单位，网络安全服务机构，测试机构。

活动输入：安全详细设计方案，安全控制集成报告。

活动描述：

本活动主要包括以下子活动内容：

a） 系统验收准备

安全控制的开发、集成完成后，要根据安全设计方案中需要达到的安全目标，准备验收方案。验收方案应立足于合同条款、需求说明书和安全设计方案，充分体现用户的安全需求。

成立验收工作组对验收方案进行审核，组织制定验收计划、定义验收的方法和验收通过准则。

b） 组织验收

由验收工作组按照验收计划负责组织实施，组织测试人员根据已通过评审的系统验收方案对等级保护对象进行验收测试。验收测试内容结合详细设计方案，对等级保护对象的功能、性能和安全性进行测试，其中功能测试涵盖功能性、可靠性、易用性、维护性、可移植性等，性能测试涵盖时间特性和资源特性，安全性测试涵盖计算环境、区域边界和通信网络的安全机制验证。

c） 验收报告

在测试完成后形成验收报告，验收报告需要用户与建设方进行确认。验收报告将明确给出验收的结论，安全服务提供商应根据验收意见尽快修正有关问题，重新进行验收或者转入合同争议处理程序。如果是网络安全等级保护三级（含）以上的等级保护对象，需提交等级保护测评报告作为验收必要文档。

d） 系统交付

在等级保护对象验收通过以后，要进行等级保护对象的交付，需要安全服务机构提交系统建设过程中的文档、指导用户进行系统运行维护的文档、服务承诺书等。

活动输出：验收报告、交付清单。

### 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全管理相配套的、包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循的行为规范和操作规程。

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、远程访问管理、特殊权限管理、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范性。

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。根据实际环境和情况的变化，对制度进行修改和完善，规范总体安全方针、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，必要时考虑管理制度的重新制定，并保留版本修订记录。

活动输出：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。

#### 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，通过管理机构的岗位设置、人员的分工和岗位培训以及各种资源的配备，保证人员具有与其岗位职责相适应的技术能力和管理能力，为等级保护对象的安全管理提供组织上的保障。

参与角色：运营、使用单位，等级保护对象管理人员，网络安全服务机构。

活动输入：安全详细设计方案，安全成员及角色说明书，各项管理制度和操作规范。

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、系统管理员、安全管理员等，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，并要征求相关人员的意见，要保证责任明确，确保所有的风险都有人负责应对。

c） 人员安全管理

针对普通员工、管理员、开发人员、主管人员以及安全人员开展特定技能培训和安全意识培训，培训后进行考核，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。

活动描述：

本活动主要包括以下子活动内容：

a） 整体管理

整体管理需要在等级保护对象建设的整个生命周期内，围绕等级保护对象安全级别的确定、整体计划制定、执行和控制，通过资源的整合将等级保护对象建设过程中所有的组成要素在恰当的时间、正确的地方、合适的人物结合在一起，在相互影响的具体目标和方案中权衡和选择，尽可能地消除各单项管理的局限性，保证各要素（进度、成本、质量和资源等）相互协调。

b） 质量管理

在创建等级保护对象的过程中，要建立一个不断测试和改进质量的过程，在整个等级保护对象的生命周期中，通过测量、分析和修正活动，保证所完成目标和过程的质量。

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，风险管理要贯穿始终。

d） 变更管理

在等级保护对象建设的过程中，由于各种条件的变化，会导致变更的出现，变更发生在工程的范围、进度、质量、成本、人力资源、沟通和合同等多方面。每一次的变更处理，应遵循同样的程序，即相同的文字报告、相同的管理办法、相同的监控过程。应确定每一次变更对系统成本、进度、风险和技术要求的影响。一旦批准变更，应设定一个程序来执行变更。

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交付成果，同时也要求有结束的日期。因此在建设等级保护对象的过程中，应制订项目进度计划，绘制进度网络图，将系统分解为不同的子任务，并进行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，在等级保护对象建设的过程中，针对每个环节都有大量的文档输出，文档管理涉及等级保护对象建设的各个环节，主要包括：系统定级、规划设计、方案设计、安全实施、系统验收、人员培训等方面。

活动输出：各阶段管理过程文档和记录。

## 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。

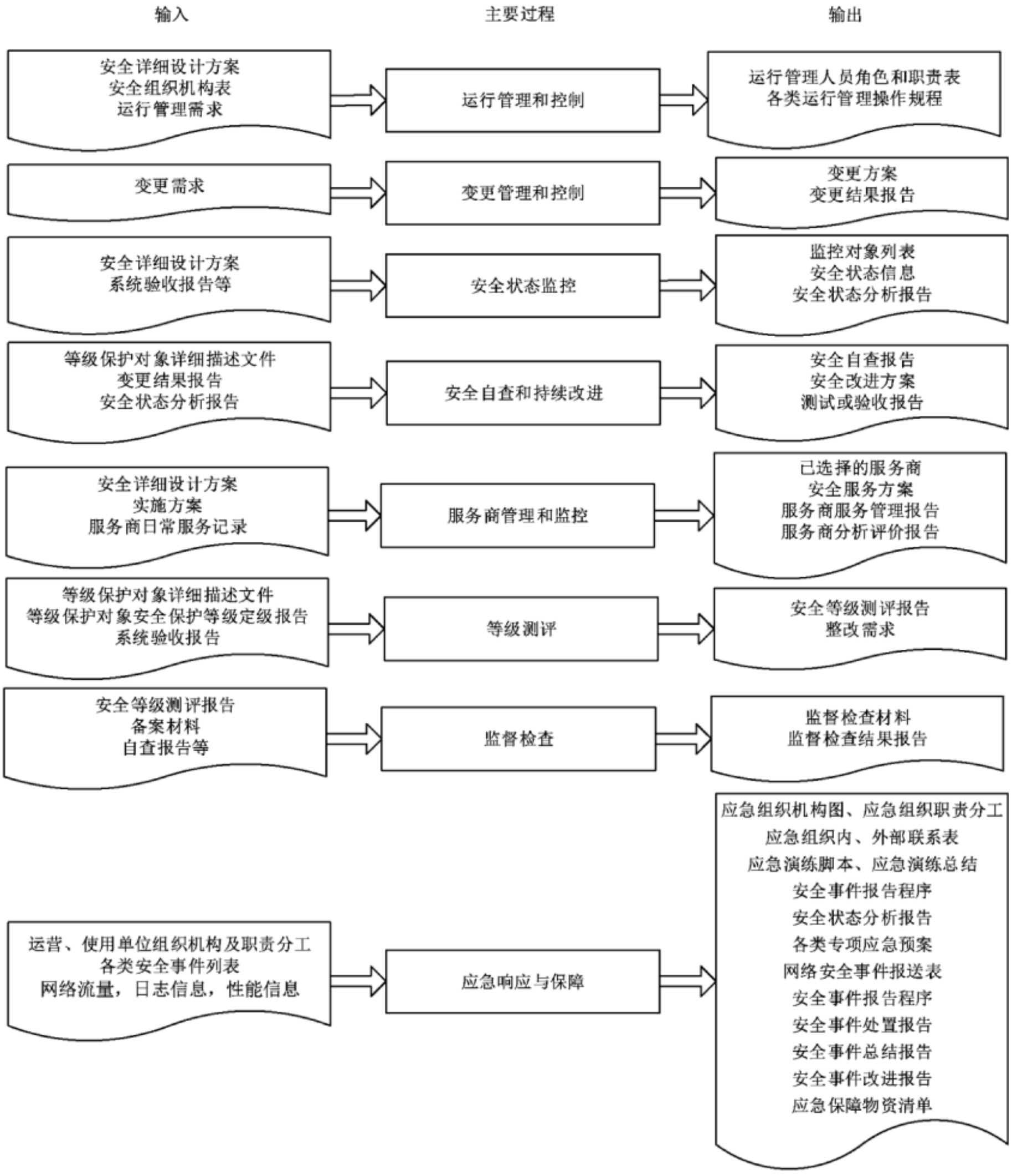


图7　安全运行与维护阶段工作流程

## 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

根据管理制度和实际运行管理需要，由安全管理员授予每一个运行管理角色及用户不同的管理权限。安全保护等级越高的系统管理权限的划分也越细。

c） 定义人员职责

根据不同的安全保护等级要求的控制粒度，分析所需要运行管理控制内容，并以此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、操作方法和流程等，并进行操作过程记录，确保对操作过程进行控制。

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、数据库操作规程等。安全保护等级越高的系统，对更多的操作要形成操作规程文件。

b） 操作过程记录

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，来确定变更的类别，计划后续的活动内容。

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，确定变更的内容、变更资源需求和变更范围等，判断变

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

确定等级保护对象是局部调整还是重大变更。如果是由等级保护对象类型发生变化、承载的信息资产类型发生变化、等级保护对象服务范围发生变化和业务处理自动化程度发生变化等原因引起等级保护对象安全保护等级发生变化的重大变更，则需要重新确定等级保护对象安全保护等级，返回到等级保护实施过程的等级保护对象定级阶段。如果是局部调整，则确定需要配套进行的其他工作内容。

d） 制定变更方案

根据 a）、b）、c）的结果制定变更方案。

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，各项变化内容进行记录，保证变更对业务的影响最小。

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） 建立变更过程日志

按照批准的变更方案实施变更，对变更过程各类系统状态、各种操作活动等建立操作记录或日志。

c） 形成变更结果报告

收集变更过程的各类相关文档，整理、分析和总结各类数据，形成变更结果报告，并归档保存。

活动输出：变更结果报告。

### 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影响的因素，即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墙、入侵检测、防病毒、核心路由器、核心交换机、主要通信线路、关键服务器或客户端等系统范围内的对象；也可能包括安全标准和法律法规等外部对象。

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综合。

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；或者是来自外部环境的安全标准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） 制定自查计划和自查方案

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和安全自查方案，说明安全自查的范围、对象、工作方法等，准备安全自查需要的各类表单和工具。

c） 安全自查实施

根据安全自查计划，通过询问、检查和测试等多种手段，进行安全状况自查，记录各种自查活动的结果数据，分析安全措施的有效性、安全事件产生的可能性和定级对象的实际改进需求等。

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，并产生安全自查报告。将安全自查过程的各类文档、资料归档保存。

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保护实施的一个新的循环过程；如果安全保护等级不变，但是调整内容较多、涉及范围较大，则应对安全改进项目进行立项，重新开始安全实施/实现过程，参见第7章；如果调整内容较小，则可以直接进行安全改进实施。

b） 制定安全改进方案

确定安全改进的工作方法、工作内容、人员分工、时间计划等，制定安全改进方案。安全改进方案只适用于小范围内的安全改进，如安全加固、配置加强、系统补丁等。

活动输出：安全改进方案。

### 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：