信息安全运维中的风险评估体系构建

唐 颖 雷 琪 李新迪
上海外高桥造船有限公司 上海 200137

摘 要：信息安全运维中的风险评估体系构建是确保信息系统安全的关键环节。该体系通过识别资产、威胁与脆弱性，采用定性与定量评估方法，结合先进工具与平台，实现风险的精准量化与有效管理。通过持续监控、定期审计及合规性检查，不断优化评估流程，确保信息安全运维的高效与可靠，为组织提供坚实的信息安全保障基础。

关键词：信息安全运维；风险评估；体系构建

引言：随着信息技术的飞速发展，信息安全已成为各组织不可忽视的重要议题。信息安全运维中的风险评估体系作为预防与应对安全威胁的核心机制，旨在通过系统化、规范化的流程，识别、分析并处置潜在的信息安全风险。构建这一体系，对于提升组织的信息安全防护能力、确保业务连续性具有重要意义，是保障信息安全、促进业务稳健发展的基石。

1 信息安全风险评估基础

1.1 信息安全风险定义及分类

1.1.1 定义及主要类型

信息安全风险是指因人为或自然因素导致信息系统资产遭受破坏、泄露、篡改等，从而引发组织利益受损的可能性及后果的组合。主要类型包括：网络攻击风险（如病毒入侵、DDoS攻击）、数据安全风险（数据泄露、篡改）、系统漏洞风险（软件缺陷、配置不当）、物理安全风险（设备被盗、环境灾害）、管理风险（人员操作失误、权限滥用）等。

1.1.2 产生原因及影响因素

产生原因分为外部与内部：外部包括黑客攻击、恶意代码传播、供应链攻击等；内部涉及人员操作失误、安全意识薄弱、管理制度缺失等。影响因素包括资产价值（价值越高风险影响越大）、威胁频率（攻击次数越频繁风险概率越高）、脆弱性程度（系统漏洞越多风险越易发生）、现有防护措施有效性（防护不足会放大风险）[1]。

1.2 信息安全风险评估原则及流程

1.2.1 基本原则

需遵循客观性原则（基于事实数据，避免主观臆断）、系统性原则（全面覆盖资产、威胁、脆弱性等要素）、动态性原则（定期更新评估，适应环境变化）、保密性原则（保护评估过程中涉及的敏感信息）、可控性原则（确保评估过程可追溯、结果可验证）。

1.2.2 典型流程

（1）资产识别：梳理硬件、软件、数据、服务等资产，评估其机密性、完整性、可用性价值。（2）威胁识别：识别可能利用脆弱性的威胁源（如黑客、恶意软件）及威胁事件（如入侵、数据窃取）。（3）脆弱性分析：找出系统在技术、管理等方面的漏洞（如未打补丁、权限混乱）。（4）风险分析：结合资产价值、威胁发生概率、脆弱性被利用可能性，计算风险等级。（5）风险评价：对照风险接受标准，判断风险是否可接受，确定需处理的风险。（6）风险处置：采取规避、转移、降低、接受等措施处理风险，并监控处置效果。

2 信息安全运维中的风险评估体系构建

2.1 风险评估体系架构

2.1.1 整体架构

信息安全运维风险评估体系采用“三层四维”架构。三层包括基础层（硬件设施、网络环境、操作系统等支撑性资源）、管控层（安全制度、流程规范、组织架构等管理机制）、应用层（业务系统、数据平台、运维工具等核心应用）；四维涵盖资产维度（资产识别与价值评估）、威胁维度（威胁监测与分析）、脆弱性维度（漏洞管理与修复）、应急维度（风险处置与响应）。

2.1.2 各组成部分功能及相互关系

基础层为体系提供运行载体，支撑管控层和应用层的功能实现，如服务器、网络设备等硬件是风险数据采集的物理基础。管控层负责制定评估规则、协调资源调度，指导基础层的安全配置和应用层的风险评估执行，例如安全制度规范了漏洞扫描的频率和标准。应用层是风险评估的核心对象，其运行状态数据反馈至管控层，驱动评估流程优化。四维要素中，资产维度是评估起点，威胁和脆弱性维度基于资产属性展开分析，应急维度则根据前三者的评估结果制定处置策略，形成“识别-分析-处置-反馈”的闭环[2]。

2.2 关键要素识别与评估

2.2.1 关键资产识别

（1）硬件：核心服务器（数据库服务器、应用服务器）、网络设备（防火墙、路由器）、终端设备（运维工作站、移动设备）。（2）软件：操作系统（WindowsServer、Linux）、数据库系统（MySQL、Oracle）、业务应用软件（ERP系统、CRM系统）、安全软件（杀毒软件、入侵检测系统）。（3）数据：客户信息、交易记录、核心技术文档、账号密码等敏感数据，以及系统日志、配置文件等运维数据。（4）人员：运维工程师、安全分析师、系统管理员等掌握核心权限的岗位人员。

2.2.2 资产价值评估

（1）保密性：客户信息、核心技术文档等敏感数据保密性价值最高，一旦泄露可能引发法律风险和声誉损失；系统日志等非敏感数据保密性价值较低。（2）完整性：交易记录、财务数据等需确保数据准确无误，完整性价值突出；临时缓存数据完整性要求相对较低。（3）可用性：核心业务系统（如电商平台交易系统）可用性价值极高，中断1小时可能造成巨额经济损失；内部测试系统可用性价值较低[3]。

2.2.3 潜在威胁及脆弱性

（1）威胁：外部包括黑客入侵、勒索病毒攻击、DDoS攻击；内部包括误操作（如误删除数据）、恶意篡改（如修改配置文件）。（2）脆弱性：技术层面（未及时修复系统漏洞、弱密码策略）、管理层面（运维流程不规范、权限划分模糊）、人员层面（安全意识薄弱、缺乏专业培训）。

2.3 风险评估方法与技术

2.3.1 常用评估方法

（1）定性评估：通过专家打分、问卷调查等方式，将风险等级划分为“高、中、低”，适用于缺乏量化数据的场景，操作简单但主观性较强。（2）定量评估：运用数学模型（如风险值 = 威胁概率×资产价值×脆弱性程度）计算具体数值，结果精确但需大量历史数据支撑，适用于核心业务系统。（3）定性与定量结合：先通过定性评估筛选关键风险点，再对重点风险进行定量分析，平衡准确性与效率，是运维中最常用的方法。

2.3.2 适用技术

（1）漏洞扫描：利用工具（如Nessus）自动检测系统漏洞，快速发现潜在风险，适用于大规模网络设备和服务器的定期巡检。（2）渗透测试：模拟黑客攻击流程，手动挖掘系统深层漏洞，针对性强，常用于重大版本更新或安全事件后的深度评估。（3）安全审计：通过分析日志（如系统日志、操作日志），追踪违规行为，识别运维过程中的管理漏洞，适用于常态化合规性检查[4]。

2.4 风险评估工具与平台

2.4.1 工具与平台推荐

（1）漏洞扫描工具：Nessus（优点：漏洞库更新快、支持多平台；缺点：高级功能需付费，适用于中小型企业）、OpenVAS（优点：开源免费；缺点：扫描速度较慢，适用于预算有限的组织）。（2）安全管理平台：IBMQRadar（优点：集成日志分析、威胁检测功能；缺点：部署复杂、成本高，适用于大型企业）、AliyunSecurityCenter（优点：云原生架构、易于扩展；缺点：对私有部署支持有限，适用于云环境为主的企业）。（3）渗透测试工具：Metasploit（优点：模块丰富、支持定制化攻击；缺点：需专业人员操作，适用于安全团队进行深度测试）。

2.4.2 有效利用建议

（1）工具组合使用：漏洞扫描工具与渗透测试工具配合，先通过扫描定位基础漏洞，再通过渗透测试验证漏洞可利用性。（2）平台联动：将安全管理平台与运维监控系统（如Zabbix）对接，实现风险数据实时同步，提升评估时效性。（3）定期更新与校准：根据新漏洞信息更新工具库，结合人工复核修正工具误报，确保评估结果准确性。（4）人员培训：组织工具操作培训，提升运维人员对工具的使用熟练度，充分发挥工具效能。

3 风险评估体系在信息安全运维中的应用实践

3.1 应用案例分析

3.1.1 典型场景应用过程及效果

以能源行业工控系统（SCADA）为例，应用过程如下：通过资产识别锁定PLC控制器、数据采集服务器、调度终端等核心资产，采用定性与定量结合法评估可用性价值（停机1小时损失超50万元）；利用工控漏洞扫描工具发现“固件版本过旧”“协议缺乏加密”等2项高危风险；结合威胁情报确认存在针对性攻击样本，评估风险等级为“极高”。实施效果：48小时内完成固件升级与加密改造，部署工控防火墙，半年内未发生安全事件，系统稳定运行率提升至99.8%。

3.1.2 经验教训与改进建议

（1）成功经验：建立“IT+OT”联合评估小组，确保风险覆盖控制层与信息层；采用“白名单”机制验证处置措施有效性。（2）教训：初期未考虑工控系统“停机风险”，评估时过度依赖扫描工具导致误判；未纳入供应链风险（第三方维护工具带毒）。（3）改进建议：新增“停机影响系数”修正评估模型；每季度开展供应链安全审计，禁止未经检测的外部工具接入。

3.2 风险处置与应对策略

3.2.1 风险处置计划

按“风险等级-修复难度”分级处置：极高风险（如远程控制漏洞）24小时内启动紧急修复，同步物理隔离；高风险（如弱口令）72小时内整改；中低风险（如日志不全）月度闭环。明确OT团队为执行主体，安全团队监督，验收标准为漏洞复测通过率100%。

3.2.2 针对性应对策略

（1）工控协议风险：部署深度包检测设备，禁用冗余协议，对关键指令加签验证。（2）固件安全风险：建立固件白名单库，升级前进行离线兼容性测试，留存应急回滚方案。（3）人员操作风险：操作权限按“岗位职能”划分，关键操作需双人复核并全程录像。（4）物理安全风险：机房实施“双门禁”管理，运维设备专人保管，外接端口物理封堵。

4 信息安全运维风险评估体系的持续改进与优化

4.1 监控与审计机制

4.1.1 持续监控和审计机制的建立

构建“实时监控+定期审计”双轨机制。实时监控方面，部署安全信息和事件管理（SIEM）系统，对关键资产运行状态、风险处置进度、异常访问行为等进行7×24小时监测，设置风险阈值自动告警（如漏洞修复超期3天触发红色预警）。定期审计采用“季度全面审计+月度专项审计”模式，组建由安全专家、运维骨干、第三方机构组成的审计组，核查评估流程合规性、工具准确性及处置效果。

4.1.2 结果分析与体系优化

每周汇总监控数据，分析风险趋势（如某类漏洞出现频率上升）；每季度结合审计报告，识别体系短板（如评估指标未覆盖新业务场景）。针对发现的问题，动态更新资产清单、调整威胁库（新增AI生成式攻击等新型威胁）、优化评估模型权重（提高数据资产保密性指标占比），形成“监控-分析-优化-验证”的闭环迭代。

4.2 法规遵循与合规性检查

4.2.1 法规与标准的符合性保障

对标《网络安全法》《数据安全法》《信息安全技术网络安全等级保护基本要求》等法规标准，将合规条款嵌入评估体系：如数据跨境传输评估需满足“安全评估+个人信息保护影响评估”双要求，等级保护三级系统需增加“异地灾备”风险项评估。建立法规动态跟踪机制，安排专人每月更新法规库，确保体系条款与最新要求同步。

4.2.2 合规性检查的实施

每半年开展一次全面合规检查，采用“条款映射法”逐一比对评估流程与法规要求的一致性；每年邀请第三方机构进行合规认证（如ISO27001）。对检查发现的合规缺口（如日志留存不足6个月），制定整改时间表，明确责任部门，整改完成后进行二次验证，确保100%闭环。

4.3 人才培养与技能提升

4.3.1 人才需求特点分析

信息安全运维风险评估人才需具备“技术+管理+法规”复合能力：熟悉漏洞扫描、渗透测试等技术工具，掌握风险矩阵、资产价值评估等方法论，了解网络安全法规条款；同时需具备较强的沟通能力（协调业务部门配合评估）和应急分析能力（快速判断风险等级）。

4.3.2 培养方法与途径

（1）内部培训：开展“每周技术分享会”（讲解新型漏洞原理）、“风险评估实战演练”（模拟业务系统评估场景）。（2）外部认证：鼓励考取CISSP（注册信息系统安全专业人员）、CRISC（风险与信息系统控制认证）等证书，企业承担部分培训费用。（3）跨岗实践：安排安全人员轮岗至运维、业务部门，深入理解系统架构和业务流程，提升评估针对性。（4）行业交流：加入信息安全协会，参与跨企业风险评估案例研讨会，借鉴先进经验。

结束语

信息安全运维中的风险评估体系构建是一个持续演进的过程，它要求组织在理解当前安全态势的基础上，不断适应新技术、新威胁的挑战。通过完善风险评估流程、引入先进技术和工具、强化合规管理与人才培养，我们能够更有效地识别和应对信息安全风险，为组织的信息资产保驾护航。未来，随着技术的不断进步，风险评估体系将更加智能化、自动化，为信息安全运维提供更加坚实的支撑。

参考文献

[1]沈昌祥,张焕国,王怀民.信息安全综述[J].中国科学:信息科学,2020,49(2):129-130.

[2]冯登国,张敏,李昊.信息安全风险评估综述[J].通信学报,2020,41(1):12-13.

[3]蔡吉人,冯登国,周仲义.信息安全保障技术框架研究[J].计算机学报,2021,44(3):401-402.

[4]周傲英,王珊,孟小峰.数据安全与隐私保护[J].计算机学报,2022,45(7):132-134.