ICS 03.060
CCS A11

JR

中华人民共和国金融行业标准

JR/T 0295—2023

证券期货业信息安全运营管理指南

Information security operations management guidance for securities and futures industry

2023-10-23 发布　　2023-10-23 实施

中国证券监督管理委员会　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由全国金融标准化技术委员会证券分技术委员会（SAC/TC 180/SC4）提出。

本文件由全国金融标准化技术委员会（SAT/TC 180）归口。

本文件起草单位：中国证券监督管理委员会科技监管局、深圳证券交易所、安信证券股份有限公司、中证信息技术服务有限责任公司、广发证券股份有限公司、国信证券股份有限公司、兴业证券股份有限公司、长江证券股份有限公司、国泰君安证券股份有限公司、海通证券股份有限公司、南方基金管理股份有限公司、安信基金管理有限责任公司、中信期货有限公司、京东科技信息技术有限公司、北京数字观星科技有限公司、北京知其安科技有限公司。

本文件主要起草人：姚前、蒋东兴、陈炜、许彦冰、李维春、聂君、李家攀、黄清华、路一、周桉、刘彬、陈传鹏、杨启、陈凯晖、王玥、吴佳伟、姚飞、唐勤、杨阳、金文佳、陆颂华、马冰、张永刚、宋辉、郭亮、王千寻、孟繁强。

证券期货业信息安全运营管理指南

1 范围

本文件提供了开展信息安全运营管理中安全管理、基础安全管理、信息资产管理、漏洞管理、开发安全管理、数据安全管理、集中监控与响应管理以及持续改进管理的指导思路及方法。

本文件适用于证券期货行业的核心机构和经营机构在完成基础的信息安全建设后开展的信息安全运营管理工作。

注：核心机构包括证券交易所、期货交易所、登记结算公司等，经营机构包括证券公司、期货公司、基金管理公司等。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

ISO/IEC 27001：2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements

ISO/IEC 27002：2022 Information security, cybersecurity and privacy protection — Information security controls

GB/T 25068.1—2020 信息技术 安全技术 网络安全 第1部分：综述和概念

GB/T 25069—2022 信息安全技术 术语

GB/T 28454—2020 信息技术 安全技术 入侵检测和防御系统（IDPS）的选择、部署和操作

GB/T 28458—2020 信息安全技术 网络安全漏洞标识与描述规范

JR/T 0158 证券期货业数据分类分级指引

3 术语和定义

GB/T 25069—2022中界定的以及下列术语和定义适用于本文件。

3.1

安全域 security domain

遵从共同安全策略的资产和资源的集合。

[来源：GB/T 25068.1—2020，3.35]

3.2

入侵 intrusion

对网络或联网系统的未授权访问，即对信息系统进行有意或无意的未授权访问，包括针对信息系统的恶意活动或对信息系统内资源的未授权使用。

[来源：GB/T 25068.1—2020，3.17]

3.3

入侵检测 intrusion detection

检测入侵的正式过程，该过程一般特征为采集如下知识：反常的使用模式、被利用的脆弱性及其类型、利用的方式，以及何时发生和如何发生。

[来源：GB/T 28454—2020，3.17]

3.4

敏感数据 sensitive data

一旦泄露可能会对用户或金融机构造成损失的数据。

注：包括但不限于用户敏感数据（如用户口令、密钥）、系统敏感数据（如系统密钥、关键系统管理数据）、关键性操作指令、敏感业务数据、系统主要配置文件等。

3.5

数据安全 data security

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

3.6

信息资产 information assets

客观存在于网络中，能被攻击者发现/利用，从而实现其系统破坏或非法获利目标的客体。

3.7

安全基线 security baseline

保障系统基本安全的最低配置要求。

3.8

网络安全漏洞 cybersecurity vulnerability

网络产品和服务在需求分析、设计、实现、配置、测试、运行、维护等过程中，无意或有意产生的、有可能被利用的缺陷或薄弱点。

注：注：这些缺陷或脆弱点以不同形式存在于网络产品和服务的各个层次和环节中，一旦被恶意主体所利用，就会对网络产品和服务的安全造成损害，从而影响其正常运行。

[来源：GB/T 28458—2020，3.1]

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Programming Interface）

APP：应用程序（Application）

CMDB：配置管理数据库（Configuration Management Database）

DHCP：动态主机配置协议（Dynamic Host Configuration Protocol）

DLP：数据防泄漏（Data Leakage Prevention）

DMZ：非军事化区（Demilitarized Zone）
DNS：域名系统（Domain Name System）
HIDS：基于主机型入侵检测系统（Host-based Intrusion Detection System）
IDS：入侵检测系统（Intrusion Detection System）
IPS：入侵防御系统（Intrusion Prevention System）
JSON：JS 对象简谱（JavaScript Object Notation）
KMS：密钥管理系统（Key Management System）
NTP：网络时间协议（Network Time Protocol）
POC：验证性测试（Proof of Concept）
UPS：不间断电源（Uninterruptible Power Supply）
URL：统一资源定位系统（Uniform Resource Locator）
WAF：Web 应用防护系统（Web Application Firewall）
SOAR：安全编排和自动化响应（Security Orchestration, Automation and Response）
SOC：安全运营中心（Security Operations Center）
SOP：标准作业程序（Standard Operating Procedure）
RASP：运行时应用自我保护（Runtime Application Self-Protection）
XML：可扩展标记语言（Extensible Markup Language）
YAML：另一种标记语言（YAML Ain't Markup Language）

5 安全管理

5.1 安全管理目标

通过设置合理的组织架构、有机的制度体系、符合实际情况的人员编制和针对性的人员培养机制，使安全管理制度化、流程化、规范化。在日常的安全工作中实践、检验、优化完善，提升组织的安全管理水平，确保组织的信息资产得到安全保护，保障投资人的合法权益，为总体安全目标赋能。

5.2 安全管理过程

5.2.1 安全目标管理

安全目标管理是指通过设置合理的目标体系，明确和分解安全职责，激发工作动机，促进工作协调，为安全考核提供依据，促进个人和组织整体安全目标的达成。

安全目标管理主要分为以下三个过程：

a) 制定目标：设置总体目标，明确组织安全意图和方向，由组织管理层审批。具体目标由总体目标分解而成，具体目标应尽可能地客观、量化、可评估；
b) 制定方案：根据具体目标分解具体项目和任务，可采用自上而下的方式，从技术和管理两方面系统性考虑；
c) 执行和改进：采取控制措施检查和评价目标完成情况，并根据结果制定针对性措施进行持续改进。

5.2.2 安全组织管理

安全组织管理的目标是建立信息安全管理组织结构、功能，明确职责分工，以保障安全目标的实现。

安全组织管理一般包括：

a) 各机构应建立信息安全管理组织，应明确主要负责人为本机构信息安全工作的第一责任人，分管信息安全工作的领导班子成员或者高级管理人员为直接责任人。应当建立网络和信息安全工作协调和决策机制，保障第一责任人和直接责任人履行职责；
b) 建立健全信息安全责任制度，对所有的信息安全职责予以明确定义与分配，确保责任落实到各级岗位及人员；
c) 确保信息安全人员具备与履行职责相匹配的专业知识和职业技能；
d) 建立与证券期货业监管单位、相关协会组织、信息系统服务机构、安全专家的沟通机制；
e) 建立基于三层架构的安全运营机制：
   1) 一线负责日常各安全系统的监控、告警及事件处理，将复杂事件上升到二线处理；
   2) 二线负责较复杂事件分析、制定告警规则、验证告警规则的有效性等工作；
   3) 三线作为高级分析团队，深度参与未形成 SOP 的事件的应急处置、验证和复盘，形成 SOP 交付一线进行常态化运营。另外，三线还负责对事件进行统筹分析，发现安全机制及体系中存在的问题，并不断推动改进。

5.2.3 安全制度管理

安全制度管理的目标是通过建立和落实科学合理的信息安全制度体系，明确管理的目标与范围、流程与活动、人员与职责、资源与条件等，使安全工作规范化、标准化，提高安全管理有效性，促进实现安全目标。

安全制度管理一般包括：

a) 建立健全信息安全制度体系，一般建议采用四级架构（一级为基本制度，二级为办法/规定，三级为实施细则/操作规程，四级为表单及记录）的制度文件体系；
b) 宜保证各项制度的健全完善、合理可行、实施有效；
c) 宜建立制度起草、评审、发布、落实、评估和持续改进的管理流程。

5.2.4 安全资源管理

安全资源管理的目标是确保人力、资金、场所等投入，以建立、维护和持续改进信息安全管理体系，实现安全目标。

安全资源管理一般包括：

a) 统筹考虑组织战略、规模、安全目标和阶段规划，评估当前安全资源的投入产出情况；
b) 参照组织的其他资源，制定相对应的人员投入和资金投入预算。

5.2.5 安全培训管理

安全培训管理的目标是让员工掌握必要的信息安全知识和技能，提高员工信息安全意识和专业素养。

安全培训管理一般包括：

a) 建立规范化的信息安全管理和技术培训体系；
b) 根据不同培训对象的培训诉求，制定合适的培训内容、培训形式和培训计划；
c) 评估培训效果，持续优化改进培训体系。

5.2.6 安全绩效管理

安全绩效管理的目标是提高员工的能力和工作绩效，从而提高和改善组织的能力和绩效，最终实现组织、部门和个人的安全绩效目标。

安全绩效管理一般包括：

a) 建立科学有效的信息安全绩效管理体系。通过制定目标与计划、绩效监控与辅导、绩效考评与反馈、绩效考核结果应用四个环节持续开展绩效管理运营；
b) 根据组织战略和管理需求选择合适的绩效管理方法体系，如基于关键绩效指标（KPI）、基于360度绩效考评、基于平衡计分卡（BSC）等。

5.2.7 安全知识管理

安全知识管理的目标是通过对安全知识创建、存储、共享、应用等过程的统一管理，传承和分享知识经验，使相关方能够及时有效地获取到所需的知识，提升组织的效能。

安全知识管理一般包括：

a) 建立健全的知识管理制度，在知识管理组织架构、职责分工、运营流程、激励考核等方面作出相应的规定，促进知识管理的长期有效开展；
b) 建立知识管理平台，支撑知识管理过程，并与安全运营流程相结合。

5.3 安全管理最佳实践

安全管理的最佳实践，包括以下：

a) 安全目标管理：根据组织战略规划，自上而下地将组织战略目标进行层层分解，安全管理部门将安全目标同步下发到各个部门落实完成；
b) 安全组织管理：从纵向层面，典型的安全组织架构可包括决策层、管理层和执行层；从横向层面，由业务部门、安全部门和审计部门在安全工作中承担不同的职责，权责分离，互相约束，共同推动安全管理体系的良性发展；
c) 安全制度管理：一般可参考ISO 27001的文件体系建立相应的安全管理制度；
d) 安全培训管理：可建立培训后员工反馈沟通机制，针对每次培训后员工的反馈结果，对培训内容进行优化。可采用实战化的方式来检验员工的安全培训效果，如钓鱼邮件、社会工程学等方式；
e) 安全绩效管理：可根据组织的管理风格、管理要求制定细化的安全考核要求，设置加分和扣分项，并与人员和组织的绩效考核挂钩；
f) 安全知识管理：安全知识的范围可包括安全漏洞库、工具库、情报库等。知识管理平台要兼具查找便捷、多人协同、可富文本编辑、可管理历史版本、操作留痕等功能，并支持和工单系统、漏洞管理系统等对接；
g) 根据组织战略和安全目标建立“层层分解、层层承诺、层层支持、层层考核”的目标指标体系，从时间维度和组织层级两个角度，将安全目标分解为可执行和可监控的绩效指标体系和目标体系。

6 基础安全管理

6.1 基础安全管理目标

基础安全管理是通过一系列通用的安全措施，达到基本的安全能力，防御大部分的安全攻击，降低系统性的安全风险。

6.2 基础安全管理过程

6.2.1 系统安全管理

6.2.1.1 系统运行管理

系统安全、稳定运行最基础的保障，遵循以下：

a) 系统的硬件设备宜安放在与其承载的业务级别相匹配的运行环境中；
b) 保障设备的业务线缆与电力线缆不受到电磁及信号干扰；
c) 机房应配备 UPS，备用电力至少保障断电后 2 小时的电力供应，应采用冗余电缆并至少采用双路市电供电；
d) 保证系统维护通道与业务通道的独立，包括但不限于端口、线缆、接入设备；
e) 系统维护通道采用可审计的方案，并定期对维护操作进行审计；
f) 在安全可控的环境内对系统进行维护；
g) 对系统的性能和可用性进行持续监控；
h) 定期对系统的容量进行评估，根据业务发展情况，确保系统有合适的容量；
i) 定期对系统的授权、维保情况进行评估，包括硬件和软件，确保授权及售后服务不中断；
j) 建立故障和问题跟踪机制，并确保相关问题得到缓解处置或根本性解决处理，如修改配置、持续监控、补丁升级等；
k) 加强对系统启动加载的管控，防止加载过程被篡改和绕过，如配置 BIOS 口令、引导顺序或安全启动选项等。

6.2.1.2 系统账号及认证管理

系统账号及认证管理宜遵循以下：

a) 所有系统账号应设置复杂口令，避免弱口令和默认口令，并设置密码更换策略，对密码进行定期更换；
b) 系统认证应有详细的日志审计记录，外发至统一日志审计中心，进行异常登录监控管理；
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；
d) 重要系统的登录，宜采用多因素方式进行身份认证；
e) 加强对域管理员账号、数据库管理员账号等重要特权账号的管理，细化特权账号的识别、授权、使用和审计要求。

6.2.1.3 系统权限管理

系统权限管理宜遵循以下：

a) 系统权限管理遵循最小权限原则；
b) 系统权限的申请要配合安全管理要求，进行流程化、规范化管理；
c) 定期对系统权限进行复核、检视，对不再需要的权限予以回收；
d) 对于特权用户登录系统后的权限分配操作，宜尽可能地详实记录操作日志。

6.2.1.4 系统配置

各系统的安全基线配置、参数配置、系统配置等配置信息宜统一管理并定期备份，并定期验证配置信息的可用性。

6.2.1.5 安全策略管理

安全策略管理宜遵循以下：

a) 宜持续对审计日志进行分析，验证策略适配后的信息系统控制措施的有效性；
b) 宜定期对安全系统的策略进行复盘，动态调整策略从而适配安全需求；
c) 安全管控类策略宜尽可能默认黑名单，再通过开通白名单方式严格限制访问权限。

6.2.1.6 系统审计管理

系统的审计日志宜发送到统一日志审计中心，保证审计日志的可用性、完整性和可审计性。

6.2.2 网络安全管理

网络安全管理宜遵循以下：

a) 宜根据业务重要性或数据敏感度，划分不同的网络安全域；
b) 不同网络安全域之间宜进行有效隔离；
c) 关键网络基础设施的通信线路和设备宜采取冗余备份，保证系统高可用；
d) 网络通信宜采用加密措施保证链路的安全性，防止中间人攻击；
e) 对于高敏感度数据的传输，可采用链路加密和内容加密两种措施；
f) 在关键网络节点部署入侵检测和防御系统，并开启双向流量检测；
g) 在关键网络节点部署恶意代码和恶意邮件防范措施，对恶意文件和钓鱼邮件进行检测、拦截。

6.2.3 主机安全管理

主机安全管理宜遵循以下：

a) 主机身份识别宜具有唯一性，口令宜具备足够的复杂性，避免弱口令；
b) 关键主机系统宜限制从终端直接登录进行运维管理，宜通过堡垒机或其他管控系统进行登录操作；
c) 主机的基本安全设置宜符合安全基线要求，定期进行安全配置核查并对问题点跟踪整改；
d) 关键主机可采用主机防火墙等方式进行访问限制；
e) 主机上宜部署 HIDS 系统，对主机入侵进行检测。

6.2.4 终端安全管理

6.2.4.1 恶意代码防护管理

恶意代码防护为终端安全管理中最基础的安全防护，宜遵循以下：

a) 所有终端要安装恶意代码防护软件，并定期更新恶意代码防护软件版本和恶意代码特征库；
b) 宜支持恶意代码防护软件的统一管理，对终端防护软件的集中升级宜有人工确认；
c) 主机防恶意代码产品可与网络防恶意代码产品采用不同的恶意代码库；
d) 宜定期检查恶意代码防护软件在线及恶意代码特征库的升级情况；
e) 宜定期进行全面扫描，对截获的恶意代码及时分析处理；
f) 宜使用终端检测与响应技术，实时感知终端的异常进程及异常连接行为。

6.2.4.2 文件交换

数据在使用过程中务必会涉及到文件交换，文件交换宜遵循以下：

a) 对敏感数据进行加密传输；
b) 可部署 DLP 系统保证文件交换的可审计性；
c) 具备对外接移动存储设备的管控能力；
d) 移动存储设备、外来电子文档、软件系统使用前宜进行病毒和木马查杀。

6.2.4.3 桌面准入管理

桌面准入管理主要是对设备、用户的访问权限进行管理，宜遵循以下：

a) 确保桌面用户身份的可识别性；

b) 对用户进行身份鉴别、授权和审计；
c) 具备用户身份鉴别失败处置策略；
d) 定期对身份鉴别方式的有效性和安全性进行评估；
e) 加强特殊权限角色身份鉴别和访问控制手段。

6.2.5 补丁管理

软件及系统功能变更及漏洞修复往往通过打补丁的形式处理，补丁管理宜遵循以下：
a) 制定补丁管理制度，对升级与补丁更新作出规定，涉及操作系统、应用软件、数据库及中间件等；
b) 准确掌握软件版本信息，做好软件补丁的统一管理；
c) 持续跟踪供应商提供的软件更新升级情况，并开展对受影响系统补丁的评估、测试、更新和验证工作；
d) 宜制定补丁更新工作相关数据备份及故障回退方案。

6.2.6 安全基线

6.2.6.1 安全基线管理

安全基线管理的目的在于保障业务系统的安全，使业务系统的风险在可控范围之类。

6.2.6.2 安全基线设置

安全基线设置宜遵循以下：
a) 宜根据组织的信息资产情况设定操作系统、网络设备、中间件、数据库等的安全基线；
b) 可通过人工或自动化的方式实现信息资产的安全基线设置。

6.2.6.3 安全基线检查

宜定期对信息资产的安全基线设置进行检查，并对检查过程中发现的问题进行跟踪处置。宜定期根据组织信息资产和漏洞情况对安全基线进行评估及更新。

6.2.6.4 安全基线例外管理

在经过缓解、限制等安全处置后，可允许部分低于安全基线配置的例外情况存在，宜建立例外管理措施，对例外情况进行详细记录。

6.3 基础安全管理最佳实践

基础安全管理最佳实践，包括以下：
a) 终端准入可结合安全基线进行，如终端未安装防病毒软件且病毒库不在最近一个月内的，禁止准入；
b) 对于恶意代码的检测，可以结合基于特征库的静态检测及基于行为特征的动态检测两种不同方法；
c) 定期检查基础安全配置的有效性，对不符合项宜及时进行整改；
d) 数据交换接口格式尽量采取纯文本格式，如 yaml、json，避免使用可能隐藏恶意代码的格式，如 xml、js；
e) 可先在负载均衡设备上对加密网络流量进行解密（如通过统一卸载 SSL 的方式），再将明文流量接入安全检测系统中做分析，以解决分析加密流量的问题；

f） 可建立供应商主动通报补丁更新的管理机制，并纳入对供应商的考评中。

7 信息资产管理

7.1 信息资产管理目标

发现、识别、梳理互联网和内网信息资产，形成完备的信息资产数据。周期性地执行信息资产威胁检测任务，结合漏洞威胁情报，发现、识别、定位及验证网络区域内资产的漏洞情况，及时进行风险处置，提升组织对信息资产的安全运营管理能力。

7.2 信息资产管理过程

7.2.1 信息资产发现

信息资产发现的目的，是对组织信息资产情况进行全面掌握，以更好地开展安全风险识别和处置工作。信息资产发现方式包括但不限于：

a） 主动发现：通过主动扫描、安装信息资产管理客户端及情报信息收集等方式，发现互联网及内网中的 IP、端口、协议、证书、域名、URL、APP、API、中间件及软件版本等信息；

b） 被动发现：通过流量监听的方式被动发现网络中的信息资产。

7.2.2 信息资产管理

7.2.2.1 信息资产梳理

信息资产梳理主要包括资产的识别与分类：

a） 对信息资产生命周期全过程进行管理，通过周期地检测比对，实现资产变更跟踪，保证资产的一致性；

b） 信息资产可依照业务系统进行分类，也可根据法律要求、信息资产价值、敏感性和关键性进行分类，便于安全信息资产的分隔管理和资源隔离；

c） 通过信息资产梳理，实现直观的信息资产画像，增强安全运营人员对信息资产的认知。

7.2.2.2 信息资产检索

宜建立对信息资产快速检索能力，检索有助于快速定位有风险的信息资产，并进行后续的处置。信息资产检索一般包括以下维度的检索条件：

a） IP、端口、域名、URL、服务/协议、应用系统名称、系统负责人、组织信息、互联网开放情况等；

b） 操作系统、应用系统、数据库、中间件、第三方组件等的版本信息。

7.2.2.3 信息资产运营

信息资产运营宜遵循以下：

a） 信息资产多维度威胁监测：从多种维度，定期监测信息资产威胁情况，包括系统漏洞、Web 应用漏洞、弱口令、代码泄露、APP 威胁等，形成信息资产威胁图谱；

b） 信息资产与威胁情报的结合：充分利用多方威胁情报，将信息资产和威胁情况与情报相结合，将威胁情报真正运用于日常工作中。当出现最新 0day 情报时，快速获取最新漏洞信息，利用 POC 插件进行全网检测，筛选可能受到影响的信息资产；

c) 网络安全漏洞应急响应：对于信息资产中发现的网络安全漏洞进行应急响应，确保在最短时间内修补信息资产对应的漏洞；
d) 信息资产漏洞全生命周期管理：包括漏洞发现、漏洞指派、漏洞处置、漏洞状态跟踪、漏洞关闭等阶段，达到对漏洞的全流程管理，掌握信息资产漏洞整体状况；
e) 信息资产安全报告：包括信息资产统计、组件开放统计、端口变化趋势、漏洞加固统计、漏洞变化趋势、信息资产威胁态势报告等，展示信息资产风险状况和安全工作成果；
f) 重点信息资产监测：标记重点信息资产，设置周期性任务，进行重点管理；
g) 信息资产安全告警：新出现高危漏洞或高危漏洞数量达到阈值时进行告警，或自定义告警条件，便于及时发现信息资产安全威胁，掌握安全态势，从而实现精准防御；
h) 态势感知支撑：为态势感知、SOC 等系统提供信息资产数据支撑；
i) 数字证书管理：对数字证书的申请、发放、使用、注销等做统一管理，保障数字证书的可用性、安全性。

7.3 信息资产管理最佳实践

信息资产管理的最佳实践，包括以下：
a) 信息资产管理是安全运营的主要基础工作之一，宜持续对信息资产进行跟踪和维护；
b) 宜使用成熟的基于生命周期的方法，对信息资产进行管理，确保信息资产为最新状态；
c) 在信息资产管理过程中宜采取自动化收集、更新维护的措施，来提升管理效率；
d) 可采用信息资产集中管理系统进行统一管理。可采用 API 调用的方式从其他周边关联系统及时获取最新信息；
e) 信息资产管理不是孤立的，宜与企业内部 IT 运营流程进行联动，使得信息资产信息输入、变更等能得到及时的更新，从而确保信息的准确性。

8 漏洞管理

8.1 漏洞管理目标

通过漏洞的及时发现、有效验证、准确评价、高效修复/加固和复测，控制漏洞暴露所形成信息安全风险。尽可能地避免攻击者利用漏洞实现其网络攻击行为和目的，保障组织业务系统及业务数据的安全性。

8.2 漏洞管理过程

8.2.1 漏洞发现

漏洞发现是漏洞管理工作的起始，通过多种方式及时发现组织系统中存在的漏洞，避免系统漏洞长期暴露。漏洞发现方式包括但不限于：
a) 利用组织自有的人工或自动化方法对漏洞进行检测；
b) 利用安全众测或第三方漏洞检测服务的形式定期对漏洞进行检测；
c) 通过接收漏洞通报机构的通报获取漏洞信息；
d) 获取软件厂商官方通报的软件漏洞信息。

8.2.2 漏洞验证

漏洞验证是验证漏洞的真实性，也是漏洞管理过程中的关键步骤，有效的漏洞验证可以提高后续漏洞分析和处置工作的效率，提升安全运营工作的整体水平。漏洞验证方式包括但不限于：

a) 利用组织自有的人工或自动化方法对漏洞进行验证；
b) 利用第三方漏洞验证服务对漏洞进行验证。

8.2.3 漏洞评估

漏洞评估是通过漏洞级别、漏洞利用方式、漏洞载体（信息系统）价值及敏感度等指标评估漏洞危害程度的过程，科学地判断多个漏洞的修复顺序和修复时限，为后续的漏洞处置过程提供依据。漏洞评估方式包括但不限于：

a) 综合评估法：结合漏洞级别、漏洞利用方式、漏洞载体价值及敏感度、漏洞载体的映射情况及访问策略等指标进行综合评估，该方法适用于信息资产规模较大的组织；
b) 单一评估法：根据漏洞载体是否映射在互联网侧、漏洞载体是否是核心系统、漏洞载体是否是生产环境等指标中的某一条进行评估，该方法适用于信息资产规模较小组织。

8.2.4 漏洞修复/加固

漏洞修复/加固是通过升级补丁、虚拟补丁、策略阻断、组件升级等方式消除或控制漏洞安全风险的过程，漏洞修复/加固的方式包括但不限于：

a) 升级补丁：通过官方渠道获取漏洞修复补丁，以对漏洞载体进行补丁升级的方式修复漏洞；
b) 虚拟补丁：通过前置防护设备有效控制用户与漏洞载体间的输入输出，阻断可能存在的漏洞利用情况；
c) 策略阻断：通过网络防护策略对漏洞载体的访问权限进行控制，根据业务需求限制允许访问漏洞载体和允许漏洞载体访问的地址范围；
d) 组件升级：通过将漏洞载体升级到最新版消除漏洞。

8.2.5 漏洞复测

漏洞复测是验证漏洞修复/加固操作的有效性，避免因为执行操作、修复/加固失败、系统重新部署导致漏洞复发等因素形成漏洞管理黑洞。漏洞复测的方式包括但不限于：

a) 利用自动化能力以漏洞扫描的方式进行复测；
b) 以人工验证的方式进行复测。

8.2.6 漏洞复盘

漏洞复盘是总结漏洞发现、漏洞验证、漏洞加固和复测每个过程的操作，识别可以改进的环节，持续优化漏洞运营工作：

a) 在漏洞闭环处置完成后，根据漏洞发现的过程、漏洞产生的原因、安全措施的有效性几个方面进行漏洞复盘；
b) 针对在漏洞复盘的过程中发现的问题，进行迭代优化和整改。

8.3 漏洞管理最佳实践

在日常安全运营工作中，及时、准确地发现漏洞，以及从海量信息资产确认漏洞信息具有较大的难度。通过结合威胁情报、信息资产和自动化关联能力，可实现高效、准确的海量信息资产高危漏洞快速处置能力：

a) 情报获取：通过外部安全服务或自有情报获取能力，可获取及时的高危漏洞情报信息；

b) 情报适配：利用资产威胁管理系统，可查看漏洞情报和信息资产的匹配情况。对于需要进行POC验证的漏洞，可以通过圈定可疑信息资产范围的方式，有效缩减POC检测的信息资产数量和范围，提升POC漏洞检测的效率；
c) 漏洞检测：利用网络安全漏洞情报配套的POC检测插件，对可疑信息资产组进行针对性地扫描，快速定位风险信息资产；
d) 协助修复/加固：利用漏洞情报配套的加固方案/补丁，配合漏洞验证结果帮助操作人员执行漏洞修复/加固实施操作；
e) 漏洞复测：通过漏洞管理平台确认漏洞修复/加固完毕后，可调用POC检测引擎进行漏洞复测。

9 开发安全管理

9.1 开发安全管理目标

开发安全管理是指在系统开发环节引入系统性的安全过程，使安全左移，以最小的成本降低安全漏洞，收敛安全风险。

9.2 开发安全管理过程

9.2.1 安全需求分析

在需求分析阶段，应充分识别出安全的需求，并将安全需求列入项目需求中。

a) 明确安全需求分析职责：
   1) 业务需求提出部门是安全需求提出的主体部门；
   2) 安全团队、研发团队和相关业务部门人员共同完成安全需求分析。
b) 需求分析开始时，应对系统的信息安全等级保护级别进行评估、确定；
c) 建立安全需求分析库，安全需求分析库是安全需求分析的标准化工具，由不同安全功能点组成。安全功能点分为强制、增强和可选三类：
   1) 强制安全功能点是所有系统提供的功能；
   2) 增强安全功能点是所有重要及以上系统提供的功能；
   3) 可选安全功能点是有条件系统宜满足的功能。
d) 建立需求变更管理流程，存在需求变更时，对变更内容开展安全需求分析。
e) 明确系统的开发方式，涉及外购、合作研发类系统，建立软件供应商安全风险管理机制：
   1) 确立供应链安全管理的目标，建立供应链安全管理、风险管理和安全保障的手段；
   2) 开展资格评估和风险评估，考察软件供应商的综合实力，选择符合要求的供应商。

9.2.2 安全架构评审

评审过程宜关注以下原则：

a) 最小攻击面，关闭不必要的对外开放的端口和服务；
b) 初始化安全，修改或删除信息系统初始化的不安全配置、账户信息；
c) 权限最小化，分配满足业务需要的最小权限即可；
d) 失败安全，当信息系统访问出现失败时宜有相应控制措施，防止权限提升、信息泄露等问题发生；
e) 不信任第三方组件，在使用第三方组件时宜充分考虑第三方组件的安全性和合规性；
f) 安全的加密算法，加密算法遵循国家、行业相关密码标准；
g) 前后端分离原则，前端代码不直接调用、写入后台数据库，防止数据库相关信息泄露；

h） 纵深防御，在信息系统的架构层面宜考虑纵深防御体系。

9.2.3 安全开发

宜建立安全开发规范，供开发人员参考执行，并开展有效的审计措施进行复核。

a） 制定安全开发相关规范：
   1） 制定覆盖不同信息系统开发语言的安全规范或手册；
   2） 定期根据安全规范或手册对开发人员进行培训。
b） 建立源代码安全审计机制，可有效验证开发团队是否参照开发安全规范编写源代码，对信息系统开发安全过程进行闭环管理；
c） 自主开发的软件采取防反编译、防篡改、防调试、防注入等安全措施，如采用环境检测、安全编译选项、混淆、加密、隐藏、加壳、签名等技术；
d） 建立自主研发、外购系统的软件成分管理机制，软件成分包括组件名称、版本号、供应商等信息；
e） 建立软件成分分析机制，对软件成分进行识别、分析和追踪，确保使用组件的安全性与合规性。

9.2.4 安全测试

在开发过程中，宜开展对源代码的白盒检测及信息系统的黑盒检测：

a） 安全测试宜采用自动化和人工双重验证机制，对于重要业务系统、面向互联网系统宜进行双重验证；
b） 测试完后形成能说明所选择的安全需求功能均已实现的测试报告。

9.2.5 安全上线

信息系统上线前，宜开展相应的安全检测，确保信息系统安全可控的上线：

a） 上线前信息系统安全检测：根据系统上线后所面对的安全风险不同，互联网系统和内网系统在上线前的安全测试实施方式将有所不同。宜重点加强互联网系统的安全上线检查，严格遵照基线要求，防止系统带病上线；
b） 部署环境安全加固：上线前除了对业务应用系统进行安全测试外，还宜对系统运行环境进行安全加固。

9.3 开发安全管理最佳实践

9.3.1 安全需求分析最佳实践

安全需求分析的最佳实践，包括以下：

a） 业务需求提出部门在提出业务需求同时宜填写好安全需求分析库，即根据系统情况选择对应的安全需求功能点；
b） 安全需求应分为通用安全需求和业务安全需求。对于通用安全需求，业务团队在提交安全需求分析时，可根据业务系统架构、服务类型、法律法规等对通用安全需求中内容进行裁剪、选择；对于业务安全需求，业务团队可与安全团队共同制定，可使用威胁建模等方法；
c） 在研发团队收到业务需求提出部门提出的安全需求后编制需求规格说明书；
d） 安全团队、研发团队和业务部门对需求规格说明书内容进行讨论、分析和确认。

9.3.2 安全架构评审最佳实践

安全架构评审的最佳实践，包括以下：

a) 系统整体架构图宜清晰标识系统和其他系统交互以及交互的目的和方式，并标识具体的安全控制措施（网络访问控制、开发安全规范、开源产品类型等）；
b) 系统部署架构图宜明确标识系统的物理部署，明确标识系统部署的网络区域；
c) 系统网络拓扑图宜清晰真实地体现系统的网络逻辑拓扑结构，系统网络边界及系统所在的安全域；
d) 系统宜设计身份认证模块，认证模块具有安全控制措施，如口令复杂度策略、登录失败处理功能、双因素认证（有条件的互联网系统）等；
e) 系统宜设计全局有效的权限管理模块，包括用户权限分配、回收等。权限控制粒度是否足够小，如请求的参数级，可有效防止越权；
f) 系统宜设计安全审计日志模块，包含用户具体操作内容，具有可审计性；
g) 系统敏感数据在存储、传输、处理和页面展示中进行保密性保护处理，如自建数据加密算法、数据隐蔽、安全加密协议、证书等；
h) 系统数据在存储、传输、处理和页面展示中进行完整性保护处理，防止被非法篡改，如：数据加密算法、数据散列、安全加密协议、证书等方式；
i) 系统宜设计全局的异常处理机制，避免异常信息向用户暴露；
j) 系统若提供 API 接口供其他系统调用时，宜对 API 接口的调用提供身份认证、权限控制、日志审计等功能；
k) 系统宜使用指定的第三方软件版本。第三方软件包括但不限于中间件、服务器软件、开源组件、开发框架等；
l) 明确系统数据备份和恢复方式与频率。备份方式包含但不限于本地备份、异地备份、同城备份、全量备份、增量备份、差异备份等；
m) 不同的业务系统、应用及组件宜分配合理的网络安全域，避免不同安全级别的业务系统、应用及组件部署在同一安全域中。

9.3.3 安全开发最佳实践

安全开发的最佳实践，包括以下：

a) 制定信息系统开发安全规范，包含身份鉴别、访问控制、安全审计、敏感信息保护、Web Service 安全要求、移动应用 APP 安全手册和编程安全手册等内容，从不同方面描述系统开发时宜执行的安全操作；
b) 在数据输入校验、输出编码、上传下载、异常处理、代码注释等方面提供参考编码样式或组件，开发过程中可直接引用；
c) 建立源代码、第三方软件自动化检测平台和 IDE 安全检测插件，可及时对源代码实施安全审计；
d) 制定源代码 TOP 20 缺陷，TOP 20 缺陷可参考 OWASP Top10、CWE/SANS Top 25、US-Cert 安全编码等国际主流标准和日常渗透测试结果进行制定；
e) 建设开发安全组件库，将安全能力标准化，以安全组件、代码包等形式交付给开发人员使用。

9.3.4 安全测试最佳实践

安全测试的最佳实践，包括以下：

a) 研发团队宜依照确定好的安全需求库进行安全功能开发，并设计测试用例，完成测试，最终形成测试报告；
b) 可将部分安全检测能力前移，由研发或功能测试团队自主进行源代码安全测试并修复代码中的漏洞；
c) 安全团队在上线前对测试报告进行评审和确认，确定所有安全功能点已实现。

9.3.5 安全上线最佳实践

表1给出了安全上线的最佳实践，在系统上线前可参照开展相关工作。

表1 系统上线前安全测试实施表

系统性质	上线类别	安全测试实施	复核实施
互联网	新系统上线	上线前完成系统所有模块的安全测试。	上线前针对发现的安全漏洞完成整改和复核，并由安全团队出具署名的《上线前安全测试复核报告》。
	滚动开发上线	若近1年内未曾进行过系统所有模块的安全测试，则按照新系统上线要求实施。	
		若近1年内曾进行过系统所有模块的安全测试，则上线前可仅完成系统新增模块的安全测试。	
内网	新系统上线	上线前完成系统所有模块的安全测试。	优先按照互联网系统要求执行，若条件不成熟，可提供安全团队认可的《上线前安全漏洞整改计划》，根据计划上线后完成安全漏洞的整改和复核。
	滚动开发上线	大版本变更，上线前完成申请安全测试，安全测试可与上线并行实施。小版本变更，上线前不进行安全测试（定期的安全测试作为补充）。	上线后根据安全团队的相关要求完成安全问题整改和复核。

上线前除了对业务应用系统进行安全测试外，还宜对系统运行环境进行安全加固。针对不同的操作系统、数据库和中间件制定不同的安全基线和加固手册，对操作系统安装、软件安装和应用系统部署等环节进行安全策略配置。

10 数据安全管理

10.1 数据安全管理目标

通过管理和技术手段，保障组织数据的安全采集、安全使用、安全传输、安全存储、安全共享或披露、安全流转，并进行流转跟踪，防止敏感数据泄露，满足合规要求。

10.2 数据安全管理过程

10.2.1 数据分级分类

10.2.1.1 数据分级分类概述

数据是指各机构在经营和管理活动中产生、采集、加工、使用或管理的各类电子数据和非电子数据，例如客户个人信息、账户信息、交易流水、日志文件、数据库文件等。数据的分类、分级宜按JR/T 0158的描述划分，并根据各机构的实际情况进行增补。

在进行数据分类之前，宜先对各机构内部业务进行梳理，同时尽可能全面地收集整理各类数据资产，包括数据表、数据项、数据文件等，作为后续工作的参考依据。

对数据进行分类时：

a) 一般可以先从业务线出发，对业务进行细分；

b) 然后对数据进行细分和归类；
c) 最终对分类后的数据进行定级。

10.2.1.2 业务分类阶段

业务分类阶段是在同一业务线下，根据实际情况对业务线进行细分，得到一系列较为清晰的业务一级、二级分类。二级分类通常是根据业务的管理主体和管理范围对业务类型的进一步划分。

示例：业务一级分类可划分为“交易类”“监管类”“信息披露类”及“其他类”。同属于“交易类”业务分类下的数据，又可以根据管理主体和管理范围的不同，划分为“交易管理”“产品管理”“结算管理”等二级分类。

10.2.1.3 数据归类阶段

数据归类阶段重点解决数据分类的问题。在业务分类阶段的基础上，对数据进行细分和归类，找到数据与业务二级分类的对应关系，经归类后确定数据的分类。

数据归类时可根据具体业务管理范围内所涉及的数据的不同，按照数据性质、业务行为、数据重要程度、管理要求等因素，对数据进行细分归类，得到各业务二级分类所对应的数据一级分类，并可根据实际需要进行进一步的细分。数据分类示例见表2。

表 2 数据分类示例

业务一级分类	业务二级分类	数据一级分类	数据二级分类
交易类	投资者管理类	投资者基本信息	个人投资者基本信息
			机构投资者基本信息

10.2.1.4 数据定级阶段

数据定级阶段是在完成数据分类后，按照一定的判定标准，对已完成分类的数据进行定级，针对每一类数据对应的数据分级结果制定差异化的信息安全保护要求。通常可用于数据定级的要素有：影响对象、影响范围、重要程度等。数据分级示例见表3。

表 3 数据分级示例

数据示例	影响对象	影响范围	影响程度	重要程度	数据分级
投资者个人信息	客户	本机构	严重	高	1

10.2.2 数据全生命周期安全管理

10.2.2.1 数据采集

数据采集安全，目标是保护数据合法合规、安全的采集过程，其中包括：

a) 通过网站、应用程序、APP 等产品进行数据采集的，宜提供个人信息收集使用说明及隐私保护政策，宜参考相关法律法规有关条款，满足相关合规要求。内容一般包括：
   1) 提供个人信息的收集规则，通常包括但不限于下列内容：收集使用个人信息的目的、种类数量、方式、范围、更正和删除方法、保存期限、过期处置方式等；
   2) 提供个人信息的使用规则，通常包括但不限于下列内容：个人信息的处理及使用方法，共享、转让和公开披露条件超出使用目的时的处理方法，Cookie 类技术使用规则等；
   3) 提供个人信息的保护规则，通常包括但不限于下列内容：个人信息的存储地点及存储期限，技术防护策略，管理策略，安全事件的应急处理机制等；

4) 其他内容，通常包括但不限于下列内容：用户权利，通知和变更方式，联系方式等。

b) 宜采用认证、鉴权、异常检测、安全加固等技术手段保证采集过程的安全性不被破坏。

10.2.2.2 数据传输

数据传输安全，是指保护数据在传输过程中的安全性，重点关注的是数据的保密性及完整性，保障数据在传输过程中未被非法获取或篡改。其中包括：

a) 可采用密码技术保证重要数据在传输过程中的保密性；

b) 可采用密码技术或校验技术保证重要数据在传输过程中的完整性。

10.2.2.3 数据存储

数据存储安全，是指保护数据在存储过程中的安全性，确保数据在存储过程中可正常使用，且未被非法获取或篡改。其中包括：

a) 可采用密码技术保证数据在存储过程中的保密性；

b) 可采用密码技术或校验技术保证数据在存储过程中的完整性；

c) 可采用备份技术保证数据在存储过程中的可用性，针对重要数据一般宜提供本地备份恢复功能和异地备份功能；

d) 可采用入侵防护、恶意代码防护、抗攻击技术等，对数据存储环境进行安全加固，避免内外部攻击对数据安全性造成影响。

10.2.2.4 数据处理

数据处理安全，是指保护数据在查询、开发、展示等有目的处置和应用行为过程中的安全性。其中包括：

a) 在设计应用系统时，宜充分调研用户数据处理需求，应用系统功能宜满足用户的主要数据处理需求；

b) 采取身份认证技术，对进行数据处理的人员进行身份标识和鉴别，并设置认证失败处理机制或风险控制措施，防止暴力破解、撞库等攻击行为；

c) 采取访问控制技术，对数据访问权限进行严格授权和管控，遵循最小化权限原则。同时结合实际情况，对访问控制粒度进行设定，如对数据处理人员的访问控制达到用户或进程级，对数据源的控制粒度达到文件级或表级；

d) 采取日志记录或安全审计技术，对数据处理行为进行留痕审计，内容包括但不限于应用层访问记录、接口调用记录、数据库审计等；

e) 涉及敏感数据处理的场景，如系统前台页面展示内容，采用脱敏等去标识化技术对数据进行处理；

f) 建立独立于生产环境的专用测试环境用于开发测试工作，并对测试数据进行脱敏；测试环境使用未脱敏数据的，采取与生产环境同等的安全控制措施。

10.2.2.5 数据交换

数据交换安全，是指在发生数据导入导出、数据共享、数据发布等行为时，实现过程中数据的安全可控与合规。其中包括：

a) 数据交换的需求，尤其是涉及数据跨境流转的场景，要满足相关法律法规、监管要求；

b) 涉及向第三方提供数据的场景，宜采用加密、脱敏等技术手段保护数据安全。如因特殊情况无法进行加密、脱敏的，宜设置单独的查询接口，并采用认证、鉴权、风控、日志记录等技术手段保护数据安全；

c) 因合作或组织架构合并、拆分等原因需要进行数据交换的场景，宜明确数据安全责任主体，并采取相应的技术手段保护数据安全。

10.2.2.6 数据销毁

数据销毁安全，是指在数据删除、存储介质报废等环节的安全性。其中包括：

a) 数据需要彻底删除时，宜采用低级格式化、文件覆盖或存储介质报废等方式避免数据可被成功恢复；
b) 数据删除时，宜考虑数据在其他环境的缓存、备份等数据，实施完整的删除方案；
c) 数据销毁时，宜先判断数据销毁必要性、销毁场景和销毁的数据级别，对于敏感类数据销毁建议使用物理销毁方式，物理销毁模式不可行可采用多次低格复写；
d) 存储介质报废时，宜采用消磁、物理破坏等手段清除所存储的数据，避免数据可被成功恢复。

10.3 数据安全管理最佳实践

数据安全管理的最佳实践，包括以下：

a) 宜从终端、网络层面，建立全面的数据交换监控体系。如终端 DLP、网络 DLP 和邮件 DLP，同时联动其他设备如上网行为管理、堡垒机，构建分析规则，对可疑数据行为进行告警，一线运营人员跟踪确认；
b) 对于敏感文件本地终端存储可采用磁盘和文件加密两种方式，同时可考虑终端水印、数据发现等方案综合应用，保障终端数据的存储和处理环境安全；
c) 数据采集方面，对于数据采集源可采用白名单、签名验签方式，保证数据采集认证、访问控制安全；
d) 数据传输方面，建议采用内容加密和通道加密方式，保证数据传输的保密性。如一般使用 HTTPS 的方式从公网采集数据到 DMZ 的采集服务网关；在内部的数据传输，一般建议使用主机白名单机制，保障数据的传输效率和可靠性；
e) 数据存储方面，结构化数据库一般采用表空间加密，对于核心字段进行列级加密。数据加密宜采用对称算法，若采用非对称算法进行数据加密，密钥应进行加密存储，也可采取 KMS 的方式进行密钥管理；
f) 数据处理和使用方面，在服务端的数据处理，宜重点关注主机加固，同时对于主机的特权管理进行收敛。在终端数据处理和使用方面，除终端环境具备数据防泄露的安全措施之外，还可采取数据脱敏、敏感数据使用打点记录，增加系统打点日志类型，进行全流程追溯；
g) 数据交换，要厘清数据共享方式，例如对于非结构化的数据，可采用统一的数据共享平台，数据共享前宜根据数据级别建立严格的审批矩阵，自动化的审批联动数据共享。对于采用接口方式提供数据的场景，在审批通过的前提下，建立白名单和严格的接口签名验签机制，同时采用 HTTPS 的方式保证数据共享链路安全；
h) 数据销毁，对于云环境存储的数据销毁，建议采用加密擦除的方式，如有必要可采取物理销毁。

11 集中监控与响应管理

11.1 集中监控与响应管理目标

集中监控与响应是指通过一系列的技术、工具、标准化的工作流程，对已部署的安全设备、网络系统、主机应用等信息系统的运行状态、安全状态进行统一的监控管理，并基于已知的告警策略，对触发的告警按照标准化的处置流程进行快速应急响应。目的在于最大化地降低系统运行风险，持续保障运营

管理的有效性，不断提升整体安全运营管理水平。

11.2 集中监控与响应管理过程

11.2.1 日志采集

日志采集是集中监控的首要工作，宜遵循以下：

a) 日志是集中监控的主要数据来源。在不影响性能的前提下，所有业务系统、设备默认开启审计功能并记录日志；
b) 日志记录应尽可能详细，例如操作日志至少包含操作时间、操作用户、来源、操作行为、操作内容、操作结果等关键信息；
c) 日志类型包括但不限于网络日志、主机日志、终端日志、应用中间件日志、业务访问日志等；
d) 日志采集方式尽可能丰富，如使用在目标服务区上安装客户端采集、Syslog 转发、日志文件读取、数据库查询、API 读取等；
e) 日志采集可根据业务系统的重要程度、信息资产的优先级设置采集周期，对于重要业务系统或安全设备宜考虑采用大数据技术，实时采集；
f) 使用开源的日志采集工具和技术，宜综合考虑日志采集和传输的安全性，尽可能采用网络访问控制或主机白名单 IP 等方式，控制日志采集的安全性；
g) 对日志采集的可靠性进行监控，如日志采集失效、日志丢失等建立告警规则，由一线运营人员进行排查分析原因，及时恢复；
h) 审计记录的时间采用一致的时钟源，并定期检测时钟偏差。

11.2.2 日志格式化

因在日志收集过程中会涉及不同系统，不同格式的日志，需要将各种类型日志格式化并形成统一的标准，供日志收集系统来采集和使用，日志采集宜遵循以下：

a) 日志格式化是指对异构日志、不同设备来源的日志建立统一的表字段，将各类异构日志映射成统一定义字段格式的日志；
b) 日志格式可以是纯文本、JSON、XML、数据库记录，日志提供方宜提供相应的字段说明及日志样例，确保解析准确；
c) 在构建统一表字段时，宜尽可能将字段设置为更灵活、通用的名称；
d) 宜在系统变更流程中增加日志变更管控手段，当系统升级导致日志变化后，宜重新制定解析规则，由一线进行日志回归验证；
e) 敏感数据应提前进行脱敏处理，日志中禁止记录敏感数据。

11.2.3 制定告警规则

日志完成统一收集后，需要制定相应的告警规则以对安全运行风险进行统一的监控管理，告警规则的制定宜遵循以下：

a) 告警规则是指单一的日志来源所产生的告警信息，如超级管理员登录活动目录域控制器告警；
b) 告警规则的制定宜根据内部关注的高风险行为定制化制定，一般建议包含以下内容，如高危操作、变更操作、特权操作、高风险安全设备告警等；
c) 告警规则一般由二线运营人员进行制定，告警规则的准确性和有效性建立在对日志的熟悉和理解基础上，一般可根据某一个场景进行操作，再通过日志还原操作行为，验证告警规则是否生效；
d) 告警规则宜参考配置管理要求，有详细的版本信息和变更日志，便于回溯管理。

11.2.4 制定事件规则

将告警信息通过规则进行关联分析，产生事件。事件规则制定宜遵循以下：

a) 事件规则重点是在关联分析。在日志格式化、各类异构日志标准字段的前提下，建立多来源的分析模型和规则，根据场景制定关联规则；
b) 关联分析一般由二线专家分析多源日志后，制定关联分析模型和规则，再根据场景验证事件规则的有效性，验证通过后，交付一线团队运营。如活动目录域控制器超级管理员登录场景，日志来源于域控、DHCP 或者准入日志，当匹配到目前登录用户与 IP 准入用户不一致时，则告警；
c) 事件规则宜有详细的版本信息和变更日志，用于规则制定的变更回溯。

11.2.5 事件响应与处理

针对产生的安全事件，安全运营人员宜遵循以下开展响应和处理工作：

a) 宜建立统一的安全运营平台，在平台上进行告警、事件的产生、处理、审核、复盘等全流程的安全运营；
b) 宜建立针对各类告警、安全事件的 SOP，一线运营人员按照 SOP 开展常态化运营工作；
c) 宜根据事件级别，制定响应策略，响应策略宜包含响应时限、响应人员、响应流程；
d) 宜周期性的进行安全运营响应的事件复盘和汇总，定期发送运营报告；
e) 应建立应急事件响应、通报流程，依据《证券期货业网络安全事件报告与调查处理办法》规定，各机构应向中国证监会及其派出机构报告并开展调查处置。

11.3 集中监控与响应管理最佳实践

集中监控与响应的最佳实践，包括以下：

a) 日志采集宜尽量覆盖重要业务系统的网络、主机、应用、关键业务操作类日志。基础系统日志至少包含 DHCP、域控、邮件服务器、DNS 等日志；安全设备的日志宜全量采集，包括不限于防火墙、防病毒、WAF、邮件网关、安全沙箱、DLP、IPS、IDS、终端安全软件等；
b) 日志采集可采用大数据相关技术，提供近实时的日志流采集，如采用 Flink、Kafka 等常用的流处理工具，尽可能保障监控响应的及时性；
c) 日志格式化，可以建立统一的 Schema，对异构日志进行解析。重点关注解析器的负载性能，保证解析的实时性和有效性；
d) 异构日志重点关注各类日志的时间同步问题。内部宜建立统一的 NTP 服务器，保障日志时间的一致性；
e) 日志格式可能会随着的系统升级或功能变更有相应的变化，宜有专人对日志格式进行验证；
f) 日志在格式化时，可进一步进行富化。例如借助 CMDB 系统中的信息，进一步完善信息资产相关属性信息；
g) 告警和事件规则，宜定期进行场景验证，保证其运行符合预期；
h) 告警方式宜尽可能丰富，如通过即时通讯工具告警、邮件告警、短信告警，避免单一告警方式的失效所带来的运营盲点；
i) 根据 SOP 进行事件响应和处理，一般 SOP 至少包括：事件编码、事件描述和现状描述、事件告警规则、告警内容、标准操作步骤、闭环条件；
j) 定期对事件进行统计分析，揭示主要风险、分析根本原因，并复盘总结处理过程；
k) 关注外部安全事件和威胁情报，并及时评估对本企业的影响性，做好后续的应急处置措施；
l) 使用 SOAR 系统将安全相关系统 API 打通，通过预定义的剧本形成标准化作业流程，对安全事件实现自动化响应和处置，可有效提升安全运营效率。

12 持续改进管理

12.1 持续改进管理目标

在现有的安全建设的基础上，通过信息安全度量指标（见附录 A）、安全检测措施、有效性验证等机制，来衡量安全工作的整体效果是否符合预期目标，对于不符合预期的安全工作进行改进优化，提升安全运营水平，不断提升组织的安全防护能力。

12.2 持续改进管理过程

12.2.1 安全检测

安全检测是指组织内部的常态化安全检测机制，一般包括定期的漏洞扫描及基线检查：

a) 定期开展漏洞扫描工作，并根据业务系统的重要程度、网络环境（是否互联网可访问）、漏洞危险级别、漏洞利用难易程度、被影响的信息资产暴露程度综合判断漏洞修复的紧急程度。一般漏洞扫描与漏洞管理平台对接完成自动化的漏洞跟踪；
b) 定期开展基线检查工作，对不合规的基线配置进行及时整改并做好复查工作。

12.2.2 安全审计

安全审计一般分为内部审计和外部审计：

a) 一般外部审计中涉及到的安全审计重点在审计安全控制点的合规性，是否落实各类控制要求，落实的技术工具和管理措施是否有对应记录文档，以此证明合规；
b) 内部审计主要是组织内部其他监管部门来执行，如审计部门。对于安全风险的发现、处置、关闭整个过程的合规性进行审计，是否有对应的风险发现报告、发现依据、处置过程记录文档、关闭风险项前置条件定义等，还会对剩余风险的缓释措施是否合规进行审计。内部审计也可对安全人员的操作进行合规检查，尤其是敏感策略配置、敏感类日志操作审计、证据文件查看等涉密性操作等进行审计，是否存在权限滥用或违规操作的情况。

12.2.3 有效性验证

一般有效性验证包括安全运行状态有效性验证、安全检测与防御能力有效性验证：

a) 安全运行状态有效性验证侧重于对系统与流程运行状态有效性的验证，主要包括以下：
    1) 安全系统运行的有效性验证，可通过监控系统对安全系统的存活状态进行统一监控，并验证其有效性。监控指标可为 CPU、内存、磁盘、网卡的使用率，网卡的状态等；
    2) 日志采集的有效性验证，可对客户端采集节点、日志采集系统、日志处理系统状态及日志采集量等进行监控，并验证其有效性；
    3) 告警规则有效性验证，可通过发起单一攻击场景事件来验证其有效性；
    4) 事件规则有效性验证，可通过发起多个不同攻击场景事件来验证其有效性；
    5) 应急响应流程的有效性验证，可通过不定期发起攻击事件来验证其有效性。
b) 安全检测与防御能力有效性侧重于验证现有的各类安全系统的功能及其内置检测、防御规则的有效性，主要包括以下：
    1) 通过在攻击链的各个环节使用不同的攻击战术开展模拟攻击，可整体验证现有安全检测与防御检测能力是否存在不足和缺陷；
    2) 通过使用新型的攻击方式或攻击工具开展模拟攻击，可快速验证现有安全检测与防御检测能力是否可以对抗此类新型战术。

12.3 持续改进管理最佳实践

持续改进的最佳实践，包括以下：

a) 漏洞扫描结果宜自动同步到漏洞运营平台，一线运营人员按照漏洞的影响性大小来确定修复优先级，在系统中下发修复指令自动通知到业务方进行漏洞确认。漏洞确认后进入修复环节，在修复环节宜有修复时长的限制，自动跟踪和提醒。修复完成后，业务方反馈修复确认，自动触发扫描任务进行扫描，扫描后判断漏洞不存在，发送结果自动关闭漏洞工单，运营人员进行审核入库；

b) 一般基线检查宜对接变更管理流程。当变更完成后，进行基线检查，将检查结果与上次结果进行对比，明确变更内容。基线检查一般除检查配置外，还宜检查主机访问控制策略、监听端口、网络连接等信息；

c) 针对安全设备功能有效性检测，可借助同类其他安全设备进行交叉验证。如公司办公网段访问互联网仅开放 80 端口和 443 端口，可通过网关流量设备检测办公网互联网出口流量，当存在非 80 端口和 443 端口访问的流量，则证明策略失效。此类规则可根据网关流量设备日志，制作有效性告警检测规则；

d) 针对日志采集有效性检测，一般是监控在单位时间内日志有无。另外，还可比对单位时间内发送日志量和接收日志量，判断日志是否有丢失情况；

e) 内部红蓝对抗或者虚拟红队，常态化的进行渗透，也是告警策略和事件规则有效性的一种检测手段；

f) 对于一线运营闭环的安全事件，二线专家宜定期进行分析其运营过程是否合理，运营时分析的日志依据、闭环的理由是否充分，及时发现运营过程中的问题，复盘改进。通过定期培训，强化运营人员的技能水平，提升运营效能。

附 录 A
（资料性）
信息安全度量指标

A.1 安全管理度量指标

安全管理相关度量指标可参考以下：

a) 安全运营总体目标完成情况，如考核期内重大安全事件数量、安全事件带来的经济损失等；
b) 年度内审及外审符合情况，如高风险不符合项的数量、上期审计问题的关闭率；
c) 员工安全教育的效果，如钓鱼邮件测试的中招人数比例、安全培训考试通过率、安全培训参与率等。

A.2 基础安全管理度量指标

基础安全管理相关度量指标可参考以下：

a) 安全软件客户端相关，如防病毒客户端安装覆盖率及客户端离线率、病毒感染和处置数量；
b) 准入产品的有效性，如准入产品造成的可用性事件，同一台机器上多个账号的准入，同一个账号在多台机器上准入等重点关注异常事件数量和处置情况等；
c) 补丁管理及处置相关，如补丁的更新率、及时率；
d) 安全基线管理有效性，如安全基线符合率。

A.3 信息资产管理度量指标

信息资产管理相关度量指标，如资产纳管率、准确性、资产总量、资产分类数量、无主资产数量、新增资产数量、下线回收资产数量。

A.4 漏洞管理度量指标

漏洞管理相关度量指标，如扫描发现的高危漏洞数量、漏洞平均修复时长、漏洞修复率等。

A.5 开发安全管理度量指标

开发安全管理相关度量指标可参考以下：

a) 安全测试能力，如全量测试应用数量/应用总数，上线前安全测试发现的漏洞数量，上线后安全测试发现的漏洞数量，监管部门发现的安全漏洞数量，自动化检测平台发现的漏洞总量、每应用的测试时间等；
b) 开发人员安全能力，如高危漏洞数量最多的应用，发现最多的漏洞类型，开发安全培训通过率，漏洞修复最长时间，漏洞修复时间最长的应用，超时未修复应用总量等；
c) 安全模块化程度，如安全团队提供的安全组件数量，安全组件被调用数量等。

A.6 数据安全管理度量指标

数据安全管理度量指标，如敏感信息监测的覆盖率、敏感信息被非法篡改的次数、年度外部单位通报的数据安全事件、年度内部发现的数据安全事件等。

A.7 集中监控与响应管理度量指标

集中监控与响应管理相关度量指标可参考以下：

a) 预警及处置能力，如安全事件发现数量、安全事件平均发现时间、安全事件平均响应时间、安全事件平均处置时间、紧急安全事件数量（监管通报等）、 红蓝对抗中未发现的安全事件数量、安全事件处置率等；
b) 风险暴露面，如问题最多的安全风险、问题最多的主机和应用、监控发现问题与渗透测试发现问题重合数量等；
c) 人员绩效情况，如一线跟进安全告警、事件处理平均时间、二线分析安全事件平均时间、升级到二线/三线的安全事件数量占比、二线人员有效分析/分析总量等；
d) 平台及规则的有效性，如规则误报率、一个月内未触发告警规则总数/规则总数、新增内部威胁情报数量等。

参 考 文 献

[1] ISO/IEC 27000 family-Information security management systems

[2] ISO/IEC 18028 family:2005-Security techniques-IT network security

[3] ISO/IEC 18043:2006 Information technology-Security techniques-Selection,deployment and operations of intrusion detection systems

[4] GB/T 25068.1-2020 信息技术 安全技术 网络安全 第1部分：综述和概念

[5] GB/T 28454—2020 信息技术 安全技术 入侵检测和防御系统（IDPS）的选择、部署和操作

[6] GB/T 28458—2020 信息安全技术 网络安全漏洞标识与描述规范

[7] 中国证券监督管理委员会.证券期货业网络安全事件报告与调查处理办法(证监会公告〔2021〕12号），2021年6月4日

[8] OWASP Top 10 web application security risks

[9] CWE/SANS Top 25 most dangerous software errors

[10] SEI CERT Coding Standards