ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX

网络安全技术 网络安全运维实施指南

Cybersecurity technology - Implementation guide of cybersecurity operation and maintenance

（征求意见稿）

2024-04-15

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件由全国网络安全标准化技术委员会（SAC/TC260）提出并归口。

本文件起草单位：中国信息安全测评中心、杭州安恒信息技术股份有限公司、国家信息中心、绿盟科技集团股份有限公司、北京长亭科技有限公司、奇安信科技集团股份有限公司、北京梆梆安全科技有限公司、中国信息通信研究院、北京天融信网络安全技术有限公司、三六零数字安全科技集团有限公司、清华大学、深信服科技股份有限公司、中国联合网络通信集团有限公司、中国科学院信息工程研究所、广州中软信息技术有限公司、新长城科技有限公司、上交所技术有限责任公司、杭州迪普科技股份有限公司、北京知其安科技有限公司、国网网安（北京）科技有限公司、上海三零卫士信息安全有限公司、中福彩科技发展（北京）有限公司、罗克佳华科技集团股份有限公司、安天科技集团股份有限公司、华能信息技术有限公司、北京威努特技术有限公司、北京升鑫网络科技有限公司、北京赛西科技发展有限责任公司、深圳市博通智能技术有限公司、北京灰度科技有限公司、天翼云科技有限公司、广东网安科技有限公司、宁波和利时信息安全研究院有限公司、黑龙江安信与诚科技开发有限公司。

本文件主要起草人：王琰、杨婧婧、袁明坤、陈星、田丽丹、刘蓓、杨莹、杨家海、曹嘉、李昀磊、许玉娜、陈祥喜、方宁、代杭旅、耿贵宁、杨坤、张龙、马玉、云瀚、卫世光、申东胜、田宝松、房慧丽、刘吉林、聂君、王喜伟、刘彪、周凯、谢美程、郭建林、王馨茹、潘中英、周森、白峻、程度、卢志刚、周灵军、吕丰丰、辛晨、魏书山、崔馨、杨亮。

网络安全技术 网络安全运维实施指南

1 范围

本文件提出了网络安全运维参考框架、网络安全运维提供方和运维人员条件、网络安全运维效果评估模型，给出了运维管理、识别、防御、监测、响应和协同等网络安全运维主要工作环节的实施内容。

本文件适用于网络安全运维提供方、网络安全运维需求方。可为网络安全运维的实施提供指导，也可为网络安全运维需求方、第三方机构对网络安全运维实施效果和安全防护水平进行评估提供参考。

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。

GB/T 20984 信息安全技术 信息安全风险评估规范

GB/T 20986-2023 信息安全技术 网络安全事件分类分级指南

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25069-2022 信息安全技术 术语

GB/T 28827.3-2012 信息技术服务 运行维护 第3部分：应急响应规范

GB/T 32914-2023 信息安全技术 网络安全服务能力要求

GB/T 42446 信息安全技术 网络安全从业人员能力基本要求

GB/T 42461 信息安全技术 网络安全服务成本度量指南

3 术语和定义

GB/T 25069-2022界定的以及下列术语和定义适用于本文件。

3.1

网络安全运维 cybersecurity operation and maintenance

组织为抵御网络空间安全威胁，控制网络安全风险，确保业务持续、稳定运行，保证业务承载数据的保密性、完整性和可用性，统筹技术、流程、人员和管理等要素，持续开展识别、防御、监测、响应、协同等工作的一种网络安全服务方式。

[来源：GB/T 30283-2022，3.10 有修改]

4 缩略语

下列缩略语适用于本文件：

DDOS：分布式拒绝服务攻击（distributed denial of service attack）

DNS：域名系统（domain name system）

IT：信息技术（information technology）

MSS：托管安全服务（managed security service）

SaaS：软件即服务（Software as a Service）
SLA：服务级别协议（service level agreement）
SOC：网络安全运维中心(security operations center)

5 概述

5.1 网络安全运维参考框架

网络安全运维包括运维管理、识别、防御、监测、响应和协同六个环节。运维管理对网络安全运维的整体活动进行管理和规划，考虑组织网络安全长期改进和投入需要做出的决策，提出网络安全运维整体方案。运维管理、识别、防御和监测四个环节是针对网络安全风险防范的常态化持续性工作，在整个网络安全运维活动中是一个长循环过程。同时，识别、防御、监测和响应这四个环节又是针对网络安全事件处置的应急性工作，在整个网络安全运维活动中是一个相对较短的循环过程。协同包括了组织内外部的协调与协作，目的是提高组织的安全运维的效能与防护水平。网络安全运维的模式、内容需与运维需求方协商一致，并在网络安全运维过程中，基于服务级别协议（SLA）和运维实际效果进行评估，评估的结果用于进一步改进网络安全运维的管理和实施水平。

网络安全运维活动存在长循环、短循环两种工作方式。在短循环内分配的资源（人员、预算、系统、跨部门、外部第三方）内，需要持续改进以解决安全响应与处置的业务过程中出现的问题。例如，任务的简单自动化，用于事件或数据分析平台工具的改进，以及报告事项的审查等。而长循环需要从长期的观点和规划角度来考虑持续改进网络安全事件的发现、响应与处置的效能，例如，引入新的安全产品、对安全策略的审查以及针对安全系统进行的大规模配置更改与升级。针对网络安全运维效果的评估既是长循环的驱动力，也是短循环的驱动力。

网络安全运维参考框架如图1所示。

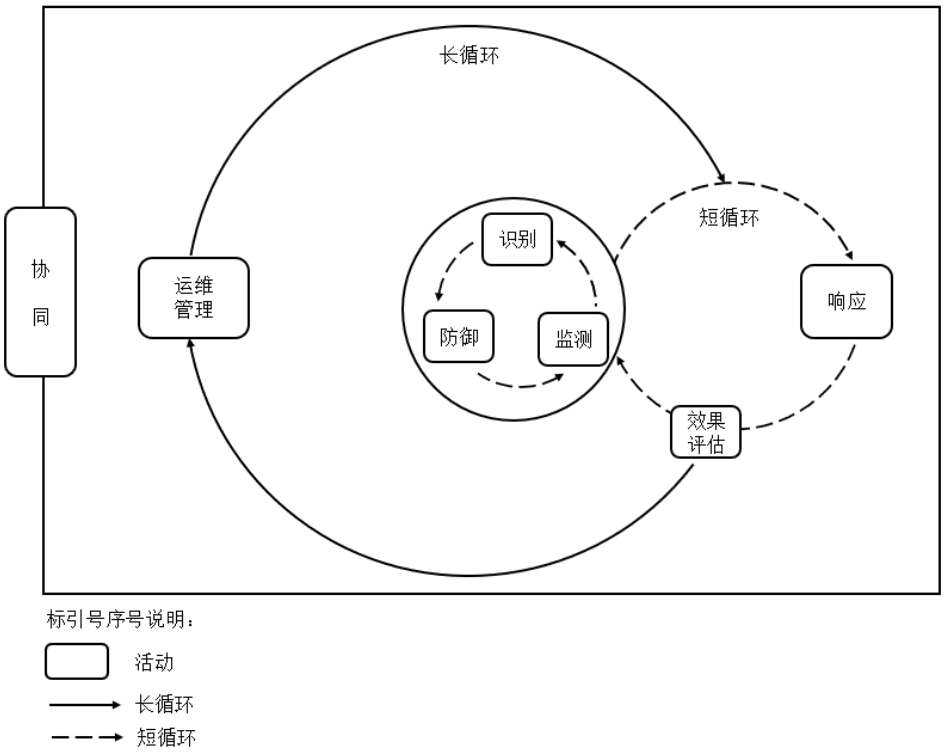

图1 网络安全运维参考框架

5.2 网络安全运维模式

网络安全运维模式主要包括以下三类：

a) 全自建网络安全运维模式。对安全性和数据保护的要求较高，具备足够的安全资源投入，能够持续有效网络安全运维的网络安全运维需求方，选择自主建设安全运维中心。此类组织、机构和设施具备完善的安全运维人员配置、管理机制和人才培养机制，自主建立安全运维中心（SOC），整合安全防护技术、安全运维工具与平台和人员等要素，建立网络安全监测、分析、处置、应急等网络安全运维流程；

b) 联合网络安全运维模式。网络安全运维需求方联合网络安全运维提供方共同建立安全运维中心（SOC），并为网络安全运维需求方提供驻场托管式网络安全运维；

c) 全托管网络安全运维模式。MSS 主要依靠网络安全运维提供方建立的企业安全运维中心（SOC），通过云平台或远程管理系统，管理组织 IT 资产的安全信息、管理安全工具、监测和改善组织的安全状况，识别、检测、分析和响应组织所面临的网络安全事件。以满足对安全人员、技术和流程外包的需要。

5.3 网络安全运维目标

网络安全运维的目标是为组织提供高效、全面的安全保障，确保组织的信息系统能够抵御各种形式的网络攻击，提高用户和员工的安全意识，以实现更高水平的网络安全防护，具体包括：

a) 保障业务持续发展：确保系统的连续性和稳定性，在面临挑战和威胁时保障业务的正常运行；

b) 使安全能力达到组织、机构和设施的需求：不同的组织、机构和设施对安全能力的要求有所不同，安全运维提供方根据这些需求来制定和实施相应的安全策略和措施，确保其安全能力能够满足要求；

c) 使组织、机构和设施的信息安全风险处于可接受的范围：网络安全运维提供方帮助组织、机构和设施识别、评估和管理所面临的信息安全风险，并采取必要的措施来降低风险；

d) 确保网络安全能力持续有效：通过网络安全运维，防范各种网络安全威胁，确保网络的安全性和可用性，使网络系统的安全性得到持续维护和提升；

e) 满足安全监管要求：网络安全运维提供方帮助组织、机构和设施满足各种安全监管要求，并提供必要的证明材料，如审计报告、安全漏洞修补证明等，确保其信息安全管理工作符合相关法规和标准。

6 网络安全运维具备的条件

6.1 网络安全运维提供方

网络安全运维提供方向网络安全运维需求方提供网络安全运维时，需满足GB/T 32914-2023中第5章的要求。如向对网络安全运维有更高要求的服务需求方（如党政机关、关键信息基础设施运营者等）提供网络安全运维时，还需满足GB/T 32914-2023中第6章的要求。

6.2 网络安全运维人员

6.2.1 网络安全运维需求方人员

网络安全运维需求方人员是指对其所在单位的信息系统、基础设施、安全设备开展安全运维工作的人员。网络安全运维需求方人员宜具备：

a) 清晰网络安全运维组织架构，明确网络安全运维角色和职责；

b) 明确本单位网络安全运维的目标和方法；
c) 掌握既有网络情况，能够明确软硬件及网络扩容需求，能够定义和评估业务系统面临的安全风险；
d) 根据应用系统特点和运行需求，充分与安全运维提供方人员沟通和协作，制定网络安全运维实施方案；
e) 能够识别与信息系统相关的所有资产，构建以资产为核心的网络安全风险管理机制；
f) 定期监督、评估网络安全运维效果，确保网络安全运维符合业务需求。

6.2.2 安全运维提供方人员

安全运维提供方人员是指向运维需求方提供安全运维的人员。运维提供方人员需满足：

a) 为正式员工。参与重要保障和关键信息基础设施的运维提供方人员还需提供无犯罪记录证明，并通过安全背景审查，确保安全运维提供方人员安全可靠；
b) 根据不同的工作角色，安全运维提供方人员除满足 GB/T 42446 中的要求外，还需具备下列技术和能力，包括但不限于：
   1) 针对物理环境、网络、系统的访问控制进行加固，以确保按照业务要求限制对信息和信息系统的访问；
   2) 基于信息安全策略，制定备份策略，保证备份的有效性和可靠性；
   3) 通过全面收集并管理信息系统及相关设备的运行日志，帮助排查定位和溯源网络安全攻击；
   4) 定期借助漏洞扫描工具对信息系统及其软硬件系统存在的漏洞进行扫描，发现存在的脆弱性，及时更新保持系统处于安全状态；
   5) 建立监视、发现、分析和报告信息安全事态和事件流程，确保快速、有效和有序地响应信息安全事件；
   6) 定期参与安全意识教育与培训，了解信息系统安全风险及安全运维责任及组织的信息安全策略和相关规程。
c) 每年完成一定时长的网络安全意识培训。

6.2.3 安全运维协助人员

安全运维协助人员是指以技术外协的方式向运维需求方提供网络安全专业培训、安全咨询、威胁信息共享、网络安全重保等专项安全运维人员。安全运维协助人员需满足：

a) 能够配合安全运维提供方人员，及时响应和处理安全事件，记录归档优化安全事件管理；
b) 能够识别与信息系统相关的所有资产；
c) 及时关注官方渠道了解信息系统及其软硬件系统存在的脆弱性，及时更新保持系统处于安全状态；
d) 定期参与安全意识教育与培训，了解信息系统安全风险及安全运维责任及组织的信息安全策略和相关规程，定期参与技能考核；
e) 对于参与重要保障和关键信息基础设施的安全运维协助人员需提供无犯罪记录证明，确保安全运维协助人员安全可靠。

7 网络安全运维业务建立

7.1 网络安全运维实施内容

基于组织对网络安全运维的具体要求，网络安全运维实施内容如图2所示。

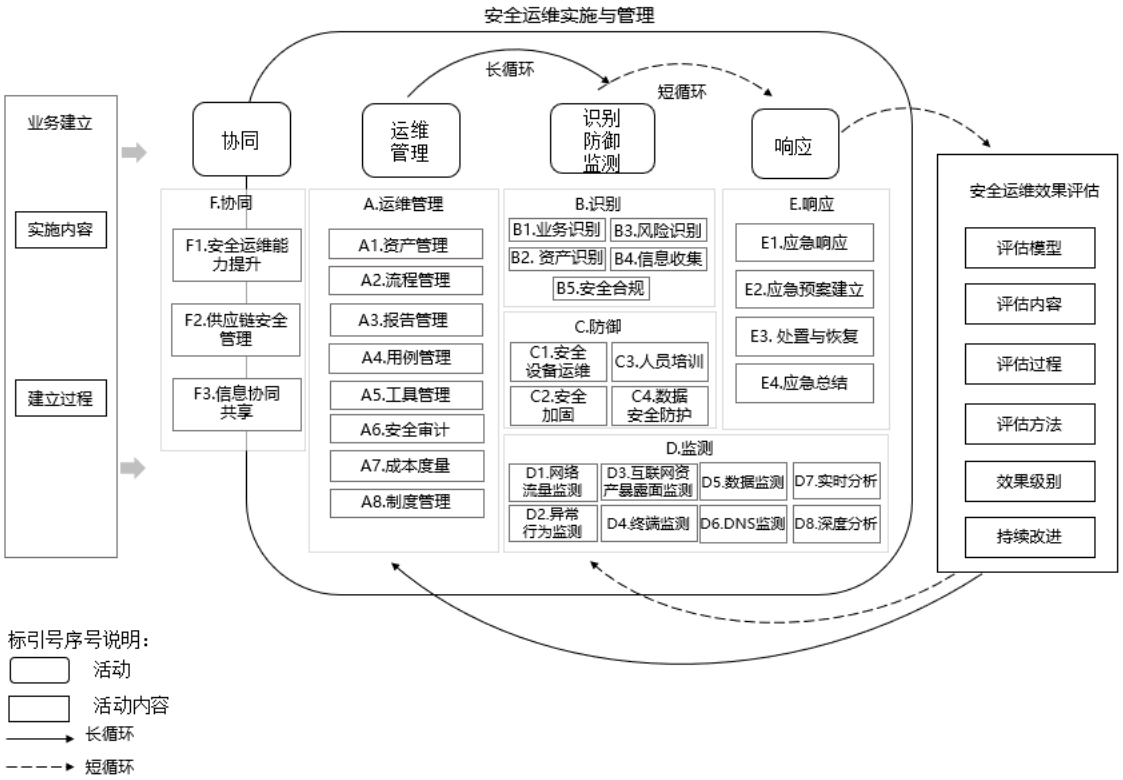

图2　网络安全运维实施内容

基于网络安全运维参考框架（如图1）和网络安全运维实施内容（如图2），结合网络安全运维实践，建立网络安全运维清单，并持续更新。如表1所示：

表1　网络安全运维清单

序号	网络安全运维内容
A	**运维管理**
A-1	安全运维资产管理
A-2	安全运维流程管理
A-3	安全运维报告管理
A-4	安全运维用例管理
A-5	安全运维工具管理
A-6	安全审计
A-7	安全运维成本度量
A-8	安全运维制度管理
B	**识别**
B-1	业务识别
B-2	资产识别
B-3	风险识别
B-4	信息收集

序号	网络安全运维内容
B-5	安全合规
C	**防御**
C-1	安全设备运维
C-2	安全加固服务
C-3	人员培训
C-4	数据安全防护
D	**监测**
D-1	网络流量监测
D-2	异常行为监测
D-3	互联网资产暴露面监测
D-4	终端监测
D-5	数据监测
D-6	DNS监测
D-7	实时分析
D-8	深度分析
E	**响应**
E-1	应急响应
E-2	应急预案建立
E-3	处置与恢复
E-4	应急总结
F	**协同**
F-1	安全运维能力提升
F-2	供应链安全管理
F-3	信息协同共享

7.2 网络安全运维业务建立过程

在实施网络安全运维之前，网络安全运维提供方根据需求方的安全需求，创建网络安全运维表单，表单如表2所示，创建过程包括：

a) 网络安全运维提供方创建并提供网络安全运维清单（参见 7.1）；
b) 根据需求方的实际需求，确定网络安全运维模式；
c) 在清单中选择运维项并添加组织特需的运维项来确定网络安全运维目录；
d) 为运维目录中的每个运维项建立一个配置文件，包括：所有者、运维团队角色、职责以及运维模式，并根据 SLA 确定运维目标。

表2 网络安全运维表单示例

运维名称	运维模式	运维目录	SLA目标
示例 1	自主型	配置文件1	效果评估报告1
示例 2	托管型	配置文件2	效果评估报告2
示例 3	托管型	配置文件3	效果评估报告3
示例 4	联合型	配置文件4	效果评估报告4

8 网络安全运维实施

8.1 运维管理

运维管理是对与定义、设计、规划、管理、架构和审计等相关的所有策略负有责任和义务，目的是确保网络安全运维活动的长期发展和业务目标的稳定运行。具体包括以下内容：

a) 资产管理。编制并保存运维需求方的资产清单，资产属性包括资产名称、资产编号、IP 地址、序列号、所处位置、责任部门、责任人、重要程度等；并根据资产的重要程度进行资产和线路标识管理；资产管理对象包括重要网络设备、安全设备、主机系统、业务系统、门户网站、邮箱及接口服务等；

b) 流程管理。建立安全运维作业流程，指导和规范运维团队开展安全运维工作，包括安全监测流程、风险处置流程、应急响应流程、策略变更流程、安全加固流程、信息共享流程、威胁信息运维流程等；

c) 报告管理。运维报告包括不限于各类日报、周报、月报、年报、建议书、安全事件报告、总结分析报告等，并建立报告审核流程，确保报告格式和内容的规范性、有效性；

d) 用例管理。用例管理覆盖识别、监测、防御和响应全过程运维管理，用例内容包括名称、执行周期要求、责任部门、内容和注意事项等，避免误操作带来的安全风险；

e) 工具管理。编制运维工具清单，包括工具名称、类型、型号、版本号、作用、存放位置、维护部门等信息，定期更新维护，提升安全运维效率；

f) 安全审计。安全审计是系统的、可测量的对组织如何在特定地点或时间内实施安全策略和控制进行审计。安全人员可间接参与审计活动，以便提供有关控制实施状态的必要信息和证据。对运维需求方的运维操作进行审计、查阅和回放，确保所有操作行为可审计、可追溯；

g) 成本度量。参照 GB/T 42461 对安全运维总成本、人力成本、非人力成本等方面进行度量；

h) 制度管理。参照 GB/T 22239 相关要求，建立网络安全运维工作领导小组，编制保密管理、介质管理、设备安全、监测预警、网络安全、系统安全、安全培训、备份与恢复、变更管理等相关制度，并制定网络和信息安全突发事件应急预案，规范运维团队日常行为，降低网络安全风险。

8.2 识别

8.2.1 概述

识别是指通过业务识别、资产识别、风险识别、信息收集和安全合规检查等工作，实现网络安全运维的风险趋势分析、预警和发现。

8.2.2 业务识别

业务是实现组织发展规划的具体活动，业务识别是开展网络安全运维的基础工作，包括业务的属性、定位、完整性和关联性识别。可根据GB/T 20984进行业务识别，业务识别内容包括：

a) 建立组织的业务台账，明确业务属性，包括业务功能、业务对象、业务流程、业务范围、覆盖地域等；

b) 识别业务在组织发展规划中的定位，包括发展规划中的职能定位、与发展规划目标的契合度、业务布局中的位置和作用、竞争关系中竞争力强弱等；

c) 识别组织中的独立业务和非独立业务；

d) 识别组织业务与其他业务的关联关系和关联程度。如：并列关系、承接关系、直接或间接关联关系等。关联程度包括紧密关联和非紧密关联；

e) 对识别的业务进行重要性赋值，确定重要业务链和关键业务链，明确支撑重要和关键业务的资源分布和运行情况。
f) 当业务范围或业务的重要性发生变化时，重新进行业务识别。

8.2.3 资产识别

资产是对组织具有价值的信息或资源，是安全策略保护的对象，也是开展体系化、精细化网络安全运维的基础。组织对资产进行全生命周期管理，建立健全资产管理制度，对资产全流程进行跟踪和管理。资产识别内容包括：

a) 建立健全完善的资产管理制度，对资产上线、变更、下线等流程进行跟踪和管理，明确资产管理责任人及资产供应链；
b) 建立健全准确的资产台账，定期通过技术手段识别未知或新增的资产，动态确认并完善更新资产基本属性、安全属性、管理属性、指纹信息，识别资产间的关联性，绘制资产关联图谱。根据 GB/T 20984 的方法进行分类分级和资产赋值，并在资产投入使用前完成资产纳管。采用主动或被动资产探测技术识别资产，并动态更新；
c) 基于资产类别、资产重要性和支撑业务的重要性，确定资产防护的优先级；梳理和验证安全防护设施对资产的防护状态，同步更新资产安全防护属性信息；
d) 定期通过技术手段感知资产属性变更，根据预设规则识别变更风险，开展安全告警、通报、处置；对变更的敏感项进行记录和审核，以便事后审计和追溯；
e) 根据域名、IP、端口、中间件、应用、技术架构、变更状态、业务类型（自定义）等条件对资产进行查询、统计，并能对资产进行周期变化监控。基于最小化原则，尽可以收敛互联网暴露面。资产转移或处置时，及时完成资产清单的更新，资产管理责任人识别可能出现的风险并予以控制，并保留相关记录。

8.2.4 风险识别

8.2.4.1 威胁识别

威胁是一种对组织及其资产构成潜在破坏的可能性因素或者事件。威胁识别主要涉及对系统或网络造成威胁的各种因素进行识别和评估。这通常包括威胁的来源、途径和意图等，以及威胁利用脆弱性的可能性。

威胁识别内容包括：

a) 威胁识别内容：包括威胁来源、主体、动机、时机和频率等；
b) 威胁来源：对威胁分类前，识别威胁来源，包括环境、意外和人为三类。根据威胁来源的不同，将威胁划分为信息损害和未授权行为等威胁种类；
c) 威胁主体：根据人为和环境区分，人为分为国家、组织团体和个人，环境氛围一般的自然灾害、较为严重的自然灾害和严重的自然灾害；
d) 威胁动机：可以分为恶意和非恶意；
e) 威胁频率：根据经验和有关的统计数据进行判断，综合以往安全事件报告中的威胁和频率统计、实际环境通过检测工具及日志发现的威胁和其频率统计、实际环境监测发现的威胁及其频率统计、近期公开发布的社会或特定行业威胁及其频率统计。

8.2.4.2 脆弱性识别

脆弱性是组织、系统和信息资产本身存在的，如果没有被相应的威胁利用，脆弱性本身不会对组织和信息资产造成损害。由于信息资产的脆弱性的存在具有隐蔽性，需针对每一项需要保护的资产，识别

可能被威胁利用的脆弱点，基于安全脆弱性问题可能造成安全威胁的风险级别评定修复优先级，并采取适合的技术或管理措施进行防范。脆弱性识别内容包括：

a) 脆弱性识别：采取问卷调查、工具检测、 人工核查、文档查阅、渗透测试等手段探测和识别资产在物理环境、网络结构、系统软件、应用中间件、应用系统、技术管理、组织管理等方面存在技术脆弱性或管理脆弱性问题。根据资产价值、类型、暴露面等维度针对资产采取不同的脆弱性探测策略；
b) 脆弱性评估：对检测发现的安全脆弱性问题进行研判和甄别，并基于资产价值、资产暴露面类型、脆弱性严重程度、脆弱性问题利用难度等维度评估可能造成安全威胁的风险级别，评定脆弱性问题修复先后次序和、脆弱性利用防范方式；
c) 脆弱性管理：借助信息系统将所有安全脆弱性问题列入统一工单管理，开展通报、接收、修复、复测等工作，定期跟踪、督促修复工作进展，复测通过后关闭工单。定期或不定期组织开展安全脆弱性问题分析总结工作，调整安全策略、优化运维流程、健全完善安全管理制度。

8.2.5 信息收集

汇集内、外部各种网络安全威胁相关的信息，如资产信息、漏洞信息、攻击信息、事件信息等，经甄别、分类、研判、整理输出具有相关性、洞察力、情景性和可行动性的信息，辅助开展安全加固、应急处置和安全决策等安全运维工作。信息收集内容包括：

a) 信息获取：审查并选择必要且适当的内外部各种途径来源的多源威胁相关信息，包括资产信息、漏洞信息、攻击信息、事件信息等，经聚合、去噪、去重、归并等一系列处置后，入库待研判；
b) 分析研判：对待研判的威胁相关信息进行核验和甄别、加工完善、分级分类、整理汇编成机读的运行级信息、可执行的战术级信息或安全决策的战略级信息；
c) 信息使用：对威胁信息进行查询查阅、数据提取分析辅助安全决策、应急响应，或基于自动化技术对威胁信息进行碰撞和关联分析开展自动化威胁处置工作，或识别、审查、净化、处理、保护可共享的威胁信息用于信息共享。

注：信息收集过程所涉及的信息宜根据其敏感程度采取适当的保护措施。

8.2.6 安全合规

安全合规主要是国家法律法规、政策、标准规范以及区域、行业的网络安全监管要求中识别、分析组织安全建设需求，并通过定期开展符合性安全合规检查，明确现有安全保障措施与安全监管要求差距，依法依规开展安全建设，确保组织始终满足国家、区域、行业监管要求。安全合规内容包括：

a) 评估检测：依据国家法律法规、政策、标准规范以及区域、行业的网络安全监管要求，对安全现状进行自查或配合安全测评机构/上级监管机构开展合规检查，查找不符合项，出具安全合规评估检测报告；
b) 合规整改建设：根据安全合规评估检测报告，制定科学、合理的安全合规建设方案，有序开展安全合规整改建设，并针对建设整改结果开展评估检测复测，确保对整改过程进行有效的闭环管理。

8.3 防御

8.3.1 概述

防御是指通过安全设备和应用运维、安全加固、人员培训和数据安全防护等活动，实现网络安全运维的纵深防御。

8.3.2 安全设备运维

安全设备运维主要是对组织内的各种安全设备进行全面、细致、有效的日常维护和管理，以确保其正常运行并能够及时需对各种安全威胁。安全设备运维内容包括：

a) 可用性监控：实时监控安全设备的运行状态和性能指标，及时发现和处理设备故障或异常情况，确保设备的可用性和可靠性；
b) 设备更新和升级：根据组织机构的安全需求和设备厂商的建议，及时更新和升级安全设备，以提高设备的防护能力和安全性；
c) 安全策略管理：根据业务及安全需求，调整和修改安全设备策略，并对策略进行归并及优化；
d) 安全配置管理：定期梳理检查安全设备的配置，如访问控制配置等。对配置文件定期进行备份，并将备份文件存储在安全可靠的位置。同时，应测试配置恢复功能，确保在需要时能够快速恢复设备配置；
e) 设备的审计和记录：对安全设备的操作进行审计和记录，包括设备的配置操作、检测和监控操作、故障处理操作等，确保设备的操作合规性和可追溯性；
f) 设备安全性管理：建立设备安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期、维修过程等方面作出规定；根据运行参数研判、预测设备故障运行隐患、安全设备的告警进行及时分析和研判；定期开展安全设备漏洞排查，经过充分测试评估后，对已有漏洞及时修补；
g) 安全有效性验证：需结合安全运维实际工作的情况，对相关安全措施的有效性进行验证，以确保安全运维工作收到应有的效果。

8.3.3 安全加固

安全加固主要是针对网络与应用系统的加固，在网络设备、安全设备、操作系统、硬件设备、应用程序等层次上建立符合安全需求的安全状态。根据专业安全评估结果，制定相应的系统加固方案，针对不同目标系统实施不同策略的安全加固，例如打补丁、修改安全配置、增加安全机制等方法，合理进行安全性加强，从而保障信息系统的安全。安全加固内容包括：

a) 安全现状调查：了解资产安全现状和资产关联关系，评估安全缺陷或安全隐患的影响范围和严重程度；
b) 制定加固方案：针对发现的安全现状问题，与相关业务部门、建设部门、管理部门、运维部门等联合确认安全加固方案，包括实施时间、范围、流程、方法等，确认每项加固措施和操作方法的可行性，同步制定回退方案和应急方案；
c) 落实加固举措：安全加固前做数据备份、版本备份，分阶段、分批次有序开展安全加固举措、测试验证。针对重要资产，需先加固资产，测试无误后再小批量、分批次开展安全加固；
d) 验证加固结果：通过测试、攻击等手段，针对安全加固后的结论进行验证，根据验证结果判断是否符合加固要求，最终按需落实加固方案。

8.3.4 人员培训

人员培训主要侧重于提高企业或组织全体员工的安全意识和安全素养，提高对安全问题的认识和理解，增强安全意识，对网络环境中的各种潜在威胁保持警觉，以便更好地应对各种安全威胁和风险。人员培训内容包括：

a) 组织理论培训：通过网络安全、信息安全、个人安全等方面的知识和技能培训和意识培训，提高员工的安全意识和安全素养，增强他们对安全问题的警觉性和防范能力；
b) 安全意识宣传：通过视频、海报、易拉宝、月刊、手册、电脑桌面等形式，对全体员工进行安全意识的宣传和教育，形成网络安全宣传教育常态化机制；

c) 开展实操演练：组织和实施安全演练，模拟真实的安全事件场景，如模拟邮件钓鱼、攻防实战演练等，帮助员工更加警觉地识别和防范各种网络安全威胁，更好地了解攻击者的手段和技术，从而提高识别和应对威胁的能力。

8.3.5 数据安全防护

数据安全防护是一种提供企业数据保护和安全防御的综合性服务。通过数据加密、访问控制、数据备份和恢复、安全审计、监控、防护有效性评估等多种安全技术和策略，保护企业的敏感数据免受未经授权的访问、泄露、篡改和破坏。数据安全防护内容包括：

a) 数据采集过程安全防护。在数据采集过程中数据采集的 API 接口需具有身份验证能力和数据来源校验能力，避免数据非法接入，同时需对数据输入输出进行验证和清洗；
b) 数据传输过程安全防护。在数据传输过程中需具有数据加密和访问控制能力。通过使用加密算法对敏感数据进行加密，并通过身份验证和访问权限管理来控制对数据的访问。加密技术可以保护数据在传输过程中的安全性，访问控制可以确保只有授权人员访问敏感数据；
c) 数据存储过程安全防护。在数据存储过程中需要具有敏感信息加密存储的能力，如个人身份信息、密钥信息等，需使用密码技术进行保护。对于加密密钥的存储和管理可使用硬件密码模块进行加密。同时，对数据库存储平台权限需采用最小权限原则进行配置，确保对数据的访问和操作权限具备合理范围的限制；
d) 数据处理过程安全防护。在数据处理过程中需具有敏感数据脱敏处理的能力，同时，需对数据的操作管理进行记录和监控，以防止数据的非法操作和篡改。此外，数据处理系统需根据存储数据的敏感程度进行不同等级的保护；
e) 数据交换过程安全防护。在数据交换过程中需具有交换数据加密传输和校验的能力，确保数据的安全性和完整性。同时，需对交换的数据进行安全检查和过滤，以防止有害数据的传入和传出。此外，需建立完善的数据交换协议和规范，确保数据交换的可靠性和合规性；
f) 数据销毁过程安全防护。在数据销毁过程中需建立完善的数据销毁规范和流程，并对销毁的存储介质进行抽样认定，确保数据被彻底删除并无法恢复；
g) 数据安全防护措施有效性验证。定期对网络数据、终端数据等数据防泄漏保护机制及有效性进行安全性评估和验证。

8.4 监测

8.4.1 概述

通过网络流量监测、异常行为监测、互联网资产暴露面监测、终端监测、数据监测、DNS监测、实时分析和深度分析等威胁监测领域的活动，实现网络安全运维的实时威胁监测。

8.4.2 网络流量监测

网络流量监测是通过对进出网络的流量进行采集和分析，识别出存在的安全威胁。网络流量监测内容包括：

a) 流量采集：通过部署网络监测设备，监测网络边界、网络出入口等关键节点的流量信息，发现网络攻击和存在的安全风险；
b) 流量分析：基于规则库和威胁信息对采集的流量数据进行分析；
c) 流量监测：基于多种技术进行网络威胁监测，包括特征匹配、网络行为分析、机器学习、关联分析、威胁信息等；

d) 流量存储：明确采集的流量范围和类别，对监测流量采取保护措施，防止其受到未授权的访问、修改和删除，原始流量需按照法规留存时间要求进行存放和归档。

8.4.3 异常行为监测

异常行为监测是通过使用多种机器学习算法挖掘各种用户异常行为模式，检测和识别前期没有发现的安全风险，基于实际安全场景的多维度异常检测功能，提升威胁发现速度和准确率。异常行为监测内容包括：

a) 已知威胁监测：依靠已知特征、已知行为模式形成的攻击特征库，结合云端威胁信息，通过预定义规则、信息匹配等方式进行威胁分析和安全处置。对全网设备日志、流数据、数据库表数据等进行采集，并对其进行数据归一化处理，针对常用协议解析的数据形成标准化日志，在标准化日志的基础之上，通过已知威胁检测，生成一次安全事件，并在一次安全事件的基础之上生成已知威胁数据；

b) 未知威胁监测：通过结合静态检测、动态检测和沙箱检测等方式，识别未知恶意代码和未知高级攻击行为，及时检测、分析并阻断物理网络中存在的安全威胁。

8.4.4 互联网资产暴露面监测

互联网资产暴露面监测是通过网络空间测绘、资产管理、脆弱性管理等技术手段对互联网出入口地址、信息系统（网站、APP、公众号、小程序等）、网络类设备、终端等进行监测，发现存在的可用性问题及安全威胁，根据监测结果采取相关举措抑制或控制事态影响。互联网资产暴露面监测内容包括：

a) 资产监测：结合网络主动扫描、流量被动还原、终端指纹采集、数据导入等方式，对合规资产、未纳管资产、隐匿资产等资产信息进行发现和持续监测，实现信息系统资产管理的全面覆盖，并将采集到数据汇聚成一份完整的资产清单；

b) 漏洞监测：通过漏洞扫描工具等技术手段对信息系统及其支撑软硬件系统存在的漏洞进行发现和监测，对漏洞影响范围进行统计分析；

c) 暴露面管理：关闭非必要互联网协议地址、端口、应用服务等，收敛互联网出口数量，减少对外暴露组织架构、邮箱账号、组织通信录等内部信息，避免在代码托管平台、文库、网盘等公共存储空间存储网络拓扑图、源代码、互联网协议地址规划等可能被攻击者利用的技术文档。

8.4.5 终端监测

终端监测是通过对终端行为进行持续监测，实时收集并提取终端的威胁信息和行为数据，结合多种异常行为分析建模工具，发现存在风险的设备并进行及时响应，防范来自终端的安全威胁。终端监测内容包括：

a) 终端数据采集：通过技术手段采集终端数据，主要包含服务、进程、端口、注册表、计划任务等；

b) 终端威胁监测：通过终端威胁检测技术对终端进行监测，包含恶意代码检测、暴力破解检测、流量攻击检测、异常行为检测等；

c) 终端监测技术：基于多种技术进行终端威胁检测，包括 IOA 行为检测、IOC 特征匹配、机器学习、关联分析、威胁图谱等。

8.4.6 数据监测

数据监测是通过数据库审计、数据防泄漏等技术手段对数据采集、存储、传输、使用等过程进行监控，及时发现并阻断对数据进行的窃取、篡改和销毁等恶意行为。数据监测内容包括：

a) 数据库监测：通过对数据库运行状态和操作行为进行监测，及时发现数据库的异常状态和异常操作行为等并定位问题；
b) 管理策略监测：对数据管理策略落实情况进行监测，确保数据的保密性、完整性符合管理要求，保障数据传输、存储和使用的安全；
c) 敏感数据监测：对敏感数据流转情况进行监测，及时发现和处置数据泄露威胁；
d) 监测信息保存：对监测信息采取保护措施，防止其受到未授权的访问、修改和删除，监测信息的保存需按照法规留存时间要求进行存放和归档。

8.4.7 DNS 监测

DNS监测是通过监控企业关键域名服务，发现DDOS攻击、域名恶意解析等异常情况，防止隐蔽的网络攻击威胁。域名系统监测服务内容包括：

a) 域名监测：监测域名 A 记录、CNAME 等解析设置，发现解析异常；
b) DNS 解析与监测：通过提供 DNS 解析服务或分光的方式，获取网络内 DNS 流量，通过重组和还原后在此基础上进行 DNS 请求/响应的分析和检测。

8.4.8 实时分析

实时分析是通过统一采集终端业务数据与边界网络安全设备的海量日志，经实时流式大数据处理引擎对数据进行实时的归一化适配处理，处理后的数据通过关联规则引擎、异常流量行为引擎、AI算法引擎等手段，运用机器学习、统计分析、构建基线等方法，从而发现网络中潜藏的网络攻击。实时分析服务内容包括：

a) 实时资产监测：通过采集系统、应用日志和系统网络流量的状态或可疑活动，对资产健康情况进行实时监测；
b) 实时关联分析：对多源安全日志进行实时关联分析，包括关联匹配、统计分析、时序分析、场景化模型、AI 引擎等；
c) 事件数据保留：通过收集和集中存储在安全监测和分析过程中所有的事件，按照法规留存时间要求进行存放和归档；
d) 警报和警告：通过安全设备告警日志、安全公告和漏洞信息、可扩散的威胁告警匹配所关注的信息资产，分析其所面临的潜在风险，第一时间发布事件预警通报；
e) 数据分析和查询：对处置报告中有关分析数据和报告所需查询数据做出实时响应支持。

8.4.9 深度分析

深度分析是通过使用数字取证和恶意软件分析等技术手段，调查受影响的系统、审查受损的数据，并分析攻击中使用的工具和方法。深度分析服务内容包括：

a) 取证分析：通过对收集自安全资产的数字证据进行分析，并将其与事件关联，以确定事件发生原因和过程；
b) 恶意软件样本分析：对每个取证过程中发现的攻击者部署的恶意软件、程序或脚本进行分析。
c) 跟踪和追踪：通过对内部和外部攻击者的属性进行跟踪和追踪，提升其攻击溯源能力，形成攻击者画像，根据其跟踪和追踪结果，结合安全防护技术手段以减少安全事件发生概率；
d) 证据收集：收集和保存与所评估安全事件相关的数字电子证据，保管证据链，确定和维持证据的有效性。

8.5 响应

8.5.1 概述

通过应急响应、应急预案建立、处置与恢复、应急总结等涵盖事件和应急响应领域的活动，实现识别发现并报告威胁级别、详细信息综合分析研判、阻断封堵、固定证据、业务恢复、溯源分析、还原攻击、事件报送以及配合执法部门追踪溯源等环节。

8.5.2 应急响应

应急响应内容包括：

a) 事前准备：包括制定应急预案，定期演练等。应急预案应基于组织的需求和特定情况，包括对可能发生的紧急情况进行风险评估和针对性的预防措施。定期演练是为了确保员工和相关部门了解应急程序，并能熟练应对各种紧急情况。
b) 事件识别和报告：建立有效的事件识别机制，以及与员工和相关利益相关者进行有效沟通的渠道，对紧急事件及时发现和报告。
c) 应急响应启动：在实施应急响应工作前，现场应急处置人员和相关技术人员第一时间取得联系，了解事件发生情况。技术人员判断事件类型，是否需要启用应急响应。现场威胁分析发现沦陷事件，由现场应急人员初步判断攻陷事件类型，确定事件发生情况，根据 GB/T 20986-2023 与相关人员确定是否启动应急响应。
d) 事件分析和系统恢复：在网络安全事件发生后，需要进行事件分析，确定存在的安全漏洞并采取必要的措施来修复漏洞，以防止类似事件的再次发生。在分析完成后，需要将被破坏的系统进行恢复，确保系统的完整性和可用性。
e) 溯源取证：遵循严格的法律程序和技术规范，以确保取证数据的真实性和完整性，为后续的应急响应和安全分析提供有力的支持。

8.5.3 应急预案建立

应急预案建立是建立健全网络安全事件应急工作机制必要手段，通过应急预案编制以提高应对网络安全事件能力，预防和减少网络安全事件造成的损失和危害，保护公众利益，维护国家安全、公共安全和社会秩序。应急预案建立内容包括：

a) 综合应急预案：应急预案是从总体上阐述事故的应急方针、政策，应急组织结构及相关应急职责，应急行动、措施和保障等基本要求和程序，是应对各类信息安全事件的综合性文件；
b) 专项应急预案：针对具体的事故类别、级别、应急保障而制定的计划或方案，是综合应急预案的组成部分，需按照应急预案的程序和要求组织制定，并作为综合应急预案的附件，明确程序和具体的应急措施；
c) 现场处置方案：现场处置方案是针对具体的场所、设施、岗位所制定的应急处置措施。现场处置方案需具体、简单、针对性强。现场处置方案需根据风险评估及脆弱性控制措施逐一编制，做到相关人员应知应会、熟练掌握，并通过应急演练，做到迅速反应、正确处置。

8.5.4 处置与恢复

处置与恢复内容包括：

a) 应急响应处置：在判断事件类型可能为安全事件，启用应急响应后，根据 GB/T 20986-2023 标准，技术人员通过现场或非现场等方式进行信息收集工作，详细了解掌握事件发生的始终、现状、可能的影响，对事件进行详细分析，提供事件处置建议，并协助相关人员解决事件。
b) 恢复：根据 GB/T 28827.3-2012 标准，基于应急响应预案、配置管理数据库、知识库等进行故障处理和系统恢复，在满足实践级别处置实践要求的前提下尽快恢复服务，采用方法、手段防止次生、衍生实践的发生。

c) 复盘总结：待事件处理结束后，应急人员整理事件分析、事件处理的过程记录和相关资料，撰写应急响应记录报告并提交。对于大型、复杂的应急响应过程还需进行整体的事件处理汇报工作，同时，依据现场情况，召集必要相关人员发起会议，对本次应急响应事件的发生进行复盘，提升优化应急效率，并根据复盘结果，完善运维方案，在安全管理制度、流程上做同步完善。

d) 事件归档：应急响应结束，输出应急响应报告、后门样本文件，同步交付作为事件归档。

8.5.5 应急总结

应急总结内容包括：

a) 应急工作总结：组织应定期对应急响应工作进行分析和回顾，总结经验教训，并采取适当的后续措施。对应急响应工作的分析和回顾应形成总结报告，并将总结报告作为改进应急响应工作及信息系统的重要依据。

b) 应急工作评审：为保证应急响应的有效性和时效性，应急响应责任者应定期组织对应急响应工作的评审，以确保应急响应过程和管理符合预定的标准和要求。评审的结果应该正式存档并通知给相关利益方。评审需至少每年举行一次。

c) 应急工作改进：应急事件总结、应急工作评审的结果应该作为应急准备阶段各项工作的改进要素。组织需根据总结报告中给出的建议项和评审结果，完善安全运维应急准备工作。

8.6 协同

8.6.1 概述

在网络安全运维体系化建设的长期过程中，要开展运维能力提升培训、供应链安全管理、信息协同共享等与多方机构协同完成的基础性和提升性工作。

8.6.2 网络安全运维能力提升

能力提升内容包括：

a) 理论知识培训：对专业技术人员提供专项提升培训和考核，掌握前沿技术、产品应用等内容，提升相关人员技术知识水平；

b) 专业技能演练：通过渗透测试、攻防演练、技能比赛等有限定地网络攻击演练，加深运维人员对网络攻击实操的认知，熟悉系统风险和应对措施，提升技术人员网络攻击防范能力。

8.6.3 供应链安全

供应链安全是对供应链实施有效的管理，建立供应链安全控制策略及机制，在网络安全运维过程中实施全过程安全管理，避免由于供应链环节的安全隐患，导致恶意代码、植入、挟持、信息泄露、钓鱼攻击和远程控制等安全问题。供应链安全内容包括：

a) 准入管理：组织需建立供应商等级评价标准及准入、准出机制，通过充分的审核和评估，确保供应商安全能力持续符合要求；

b) 安全协议：确定供应商及内部组织在供应链安全管理中的责任，明确与供应商发生业务关系时的安全性要求，并定期评估协议的符合性；

c) 安全监控：组织需明确供应链安全的要求，并对运维过程实施监控；建立监控机制以及时发现并上报存在的风险和问题；

d) 安全响应：需建立供应商安全响应机制，以确保在发生安全事态或事件时，供应商能够积极配合响应，至正式关闭。若必要，供应商应进行事后分析，确定起因；

e) 绩效管理：组织需按计划的时间间隔监视供应商的安全绩效。如果未达成绩效目标或未履行协议义务的，需确保及时识别改进机会，并制定相应措施。

f) 风险管理：结合组织业务特点，识别和梳理供应链面临的风险，分析风险发生概率，评估影响范围和程度，制定相应措施或预案以控制风险，并针对供应链关键环节，实施风险评估审查。

8.6.4 信息协同共享

信息协调共享内容包括：

a) 信息收集：组织需持续关注、抓取、汇总、甄别、整理获取到的安全相关信息，并结合研究成果，形成安全通报或专题报告等信息文档；

b) 信息共享：组织需建立信息共享渠道，明确信息共享流程，定期组织沟通、交流，保障组织间的信息同步；

c) 协同响应：组织需明确共同目标，建立协同机制，实现跨组织合作，以更好地利用外部资源提升效率。

9 网络安全运维效果评估模型

9.1 评估模型

本文件参考GB/T 20261-2020和GB/T 37988-2019的定级方法。对网络安全运维的效果进行等级评估。

网络安全运维效果评估模型由以下三方面内容构成，如图3所示：

a) 网络安全运维实施内容：主要针对与网络运维实施活动直接相关的识别、防御、监测和响应四个环节，运维管理和协同两个环节的内容包含在网络安全运维关键要素之中；

b) 网络安全运维关键要素：明确组织机构在整个安全领域中所具备的关键要素，明确为安全运维团队、安全运维工具或平台以及安全运维管理的各类流程；

c) 网络安全运维效果等级：基于统一的评估模型，定义组织在网络安全运维域的五个效果级别。

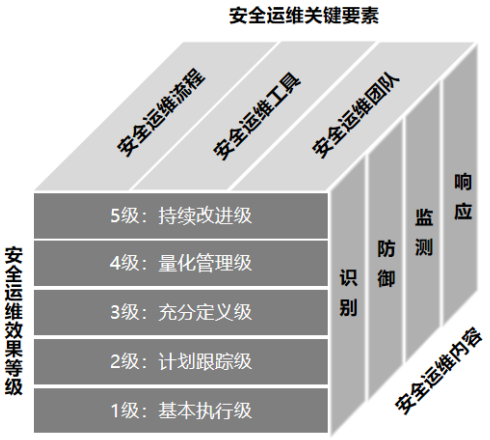

图3 网络安全运维效果评估模型

安全运维效果级别分为五个等级，一级是基本执行级，二级是计划跟踪级，三级是充分定义级，四级是量化控制级，五级是持续改进级。运维效果等级从一级至五级逐级提升。对运维效果等级的描述如表6所示：

表3　网络安全运维效果等级

运维效果级别	定义内容	执行表现	特征
等级一：基本执行级	● 未形成成熟的机制保证安全运维工作的有序开展 ● 安全运维工作处于被动执行阶段	执行力较差，资源、能力严重不足。	以边界防护为核心。
等级二：计划跟踪级	● 工作有计划并可执行，对安全运维过程进行了规划，提前分配资源和责任。 ● 按照预定的方式执行并能通过结果进行踪和纠偏	实现了安全过程的计划与执行，不成体系。	以技术产品部署为核心的基础防范。
等级三：充分定义级	● 有标准化的制度和流程，有清晰的标准化文档支撑安全运维各项目 ● 形成业务系统内、各业务系统之间、组织机构外部活动的协调机制	执行效果较好，但有较大改进空间	以合规体系建设为核心的体系化控制
等级四：量化控制级	● 有清晰可测的网络安全运维指标，安全运维内容可量化 ● 通过量化测量来管理安全运维的全过程，并可以修正安全运维相关行动	执行效果非常好，改进空间较小	以攻防对抗为核心的主动防御
等级五：持续改进级	● 形成了内生的安全循环机制并不断演化 ● 防护能力和人员能力不断提升	执行效果非常好，人员的信息安全意识很高，形成信息安全文化	

9.2　评估内容

9.2.1　网络安全运维的实施内容评估

网络安全运维的实施内容评估包括：

a)　识别：对资产发现与管理、脆弱性评估与管理、威胁信息收集评估与预警和安全合规等内容进行评估；

b)　防御：对安全设备运维、安全加固和人员培训进行评估；

c)　监测：对实时分析、深度分析、异常行业监测和网站安全监测时行评估；

d)　响应：对应急预案编制、应急响应与处置、安全应急演练和内部异常行为的响应进行评估。

9.2.2　安全运维关键要素评估

网络安全运维关键要素相关的评估内容包括：

a)　安全运维团队。从承担安全运维工作的组织机构建设具备的能力出发，从以下方面进行能力的效果评估：

1)　安全运维组织架构对组织业务的适用性；

2)　安全运维组织机构承担的工作职责的明确性、人员能力的匹配性；

3)　安全运维组织机构运作、沟通协调的有效性。

b)　安全运维流程。约定和规范日常安全运维工作中各操作环节、操作步骤、操作工具、操作方法，以维持工作进程的一致性和统一性，实现精细化、标准化的安全运维管理，提工作效率，从以下方面进行能力的效果度量：

1)　安全运维活动中关键控制节点授权审批流程的完整性；

2)　相关流程制度的制定、发布、修订的规范性和专业性；

3) 安全要求及流程落地执行的一致性和有效性和体系化。

c) 安全运维工具。从安全运维组织用于开展工作的安全技术、应用系统和自动化工具出发，从以下方面进行能力的效果度量：

1) 从网络侧、主机侧、应用侧、策略侧、终端侧和用户侧等多个维度获取多源数据的能力；
2) 对比历史数据，形成趋势性、合理性判断，实现全方位、多层次、多角度、细粒度感知，为安全运维提供重要分析能力；
3) 将团队、流程、工具有机结合以实现自动化、数据化、智能化的业务流转、业务监控和业务考核，快速提升和持续改进安全能力。

9.2.3 网络安全运维建设与执行过程评估

网络安全运维建设与执行过程相关评估内容包括：

a) 建设情况：评估各项安全运维流程、工具、团队是否建立，是否匹配组织安全需求，如是否建立异常行为监测系统和流程；
b) 运行能力：评估各项安全运维工作是否按预期开展，执行效率如何，如安全事件 MTTD、MTTR；
c) 安全态势：持续观测客观安全态势，评估安全运维工作实际的保障结果，如重大安全事件发生数量。

9.3 评估过程

网络安全运维需求方与提供方需定期对安全运维效果预期目标进行审查，每年可组织一次安全运维效果评估，以保证网络安全运维工作有效性。

评估过程可遵循以下内容：

a) 科学性：按照网络安全运维效果评估模型，选择科学的评估方法（详见 B.3 进行评估。
b) 公正性：网络安全运维效果评估评估过程需符合法规和组织原则，保证评估结果是客观公正准确的。
c) 安全性：向网络安全运维需求方告知评估时间、评估工具、评估技术方式以及可能对信息系统造成的影响等，确保评估活动自身安全性。
d) 保密性：有外部人员参与评估的情况下，相关人员签署保密协议，若需提供实际数据进行评估参考，需脱敏处理，并对评估过程数据和结果数据进行严格管理。
e) 计划性：开展评估前需制定评估计划，明确评估目标、范围、时间、方法和预期结果，由运维需求方和运维提供方达成共识。
f) 透明性：网络安全运维提供方按评估目标提供必要的过程数据（包括但不限于安全漏洞评估报告、安全防护有效性验证报告、安全监测操作记录等），确保评估结果的准确透明。

9.4 评估方法

9.4.1 方法选择

安全运维效果评估可根据评估场景选择具体的评估方法，包括顾问访谈、问卷调研、文件审核、勘查调研、漏洞扫描、渗透测试、红蓝对抗、技术验证等。

a) 顾问访谈：顾问访谈是通过与安全专家或顾问进行面对面或远程对话，以了解系统安全性和潜在风险的方法。适用于包括提问有关安全人员组织、管理策略与制度、系统配置和实施相关的评估指标。
b) 问卷调研：问卷调研是一种通过向相关人员发送一系列安全问题或调查表，以便收集他们的观点和反馈的方法。适用于人员安全意识和安全实践情况相关的评估指标。

c) 文件审核：文件审核涉及检查系统、应用程序或网络的相关文件和文档，如安全策略、配置文件和日志记录，有助于发现潜在的安全问题和不符合安全标准的情况。适用于安全人员组织、管理策略与制度、系统配置和实施相关的评估指标。
d) 勘查调研：通过实地勘查或远程调查，了解物理设备、网络拓扑和环境因素对安全性的影响。适用于物理安全相关的评估指标。
e) 漏洞扫描：使用自动化工具来识别系统或应用程序中的已知漏洞和弱点。适用于技术性相关的评估指标。
f) 渗透测试：渗透测试人员模拟攻击者的行为尝试入侵系统，发现潜在漏洞但不会造成破坏，并提供详细的报告和建议，以加强安全。适用于技术性相关的评估指标。
g) 红蓝对抗：红蓝对抗是一种模拟攻击和防御的综合性安全测试方法。红蓝两队在模拟环境中对抗，以评估系统的安全性和响应能力。适用于技术性相关的评估指标。
h) 技术验证：通过技术手段模拟真实的各类攻击，对组织已部署的各类安全产品和规则策略开展效果验证。通常与常规评估方法进行结合，验证安全运维工作的实际效果。适用于技术性相关的评估指标。

9.4.2 效果评分

安全运维效果评分用于量化评价、考核安全运维工作的实际效果。组织可按照安全运维需求和目标，选取安全建设指标、运行能力指标和安全态势指标，确定各指标类别权重，形成评估基线。各指标项根据达成情况评分，并按照权重转化为百分制，实现安全运维效果的量化考核。

表4 安全运维效果评分示例

指标类别	权重（相加等于 100）	达成情况	得分
安全管理指标	10	8/14	5.7
安全建设指标	20	10/12	16.7
安全运维执行指标	20	15/21	14.3
网络安全态势和效果指标	50	18/27	33.3
总分			70

9.4.3 效果评级

安全运维效果评级是在B.3.2的基础上，用于定性评价组织整体网络安全运维效果，指导组织长期的安全运维规划与建设。

组织可按照安全运维效果评估模型，针对特定运维项评估各项指标的满足情况。仅符合某一级别全部指标的情况下，认定组织机构达到该级别能力要求，由低到高以此类推可测得最终能力级别。实际评估中，需根据组织安全运维情况剔除不涉及的指标条款。

表5 安全运维效果级别评估示例

评估内容	1级符合度	2级符合度	3级符合度	4级符合度	5级符合度	安全运维等级
识别	17/17	30/30	50/50	6/25	0/13	3级
防御	3/3	7/7	11/11	1/6	0/4	3级
监测	5/5	9/9	21/31	2/18	0/9	2级
响应	8/8	12/12	17/21	1/10	0/5	2级

表6　机构整体安全运维效果级别评估示例

评估内容	1级符合度	2级符合度	3级符合度	4级符合度	5级符合度	总体等级评价
整体评估结果	33/33	58/58	99/113	10/59	0/31	2级

9.5　持续改进

安全运维效果评估后需持续跟踪改进。安全运维需求方和提供方应共同分析评估结果，制定改进计划并持续跟踪，针对评估中发现的问题和风险进行解决，改进计划需具体明确，满足以下要求。

a)　明确具体部门、人员参与网络安全运维的整改建议计划、所需资源，及其形成的任务（项目）。

b)　确定实施改进任务项目计划的时间安排和任务分配，包括评估后一周内、一月内、一个季度内的具体安排节点和重要里程碑。

c)　确定对网络安全运维的能力提升效果和整改任务的实施情况进行监控的措施。

d)　需注意及时发现在整改过程中产生新的风险或已知风险随着环境和时间发生的变化，以及持续进行评估和改进的计划。

e)　按照预定的时间和任务安排跟进整改进度，完成整改任务的验收总结和复审。

附 录 A
（资料性）
网络安全运维中心建设

A.1 建设思路

网络安全运维中心是组织为抵御网络安全威胁，保障IT基础设施安全稳定运行，有机结合人员、流程和技术，提供网络安全运维的组织单元。已经具备自主网络安全威胁管理和漏洞管理能力的组织和机构，宜考虑建立网络安全运维中心。网络安全运维中心的建设在满足国家相关法律法规，以及行业监管要求的前提下，宜考虑以下方面：

a) 广泛参与。组织和机构的相关信息技术和业务部门宜广泛参与；
b) 最小业务影响。组织和机构的网络安全运维中心建设和实施在达成组织安全目标的前提下，将对业务可能造成的影响降低到最小；
c) 持续改进。组织和机构不断提升网络安全运维中心的安全能力和运维水平；
d) 自身安全。组织和机构网络安全运维中心的建设保障自身安全性和业务连续性，建立相适应的网络安全管理、数据安全管理机制，并将供应链安全、外包安全等因素纳入到自身安全建设的考虑范围之中。

A.2 建设模式

A.2.1 概述

网络安全运维中心建设模式包括全自建、联合和全托管三种模式，组织采用哪种模式，由安全性要求、运维资源投入和安全运维能力决定。当组织对安全性和数据保护的要求非常高，有足够的安全资源投入，且自身安全运维能力强时，可选择全自建模式；当组织对安全性和数据保护的要求较高，有较充足的安全资源投入，自身安全运维能力较强时，可选择联合模式；当组织对安全性和数据保护的要求不高，有一定的安全资源投入，自身安全运维能力不强时，宜选择全托管模式。三种模式的网络安全运维中心在安全运维人员与岗位条件、安全运维管理流程上存在不同。一般情况下，三种模式的网络安全运维中心均需设置两类工作岗位，分别是管理类和技术类，其中技术类又分为分析研判和实施操作两种。

A.2.2 全自建网络安全运维

A.2.2.1 岗位条件

A.2.2.1.1 管理类

全自建模式下的管理类主要包括安全运维中心负责人、安全运维主管、安全监测主管和风险与合规管理四个岗位。

a) SOC 负责人。主要工作包括负责组织制定安全运维目标和工作计划、安全运维能力规划和建设、安全运维制度和流程，跟踪监督执行效果，重大运维事项的决策等；
b) 安全运维主管。向安全运维中心负责人汇报，主要工作包括负责落实安全运维目标、执行工作计划、优化改进安全运维制度和流程和落实重大运维事项决策等；
c) 安全监测主管。向安全运维负责人汇报，主要工作包括负责管理网络安全事件，突发事件的应急响应、调查分析和追踪溯源，安全事件的联动处置和网络安全态势报告的编制等；

d) 风险与合规管理岗。向安全运维中心负责人汇报，主要工作包括负责网络安全风险全过程管理与网络安全合规管理等。

A.2.2.1.2 技术类

全自建模式下的技术类包括分析研判和实施操作，其中分析研判类主要包括分析研判岗、漏洞分析岗、威胁信息管理岗、防护策略管理岗四个岗位。

a) 分析研判岗。向安全监测主管汇报，主要工作包括负责分析安全威胁告警报告、分析是否启动应急流程、网络安全威胁事件深入分析与溯源，分析和报告网络安全防御措施缺陷等；
b) 漏洞分析岗。向安全监测主管汇报，主要工作包括负责安全漏洞跟踪分析评估、预警信息发布、漏洞修复方案和加固措施制定、漏洞处置过程监控、漏洞修复情况验证分析等；
c) 威胁信息分析岗。向安全监测主管汇报，主要工作包括负责威胁信息的采集分析评估、获取数据的归类分析整合等；
d) 防护策略分析岗。向安全监测主管汇报，主要工作包括负责安全防护策略的管理、优化、制定、执行和有效性分析等。

实施操作主要包括安全监控岗、资产管理岗、平台维护岗、主机安全维护岗、终端安全维护岗、集权设备维护岗六个岗位。

a) 安全监控岗。向安全监测主管汇报，主要工作包括负责相关设备的日志分析、策略调整、规则优化、威胁事件监测上报，执行和落实网络安全态势监测分析方案，处置突发事件，跟踪安全事件整改情况；
b) 资产维护岗。向安全监测主管汇报，主要工作包括负责组织信息资产的发现、资产清单的管理、资产档案的维护、问题资产的发现和处置等；
c) 平台维护岗。向安全运维主管汇报，主要工作包括负责安全设备与平台的定期升级更新、状态巡检、故障排除、设备与平台预置及自定义规则、策略、预案、脚本、知识的建设、维护及发布等；
d) 主机安全维护岗。向安全运维主管汇报，主要工作包括负责主机服务器的定期升级更新、状态巡检、故障排除、主机服务器预置及自定义规则、策略、预案、脚本、知识的建设、维护及发布等；
e) 终端安全维护岗。向安全运维主管汇报，主要工作包括负责终端设备的定期升级更新、状态巡检、故障排除、终端设备预置及自定义规则、策略、预案、脚本、知识的建设、维护及发布等；
f) 集权设备维护岗。向安全运维主管汇报，主要工作包括负责集权设备的定期升级更新、状态巡检、故障排除、集权设备预置及自定义规则、策略、预案、脚本、知识的建设、维护及发布等。

A.2.2.2 管理流程

全自建网络安全运维管理流程主要是熟悉组织文化与业务、理解安全需求透彻，创建的流程贴合组织实际；劣势是对最佳实践和新技术理念了解滞后，对流程的优化和变革缺乏驱动力。全自建网络安全运维中心在网络安全运维流程管理包括：

a) 识别流程。通过确定对象、收集数据、选择方法、分析规律、判断检查、建立模型和验证评估等环节完成。全自建网络安全运维中心可参照 GB/T 20984 标准，创建和管理业务识别流程、资产发现与管理流程、风险管理流程。业务识别流程包括业务发展战略和业务关联关系内容；资产发现与管理流程包括依据资产业务承载性

确定资产重要性的内容，同时要结合最新的资产识别和管理平台设计流程；风险管理流程包括必要时引入外部机构进行风险评估的子流程。威胁信息收集/评估/预警流程和安全合规管理流程考虑引入外部机构的条件和时机；

b) 防御流程。通过识别网络安全缺失和漏洞、评估危害和级别、分析防御措施、制定工作任务和实施步骤、考核和修正等环节完成，一般包括安全设备和应用运维流程、安全加固流程、人员培训流程、数据安全防护流程等涵盖纵深防御领域的流程。全自建网络安全运维中心在创建防御流程时需充分了解最佳实践，评估技术发展趋势，持续优化改进防御流程；

c) 监测流程。通过数据采集和存储、分析与合成、告警和查询、检测和发现等环节完成，一般包括网络流量监测、异常行为监测、互联网资产暴露面监测、终端监测、数据监测、域名系统监测、实时分析、深度分析等涵盖威胁监测领域的流程。全自建网络安全运维中心需注重外部网络安全热点事件，结合威胁信息，及时调整监测重点，必要时调整防御策略；

d) 响应流程。在日常工作中需遵循准备、诊断、抑制、根除、恢复和跟踪等应急响应流程，处置突发事件的过程中通过识别发现并报告威胁级别、详细信息综合分析研判、阻断封堵、固定证据、业务恢复、溯源分析、还原攻击、事件报送以及配合相关部门追踪溯源等环节完成，该领域一般包括应急预案编制、应急响应与处置、安全应急演练和内部异常行为响应等涵盖应急响应领域的流程。全自建网络安全运维中心在应急响应流程中更需充分考虑在保证安全的前提下，引入外部专家力量的条件、时机及相关的协同与保障机制；

e) 网络安全运维沟通机制建立。全自建网络安全运维中心需建立内部沟通机制和外部沟通机制。内部沟通机制需包括与上级部门或管理层的汇报机制、与业务部门的通报与协同机制、与行政管理部门的保障与支撑机制等。外部沟通机制需包括与国家主管机关和上级单位的信息上报机制、与下属单位的通报预警机制、与其他单位的信息共享机制、与专业机构的协同机制等。

A.2.3 联合网络安全运维

A.2.3.1 岗位条件

A.2.3.1.1 管理类

联合模式下的管理类主要包括SOC负责人、安全运维主管、安全技术主管、风险与合规管理岗四个岗位。

a) SOC 负责人。安全运维中心负责人主要工作包括负责组织制定总体安全目标和工作计划、安全能力规划和建设、安全制度和流程的制定与落实、跟踪监督执行效果，重大事项的决策等；

b) 安全运维主管。向安全运维中心负责人汇报，主要工作包括负责安全运维领域总体安全目标的分解和对应各分计划的制定、安全运维人员组织和能力的规则与建设、安全运维领域的安全制度和工作流程制定与落实等；

c) 安全技术主管。向安全运维中心负责人汇报，主要工作包括负责安全运维中心技术平台与工具整体架构体系设计及其建设规划、技术平台与工具选型上架、组织内技术标准制定、技术平台与工具定制开发与维护等；

d) 风险与合规管理主管。向安全运维中心负责人汇报，主要工作包括负责组织风险合规管理体系的构建和推进、风险控制机制的建立和实施、合规制度和流程的维护等。

A.2.3.1.2 技术类

联合模式下的技术类分为分析研判和实施操作，其中分析研判岗位一般由合作方担任，依据安全运维需求，以驻场或远程方式提供安全运维服务，主要包括项目经理岗、安全运维咨询岗、分析研判岗、应急响应分析岗、攻防对抗分析岗、平台设备安全分析岗六个岗位。

a) 项目经理岗。向安全运维中心负责人汇报，主要工作包括负责项目资源协调和赋能申请、负责项目情况及问题跟进、项目交付周期管理、项目定期汇报及项目验收工作；
b) 安全运维咨询岗。向安全运维中心负责人汇报，主要工作包括负责网络安全运维中心流程制度设计、技术体系设计、人员组织架构设计及落地跟进，并参与指导改进优化；负责根进行整体运维成熟度度量，依照度量结果动态改良整体运维体系等；
c) 分析研判岗。向项目经理岗汇报。负责向驻场运维人员提供安全威胁告警分析研判专家能力支持；
d) 应急响应分析岗。向项目经理岗汇报。负责向驻场运维人员提供信息安全事件应急响应专家能力支持；
e) 攻防对抗分析岗。向项目经理岗汇报。负责向驻场运维人员提供红蓝对抗演练、渗透测试、代码审计等攻防专家能力支持；
f) 平台设备安全分析岗。向项目经理岗汇报。负责向驻场运维人员提供平台与设备运维问题解决能力支持；同时提供平台与设备定制开发能力支持。

联合模式下的实施操作类相关岗位人员一般由合作方提供，并以驻场运维的形式，为主建单位提供安全运维服务，主要包括安全监测岗、安全响应岗、识别评估岗、设备平台维护岗四个岗位。

a) 安全监测岗。向安全运维主管汇报，工作内容包括负责安全设备日志分析、策略调整、规则优化、威胁事件日常监测上报等；
b) 安全响应岗。向安全运维主管汇报，工作内容包括负责威胁信息事件响应、安全事件处置、应急响应等事件闭环等；
c) 识别评估岗。向安全运维主管汇报，工作内容包括负责资产梳理发现、资产稽查及对资产进行渗透测试、弱口令扫描、配置基线扫描、安全意识演练技术支持、漏洞与安全事件信息的定级判断、接收、下发与跟进闭环等；
d) 设备平台维护岗。向安全技术主管汇报，工作内容包括负责安全设备、平台的定期升级更新、状态巡检、故障排除、设备与平台预置及自定义规则、策略、预案、脚本、知识的建设、维护及发布等。

A.2.3.2 管理流程

在联合网络安全运维中心模式中，为确保安全运维管理流程可切实落地，需明确安全运维各项工作中主建单位和合作单位的分工界面，整体分工界面可为主建方负责决策管理、跨部门沟通、资源及信息协调相关工作；合作方负责专业技术能力交付、安全运维专家咨询、云端技术能力支持等工作。在安全运维各工管理流程中，主建单位和合作单位分工界面如下：

a) 识别流程。包含业务识别、资产识别、风险识别、信息收集、安全合规等识别领域的流程。工作流程一般由信息收集、信息确认、确认反馈、信息梳理、信息消费等环节组成。其中信息确认及确认反馈环节需由主建单位主责，信息收集、信息梳理及信息消费需由合作单位主责；
b) 防御流程。包含安全设备运维、安全加固、人员培训、安全数据防护等防御领域的流程。工作流程一般由安全运维需求提出、安全服务/工具清单提供、安全服务/工具确定、安全服务/工具实施、服务/工具实施成果验收等环节组成。其中安全运维

需求提出、安全服务/工具确定及服务/工具实施成果验收环节需由主建单位主责，安全服务/工具清单提供、安全服务/工具实施环节需由合作单位主责；

c) 监测流程。包含网络流量监测、异常行为监测、互联网资产暴露面监测、终端监测、数据监测、域名系统监测、实时分析、深度分析等监测领域的流程。工作流程一般由监测范围覆盖、监测实施、分析实施、结果上报等环节组成。其中监测范围覆盖需由主建单位主责，监测实施、分析实施、结果上报等环节由合作单位主责；

d) 响应流程。包含应急响应、应急预案建立、应急处置、应急总结等应急领域的流程。工作流程一般由准备阶段、检测阶段、抑制阶段、根除阶段、恢复阶段、总结阶段等环节组成，其中抑制阶段、恢复阶段、总结阶段需由主建单位主责，准备阶段、检测阶段、根除阶段需由合作单位主责；

e) 建立安全运维协同机制。在联合网络安全运维中心模式中，为确保信息传递畅通，工作协同高效，建立安全运维协同机制。

1) 接口人机制。由信息安全管理领导和合作单位指定主建单位和合作单位接口人，合作单位接口人一般由项目经理担任。确保项目信息准确有效同步，并能统一归口；

2) 云地协同机制。由合作单位提供覆盖安全运维工作能力需求的云端专家能力团队，并针对云端威胁信息预警、云端 SaaS 化能力、地端协调指挥能力等云地协同工作提供便捷可靠的协同工具。

A.2.4 全托管网络安全运维

A.2.4.1 岗位条件

A.2.4.1.1 管理类

全托管模式下的运维管理类主要包括SOC负责人、安全运维主管、项目经理、质量管理专家、风险与合规管理岗五个岗位。

a) SOC 负责人：负责安全运维中心的领导工作以及重大事项的决策，能组织制定安全运维的发展目标和规划、指导制定安全运维的制度和流程，并跟踪监督执行效果；

b) 安全运维主管：负责安全托管项目实施的监察、协调等管理工作，能帮助用户识别和确定网络安全需求、与甲方用户就共同安全目标进行沟通与协调，能组织建立和运行应急体系，能协调内、外部相关方进行高等级网络安全威胁事件联动处置工作；

c) 项目经理：负责项目实施的各项管理、协调工作以及项目进度与问题沟通，能够向甲方用户定期进行项目成果汇报，组织项目启动会与项目验收，能对项目过程进行复盘和管理，能够及时发现项目风险，保障运维效果；

d) 质量管理专家：负责安全托管整体质量管理、用户满意度管理，能制定质量标准及客户满意度标准，能及时进行质量审查及审查结果汇报，能对运维过程进行质量改进管理；

e) 风险与合规管理岗：负责项目风险管理，对项目方案的风险进行识别和评估，能够依据相关法律法规、标准要求，结合实际业务需求和项目情况，提供合规咨询，进行风险分析并提供解决方案，进行合规监管、项目风险管控及评估。

A.2.4.1.2 技术类

全托管模式下的技术类分为分析研判和实施操作，其中分析研判包括整体分析研判岗、漏洞分析岗、威胁信息管理岗、防护策略管理岗等四个岗位。

a) 整体分析研判岗：负责对各类安全事件进行研判分析，能够快速准确地进行事件确认、定级、问题定位、溯源分析，并提供可靠的遏制和恢复方案，能针对新型威胁进行深度分析、支持高级别攻击的分析和溯源，能开展运维自动化流程设计，帮助持续提升安全托管效果，为技术人员提供支撑；
b) 漏洞分析岗：负责对最新安全漏洞进行跟踪、分析，能对漏洞和安全威胁进行评估，并制定适当的漏洞修复方案和加固措施；
c) 威胁信息管理岗：负责云端威胁信息管理，能进行威胁信息源整合并沉淀为知识库，能够识别并应用适当的威胁信息与框架进行攻击者能力的跟踪与评估；
d) 防护策略管理岗：负责安全防护策略的管理及优化工作，能够制定并执行安全策略并提供策略的有效性分析。

实施操作包括安全监控岗、资产管理岗、安全运维岗、应急响应岗四个岗位。

a) 安全监控岗：负责常态化安全监控工作，负责提供远程技术支撑、远程威胁分析、远程响应处置、定期对安全事件进行统计和报告等，能使用各类方法和工具对安全设备日志和流量等安全数据进行云端监控和分析，能规划设计安全监测分析方案，给出网络安全态势的合理评价；
b) 资产管理岗：负责数据资产识别、脆弱性识别等工作，需能针对企业业务现状制定数据资产梳理方案和数据分类分级实施准则，指导数据资产梳理工作的落地，并具备对网络安全资产安全风险等级分析与评估能力；
c) 安全运维岗：负责运维管理工作部署、监控、优化、故障处理、周期性安全运维报告编制工作，需具备安全隐患的排查分析能力，能对服务器、网络设备、安全产品、信息系统进行安全维护、安全巡检、策略维护管理、配置变更、故障处置与安全分析等，消除和降低所发现的威胁；
d) 应急响应岗：负责制定安全事件应急响应预案，提供远程应急响应处置，能够对网络威胁和安全事件进行跟踪响应，能协同甲方团队进行事件处置和升级（远程/现场）。

A.2.4.2 管理流程

在全托管安全运维模式下，通过SaaS化的网络安全运维中心或远程接入本地网络安全运维中心，对用户侧的安全事件和相关数据源（包括日志、流量等）进行安全监控和威胁检测，并将各类监测结果以告警信息方式推送到网络安全运维中心/平台，自动生成处置工单后推送分配相应运维人员，对客户的安全事件进行研判、排查和响应，形成“平台+流程+人”的安全托管服务。全托管网络安全运维中心需建立以下流程：

a) 识别流程。需包括业务识别、资产识别、威胁识别、脆弱性识别、信息收集、安全合规检查等子流程的创建。托管安全服务商与运维对象需就安全运维目标达成一致，服务商需对用户侧现网安全情况及相应业务流程现状进行调研，并根据调研结果进行设备部署接入、远程策略配置、测试和服务开通。由云端运维专家通过用户自主上报、安全工具扫描等主动或被动探测技术对用户资产、威胁信息进行全面识别与梳理，建立资产管理台账、威胁信息库等，并通过云端漏洞扫描、渗透测试等多种脆弱性评估手段及威胁发现方法，识别资产暴露面；
b) 防御流程。需包括安全设备运维、安全加固、人员培训、数据安全防护等子流程的创建。托管安全服务商需获取管理企业内部的特定安全工具的权限，通过识别安全隐患和漏洞、评估危害和级别、分析防御措施等一系列流程活动，提供安全加固措施及处置方案，并对用户安全设备和工具上的安全策略进行统一管理调整，确保安全策略保持处于最优水平；

c) 监测流程。需包括网络流量监测、异常行为监测、互联网资产暴露面监测、终端监测、数据监测、域名系统监测、实时分析、深度分析等子流程的创建。由托管安全服务商通过用户的本地收集器将原始日志、流量等数据传输到网络安全运维中心，持续分析监测网络安全状态，综合发现漏洞、弱口令、勒索等安全风险和异常行为，由云端安全分析人员对研判结果进行复核，在安全分析人员无法处置时，由安全专家对问题进行深入分析调查，获取授权后采取行动，借助本地或远程部署的相关安全工具完成查杀、封锁等处置流程，形成报告推送用户；

d) 响应流程。需包括应急响应、应急预案建立、应急处置、应急总结等子流程的创建。托管安全服务商需遵循准备、诊断、抑制、根除、恢复和跟踪等应急响应流程，帮助用户在遭受突发事件后进行应急处理。通过识别发现并报告威胁级别、详细信息综合分析研判、阻断封堵、固定证据、业务恢复、溯源分析、还原攻击、事件报送以及配合公安部门追踪溯源等环节完成，同时定期复盘组织内的安全事件和风险情况，由托管安全服务商提供阶段性报告，并通过线上线下相结合的方式进行汇报，对重大事件复盘分析、总结经验，更新应急预案；

e) 网络安全运维沟通机制建立。需包括安全运维能力提升、信息协同共享、运维质量回访等子流程的创建。托管安全服务商及用户侧需分别指定接口人（通常为项目经理），由服务商针对安全运维整体工作情况定期进行总结和汇报，并定期组织用户侧进行安全培训和演练活动，同时通过运维质量回访，及时调整运维策略。

A.3 场所条件

A.3.1 概述

条件许可的组织需考虑建立独立的网络安全运维场所，以避免工作过程中安全保密信息违规扩散，提升网络安全工作人员协同效率。网络安全运维场所建设主要需考虑两个方面：场所功能要求和场所安全要求。

A.3.2 场所功能

网络安全运维场所分为运维工作和指挥工作两类。

运维工作场所用于网络安全运维人员开展日常威胁事件监控、分析、调查等工作。运维场所在建设时需考虑如下因素：

a) 场所的空间不宜过于狭小，避免对工作氛围产生负面影响，阻碍网络安全运维人员之间的沟通和协作；

b) 场所需配备安全态势视屏墙，使用大型显示幕墙，集中化、可视化展现组织的网络安全态势和威胁感知信息，帮助安全运维人员及时了解安全动态，对风险进行预判；

c) 场所需根据监控分析的需求，为每名安全运维人员配置足够的操作终端，以显示监控仪表信息，操控各种威胁分析工具；

d) 安全运维人员的操作台面和座椅需考虑人体工学因素，避免监控分析人员长期工作造成不良健康影响。

指挥工作场所用于发生网络安全事件时，管理人员决策处置方案，指挥调度处置工作等。运维指挥工作场所需考虑配备相应的网络安全态势显示、威胁信息显示大屏，指挥操作终端，以及多渠道（如电话、视频会议、电子邮件、即时通讯）的通讯工具。指挥场所的要求包括：

a) 网络安全运维场所的物理环境安全需按照相关国家标准进行建设；

b) 网络安全运维场所需设置访问控制机制配置人员访问权限；

c) 网络安全运维场所需配备门禁控制设备，限制和记录对网络安全运维场所的所有出入，并具备可调阅、查看实现回溯出入记录的能力；

d) 在条件允许的情况下，可以网络安全运维场所的出入口安装防尾随设施；
e) 网络安全运维场所需安装闭路电视摄像头，监测和记录网络安全运维场所日常情况，并具备可调阅、查看实现回溯视频记录的能力；
f) 安全运维场所需安装隔音材料，以避免内部通话信息外泄。

A.4 平台与工具

A.4.1 概述

安全运维的平台与工具是指为达到网络安全运维目标采用的系统或工具，主要功能包括传统信息安全管理、防御和运维等板块。在网络安全运维活动过程的整个过程中，可以使用某种类型开源和商业化的平台、系统和工具，技术体系涉及的平台、系统和工具涵盖识别、防御、监测和响应领域的技术支撑。

A.4.2 资产管理类平台

对资产管理类平台的条件包括：
a) 能够识别网络流量及探测、探针类设备上报的资产信息，实现多来源资产信息标准化输出；
b) 能够根据资产部署位置、受攻击情况、防护情况等维度进行资产自动分级分类，发现重要、核心资产；
c) 应用漏洞扫描工具和安全配置管理工具自动发现网络中的漏洞和安全配置问题。

A.4.3 安全运维管理与态势感知类平台

对态势感知类平台的条件包括：
a) 需支持流量数据、各类日志等对海量多源安全数据集中采集和存储，能够对安全数据进行查询、统计、关联分析，支持分析自定义分析规则；
b) 需能够通过威胁信息、机器学习、关联分析和基线分析等多个维度进行威胁的检测，提升威胁检测准确度，快速定位真正的威胁；
c) 需能够通过场景分析、实体分析、事件调查等威胁分析工具，结合安全运维工作实际场景，帮助提升安全事件研判和溯源的效率，及时进行响应处置；
d) 需能够帮助建立资产风险评估能力，实现资产安全风险综合评估，反映资产安全状态，以量化的方式体现资产安全风险和安全工作成果；
e) 需能够帮助用户持续监测网络安全态势，为安全管理者提供风险评估和应急响应的决策支撑，为安全运维人员提供威胁发现、调查分析及响应处置的能力。需部署网络安全防御平台或系统，包括加密与身份认证、防火墙、入侵检测和防御、DDoS 防御、Web 应用防火墙、防病毒系统、终端防护、漏洞扫描和修复等，以防止恶意攻击对网络和应用程序造成破坏等风险。

A.4.4 威胁检测类平台

对威胁检测类平台的条件包括：
a) 需支持全流量检测，对失陷主机、网络入侵、网络病毒、异常流量、异常行为等进行精准检测，及时识别出潜在的安全威胁；
b) 需支持基于攻击事件特征库和多维度事件分析技术，实时检测各种网络入侵及违规行为，可通过邮件、Syslog 等多种响应方式及时告誓，实时、全面检测网络攻击，需支持特征库升级；

c) 需能够提供基于 ATT&CK 标签分析告警的能力，并支持与其他系统联动，快速研判和处置告警事件；
d) 需能够发现、研判和处置重大安全事件，特别是针对新型网络攻击和 APT 攻击。应用大模型日志分析技术，通过预训练的大模型学习各种攻击和异常访问流程具备智能分析海量日志的能力，能够替代传统运维人员完成数据分析工作。

A.4.5 自动化处置工具

对自动化处置工具的条件包括：

a) 需支持将分散的工具、人员和流程有机地整合到一起，整合安全运维所需的各种资源，实现人与工具、工具与工具的连接与协作；
b) 需能够将安全操作流程或其片段转变成编排化的安全剧本，并尽可能自动化的执行，大幅降低安全运维人员的工作负担，提升工作效率；
c) 需能够便捷地对告警信息进行调查与增强，根据实战情况动态调整和组合剧本，更快速地进行告警分诊，提升单位时间内处理告警的数量和质量；
d) 需能够通过编排与自动化快速进行响应处置，实现安全运维效果的自动化、数字化度量，降低平均响应时长，提升运维水平；
e) 需能够自动记录所有对抗过程的操作记录，便于事后总结归纳，将有经验的安全运维人员的知识进行固化、沉淀、分享，并不断优化。

A.4.6 运维工具管理条件

对运维工具的管理条件包括：

a) 需建立运维工具的检测机制和能力，检测手段包括代码审查、恶意代码检测、沙箱分析等；
b) 所有运维工具均应经过安全检测，通过后应登记备案，形成运维工具清单和运维工具库；
c) 需优先使用运维工具库中的工具，使用未登记备案的运维工具前需先进行安全检测；
d) 关键信息基础设施运维采用的工具符合 GB/T 39204 7.9 的要求。

参 考 文 献

[1] GB/T 20261-2020 信息安全技术 系统安全工程 能力成熟度模型

[2] GB/T 30283-2022 信息安全技术 信息安全服务 分类与代码

[3] GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

[4] ITU-T X.1060 (06/2021) 创建和运营网络防御中心的框架（Framework for the creation and operation of a cyber defence centre）