ICS 55.020
CCS A 80

团　　体　　标　　准

T/GDIOT ×××-20××

网络安全管理运营规范

Standard for network security management and operation

（征集意见稿）

20××-××-××发布　　20××-××-××实施

广东省物联网协会　　发布

目录

前　言

本文件依据 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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由广东省物联网协会归口。

本文件由广东技术师范大学提出。

本文件起草单位：广东技术师范大学、 北京安博通科技股份有限公司、华南农业大学、广州医科大学、广东工业大学、广东食品药品职业学院、广州犀甲信息安全技术有限公司、奇安信安全技术（ 广东） 有限公司、广州非凡信息安全技术有限公司、广州安有信科技有限公司 、广东悦学科技有限公司。

本文件主要起草人：陈志华、黄经赢、刘斌、徐省华、欧威健、蔡金玲、王强、马威、阎连龙、魏文国、王小松、黄志宏、柯家海、王岗、黄慧武、唐润华、陈泉泉、李双喜、 林旭滨、苏妍、李岳学。

网络安全运营管理规范

1 范围

本标准旨在明确网络安全运营管理的流程、职责和要求，提供网络安全运营中安全管理技术要求、人员要求，以及管理要求的指导思路及方法。

本标准适用于在完成初期安全建设后教育系统内部网络系统的信息安全运营管理工作。

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。其中包括：

GB/T 25068.1-2020 信息技术 安全技术 网络安全 第一部分：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

3 术语和定义

下列术语和定义适用于本文件。

3.1 安全基线 security baseline

保障系统基本安全的最低配置要求。

3.2 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。

[来源:GB/T28458-2020,3.1]

3.3 个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合来识别特定自然人身份或者反映其活动情况的各种信息。

注 1:个人信息包括姓名、出生日期、居民身份证号码、个人生物特征信息、住址、联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注 2:个人信息控制者通过个人信息或其他加工处理后形成的信息，例如,用户画像特征标签,能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的,也属于个人信息。

[来源:GB/T25069-2022,3.196]

3.4 安全审计 security audit

对网络、信息系统及其组件的记录与活动的独立评审和考察，以测试系统控制的充分程度，确保对于既定安全策略和运行规程的符合性,发现安全违规，并在控制、安全策略和过程三方面提出改进建

议。

[来源:GB/T25069-2022,3.2,有修改]

3.5 网络安全 network security

对网络环境下存储、传输和处理的信息的保密性、完整性和可用性的保持。

[来源:GB/T25069-2022,3616]

4 网络安全运营管理框架及内容

网络安全运营管理架构是按照国家政策法律法规和教育行业网络安全方针，对网络安全进行全面规划和管理的体系结构，包括技术要求、人员要求、管理要求等方面的内容。

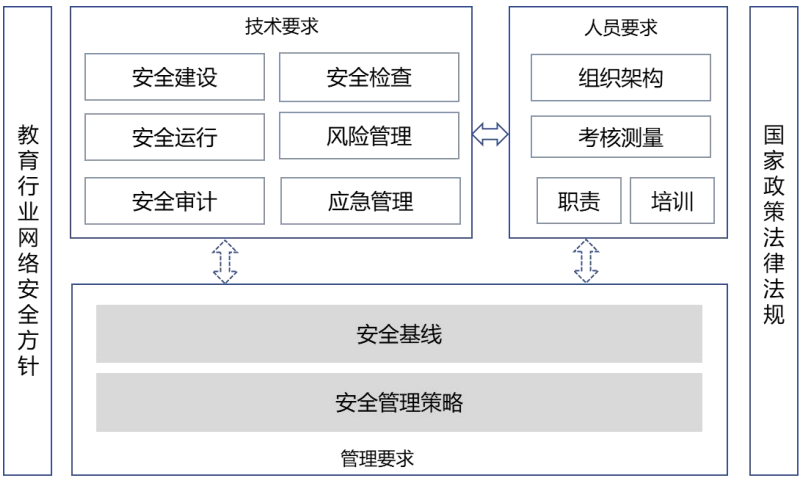

图 1 网络安全运营管理架构

5 网络安全运营技术要求

网络安全运营技术要求是通过一系列的通用安全措施，达到基本的安全运营能力，保障教育行业在网络运营过程中对各个环节进行标准化管理，并能对其建设过程中技术给予指导和要求。

5.1 网络安全制度建设

安全制度建设的目的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、资源和条件等，使安全工作规范化、标准化，提高安全管理的有效性，促进实现安全目标。

安全制度建设管理一般包括：

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) 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 网络安全运行要求

系统安全、稳定运行最基础的保障，遵循以下要求：

a) 系统的硬件设备宜部署在与其承载的业务级别相匹配的运行环境中。

b) 保障设备的业务与电力线缆不受电磁及信号干扰。

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) 保证系统维护通道和业务通道的独立，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) 在系统安全可控的环境内对系统进行维护。

g) 定期对系统的性能和安全策略进行持续的监控。

h) 定期对系统的攻击面进行量化评估，并根据业务发展情况，确保系统合规。

i) 定期对系统的授权、维权情况进行评估，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者根本性解决处置，如修改配置、持续控制、补丁升级等。

5.3 网络安全策略要求

企业应制定符合自身实际情况的网络安全策略，包括网络安全目标、原则、要求和措施。

安全策略管理宜遵循如下：

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。

5.4 网络安全漏洞管理

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。

a) **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：

—— 利用组织自有的人工或自动化方法对漏洞进行检测。

—— 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。

—— 通过接受漏洞通报机构的通报获取漏洞信息。

—— 获取软件厂商官方通报的软件漏洞信息。

b) **漏洞评估与检测**

漏洞评估师通过漏洞级别、漏洞利用方式、漏洞载体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：

—— 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。

—— 单一评估法：根据漏洞载体是否映射在互联网侧、漏洞载体是否在核心系统、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的组织。

c) **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：

—— 利用组织自有的人工或者自动化方法对漏洞进行验证。

—— 利用第三方漏洞验证服务对漏洞进行验证。

d) **漏洞通报与反馈**

对存在的漏洞进行内部通报，并向上级主管部门报告，及时获取修复方案和安全建议。

5.5 系统弱口令管理

系统的账号口令应该遵循以下：

a) 所有系统账号应设置复杂的口令，避免弱口令和默认口令，并设置密码更换策略，对密码进行定期的更换。

b) 系统认证应有详细的日志审计记录，外发至日志审计中心，进行异常登录监控管理。

c) 应及时删除或停用多余的、过期的账号，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。

5.6 网络安全基线管理

安全运营基线管理的目的在于保证业务系统的安全，使业务系统的风险在可控范围内。

a) **安全基线设置**

安全基线设置宜遵循以下：

—— 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、数据库等安全基线。

—— 可通过人工或者自动化的方式实现信息资产的安全基线设置。

b）**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和更新。

c）**安全基线例外管理**

宜定期对信息资产的安全基线设置进行检查，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 网络安全威胁管理

通过有效的措施防止网络攻击、检测网络威胁和响应安全事件，形成安全威胁闭环管理，主要的工作有检测、识别、保护、响应和恢复。

6.1 网络安全威胁监测

网络安全威胁监测的基础是数据采集，数据采集范围至少涵盖安全设备、主机设备、网络设备和应用系统，可通过大数据关联分析技术、情报碰撞技术、基线分析技术、AI 智能应用技术等进行数据分析和威胁检测，发现更复杂的、更具价值的威胁事件，并将威胁事件规模控制在可人工处理的数量级，最终以事件为线索，以海量的流量数据、安全日志数据为基础数据，对分析结果进行回溯分析。

采集类型应包含以下类型：

a）网络日志：流量会话、应用行为、文件传输、账号登录等。

b）安全日志：网络设备、主机、数据库、安全设备、中间件、虚拟化、应用系统、网关系统等。

c）终端日志：文件行为、进程行为、邮件行为、注册表等。

d）系统日志：系统登录、系统操作等。

6.2 网络安全威胁处置

网络安全威胁处置是威胁闭环管理的重要环节，通过对威胁告警的综合分析研判，将一条或多条可能对企业产生威胁的告警合并生成一个事件。借助自动化分析等技术驱动工具自动化统计分析事件对学校内资产的影响范围，关键证据信息，并自动提供常见威胁事件的处置建议。

根据专业的处置建议，通过手动或自动化的方式联动网内防火墙、杀毒等安全设备进行攻击阻断，并通知相关业务负责人修复系统脆弱性，若遇到重大网络安全事故，需启动应急响应流程，及时应对。

6.3 网络安全审计

通过网络安全审计，对网络数据进行识别、采集、分析，对校园网用户网络行为进行实时动态监测，及时捕获用户网络违规行为，响应实时警报全面记录网络对话和事件，对网络信息、事件进行安

全智能关联全程跟踪、分析、评估，准确掌，握校园网安全状态，第一时间发现违规、不安全事件，实时记录、警告，同时进行定位分析、追查取证，满足校园网安全审计需求，满足校园网安全管理需求。

6.4 网络安全内容审计

通过对校园网安全自定义关键词， 对校园网访问网站、收发邮件、 远程终端访问、 文件共享、数据传输、 数据库访问等内容进行完整检测、 信息还原、 细粒度审计追踪等功能。

6.5 网络安全行为审计

通过技术手段结合网络安全审计设定校园网行为审计的策略，对校园网访问网站、收发邮件、远程终端访问、文件共享、数据传输、数据库访问、滥用网络资源等用户行为进行动态监测，并对不符合网络安全行为策略的用户事件实时记录并警告。

6.6 网络安全流量审计

通过网络安全流量可对校园网实时报文流量进行基于协议识别的综合流量分析，为校园网流量管理提供支持。

6.7 网络安全检查

网络安全检查是保障企业或个人在网络中使用安全的重要环节。

7 技术防范措施

包括但不限于网页防篡改、防病毒、防攻击等技术措施、帐户和口令的管理措施、操作系统、应用软件、病毒防护软件等的补丁升级、网站域名安全管理措施等。宜定期开展网络安全检查和网络安全应急响应措施。

7.1 应急预案制定与演练

制定详细的网络事件应急预案，包括预警机制、响应流程、处置措施等，定期进行应急演练，确保预案的有效性和可操作性。

7.2 应急响应实施

在发生网络事件时，迅速启动应急预案，进行事件处置和分析，确保事件的及时解决，并防止事件扩大和扩散。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置工作：

a） 宜建立统一的安全运营平台，在平台上进行集中告警、事件的产生、处理、审核、复盘等全流程的安全运营工作。

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 开展常态化的运营工作。

c） 宜根据事件级别，制定响应策略，响应策略宜包括响应时限、响应人员、响应流程。

d） 宜周期性地进行安全运营响应的时间复盘和汇总，定期发送运营报告。

e） 应建立应急事件响应、通报流程。

8 集中监管与响应管理

集中监管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，持续保障运营安全管理的有效性，不断提升整体安全运营管理水平。

8.1 网络设备安全管理

通过选择符合安全要求的网络设备，做好设备的维护与管理，加强个人信息的采集、应用和管理，加强网络设备的安全管理和维护。

8.2 设备选型与部署

选择符合安全要求的网络设备，合理部署在企业的各个网络区域，并采取必要的安全措施如访问控制、加密传输等。

8.3 设备维护与管理

对网络设备进行定期维护和管理，包括升级备份、故障排除等，确保设备正常运行，防止因设备故障导致的网络安全事件。

8.4 个人信息安全运营

在安全运营过程中个人的信息应包括但不限于自然人的姓名、出生日期、身份证号码、通信通讯联系方式、个人生物特征信息、住址、账号密码、成绩和行为信息等。

8.5 个人信息采集管理

教育网络运营者在收集采集个人信息的行为应满足以下要求：

a） 个人信息收集前，应向被收集的个人信息主体公示本机构收集的目的、范围、方法和手段、处理方式等信息。

b） 个人信息收集应获得个人信息主体的同意和授权。

c） 个人信息收集应执行收集前签署的约定和协议，不应有超范围收集的现象。

d） 应确保收集个人信息过程的安全性，收集个人信息之前，应有对被收集人进行身份认证的机制；收集个人信息时，信息在传输过程中应进行加密等保护处理；收集个人信息时应有对收集内容进行安全检测和过滤的机制，防止非法内容提交。

8.6 个人信息应用管理

教育网络运营者在应用个人信息时应满足以下要求：

a） 对个人信息的应用，应符合与个人信息主体签署的相关协议和规定，不应超范围应用个人信息。

b）个人信息主体应拥有控制本人信息的权限，包括：允许对本人信息的访问；允许对本人信息的修改，包括纠正不准确和不完整的数据。

c）应对个人信息的接触者设置相应的访问控制措施，包括对被授权访问个人信息数据的工作人员按照最小授权的原则，只能访问最少够用的信息，只具有完成职责所需的最少的数据操作权限和对个人信息的重要操作设置内部审批流程，如批量修改、拷贝、下载等，以及对特定人员超限制处理个人信息时配置相应的责任人或负责机构进行审批，并对这种行为进行记录。

d）应对必须要通过界面展示的个人信息进行去标识化的处理。

8.7 个人信息数据分类

a）教育网络运营者应采取数据分类、重要数据备份和加密等措施。

b）网络运营者应遵守其他法律、行政法规规定的其他义务。

9 网络安全运营人员管理

通过设置合理的组织架构、邮寄的制度体系、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，为总体安全目标赋能。

9.1 组织架构与职责

根据校园网络安全管理目标，合理设置网络安全组织架构，明确工作职责，各司其职，共同维护校园网络安全。企业应设立完善的网络安全管理体系，包括组织架构、职责、流程和培训等，以确保网络安全得到有效管理和保障。

9.2 组织架构

企业应设立完善的网络安全管理体系，包括组织架构、职责、流程和培训等，以确保网络安全得到有效管理和保障。

9.3 岗位与职责

根据组织架构设置相应的工作岗位，明确岗位职责，细化工作任务。

9.4 网络安全主管

负责制定、审核和监督网络安全策略、政策和制度，并组织协调各部门进行网络安全管理。

9.5 网络安全管理部门

负责日常网络安全监控和维护，及时处理网络安全事件，并配合网络安全主管完成网络安全管理工作，负责制定、监督和执行网络安全策略和制度的部门。

主要职责应包括：

a）制定网络安全策略和制度，并监督执行。

b）组织网络安全培训和演练，提高员工的安全意识和技能。

c）监测网络流量和安全状况，及时发现并处理安全事件。

d）织对网络安全设备进行升级和维护，提高防护能力。

9.6 各部门负责人职责

负责落实本部门网络安全责任，执行网络安全策略和制度，并组织本部门人员参加网络安全培训和应急演练、网络安全策略与制度。

a）网络管理员：负责日常网络设备的配置和维护，监测网络流量和安全状况，协助处理网络安全事件，配置网络设备的参数，确保网络正常运行。

b）安全管理员：负责安全设备的配置和维护，定期进行安全漏洞扫描和风险评估，及时更新安全策略，监测网络设备的状态，及时发现并处理异常情况。

c）系统管理员：负责服务器和应用的配置和维护，保障数据安全和系统稳定运行，对网络流量进行分析和监控，防止网络攻击和异常流量。

d）用户部门：负责终端设备的日常管理和使用，遵守网络安全规定，及时报告网络安全问题。

9.7 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。

10 网络资产管理

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、标识、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，提升教育行业对信息安全运营管理能力。

10.1 网络资产发现

网络资产发现的目的，是对组织网络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，网络资产发现方式包括但不限于：

a）主动发现：通过主动扫描安装网络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、ARP、API、中间件及软件版本等信息。

b）被动发现：是通过流量监听的方式被动发现网络中的网络资产。

10.2 网络资产运营

网络资产运营宜遵循以下：

a) 网络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，形成网络资产威胁图谱。

b) 网络资产与威胁情报的结合:充分利用多方威胁情报，将网络资产和威胁情况结合，将威胁情报真正运用到日常工作中，当出现 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网络资产。

c) 网络安全漏洞应急响应：对于网络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网络资产对应的漏洞。

d) 网络资产漏洞全生命周期的管理：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，掌握网络资产漏洞整体状态。

e) 网络资产安全报告：包括网络资产统计、组件开放统计、端口变化趋势、漏洞加固统计、漏洞变化趋势、网络资产威胁态势报告等，展示网络资产风险状态和安全工作成果。

f) 重点网络资产监测：标记重点网络资产，设置周期性任务、进行重点管理。

g) 网络资产安全告警：新出现高危漏洞或高危漏洞数量达到阈值时进行告警，或者自定义告警条件，便于及时发现网络资产威胁、掌握安全态势，从而实现精准防御。

11 网络安全管理要求

网络安全管理宜遵循以下：

a) 定期进行网络安全风险评估，了解网络系统的安全状况和薄弱环节，制定相应的安全措施。

b) 建立完善的网络安全日志审计机制，及时发现并记录异常行为和安全事件。

c) 加强对网络设备和安全设备的巡检和维护，确保设备正常运行和安全策略有效。

d) 定期进行网络安全培训和演练，提高员工的安全意识和应急响应能力。

e) 建立网络安全事件应急预案，明确应急响应流程和责任人，确保及时有效地处理网络安全事件。

f) 定期对服务器和数据进行备份和恢复测试，确保数据安全和系统稳定性。

g) 对重要信息和数据进行加密和权限管理，防止数据泄露和非法访问。

h) 对网络流量进行监控和分析，及时发现并阻止异常流量和攻击行为。

i) 定期对网络设备和安全设备进行升级和维护，提高设备的安全性能和防护能力。

j) 与第三方合作伙伴建立紧密的网络安全合作关系，共同应对网络安全威胁。

12 安全绩效考核

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。

安全绩效管理包括但不限于：

a) 网络安全管理部门应对各部门的安全运营管理工作进行监督和考核。

b) 监督内容包括但不限于：安全制度的执行情况、安全培训和演练的开展情况、网络安全设备的配置和维护情况等。

c) 考核内容包括但不限于：网络安全事件的处理效果、数据安全的保障程度、网络安全运营管理的整体效果等。

d) 对于发现的问题和不足，应提出整改意见并跟踪落实情况，确保网络安全运营管理工作的持续改进。

e) 对于在网络安全工作中做出突出贡献的部门和个人，应给予相应的奖励和表彰。

附 录 A

（规范性）

安全运营管理度量指标

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等。

c)　教职工安全教育的效果，如钓鱼邮件测试中招人数比例、安全培训考试通过率、安全培训参与率等。

A.2　安全运营度量指标

a)　安全软件或设备相关，如：防病毒客户端、防火墙、安全策略核查工具、上网行为管理、入侵防御检测等处置数量或者检测通告率。

b)　准入设备的有效性：如准入产品造成的可用性、同一台机器上多账号的准入、同一账号多机器上的准入等重点关注异常事件的数量和处置情况。

c)　补丁管理及处置相关，如：补丁的更新率、及时率。

d)　安全基线管理的有效性，如安全基线符合率。

A.3　安全策略度量指标

网络安全运营的管理策略，如：防火墙宽松策略、冗余策略、隐藏测量、弱口令、大段策略等相关的数量和合规性要求的匹配度等。

A.4　网络资产度量指标

网络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、无主资产数量、新增资产数量等。

A.5　漏洞管理度量指标

漏洞管理相关度量指标，如:扫描发现高危漏洞数量、漏洞平均修复时长、漏洞修复等。