国家标准《信息安全技术 安全运维系统技术规范》

（征求意见稿）编制说明

**一、工作简况**

**1.1 任务来源**

根据国家标准化管理委员会2022年下达的国家标准制修订计划，《信息安全技术 安全运维系统技术规范》由上海辰锐信息科技公司负责承办，计划号：20230260-T-469。该标准由全国信息安全标准化技术委员会（SAC/TC260）归口管理。

**1.2 主要起草单位和工作组成员**

《信息安全技术 安全运维系统技术规范》由上海辰锐信息科技公司牵头制定，参与起草单位包括：公安部第三研究所、中国科学院软件研究所、华为技术有限公司、中国网络安全审查技术与认证中心、国家工业信息安全发展研究中心、浙江齐治科技股份有限公司、北京天融信网络安全技术有限公司、奇安信网神信息技术（北京）股份有限公司、北京神州绿盟科技有限公司、西安交大捷普网络科技有限公司、杭州中尔网络科技有限公司、北京蓝象标准咨询服务有限公司、长杨科技（北京)股份有限公司、杭州安恒信息技术股份有限公司、北京时代新威信息技术有限公司、北京启明星辰信息安全技术有限公司、上海三零卫士信息安全有限公司、成都卫士通信息产业股份有限公司、上海观安信息技术股份有限公司、广东安创信息科技开发有限公司、北京神州绿盟科技有限公司、远江盛邦（北京）网络安全科技股份有限公司、蓝盾信息安全技术股份有限公司、北京智游网安科技有限公司、深信服科技股份有限公司、陕西省网络与信息安全测评中心、北京信安世纪科技股份有限公司、河南中科安永科技有限公司、国网区块链科技（北京）有限公司、广东省信息安全测评中心、国网新疆电力有限公司电力科学研究院、广电计量检测集团股份有限公司。

本文件主要起草人：张艳、邹春明、胡津铭、沈亮、晏敏、王峰、申永波、王冲华、于遨洋、安高峰、杨春鹏、周进、何建锋、葛方隽、张德保、赵华、田丽丹、俞政臣、周瑞群、刘彪、鄢昱恒、谢江、钟英南、周进、刘强、韩云、刘晨、冯燕飞、付军、郭军武、石竹玉、叶劲宏、加依达尔.金格斯、唐迪。

在编制本文件的过程中，起草单位的主要分工如下：上海辰锐信息科技公司牵头组织项目的修订工作，制定修订思路，组织召开项目评审，汇总各参与单位的编制内容、拟制项目编制说明、汇总意见汇总表等。参与起草的单位中，研发生产和运维服务厂商主要承担应用场景及运维技术跟踪、安全功能要求的编制及应用试点，以及推进标准在产品研发中的应用；检测、认证机构主要负责安全保障要求及测试评价方法的编制、测评方法的试点验证，以及推进标准在认证、检测中的应用；科研院所机构主要负责安全运维技术发展跟踪、自身安全功能要求的编制，以及测评技术方法研究；咨询服务机构主要负责行业用户需求的收集、运营企业侧标准试点验证，以及后续标准的宣传、推广。

**1.3 制定背景**

随着网络技术的迅速发展，网络环境变得日趋复杂，特别是重要信息系统和关键信息基础设施中的资产数量和类型均急剧增长。误操作、违规运维操作可能会直接导致这些重要业务系统的宕机、数据丢失等风险，对安全运维的规范化管理已和外部安全防护同等重要。安全运维系统已广泛应用于各行业信息化内控管理，随着云、工控等应用场景和安全产品的发展，运维管理和审计的范畴和技术形态都有了新的变化，云安全运维、便携式移动运维、工控运维等新形态和新特性不断呈现。此外，近年来相关法律法规及行业规范对于系统的运维管理提出了诸多合规要求：网络安全法对于网络运营者、网络服务提供者提出了制定内网操作规程、持续提供安全维护、采取技术措施保障网络安全稳定运行、留存相关网络日志不少于六个月等安全保护义务；ISO 27001标准中要求组织必须记录用户访问、意外和信息安全事件的日志，并保留一定期限，以便为安全事件的调查和取证；国家网络安全等级保护要求中对重要信息系统、云租户业务应用系统等保护对象的集中身份认证、运维操作审计和细粒度的权限管控也提出了诸多要求。安全运维系统由于其安全功能属性，成为系统的核心安全管控枢纽，存储着资产管理账号、具备重要资源的访问权限等，一旦其自身存在安全短板将会为重要信息系统和关键信息基础设施引入极大的安全风险。

因此，本标准的制定一方面支撑安全运维系统的规范化管理，同时也紧密贴合重要信息系统及关键信息基础设施安全运维和资产内控管理的合规性需求，为等保和关基相关要求的技术实现规范化提供重要参考，降低运维管理安全风险。

此外，2022年3月6日全国信息安全标准化技术委员会发布的“《关于发布2022年度网络安全国家标准需求的通知》（信安秘字〔2022〕47号）”中将《信息安全技术 安全运维系统技术规范》列为支持的国家标准制定项目之一。

**1.4 起草过程**

标准制定的主要工作过程如下：

1. **申报立项阶段**

2021年11月至2022年3月，成立了标准编制组，对安全运维系统的产品技术文档、解决方案等材料进行调研梳理，查阅有关资料，编写标准编制提纲，起草了标准草案初稿，形成了申报材料;

2022年4月，标准编制组在2022年信安标委WG5第一次工作组会议上进行了立项汇报。

1. **草案阶段**

2022年4月，标准编制组根据工作组成员单位专家意见组织标准编制组讨论并修改了草案内容；2022年5月至11月，标准编制组通过内部研讨、交流，对标准草案文本进行了进一步的修改完善。

2022年12月7日，标准编制组在2022年信安标准周工作组会议上进行了标准草案的汇报，征集了成员单位专家代表的意见，并通过投票，同意修改后推进为征求意见稿。

1. **征求意见稿阶段**

标准编制组根据2022年12月7日会议周上专家代表的意见，于2022年12月8日~2023年1月5日期间对标准草案文本进行了多次编制组内部的线上会议讨论、修改和完善，并提交责任专家和标委会专家进行审阅；标准编制组根据专家意见进行了进一步修改，形成征求意见稿第一稿。

2023年2月3日，WG5工作组召开了专家研讨会，对征求意见稿进行了研讨并提出了修改意见，会后编制组根据专家意见进行了修改完善，形成征求意见稿第二稿。

2023年4月4日，信安标委会秘书处召开了专家评审会，对征求意见稿进行了评审并提出了修改意见，会后编制组根据专家意见进行了修改完善，并在编制组内部进行了集中讨论，最终形成征求意见稿第三稿。

2023年6月1日，在昆明召开的2023 年第一次“标准周”会上，编制组代表在WG5分会场上，面向全体与会人员、会员单位代表汇报了该标准的编制情况以及标准内容重点；会后，编制组对标准文稿再次进行了审查，对部分文字表述等进行了修订完善。

1. **试点验证阶段**

为提升标准质量，检验标准适用性和可操作性，全国信息安全标准化技术委员会秘书处于2023年4月13日在北京组织召开了网络安全国家标准试点工作部署会。会后标准编制组依据《2023年度网络安全国家标准试点工作方案》的工作要求，征集了试点验证参与单位，并制定了试点工作方案。

WG5工作组于4月26日在线上组织召开了标准试点工作方案讨论会。会后标准编制组根据专家意见修改完善了试点工作方案，在编制组内部进行了宣贯，明确了试点内容、计划及分工，自5月至6月开展了标准试点验证工作。

**二、标准编制原则、主要内容及其确定依据**

**2.1 标准编制原则**

为了使本标准与现有其他国家标准保持协调一致，本标准的制定参考了现行的其他国家标准，主要有GB/T 25066-2020、GB/T 18336-2015、GB/T 22239-2019、GB/T 36626-2018等。

本标准符合我国的实际情况，遵从我国有关法律、法规的规定。具体原则与要求如下：

1. 实用性原则

标准必须是可用的，才有实际意义，本标准在制定过程中严格按照流程对产品的现状、技术等相关领域展开系统的、全面的调研工作，注重与相关产品生产单位的交流，使得标准更贴近产品实际情况，保证操作性。

1. 先进性原则

标准是先进经验的总结，同时也是技术的发展趋势。要制定出先进的国家标准，必须广泛了解市场上主流产品的功能，吸收其精华，制定出具有先进水平的标准。本标准的编写始终遵循这一原则。

1. 兼容性原则

本标准既要与国际接轨，更要与我国现有的政策、法规、标准、规范等相一致。编制组在对标准起草过程中始终遵循此原则，其内容符合我国已经发布的有关政策、法律和法规。

**2.2 主要内容及其确定依据**

本项目标准规范的安全运维系统，是针对系统内控合规、降低运维管理风险、提升内部风险控制水平等需求而形成的安全产品，为企业针对服务器、虚拟机、网络设备、数据库等系统资产、云计算资源的安全运维与审计提供集中的帐号、授权、认证和审计等管理服务。标准拟规范安全运维系统的安全技术要求（安全功能要求、自身安全要求、安全保障要求）和测试评价方法，适用于该类产品的研发、采购、使用、维护、管理及检测。

1. 标准结构

本标准的编写格式和方法依照GB/T 1.1-2020 标准化工作导则 第一部分：标准的结构和编写规则，主要结构包括：

* 1. 范围
	2. 规范性引用文件
	3. 术语和定义
	4. 缩略语
	5. 概述
	6. 安全技术要求
	7. 测试评价方法
	8. 附录A
1. 范围、规范性引用文件、术语和定义和缩略语

该部分定义了本标准适应的范围，所引用的其它标准情况及以何种方式引用，术语和定义部分明确了该标准所涉及的一些术语。

在术语中明确了“安全运维系统”、“运维用户”、“运维对象”、“授权管理员”、“运维服务协议”等重要概念。

缩略语部分主要列出本标准中用的缩略语全称及中文解释。

1. 概述

对安全运维系统的安全目的、保护的对象以及安全技术要求分类及等级划分进行了概要描述，对安全技术要求的分类、主要的指标项、等级划分的原则等进行了说明。

安全运维系统为运维用户提供统一资源访问入口，借助身份认证接口实现对运维用户的身份鉴别，对资产及其账号等进行集中管理和授权，监控和审计运维操作过程，并对违规操作行为进行报警、阻断。该类产品保护的对象是服务器、虚拟机、网络设备、安全产品、数据库、云平台等信息系统重要资产。此外，安全运维系统本身及其内部的重要数据也是受保护的对象。

本文件将安全运维系统的安全技术要求分为安全功能要求、自身安全要求、安全保障要求三类。本文件按照安全运维系统安全功能要求强度划分级别，按照GB/T 18336.3-2015划分安全保障要求的级别。安全等级突出安全特性，分为基本级和增强级，安全功能、自身安全强弱和安全保障要求高低是等级划分的具体依据。

此外说明了与基本级安全技术要求相比，本文件中增强级内容有所增加或变更的内容在正文中通过“**宋体加粗**”表示。安全运维系统的安全功能要求、自身安全要求、安全保障要求应符合GB 42250-2022《信息安全技术 网络安全专用产品安全技术要求》的相关要求。

另外，以表格形式对本标准中涉及的管理员及用户角色进行了详细描述：

表1 角色描述表

|  |  |
| --- | --- |
| 角色 | 角色描述 |
| 运维用户 | 通过安全运维系统对信息资产进行运行维护和管理的用户（人员或自动化运维工具），通常以账号作为用户标识，账号由安全运维系统进行管理 |
| 管理账户（运维对象） | 受安全运维系统保护的信息资产的各类管理账户，该账户由受保护的信息资产进行维护，运维用户登录安全运维系统后通过该账户对受保护的信息资产进行运维和管理 |
| 管理员 | 对安全运维系统进行维护和管理的用户角色，包括操作员、安全员、审计员或其他自定义角色，通常不具备受保护资产的运维管理权限 |
| 操作员 | 管理员角色的一种，具有系统配置管理权限，如产品IP地址、运维用户、运维对象管理等 |
| 安全员 | 管理员角色的一种，具有安全管理权限，如访问控制策略管理等 |
| 审计员 | 管理员角色的一种，具有审计管理权限，如审计日志的查阅、分析、管理等 |

1. 安全技术要求

安全技术要求分为安全功能要求、自身安全要求、安全保障要求三类。其中，安全功能要求是对安全运维系统应具备的安全功能提出具体要求，包括运维用户管理、运维对象管理、运维服务协议支持、运维访问控制、告警、远程访问加密、运维审计、运维会话管理、高可用性、设备虚拟化、IPv6支持等；自身安全要求是对安全运维系统的自身安全保护提出具体要求，包括标识与鉴别、安全管理、审计日志等；安全保障要求针对安全运维系统的开发和使用文档的内容提出具体的要求，例如开发、指导性文档、生命周期支持、测试和脆弱性评定等。

1. 测试评价方法

本文件针对安全运维系统的安全技术要求提出对应的测试评价方法，为使用本文件的人员提供一个测试评价安全运维系统的技术准则。

测评方法部分包括了安全功能要求测评、自身安全要求测评、安全保障要求测评等，其内容是针对安全技术要求中的基本级安全要求和增强级安全要求逐项制定的测试评价方法，可用于指导和规范安全运维系统的检测工作。

1. 附录A

针对安全运维系统的典型应用场景、部署方式进行了描述。

**2.3 修订前后技术内容的对比**[仅适用于国家标准修订项目]

标准制定项目，不涉及。

**三、主要试验[或验证]情况分析**

**3.1 试验验证的分析、综述报告**

为了更全面地了解企业在攻击面管理上的现状以及所面临的困难与挑战，Randori与ESG日前开展了一项调查，对398位企业安全团队负责人进行了访谈和调研，并发布了《2022年攻击面管理现状报告》，报告数据显示：67%的受访组织表示，他们的外部攻击面在过去12个月中扩大了；69%的组织因未知、未受管理或管理不善的面向互联网的资产而受到威胁。报告调研发现，在过去一年中，随着远程办公人员数量、云解决方案和SaaS应用程序使用量的不断增加，企业组织的外部攻击面进一步扩大。近几年运维安全事故的不断发生让越来越多的政企客户意识到组织内部人员以及第三方运维人员的违规操作将给组织带来巨大的甚至难以逆转的经济利益损失，政企运维过程中的安全也成为了近两年众多客户所关注的重点领域，安全运维管理市场呈现强势发展的态势。

在《网络安全法》、《数据安全法》、《关键信息基础设施安全保护条例》、“等保2.0”以及各行业规范的推动下，安全运维系统的应用市场迎来了新的发展机遇，市场规模整体呈持续增长趋势。2022年3月31日，安全牛发布了行业广泛关注的《中国网络安全行业全景图（第九版）》，涉及二级细分领域2609项。其中，堡垒机位列收录企业数量最多的细分领域TOP10。

经调研近两年内国内安全运维系统相关的产品近300款，涉及230余家不同厂商，包括华为、腾讯、阿里云、安恒、齐治科技、天融信、奇安信、360、杭州美创、华软金盾、山东兆物、西安交大捷普、网神、格尔软件、安天、山石网科、神州绿盟、启明星辰、网御星云等等安全厂商。

**3.2 技术经济论证**

本标准的实施将有助于为国内相关研发厂商、安全运维系统部署单位和检验检测机构的测评工作提供支持，确保要求、方法的一致性，提高测评的准确性、规范性、公平性，产品的合规性，以及重要信息系统安全运维保障能力，从而降低第三方测评机构的测评开销和企业自身的合规投入。

**3.3 预期的经济效益、社会效益和生态效益**

根据中共中央、国务院印发的《国家标准化发展纲要》中的要求，强化标准实施应用。为此，本项目将遵循国家“完善认证认可、检验检测、政府采购、招投标等活动中应用先进标准机制，推进以标准为依据开展宏观调控、产业推进、行业管理、市场准入和质量监管”的思路，结合牵头单位和参与单位的优势，开展标准的实施应用。

本标准的制定一方面支撑安全运维系统的规范化管理，同时也紧密贴合重要信息系统及关键信息基础设施安全运维和资产内控管理的合规性需求，为等保和关基相关要求的技术实现规范化提供重要参考，降低运维管理安全风险。

标准的适用对象包括安全运维系统的生产厂商、部署安全运维系统的系统运营单位、网络安全主管部门以及进行安全检测评估的检验检测机构。

本项目标准发布后，首先，能够指导产品的生产厂商对产品进行研发、生产和销售；其次、能够指导检测认证机构对该类型产品进行测评认证工作，标准可应用于几乎所有的网络安全专用产品管理领域；此外，还能够对用户单位的应用部署进行有效指导，形成部署方案并落地，满足等级保护、关键信息基础设施保护等相关法律法规的合规性要求。

**四、与国际、国外同类标准技术内容的对比情况，或者与测试的国外样品、样机的有关数据对比情况**

目前国际上无相关标准。

**五、以国际标准为基础的起草情况，以及是否合规引用或者采用国际国外标准，并说明未采用国际标准的原因**

未采用国际标准。

**六、与有关法律、行政法规及相关标准的关系**

本标准与现行法律、法规以及国家标准不存在冲突与矛盾，且与《中华人民共和国网络安全法》、网络安全等级保护等合规性要求保持一致：

《中华人民共和国网络安全法》第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。

网络安全等级保护基本要求在技术层面对安全运维提出了身份鉴别、访问控制、操作审计等相关要求；在安全管理层面提出了系统运维管理、安全管理制度、安全事件处置等的相关要求。

ISO 27001标准中要求组织必须记录用户访问、意外和信息安全事件的日志，并保留一定期限，以便为安全事件的调查和取证。

相关的国家标准有GB/T 36626-2018《信息安全技术 信息系统安全运维管理指南》、GB/T 34990-2017《信息安全技术信息系统安全管理平台技术要求和测试评价方法》，但上述标准与本项目拟制定标准存在较大差异：

1）从适用的对象和范围来说：GB/T 36626-2018是为信息系统运营者针对信息系统安全运维管理体系的建设提出指导；GB/T 34990-2017中规范的对象是安全管理平台，是基于等保要求对信息系统安全机制进行集中管理的平台，管理对象是管理对象是计算环境、区域边界和通信网络。而本项目标准规范的对象是针对内控合规、降低运维管理风险、提升内部风险控制水平等需求而形成的安全产品，并覆盖传统信息系统以及云、工控等应用场景，是对系统重要IT资产（服务器、虚拟机、网络设备、安全产品、数据库、应用等）的运维过程实现集中鉴别、接入控制、授权、管理、操作审计和违规阻断。

2）从标准主要内容来看：GB/T 36626-2018主要规范了安全运维策略、组织、规程和支撑系统等方面相关活动的目的、要求和实施指南；GB/T 34990-2017提出了安全管理平台的安全技术要求和测评方法。而本项目标准拟从规范运维管理与审计系统的角度提出产品需符合的安全技术要求和相应的测试评价方法，从而为运维管理与审计系统的研发、生产、测试等提供指导和参考。

因此，从解决的问题来看，本项目拟制定的标准一方面支撑运维管理与审计系统的规范化管理，同时也紧密贴合重要信息系统及关键信息基础设施安全运维和资产内控管理的合规性需求，为等保和关基相关要求的技术实现规范化提供重要参考，降低运维管理安全风险。而GB/T 36626-2018旨在指导运营者如何开展信息系统安全运维管理体系的建立和运行等相关活动，GB/T 34990-2017规范了安全管理平台对安全策略的统一管理和执行流程的技术实现，两者均不涉及针对运维管理与审计系统的规范化安全技术要求和测试评价方法，与本项目标准制定的出发点、规范的对象、内容侧重点等各方面均有明显区别。

**七、重大分歧意见的处理经过和依据**

无。

**八、涉及专利的有关说明**

本标准不涉及专利。

**九、实施国家标准的要求，以及组织措施、技术措施、过渡期和实施日期的建议等措施建议**

本标准为生产、测试和评估安全运维系统产品提供指导性意见，建议将本标准作为推荐性国家标准在全国实施。

**十、其他应当说明的事项**

无。

国家标准《信息安全技术 安全运维系统技术规范》编制工作组

2023年6月8日