网络安全风险管理
职业技能等级标准

标准代码：510031

（2021年2.0版）

启明星辰信息技术集团股份有限公司　制定

2021 年 12 月　发布

目 次

前　　言

本标准按照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。

本标准起草单位：启明星辰信息技术集团股份有限公司、北京网御星云信息技术有限公司、北京永信至诚科技股份有限公司、山东星维九州安全技术有限公司、江苏君立华域信息安全技术股份有限公司、北京中师国培教育科技有限公司、广州市闰业职业培训学校、上海交通大学、同济大学、吉林师范大学、北京信息职业技术学院、金华职业技术学院。

本标准主要起草人：温志宇、庄志诚、杨海鹏、谢瑞璇、张镇、张帆、孙涛、刘岗、崔晓鑫、宋亦男、金建军、李禄、刘润乾、林祥、汪海航、滕鑫鹏、史宝会、苏红富、杨志鹏。

1 范围

本标准规定了网络安全风险管理职业技能等级对应的工作领域、工作任务及职业技能要求。

本标准适用于网络安全风险管理职业技能培训、考核与评价，相关用人单位的人员聘用、培训与考核可参照使用。

2 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 20270-2006 信息安全技术网络基础安全技术要求

GB/T 20271-2006 信息安全技术信息系统通用安全技术要求

GB/T 20272-2006 信息安全技术操作系统安全技术要求

GB/T 20273-2006 信息安全技术数据库管理系统安全技术要求

GB/T 25069 信息安全技术 术语

GB/T 20272-2006 信息安全技术 信息安全服务 分类

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

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

3 术语和定义

国家、行业标准界定的以及下列术语和定义适用于本标准。

3.1 基线 baseline

针对操作系统、网络、应用等安全配置基础规范基准。

3.2 残留风险 residual risk

在实施防护措施之后仍然存在的风险

[GB/T25069-2010 定义2.3.26]

3.3 风险评估 risk assessment

风险标识、分析和评价的整个过程

[GB/T25069-2010 定义2.3.44]

3.4 网络安全 cybersecurity

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[GB/T22239-2019 定义 3.1]

3.5 POC Proof of Concept

这个短语会在漏洞报告中使用，漏洞报告中的POC为一段说明或者一个攻击样例。

3.6 EXP Exploit

一段对漏洞如何利用的详细说明或者一个演示的漏洞攻击代码

4 适用院校专业

4.1 参照原版专业目录

中等职业学校：计算机应用、计算机网络技术、网络安防系统安装与维护、网络信息安全等专业。

高等职业学校：计算机应用技术、计算机网络技术、大数据技术与应用、计算机网络与安全管理、信息安全与管理等专业。

应用型本科学校：计算机科学与技术、计算机应用工程、网络工程、信息安

全与管理、信息对抗技术、网络安全与执法、网络空间安全等专业。

4.2 参照新版职业教育专业目录

中等职业学校：计算机应用、计算机网络技术、网络安防系统安装与维护、大数据技术应用、网络信息安全等专业。

高等职业学校：计算机应用技术、计算机网络技术、大数据技术、信息安全技术应用、工业互联网技术、计算机信息管理等专业。

应用型本科学校：计算机科学与技术、计算机应用工程、网络工程、信息安全与管理、信息对抗技术、网络安全与执法、大数据技术与应用、工业互联网技术、网络空间安全等专业。

高等职业教育本科学校：计算机应用工程、网络工程技术、大数据工程技术、信息安全与管理、工业互联网技术等专业。

5 面向职业岗位（群）

【网络安全风险管理】（初级）：主要面向各企事业单位、政府部门等的信息化数字化部门，从事风险评估、基线核查、基线加固、安全设备部署与使用、识别基本的 Web 攻击等工作。

【网络安全风险管理】（中级）：主要面向各企事业单位、政府部门等的信息化建设和服务的部门，从事 Web 安全分析与防护、系统安全分析与防护、一般安全事件分析等工作。

【网络安全风险管理】（高级）：主要面向各企事业单位、政府部门等的规划、建设、服务的部门，从事网络安全事件监控及应急响应、网络安全架构设计、威胁评估及情报加工等工作。

6 职业技能要求

6.1 职业技能等级划分

网络安全风险管理职业技能等级分为三个等级：初级、中级、高级，三个级别依次递进，高级别涵盖低级别职业技能要求。

【网络安全风险管理】(初级)：应用基础运维的能力，在掌握风险评估和相关安全设备的基础知识与配置使用的基础上，完成对风险管理过程中的各个流程的了解，基线的核查与检查，以及对基本的 Web 攻击的识别，实现初级网络安全风险管理人员在各企事业单位、政府部门等的信息化数字化部门中，拥有对风险管理过程的认知能力，能够使用工具进行日常的检查工作，以及对 Web 攻击的辨别能力，能够发现攻击行为。

【网络安全风险管理】(中级)：应用落实对安全事件发现处置的标准和原则，完成对一般安全事件的分析后，从中发现风险，对具体漏洞进行分析、利用、加固。针对该风险有自己的见解及解决方案，实现中级网络安全风险管理人员在各企事业单位、政府部门等的信息化建设和服务部门中，拥有独立思想和分析能力，并能够完成相应的修复工作。

【网络安全风险管理】(高级)：应用对网络安全事件的各类知识储备与完善的应急响应预案，完成在出现突发情况时，对网络安全事件全程监控并进行应急响应，并能够独立解决问题，在日常工作中可以根据网络安全的各项标准对网络架构和威胁情报进行优化。实现高级网络安全风险管理人员在各企事业单位、政府部门等的规划、建设、服务的部门中有快速响应、处置突发网络安全事件的能力，并对网络安全事件拥有预判能力，并迅速进行响应。

6.2 职业技能等级要求描述

表 1 网络安全风险管理职业技能等级要求（初级）

工作领域	工作任务	职业技能要求
1. 网络安全法与职业素养学习	1.1 网络安全法学习	1.1.1 能够深刻理解《中华人民共和国网络安全法》，并能够在工作中严格遵守法律法规中的各项条例。 1.1.2 能够深刻理解《信息安全技术网络信息安全等级保护基本要求》。当遇到信息安全事件时，可以有效的进行预防与处置。 1.1.3 能够深刻理解我国相关的法律法规，并能够在工作中严格遵守法律法规中的各项条例。
	1.2 职业素养认知	1.2.1 树立自觉维护国家、社会和公众的信息安全观念。在工作中严格律己。 1.2.2 诚实守信，遵纪守法。 1.2.3 发展自身，维护荣誉。具有社会荣誉感。 1.2.4 具有基本的网络安全风险认知，能够识别网络安全风险，并加以处置。 1.2.5 具有基本的网络安全意识，能够在工作中严格律己，恪守网络安全准则。
	1.3 信息化素养提升	1.3.1 具有基本的信息化素养，能够有基础的 IT 设备操作能力。 1.3.2 具有安全设备信息化素养，能够识别安全设备，并知晓作用及操作方法。 1.3.3 具有网络设备信息化素养,能够配置并测试网络设备，能够完成组网等基础操作。
2. 风险评估方法与标准	2.1 风险管理基础学习	2.1.1 能够深刻理解风险管理的概念、目的和意义，当遇到风险时，能够进行识别，并知道如何处置。 2.1.2 能够深刻理解风险管理中威胁、脆弱性、防护措施、资产、影响、风险等风险管理要素及相互关系。将风险管理应用于日常工作中，降低风险产生的概率。 2.1.3 理解风险管理的工作内容。能够配合相关人员进行风险管理与防范。 2.1.4 理解信息安全风险相关政策与标准，并且可以将其进行贯彻
	2.2 风险评估方法掌握	2.2.1 能够深刻理解风险评估的价值与意义，将风险评估使用至日常工作。 2.2.2 能够深刻理解风险评估资产、脆弱性、威胁等要素关系。 2.2.3 掌握风险评估的定量分析方法。 2.2.4 掌握风险评估的定性分析方法。 2.2.5 掌握风险评估前准备工作。 2.2.6 掌握资产识别、威胁识别、脆弱性识别、已有安全措施识别等风险识别方法。

工作领域	工作任务	职业技能要求
	2.3 风险评估标准掌握	2.3.1 熟悉 TCSEC（可信计算机系统评估标准）。 2.3.2 熟悉 ITSEC（信息技术安全评估标准）。 2.3.3 熟悉 CC（信息技术安全评估通用标准）。 2.3.4 了解其他风险评估标准。
3.基线核查	3.1 系统基线核查	3.1.1 能够根据系统基线核查表独立完成对目标系统的口令策略基线核查。 3.1.2 能够根据系统基线核查表独立完成对目标系统的权限策略基线核查。 3.1.3 能够根据系统基线核查表独立完成对目标系统的系统服务基线核查。 3.1.4 能够根据系统基线核查表独立完成对目标系统的认证授权基线核查。 3.1.5 能够根据系统基线核查表独立完成对目标系统的日志审计基线核查。 3.1.6 能够根据系统基线核查表独立完成对目标系统的网络通信基线核查。
	3.2 网络基线核查	3.2.1 能够根据网络设备安全基线核查表独立完成对网络设备的口令策略基线核查。 3.2.2 能够根据网络设备安全基线核查表独立完成对网络设备的身份与访问控制基线核查。 3.2.3 能够根据网络设备安全基线核查表独立完成对网络设备的会话管理基线核查。 3.2.4 能够根据网络设备安全基线核查表独立完成对网络设备的认证授权基线核查。 3.2.5 能够根据网络设备安全基线核查表独立完成对网络设备的日志审计基线核查。 3.2.6 能够根据网络设备安全基线核查表独立完成对网络设备的网络通信基线核查
	3.3 应用基线核查	3.3.1 能够根据 Web 应用安全配置基线核查表独立完成对应用系统的身份与访问控制基线核查。 3.3.2 能够根据 Web 应用安全配置基线核查表独立完成对应用系统的会话管理基线核查。 3.3.3 能够根据 Web 应用安全配置基线核查表独立完成对应用系统的代码核查。 3.3.4. 能够根据 Web 应用安全配置基线核查表独立完成对应用系统的内容核查。 3.3.5 能够根据 Web 应用安全配置基线核查表独立完成对应用系统的防钓鱼与防垃圾邮件核查。 3.3.6 能够根据 Web 应用安全配置基线核查表独立完成对应用系统的密码算法核查。

工作领域	工作任务	职业技能要求
4.安全检查	4.1 主机脆弱性扫描	4.1.1 能够使用主机漏扫对测试目标进行主机脆弱性扫描。 4.1.2 能够掌握系统漏洞基础原理并对常见攻击手段、方法、行为与实现原理有一定得了解。 4.1.3 能够对系统漏洞相关安全工具报告进行深入分析。 4.1.4 能够根据系统漏洞相关安全工具提供的报告独立完成漏洞验证。 4.1.5 能够对漏洞验证后的验证结果进行梳理并完成验证报告的书写。
	4.2 Web 漏洞扫描	4.2.1 能够使用 Web 漏洞扫描工具对测试目标进行 Web 漏洞扫描。 4.2.2 能够根据Web漏洞相关安全工具提供的报告独立完成分析和漏洞验证。 4.2.3 能够对漏洞验证后的验证结果进行梳理。 4.2.4 能够对漏洞验证后加固建议进行书写。
	4.3 常见漏洞验证	4.3.1 能够掌握 Web 漏洞基础原理并对常见攻击手段、方法、行为与实现原理有一定得了解。 4.3.2 能够根据Web漏洞基础利用原理进行相对应漏洞实践学习。 4.3.3 能够根据Web漏洞相关利用方式进行分析和漏洞验证。 4.3.4 能够对漏洞验证后的验证结果进行梳理并完成验证报告及加固建议的书写。 4.3.5 能根据漏洞检测工作任务书要求，使用相应 POC 完成漏洞验证。
5.基线加固	5.1 系统基线加固	5.1.1 能够根据系统基线核查表独立完成对目标系统的口令策略基线加固。 5.1.2 能够根据系统基线核查表独立完成对目标系统的权限策略基线加固。 5.1.3 能够根据系统基线核查表独立完成对目标系统的系统服务基线加固。 5.1.4 能够根据系统基线核查表独立完成对目标系统的认证授权基线加固。 5.1.5 能够根据系统基线核查表独立完成对目标系统的日志审计基线加固。 5.1.6 能够根据系统基线核查表独立完成对目标系统的网络通信基线加固。
	5.2 网络基线加固	5.2.1 能够根据网络设备安全基线核查表独立完成对网络设备的口令策略基线加固。 5.2.2 能够根据网络设备安全基线核查表独立完成对网络设备的身份与访问控制基线加固。

工作领域	工作任务	职业技能要求
		5.2.3 能够根据网络设备安全基线核查表独立完成对网络设备的会话管理基线加固。 5.2.4 能够根据网络设备安全基线核查表独立完成对网络设备的认证授权基线加固。 5.2.5 能够根据网络设备安全基线核查表独立完成对网络设备的日志审计基线加固。 5.2.6 能够根据网络设备安全基线核查表独立完成对网络设备的网络通信基线加固。
	5.3 应用基线加固	5.3.1 能够根据 Web 应用安全配置基线核查表独立完成对应用系统的身份与访问控制基线加固。 5.3.2 能够根据 Web 应用安全配置基线核查表独立完成对应用系统的会话管理基线加固。 5.3.3 能够根据 Web 应用安全配置基线核查表独立完成对应用系统的代码规范加固。 5.3.4 能够根据 Web 应用安全配置基线核查表独立完成对应用系统的内容加固。 5.3.5 能够根据 Web 应用安全配置基线核查表独立完成对应用系统的防钓鱼与防垃圾邮件加固。 5.3.6 能够根据 Web 应用安全配置基线核查表独立完成对应用系统的密码算法加固。
6.安全设备使用	6.1 网关安全设备使用学习	6.1.1 能够掌握防火墙安全设备相关基础原理并可以对防火墙进行基础配置。 6.1.2 能够根据目标客户实际业务环境独立部署防火墙安全设备，完成针对目标客户相应防护策略配置。 6.1.3 能够对防火墙安全设备日常故障进行分析排查。 6.1.4 能够掌握 VPN 安全设备相关基础原理并可以对 VPN 进行基础配置。 6.1.5 能够根据目标客户实际业务环境独立部署 VPN 安全设备，完成针对目标客户相应防护策略配置。 6.1.6 能够对 VPN 安全设备日常故障进行分析排查。
	6.2 检测安全设备使用学习	6.2.1 能够掌握入侵检测安全设备相关基础原理并可以对入侵检测进行基础配置。 6.2.2 能够根据目标客户实际业务环境独立部署入侵检测安全设备,完成针对目标客户相应防护策略配置。 6.2.3 能够对入侵检测安全设备日常故障进行分析排查。 6.2.4 能够掌握漏洞扫描安全设备相关基础原理并可以对网络审计进行基础配置。 6.2.5 能够根据目标客户实际业务环境独立部署漏

工作领域	工作任务	职业技能要求
		洞扫描安全设备,完成针对目标客户相应防护策略配置。 6.2.6 能够对漏洞扫描安全设备日常故障进行排查。
	6.3 终端安全设备使用学习	6.3.1 能够掌握堡垒机安全设备相关基础原理并可以对堡垒机进行基础配置。 6.3.2 能够根据目标客户实际业务环境独立部署堡垒机安全设备，完成针对目标客户相应权限策略配置。 6.3.3 能够对堡垒机安全设备日常故障进行分析排查。 6.3.4 能够编写堡垒机故障排查分析报告。

表 2 网络安全风险管理职业技能等级要求（中级）

工作领域	工作任务	职业技能要求
1.Web 安全分析与防御	1.1 Web 漏洞分析	1.1.1 能够掌握 Web 漏洞基础原理并对常见攻击手段、方法、行为与实现原理有一定的了解。 1.1.2 能够掌握 Web 漏洞相关安全工具的使用，并在日常工作中使用工具进行检测。 1.1.3 能够对 Web 漏洞相关安全工具报告进行深入解读，分析出 web 漏洞的内容和解决方案。 1.1.4 能够根据 Web 漏洞相关安全工具提供的报告独立完成分析和漏洞验证。 1.1.5 能够对漏洞验证后的验证结果进行梳理并完成验证报告及加固建议的书写。 1.1.6 能够掌握一门编程语言,实现 Web 漏洞相关 POC 的编写。
	1.2 Web 漏洞利用	1.2.1 能够对 Web 漏洞基础利用原理有一定的了解。 1.2.2 能够根据 Web 漏洞基础利用原理进行相对应漏洞实践学习。 1.2.3 能够根据 Web 漏洞相关利用方式进行分析和漏洞验证。 1.2.4 能够对漏洞验证后的验证结果进行梳理并完成验证报告及加固建议的书写。 1.2.5 能够掌握一门编程语言，实现系统漏洞相关 EXP 的编写。
	1.3 Web 漏洞加固	1.3.1 能够掌握 Web 漏洞常见加固注意事项及加固点校验。 1.3.2 能够针对目标客户 Web 服务进行加固方案编写。

工作领域	工作任务	职业技能要求
		1.3.3 能够针对目标客户 Web 服务进行已知分析和漏洞修复。 1.3.4 能够针对目标客户 Web 服务已修复漏洞进行二次验证。 1.3.5 能够针对目标客户 Web 服务已知漏洞进行漏洞管理与补丁管理。
2. 系统安全分析与防御	2.1 系统漏洞分析	2.1.1 能够掌握系统漏洞基础原理并对常见攻击手段、方法、行为与实现原理有一定的了解。 2.1.2 能够掌握系统漏洞相关安全工具的使用，并在日常工作中使用工具进行检测。 2.1.3 能够对系统漏洞相关安全工具报告进行深入分析，分析出系统漏洞的内容和解决方案。 2.1.4 能够根据系统漏洞相关安全工具提供的报告独立完成漏洞验证。 2.1.5 能够对漏洞验证后的验证结果进行梳理并完成验证报告的书写。 2.1.6 能够掌握一门编程语言，实现系统漏洞相关 POC 的编写。
	2.2 系统漏洞利用	2.2.1 能够对系统漏洞基础利用原理有一定的了解。 2.2.2 能够根据系统漏洞基础利用原理进行相对应漏洞实践学习。 2.2.3 能够根据系统漏洞相关利用方式进行分析和漏洞验证。 2.2.4 能够对漏洞验证后的验证结果进行梳理并完成验证报告及加固建议的书写。 2.2.5 能够掌握一门编程语言，实现系统漏洞相关 EXP 的编写
	2.3 系统漏洞加固	2.3.1 能够掌握系统漏洞常见加固注意事项及加固点校验。 2.3.2 能够针对目标客户系统进行加固方案编写。 2.3.3 能够针对目标客户系统进行已知漏洞分析和修复。 2.3.4 能够针对目标客户系统已修复漏洞进行二次验证。 2.3.5 能够针对目标客户系统已知漏洞进行漏洞管理与补丁管理。
3.安全事件分析	3.1 风险情报分析	3.1.1 能够结合风险情报信息对安全事件进行确认。 3.1.2 能够结合风险情报信息对安全事件进行归类。 3.1.3 能够对安全事件进行优先性排序。 3.1.4 能够将分析处置的事件中定位的攻击侧特征提取为可用情报，为整合情报提供素材。

工作领域	工作任务	职业技能要求
	3.2 分析用例编写	3.2.1 能够了解常见安全事件分析原理，编写分析用例。 3.2.2 了解应急响应过程中的各个流程及方法。 3.2.3 能够掌握应急响应过程中相关工具使用，在应急预案生效时可以熟练使用。 3.2.4 能够对应急响应过程产生文档进行归类。

表 3 网络安全风险管理职业技能等级要求（高级）

工作领域	工作任务	职业技能要求
1. 网络安全事件应急响应	1.1 Web 安全事件分析与处置	1.1.1 能够熟练掌握Web 安全事件分析的方法、原理、基本要素，针对目标发生的 Web 安全事件可以进行定位核查。 1.1.2 能够熟练应用 Web 安全事件分析相关安全工具，通过相关安全工具可以对目标发生的 Web 安全事件能进行快速、精准定位。 1.1.3 能够熟练应用 Web 安全事件处置工具，针对目标发生的 Web 安全事件进行处置。 1.1.4 能够根据 Web 安全事件定位、分析、处理流程撰写 Web 安全事件报告。 1.1.5 能够根据 Web 安全事件报告进行后续监控。
	1.2 系统安全事件分析与处置	1.2.1 能够熟练掌握系统安全事件分析的方法、原理、基本要素，针对目标发生的系统安全事件可以进行定位核查。 1.2.2 能够熟练应用系统安全事件分析相关安全工具，通过相关安全工具可以对目标发生的系统安全事件能进行快速、精准定位。 1.2.3 能够熟练应用系统安全事件处置工具，针对目标发生的系统安全事件进行处置。 1.2.4 能够根据系统安全事件定位、分析、处理流程撰写系统安全事件报告。 1.2.5 能够根据系统安全事件报告进行后续监控
	1.3 网络安全事件分析与处置	1.3.1 能够熟练掌握网络安全事件分析的方法、原理、基本要素，针对目标发生的网络安全事件可以进行定位核查。 1.3.2 能够熟练应用系统安全事件分析相关安全工具，通过相关安全工具可以对目标发生的网络安全事件能进行快速、精准定位。 1.3.3 能够熟练应用系统安全事件处置工具，针对目标发生的网络安全事件进行处置。 1.3.4 能够根据系统安全事件定位、分析、处理流程

工作领域	工作任务	职业技能要求
		撰写网络安全事件报告。 1.3.5 能够根据网络安全事件报告进行后续监控
2. 网络安全架构分析与优化	2.1 网络安全架构设计	2.1.1 能够根据信息系统实际情况选择网络设备。 2.1.2 能够根据服务系统的实际需求确定基本技术参数。 2.1.3 能够根据不同区域的不同功能和安全要求，将网络划分为不同的安全域。 2.1.4 能够根据不同的安全域，能够指定不同的安全策略。 2.1.5 能够根据网络实际情况，设计网络线路和网络重要设备冗余措施； 2.1.6 能够明确网络安全防护策略，更具需求部署安全设备；
	2.2 网络安全架构故障分析与解决	2.2.1 能够分析企业前期设计网络架构拓扑图。 2.2.2 能够根据安全事件报告分析常见网络安全架构故障。 2.2.3 能够根据安全事件报告诊断网络安全架构故障。 2.2.4 能够根据安全事件报告排除网络安全架构故障。
	2.3 网络安全架构优化	2.3.1 能够编写网络安全架构优化方案。 2.3.2 能够针对目标 Web 服务存在的残留风险进行优化。 2.3.3 能够针对目标系统存在的残留风险进行优化。 2.3.4 能够针对目标网络设备存在的残留风险进行优化。
3.威胁情报分析	3.1 威胁情报加工	3.1.1 能够掌握情报平台中的功能使用。 3.1.2 能够从情报平台中提取并汇聚存在威胁的情报。 3.1.3 能够对提取到的威胁情报进行优先性排序。 3.1.4 能够将收集到的威胁情报转化为可以指导风险管理团队进行威胁分析的战术级情报。
	3.2 开源工具的使用	3.2.1 能够掌握 Elasticsearch 工具使用。 3.2.2 能够掌握 Kibana 工具使用。 3.2.3 能够掌握 SIEM 工具使用。 3.2.4 能够掌握 Beats 工具使用。 3.2.5 能够掌握开源蜜罐工具使用。

工作领域	工作任务	职业技能要求
	3.3 威胁检测规则脚本编制	3.3.1 能够掌握常见威胁检测规则。 3.3.2 能够根据规则编写相应的检测规则脚本。 3.3.3 能够独立完成上机检查，并对编写脚本进行测试。 3.3.4 能够对整体流程进行规范化，并输出威胁检测规则脚本。
	3.4 告警规则编写	3.4.1 能够掌握常见告警规则。 3.4.2 能够根据规则编写相应的告警规则脚本。 3.4.3 能够独立完成上机检查，并对编写脚本进行测试。 3.4.4 能够对整体流程进行规范化，并输出告警规则脚本。
	3.5 风险管理优化改进	3.5.1 能够通过威胁情报、威胁检测工具对系统进行风险评估并对评估过程进行监控。 3.5.2 能够通过威胁情报、威胁检测工具对网络进行风险评估并对评估过程进行监控。 3.5.3 能够通过威胁情报、威胁检测工具对应用进行风险评估并对评估过程进行监控。 3.5.4 能够通过威胁情报、威胁检测工具对系统、网络、应用的风险评估结果和管理技术工作进行持续有效性验证。并给出风险管理优化改进的可行性方案。

参考文献

[1] 教育部关于印发《职业教育专业目录（2021 年）》的通知（教职成〔2021〕2 号）

[2] 《教育部关于公布 2019 年度普通高等学校本科专业备案和审批结果的通知》（教高函〔2020〕2 号）

[3] 《教育部关于公布 2020 年度普通高等学校本科专业备案和审批结果的通知》（教高函〔2021〕1 号）

[4] 高等职业学校专业教学标准.2019

[5] 本科专业教学质量国家标准

[6] 中等职业学校专业教育标准（试行）

[7] GB/T 20270-2006 信息安全技术网络基础安全技术要求

[8] GB/T 20271-2006 信息安全技术信息系统通用安全技术要求

[9] GB/T 20272-2006 信息安全技术操作系统安全技术要求

[10] GB/T 20273-2006 信息安全技术数据库管理系统安全技术要求

[11] GB/T 25069-2010 信息安全技术 术语

[12] GB/T 30283-2013 信息安全技术 信息安全服务 分类

[13] 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

[14] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

[15] GB_T 20984-2007《信息安全技术 信息安全风险评估规范》