# 网络与信息安全管理员 S
# （网络安全咨询员）
# 国家职业标准

（征求意见稿）

## 1 职业概况

### 1.1 职业名称

网络与信息安全管理员[1]（网络安全咨询员）[2]

### 1.2 职业（工种）编码

4-04-04-02-005

### 1.3 职业（工种）定义

网络与信息安全管理员：从事网络及信息安全管理、防护、监控工作的人员。

网络安全咨询员：从事网络安全规划、设计、管理、风险评估以及培训指导等咨询工作的人员。

### 1.4 职业技能等级

本工种共设三个等级，分别为：三级/高级工、二级/技师、一级/高级技师。

### 1.5 职业环境条件

室内、常温。

### 1.6 职业能力特征

具有学习、观察、、沟通协调、计算、色觉、视觉能力，动作协调。

### 1.7 普通受教育程度

高中毕业（或同等学力）。

### 1.8 职业培训要求

#### 1.8.1 培训参考时长

三级/高级工不少于 120 标准学时；二级/技师不少于 100 标准学时；一级/高级技师不少于 80 标准学时。

---

[1]本职业分为网络安全管理员、信息安全管理员、网络信息审核员、数据安全管理员、网络安全咨询员、关键信息基础设施安全监测防护技术员六个工种，本标准仅~~针对~~适用于网络安全咨询员工种。

。

### 1.8.2 培训教师

培训三级/高级工的教师应具有本职业二级/技师及以上职业资格（职业技能等级）证书或相关专业中级及以上专业技术职务任职资格；培训二级/技师的教师应具有本职业一级/高级技师职业资格（职业技能等级）证书或相关专业高级专业技术职务任职资格；培训一级/ 高级技师的教师应具有本职业一级/高级技师职业资格（职业技能等级）证书 2 年以上或相关专业高级专业技术职务任职资格 2 年以上。

### 1.8.3 培训场所设备

理论知识培训在教室或计算机房进行；操作技能培训在具有必备的网络安全设备、软硬件等设施设备的场所进行。

## 1.9 职业技能评价要求

### 1.9.1 申报条件

具备以下条件之一者，可申报三级/高级工：

（1）累计从事本职业或相关职业[1]工作满 10 年。

（2）取得本职业或相关职业四级/中级工职业资格（职业技能等级）证书后，累计从事本职业或相关职业工作满 4 年。

（3）取得符合专业对应关系的初级职称（专业技术人员职业资格）后，累计从事本职业或相关职业工作满 1 年。

（4）取得本专业或相关专业[2]的技工院校高级工班及以上毕业证书（含在读

[1] 相关职业：信息安全测试员、信息通信网络运行管理员、信息通信信息化系统管理员、信息安全工程技术人员、数据安全工程技术人员、计算机软件测试员、计算机程序设计员、电子数据取证分析师、信息系统运行维护工程技术人员、计算机软件工程技术人员、计算机网络工程技术人员。

[2] 本专业或相关专业：信息安全、网络空间安全、网络信息安全、网络与信息安全、信息安全与管理、网络安全与执法、保密技术、大数据技术与应用、电子技术应用、电子商务技术、电子与计算机工程、电子与信息技术、工业互联网技术应用、计算机程序设计、计算机科学与技术、计算机网络技术、计算机网络

应届毕业生）。

（5）取得本职业或相关职业四级/中级工职业资格（职业技能等级）证书，并取得高等职业学校、专科及以上普通高等学校本专业或相关专业毕业证书（含在读应届毕业生）。

（6）取得经评估论证的高等职业学校、专科及以上普通高等学校本专业或相关专业的毕业证书（含在读应届毕业生）。

具备以下条件之一者，可申报二级/技师：

（1）取得本职业或相关职业三级/高级工职业资格（职业技能等级）证书后，累计从事本职业或相关职业工作满 5 年。

（2）取得符合专业对应关系的初级职称（专业技术人员职业资格）后，累计从事本职业或相关职业工作满 5 年，并在取得本职业或相关职业三级/高级工职业资格（职业技能等级）证书后，从事本职业或相关职业工作满 1 年。

（3）取得符合专业对应关系的中级职称（专业技术人员职业资格）后，累计从事本职业或相关职业工作满 1 年。

（4）取得本职业或相关职业三级/高级工职业资格（职业技能等级）证书的高级技工学校、技师学院毕业生，累计从事本职业或相关职业工作满 2 年。

（5）取得本职业或相关职业三级/高级工职业资格（职业技能等级）证书满 2 年的技师学院预备技师班、技师班学生。

---

应用、网络工程、计算机系统与维护、计算机信息管理、计算机应用技术、计算机应用与维修、计算机与数码产品维修、空间信息与数字技术、区块链工程、人工智能技术服务、人工智能技术应用、软件工程、软件技术、软件与信息服务、数据科学与大数据技术、数字媒体技术、数字媒体技术应用、通信技术、通信网络应用、通信系统工程安装与维护、通信运营服务、网络安防系统安装与维护、网站建设与管理、物联网工程、物联网技术应用、物联网应用技术、新媒体技术、虚拟现实技术、虚拟现实技术应用、虚拟现实应用技术、移动应用技术与服务、移动应用开发、云计算技术应用、云计算技术与应用、智能科学与技术等专业。

具备以下条件者，可申报一级/高级技师：

（1）取得本职业或相关职业二级/技师职业资格（职业技能等级）证书后，累计从事本职业或相关职业工作满 5 年。

（2）取得符合专业对应关系的中级职称后，累计从事本职业或相关职业工作满 5 年，并在取得本职业或相关职业二级/技师职业资格（职业技能等级）证书后，从事本职业或相关职业工作满 1 年。

（3）符合专业对应关系的高级职称（专业技术人员职业资格）后，累计从事本职业或相关职业工作满 1 年。

### 1.9.2 评价方式

分为理论知识考试、操作技能考核以及综合评审。理论知识考试以笔试、机考等方式为主，主要考核从业人员从事本职业应掌握的基本要求和相关知识要求；操作技能考核主要采用现场操作、模拟操作等方式进行，主要考核从业人员从事本职业应具备的技能水平；综合评审主要针对二级/技师和一级/高级技师，通常采取审阅申报材料、答辩等方式进行全面评议和审查。

理论知识考试、操作技能考核和综合评审均实行百分制，成绩皆达 60 分（含）以上者为合格。

### 1.9.3 监考人员、考评人员与考生配比

理论知识考试中的监考人员与考生配比不低于 1:15（其中，采用机考方式的一般不低于 1:30），且每个考场不少于 2 名监考人员；操作技能考核中的考评人员与考生配比不低于 1：10，且考评人员为 3 名（含）以上单数，每位考生由不少于 3 名（含）考评员评分；综合评审委员为 3 人（含）以上单数。

### 1.9.4 评价时长

理论知识考试时间不少于 90 分钟，操作技能考核时间不少于 90 分钟。综合评审时间不少于 20 分钟。

### 1.9.5 评价场所设备

理论知识考试在标准教室或计算机房进行；操作技能考核在具有必备的网络与信息安全设备、软硬件、设施完善的场所进行；综合评审在具有录音/录像设备的场地进行。

## 2 基本要求

### 2.1 职业道德

#### 2.1.1 职业道德基本知识

#### 2.1.2 职业守则

（1）遵纪守法，爱岗敬业。

（2）勤奋进取，忠于职守。

（3）认真负责，团结协作。

（4）爱护设备，安全操作。

（5）诚实守信，保守秘密。

（6）勇于创新，精益求精。

### 2.2 基础知识

#### 2.2.1 基础理论知识

（1）网络安全的基础知识。

（2）数据安全的基础知识。

（3）个人信息保护的基础知识。

（4）网络和通信的原理知识。

（5）计算机的组成原理知识。

（6）密码学的基础知识。

（7）网络安全管理的基础知识。

（8）咨询的概念、特征和功能。

#### 2.2.2 基础技术知识

（1）操作系统的基础知识。

（2）身份鉴别的基础技术。

（3）访问控制的基础技术。

（5）网络攻防的基础知识。

（6）网络产品的原理与应用知识。

#### 2.2.3 相关法律法规、管理规定、标准知识

（1）《中华人民共和国民法典》的相关知识。

（2）《中华人民共和国劳动法》的相关知识。

（3）《中华人民共和国网络安全法》的相关知识。

（4）《中华人民共和国数据安全法》的相关知识。

（5）《中华人民共和国个人信息保护法》的相关知识。

（6）《中华人民共和国密码法》的相关知识。

（7）《关键信息基础设施安全保护条例》的相关知识。

（8）其他国内外网络安全、数据安全、个人信息保护相关法律法规、管理规定、技术标准的相关知识。

## 3 工作要求

本标准对三级/高级工、二级/技师、一级/高级技师的技能要求和相关知识要求依次递进，高级别涵盖低级别的要求。

### 3.1 三级/高级工

| 职业功能 | 工作内容 | 技能要求 | 相关知识要求 |
| --- | --- | --- | --- |
| 1.网络安全规划咨询 | 1.1 网络安全规划需求识别和确定 | 1.1.1 能通过调研、访谈等方式识别咨询方对网络安全的整体需求，编制需求清单<br>1.1.2 能分析并确定网络安全事件对咨询方的业务影响<br>1.1.3 能确定网络安全规划在咨询方内部的覆盖范围 | 1.1.1 网络安全保障框架模型<br>1.1.2 网络安全管理体系和流程 |
| | 1.2 数据安全规划需求识别和确定 | 1.2.1 能通过调研、访谈的方式识别咨询方的数据安全需求，编制需求清单<br>1.2.2 能分析并确定数据安全事件对咨询方的业务影响<br>1.2.3 能确定数据安全规划在咨询方内部的覆盖范围 | 1.2.1 数据安全需求的分析方法<br>1.2.2 数据分类分级和敏感性评估的方法和工具<br>1.2.3 数据安全的技术、工具 |
| | 1.3 网络安全规划制定 | 1.3.1 能分析梳理出现有网络安全法律法规及标准等对网络安全规划组成内容的合规性要求<br>1.3.2 能与咨询方各部门和 IT 系统供应商进行有效沟通，收集制定网络安全规划所需的信息，编制规划提纲 | 1.3.1 网络安全技术和工具的使用方法<br>1.3.2 分布式拒绝服务、恶意代码、社会工程等常见的网络攻击和威胁<br>1.3.3 全国信息安全标准化技术委员会、国际标准化组织等发布的网络安全技术指引和最佳实践案例 |
| | 1.4 网络安全建设规划实施 | 1.4.1 能根据要求选择安全硬件、软件、服务等，并组织实施<br>1.4.2 能按照法律、行政法规的规定和国家标准的强制性要求， | 1.4.1 网络安全技术工具的使用规范<br>1.4.2 网络安全国家标准规定的强制性要求 |

| | | | |
|---|---|---|---|
| | | 检查网络安全建设的合规性和完备性 | 1.4.3 项目管理的基本知识 |
| 2.网络安全设计咨询 | 2.1 网络安全设计需求识别和确定 | 2.1.1 能调研咨询方网络和信息系统组成架构<br>2.1.2 能识别咨询方网络和信息系统各组成部分对安全保护设计的需求 | 2.1.1 网络架构设计规范、数据业务流程、系统功能和业务需求的方法<br>2.1.2 网络安全设计的方法和技巧，局域网、广域网、云计算等常见的网络架构和技术的原理<br>2.1.3 防火墙、入侵检测、安全网关等各类网络安全产品和解决方案 |
| | 2.2 数据安全设计需求识别和确定 | 2.2.1 能调研咨询方网络和信息系统组成架构，了解各网络和信息系统承载的数据类型<br>2.2.2 能识别咨询方数据处理的全流程活动，确定各数据处理环节对安全保护的设计需求 | 2.2.1 网络架构设计规范、数据业务流程、系统功能和业务需求的方法<br>2.2.2 数据处理活动的识别和表示方法<br>2.2.3 数据处理活动的安全需求识别方法 |
| | 2.3 网络安全策略设计 | 2.2.1 能分析网络安全风险，确定网络安全威胁和风险信息，为制定网络安全策略提供依据<br>2.2.2 能分析网络安全策略的成本和效益 | 2.2.1 行业业务需求的分析方法<br>2.2.2 防火墙、入侵检测、安全信息和事件管理系统等各类安全技术和工具的使用方法<br>2.2.3 网络安全事件影响的分析方法<br>2.2.4 安全策略、设备成本评估及实用性分析的知识 |
| 3.网络安全管理咨询 | 3.1 网络安全管理制度机制建设 | 3.1.1 能调研咨询方网络安全管理现状，撰写分析报告<br>3.1.2 能检查咨询方的网络安全管理制度漏洞，研判网络安全风险 | 3.1.1 网络安全管理体系的要求、组成要素<br>3.1.2 网络安全风险管理的基本概念、方法和工具 |
| | 3.2 网络资产管理 | 3.2.1 能收集网络资产信息<br>3.2.2 能使用专业工具对网络资产进行识别、分类<br>3.2.3 能执行网络资产管理策略 | 3.2.1 网络体系结构、网络设备、服务器等的基本工作原理<br>3.2.2 操作系统、数据库、应用程序等信息系统的组成和工作原理<br>3.2.3 网络资产管理的原理和方法<br>3.2.4 防火墙、入侵检测、网关和 VPN 等常见的网络安全技术和工具的使用方法 |

| | | | |
|---|---|---|---|
| | 3.3 数据资产识别与安全管理 | 3.3.1 能识别数据测绘工具，对咨询方的数据资产进行收集、整理<br>3.3.2 能根据分类分级指南，对咨询方的数据资产进行分类分级标识和管理<br>3.3.3 能依据个人信息保护的相关规定，提出适合咨询方的隐私政策建议 | 3.3.1 数据资产管理的原理和方法<br>3.3.2 数据分类分级的技术方法、实践案例以及数据分类分级产品知识<br>3.3.3 个人信息保护的影响评估和工程化方法 |
| | 3.4 网络安全应急管理 | 3.4.1 能确定和分析安全事件，并能采取应急响应措施<br>3.4.2 能及时向相关部门报告安全事件的详细信息<br>3.4.3 能评估和处理系统中的安全漏洞 | 3.4.1 网络安全事件响应的整体流程<br>3.4.2 常见的攻击手段和攻击方式<br>3.4.3 漏洞扫描工具的使用、漏洞验证和修复建议等安全漏洞评估的方法和流程<br>3.4.4 日志记录、事件溯源、取证分析等安全事件记录和分析的方法和技巧，安全事件分析工具的使用方法 |
| 4.网络安全风险评估 | 4.1 风险评估准备 | 4.1.1 能确定风险评估目标<br>4.1.2 能确定风险评估范围并收集相关网络和数据资产<br>4.1.3 能进行网络资产测绘<br>4.1.4 能根据评估范围和目标选择合适的评估方法 | 4.1.1 网络安全风险评估方法<br>4.1.2 网络资产测绘的方法<br>4.1.3 外部威胁种类 |
| | 4.2 风险识别 | 4.2.1 能利用漏洞扫描工具进行漏洞检测<br>4.2.2 能进行脆弱性识别 | 4.2.1 网络安全运维管理相关知识<br>4.2.2 漏洞检测的流程<br>4.2.3 脆弱性评估与管理的方法<br>4.2.4 可拓展威胁检测与响应方法 |
| | 4.3 风险分析 | 4.3.1 能整理、归纳和分析网络安全风险相关的数据和信息<br>4.3.2 能根据威胁程度和频率，以及漏洞被利用的难易程度，评估安全事件发生的可能性 | 4.3.1 网络安全风险分析方法<br>4.3.2 网络安全态势感知分析方法及工具使用 |

## 3.2 二级/技师

| 职业功能 | 工作内容 | 技能要求 | 相关知识要求 |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 1.网络安全规划咨询 | 1.1 网络安全规划需求识别和确定 | 1.1.1 能调研、分析咨询方的网络环境、业务场景和业务系统，识别出存在的网络安全问题<br>1.1.2 能评估咨询方的安全要求，包括对核心业务连续性的保护需求、对合规性要求的满足程度等，充分理解咨询方网络安全规划提纲要求 | 1.1.1 网络拓扑、系统架构、安全策略、风险状况，以及各种常见的网络安全漏洞和对策<br>1.1.2 分析业务需求和关键业务流程<br>1.1.3 业务流程和风险管理，项目管理方法<br>1.1.4 网络安全规划相关的法律法规和标准要求 |
| | 1.2 数据安全规划需求识别和确定 | 1.2.1 能判断咨询方数据规模，并依据咨询方业务性质对数据进行分类分级和评估，确定数据的敏感性<br>1.2.2 能分析和评估数据在收集、存储、传输、使用和销毁等处理过程中的风险和安全威胁，识别潜在的数据安全风险 | 1.2.1 数据分类分级和敏感性评估的方法和工具<br>1.2.2 数据风险识别的原理、方法<br>1.2.3 数据安全工具和产品的使用方法 |
| | 1.3 网络安全规划制定 | 1.3.1 能评估网络安全的风险和威胁，确定网络安全规划的核心要素<br>1.3.2 能根据咨询方的需求和风险评估结果，确定网络安全管理目标、控制措施和工作计划<br>1.3.3 能运用网络安全规划模型制定设计方案 | 1.3.1 网络安全风险和威胁的识别原理、方法和工具<br>1.3.2 主流网络安全产品的功能、特点<br>1.3.3 国内外主要网络安全保障模型的设计原理和方法<br>1.3.4 网络安全控制措施的制定原理和要求 |
| | 1.4 数据安全规划制定 | 1.4.1 能评估、分析和管理已知数据安全威胁，并建立数据安全威胁分析模型<br>1.4.2 能设计并评估数据安全的解决方案，确保安全措施的合理性和可操作性 | 1.4.1 数据分类分级标准、敏感数据标识等数据安全分类分级方法和原则<br>1.4.2 身份认证与访问控制、加解密等常见的数据安全技术和工具<br>1.4.3 咨询方安全意识培训的方法和策略<br>1.4.4 风险评估和管理的方法和工具 |
| | 1.5 网络安全建设规划指导 | 1.5.1 能根据网络安全系统规划和确定的建设目标，面向咨询方实际安全需求，制定网络安全建设的实施计划<br>1.5.2 能根据建设特点和咨询方情况合理进行任务分解<br>1.5.3 能根据咨询方需求和业 | 1.5.1 识别和确定咨询方的业务流程和网络安全需求的方法<br>1.5.2 主流网络安全产品的功能、特点<br>1.5.3 常规网络安全事件分析与处置的技术和方法 |

| | | | |
|---|---|---|---|
| | | 务特点，对安全的硬件、软件、服务、工具等进行合理选型<br>1.5.4 能及时了解行业最新的安全技术进展、安全发展趋势、安全威胁情报等，了解最新典型的网络安全事件基本情况 | 1.5.4 行业典型网络安全事件案例过程 |
| 2.网络安全设计咨询 | 2.1 网络安全设计需求识别和确定 | 2.1.1 能根据调研问题，总结咨询方的网络安全架构设计需求<br>2.1.2 能够根据咨询方网络安全架构设计需求，确定网络安全架构的组成要素 | 2.1.1 网络架构的设计规范方法<br>2.1.2 网络安全设计的方法和技巧，局域网、广域网、云计算等常见的网络架构和技术的原理<br>2.1.3 咨询方的业务需求和行业特点 |
| | 2.2 数据安全设计需求识别和确定 | 2.2.1 能根据调研问题，总结咨询方的数据安全体系架构设计需求<br>2.2.2 能根据咨询方数据安全体系架构设计需求，确定架构的组成要素 | 2.2.1 数据安全成熟度能力模型等国内外数据安全保护体系的理论、方法<br>2.2.2 国内外数据安全保护的实践案例 |
| | 2.3 网络安全架构设计 | 2.3.1 能设计网络安全架构的组件，包括网络边界的防护、内部网络的隔离和访问控制、安全设备的部署等<br>2.3.2 能评估网络安全架构的性能和效果，识别潜在的风险和改进的可能性，为安全架构的优化提供建议<br>2.3.3 能根据需求选择和配置适当的安全技术 | 2.3.1 网络安全架构的设计原理和方法，适应性、分层原则、防御深度原则等网络安全架构设计的基本原则<br>2.3.2 网络安全架构分析原则，包括安全架构的设计要点、难点和解决方案等<br>2.3.3 防火墙、入侵检测和防御系统、虚拟专用网络、数据加密等网络安全技术 |
| | 2.4 网络安全策略设计 | 2.4.1 能对网络安全威胁和风险进行建模，确定网络安全策略的组成要素<br>2.4.2 能评估和选择安全技术和产品 | 2.4.1 行业业务需求、模型构建、风险评估标准、合规要求规范<br>2.4.2 防火墙、入侵检测系统、安全信息和事件管理系统等各类安全技术和工具<br>2.4.3 咨询方的业务需求和行业特点，识别和分析安全事件的影响<br>2.4.4 安全策略、设备成本评估及实用性分析 |

| | | | |
|---|---|---|---|
| 3.网络安全管理体系咨询 | 3.1 网络安全管理制度机制建设 | 3.1.1 能分析咨询方的组织架构，针对性地制定网络安全岗位责任制度<br>3.1.2 能根据实际情况，制定网络安全监测报告、合规检查、评估审计、安全审查等管理机制 | 3.1.1 网络安全管理的基本原理和方法，网络安全管理体系的组成部分和要求<br>3.1.2 网络安全流程和控制的要求和方法，访问控制、安全审计、事件响应等流程和控制措施<br>3.1.3 组织管理、流程管理、人员管理等管理学的基本理论和方法 |
| | 3.2 网络资产管理 | 3.2.1 能协调相关部门，收集和整理咨询方的硬件、软件、网络、数据、文档等相关信息，编制资产清单<br>3.2.2 能根据各类资产的特点和重要性，进行分类和归档，为不同资产采取相应的安全措施提供建议<br>3.2.3 能评估和分析不同资产的安全价值和风险，确定其在网络安全中的重要性和关联性，为资源配置和风险管理提供指导<br>3.2.4 能使用资产管理工具进行资产管理和跟踪 | 3.2.1 资产清单的编制、资产分类和归档、资产价值评估等资产管理的基本原理和方法<br>3.2.2 网络扫描、被动嗅探等技术工具等资产识别的相关技术和工具<br>3.2.3 评估资产价值的方法和指标<br>3.2.4 部门资产管理的规范、业务流程 |
| | 3.3 数据资产识别与安全管理 | 3.3.1 能识别咨询方的数据资产风险类型，判断威胁程度<br>3.3.2 能对咨询方个人信息保护政策和个人信息处理情况，进行合规评估<br>3.3.3 能根据咨询方的数据资产情况，制定数据分级分类标准指南 | 3.3.1 数据安全的管理流程和方法<br>3.3.2 敏感数据和非敏感数据的分类和处理方式<br>3.3.3 数据安全国家标准规定的分类分级要求<br>3.3.4 个人信息匿名化、去标识化的技术方法 |

| | | | |
|---|---|---|---|
| | 3.4 网络安全应急管理 | 3.4.1 能制定应急响应规程文件和应急响应演练预案<br>3.4.2 能根据应急响应规程文件协调处理网络安全事件<br>3.4.3 能根据应急响应演练预案组织咨询方的网络安全部门参加应急演练，提高应急响应能力 | 3.4.1 不同类型安全事件的应急处置策略和措施<br>3.4.2 国家网络安全事件应急预案、网络安全应急演练和培训的流程和方法<br>3.4.3 网络安全事件调查的方法和工具<br>3.4.4 威胁情报收集和分析的方法和工具的使用方法<br>3.4.5 信息系统灾难恢复和数据备份的方法、技术手段 |
| | 3.5 供应链安全管理 | 3.5.1 能识别供应链中各个环节的风险<br>3.5.2 能对供应链安全实施风险评估<br>3.5.3 能从供应链生命周期和安全风险等方面提出安全需求<br>3.5.4 能制定供应链安全管理的策略和流程，并确保合规<br>3.5.5 能制定供应商安全要求、进行供应商审查、签订合同和监督履约 | 3.5.1 国内外供应链安全政策法规、国内外供应链安全标准以及供应链安全防护的实践案例<br>3.5.2 供应链安全风险评估知识<br>3.5.3 ISO 28000、美国国家标准技术研究院（NIST）网络安全框架等国内外供应链安全标准提出的防护框架的原理、方法<br>3.5.4 仿冒伪造、供应中断、信息泄露、安全漏洞等供应链安全威胁的知识<br>3.5.5 信息技术产品供应方行为安全的检查要求 |
| 4. 网络安全风险评估 | 4.1 风险评估准备 | 4.1.1 能明确风险评估目标<br>4.1.2 能根据评估目标确定评估范围和重点领域<br>4.1.3 能制定评估方案和计划，并组织实施评估活动 | 4.1.1 网络安全风险界定的方法<br>4.1.2 网络安全风险评估计划编制方法 |
| | 4.2 风险识别 | 4.2.1 能根据收集到的数据和信息，识别出潜在的安全威胁、漏洞以及脆弱性<br>4.2.2 能通过攻防对抗、渗透测试等方法进行深度的风险识别 | 4.2.1 网络安全风险识别方法和工具<br>4.2.2 流量分析、渗透测试、入侵检测和防御等安全防护手段的原理、方法 |
| | 4.3 风险分析 | 4.3.1 能使用网络安全工具对安全风险数据建模<br>4.3.2 能对识别的风险进行测度 | 4.3.1 网络安全风险分析的方法<br>4.3.2 GB/T 27984、NIST SP 800-30、ISO/IEC 27005 等国内 |

| | | | |
|---|---|---|---|
| | | | 外风险评估和分析的方法和指南<br>4.3.3 安全脆弱性评估工具的使用方法<br>4.3.4 网络安全风险计算和确定原理 |
| | 4.4 风险评估 | 4.4.1 能够收集用于风险评估的数据和信息<br>4.4.2 能够根据确定的评估标准判定风险等级 | 4.4.1 网络安全风险评估报告的编制方法 |
| 5.培训指导 | 5.1 培训实施 | 5.1.1 能制订培训工作计划<br>5.1.2 能编制和实施培训方案<br>5.1.3 能根据培训大纲、教材编写本职业培训讲义、课件<br>5.1.4 能讲解培训网络安全管理制度和安全保护技术 | 5.1.1 培训工作计划的制订要求和方法<br>5.1.2 培训方案编制和实施的要求和方法<br>5.1.3 培训讲义、课件的编写知识<br>5.1.4 教学教法知识<br>5.1.5 培训质量管理体系要求和方法 |
| | 5.2 技术指导 | 5.2.1 能对本职业三级/高级工及以下级别人员进行技术业务指导<br>5.2.2 能对本职业三级/高级工及以下级别人员技能水平和学习效果进行考核 | 5.2.1 操作经验和技能总结的方法<br>5.2.2 技能和理论基础知识水平考核的要求和方法 |

### 3.3 一级/高级技师

| 职业功能 | 工作内容 | 技能要求 | 相关知识要求 |
|---|---|---|---|
| 1.网络安全规划咨询 | 1.1 网络安全规划需求识别和确定 | 1.1.1 能根据咨询方网络的重要程度和受到的威胁类型，确定网络安全规划的组成要素<br>1.1.2 能定性或定量描述网络安全规划的重点和优先级 | 1.1.1 网络安全组织的业务模式、工作流程和信息系统架构等方面知识<br>1.1.2 国内外网络安全防护模型的原理、方法<br>1.1.2 网络安全风险识别方法<br>1.1.3 业务流程和风险管理，项目管理方法，网络安全治理的理论和实践 |

| | | | |
|---|---|---|---|
| | 1.2 数据安全规划需求识别和确定 | 1.2.1 能根据咨询方数据的重要程度和受到的威胁类型，确定数据安全规划的组成要素<br>1.2.2 能定性或定量描述数据安全规划的重点和优先级 | 1.2.1 数据泄露、篡改、丢失等数据安全威胁的防护原理、方法<br>1.2.2 国内外重要数据保护的法律和标准要求<br>1.2.3 数据加密/解密、访问控制、身份认证、隐私计算等技术的概念、原理及其实现机制<br>1.2.4 数据备份和恢复的概念、原理、方法和技术工具 |
| | 1.3 网络安全规划制定 | 1.3.1 能够理解咨询方经营逻辑、业务流程，发掘可能存在的安全风险<br>1.3.2 能够组织、协调各部门和供应商进行有效沟通，收集制定战略规划所需的信息<br>1.3.3 能持续追踪国内外网络安全态势和技术趋势，并合理地将相关知识应用到战略规划制定<br>13.4 能编制兼具合规性、可行性与技术领先性的战略规划书 | 1.3.1 企业战略管理方法<br>1.3.2 国内外网络安全战略的内容分析方法<br>1.3.3 企业与 IT 治理知识 |
| | 1.4 数据安全规划制定 | 1.4.1 能制定和实施数据安全管理策略，包括数据安全政策和流程，数据安全保护措施，确保数据的机密性、完整性和可用性<br>1.4.2 能根据数据安全风险评估结果，建立数据安全监控和应对机制<br>1.4.3 能制定重要数据和个人信息保护策略和控制措施<br>1.4.4 能协调各部门和各个环节的工作，实施并监控数据安全规划的执行情况 | 1.4.1 数据分类、备份与恢复、销毁等数据安全管理的生命周期和过程的知识<br>1.4.2 数据安全风险评估和管理的概念、原理和基本方法，ISO31000 等数据风险评估模型和方法<br>1.4.3 重要数据安全处理和个人信息保护工程的方法<br>1.4.4 数据加密算法、访问控制机制、身份认证技术、隐私计算技术等常见数据安全技术的概念、原理及其应用方法 |
| | 1.5 网络安全建设规划指导 | 1.5.1 能形成完善的风险评估报告，提出建设策略和目标<br>1.5.2 能明确关键任务和里程碑节点，并制定验收指标<br>1.5.3 能对高级别网络安全事件进行分析和处置<br>1.5.4 能从最新的行业网络安全技术发展、威胁情报、典型网络安全事件中总结存在问题，提 | 1.5.1 网络安全风险评估方法<br>1.5.2 高级别安全威胁的分析与处置知识<br>1.5.3 对行业最新的安全技术和典型安全案例实现原理、执行过程的分析技术和知识 |

| | | | |
|---|---|---|---|
| | | 出有针对性的应对方案 | |
| | 1.6 网络安全投资规划制定 | 1.6.1 能分析和评估网络安全投资的必要性和优先级<br>1.6.2 能对网络安全威胁进行风险评估，识别和管理与之相关的风险，并提出相应的投资方案<br>1.6.3 能对网络安全投资项目做成本预算和财务分析<br>1.6.4 能制定网络安全项目的资金配置方案<br>1.6.5 能评估和选择网络安全供应商，进行合同谈判和合同管理 | 1.6.1 网络安全工程管理的基本概念和方法<br>1.6.2 供应商评估和管理的基本原理和方法<br>1.6.3 常见网络安全产品和服务的功能特点<br>1.6.4 财务分析和预算编制的基本原理和方法<br>1.6.5 招标采购和建设项目信息管理基础知识 |
| 2.网络安全设计咨询 | 2.1 网络安全设计需求识别和确定 | 2.1.1 能设计符合咨询方需求的网络安全架构<br>2.1.2 能评估和选择适合咨询方的安全技术和解决方案<br>2.1.3 能设计合理的网络拓扑和安全防护措施，保证网络安全的可靠性和稳定性 | 2.1.1 网络架构设计规范、数据业务流程、系统功能和业务需求的方法<br>2.1.2 风险矩阵、风险评估工具等常见的风险管理和评估方法<br>2.1.3 安全策略和规则的设计原理和方法，包括用户权限管理、访问控制、数据保护等方面的设计<br>2.1.4 网络架构设计的原理和方法，网络拓扑和安全防护措施合理设计<br>2.1.5 防火墙、入侵检测系统、加密技术等常见的安全产品和技术的分析、使用方法 |
| | 2.2 数据安全设计需求识别和确定 | 2.2.1 能设计符合咨询方需求的数据安全架构<br>2.2.2 能评估和选择适合咨询方的数据安全技术和解决方案 | 2.2.1 数据安全成熟度能力模型等国内外数据安全保护体系的理论、方法<br>2.2.2 主要的数据安全产品、方案的功能和技术能力分析方法<br>2.2.3 国内外数据安全保护的实践案例 |

| | | | |
|---|---|---|---|
| | 2.3 网络安全架构设计 | 2.3.1 能设计网络安全架构，包括需求分析、风险评估和控制措施等<br>2.3.2 能协调咨询方内部的技术团队、安全团队以及供应商进行协作和沟通，确保网络安全架构的成功实施和运维<br>2.3.3 能分析网络安全架构的漏洞和弱点，提出相应的改进方案<br>2.3.4 能分析已有安全架构，进行全面审查和发现潜在的安全风险，并提供优化建议和改进方案 | 2.3.1 制定和实施网络安全规则和政策的原则和方法，包括访问控制、实时监控、数据保护等方面的知识<br>2.3.2 咨询方的业务流程和需求，各个业务环节的风险点和安全需求的知识<br>2.3.3 信息系统和网络设备的安全原理和技术，包括防火墙、入侵检测系统、VPN 等安全设备和技术<br>2.3.4 网络安全设备的风险评估技巧，网络安全架构设计优化技巧 |
| | 2.4 网络安全策略设计 | 2.4.1 能制定适应咨询方环境和需求的网络安全策略<br>2.4.2 能根据咨询方需求设计适合的安全控制措施 | 2.4.1 网络安全策略设计的方法和技术，包括网络攻击与防护方法、身份认证、访问控制等方面的知识<br>2.4.2 ISO 27001、NIST 等提出的国内外网络安全防护的框架方法<br>2.4.3 咨询方的业务流程、需求及能力<br>2.4.4 云安全、物联网安全、工控系统安全等网络安全领域的新兴技术和趋势 |
| 3. 网络安全管理体系咨询 | 3.1 网络安全管理制度机制建设 | 3.1.1 能根据咨询方网络安全调查情况，撰写网络安全管理制度建议报告<br>3.1.2 能根据国家法律法规，结合咨询方业务情况，建设网络安全管理原则和制度<br>3.1.3 能整理并分析网络安全管理制度的优化建议，并组织开展应用试点工作，撰写试点成果报告 | 3.1.1 网络安全管理的基本原理和方法，网络安全管理体系的组成部分和要求<br>3.1.2 网络安全法、ISO 27001 等对网络安全管理的规定和要求<br>3.1.3 国内外网络安全管理的理论模型和实践案例 |
| | 3.2 网络资产管理 | 3.2.1 能根据各类资产的特点和重要性，进行分类和归档，为不同资产采取相应的安全措施提供建议<br>3.2.2 能评估和分析不同资产的安全价值和风险，确定其在网络安全中的重要性和关联性，为资源配置和风险管理提供指导 | 3.2.1 资产清单的编制、资产分类和归档、资产价值评估等资产管理的基本原理和方法<br>3.2.2 网络扫描、被动嗅探等资产识别的相关技术和工具的使用方法<br>3.2.3 评估资产价值的方法和指标 |

| | | | |
|---|---|---|---|
| | | 3.2.3 能使用各类资产管理工具进行资产管理和跟踪<br>3.2.4 能制定网络资产管理策略 | 3.2.4 数据分类和归档的原理和方法<br>3.2.5 部门资产管理的规范、业务流程 |
| | 3.3 数据资产识别与安全管理 | 3.3.1 能对咨询方的数据资产风险进行分析，提出优化改进建议<br>3.3.2 能根据个人信息合规评估情况，分析隐私政策风险，个人信息隐私政策改进<br>3.3.3. 能根据分类分级指南，对咨询方数据资产的重要数据和个人敏感信息进行识别<br>3.3.4 能在各类业务场景下，对咨询方的数据处理行为进行风险评估 | 3.3.1 数据资产风险分析方法<br>3.3.2 隐私政策编制的合规性要求<br>3.3.3 重要数据和个人敏感信息的识别、影响评估方法<br>3.3.4 数据安全监控与审计的技术知识<br>3.3.5 数据安全备份及恢复的技术知识 |
| | 3.4 网络安全应急管理 | 3.4.1 能溯源、追踪网络安全事件的起因和影响范围，并提供相应的解决方案<br>3.4.2 能处理网络安全事件并控制其扩散的能力，包括切断恶意攻击源、修复受影响系统等<br>3.4.3 能够设计和组织大规模的应急演练活动<br>3.4.4 能快速恢复受攻击的系统和网络服务的正常运行，最小化损失<br>3.4.5 组织和实施红队攻防演练，发现和修复系统和人员的安全弱点 | 3.4.1 高级的安全攻击技术和防御策略、网络安全威胁情报来源和分类的知识<br>3.4.2 恶意软件检测、溯源取证的技术知识<br>3.4.3 降低网络安全事件影响的流程和步骤<br>3.4.4 网络安全应急响应和处置演练操作流程<br>3.4.5 信息系统灾难恢复和数据备份的方法、技术手段<br>3.4.6 红蓝对抗和网络安全靶场实用技术知识 |
| | 3.5 供应链安全管理 | 3.5.1 能制定和设计供应链安全管理体系<br>3.5.2 能指导咨询方根据供应商的安全能力和合规性选择合适的供应商，并与供应商建立有效的合作关系<br>3.5.3 能针对 ICT 供应链生命周期中各环节安全风险做出风险提示，并提出风险防范和控制建议 | 3.5.1 供应链风险评估、风险管理的知识<br>3.5.2 供应链安全风险评估指标体系和供应商安全能力评估的知识<br>3.5.3 国内外供应链安全防护的实践案例<br>3.5.4 供应链监测及审计的知识<br>3.5.5 供应链安全事件应急 |

| | | | |
|---|---|---|---|
| | | 3.5.4 能审计和监控供应链安全，发现供应链中的安全漏洞和问题，并及时进行纠正和处理<br>3.5.5 能迅速响应供应链安全事件和危机，并采取相应措施定位和解决问题 | 管理的知识 |
| 4.网络安全风险评估 | 4.1 风险评估准备 | 4.1.1 能建立网络安全风险评估流程策略和制度规范<br>4.1.2 能使用网络靶场搭建全面、持续的风险评估所需的仿真环境<br>4.1.3 能持续优化风险评估管理机制 | 4.1.1 网络安全风险评估的方法、流程要求<br>4.1.2 网络安全靶场使用的方法<br>4.1.3 网络安全风险管理的方法 |
| | 4.2 风险识别 | 4.2.1 能识别和辨别咨询方网络、系统和应用潜在的安全风险<br>4.2.2 能对已有安全控制措施的有效性进行分析并提出系统性改进措施 | 4.2.1 风险识别的工作流程<br>4.2.2 风险识别的方法 |
| | 4.3 风险分析 | 4.3.1 能对网络安全风险进行全面分析判断<br>4.3.2 能分析业务需求和系统运作方式，并根据风险分析结果提出业务优化或调整建议 | 4.3.1 风险矩阵法、定性和定量风险分析等风险分析方法<br>4.3.2 风险评估、风险控制和风险监控的流程和技术的使用方法<br>4.3.3 相关行业的业务流程和系统结构的知识<br>4.3.4 高级风险分析、决策支持协议的知识，以及对风险事件的频率和影响进行量化的方法 |
| | 4.4 风险评估 | 4.4.1 能够使用可视化工具量化风险评估结果<br>4.4.2 能够清晰地展示或解释风险评估结果，编制风险评估报告 | 4.4.1 网络安全风险评价基本概念和方法<br>4.4.2 数据统计分析的基本方法和工具使用知识<br>4.4.3 网络安全风险评估结果的展示化方法 |
| | 4.5 风险控制 | 4.5.1 能根据评估结果制定或调整风险控制策略和措施<br>4.5.2 能组织开展风险评估效果的持续性监控评价 | 4.5.1 风险控制策略和方法<br>4.5.2 风险评估监控工具的使用知识 |

| | | | |
|---|---|---|---|
| 5. 培训指导 | 5.1 培训实施 | 5.1.1 能对培训需求进行分析<br>5.1.2 能编制培训规划<br>5.1.3 能组织编写本职业培训教材<br>5.1.4 能进行本职业培训宣讲 | 5.1.1 培训需求分析要求、方法<br>5.1.2 培训规划编制要求<br>5.1.3 培训教材的编写知识<br>5.1.4 培训预算与决算审核方法 |
| | 5.2 技术指导 | 5.2.1 能对本职业三级/高级工及以下级别人员进行技术业务指导<br>5.2.2 能对本职业三级/高级工及以下级别人员技能水平和学习的效果进行考核<br>5.2.3 能组织开展咨询工具、咨询方法的改进创新活动 | 5.2.1 指导技能操作知识<br>5.2.2 案例分析与教学方法<br>5.2.3 技术改造与革新方法 |

## 4 权重表

### 4.1 理论知识权重表

| 项目 \ 技能等级 | | 三级（%） | 二级（%） | 一级（%） |
|---|---|---|---|---|
| 基本要求 | 职业道德 | 5 | 5 | 5 |
| | 基础知识 | 15 | 10 | 5 |
| 相关知识要求 | 网络安全规划咨询 | 30 | 25 | 20 |
| | 网络安全设计咨询 | 15 | 20 | 15 |
| | 网络安全管理体系咨询 | 20 | 15 | 20 |
| | 网络安全风险评估 | 15 | 15 | 20 |
| | 培训指导 | - | 10 | 15 |
| 合计 | | 100 | 100 | 100 |

### 4.2 技能要求权重表

| 项目 \ 技能等级 | 三级（%） | 二级（%） | 一级（%） |
|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| 专业能力要求 | 网络安全规划咨询 | 40 | 30 | 20 |
| | 网络安全设计咨询 | 15 | 20 | 20 |
| | 网络安全管理体系咨询 | 25 | 20 | 25 |
| | 网络安全风险评估 | 20 | 15 | 20 |
| | 培训指导 | - | 15 | 15 |
| 合计 | | 100 | 100 | 100 |

# 5 职业标准附录

## 5.1 参考文献


[ 1 ] GB/T 20984-2-2022《信息安全技术 信息安全风险评估方法》

[ 2 ] GB/T 28450-2020《信息技术 安全技术 信息安全管理体系审核指南》

[ 3 ] GB/T 29246-2017《信息技术 安全技术 信息安全管理体系 概述和词汇》

[ 4 ] GB/T 30271-2013《信息安全技术 信息安全服务能力评估准则》

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

[ 6 ] GB/T 31496-2015《信息技术 安全技术 信息安全管理体系实施指南》

[ 7 ] GB/T 37961-2019《信息技术服务 服务基本要求》

[ 8 ] GB/T 42446-2023《信息安全技术 网络安全从业人员能力基本要求》