ICS 35.020
CCS L70

DB21

辽 宁 省 地 方 标 准

DB21/T1793.7—XXXX

人才评价网络安全技能技术要求

Talent evaluation—Technical requirements for network security skills

（征求意见稿）

本草案完成时间：2023-01-18

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

辽宁省市场监督管理局　　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。

本文件是DB21/1793《信息技术职业技能规范》的第7部分。DB21/T 1793已经发布了以下部分：

——信息技术职业技能规范第1部分：要求

——信息技术职业技能规范第3部分：软件开发

——信息技术职业技能规范第4部分：系统集成

本文件由辽宁省工业和信息化厅提出并归口。

本文件起草单位：辽宁省先进装备制造业基地建设工程中心、辽宁职业学院、国网辽宁省电力有限公司电力科学研究院、国网辽宁省电力有限公司信息通信分公司、辽宁省大数据管理中心、大连软信咨询服务有限公司。

本文件主要起草人：姜胜海、张雪、任帅、陈剑、李博文、滕子贻、李洪涛、尹宏、刘宏。

本文件发布实施后，任何单位和个人如有问题和意见建议，均可以通过来电和来函等方式进行反馈，我们将及时答复并认真处理，根据实际情况依法进行评估及复审。

本文件归口单位通讯地址：沈阳市北陵大街45-2号，联系电话：024-86913384

本文件起草单位通讯地址：沈阳市和平区太原北街2号综合楼A座10层024-88785218

人才评价网络安全技能技术要求

1 范围

本文件规定了网络安全服务从业人员的职业分类和职业等级、各职业等级技能技术要求以及从业人员的基本条件和能力评价准则等内容。

本文件适用于网络安全服务相关的政府、企事业单位、科研院所以及相关组织机构等。

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（包括所有的修订单）适用于本文件。

GB/T25069-2022 信息安全技术术语

GB/T30283-2022 信息安全技术网络安全服务分类与代码

GB/T37696-2019 信息技术服务从业人员能力评价要求

DB21/T 1793 信息技术职业技能规范

3 术语和定义

GB/T25069、GB/T30283、GB/T 37696、DB21/T 1793系列界定的以及下列术语和定义适用于本文件。

3.1

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。

3.2

网络安全服务 network security service

面向组织或个人的各类网络安全需求和网络安全保障需求，由服务提供方按照服务协议所执行的网络安全过程或任务。

注1：网络安全服务通常是基于网络安全技术、产品或管理体系，通过外包的形式，由专业网络安全人员所提供的支持和帮助。

注2：网络安全服务通常以网络安全服务提供方和网络安全服务需求方之间的服务项目方式进行。

3.3

网络渗透测试 network penetration testing

以未经授权的动作绕过某一系统的安全机制来检查网络中信息系统、网络设备等的安全功能，以发现网络中安全问题的手段和安全评估方法。

4 缩略语

下列缩略语适用于本文件。

K：知识(Knowledge)

S：技能(Skill)

E：经验(Experience)

5 网络安全服务从业人员职业分类和等级

5.1 职业分类

网络安全服务职业基于网络安全技术服务行业的业务形态、网络技术发展和应用的规律进行分类，按照GB/T37696-2019和GB/T30283-2022，网络安全服务职业分类划分见表1。

表 1 网络安全服务职业分类

职业种类	职业分类
网络安全服务	网络安全咨询与监理
	网络安全设计与开发
	网络安全测试
	网络安全集成
	网络安全运维
	数据存储与保护
	网络安全审计
	网络安全培训

5.2 职业等级

本文件依据GB/T37696-2019中的职业等级要求和GB/T30283-2022，在职业分类的基础上，将网络安全职业等级划分为六个等级，见表2。

表 2 网络安全职业等级

等级	网络安全咨询与监理	网络安全设计与开发	网络安全测试	网络安全集成	网络安全运维	数据存储与保护	网络安全审计	网络安全培训
6级	资深网络安全咨询与监理师	-	-	-		-	-	-
5级	高级网络安全咨询与监理师	资深网络安全开发实施工程师	资深网络安全测试工程师	资深网络安全集成工程师	资深网络安全运维工程师	资深数据存储与保护工程师	资深网络安全审计工程师	资深网络安全培训师
4级	网络安全咨询与监	高级网络安全开发实施	高级网络安全测试工程	高级网络安全集成工程	高级网络安全运维工程	高级数据存储与保护工	高级网络安全审计工程	高级网络安全培训师

	理师	工程师	师	师	师	程师	师	
3 级	初级网络安全咨询与监理师	网络安全开发实施工程师	网络安全测试工程师	网络安全集成工程师	网络安全运维工程师	数据存储与保护工程师	网络安全审计工程师	网络安全培训师
2 级	- -	初级网络安全开发实施工程师	初级网络安全测试工程师	初级网络安全集成工程师	初级网络安全运维工程师	初级数据存储与保护工程师	初级网络安全审计工程师	初级网络安全培训师
1 级	- -	助理网络安全开发实施工程师	助理网络安全测试工程师	助理网络安全集成工程师	助理网络安全运维工程师	助理数据存储与保护工程师	助理网络安全审计工程师	-

5.3 职业能力要素等级要求

本文件依据GB/T 37696-2019中从业人员能力模型，按知识、技能和经验三个维度提出了网络安全职业能力人才评价要素。

本文件对应职业等级，按知识要素等级、技能要素等级和经验要素等级三个维度提出了网络安全从业人员职业能力人才评价要素等级体系。

5.3.1 知识要素等级

知识要素包括基础知识、专业知识、相关知识。

a) 基础知识：计算机硬件基础知识、计算机软件基础知识、数据传输与通信基础知识、计算机网络基础知识、项目管理基础知识、网络安全知识、质量管理知识。

b) 专业知识：网络攻防知识、恶意代码防护知识；数据安全及灾备知识、大数据安全知识；应用安全知识、移动应用安全知识；网络安全审计知识、网络安全测试技术；区块链安全知识、供应链安全知识；网络攻击溯源知识、网络安全流量知识等专业知识。

c) 相关知识：营销、策划基础知识、知识产权知识、劳动法知识、国家信息技术服务相关法律、法规。

知识要素等级说明参见附录A、附录B和附录C。

5.3.2 技能要素等级

技能要素包括基本技能、专业技能、软技能。

a) 基本技能：计算机硬件基础应用能力、计算机软件基础应用能力、计算机网络基础应用能力、技术文档撰写能力、外语应用能力。

b) 专业技能：网络安全测试、网络安全风险评估；网络安全加固、应急响应；区块链安全技能、供应链安全测试能力；网络安全规划设计、工程项目管理；云平台安全技术、大数据安全技术；安全管理体系建设、网络安全评估分析；移动应用安全技能、移动终端测试能力等专业技能。

c) 软技能：沟通能力、学习能力、问题判断与解决能力、创新能力、知识分享能力。

技能要素等级说明参见附录D、附录E和附录F。

5.3.3 经验要素等级

经验要素等级要求见各职业分类的职级对应的经验项。

6 网络安全咨询与监理

6.1 职责要求

具有相关资质的监理单位受网络安全工程建设单位的委托，依据国家批准的信息化工程项目建设文件、有关工程建设的网络安全的法律法规和工程建设监理合同，在工程建设各个阶段向建设单位提供网络安全咨询。面向组织或个人，通过知识传递、工作辅导和系统规划等方法提出解决网络安全问题的建议和方案。

6.2 职业等级

网络安全咨询与监理分4个等级，即：职级6级（资深网络安全咨询与监理师）、职级5级（高级网络安全咨询与监理师）、职级4级（网络安全咨询与监理师）和职级3级（初级网络安全咨询与监理师）。

6.3 基本条件

申请各职业等级的人员，符合以下条件之一，即可满足申请基本条件。见表3。

表 3 网络安全咨询与监理基本条件

职业等级	基本条件
6 级	1. 取得网络安全咨询与监理从业能力等级 5 级 2 年，且近 3 年连续从事本专业； 2. 取得网络安全咨询与监理或相关专业博士学位，且近 3 年连续从事本专业； 3. 取得国家计算机技术与软件专业技术资格（水平）考试相关高级资格，且近 4 年连续从事本专业。
5 级	1. 取得网络安全咨询与监理从业能力等级 4 级 2 年，且近 3 年连续从事本专业； 2. 取得网络安全咨询与监理或相关专业博士学位，且近 1 年连续从事本专业； 3. 取得网络安全咨询与监理或相关专业硕士学位，且近 3 年连续从业本专业； 4. 取得国家计算机技术与软件专业技术资格（水平）考试相关高级资格，且近 2 年连续从事本专业。
4 级	1. 取得网络安全咨询与监理从业能力等级 3 级 2 年，且近 2 年连续从事本专业； 2. 取得网络安全咨询与监理或相关专业硕士学位，且近 1 年连续从业本专业； 3. 取得网络安全咨询与监理或相关专业学士学位，且近 2 年连续从事本专业； 4. 取得国家计算机技术与软件专业技术资格（水平）考试相关中级资格，且近 2 年连续从事本专业； 5. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 10 个以上（包含 10 个）。
3 级	1. 取得网络安全咨询与监理或相关专业硕士学位及以上； 2. 取得网络安全咨询与监理或相关专业学士学位，且近 1 年连续从事本专业； 3. 取得国家计算机技术与软件专业技术资格（水平）考试相关中级资格； 4. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 5 个以上；（包含 5 个） 5. 取得网络安全方向省级一类竞赛第 1 名。

6.4 能力评价准则

6.4.1 知识

网络安全咨询与监理的知识评价规则见表4。

表 4　网络安全咨询与监理各等级知识评价规则

能力要素	能力项		网络安全咨询与监理			
			资深网络安全咨询与监理师（6 级）	高级网络安全咨询与监理师（5 级）	网络安全咨询与监理师（4 级）	初级网络安全咨询与监理师（3 级）
基础知识	GK01	计算机硬件基础知识	K2	K2	K2	K2
	GK02	计算机软件基础知识	K2	K2	K2	K2
	GK03	数据传输与通信基础知识	K2	K2	K2	K2
	GK04	计算机网络基础知识	K2	K2	K2	K2
	GK05	项目管理基础知识	K3	K2	K2	K2
	GK06	网络安全知识	K2	K2	K2	K2
	GK07	质量管理知识	K3	K2	K2	K2
专业知识	D-PK01	应用安全知识	K4	K3	K2	K1
	D-PK02	网络攻防知识	K4	K3	K2	K1
	D-PK03	恶意代码防护知识	K4	K3	K1	K1
	D-PK04	数据安全及灾备知识	K3	K3	K2	K1
	D-PK05	基础软件系统安全知识	K4	K2	K1	K1
	D-PK06	物理环境安全知识	K3	K3	K1	K1
	D-PK07	密码学知识	K4	K3	K2	K1
	D-PK08	网络安全审计知识	K3	K2	K1	—
	D-PK09	网络安全测试技术	K2	K1	K1	—
	D-PK10	安全管理体系	K3	K2	K1	K1
	D-PK11	云平台安全知识	K3	**K2**	**K1**	**K1**
	D-PK12	大数据安全知识	K3	**K2**	**K1**	**K1**
	D-PK13	物联网安全知识	K3	K2	**K1**	**K1**
	D-PK14	工业控制系统安全知识	K3	K2	**K1**	**K1**
	D-PK15	移动应用安全知识	K3	K2	K1	K1
	D-PK16	区块链安全知识	K3	K2	K1	K1
	D-PK17	终端安全知识	K4	K2	K1	K1
	D-PK18	网络攻击溯源知识	—	—	—	—
	D-PK19	网络安全流量知识	K2	K2	K1	K1

表 4　网络安全咨询与监理各等级知识评价规则（续）

相关知识	RK01	营销、策划基础知识	K2	K2	K1	K1
	RK02	知识产权知识	K1	K1	K1	K1
	RK03	劳动法知识	K1	K1	K1	K1
	RK04	国家信息技术服务相关法律、法规	K1	K1	K1	K1

6.4.2　技能

网络安全咨询与监理的技能评价规则见表5。

表 5　网络安全咨询与监理的技能评价规则

能力要素	能力项		网络安全咨询			
			资深网络安全咨询与监理师（6 级）	高级网络安全咨询与监理师（5 级）	网络安全咨询与监理师（4 级）	初级网络安全咨询与监理师（3 级）
基本技能	BS01	计算机硬件基础应用能力	S2	S2	S2	S2
	BS02	计算机软件基础应用能力	S2	S2	S2	S2
	BS03	计算机网络基础应用能力	S2	S2	S2	S2
	BS04	文档撰写能力	S4	S4	S3	S2
	BS05	外语应用能力	S2	S2	S2	S1
专业技能	D-PS01	网络安全测试	S2	S2	S1	—
	D-PS02	网络安全风险评估	S4	S4	S3	S1
	D-PS03	需求分析	S3	S2	S1	—
	D-PS04	网络安全规划设计	S3	S2	S1	—
	D-PS05	安全管理体系建设	S3	S2	S1	S1
	D-PS06	系统建模及架构设计能力	S3	S2	S1	—
	D-PS07	网络安全评估分析	S4	S3	S2	S1
	D-PS08	网络安全加固	S2	S1	—	—
	D-PS09	工程项目管理	S2	S1	—	—
	D-PS10	网络渗透测试	S4	S3	S2	—
	D-PS11	网络安全态势分析	S3	S2	S1	—
	D-PS12	应急响应	S3	S2	—	—
	D-PS13	渗透工具的使用及研发	S4	S3	S2	—

表 5 网络安全咨询与监理的技能评价规则（续）

	D-PS14	网络安全审计	S4	S3	S2	—
	D-PS15	信息系统工程监理	—	—	—	—
	D-PS16	安全产品设计	—	—	—	—
	D-PS17	云平台安全技术	S4	S3	S2	S1
	D-PS18	大数据安全技术	S4	S3	S2	S1
	D-PS19	物联网安全	S4	S3	S2	S1
	D-PS20	工业控制系统安全	S4	S3	S2	S1
	D-PS21	移动应用架构设计能力	S3	S2	S1	—
	D-PS22	移动应用安全技能	S3	S2	S1	—
	D-PS23	区块链安全技能	S2	S1	—	—
	D-PS24	网络安全数据处理	S4	S3	S2	S1
	D-PS25	供应链安全测试能力	S3	S2	S1	S1
	D-PS26	移动终端测试能力	S3	S2	S1	S1
	D-PS27	网络攻击溯源能力	—	—	—	—
	D-PS28	网络安全流量分析能力	S3	S2	S1	S1
软技能	SS01	沟通能力	S4	S3	S2	S1
	SS02	学习能力	S3	S3	S3	S2
	SS03	问题判断与解决能力	S4	S3	S3	S2
	SS04	创新能力	S2	S2	S1	S1
	SS05	知识分享能力	S3	S3	S2	S1

6.4.3 经验

网络安全咨询与监理的经验评价规则，满足下列条件之一即可，见表6。

表 6 网络安全咨询与监理的经验评价规则

经验	职位及经验等级			
	资深网络安全咨询与监理师（6 级）E4	高级网络安全咨询与监理师（5 级）E3	网络安全咨询与监理师（4 级）E2	初级网络安全咨询与监理师（3 级）E2
工作年限	1.网络安全咨询与监理及相关专业连续从业 9 年，且近 3 年连续从事本专业；	1.网络安全咨询与监理及相关专业连续从业 7 年，且近 3 年连续从事本专业；	1.网络安全咨询与监理及相关专业连续从业 5 年，且近 2 年连续从事本专业；	1.网络安全咨询与监理或相关专业连续从业 3 年，且近 1 年连续从事本专业；

表 6 网络安全咨询与监理的经验评价规则（续）

工作年限	2.取得网络安全咨询与监理从业能力等级5级2年，且近3年连续从事本专业； 3.取得网络安全咨询与监理的相关专业博士学位，且近3年连续从事本专业。	2.取得网络安全咨询与监理从业能力等级4级2年，且近3年连续从事本专业； 3.取得网络安全咨询与监理的相关专业博士学位，且近1年连续从事本专业； 4.取得网络安全咨询与监理或相关专业硕士学位，且近3年连续从业本专业。	2.取得网络安全咨询与监理从业能力等级3级2年，且近2年连续从事本专业； 3.取得网络安全咨询与监理的相关专业硕士学位，且近1年连续从业本专业； 4.取得网络安全咨询与监理或相关专业学士学位，且近2年连续从事本专业。	2.取得网络安全咨询与监理或相关专业硕士学位及以上； 3.取得网络安全咨询与监理的相关专业学士学位，且近1年连续从事本专业。
工作履历	1.近5年，作为前5名参加国家、省、市或大型组织网络安全项目300万人民币及以上4个的咨询设计或监理； 2.近5年，参加地市级网络安全项目200万人民币及以上8个的咨询设计或监理。	1.近5年，作为前5名参加国家、省、市或大型组织网络安全项目200万人民币及以上2个的咨询设计或监理； 2.近5年，参加地市级网络安全项目100万人民币及以上5个的咨询设计或监理。	1.近5年，参加网络安全项目100万人民币及以上5个的咨询设计或监理。	1.近3年，参加网络安全项目3个的咨询设计或监理及相关工作。
工作传承	1.近3年，在国家2级以上刊物发表本专业或相关专业文章4篇； 2.近5年参加的200万人民币及以上网络安全项目，独立编写3个项目的咨询设计或监理技术文档； 3.近1年，本专业或相关专业的年授课20人天。备注：培养新人考核合格1人，当年计授课10人天。	1.近3年，在国家2级以上刊物发表本专业或相关专业文章2篇； 2.近5年参加的100万人民币及以上网络安全项目，独立编写2个项目的咨询设计或监理技术文档； 3.近1年，本专业或相关专业的年授课15人天。备注：培养新人考核合格1人，当年计授课10人天。	1.近3年，在省市以上刊物发表本专业或相关专业文章2篇； 2.近5年参加的100万网络安全项目，独立编写1个项目的咨询设计或监理技术文档； 3.近1年，本专业或相关专业的年授课10人天。备注：培养新人考核合格1人，当年计授课10人天。	1.近3年，在省市以上刊物发表本专业或相关专业文章1篇； 2.近3年参加的网络安全项目，参加编写1个项目的咨询设计或监理技术文档。

7 网络安全设计与开发

7.1 职责要示

网络安全设计与开发主要针对需方不能通过采购现有网络安全系统或产品予以满足的安全需求，由供方通过需求分析创建网络安全系统设计方案，在此基础上，按照安全要求、安全基线要求、设计要求、安全策略制定、威胁建模、安全编码规范设计、事件响应计划制定、安全评价等信息系统开发流程设计、开发网络安全系统或产品，并可按照GB/T38674-2020提出的应用软件安全编程通用框架的要求，采取相应的措施保障网络安全系统或产品的安全性，以满足需方特定的安全需求并最大程度地减少网络安全系统或产品的安全缺陷。网络安全设计与开发也可以基于已有的网络安全系统或产品进行二次开发。

7.2 职业等级

网络安全设计与开发分5个等级，即：职级5级（资深网络安全设计与开发工程师）、职级4级（高级网络安全设计与开发工程师）、和职级3级（网络安全设计与开发工程师）、职级2级（初级网络安全设计与开发工程师）、职级1级（助理网络安全设计与开发工程师）。

7.3 基本条件

申请各职业等级的人员，符合以下条件之一，即可满足申请基本条件。见表7。

表 7 网络安全设计与开发的基本条件

职业等级	基本条件
5 级	1. 取得网络安全设计与开发从业能力等级 4 级 2 年，且近 3 年连续从事本专业； 2. 取得网络安全设计与开发或相关专业博士学位，且近 1 年连续从事本专业； 3. 取得网络安全设计与开发或相关专业硕士学位，且近 3 年连续从业本专业； 4. 取得国家计算机技术与软件专业技术资格（水平）考试相关高级资格，且近 2 年连续从事本专业。
4 级	1. 取得网络安全设计与开发从业能力等级 3 级 2 年，且近 2 年连续从事本专业； 2. 取得网络安全设计与开发或相关专业硕士学位，且近 1 年连续从业本专业； 3. 取得网络安全设计与开发或相关专业学士学位，且近 2 年连续从事本专业； 4. 取得国家计算机技术与软件专业技术资格（水平）考试相关中级资格，且近 2 年连续从事本专业； 5. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 10 个以上（包含 10 个）。
3 级	1. 取得网络安全设计与开发或相关专业硕士学位及以上； 2. 取得网络安全设计与开发或相关专业学士学位，且近 1 年连续从事本专业； 3. 取得国家计算机技术与软件专业技术资格（水平）考试相关中级资格； 4. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 5 个以上（包含 5 个）； 5. 取得网络安全方向省级一类竞赛第 1 名。
2 级	1. 网络安全设计与开发及相关专业连续从业 2 年； 2. 取得网络安全设计与开发或相关专业学士学位及以上； 3. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 1 个以上（包含 1 个）； 4. 取得网络安全方向省级一类竞赛第 2-3 名。
1 级	1. 网络安全设计与开发及相关专业连续从业 1 年； 2. 取得网络安全设计与开发或相关专业大专及以上； 3. 取得网络安全方向省级一类竞赛第 4-5 名。

7.4 能力评价准则

7.4.1 知识

网络安全设计与开发的知识评价规则见表8。

表 8　网络安全设计与开发的知识评价规则

能力要素	能力项		网络安全设计与开发				
			资深网络安全设计与开发工程师（5级）	高级网络安全设计与开发工程师（4级）	网络安全设计与开发工程师（3级）	初级网络安全设计与开发工程师（2级）	助理网络安全设计与开发工程师（1级）
基础知识	GK01	计算机硬件基础知识	K2	K2	K2	K1	K1
	GK02	计算机软件基础知识	K2	K2	K2	K1	K1
	GK03	数据传输与通信基础知识	K2	K2	K2	K1	K1
	GK04	计算机网络基础知识	K2	K2	K2	K1	K1
	GK05	项目管理基础知识	K2	K2	K2	K1	—
	GK06	网络安全知识	K2	K2	K2	K1	—
	GK07	质量管理知识	K2	K2	K2	K1	—
专业知识	D-PK01	应用安全知识	K4	K3	K3	K2	K1
	D-PK02	网络攻防知识	K4	K3	K3	K2	K1
	D-PK03	恶意代码防护知识	K4	K3	K3	K2	K1
	D-PK04	数据安全及灾备知识	K3	K2	K2	K1	K1
	D-PK05	基础软件系统安全知识	K3	K2	K2	K1	K1
	D-PK06	物理环境安全知识	K4	K3	K3	K2	K1
	D-PK07	密码学知识	K1	K1	K1	—	—
	D-PK08	网络安全审计知识	K3	K2	K1	—	—
	D-PK09	网络安全测试技术	K3	K2	K2	K1	K1
	D-PK10	安全管理体系	K4	K3	K2	K2	K1
	D-PK11	云平台安全知识	K3	K3	K1	K1	—
	D-PK12	大数据安全知识	K3	K2	K1	K1	—
	D-PK13	物联网安全知识	K3	K2	K1	K1	—
	D-PK14	工业控制系统安全知识	K3	K2	K1	K1	—
	D-PK15	移动应用安全知识	K4	K3	K2	K1	—
	D-PK16	区块链安全知识	K3	K2	K1	—	—
	D-PK17	终端安全知识	K4	K3	K2	K1	—
	D-PK18	网络攻击溯源知识	K3	K2	K1	—	—
	D-PK19	网络安全流量知识	K3	K2	K1	—	—

表 8 网络安全设计与开发的知识评价规则（续）

相关知识	RK01	营销、策划基础知识	—	—	—	—	—
	RK02	知识产权知识	K1	K1	K1	K1	K1
	RK03	劳动法知识	K1	K1	K1	K1	K1
	RK04	国家信息技术服务相关法律、法规	K1	K1	K1	K1	K1

7.4.2 技能

网络安全设计与开发的技能评价规则见表9。

表 9 网络安全设计与开发的知识评价规则

能力要素	能力项		网络安全设计与开发				
			资深网络安全设计与开发工程师（5 级）	高级网络安全设计与开发工程师（4 级）	网络安全设计与开发工程师（3 级）	初级网络安全设计与开发工程师（2 级）	助理网络安全设计与开发工程师（1 级）
基础技能	BS01	计算机硬件基础应用能力	S2	S2	S2	S1	S1
	BS02	计算机软件基础应用能力	S2	S2	S2	S1	S1
	BS03	计算机网络基础应用能力	S2	S2	S2	S1	S1
	BS04	文档撰写能力	S4	S3	S2	S1	S1
	BS05	外语应用能力	S2	S2	S1	S1	S1
专业技能	D-PS01	网络安全测试	S3	S2	S2	S1	S1
	D-PS02	网络安全风险评估	S3	S2	S2	S1	S1
	D-PS03	需求分析	S4	S3	S2	S1	—
	D-PS04	网络安全规划设计	S2	S1	S1	S1	—
	D-PS05	安全管理体系建设	S3	S2	S1	S1	—
	D-PS06	系统建模及架构设计能力	S4	S3	S2	S1	S1
	D-PS07	网络安全评估分析	S4	S3	S2	S1	—
	D-PS08	网络安全加固	S4	S3	S2	S1	S1
	D-PS09	工程项目管理	—	—	—	—	—
	D-PS10	网络渗透测试	S3	S2	S2	S1	—
	D-PS11	网络安全态势分析	S2	S1	S1	—	—
	D-PS12	应急响应	S2	S1	S1	—	—
	D-PS13	渗透工具的使用和研发	S1	S1	—	—	—

表 9 网络安全设计与开发的知识评价规则（续）

专业技能	D-PS14	网络安全审计	S3	S2	S1	S1	—
	D-PS15	信息系统工程监理	S2	S1	—	—	—
	D-PS16	安全产品设计	S3	S2	S1	S1	—
	D-PS17	云平台安全技术	S3	S2	S1	S1	—
	D-PS18	大数据安全技术	S3	S2	S1	S1	—
	D-PS19	物联网安全	S3	S2	S1	S1	—
	D-PS20	工业控制系统安全	S3	S2	S1	S1	—
	D-PS21	移动应用架构设计能力	S4	S3	S2	S1	—
	D-PS22	移动应用安全技能	S4	S3	S2	S1	—
	D-PS23	区块链安全技能	S3	S2	S1	—	—
	D-PS24	网络安全数据处理	S4	S3	S2	S1	S1
	D-PS25	供应链安全测试能力	S2	S1	—	—	—
	D-PS26	移动终端测试能力	S4	S3	S2	S1	S1
	D-PS27	网络攻击溯源能力	—	—	—	—	—
	D-PS28	网络安全流量分析能力	S2	S1	—	—	—
软技能	SS01	沟通能力	S3	S2	S1	S1	S1
	SS02	学习能力	S3	S3	S2	S2	S1
	SS03	问题判断与解决能力	S3	S3	S2	S1	S1
	SS04	创新能力	S2	S1	S1	—	—
	SS05	知识分享能力	S3	S2	S1	—	—

7.4.3 经验

网络安全设计与开发的经验评价规则，满足下列条件之一即可，见表10。

表 10 网络安全设计与开发的经验评价规则

经验	职位及经验等级				
	资深网络安全设计与开发工程师（5 级）E3	高级网络安全设计与开发工程师（4 级）E2	网络安全设计与开发工程师（3 级）E2	初级网络安全设计与开发工程师（2 级）E1	助理网络安全设计与开发工程师（1 级）E1
工作年限	1.网络安全设计与开发及相关专业连续从业 7 年，且近 3 年连续从事本专业；	1.网络安全设计与开发及相关专业连续从业 5 年，且近 2 年连续从事本专业；	1.网络安全设计与开发或相关专业连续从业 3 年，且近 1 年连续从事本专业；	1.网络安全设计与开发及相关专业连续从业 2 年。	1.网络安全设计与开发及相关专业连续从业 1 年。

表 10 网络安全设计与开发的经验评价规则（续）

工作年限	2.取得网络安全设计与开发从业能力等级 4 级 2 年，且近 3 年连续从事本专业； 3.取得网络安全设计与开发或相关专业博士学位，且近 1 年连续从事本专业； 4.取得网络安全设计与开发或相关专业硕士学位，且近 3 年连续从业本专业。	2.取得网络安全设计与开发从业能力等级 3 级 2 年，且近 2 年连续从事本专业； 3.取得网络安全设计与开发或相关专业硕士学位，且近 1 年连续从业本专业； 4.取得网络安全设计与开发或相关专业学士学位，且近 2 年连续从事本专业。	2.取得网络安全设计与开发或相关专业硕士学位及以上； 3.取得网络安全设计与开发或相关专业学士学位，且近 1 年连续从事本专业。		
工作履历	1.近 5 年，作为前 5 名参加国家、省、市或大型组织网络安全项目 200 万人民币及以上 2 个的网络安全设计与开发； 2.近 5 年，参加地市级网络安全项目 100 万人民币及以上 5 个的网络安全设计与开发。	1.近 5 年，参加网络安全项目 100 万人民币及以上 5 个的网络安全设计与开发。	1.近 3 年，参加网络安全项目 3 个的网络安全设计与开发及相关工作。	1.参加网络安全项目 2 个的网络安全设计与开发及相关工作。	1.参加网络安全项目 1 个的网络安全设计与开发及相关工作。
工作传承	1.近 3 年，在国家 2 级以上刊物发表本专业或相关专业文章 2 篇； 2.近 5 年参加的 100 万人民币及以上网络安全项目，独立编写 2 个项目的网络安全设计与开发技术文档； 3.近 1 年，本专业或相关专业的年授课 15 人天。备注：培养新人考核合格 1 人，当年计授课 10 人天。	1.近 3 年，在省市以上刊物发表本专业或相关专业文章 2 篇； 2.近 5 年参加的 100 万网络安全项目，独立编写 1 个项目的网络安全设计与开发技术文档； 3.近 1 年，本专业或相关专业的年授课 10 人天。备注：培养新人考核合格 1 人，当年计授课 10 人天。	1.近 3 年，在省市以上刊物发表本专业或相关专业文章 1 篇； 2.近 3 年参加的网络安全项目，参加编写 1 个项目的技术文档。	1.能运用所需的知识和技能，在他人的指导下完成所承担的工作，并具有一定独立工作能力和实践经历。	1.能运用所需的知识和技能，在他人的指导下完成所承担的工作。

8 网络安全测试

8.1 职责要求

网络安全测试主要是针对信息系统、软硬件产品等被测对象的安全属性，由供方在特定的测试环境下，根据需方授权，按照测试准备、测试实施、测试分析、测试结果反馈等工作流程，选择适用的方法或工具，动态分析测试数据，发现被测对象存在的安全隐患，验证被测对象安全保障措施的符合性及有效性，提出安全整改建议。网络安全测试通常包括信息系统安全测试、APP安全测试、漏洞安全扫描、

基线配置核查、渗透测试、源代码审计等。网络安全测试工具应符合相关国家标准要求，确保可靠性和安全性。

8.2 职业等级

网络安全测试分5个等级，即：职级5级（资深网络安全测试工程师）、职级4级（高级网络安全测试工程师）、和职级3级（网络安全测试工程师）、职级2级（初级网络安全测试工程师）、职级1级（助理网络安全测试工程师）。

8.3 基本条件

申请各职业等级的人员，符合以下条件之一，即可满足申请基本条件，见表11。

表 11 网络安全测试的基本条件

职业等级	基本条件
5 级	1. 取得网络安全测试从业能力等级 4 级 2 年，且近 3 年连续从事本专业； 2. 取得网络安全测试或相关专业博士学位，且近 1 年连续从事本专业； 3. 取得网络安全测试或相关专业硕士学位，且近 3 年连续从业本专业； 4. 取得国家计算机技术与软件专业技术资格（水平）考试相关高级资格，且近 2 年连续从事本专业。
4 级	1. 取得网络安全测试从业能力等级 3 级 2 年，且近 2 年连续从事本专业； 2. 取得网络安全测试或相关专业硕士学位，且近 1 年连续从业本专业； 3. 取得网络安全测试或相关专业学士学位，且近 2 年连续从事本专业； 4. 取得国家计算机技术与软件专业技术资格（水平）考试相关中级资格，且近 2 年连续从事本专业； 5. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 10 个以上（包含 10 个）。
3 级	1. 取得网络安全测试或相关专业硕士学位及以上； 2. 取得网络安全测试或相关专业学士学位，且近 1 年连续从事本专业； 3. 取得国家计算机技术与软件专业技术资格（水平）考试相关中级资格； 4. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 5 个以上（包含 5 个）； 5. 取得网络安全方向省级一类竞赛第 1 名。
2 级	1. 取得网络安全测试及相关专业连续从业 2 年； 2. 取得网络安全测试或相关专业学士学位及以上； 3. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 1 个以上（包含 1 个）； 4. 取得网络安全方向省级一类竞赛第 2-3 名。
1 级	1. 取得网络安全测试及相关专业连续从业 1 年； 2. 取得网络安全测试或相关专业大专及以上； 3. 取得网络安全方向省级一类竞赛第 4-5 名。

8.4 能力评价准则

8.4.1 知识

网络安全测试的知识评价规则见表12。

表 12　网络安全测试的知识评价规则

能力要素	能力项		网络安全测试				
			资深网络安全测试工程师（5 级）	高级网络安全测试工程师（4 级）	网络安全测试工程师（3 级）	初级网络安全测试工程师（2 级）	助理网络安全测试工程师（1 级）
基础知识	GK01	计算机硬件基础知识	K2	K2	K2	K1	K1
	GK02	计算机软件基础知识	K2	K2	K2	K1	K1
	GK03	数据传输与通信基础知识	K2	K2	K2	K1	K1
	GK04	计算机网络基础知识	K2	K2	K2	K1	K1
	GK05	项目管理基础知识	K2	K2	K2	K1	—
	GK06	网络安全知识	K2	K2	K2	K1	—
	GK07	质量管理知识	K2	K2	K2	K1	—
专业知识	D-PK01	应用安全知识	K4	K4	K3	K2	—
	D-PK02	网络攻防知识	K3	K2	K1	K1	—
	D-PK03	恶意代码防护知识	K4	K4	K3	K2	K1
	D-PK04	数据安全及灾备知识	K2	K1	—	—	—
	D-PK05	基础软件系统安全知识	K4	K4	K3	K2	K1
	D-PK06	物理环境安全知识	K4	K4	K3	K2	K1
	D-PK07	密码学知识	K3	K2	K2	K1	K1
	D-PK08	网络安全审计知识	K3	K3	K2	K2	K1
	D-PK09	网络安全测试技术	K4	K4	K3	K2	K1
	D-PK10	安全管理体系	K4	K4	K3	K2	K1
	D-PK11	云平台安全知识	K4	K3	K2	K1	K1
	D-PK12	大数据安全知识	K4	K3	K2	K1	K1
	D-PK13	物联网安全知识	K4	K3	K2	K1	K1
	D-PK14	工业控制系统安全知识	K4	K3	K2	K1	K1
	D-PK15	移动应用安全知识	K3	K3	K2	K1	K1
	D-PK16	区块链安全知识	K4	K3	K2	K1	—
	D-PK17	终端安全知识	K4	K3	K2	K1	K1
	D-PK18	网络攻击溯源知识	K4	K3	K2	K1	K1
	D-PK19	网络安全流量知识	K4	K3	K2	K1	K1

表 12 网络安全测试的知识评价规则（续）

相关知识	RK01	营销、策划基础知识	—	—	—	—	—
	RK02	知识产权知识	K1	K1	K1	K1	K1
	RK03	劳动法知识	K1	K1	K1	K1	K1
	RK04	国家信息技术服务相关法律、法规	K1	K1	K1	K1	K1

8.4.2 技能

网络安全测试的技能评价规则见表13

表 13 网络安全测试的技能评价规则

能力要素	能力项		网络安全测试				
			资深网络安全测试工程师（5 级）	高级网络安全测试工程师（4 级）	网络安全测试工程师（3 级）	初级网络安全测试工程师（2 级）	助理网络安全测试工程师（1 级）
基础技能	BS01	计算机硬件基础应用能力	S2	S2	S2	S1	S1
	BS02	计算机软件基础应用能力	S2	S2	S2	S1	S1
	BS03	计算机网络基础应用能力	S2	S2	S2	S1	S1
	BS04	文档撰写能力	S4	S3	S2	S1	S1
	BS05	外语应用能力	S2	S2	S1	S1	S1
专业技能	D-PS01	网络安全测试	S4	S4	S3	S2	S1
	D-PS02	网络安全风险评估	S4	S4	S3	S2	S1
	D-PS03	需求分析	S4	S4	S3	S2	S1
	D-PS04	网络安全规划设计	S4	S4	S3	S2	S1
	D-PS05	安全管理体系建设	S4	S4	S3	S2	S1
	D-PS06	系统建模及架构设计能力	S4	S4	S3	S2	S1
	D-PS07	网络安全评估分析	S4	S4	S3	S2	S1
	D-PS08	网络安全加固	S4	S4	S3	S2	S1
	D-PS09	工程项目管理	—	—	—	—	—
	D-PS10	网络渗透测试	S4	S4	S3	S2	S1
	D-PS11	网络安全态势分析	S4	S4	S3	S2	S1
	D-PS12	应急响应	S4	S4	S3	S2	S1
	D-PS13	渗透工具的使用和研发	S3	S3	S2	S1	S1

表 13 网络安全测试的技能评价规则（续）

专业技能	D-PS14	网络安全审计	S4	S4	S3	S2	S1
	D-PS15	信息系统工程监理	—	—	—	—	—
	D-PS16	安全产品设计	—	—	—	—	—
	D-PS17	云平台安全技术	S3	S3	S2	S1	S1
	D-PS18	大数据安全技术	S3	S3	S2	S1	S1
	D-PS19	物联网安全	S3	S3	S2	S1	S1
	D-PS20	工业控制系统安全	S3	S3	S2	S1	S1
	D-PS21	移动应用架构设计能力	S2	S1	—	—	—
	D-PS22	移动应用安全技能	S4	S4	S3	S2	S1
	D-PS23	区块链安全技能	S4	S3	S2	S1	—
	D-PS24	网络安全数据处理	S4	S3	S2	S1	S1
	D-PS25	供应链安全测试能力	S4	S3	S2	S1	—
	D-PS26	移动终端测试能力	S4	S3	S2	S1	S1
	D-PS27	网络攻击溯源能力	S4	S3	S2	S1	S1
	D-PS28	网络安全流量分析能力	S4	S3	S2	S1	S1
软技能	SS01	沟通能力	S3	S2	S1	S1	S1
	SS02	学习能力	S3	S3	S2	S2	S1
	SS03	问题判断与解决能力	S3	S3	S2	S1	S1
	SS04	创新能力	S2	S1	S1	—	—
	SS05	知识分享能力	S3	S2	S1	—	—

8.4.3 经验

网络安全测试的经验评价规则，满足下列条件之一即可见表14。

表 14　网络安全测试的经验评价规则

经验	职位及经验等级				
	资深网络安全测试工程师（5级）E3	高级网络安全测试工程师（4级）E2	网络安全测试工程师（3级）E2	初级网络安全测试工程师（2级）E1	助理网络安全测试工程师（1级）E1
工作年限	1.网络安全测试及相关专业连续从业7年，且近3年连续从事本专业；	1.网络安全测试及相关专业连续从业5年，且近2年连续从事本专业；	1.网络安全测试或相关专业连续从业3年，且近1年连续从事本专业；	1.网络安全测试及相关专业连续从业2年；	1.网络安全测试及相关专业连续从业1年；
工作年限	2.取得网络安全测试从业能力等级4级2年，且近3年连续从事本专业； 3.取得网络安全测试或相关专业博士学位，且近1年连续从事本专业； 4.取得网络安全测试或相关专业博士学位，且近1年连续从事本专业； 5.取得网络安全测试或相关专业硕士学位，且近3年连续从业本专业	2.取得网络安全测试从业能力等级3级2年，且近2年连续从事本专业； 3.取得网络安全测试或相关专业硕士学位，且近1年连续从业本专业； 4.取得网络安全测试或相关专业学士学位，且近2年连续从事本专业；	2.取得网络安全测试或相关专业硕士学位及以上； 3.取得网络安全测试或相关专业学士学位，且近1年连续从事本专业；		
工作履历	1.近5年，参加国家、省、市或大型组织网络安全项目200万人民币及以上2个的独立测试； 2.近5年，作为测试负责人参加地市级网络安全项目100万人民币及以上5个独立测试。	1.近5年，参加网络安全项目100万人民币及以上5个的测试。	1.近3年，参加网络安全项目3个的测试及相关工作。	1.参加网络安全项目2个的测试及相关工作。	1.参加网络安全项目1个的测试及相关工作。
工作传承	1.近3年，在国家2级以上刊物发表本专业或相关专业文章2篇； 2.近5年参加的100万人民币及以上网络安全项目，独立编写2个项目的测试文档； 3.近1年，本专业或相关专业的年授课15人天。备注：培养新人考核合格1人，当年计授课10人天。	1.近3年，在省市以上刊物发表本专业或相关专业文章2篇； 2.近5年参加的100万网络安全项目，独立编写1个项目的测试文档； 3.近1年，本专业或相关专业的年授课10人天。备注：培养新人考核合格1人，当年计授课10人天。	1.近3年，在省市以上刊物发表本专业或相关专业文章1篇； 2.近3年参加的网络安全项目，参加编写1个项目的测试文档。	1.能运用所需的知识和技能，在他人的指导下完成所承担的工作，并具有一定独立工作能力和实践经历。	1.能运用所需的知识和技能，在他人的指导下完成所承担的工作.

9 网络安全集成

9.1 职责要求

网络安全集成主要是针对需方采购或租赁的网络安全硬件设备、网络安全软件、系统（包括软件构件）等各类网络安全设备，由供方根据已制定的系统集成方案（包含设计方案和实施方案等），明确部署方式，按照部署环境搭建、集成实施等工作流程规范开展集成部署工作，确保软硬件安全、高效稳定运行。

9.2 职业等级

网络安全集成分4个等级，即：职级6级（资深网络安全集成工程师）、职级5级（高级网络安全集成工程师）、和职级4级（网络安全集成工程师）、职级3级（初级网络安全集成工程师）。

9.3 基本条件

申请各职业等级的人员，符合以下条件之一，即可满足申请基本条件。见表15。

表 15 网络安全集成的基本条件

职业等级	基本条件
6 级	1. 取得网络安全集成从业能力等级 5 级 2 年，且近 3 年连续从事本专业； 2. 取得网络安全集成或相关专业博士学位，且近 3 年连续从事本专业； 3. 取得国家计算机技术与软件专业技术资格（水平）考试相关高级资格，且近 4 年连续从事本专业。
5 级	5. 取得网络安全集成从业能力等级 4 级 2 年，且近 3 年连续从事本专业； 6. 取得网络安全集成或相关专业博士学位，且近 1 年连续从事本专业； 7. 取得网络安全集成或相关专业硕士学位，且近 3 年连续从业本专业； 8. 取得国家计算机技术与软件专业技术资格（水平）考试相关高级资格，且近 2 年连续从事本专业。
4 级	6. 取得网络安全集成从业能力等级 3 级 2 年，且近 2 年连续从事本专业； 7. 取得网络安全集成或相关专业硕士学位，且近 1 年连续从业本专业； 8. 取得网络安全集成或相关专业学士学位，且近 2 年连续从事本专业； 9. 取得国家计算机技术与软件专业技术资格（水平）考试相关中级资格，且近 2 年连续从事本专业； 10. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 10 个以上（包含 10 个）。
3 级	6. 取得网络安全集成或相关专业硕士学位及以上； 7. 取得网络安全集成或相关专业学士学位，且近 1 年连续从事本专业； 8. 取得国家计算机技术与软件专业技术资格（水平）考试相关中级资格； 9. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 5 个以上（包含 5 个）； 10. 取得网络安全方向省级一类竞赛第 1 名。

9.4 能力评价准则

9.4.1 知识

网络安全集成的知识评价规则见表16。

表 16　网络安全集成的知识评价规则

能力要素	能力项		网络安全集成			
			资深网络安全集成工程师（6 级）	高级网络安全集成工程师（5 级）	网络安全集成工程师（4 级）	初级网络安全集成工程师（3 级）
基础知识	GK01	计算机硬件基础知识	K4	K3	K2	K2
	GK02	计算机软件基础知识	K4	K3	K2	K2
	GK03	数据传输与通信基础知识	K3	K2	K2	K2
	GK04	计算机网络基础知识	K3	K2	K2	K2
	GK05	项目管理基础知识	K3	K2	K2	K2
基础知识	GK06	网络安全知识	K3	K2	K2	K2
	GK07	质量管理知识	K3	K2	K2	K2
专业知识	D-PK01	应用安全知识	K4	K4	K3	K2
	D-PK02	网络攻防知识	K3	K3	K2	K2
	D-PK03	恶意代码防护知识	K3	K3	K2	K2
	D-PK04	数据安全及灾备知识	K3	K3	K2	K1
	D-PK05	基础软件系统安全知识	K4	K4	K3	K2
	D-PK06	物理环境安全知识	K4	K4	K3	K2
	D-PK07	密码学知识	K2	K2	K2	K1
	D-PK08	网络安全审计知识	K2	K2	K2	K1
	D-PK09	网络安全测试技术	K2	K2	K2	K1
	D-PK10	安全管理体系	K3	K3	K2	K2
	D-PK11	云平台安全知识	K4	K4	K3	K2
	D-PK12	大数据安全知识	K4	K4	K3	K2
	D-PK13	物联网安全知识	K3	K3	K2	K1
	D-PK14	工业控制系统安全知识	K3	K3	K2	K1
	D-PK15	移动应用安全知识	K3	K3	K2	K1
	D-PK16	区块链安全知识	K2	K2	K1	—
	D-PK17	终端安全知识	K3	K3	K2	K1
	D-PK18	网络攻击溯源知识	K2	K1	—	—
	D-PK19	网络安全流量知识	K2	K1	—	—

表 16 网络安全集成的知识评价规则（续）

相关知识	RK01	营销、策划基础知识	K2	K2	K1	K1
	RK02	知识产权知识	K1	K1	K1	K1
	RK03	劳动法知识	K1	K1	K1	K1
	RK04	国家信息技术服务相关法律、法规	K1	K1	K1	K1

9.4.2 技能

网络安全集成的技能评价规则见表17

表 17 网络安全集成的技能评价规则

能力要素	能力项		网络安全集成			
			资深网络安全集成工程师（6 级）	高级网络安全集成工程师（5 级）	网络安全集成工程师（4 级）	初级网络安全集成工程师（3 级）
基本技能	BS01	计算机硬件基础应用能力	S4	S3	S2	S2
	BS02	计算机软件基础应用能力	S4	S3	S2	S2
	BS03	计算机网络基础应用能力	S4	S3	S2	S2
	BS04	文档撰写能力	S4	S4	S3	S2
	BS05	外语应用能力	S2	S2	S2	S1
专业技能	D-PS01	网络安全测试	—	—	—	—
	D-PS02	网络安全风险评估	S4	S4	S3	S2
	D-PS03	需求分析	S2	S2	S2	S1
	D-PS04	网络安全规划设计	—	—	—	—
	D-PS05	安全管理体系建设	—	—	—	—
	D-PS06	系统建模及架构设计能力	S2	S2	S2	S1
	D-PS07	网络安全评估分析	S2	S2	S2	S1
	D-PS08	网络安全加固	S4	S4	S3	S2
	D-PS09	工程项目管理	S4	S4	S3	S2
	D-PS10	网络渗透测试	—	—	—	—
	D-PS11	网络安全态势分析	—	—	—	—
	D-PS12	应急响应	—	—	—	—
	D-PS13	渗透工具的使用及研发	—	—	—	—
	D-PS14	网络安全审计	—	—	—	—
	D-PS15	信息系统工程监理	S2	S2	S2	S1

表 17 网络安全集成的技能评价规则（续）

专业技能	D-PS16	安全产品设计	—	—	—	—
	D-PS17	云平台安全技术	—	—	—	—
	D-PS18	大数据安全技术	—	—	—	—
	D-PS19	物联网安全	—	—	—	—
	D-PS20	工业控制系统安全	—	—	—	—
	D-PS21	移动应用架构设计能力	—	—	—	—
	D-PS22	移动应用安全技能	S2	S2	S2	S1
	D-PS23	区块链安全技能	—	—	—	—
	D-PS24	网络安全数据处理	S4	S4	S2	S1
	D-PS25	供应链安全测试能力	S2	S2	S2	S1
	D-PS26	移动终端测试能力	—	—	—	—
	D-PS27	网络攻击溯源能力	—	—	—	—
	D-PS28	网络安全流量分析能力	—	—	—	—
软技能	SS01	沟通能力	S4	S3	S2	S1
	SS02	学习能力	S3	S3	S3	S2
	SS03	问题判断与解决能力	S4	S3	S3	S2
	SS04	创新能力	S2	S2	S1	S1
	SS05	知识分享能力	S3	S3	S2	S1

9.4.3 经验

网络安全集成的经验评价规则，满足下列条件之一即可见表18。

表 18　网络安全集成的经验评价规则

经验	职位及经验等级			
	资深网络安全集成工程师（6 级）E4	高级网络安全集成工程师（5 级）E3	网络安全集成工程师（4 级）E2	初级网络安全集成工程师（3 级）
工作年限	1.网络安全集成及相关专业连续从业 9 年，且近 3 年连续从事本专业； 2.取得网络安全集成从业能力等级 5 级 2 年，且近 3 年连续从事本专业； 3.取得网络安全集成或相关专业博士学位，且近 3 年连续从事本专业； 4.取得国家计算机技术与软件专业技术资格（水平）考试相关高级资格，且近 4 年连续从事本专业。	1.网络安全集成及相关专业连续从业 7 年，且近 3 年连续从事本专业； 2.取得网络安全集成从业能力等级 4 级 2 年，且近 3 年连续从事本专业； 3.取得网络安全集成或相关专业博士学位，且近 1 年连续从事本专业； 4.取得网络安全集成或相关专业硕士学位，且近 3 年连续从业本专业； 5.取得国家计算机技术与软件专业技术资格（水平）考试相关高级资格，且近 2 年连续从事本专业。	1.网络安全集成及相关专业连续从业 5 年，且近 2 年连续从事本专业； 2.取得网络安全集成从业能力等级 3 级 2 年，且近 2 年连续从事本专业； 3.取得网络安全集成或相关专业硕士学位，且近 1 年连续从业本专业； 4.取得网络安全集成或相关专业学士学位，且近 2 年连续从事本专业； 5.取得国家计算机技术与软件专业技术资格（水平）考试相关中级资格，且近 2 年连续从事本专业。	1.网络安全集成或相关专业连续从业 3 年，且近 1 年连续从事本专业； 2.取得网络安全集成或相关专业硕士学位及以上； 3.取得网络安全集成或相关专业学士学位，且近 1 年连续从事本专业。
工作履历	1.近 5 年，负责国家、省、市或大型组织网络安全项目 300 万人民币及以上 4 个的集成； 2.近 5 年，参加地市级网络安全项目 200 万人民币及以上 8 个的集成。	1.近 5 年，负责国家、省、市或大型组织网络安全项目 200 万人民币及以上 2 个的集成； 2.近 5 年，参加地市级网络安全项目 100 万人民币及以上 5 个的集成。	1.近 5 年，参加网络安全项目 100 万人民币及以上 2 个的集成。	1.近 3 年，参加网络安全项目 3 个的集成及相关工作。
工作传承	1.近 3 年，在国家 2 级以上刊物发表本专业或相关专业文章 4 篇； 2.近 5 年独立编写 200 万人民币及以上 3 个项目的集成技术文档； 3.近 1 年，本专业或相关专业的年授课 20 人天。备注：培养新人考核合格 1 人，当年计授课 10 人天。	1.近 3 年，在国家 2 级以上刊物发表本专业或相关专业文章 2 篇； 2.近 5 年独立编写 100 万人民币及以上 2 个项目的集成技术文档； 3.近 1 年，本专业或相关专业的年授课 15 人天。备注：培养新人考核合格 1 人，当年计授课 10 人天。	1.近 3 年，在省市以上刊物发表本专业或相关专业文章 2 篇； 2.近 5 年独立编写 100 万人民币及以上 1 个项目的集成技术文档； 3.近 1 年，本专业或相关专业的年授课 10 人天。备注：培养新人考核合格 1 人，当年计授课 10 人天。	1.近 3 年，在省市以上刊物发表本专业或相关专业文章 1 篇； 2.近 3 年参加编写 1 个项目的集成技术文档。

10 网络安全运维

10.1 职责要求

网络安全运维主要是针对技术设施安全监测、技术设施安全预警、技术设施安全加固、安全漏洞补丁通告、恶意代码防范和处理、安全事件响应与取证以及其它网络安全运维工作，协助组织信息系统管理人员进行信息系统安全运维工作，以发现并修复信息系统中所存在的安全隐患，降低安全隐患被非法利用的可能性，并在安全隐患被利用后及时加以响应。

10.2 职业等级

网络安全运维分5个等级，即：职级5级（资深网络安全运维工程师）、职级4级（高级网络安全运维工程师）、和职级3级（网络安全运维工程师）、职级2级（初级网络安全运维工程师）、职级1级（助理网络安全运维工程师）。

10.3 基本条件

申请各职业等级的人员，符合以下条件之一，即可满足申请基本条件。见表19。

表 19 网络安全运维的基本条件

职业等级	基本条件
5 级	1. 取得网络安全运维从业能力等级 4 级 2 年，且近 3 年连续从事本专业； 2. 取得网络安全运维或相关专业博士学位，且近 1 年连续从事本专业； 3. 取得网络安全运维或相关专业硕士学位，且近 3 年连续从业本专业； 4. 取得国家计算机技术与软件专业技术资格（水平）考试相关高级资格，且近 2 年连续从事本专业。
4 级	1. 取得网络安全运维从业能力等级 3 级 2 年，且近 2 年连续从事本专业； 2. 取得网络安全运维或相关专业硕士学位，且近 1 年连续从业本专业； 3. 取得网络安全运维或相关专业学士学位，且近 2 年连续从事本专业； 4. 取得国家计算机技术与软件专业技术资格（水平）考试相关中级资格，且近 2 年连续从事本专业； 5. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 10 个以上（包含 10 个）。
3 级	1. 取得网络安全运维或相关专业硕士学位及以上； 2. 取得网络安全运维或相关专业学士学位，且近 1 年连续从事本专业； 3. 取得国家计算机技术与软件专业技术资格（水平）考试相关中级资格； 4. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 5 个以上（包含 5 个）； 5. 取得网络安全方向省级一类竞赛第 1 名。
2 级	1. 网络安全运维及相关专业连续从业 2 年； 2. 取得网络安全运维或相关专业学士学位及以上； 3. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 1 个以上（包含 1 个）； 4. 取得网络安全方向省级一类竞赛第 2-3 名。
1 级	1. 网络安全运维及相关专业连续从业 1 年； 2. 取得网络安全运维或相关专业大专及以上； 3. 取得网络安全方向省级一类竞赛第 3-4 名。

10.4 能力评价准则

10.4.1 知识

网络安全运维的知识评价规则见表20。

表 20 网络安全运维的知识评价规则

能力要素	能力项		网络安全运维				
			资深网络安全运维工程师（5 级）	高级网络安全运维工程师（4 级）	网络安全运维工程师（3 级）	初级网络安全运维工程师（2 级）	助理网络安全运维工程师（1 级）
基础知识	GK01	计算机硬件基础知识	K4	K3	K2	K1	K1
	GK02	计算机软件基础知识	K4	K3	K2	K1	K1
	GK03	数据传输与通信基础知识	K4	K3	K2	K1	K1
	GK04	计算机网络基础知识	K4	K3	K2	K1	K1
基础知识	GK05	项目管理基础知识	K2	K2	K2	K1	—
	GK06	网络安全知识	K4	K3	K2	K1	K1
	GK07	质量管理知识	K2	K2	K2	K1	—
专业知识	D-PK01	应用安全知识	K4	K3	K2	K1	—
	D-PK02	网络攻防知识	K4	K3	K3	K2	K1
	D-PK03	恶意代码防护知识	K4	K3	K2	K1	—
	D-PK04	数据安全及灾备知识	K4	K3	K2	K1	—
	D-PK05	基础软件系统安全知识	K4	K3	K3	K2	K1
	D-PK06	物理环境安全知识	K4	K3	K3	K2	K1
	D-PK07	密码学知识	K2	K1	—	—	—
	D-PK08	网络安全审计知识	K4	K3	K2	K1	—
	D-PK09	网络安全测试技术	K4	K3	K3	K2	K1
	D-PK10	安全管理体系	K4	K3	K2	K1	K1
	D-PK11	云平台安全知识	K3	K2	K1	—	—
	D-PK12	大数据安全知识	K3	K2	K1	—	—
	D-PK13	物联网安全知识	K3	K2	K1	—	—
	D-PK14	工业控制系统安全知识	K3	K2	K1	—	—
	D-PK15	移动应用安全知识	K3	K2	K1	—	—
	D-PK16	区块链安全知识	K3	K2	K1	—	—
	D-PK17	终端安全知识	K4	K3	K2	K1	K1

	D-PK18	网络攻击溯源知识	K4	K3	K2	K1	—
	D-PK19	网络安全流量知识	K4	K3	K2	K1	K1
相关知识	RK01	营销、策划基础知识	—	—	—	—	—
	RK02	知识产权知识	K1	K1	K1	K1	K1
	RK03	劳动法知识	K1	K1	K1	K1	K1
	RK04	国家信息技术服务相关法律、法规	K1	K1	K1	K1	K1

10.4.2 技能

网络安全运维的技能评价规则见表21。

表 21 网络安全运维的技能评价规则

能力要素	能力项		网络安全运维				
			资深网络安全运维工程师（5 级）	高级网络安全运维工程师（4 级）	网络安全运维工程师（3 级）	初级网络安全运维工程师（2 级）	助理网络安全运维工程师（1 级）
基础技能	BS01	计算机硬件基础应用能力	S4	S3	S2	S1	S1
	BS02	计算机软件基础应用能力	S4	S3	S2	S1	S1
	BS03	计算机网络基础应用能力	S4	S3	S2	S1	S1
	BS04	文档撰写能力	S4	S3	S2	S1	S1
	BS05	外语应用能力	S2	S2	S1	S1	S1
专业技能	D-PS01	网络安全测试	—	—	—	—	—
	D-PS02	网络安全风险评估	S2	S1	—	—	—
	D-PS03	需求分析	S3	S2	S1	S1	—
	D-PS04	网络安全规划设计	S3	S2	S1	—	—
	D-PS05	安全管理体系建设	S3	S2	S2	—	—
	D-PS06	系统建模及架构设计能力	S2	S1	S1	—	—
	D-PS07	网络安全评估分析	S3	S2	S1	—	—
	D-PS08	网络安全加固	S4	S3	S3	S2	S1
	D-PS09	工程项目管理	S4	S3	S3	S2	S1
	D-PS10	网络渗透测试	S2	S1	—	—	—
	D-PS11	网络安全态势分析	S4	S3	S3	S2	S1
	D-PS12	应急响应	S4	S3	S3	S2	S1
	D-PS13	渗透工具的使用和研发	—	—	—	—	—

	D-PS14	网络安全审计	—	—	—	—	—
	D-PS15	信息系统工程监理	—	—	—	—	—
	D-PS16	安全产品设计	—	—	—	—	—
	D-PS17	云平台安全技术	S3	S3	S2	S1	S1
	D-PS18	大数据安全技术	S3	S3	S2	S1	S1
	D-PS19	物联网安全	S3	S3	S2	S1	S1
	D-PS20	工业控制系统安全	S3	S3	S2	S1	S1
	D-PS21	移动应用架构设计能力	—	—	—	—	—
	D-PS22	移动应用安全技能	S3	S2	S1	—	—
专业技能	D-PS23	区块链安全技能	—	—	—	—	—
	D-PS24	网络安全数据处理	S4	S4	S3	S2	S1
	D-PS25	供应链安全测试能力	S2	S1	S1	—	—
	D-PS26	移动终端测试能力	S2	S1	S1	—	—
	D-PS27	网络攻击溯源能力	S2	S1	S1	—	—
	D-PS28	网络安全流量分析能力	S4	S4	S3	S2	S1
软技能	SS01	沟通能力	S3	S2	S1	S1	S1
	SS02	学习能力	S3	S3	S2	S2	S1
	SS03	问题判断与解决能力	S3	S3	S2	S1	S1
	SS04	创新能力	S2	S1	S1	—	—
	SS05	知识分享能力	S3	S2	S1	—	—

10.4.3 经验

网络安全运维的经验评价规则，满足下列条件之一即可见表22。

表 22　网络安全运维的经验评价规则

经验	职位及经验等级				
	资深网络安全运维工程师（5 级）E3	高级网络安全运维工程师（4 级）E2	网络安全运维工程师（3 级）E2	初级网络安全运维工程师（2 级）E1	助理网络安全运维工程师（1 级）E1
工作年限	1.网络安全运维及相关专业连续从业 7 年，且近 3 年连续从事本专业； 2.取得网络安全运维从业能力等级 4 级 2 年，且近 3 年连续从事本专业； 3.取得网络安全运维或相关专业博士学位，且近 1 年连续从事本专业； 4.取得网络安全运维或相关专业硕士学位，且近 3 年连续从业本专业。	1.网络安全运维及相关专业连续从业 5 年，且近 2 年连续从事本专业； 2.取得网络安全运维从业能力等级 3 级 2 年，且近 2 年连续从事本专业； 3.取得网络安全运维或相关专业硕士学位，且近 1 年连续从业本专业； 4.取得网络安全运维或相关专业学士学位，且近 2 年连续从事本专业。	1.网络安全运维或相关专业连续从业 3 年，且近 1 年连续从事本专业； 2.取得网络安全运维或相关专业硕士学位及以上； 3.取得网络安全运维或相关专业学士学位，且近 1 年连续从事本专业。	1.网络安全运维及相关专业连续从业 2 年。	1.网络安全运维及相关专业连续从业 1 年。
工作履历	1.近 5 年，参加网络安全运维项目 100 万人民币及以上 5 个的独立运维，每个项目有一年的运维时间。	1.近 5 年，参加网络安全运维项目 50 万人民币及以上 5 个的独立运维，每个项目有一年的运维时间。	1.近 3 年，参加网络安全运维项目 3 个的运维及相关工作，每个项目有 6 个月的运维时间。	1.参加网络安全项目 2 个的运维及相关工作。	1.参加网络安全项目 1 个的运维及相关工作。
工作传承	1.近 3 年，在国家 2 级以上刊物发表本专业或相关专业文章 2 篇； 2.近 5 年，独立编写 2 个 100 万人民币及以上运维项目的技术文档； 3.近 1 年，本专业或相关专业的年授课 15 人天。备注：培养新人考核合格 1 人，当年计授课 10 人天。	1.近 3 年，在省市以上刊物发表本专业或相关专业文章 2 篇； 2.近 5 年，独立编写 2 个 50 万元人民币及以上运维项目的技术文档； 3.近 1 年，本专业或相关专业的年授课 10 人天。备注：培养新人考核合格 1 人，当年计授课 10 人天。	1.近 3 年，在省市以上刊物发表本专业或相关专业文章 1 篇； 2.近 3 年参加编写 1 个运维项目的技术文档；	1.能运用所需的知识和技能，在他人的指导下完成所承担的工作，并具有一定独立工作能力和实践经历。	1.能运用所需的知识和技能，在他人的指导下完成所承担的工作

11 数据存储与保护

11.1 职责要求

数据存储与保护主要是针对需方生产经营活动中所涉及的业务数据、个人信息以及其他重要数据，由供方对数据收集、传输、存储、处理、使用以及销毁等数据生命周期中的相关行为以及数据的交易、公开等活动，实施分类分级、标识、风险评估、保护措施，协助需方保证数据的机密性、完整性、可用性等一系列的数据安全保护措施的服务。

11.2 职业等级

数据存储与保护分5个等级，即：职级5级（资深数据存储与保护工程师）、职级4级（高级数据存储与保护工程师）、和职级3级（数据存储与保护工程师）、职级2级（初级数据存储与保护工程师）、职级1级（助理数据存储与保护工程师）。

11.3 基本条件

申请各职业等级的人员，符合以下条件之一，即可满足申请基本条件。见表23。

表 23 数据存储与保护的基本条件

职业等级	基本条件
5 级	1. 取得数据存储与保护从业能力等级 4 级 2 年，且近 3 年连续从事本专业； 2. 取得数据存储与保护或相关专业博士学位，且近 1 年连续从事本专业； 3. 取得数据存储与保护或相关专业硕士学位，且近 3 年连续从业本专业； 4. 取得国家计算机技术与软件专业技术资格（水平）考试相关高级资格，且近 2 年连续从事本专业。
4 级	1. 取得数据存储与保护从业能力等级 3 级 2 年，且近 2 年连续从事本专业； 2. 取得数据存储与保护或相关专业硕士学位，且近 1 年连续从业本专业； 3. 取得数据存储与保护或相关专业学士学位，且近 2 年连续从事本专业； 4. 取得国家计算机技术与软件专业技术资格（水平）考试相关中级资格，且近 2 年连续从事本专业； 5. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 10 个以上（包含 10 个）。
3 级	1. 取得数据存储与保护或相关专业硕士学位及以上； 2. 取得数据存储与保护或相关专业学士学位，且近 1 年连续从事本专业； 3. 取得国家计算机技术与软件专业技术资格（水平）考试相关中级资格； 4. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 5 个以上（包含 5 个）； 5. 取得网络安全方向省级一类竞赛第 1 名。
2 级	1. 数据存储与保护及相关专业连续从业 2 年； 2. 取得数据存储与保护或相关专业学士学位及以上； 3. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 1 个以上（包含 1 个）。 4. 取得网络安全方向省级一类竞赛第 2-3 名。
1 级	1. 数据存储与保护及相关专业连续从业 1 年； 2. 取得数据存储与保护或相关专业大专及以上； 3. 取得网络安全方向省级一类竞赛第 4-5 名。

11.4 能力评价准则

11.4.1 知识

数据存储与保护的知识评价规则见表24。

表 24 数据存储与保护的知识评价规则

能力要素	能力项		数据存储与保护				
			资深数据存储与保护工程师（5 级）	高级数据存储与保护工程师（4 级）	数据存储与保护工程师(3 级）	初级数据存储与保护工程师（2 级）	助理数据存储与保护工程师（1 级）
基础知识	GK01	计算机硬件基础知识	K2	K2	K2	K1	K1
	GK02	计算机软件基础知识	K2	K2	K2	K1	K1
	GK03	数据传输与通信基础知识	K4	K3	K2	K2	K1
	GK04	计算机网络基础知识	K2	K2	K2	K1	K1
	GK05	项目管理基础知识	K2	K2	K2	K1	—
	GK06	网络安全知识	K4	K3	K2	K2	K1
	GK07	质量管理知识	K2	K2	K2	K1	—
专业知识	D-PK01	应用安全知识	K4	K4	K3	K2	K1
	D-PK02	网络攻防知识	K2	K2	K2	K1	K1
专业知识	D-PK03	恶意代码防护知识	K2	K2	K2	K1	K1
	D-PK04	数据安全及灾备知识	K4	K3	K2	K2	K1
	D-PK05	基础软件系统安全知识	K2	K1	—	—	—
	D-PK06	物理环境安全知识	K4	K3	K2	K2	K1
	D-PK07	密码学知识	K4	K3	K2	K2	K1
	D-PK08	网络安全审计知识	K2	K2	K2	K1	K1
	D-PK09	网络安全测试技术	K2	K1	—	—	—
	D-PK10	安全管理体系	K2	K2	K2	K1	K1
	D-PK11	云平台安全知识	K3	K3	K2	K1	K1
	D-PK12	大数据安全知识	K3	K3	K2	K1	K1
	D-PK13	物联网安全知识	—	—	—	—	—
	D-PK14	工业控制系统安全知识	—	—	—	—	—
	D-PK15	移动应用安全知识	—	—	—	—	—
	D-PK16	区块链安全知识	K3	K3	K2	K1	K1
	D-PK17	终端安全知识	—	—	—	—	—

	D-PK18	网络攻击溯源知识	—	—	—	—	—
	D-PK19	网络安全流量知识	—	—	—	—	—
相关知识	RK01	营销、策划基础知识	—	—	—	—	—
	RK02	知识产权知识	K1	K1	K1	K1	K1
	RK03	劳动法知识	K1	K1	K1	K1	K1
	RK04	国家信息技术服务相关法律、法规	K1	K1	K1	K1	K1

11.4.2 技能

数据存储与保护的技能评价规则见表25。

表 25 数据存储与保护的技能评价规则

能力要素	能力项		数据存储与保护				
			资深数据存储与保护工程师（5 级）	高级数据存储与保护工程师（4 级）	数据存储与保护工程师(3 级）	初级数据存储与保护工程师（2 级）	助理数据存储与保护工程师（1 级）
基础技能	BS01	计算机硬件基础应用能力	S2	S2	S2	S1	S1
	BS02	计算机软件基础应用能力	S2	S2	S2	S1	S1
基础技能	BS03	计算机网络基础应用能力	S2	S2	S2	S1	S1
	BS04	文档撰写能力	S4	S3	S2	S1	S1
	BS05	外语应用能力	S2	S2	S1	S1	S1
专业技能	D-PS01	网络安全测试	S1	S1	S1	—	—
	D-PS02	网络安全风险评估	S2	S2	S2	S1	S1
	D-PS03	需求分析	S4	S3	S2	S1	—
	D-PS04	网络安全规划设计	S4	S3	S2	S1	—
	D-PS05	安全管理体系建设	S4	S4	S3	S2	S1
	D-PS06	系统建模及架构设计能力	—	—	—	—	—
	D-PS07	网络安全评估分析	S4	S3	S2	S1	—
	D-PS08	网络安全加固	S4	S3	S2	S1	—
	D-PS09	工程项目管理	S4	S4	S3	S2	S1
	D-PS10	网络渗透测试	S1	S1	S1	—	—
	D-PS11	网络安全态势分析	—	—	—	—	—
	D-PS12	应急响应	—	—	—	—	—

	D-PS13	渗透工具的使用和研发	—	—	—	—	—
	D-PS14	网络安全审计	—	—	—	—	—
	D-PS15	信息系统工程监理	—	—	—	—	—
	D-PS16	安全产品设计	—	—	—	—	—
	D-PS17	云平台安全技术	S4	S4	S3	S2	S1
	D-PS18	大数据安全技术	S4	S4	S3	S2	S1
	D-PS19	物联网安全	—	—	—	—	—
	D-PS20	工业控制系统安全	—	—	—	—	—
	D-PS21	移动应用架构设计能力	—	—	—	—	—
	D-PS22	移动应用安全技能	—	—	—	—	—
	D-PS23	区块链安全技能	S3	S2	S2	S1	—
	D-PS24	网络安全数据处理	S4	S4	S3	S2	S1
	D-PS25	供应链安全测试能力	—	—	—	—	—
	D-PS26	移动终端测试能力	—	—	—	—	—
	D-PS27	网络攻击溯源能力	—	—	—	—	—
	D-PS28	网络安全流量分析能力	—	—	—	—	—
软技能	SS01	沟通能力	S3	S2	S1	S1	S1
	SS02	学习能力	S3	S3	S2	S2	S1
	SS03	问题判断与解决能力	S3	S3	S2	S1	S1
	SS04	创新能力	S2	S1	S1	—	—
	SS05	知识分享能力	S3	S2	S1	—	—

11.4.3 经验

数据存储与保护的经验评价规则，满足下列条件之一即可见表26。

表 26　数据存储与保护的经验评价规则

经验	职位及经验等级				
	资深数据存储与保护工程师（5 级）E3	高级数据存储与保护工程师（4 级）E2	数据存储与保护工程师（3 级）E2	初级数据存储与保护工程师(2级）E1	助理数据存储与保护工程师（1 级）E1
工作年限	1.数据存储与保护及相关专业连续从业 7 年，且近 3 年连续从事本专业； 2.取得数据存储与保护从业能力等级 4 级 2 年，且近 3 年连续从事本专业； 3.取得数据存储与保护或相关专业博士学位，且近 1 年连续从事本专业； 4.取得数据存储与保护或相关专业硕士学位，且近 3 年连续从业本专业； 5.取得国家计算机技术与软件专业技术资格（水平）考试相关高级资格，且近 2 年连续从事本专业。	1.数据存储与保护及相关专业连续从业 5 年，且近 2 年连续从事本专业； 2.取得数据存储与保护从业能力等级 3 级 2 年，且近 2 年连续从事本专业； 3.取得数据存储与保护或相关专业硕士学位，且近 1 年连续从业本专业； 4.取得数据存储与保护或相关专业学士学位，且近 2 年连续从事本专业； 5.取得国家计算机技术与软件专业技术资格（水平）考试相关中级资格，且近 2 年连续从事本专业。	1.数据存储与保护或相关专业连续从业 3 年，且近 1 年连续从事本专业； 2.取得数据存储与保护或相关专业硕士学位及以上； 3.取得数据存储与保护或相关专业学士学位，且近 1 年连续从事本专业。	1.数据存储与保护及相关专业连续从业 2 年。	1.数据存储与保护及相关专业连续从业 1 年。
工作履历	1.近 5 年，负责信息系统项目 300 万人民币及以上 5 个的数据存储与保护工作。	1.近 5 年，负责信息系统项目 200 万人民币及以上 5 个的数据存储与保护工作。	1.近 3 年，参加信息系统项目 3 个的数据存储与保护及相关工作。	1.参加信息系统项目 2 个的数据存储与保护及相关工作。	1.参加网络安全项目 1 个的数据存储与保护及相关工作。
工作传承	1.近 3 年，在国家 2 级以上刊物发表本专业或相关专业文章 2 篇； 2.近 5 年，独立编写 300 万人民币及以上 2 个信息系统项目的数据存储与保护文档； 3.近 1 年，本专业或相关专业的年授课 15 人天。 备注：培养新人考核合格 1 人，当年计授课 10 人天。	1.近 3 年，在省市以上刊物发表本专业或相关专业文章 2 篇； 2.近 5 年，独立编写 200 万人民币及以上 1 个信息系统项目的数据存储与保护文档； 3.近 1 年，本专业或相关专业的年授课 10 人天。 备注：培养新人考核合格 1 人，当年计授课 10 人天。	1.近 3 年，在省市以上刊物发表本专业或相关专业文章 1 篇； 2.近 3 年，参加编写 1 个信息系统项目的数据存储与保护文档。	1.能运用所需的知识和技能，在他人的指导下完成所承担的工作，并具有一定独立工作能力和实践经历。	1.能运用所需的知识和技能，在他人的指导下完成所承担的工作。

12 网络安全审计

12.1 职责要求

网络安全审计主要是针对需方的网络安全相关活动，由供方通过文件审核、记录检查、技术测试、现场访谈等手段，获得审计证据，并对其进行客观的评价，形成审计报告，确定被审计对象满足审计依据的程度，帮助需方全面了解和掌握其网络安全工作的有效性、充分性和适宜性。网络安全审计的范围通常包括网络安全管理目标、方针和策略，网络安全管理组织的建立，网络安全管理制度和流程，网络安全信息分类和保护体系，网络安全事件管理，网络安全教育和培训，物理安全，系统开发安全，网络安全，设备安全，操作系统安全，应用系统安全，数据安全，业务连续性管理以及供应商管理等。

12.2 职业等级

网络安全审计分5个等级，即：职级5级（资深网络安全审计工程师）、职级4级（高级网络安全审计工程师）、和职级3级（网络安全审计工程师）、职级2级（初级网络安全审计工程师）、职级1级（助理网络安全审计工程师）。

12.3 基本条件

申请各职业等级的人员，符合以下条件之一，即可满足申请基本条件。见表27。

表 27 网络安全审计的基本条件

职业等级	基本条件
5 级	1. 取得网络安全审计从业能力等级 4 级 2 年，且近 3 年连续从事本专业； 2. 取得网络安全审计或相关专业博士学位，且近 1 年连续从事本专业； 3. 取得网络安全审计或相关专业硕士学位，且近 3 年连续从业本专业； 4. 取得国家计算机技术与软件专业技术资格（水平）考试相关高级资格，且近 2 年连续从事本专业。
4 级	1. 取得网络安全审计从业能力等级 3 级 2 年，且近 2 年连续从事本专业； 2. 取得网络安全审计或相关专业硕士学位，且近 1 年连续从业本专业； 3. 取得网络安全审计或相关专业学士学位，且近 2 年连续从事本专业； 4. 取得国家计算机技术与软件专业技术资格（水平）考试相关中级资格，且近 2 年连续从事本专业； 5. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 10 个以上（包含 10 个）。
3 级	1. 取得网络安全审计或相关专业硕士学位及以上； 2. 取得网络安全审计或相关专业学士学位，且近 1 年连续从事本专业； 3. 取得国家计算机技术与软件专业技术资格（水平）考试相关中级资格； 4. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 5 个以上（包含 5 个）； 5. 取得网络安全方向省级一类竞赛第 1 名。
2 级	1. 网络安全审计及相关专业连续从业 2 年； 2. 取得网络安全审计或相关专业学士学位及以上； 3. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 1 个以上（包含 1 个）； 4. 取得网络安全方向省级一类竞赛第 2-3 名。

1级	1. 网络安全审计及相关专业连续从业1年； 2. 取得网络安全审计或相关专业大专及以上； 3. 取得网络安全方向省级一类竞赛第4-5名。

12.4 能力评价准则

12.4.1 知识

网络安全审计的知识评价规则见表28。

表28 网络安全审计的知识评价规则

能力要素	能力项		网络安全审计				
			资深网络安全审计工程师（5级）	高级网络安全审计工程师（4级）	网络安全审计工程师（3级）	初级网络安全审计工程师（2级）	理网络安全审计工程师(1级）
基础知识	GK01	计算机硬件基础知识	K2	K2	K2	K1	K1
	GK02	计算机软件基础知识	K2	K2	K2	K1	K1
	GK03	数据传输与通信基础知识	K2	K2	K2	K1	K1
	GK04	计算机网络基础知识	K2	K2	K2	K1	K1
	GK05	项目管理基础知识	K2	K2	K2	K1	—
	GK06	网络安全知识	K2	K2	K2	K1	—
	GK07	质量管理知识	K2	K2	K2	K1	—
专业知识	D-PK01	应用安全知识	K4	K3	K2	K1	K1
	D-PK02	网络攻防知识	K3	K2	K2	K1	K1
专业知识	D-PK03	恶意代码防护知识	K3	K2	K2	K1	K1
	D-PK04	数据安全及灾备知识	K3	K2	K2	K1	K1
	D-PK05	基础软件系统安全知识	K4	K3	K2	K1	K1
	D-PK06	物理环境安全知识	K3	K2	K2	K1	K1
	D-PK07	密码学知识	K3	K2	K2	K1	K1
	D-PK08	网络安全审计知识	K4	K4	K3	K3	K2
	D-PK09	网络安全测试技术	K3	K2	K2	K1	K1
	D-PK10	安全管理体系	K4	K3	K3	K2	K2
	D-PK11	云平台安全知识	K2	K2	K1	K1	—
	D-PK12	大数据安全知识	K2	K2	K1	K1	—
	D-PK13	物联网安全知识	K2	K2	K1	K1	—
	D-PK14	工业控制系统安全知识	K2	K2	K1	K1	—

	D-PK15	移动应用安全知识	K4	K3	K2	K1	K1
	D-PK16	区块链安全知识	K3	K2	K1	—	—
	D-PK17	终端安全知识	K4	K3	K2	K1	K1
	D-PK18	网络攻击溯源知识	K2	K1	K1	—	—
	D-PK19	网络安全流量知识	K2	K1	K1	—	—
相关知识	RK01	营销、策划基础知识	—	—	—	—	—
	RK02	知识产权知识	K1	K1	K1	K1	K1
	RK03	劳动法知识	K1	K1	K1	K1	K1
	RK04	国家信息技术服务相关法律、法规	K1	K1	K1	K1	K1

12.4.2 技能

网络安全审计的技能评价规则见表29。

表 29 网络安全审计的技能评价规则

能力要素	能力项		网络安全审计				
			资深网络安全审计工程师（5级）	高级网络安全审计工程师（4级）	网络安全审计工程师（3级）	初级网络安全审计工程师（2级）	助理网络安全审计工程师（1级）
基础技能	BS01	计算机硬件基础应用能力	S2	S2	S2	S1	S1
	BS02	计算机软件基础应用能力	S2	S2	S2	S1	S1
基础技能	BS03	计算机网络基础应用能力	S2	S2	S2	S1	S1
	BS04	文档撰写能力	S4	S3	S2	S1	S1
	BS05	外语应用能力	S2	S2	S1	S1	S1
专业技能	D-PS01	网络安全测试	S3	S2	S2	S1	S1
	D-PS02	网络安全风险评估	S3	S2	S2	S1	S1
	D-PS03	需求分析	S3	S2	S1	S1	—
	D-PS04	网络安全规划设计	S3	S2	S2	S1	S1
	D-PS05	安全管理体系建设	S4	S3	S3	S2	S2
	D-PS06	系统建模及架构设计能力	S3	S2	S2	S1	S1
	D-PS07	网络安全评估分析	S3	S2	S2	S1	S1
	D-PS08	网络安全加固	S3	S2	S2	S1	S1
	D-PS09	工程项目管理	S3	S2	S2	S1	S1
	D-PS10	网络渗透测试	S3	S2	S2	S1	S1
	D-PS11	网络安全态势分析	S3	S2	S2	S1	S1

	D-PS12	应急响应	S3	S2	S2	S1	S1
	D-PS13	渗透工具的使用和研发	—	—	—	—	—
	D-PS14	网络安全审计	S4	S4	S3	S3	S2
	D-PS15	信息系统工程监理	—	—	—	—	—
	D-PS16	安全产品设计	—	—	—	—	—
	D-PS17	云平台安全技术	—	—	—	—	—
	D-PS18	大数据安全技术	—	—	—	—	—
	D-PS19	物联网安全	—	—	—	—	—
	D-PS20	工业控制系统安全	—	—	—	—	—
	D-PS21	移动应用架构设计能力	—	—	—	—	—
	D-PS22	移动应用安全技能	S3	S2	S1	—	—
	D-PS23	区块链安全技能	S2	S1	—	—	—
	D-PS24	网络安全数据处理	—	—	—	—	—
	D-PS25	供应链安全测试能力	—	—	—	—	—
	D-PS26	移动终端测试能力	—	—	—	—	—
	D-PS27	网络攻击溯源能力	—	—	—	—	—
	D-PS28	网络安全流量分析能力	—	—	—	—	—
软技能	SS01	沟通能力	S3	S2	S1	S1	S1
	SS02	学习能力	S3	S3	S2	S2	S1
	SS03	问题判断与解决能力	S3	S3	S2	S1	S1
	SS04	创新能力	S2	S1	S1	—	—
	SS05	知识分享能力	S3	S2	S1	—	—

12.4.3 经验

网络安全审计的经验评价规则，满足下列条件之一即可见表30。

表 30 网络安全审计的经验评价规则

经验	职位及经验等级				
	资深网络安全审计工程师（5 级）E3	高级网络安全审计工程师（4 级）E2	网络安全审计工程师（3 级）E2	初级网络安全审计工程师（2 级）E1	助理网络安全审计工程师（1 级）E1

工作年限	1.网络安全审计及相关专业连续从业 7 年，且近 3 年连续从事本专业； 2.取得网络安全审计从业能力等级 4 级 2 年，且近 3 年连续从事本专业； 3.取得网络安全审计或相关专业博士学位，且近 1 年连续从事本专业； 4.取得网络安全审计或相关专业硕士学位，且近 3 年连续从业本专业。 5.取得国家计算机技术与软件专业技术资格（水平）考试相关高级资格，且近 2 年连续从事本专业。	1.网络安全审计及相关专业连续从业 5 年，且近 2 年连续从事本专业； 2.取得网络安全审计从业能力等级 3 级 2 年，且近 2 年连续从事本专业； 3.取得网络安全审计或相关专业硕士学位，且近 1 年连续从业本专业； 4.取得网络安全审计或相关专业学士学位，且近 2 年连续从事本专业。 5.取得国家计算机技术与软件专业技术资格（水平）考试相关中级资格，且近 2 年连续从事本专业。	1.网络安全审计或相关专业连续从业 3 年，且近 1 年连续从事本专业； 2.取得网络安全审计或相关专业硕士学位及以上。 3.取得网络安全审计或相关专业学士学位，且近 1 年连续从事本专业。	1.网络安全审计及相关专业连续从业 2 年。	1.网络安全审计及相关专业连续从业 1 年。
工作履历	1.近 5 年，负责网络安全项目 300 万人民币及以上 5 个的审计。	1.近 5 年，参加网络安全项目 100 万人民币及以上 5 个的审计。	1.近 3 年，参加网络安全项目 3 个的审计及相关工作。	1.参加网络安全项目 2 个的审计及相关工作。	1.参加网络安全项目 1 个的审计及相关工作。
工作传承	1.近 3 年，在国家 2 级以上刊物发表本专业或相关专业文章 2 篇；	1.近 3 年，在省市以上刊物发表本专业或相关专业文章 2 篇；	1.近 3 年，在省市以上刊物发表本专业或相关专业文章 1 篇；	1.能运用所需的知识和技能，在他人的指导下完成所承担	1.能运用所需的知识和技能，在他人的
工作传承	2.近 5 年，独立编写 100 万人民币及以上 2 个项目的审计文档； 3.近 1 年，本专业或相关专业的年授课 15 人天。备注：培养新人考核合格 1 人，当年计授课 10 人天。	2.近 5 年，独立编写 100 万人民币及以上 1 个项目的审计文档； 3.近 1 年，本专业或相关专业的年授课 10 人天。备注：培养新人考核合格 1 人，当年计授课 10 人天。	2.近 3 年参加的网络安全项目，参加编写 1 个项目的审计文档。	的工作，并具有一定独立工作能力和实践经历。	指导下完成所承担的工作。

13 网络安全培训

13.1 职责要求

面向网络安全相关人员，提供网络安全意识、技术、管理、体系、工程、法律、政策和标准等方面的培训，以满足提高网络安全意识、完善网络安全知识、掌握网络安全技能的需求、从而提高相关人员的网络安全能力水平。

13.2 职业等级

网络安全培训服务分4个等级，即：职级5级（资深网络安全培训师）、职级4级（高级网络安全培训师）、和职级3级（网络安全培训师）、职级2级（初级网络安全培训师）。

13.3 基本条件

申请各职业等级的人员，符合以下条件之一，即可满足申请基本条件。见表31。

表 31 网络安全培训的基本条件

职业等级	基本条件
5 级	1. 取得网络安全培训从业能力等级 4 级 2 年，且近 3 年连续从事本专业； 2. 取得网络安全培训或相关专业博士学位，且近 1 年连续从事本专业； 3. 取得网络安全培训或相关专业硕士学位，且近 3 年连续从业本专业； 4. 取得国家计算机技术与软件专业技术资格（水平）考试相关高级资格，且近 2 年连续从事本专业。
4 级	1. 取得网络安全培训从业能力等级 3 级 2 年，且近 2 年连续从事本专业； 2. 取得网络安全培训或相关专业硕士学位，且近 1 年连续从业本专业； 3. 取得网络安全培训或相关专业学士学位，且近 2 年连续从事本专业； 4. 取得国家计算机技术与软件专业技术资格（水平）考试相关中级资格，且近 2 年连续从事本专业； 5. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 10 个以上（包含 10 个）。
3 级	1. 取得网络安全培训或相关专业硕士学位及以上； 2. 取得网络安全培训或相关专业学士学位，且近 1 年连续从事本专业； 3. 取得国家计算机技术与软件专业技术资格（水平）考试相关中级资格。 4. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 5 个以上（包含 5 个）； 5. 取得网络安全方向省级一类竞赛第 1 名。
2 级	1. 网络安全培训及相关专业连续从业 2 年； 2. 取得网络安全培训或相关专业学士学位及以上； 3. 取得国家网络安全漏洞共享平台颁发的 CNVD 最有价值漏洞证书 1 个以上（包含 1 个）。 4. 取得网络安全方向省级一类竞赛第 2-3 名。

13.4 能力评价准则

申报网络安全培训各等级资格，宜具备相应的知识、技能和经验。

13.4.1 知识

网络安全培训的知识评价规则见表32。

表 32 网络安全培训的知识评价规则

能力要素	能力项		网络安全培训			
			资深网络安全培训师（5 级）	高级网络安全培训师（4 级）	网络安全培训师（3 级）	初级网络安全培训师（2 级）
基	GK01	计算机硬件基础知识	K4	K3	K2	K1

础知识	GK02	计算机软件基础知识	K4	K3	K2	K1
	GK03	数据传输与通信基础知识	K4	K3	K2	K1
	GK04	计算机网络基础知识	K4	K3	K2	K1
	GK05	项目管理基础知识	K2	K2	K2	K1
	GK06	网络安全知识	K4	K3	K2	K1
	GK07	质量管理知识	K2	K2	K2	K1
专业知识	D-PK01	应用安全知识	K3	K2	K2	K1
	D-PK02	网络攻防知识	K4	K3	K2	K1
	D-PK03	恶意代码防护知识	K3	K2	K2	K1
	D-PK04	数据安全及灾备知识	K2	K1	K1	K1
	D-PK05	基础软件系统安全知识	K3	K2	K2	K1
	D-PK06	物理环境安全知识	K3	K2	K2	K1
	D-PK07	密码学知识	K2	K2	K2	K1
	D-PK08	网络安全审计知识	K3	K2	K2	K1
	D-PK09	网络安全测试技术	K2	K2	K2	K1
	D-PK10	安全管理体系	K3	K2	K2	K1
	D-PK11	云平台安全知识	K2	K2	K1	K1
专业知识	D-PK12	大数据安全知识	K2	K2	K1	K1
	D-PK13	物联网安全知识	K2	K2	K1	K1
	D-PK14	工业控制系统安全知识	K2	K2	K1	K1
	D-PK15	移动应用安全知识	K2	K2	K1	K1
	D-PK16	区块链安全知识	K2	K2	K1	K1
	D-PK17	终端安全知识	K2	K2	K1	K1
	D-PK18	网络攻击溯源知识	K2	K2	K1	K1
	D-PK19	网络安全流量知识	K2	K2	K1	K1
相关知识	RK01	营销、策划基础知识	K1	K1	K1	K1
	RK02	知识产权知识	K1	K1	K1	K1
	RK03	劳动法知识	K1	K1	K1	K1
	RK04	国家信息技术服务相关法律、法规	K4	K3	K2	K1

13.4.2 技能

网络安全培训的技能评价规则见表33。

表 33　网络安全培训的技能评价规则

能力要素	能力项		网络安全培训			
			资深网络安全培训师（5 级）	高级网络安全培训师（4 级）	网络安全培训师（3 级）	初级网络安全培训师（2 级）
基本技能	BS01	计算机硬件基础应用能力	S2	S2	S2	S1
	BS02	计算机软件基础应用能力	S2	S2	S2	S1
	BS03	计算机网络基础应用能力	S2	S2	S2	S1
	BS04	文档撰写能力	S4	S3	S2	S1
	BS05	外语应用能力	S2	S2	S1	S1
专业技能	D-PS01	网络安全测试	—	—	—	—
	D-PS02	网络安全风险评估	—	—	—	—
	D-PS03	需求分析	S4	S3	S2	S1
	D-PS04	网络安全规划设计	S3	S2	S1	S1
	D-PS05	安全管理体系建设	—	—	—	—
	D-PS06	系统建模及架构设计能力	—	—	—	—
	D-PS07	网络安全评估分析	S3	S2	S1	—
专业技能	D-PS08	网络安全加固	—	—	—	—
	D-PS09	工程项目管理	S4	S3	S2	S1
	D-PS10	网络渗透测试	—	—	—	—
	D-PS11	网络安全态势分析	—	—	—	—
	D-PS12	应急响应	—	—	—	—
	D-PS13	渗透工具的使用及研发	—	—	—	—
	D-PS14	网络安全审计	—	—	—	—
	D-PS15	信息系统工程监理	—	—	—	—
	D-PS16	安全产品设计	—	—	—	—
	D-PS17	云平台安全技术	—	—	—	—
	D-PS18	大数据安全技术	—	—	—	—
	D-PS18	物联网安全	—	—	—	—
	D-PS19	工业控制系统安全	—	—	—	—
	D-PS21	移动应用架构设计能力	—	—	—	—
	D-PS22	移动应用安全技能	—	—	—	—

	D-PS23	区块链安全技能	—	—	—	—
	D-PS24	网络安全数据处理	—	—	—	—
	D-PS25	供应链安全测试能力	—	—	—	—
	D-PS26	移动终端测试能力	—	—	—	—
	D-PS27	网络攻击溯源能力	—	—	—	—
	D-PS28	网络安全流量分析能力	—	—	—	—
软技能	SS01	沟通能力	S4	S4	S3	S2
	SS02	学习能力	S4	S4	S3	S2
	SS03	问题判断与解决能力	S4	S4	S3	S2
	SS04	创新能力	S2	S2	S1	S1
	SS05	知识分享能力	S4	S4	S3	S2

13.4.3 经验

网络安全培训的经验评价规则，满足下列条件之一即可见表34。

表 34 网络安全培训的经验评价规则

经验	职位及经验等级			
	资深网络安全培训师（5 级）E3	高级网络安全培训师（4 级）E2	网络安全培训师（3 级）E2	初级网络安全培训师（2 级）E1
工作年限	1.网络安全培训及相关专业连续从业 7 年，且近 3 年连续从事本专业； 2.取得网络安全培训从业能力等级 4 级 2 年，且近 3 年连续从事本专业； 3.取得网络安全培训或相关专业博士学位，且近 1 年连续从事本专业； 4.取得网络安全培训或相关专业硕士学位，且近 3 年连续从业本专业； 5.取得国家计算机技术与软件专业技术资格（水平）考试相关高级资格，且近 2 年连续从事本专业。	1.网络安全培训及相关专业连续从业 5 年，且近 2 年连续从事本专业； 2.取得网络安全培训从业能力等级 3 级 2 年，且近 2 年连续从事本专业； 3.取得网络安全培训或相关专业硕士学位，且近 1 年连续从业本专业； 4.取得网络安全培训或相关专业学士学位，且近 2 年连续从事本专业； 5.取得国家计算机技术与软件专业技术资格（水平）考试相关中级资格，且近 2 年连续从事本专业。	1.网络安全培训或相关专业连续从业 3 年，且近 1 年连续从事本专业； 2.取得网络安全培训或相关专业硕士学位及以上； 3.取得网络安全培训或相关专业学士学位，且近 1 年连续从事本专业。	1.网络安全培训及相关专业连续从业 2 年。
工作	1.近 5 年内，设计网络安全培训项目 8 个； 2.近 1 年，累计讲课 400 学时。	1.近 5 年，设计网络安全培训项目 5 个及以上 2.近 1 年，累计讲课 300	1.近 2 年，累计讲课 300 学时。	1.近 2 年，累计讲课 200 学时。

履历		学时。		
工作传承	1.近 3 年，在国家 2 级以上刊物发表本专业或相关专业文章 2 篇； 2.近 1 年，本专业或相关专业的年授课 15 人天。备注：培养新人考核合格 1 人，当年计授课 10 人天。	1.近 3 年，在省市以上刊物发表本专业或相关专业文章 2 篇； 2.近 1 年，本专业或相关专业的年授课 10 人天。备注：培养新人考核合格 1 人，当年计授课 10 人天。	1.近 3 年，在省市以上刊物发表本专业或相关专业文章 1 篇。	1.能运用所需的知识和技能，在他人的指导下完成所承担的工作，并具有一定独立工作能力和实践经历

14 评价过程

14.1 适用对象

网络安全技能技术人才评价适用于申报职业等级评价及从事或准备从事网络安全职业的人员。

14.2 评价方式

对网络安全人才进行评价和定级，评价结果可作为人才能力培养、职业发展等活动的依据。

a) 宜根据 GB/T37696-2019 中能力要素等级及基本要求、能力综合评价模型，结合具体的服务领域，参考本文件内容，建立评价指标体系；

b) 按照以下方式定期对从业人员的各项能力进行评价：

1) 知识：建议主要通过考试等方式进行评价，考试形式包括笔试、机考等；

2) 技能：建议主要通过考试和答辩等方式进行评价；

3) 经验：建议主要通过职业履历鉴定和答辩等方式进行评价。

基于评价结果，组织或个人应根据职业分类和从业人员能力要求，按照附录G，制定从业人员能力培养计划，确定培养目标、内容、方式和周期，并由符合要求的培训师实施培养活动。

附 录 A
（资料性）
通用基础知识词典

通用基础知识词典见表A.1。

表A.1 通用基础知识词典

序号	基础知识	知识编码	知识内容	知识等级描述	
1	计算机硬件基知识	GK01	包括计算机科学基础知识，桌面及外围设备、主机、存储等IT系统的组成、体系结构、工作原理，主机与外设之间的接口技术，常用外部设备，多媒体技术等知识。	K1	了解计算机系统常用IT设备的体系结构以及各主要部件的功能，了解计算机系统基本工作原理。
				K2	理解计算机系统的数据表示、算术和逻辑运算方法，理解计算机系统体系结构、基本工作原理。
				K3	掌握计算机系统的数据表示、算术和逻辑运算方法，掌握计算机系统体系结构、基本工作原理，掌握接口和多媒体相关知识。
				K4	精通计算机系统的数据表示、算术和逻辑运算方法，精通计算机系统体系结构、基本工作原理，精通接口和多媒体相关知识。
2	计算机软件基础知识	GK02	包括计算机软件分类、系统软件、应用软件、程序设计语言和语言处理程序等知识。	K1	了解操作系统知识、程序设计语言、数据库知识、应用软件种类和功能，了解语言处理程序知识。
				K2	理解操作系统知识、程序设计语言、数据库知识、应用软件种类和功能，理解语言处理程序知识。
				K3	掌握操作系统知识、程序设计语言、数据库知识、应用软件种类和功能，掌握语言处理程序知识。
				K4	精通操作系统知识、程序设计语言、数据库知识、应用软件种类和功能，精通语言处理程序知识。
3	数据传输与通信基础知识	GK03	包括数据信号、信道的基本概念，数据通信系统的构成，传输信道特性，数据编码，多路复用技术，数据交换技术，同步控制与差错控制，传输媒体等知识。	K1	熟悉数据通信基本概念，了解数据编码基本知识，熟悉数据通信系统组成，熟悉传输媒体。
				K2	理解数据通信原理，理解数据编码的分类和基本原理，理解多路复用技术的基本原理和应用，理解数据交换技术的基本原理和性能特点。
				K3	掌握数据信号、信道的基本概念，掌握数据通信系统的构成，掌握传输信道特性，掌握数据编码的分类和基本原理，掌握多路复用技术的基本原理和应用，掌握数据交换技术的基本原理和性能特点，掌握同步控制与差错控制方法。
				K4	精通数据通信、数据编码、数据交换知识。

表 A.1 通用基础知识词典（续）

4	计算机网络基础知识	GK04	包括计算机网络的概念、分类和组成，网络拓扑结构，通信协议，开放系统互连参考模型，网络协议，常用网络设备，局域网，广域网连接，网络接入，网络管理等知识。	K1	熟悉计算机网络基本概念，了解网络拓扑结构，了解网络协议，了解常用网络设备。
				K2	理解计算机网络分类和组成，理解网络拓扑结构，理解通信协议的概念，理解开放系统互连参考模型，理解网络协议，熟悉路由器、交换机等网络设备，理解局域网组成、类型和工作原理，理解帧中继、ATM 等广域网连接技术，熟悉网络接入技术、网络管理基础知识。
				K3	掌握计算机网络分类和组成，掌握通信协议的概念，掌握开放系统互连参考模型的结构及各层的功能，掌握 TCP/IP 协议内涵，掌握局域网组成、类型和工作原理，掌握帧中继、ATM 等广域网连接技术，掌握网络接入技术，理解网络管理协议、网络管理命令，熟悉常用网络管理工具和网络管理平台。
				K4	精通网络拓扑结构，精通 TCP/IP 协议，精通局域网和广域网技术，了解下一代网络的发展方向。
5	项目管理基础知识	GK05	项目管理知识是指：为满足项目要求，而在实施过程中将人员、流程、技术、资源进行合理规划、整合、使用的方法论。其中涉及：项目规划设计、范围管理、时间管理、产品生命周期管理、成本管理、质量管理、资源管理、沟通管理、风险管理、相关方管理等方面。	K1	了解项目的规划设计、范围、时间、产品生命周期、成本、资源、风险管理的方法论。
				K2	理解项目的规划设计、范围、时间、产品生命周期、成本、资源、风险管理的方法论，具备进行项目评估及执行项目工作所需要的相关知识。
				K3	掌握项目的规划设计、范围、时间、产品生命周期、成本、资源、风险管理的方法论，具备从事项目管理工作所需要的相关知识。
				K4	精通项目的规划设计、范围、时间、产品生命周期、成本、资源、风险管理的方法论，具备指导他人进行项目管理工作所需要的相关知识。
6	网络安全知识	GK06	包括网络安全基本概念和基本属性，网络安全主要形式，网络安全风险，常用网络安全技术，网络安全管理，网络安全，网络安全等级保护，网络安全法律法规与标准等知识。	K1	了解网络安全基本概念、基本属性、网络安全主要形式和常用网络安全技术。
				K2	理解网络安全风险、常用的网络安全技术、网络安全等级保护内容和网络安全法律法规与标准。
				K3	掌握网络安全风险内容、常用网络安全技术、网络安全等级保护内容和网络安全法律法规与标准。
				K4	精通网络安全风险内容、常用网络安全技术、网络安全等级保护内容和网络安全法律法规与标准。
7	质量管理知识	GK07	包括质量管理的管理方针（目的和原则），管理准则（裁剪原则），管理过程	K1	了解质量管理准则；了解质量管理过程、文档框架。
				K2	理解质量管理方针；理解管理准则；理解质量管理过程、管理方法、管理工具。

表 A.1 通用基础知识词典（续）

7	质量管理知识	GK07	（输入、输出、执行过程），管理方法（PDCA 等），文档框架等知识。	K3	掌握质量管理方针，管理准则；掌握质量管理过程、管理方法、管理工具，掌握质量管理体系知识。
				K4	精通质量管理方针、管理准则、管理过程、管理方法、管理工具，精通质量管理体系知识。

附 录 B
（资料性）
网络安全专业知识词典

网络安全专业知识词典见B.1。

表B.1 网络安全专业知识词典

序号	专业知识	知识编码	知识内容	知识等级描述	
1	应用安全知识	D-PK01	为保障应用程序使用过程和结果的安全，而涉及的相关安全知识。包括应用安全概念、内涵、威胁和保护措施等相关知识；应用安全配置基础知识；常用网络应用服务概念及安全配置相关知识；桌面及外围设备应用安全保护知识。	K1	了解应用安全配置和防护知识、常用网络应用服务及安全配置知识、应用安全保护知识。
				K2	理解应用安全配置和防护知识、常用网络应用服务及安全配置知识、应用安全保护知识。
				K3	掌握应用安全配置和防护知识、常用网络应用服务及安全配置知识、应用安全保护知识。
				K4	精通应用安全配置和防护知识、常用网络应用服务及安全配置知识、应用安全保护知识。
2	网络攻防知识	D-PK02	包括网络协议概念及其安全知识；网络架构安全知识；信息收集与分析相关知识；常见网络攻击方法原理，攻击过程与防范措施等相关知识。包括网络安全测试技术、网络安全技术及相关协议、密码学知识、病毒机制与防护技术及数字鉴别及认证系统。	K1	了解网络协议安全知识、网络架构安全知识、常见网络攻击方法概念。
				K2	理解网络协议安全知识、网络架构安全知识、信息收集与分析方法、理解常见网络攻击方法原理。
				K3	掌握网络协议安全、网络架构安全、信息收集与分析方法；理解常见网络攻击方法及其防范措施。
				K4	精通网络协议安全、网络架构安全、信息收集与分析、常见网络攻击方法及其防范措施。
3	恶意代码防护知识	D-PK03	恶意代码的基本概念，恶意代码的基本原理，恶意代码的主要特征，恶意代码的主要类型，常见的恶意代码攻击模型，恶意代码分析方法，恶意代码的防护原理、技术（如特征码签名技术、主动防御技术等），恶意代码的检测，恶意代码的清除，例如内存检测技术、沙箱技术、主动防护技术等。	K1	了解恶意代码的基本概念、基本原理、主要特征、主要类型。
				K2	理解恶意代码的基本概念、基本原理、主要特征，攻击模式，分析方法，并在一定程度上具备基本的恶意代码防范能力。
				K3	掌握恶意代码的防护原理、分析方法、检测技术，并能独立组织并完成恶意代码的防护工作。
				K4	精通恶意代码的防护技术、检测方法，攻击模型，并能不断改进恶意代码的检测与防护技术，能应对新的恶意代码安全威胁。

表 B.1 网络安全专业知识词典（续）

4	数据安全及灾备知识	D-PK04	为了保护数据存储的安全,而涉及的相关知识，包括存储媒体、数据存储、数据复制、数据快照、数据镜像、数据备份与恢复、数据容灾等相关知识，并了解业界的相关产品。	K1	了解数据存储媒体的分类、数据存储原理及架构，了解数据复制、快照、镜像和数据备份等相关概念。
				K2	理解数据存储架构、存储原理及各类存储媒体的优劣势，理解数据复制、快照、镜像等数据保护技术，理解数据备份和容灾技术，了解相关设备厂商的数据存储和备份产品。
				K3	掌握数据存储系统搭建方法，掌握数据复制、快照、镜像等数据保护技术，掌握数据备份和容灾技术，掌握相关设备厂商的数据存储和备份产品。
				K4	精通数据存储及备份容灾系统搭建方法，精通各类数据复制技术、快照技术、镜像技术等数据保护技术，精通数据备份和容灾技术和相关标准，精通相关设备厂商的数据存储和备份产品。
5	基础软件系统安全知识	D-PK05	为保证基础软件系统的运行所提供的安全技术与控制措施,操作系统安全、数据库安全、中间件安全等知识，包括：中标麒麟、普华等各类操作系统，东方通等各类中间件，达梦、虚谷等数据库安全知识。	K1	了解操作系统安全、数据库安全、中间件安全等知识，如：能够部分地简单地配置操作系统安全功能等。
				K2	理解操作系统安全、数据库安全、中间件安全等知识，如：能够配置操作系统安全、数据库安全、中间件安全功能等。
				K3	掌握操作系统安全、数据库安全、中间件安全等知识，如：能够熟练配置操作系统安全、数据库安全、中间件安全功能等。
				K4	精通操作系统安全、数据库安全、中间件安全等知识，如：能够熟练配置操作系统安全、数据库安全、中间件安全功能，并能根据规范标准等进行系统与全面安全优化与配置，提出具有针对性的解决方案等。
6	物理环境安全知识	D-PK06	为保证信息系统的安全可靠运行所提供的安全运行环境,使信息系统得到物理上的严密保护,从而降低或避免各种安全风险。包括从物理访问控制、防盗窃、防破坏、防雷击、防火、防水、防潮、温湿度控制、电力供应、防电磁辐射等方面保障环境安全的措施与技术的知识。	K1	了解环境管理相关规范，如：GB/T2887-2011《计算机场地通用规范》和 GB/T9361-2011《计算机场地安全要求》等，能分辨环境管理各类设施。
				K2	理解环境管理相关规范，如：GB/T2887-2011《计算机场地通用规范》和 GB/T9361-2011《计算机场地安全要求》等，能操作环境管理各类设施。

表 B.1 网络安全专业知识词典（续）

6	物理环境安全知识	D-PK06		K3	掌握环境管理相关规范，如：GB/T2887-2011《计算机场地通用规范》和 GB/T9361-2011《计算机场地安全要求》等，能熟练操作和维护环境管理系统各类设施。
				K4	精通环境管理相关规范，如：GB/T2887-2011《计算机场地通用规范》和 GB/T9361-2011《计算机场地安全要求》等，能熟练操作和维护环境管理系统各类设施，并按规范设计布置相关环境管理设施。
7	密码学知识	D-PK07	如密码编码和密码分析、密码的基本类型、影响密码安全的基本因素，密码破解的典型方式、公钥密码体制的分类、密钥管理、对称密码的算法、密码协议等知识。	K1	了解密码学基础概念、对称密码算法、非对称密码算法、哈希函数等知识。
				K2	理解密码学基础概念，并在一定程度上具备执行对称加密、非对称加密和数字签名加密等的密码知识。
				K3	掌握密码学概念，并具备能够独立组织对称加密、非对称加密和数字签名加密等的密码知识。
				K4	精通密码学概念，加密算法和密钥管理，并具备对加密方法不断提出创新思想的密码知识。
8	网络安全审计知识	D-PK08	针对与网络安全有关的活动，从外部独立进行相关信息的识别、记录、存储和分析，确保各项活动符合组织已建立的安全策略和操作过程，并评估它们的有效性和准确性，发现安全违规，掌握安全动态，提出改进建议。网络安全审计的具体对象是在组织的网络安全层面上，技术和管理、物理和逻辑等方面的控制措施，包括数据中心物理安全、信息系统脆弱性、应用系统安全、数据库逻辑安全、以及组织的网络安全合规性等进行审核。	K1	了解针对与网络安全有关的活动，从外部独立进行相关信息的识别、记录、存储和分析，确保各项活动符合组织已建立的安全策略和操作过程，并评估它们的有效性和准确性，发现安全违规，掌握安全动态，提出改进建议。
				K2	理解针对与网络安全有关的活动，从外部独立进行相关信息的识别、记录、存储和分析，确保各项活动符合组织已建立的安全策略和操作过程，并评估它们的有效性和准确性，发现安全违规，掌握安全动态，提出改进建议。
				K3	掌握针对与网络安全有关的活动，从外部独立进行相关信息的识别、记录、存储和分析，确保各项活动符合组织已建立的安全策略和操作过程，并评估它们的有效性和准确性，发现安全违规，掌握安全动态，提出改进建议。
				K4	精通针对与网络安全有关的活动，从外部独立进行相关信息的识别、记录、存储和分析，确保各项活动符合组织已建立的安全策略和操作过程，并评估它们的有效性和准确性，发现安全违规，掌握安全动态，提出改进建议。

表 B.1 网络安全专业知识词典（续）

9	网络安全测试技术	D-PK9	主要是针对信息系统及其产品的安全属性，采取动态的手段进行问题发现、符合性和有效性验证。一般包括信息系统测试，漏洞扫描和渗透性测试等。	K1	了解安全测试概念和原理、测试工具、测试技术、测试过程。
				K2	理解安全测试概念和原理、测试工具、测试技术，并在一定程度上具备执行安全测试过程的测试知识。
				K3	掌握安全测试基础、测试工具、测试技术、测试相关的度量和测试过程，并具备能够独立组织测试工作的测试知识。
				K4	精通安全测试基础、测试工具、测试技术、测试相关的度量和测试过程，并具备对测试方法不断提出创新思想的测试知识。
10	网络安全管理体系	D-PK10	依照国际或国家网络安全管理体系相关标准，基于业务风险方法，通过定义范围和方针、业务分析、风险评估、设计、实施等步骤，面向组织建立、实施、运维、监视、评审、保持和改进网络安全体系。	K1	了解依照国际或国家网络安全管理体系相关标准，基于业务风险方法，通过定义范围和方针、业务分析、风险评估、设计、实施等步骤，面向组织建立、实施、运维、监视、评审、保持和改进网络安全体系。
				K2	理解依照国际或国家网络安全管理体系相关标准，基于业务风险方法，通过定义范围和方针、业务分析、风险评估、设计、实施等步骤，面向组织建立、实施、运维、监视、评审、保持和改进网络安全体系。
				K3	掌握依照国际或国家网络安全管理体系相关标准，基于业务风险方法，通过定义范围和方针、业务分析、风险评估、设计、实施等步骤，面向组织建立、实施、运维、监视、评审、保持和改进网络安全体系。
				K4	精通依照国际或国家网络安全管理体系相关标准，基于业务风险方法，通过定义范围和方针、业务分析、风险评估、设计、实施等步骤，面向组织建立、实施、运维、监视、评审、保持和改进网络安全体系。
11	云平台安全知识	D-PK11	基于云平台及云计算，信息在其生命周期内的产生、传输、交换、处理和存储的各个环节的保密性、完整性和可用性等安全状态有关的知识。	K1	了解云平台及云计算技术、体系结构组成、应用等方面的知识，了解云平台及云计算安全体系结构、技术特点、技术应用等方面的知识。
				K2	理解云平台及云计算技术、体系结构组成、应用等方面的知识，理解云平台及云计算安全体系结构、技术特点、技术应用等方面的知识。

表 B.1 网络安全专业知识词典（续）

11	云平台安全知识	D-PK11	基于云平台及云计算，信息在其生命周期内的产生、传输、交换、处理和存储的各个环节的保密性、完整性和可用性等安全状态有关的知识。	K3	掌握云平台及云计算技术、体系结构组成、应用等方面的知识，掌握云平台及云计算安全体系结构、技术特点、技术应用等方面的知识。
				K4	精通云平台及云计算技术、体系结构组成、应用等方面的知识，精通云平台及云计算安全体系结构、技术特点、技术应用等方面的知识。
12	大数据安全知识	D-PK12	基于大数据，信息在其生命周期内的产生、传输、交换、处理和存储的各个环节的保密性、完整性和可用性等安全状态有关的知识。	K1	了解大数据技术、体系结构组成、应用等方面的知识，了解大数据安全体系结构、技术特点、技术应用等方面的知识。
				K2	理解大数据技术、体系结构组成、应用等方面的知识，理解大数据安全体系结构、技术特点、技术应用等方面的知识。
				K3	掌握大数据技术、体系结构组成、应用等方面的知识，掌握大数据安全体系结构、技术特点、技术应用等方面的知识。
				K4	精通大数据技术、体系结构组成、应用等方面的知识，精通大数据安全体系结构、技术特点、技术应用等方面的知识。
13	物联网安全知识	D-PK13	基于物联网，信息在其生命周期内的产生、传输、交换、处理和存储的各个环节的保密性、完整性和可用性等安全状态有关的知识。	K1	了解物联网技术、体系结构组成、应用等方面的知识，了解物联网安全体系结构、技术特点、技术应用等方面的知识。
				K2	理解物联网技术、体系结构组成、应用等方面的知识，理解物联网安全体系结构、技术特点、技术应用等方面的知识。
				K3	掌握物联网技术、体系结构组成、应用等方面的知识，掌握物联网安全体系结构、技术特点、技术应用等方面的知识。
				K4	精通物联网技术、体系结构组成、应用等方面的知识，精通物联网安全体系结构、技术特点、技术应用等方面的知识。
14	工业控制系统安全知识	D-PK14	基于工业控制，信息在其生命周期内的产生、传输、交换、处理和存储的各个环节的保密性、完整性和可用性等安全状态有关的知识。	K1	了解工业控制系统的技术体系结构、应用等方面的知识，了解工业控制系统安全体系结构、技术特点、安全技术应用等方面的知识。
				K2	理解工业控制系统的技术体系结构、应用等方面的知识，理解工业控制系统安全体系结构、技术特点、安全技术应用等方面的知识。

表 B.1 网络安全专业知识词典（续）

14	工业控制系统安全知识	D-PK14	基于工业控制，信息在其生命周期内的产生、传输、交换、处理和存储的各个环节的保密性、完整性和可用性等安全状态有关的知识。	K3	掌握工业控制系统的技术体系结构、应用等方面的知识，掌握工业控制系统安全体系结构、技术特点、安全技术应用等方面的知识。
				K4	精通工业控制系统的技术体系结构、应用等方面的知识，精通工业控制系统安全体系结构、技术特点、安全技术应用等方面的知识。
15	移动应用安全知识	D-PK15	基于移动应用，信息在其生命周期内的产生、传输、交换、处理和存储的各个环节的保密性、完整性和可用性等安全状态有关的知识。	K1	了解移动应用的技术体系结构、应用等方面的知识，了解移动应用安全体系结构、技术特点、安全技术应用等方面的知识。
				K2	理解移动应用的技术体系结构、应用等方面的知识，理解移动应用安全体系结构、技术特点、安全技术应用等方面的知识。
				K3	掌握移动应用的技术体系结构、应用等方面的知识，掌握移动应用安全体系结构、技术特点、安全技术应用等方面的知识。
				K4	精通移动应用的技术体系结构、应用等方面的知识，精通移动应用安全体系结构、技术特点、安全技术应用等方面的知识。
16	区块链安全知识	D-PK16	基于区块链，信息在其生命周期内的产生、传输、交换、处理和存储的各个环节的保密性、完整性和可用性等安全状态有关的知识。	K1	了解区块链的技术体系结构、应用等方面的知识，了解区块链安全体系结构、技术特点、安全技术应用等方面的知识。
				K2	理解区块链的技术体系结构、应用等方面的知识，理解区块链安全体系结构、技术特点、安全技术应用等方面的知识。
				K3	掌握区块链的技术体系结构、应用等方面的知识，掌区块链安全体系结构、技术特点、安全技术应用等方面的知识。
				K4	精通区块链的技术体系结构、应用等方面的知识，精通终端安全体系结构、技术特点、安全技术应用等方面的知识。
17	终端安全知识	D-PK17	基于终端，信息在其生命周期内的产生、传输、交换、处理和存储的各个环节的保密性、完整性和可用性等安全状态有关的知识。	K1	了解终端的技术体系结构、应用等方面的知识，了解终端安全体系结构、技术特点、安全技术应用等方面的知识。
				K2	理解终端的技术体系结构、应用等方面的知识，理解终端安全体系结构、技术特点、安全技术应用等方面的知识。

表 B.1 网络安全专业知识词典（续）

17	终端安全知识	D-PK17	基于终端，信息在其生命周期内的产生、传输、交换、处理和存储的各个环节的保密性、完整性和可用性等安全状态有关的知识。	K3	掌握终端的技术体系结构、应用等方面的知识，掌终端安全体系结构、技术特点、安全技术应用等方面的知识。
				K4	精通终端的技术体系结构、应用等方面的知识，精通终端安全体系结构、技术特点、安全技术应用等方面的知识。
18	网络攻击溯源知识	D-PK18	针对网络对目标系统的攻击方式、攻击目标、攻击使用的弱点，对攻击者所使用的工具、利用的漏洞，进一步可以对攻击者所使用的网络地址进行跟踪和反渗透，构建攻击者画像的相关知识。	K1	了解网络攻击溯源的理论和知识，了解攻击痕迹分析、攻击路径分析、攻击反制技术、攻击者画像等方面知识。
				K2	理解网络攻击溯源的理论和知识，理解攻击痕迹分析、攻击路径分析、攻击反制技术、攻击者画像等方面知识。
				K3	掌握网络攻击溯源的理论和知识，掌握攻击痕迹分析、攻击路径分析、攻击反制技术、攻击者画像等方面知识。
				K4	精通网络攻击溯源的理论和知识，精通攻击痕迹分析、攻击路径分析、攻击反制技术、攻击者画像等方面知识。
19	网络安全流量知识	D-PK19	针对网络中抓取的流量数据，对流量中的内容进行解密、解构、分析，获得流量中有效的信息，能够分离出正常业务访问和业务操作流量数据，分辨对目标系统有害的数据包，同时可以对流量中数据的有效性进行验证和识别的线管知识。	K1	了解网络流量分析的知识，了解流量解密、流量去重、流量协议、流量统计、流量优化等技术方面知识。
				K2	理解网络流量分析的知识，理解流量解密、流量去重、流量协议、流量统计、流量优化等技术方面知识。
				K3	掌握网络流量分析的知识，掌握流量解密、流量去重、流量协议、流量统计、流量优化等技术方面知识。
				K4	精通网络流量分析的知识，精通流量解密、流量去重、流量协议、流量统计、流量优化等技术方面知识。

附 录 C
（资料性）
通用相关知识词典

通用相关知识词典见表C.1。

表C.1 通用相关知识词典

序号	相关知识	知识编码	知识内容	知识等级描述	
1	营销、策划基础知识	RK01	包括公共关系学、客户关系管理、市场营销、贸易学、商务策划的内容和方法。	K1	了解市场营销、贸易学的基本概念、要素。
				K2	了解客户关系管理、市场营销、贸易学的基本内容。
				K3	了解公共关系学、客户关系管理、市场营销、贸易学、商务策划等知识内容。
				K4	具备商务策划活动的组织、流程与营销管理理论基础。
2	知识产权知识	RK02	包括《著作权法》、《专利法》、《知识产权海关保护条例》、《商标法集成电路布图设计保护条例》、《展会知识产权保护办法》、《关于中华人民共和国知识产权海关保护条例的实施办法》《著作权集体管理条例》等法律法规。	K1	了解相关知识产权法律及涉及范围。
				K2	理解相关知识产权法律，能够在工程中考虑法律的因素。
				K3	掌握工作相关法律知识，能够提前在工作中避免触犯相关法律条文风险。
				K4	精通相关的全部法律知识，并就条文范围内，制定出组织风险防范应对机制。
3	劳动法知识	RK03	包含劳动合同法和地方劳动管理相关规定、以及工会组织条例的有关条文内容。	K1	了解劳动法中关于劳动合同的基本规定。
				K2	理解劳动法中劳动合同签订到解除的基本规定，并能维护基本权益。
				K3	掌握劳动法外，了解其他有关劳动法管理条例－劳动法解释、《劳动保障监察条例》、竞业管理、工会组织管理等。
				K4	精通劳动法，能够运用劳动法知识，指导他人遵守有关法律规定。
4	国家信息技术服务相关法律、法规	RK04	包括《计算机软件保护条例》、《中华人民共和国计算机信息系统安全保护条例》《关于加强中国公用计算机互联网chinanet网络安全管理的通知》《计算机信息网络国际联网安	K1	了解工作相关法律及涉及范围。
				K2	理解工作相关法律，能够在工程中考虑法律的因素。
				K3	掌握工作相关法律知识，能够提前在工作中避免触犯相关法律条文风险。

表 C.1 通用相关知识词典（续）

4	国家信息技术服务相关法律、法规	RK04	全保护管理办法》、《中华人民共和国刑法》、《中国公用计算机互连网国际联网管理办法》、《信息网络传播权保护条例》、《合同法》、《对外贸易法》中有关信息技术服务的相关法律法规的规定。	K4	精通相关的全部法律知识，并就条文范围内，制定出公司风险防范应对机制。

附 录 D
（资料性）
通用基本技能词典

通用基本技能词典见表D.1。

表D.1 通用基本技能词典

序号	基本技能	技能编码	技能内容	技能等级描述	
1	计算机硬件基础应用能力	BS01	对桌面及外围设备、服务器、存储备份、办公设备等硬件设备的应用能力；掌握计算机硬件的各种功能，可应用于日常办公与作业。	S1	在他人协助下,能够参与计算机硬件的基础应用工作。
				S2	能够完成计算机硬件的基础应用工作;使用计算机硬件完成相关工作。
				S3	能够组织计算机硬件的基础应用工作;具备指导他人使用计算机硬件完成相关工作的能力。具备参与编写组织内计算机硬件基础应用规范与指南的能力。
				S4	能够组织计算机硬件的基础应用工作;具备指导他人使用计算机硬件完成相关工作的能力。具备编写组织内计算机硬件基础应用规范与指南的能力,对计算机硬件基础应用工作给出专家级意见。
2	计算机软件基础应用能力	BS02	对操作系统、中间件、数据库、基础软件的应用能力，包括：中标麒麟、普华等各类操作系统，东方通等各类中间件，达梦、虚谷等数据库常用的备份软件，集群软件等。	S1	在他人协助下,能够参与计算机软件的基础应用工作。
				S2	能够完成计算机软件的基础应用工作;使用计算机软件完成相关工作。
				S3	能够组织计算机软件的基础应用工作;具备指导他人使用计算机软件完成相关工作的能力。具备参与编写组织内计算机软件基础应用规范与指南的能力。
				S4	能够组织计算机软件的基础应用工作;具备指导他人使用计算机软件完成相关工作的能力。具备编写组织内计算机软件基础应用规范与指南的能力,对计算机软件基础应用工作给出专家级意见。
3	计算机网络基础应用能力	BS03	对网络基础设备、架构、技术的应用能力；主流网络产品的应用，如cisco、huawei、h3c、天融信、启明星辰、绿盟等。	S1	在他人协助下，能够参与网络基础应用工作。
				S2	能够完成网络基础应用工作;使用网络完成相关工作。

表 D.1 通用基本技能词典（续）

3	计算机网络基础应用能力	BS03	各种组网架构的应用，如局域网、城域网、广域网。网络tcp/ip协议，sdh、mpls、vpn等技术的应用。	S3	能够组织网络的基础应用工作;具备指导他人使用网络完成相关工作的能力。具备参与编写组织内网络基础应用规范与指南的能力。
				S4	能够组织网络的基础应用工作;具备指导他人使用网络完成相关工作的能力。具备编写组织内网络基础应用规范与指南的能力,对网络基础应用工作给出专家级意见。
4	文档撰写能力	BS04	熟知各类常规商务文书的写作，掌握一定专业技术资料的编写能力，文笔流畅、简洁，标准化。	S1	在他人协助下，能够参与各类常规商务文书、专业技术资料等文档的编写工作。
				S2	能够完成各类常规商务文书、专业技术资料等文档的编写工作。
				S3	能够组织各类常规商务文书、专业技术资料等文档的编写工作;具备指导与评审他人进行文档编写的能力。
				S4	能够组织各类常规商务文书、专业技术资料等文档的编写工作;具备指导他人进行文档编写的能力。具备组织文档编写规范与指南的能力，对于关键文档具备组织评审工作的能力,对文档编写工作给出专家级意见。
5	外语应用能力	BS05	对外语沟通、文档阅读及书写的能力，使用外语完成日常工作。	S1	能够参与外语的沟通工作；在他人协助下，完成简单的日常沟通。
				S2	能够完成外语的沟通工作；完成外语沟通、文档阅读及简单书写反馈。
				S3	能够组织外语的沟通工作;具备指导他人完成外语沟通、文档撰写及阅读工作的能力。
				S4	能够组织外语的沟通工作;具备指导他人完成外语沟通、文档撰写及阅读工作的能力。具备编写组织内外语应用规范与指南的能力,对外语应用工作给出专家级意见。

附 录 E
（资料性）
网络安全专业技能词典

网络安全专业技能词典E.1。

表E.1 网络安全专业技能词典

序号	专业技能	技能编码	技能内容	技能等级描述	
1	网络安全测试	D-PS01	根据软件项目规范编制测试计划，设计测试数据和示例，完成项目模块测试、系统测试，跟踪、分析发现的问题，评估解决方案的合理性。	S1	在他人指导下，组织网络安全测试，参与准备和搭建测试环境，根据测试设计文档，参与执行所承担功能模块的测试过程，协助记录测试结果并验证测试的执行；协助提交缺陷报告，并反馈和跟踪缺陷的修改。
				S2	能够独立工作，可以完成大部分的如下任务：网络安全测试的组织，准备和搭建测试环境，按照测试设计文档，执行所承担功能模块的测试过程，提交缺陷报告；对开发人员修改过的缺陷进行测试确认，形成测试报告。
				S3	能够带领其他人有效完成安全测试工作。
				S4	能够给出专家级的意见，能够领导其他人成功完成安全测试工作。
2	网络安全风险评估	D-PS02	对信息资产面临的威胁、存在的弱点、造成的影响，以及三者综合作用而带来风险的可能性进行评估。	S1	在他人指导下，完成网络安全风险评估。
				S2	能够独立工作，可以完成大部分的网络安全风险的评估工作。
				S3	能够带领其他人有效掌握各种网络安全风险评估方法，在准确识别风险因素的基础上，通过制定网络安全方针，采取适当的控制目标与控制方式对风险进行控制，使风险被避免、转移或降至一个可被接受的水平。
				S4	能够给出专家级的意见，能够领导其他人有效分析和识别复杂网络信息系统中的风险因素，综合应用各种工具及分析方法对网络风险进行定性定量分析得出准确的网络安全风险结论，并制定出周密的风险控制实施计划。
3	需求分析	D-PS03	通过收集、分析、导出的方法，将客户、业务、用户的需求转换为对应的（软件）系统需求的过程。	S1	在他人指导下，能够参与系统（或产品）需求的获取工作；协助进行业务数据整理与分析工作。
				S2	能够独立工作，可以完成大部分的系统（或产品）需求的获取工作，规范化描述系统的功能需求和非功能需求。

表 E.1 网络安全专业技能词典（续）

3	需求分析	D-PS03	通过收集、分析、导出的方法，将客户、业务、用户的需求转换为对应的（软件）系统需求的过程。	S3	能够带领其他人有效组织系统（或产品）需求的获取工作；构建和完善系统的功能需求和非功能需求的描述标准；遵循 UI 设计和规范，参与构建界面原型；编写用户手册。
				S4	能够给出专家级的意见，能够领导其他人组织系统（或产品）需求的获取工作；主持构建和完善系统的功能需求和非功能需求的描述标准；能够遵循 UI 设计和规范，参与构建界面原型；组织编写并检查用户手册。
4	网络安全规划设计	D-PS04	依据相关标准以及行业监管要求，从物理、网络、系统、应用、数据、终端等层面进行网络安全防护体系规划。	S1	在他人指导下，能够参与对系统进行风险评估，并在评估基础之上，制定相应的网络安全策略；能够从物理、网络、系统、应用、数据、终端等任意某个层面进行中小型企事业单位的网络安全防护体系规划。
				S2	能够独立工作，可以完成大部分的如下工作：进行信息系统安全现状调查与分析，制定编写信息系统安全建设规划方案设计；从物理、网络、系统、应用、数据、终端等任意某个层面进行大型企事业单位（或集团性公司）的网络安全防护体系规划。
				S3	能够带领其他人根据公司设定的安全目标，定义安全模型，设计安全策略。对网络和系统进行安全风险分析、能提出合理化安全建议和安全规划，针对目标客户需求，提供安全有效地设计方案，从物理、网络、系统、应用、数据、终端等多层次构建网络安全防护体系。
				S4	能够给出专家级的意见，能够领导其他人承担大型企事业单位（或集团性公司）的网络安全规划，依据国内外相关标准以及行业监管要求，从物理、网络、系统、应用、数据、终端等多层次构建网络安全防护体系。
5	安全管理体系建设	D-PS05	结合国内外相关标准以及行业监管要求，完成企事业单位的网络安全管理体系的方针、策略、组织、人员等方面的规划设计、实施和持续改进	S1	在他人指导下，能够参与明确网络安全建设工作的内容和重点，参与制定网络安全总体策略，结合国内外相关标准以及行业监管要求，对中小型企事业单位现有安全管理体系进行独立审核，通过差距分析分析。

表 E.1 网络安全专业技能词典（续）

5	安全管理体系建设	D-PS05	结合国内外相关标准以及行业监管要求，完成企事业单位的网络安全管理体系的方针、策略、组织、人员等方面的规划设计、实施和持续改进	S2	能够独立工作，可以成功完成监督安全制度及技术执行，持续改进和完善公司安全体系，结合国内外相关标准以及行业监管要求，通过独立审核、差距分析，能够协助中小型企事业单位完成网络安全管理体系的制度及流程。
				S3	能够带领其他人完成公司安全体系建设，充分参考和借鉴国际网络安全管理的相关标准，从多个维度建立一套完整的网络安全管理体系。结合国内外相关标准以及行业监管要求，通过独立审核、差距分析，能够协助中小型企事业单位完成网络安全管理体系的方针、策略、组织、人员等方面的规划设计。
				S4	能够给出专家级的意见，能够领导其他人根据信息系统安全保障评估的结果进行改进，形成满足信息系统安全保障需求的可持续改进的信息系统安全保障能力。信息系统安全保障需要覆盖信息系统的整个生命周期，形成持续改进的信息系统安全保障能力。结合国内外相关标准以及行业监管要求，通过独立审核、差距分析，能够协助大型企事业（或集团性公司）单位完成网络安全管理体系的方针、策略、组织、人员、制度流程等方面的规划设计。
6	系统建模及架构设计能力	D-PS06	分析面临的威胁和潜在风险，编制模型和应对策略制定网络安全方案和应对措施设计网络安全系统的体系结构根据系统和系统组件的需求，提出提升和完善计划。	S1	在他人指导下，能够确定、协调系统的项目相关人员；对相关工作结果能够有清晰的文档描述并存档。
				S2	能够独立工作，可以领导与协调系统相关工作；定义网络安全规范并规范化描述系统的功能需求和非功能需求；有效管理网络安全需求、维护需求矩阵。
				S3	能够带领其他人把握相关安全领域的产品和系统的定义，并参与组织相关的评审；能够确定网络安全系统边界、系统的主要特性、能实现的功能等。
				S4	能够给出专家级的意见，能够领导其他人完成系统建模及架构设计的工作。
7	网络安全评估分析	D-PS07	对信息化系统的安全设备、网络及业务系统进行数据收集、通过使用漏洞扫描、网管系统及其他的专业评估工具对系统进行分析。	S1	熟在他人指导下，能够悉发现信息化系统的安全风险并定期统计。
				S2	能够独立工作，可以识别不安全因素及进行数据分析，得出分析报告，提出安全保护解决思路。
				S3	能够带领其他人，有效地对中大型系统的整体网络安全性进行检查分析，检查分析对象包括安全管理制度、安全保护技术、业务数据安全保护流程等，并对此提出详细解决方案。

表 E.1 网络安全专业技能词典（续）

7	网络安全评估分析	D-PS07	对信息化系统的安全设备、网络及业务系统进行数据收集、通过使用漏洞扫描、网管系统及其他的专业评估工具对系统进行分析。	S4	能够给出专家级的意见，能够领导其他人进行网络安全评估分析，对得到的评估分析结果进行审核和评价，对复杂信息化系统的细节性安全技术指标进行划分和检查，得到更加详细的分析报告并提出解决方案。
8	网络安全加固	D-PS08	主机加固、数据库加固、网站应用加固、应用系统加固、网络架构加固优化、域架构优化、应用系统架构优化（流程状态调查、制定加固方案、实施加固、生成加固报告）	S1	在他人的指导下，完成网络安全加固的工作。
				S2	能够独立工作，可以完成大部的网络安全加固工作。
				S3	能够带领其他人有效完成网络安全加固工作，满足客户的需求。
				S4	能够给出专家意见，领导其他人高效完成网络安全加固工作。
9	工程项目管理	D-PS09	项目规划设计、范围管理、时间管理、产品生命周期管理、成本管理、质量管理、资源管理、沟通管理、风险管理、相关方管理等方面。	S1	在他人的指导下，能够认识自身在项目中的角色；通过已有的项目管理基本知识，实施工程项目管理的工作。
				S2	能够独立工作，可以完成工程项目管理的大部分工作。
				S3	能够带领其他人，通过管理活动，有效保证项目相关过程及因素符合项目目标。
				S4	能够给出专家意见，领导其他人对若干项目进行管理。
10	网络渗透测试	D-PS10	对信息系统进行渗透测试，找出系统的漏洞。包括黑盒渗透、白盒渗透，以及内网，外网的测试。	S1	在他人的指导下，能够搭建通用的测试环境，完成测试工作。
				S2	能够独立工作，可以完成对客户的测试需求，撰写渗透测试报告。
				S3	能够带领其他人，分析扫描结果和入侵记录，查找安全漏洞，针对客户网站、服务器等系统存在的漏洞进行修补，为网络工程师、操作系统管理员提供安全指导和漏洞修复建议，并督促实施。熟练使用各种安全扫描，渗透工具。
				S4	能够给出专家意见，领导其他人帮助客户进行必要的安全加固和应急响应、应急支撑。熟悉挂马、黑链等黑客惯用手法并进行防护。根据客户需求规划渗透测试方案。

表 E.1 网络安全专业技能词典（续）

11	网络安全态势分析	D-PS11	包括数据采集、数据预处理、事件关联和目标识别、态势评估、威胁评估、响应与预警、态势可视化显示、过程优化控制与管理。	S1	在他人的指导下，能够执行网络安全态势分析。
				S2	能够独立工作，可以成功完成大部分的网络安全态势分析工作。
				S3	能够带领其他人，有效地完成网络安全态势分析。
				S4	能够给出专家意见，领导其他人成功完成网络安全态势分析。
12	应急响应	D-PS12	对网络安全事件能够有效识别、预警、处置、组织开展恢复并产生有效响应。	S1	在他人指导下能够开展应急响应的部分工作。
				S2	能够独立工作，可以成功在应急响应中解决数据恢复、检测、遏制等关键步骤的技术工作。
				S3	能够带领其他人，有效地组织开展应急响应工作。
				S4	能够给出专家意见，领导其他人成功制定与目标系统相适应的应急响应方案。
13	渗透工具的使用及研发	D-PS13	包括网络扫描工具、通用漏洞检测工具以及自主研发渗透工具。	S1	在他人指导下能够熟练使用常见的几种渗透工具。
				S2	能够独立工作，能够掌握主流的渗透工具的使用，完成部分的渗透工具的研发。
				S3	能够带领其他人，熟练使用各种渗透工具，发现有工具的不足，有效完成渗透工具的研发。
				S4	能够给出专家意见，领导其他人完善，开发渗透工具。
14	网络安全审计	D-PS14	针对与网络安全有关的活动，从外部独立进行相关信息的识别、记录、存储和分析，确保各项活动符合组织已建立的安全策略和操作过程，并评估它们的有效性和准确性，发现安全违规，掌握安全动态，提出改进建议。	S1	能够根据审计计划，在他人指导下完成审计任务的执行，记录审计过程和结果，协助编辑审计报告。
				S2	能够根据审计章程，参与编写审计计划，能独立执行审计任务，记录审计过程和结果，编写审计报告。
				S3	能够编写审计章程并指导审计计划的编写，能够指导审计过程，审核审计报告。
				S4	能够指导审计章程的编写并评审审计章程，提炼、改进网络安全审计方法与技术，优化审计流程。
15	信息系统工程监理	D-PS15	依据国家批准的信息化工程项目建设文件、有关工程建设的法律法规和工程建设监理合同及其他工程建	S1	在他人指导下，能够完成检查类监理工作。
				S2	能够在个别技术方向上独立开展监理工作，对项目建设过程中的问题能够及时发现，并能够运用监理手段确保项目有效推进。

表 E.1 网络安全专业技能词典（续）

15	信息系统工程监理	D-PS15	设合同，尤其是依据网络安全方面的标准和要求，在工程建设各个阶段向建设单位提供相关咨询，并协助建设单位实施专业化的网络安全	S3	能够带领其他人，开展项目监理工作，对项目中的问题能够及时发现并准确定位，有效确保项目整体质量。
				S4	能够给出专家意见，领导其他人成功开展项目监理，在项目建设中存在质量进度等方面发挥关键作用。
16	安全产品设计	D-PS16	理解客户业务流程，确认项目范围，获取、分析、定义、确认、验证客户需求，根据软件架构人员的架构设计，分析、设计适合客户业务需求的软件系统。	S1	在他人指导下，能够确定、协调系统的项目干系人、对有待解决的问题达成一致；对相关工作结果能够有清晰的文档描述并存档。
				S2	能够独立工作，能够协调系统/产品的需求获取工作；定义软件需求规范并规范化描述系统的功能需求和非功能需求；能够有效管理软件需求、维护需求矩阵。
				S3	能够带领其他人，把握相关领域的产品线功能的定义，确定系统边界、系统的主要特性、质量范围。
				S4	能够给出专家意见，领导其他人成功产品的设计工作。
17	云平台安全技术	D-PS17	云平台及云计算安全脆弱性分析、安全需求分析、安全防护体系设计与实施。	S1	在他人的指导下，能够进行云平台及云计算安全技术实施。
				S2	能够独立工作，可以成功完成云平台及云计算安全技术规划、实施、检查。
				S3	能够带领其他人，有效地完成云平台及云计算安全技术规划、实施、检查、处置。
				S4	能够给出专家意见，领导其他人成功完成云平台及云计算安全技术规划、实施、检查、处置。
18	大数据安全技术	D-PK18	大数据安全脆弱性分析、安全需求分析、安全防护体系设计与实施。	S1	在他人的指导下，能够进行大数据安全技术实施。
				S2	能够独立工作，可以成功完成大数据安全技术规划、实施、检查。
				S3	能够带领其他人，有效地完成大数据安全技术规划、实施、检查、处置。
				S4	能够给出专家意见，领导其他人成功完成大数据安全技术规划、实施、检查、处置。
19	物联网安全	D-PS18	联网安全脆弱性分析、安全需求分析、安全防护体系设计与实施。	S1	在他人的指导下，能够执行物联网安全的实施。
				S2	能够独立工作，可以成功完成物联网网络安全规划、实施、检查。

表 E.1 网络安全专业技能词典（续）

19	物联网安全	D-PS18	联网安全脆弱性分析、安全需求分析、安全防护体系设计与实施。	S3	能够带领其他人，有效地完物联网网络安全规划、实施、检查、处置。
				S4	能够给出专家意见，领导其他人成功完物联网网络安全规划、实施、检查、处置。
20	工业控制系统安全	D-PS19	工业控制系统安全脆弱性分析、安全需求分析、安全防护体系设计与实施。	S1	在他人的指导下，能够执行工业控制系统安全的实施。
				S2	能够独立工作，可以成功完成工业控制系统网络安全规划、实施、检查。
				S3	能够带领其他人，有效地完成工业控制系统网络安全规划、实施、检查、处置。
				S4	能够给出专家意见，领导其他人成功完成工业控制系统网络安全规划、实施、检查、处置。
21	移动应用架构设计能力	D-PS21	移动应用架构分析及设计。	S1	在他人的指导下，能够进行移动应用架构部分设计。
				S2	能够独立工作，可以成功进行移动应用架构设计、检查。
				S3	能够带领其他人，有效地完成移动应用架构设计、规划、实施、检查。
				S4	能够给出专家意见，领导其他人成功完成移动应用架构设计、规划、实施、检查。
22	移动应用安全技能	D-PS22	移动应用安全脆弱性分析、安全需求分析、安全防护体系设计与实施。	S1	在他人的指导下，能够执行移动应用安全的实施。
				S2	能够独立工作，可以成功完成移动应用安全规划、实施、检查。
				S3	能够带领其他人，有效地完成移动应用安全规划、实施、检查、处置。
				S4	能够给出专家意见，领导其他人成功完成移动应用安全规划、实施、检查、处置。
23	区块链安全技能	D-PS23	区块链安全脆弱性分析、安全需求分析、安全防护体系设计与实施。	S1	在他人的指导下，能够执行区块链安全的实施。
				S2	能够独立工作，可以成功完成区块链安全规划、实施、检查。
				S3	能够带领其他人，有效地完成区块链安全规划、实施、检查、处置。
				S4	能够给出专家意见，领导其他人成功完区块链安全规划、实施、检查、处置。
24	网络安全数据处理	D-PS24	在数据处理（收集、存储、使用、加工、传输	S1	在他人的指导下，能够执行数据安全处理。

表 E.1 网络安全专业技能词典（续）

24	网络安全数据处理	D-PS24	、提供、公开）过程中，满足相关安全性要求。	S2	能够独立工作，可以成功完成数据安全处理。
				S3	能够带领其他人，有效地完成数据安全处理。
				S4	能够给出专家意见，领导其他人成功完成数据安全处理。
25	供应链安全测试能力	D-PS25	供应链安全脆弱性分析、安全需求分析、安全防护体系设计与实施。	S1	在他人的指导下，能够完成供应链安全脆弱性分析。
				S2	能够独立工作，可以成功完成供应链安全脆弱性分析、安全需求分析。
				S3	能够带领其他人，可以成功完成供应链安全脆弱性分析、安全需求分析
				S4	能够给出专家意见，领导其他人成功完成供应链安全脆弱性分析、安全需求分析、安全防护体系设计与实施。
26	移动终端测试能力	D-PS26	对移动终端功能性、安全性、兼容性等内容进行测试。	S1	在他人的指导下，能够对移动终端进行功能性、安全性、兼容性等内容进行测试。
				S2	能够独立工作，可以完成对移动终端的功能性、安全性、兼容性等内容进行测试。
				S3	能够带领其他人，有效地完成对移动终端的功能性、安全性、兼容性等内容进行测试。
				S4	能够给出专家意见，领导其他人成功完成对移动终端的功能性、安全性、兼容性等内容进行测试。
27	网络攻击溯源能力	D-PS27	对网络安全攻击的攻击方式、攻击目标、攻击点、攻击工具溯源，对攻击者进行跟踪、反渗透，构建攻击者画像。	S1	在他人的指导下，能够执行对攻击方式、攻击目标、攻击点、攻击工具溯源。
				S2	能够独立工作，可以成功完成对攻击方式、攻击目标、攻击点、攻击工具溯源，对攻击者进行跟踪、反渗透。
				S3	能够带领其他人，有效地完成对攻击方式、攻击目标、攻击点、攻击工具溯源，对攻击者进行跟踪、反渗透，构建攻击者画像。
				S4	能够给出专家意见，领导其他人成功对攻击方式、攻击目标、攻击点、攻击工具溯源，对攻击者进行跟踪、反渗透，构建攻击者画像。
28	网络安全流量分析能力	D-PS28	网络安全流量抓取、分析、取证	S1	在他人的指导下，能够执行网络安全流量抓取、分析。
				S2	能够独立工作，可以成功完成网络安全流量抓取、分析、取证。

表 E.1 网络安全专业技能词典（续）

28	网络安全流量分析能力	D-PS28	网络安全流量抓取、分析、取证	S3	能够带领其他人，有效地完成网络安全流量抓取、分析、取证。
				S4	能够给出专家意见，领导其他人成功完成网络安全流量抓取、分析、取证。

附 录 F
（资料性）
软技能词典

软技能词典见表F.1。

表F.1 软技能词典

序号	软技能	技能编码	技能内容	技能等级描述	
1	沟通能力	SS01	清楚地传达和接受信息来满足所有的需求，可能包含倾听、解释说明、系统阐述和评论：口头的、非口头的、书面的和或电子信件。	S1	有效地表达自己。不管采用什么媒介，沟通的方式准确、及时和易于理解；以一种公开的和坦诚的方式共享信息。
				S2	有效地倾听。能够深查理解没有表达出的或表达不清楚的思想、关系的事情或感受；能够准确理解身体语言和其他非口头的暗示，并运用这种理解来形成和做出一种适当的反应；在做出结论之前，解释信息来检核理解是否准确。
				S3	理解潜在的问题。试图理解他人的理论观点；理解他人为什么在特定的环境下以一定的方式表现出来某种行为；运用信息来更好理解一个人或确定直接的沟通需求；以一种促进长期解决方案的方式来响应他人关心的事情。
				S4	在不同的环境下采用相适应的沟通方式。运用对当前潜在问题的理解，识别最有效传递信息的方式/方法；运用不同传递信息的方式来增强沟通的清晰度和意义；从接收者的角度来理解信息，预期他人的反应，并灵活调整自身的行为来做出适当的反应。
2	学习能力	SS02	以最快的速度、在最短的时间内把学习的新知识和获得的新信息应用在工作中。	S1	初学者以最快的速度，在最短的时间内：学习者对该领域有初步的认识；对概念和思想有纯理性的认识，但无法轻易看清“问题”，更无法对问题进行分析；可以根据规范指导应用新的或不熟悉的技术。
				S2	合格学习者以最快的速度，在最短的时间内学习者在一些真实场景下可以进行初步的操作；对专业领域范围有更多的认识，清楚自己在该学科知识上的欠缺；只要情况和他们研究过的案例相似，或者是他们曾经遇到过的，就可以放心让他们按照规定的步骤执行。
				S3	将学习到的系列知识应用到工作中，以最快的速度，在最短的时间内；学习者对该领域的系列知识已经有了全面的理性接触，补充指导和提示将不再对他们能力的提高有什么帮助；可以超越简单地按照规则和程序行事，

表 F.1 软技能词典（续）

2	学习能力	SS02	以最快的速度、在最短的时间内把学习的新知识和获得的新信息应用在工作中。	S3	能够根据环境的变化对技术方法做相应的调整，因为他们已经将这些技术内化了；能结合环境，通过持续不断地实践来获得经验，并在该能力上获得扎实的进步；能够指导别人/实习生进行学习。
				S4	专业性地思考。对问题有了全面的把握，可以运用专业工具和方法，令人放心地处理任何一种情况；能够打破常规，超越目标，他们的经验已经全部内化；能够组织团队进行学习，并在此过程中，传播专业化的思考/想法；通过跟其他专家/客户的相互交流（如在指导新员工、客户需求调研等）中继续学习，并形成专业化的建议或解决方案。
3	问题判断与解决能力	SS03	针对问题能够识别出一种解决方案，并能够评估选择方案和隐含的含义。	S1	分解问题。为识别必要的任务或活动，把问题分解成简单的组成部分（例如，一个“任务”清单）。
				S2	看清问题的基本关系。分析问题中几个部分之间的关系，并按重要优先级排列任务的次序；认清原因和影响的关系（即因果式的思考）；看清一个问题或情形不同的组成部分之间的简单联系和关系。
				S3	看清问题的多重关系。以一种系统的方法把复杂的情形分解成可管理/处理的部分；分析问题中若干部分之间的关系及若干可能的目标和行动结果，并采取相应的措施或行动（例如，这种变化将如何影响这个项目以及涉及的策略和人员）；通常预期可能遇到的障碍，提前对下一步进行思考和准备：获取新的信息并运用知识来分析问题和解决问题。
				S4	做出综合的计划或分析。识别多种解决方案并权衡每种解决方案对提高成果的价值；把复杂问题剥离成多层关系：运用几种分析技术来分解复杂的情形或问题，形成一个解决方案；表现出出色的可估价的判断，这种判断不仅仅是做出结论。
4	创新能力	SS04	运用新颖和创造性的思考来进行改进和或形成和发展起新的方法方式。	S1	增强过程或产品。寻求能把自身工作做得更好的各种方式，并贯彻执行；通过参与积极认真的讨论，不断地探寻和挑战传统思维（即一贯做事的方式）的合适性和质量。
				S2	形成新的工作方式。通过在该领域内以一种新的和不同的方式做事（但对工作单元或组织未必是新的），从而对工作效率和目标产生积极影响；寻求改进活动及其结果的各种方式，并予以贯彻执行；针对新的环境调整现有的过程或产品，在工作中应用新的技术。

表 F.1 软技能词典（续）

4	创新能力	SS04	运用新颖和创造性的思考来进行改进和或形成和发展起新的方法方式。	S3	形成部门新的工作方式。通过以新的或不同的方式（对部门来说）做事而提升绩效，寻求方式来改进和超越工作单元的活动及其结果；激励和奖励别人的创新，在自身工作里采用跨边界的心理状态来鼓励别人采用同类方式；正式或非正式领导执行过程。
				S4	形成组织新的工作方式，创建创新文化。通过可能对组织来说是以独特的、开先河或新的做事方式来提升绩效，突出创新和变革对整个组织绩效和/或具体领域绩效的显著利益；在整个领域里积极共享信息和资源来更好地提升组织的能力，运用创造性的方法来建立一种鼓励创新、鼓励对变化的敏锐性和经验学习的氛围；在分析关键的趋势和复杂（或有分歧的）问题之后，制定出创造性的解决方案，并以一种能帮助他人产生突破性想法、新的视角和新的机会来采取行动。
5	知识分享能力	SS05	指对相关专业知识（包括技术、职业或管理方面）向别人进行延伸、利用和传播的动机。	S1	愿意分享自己的成果专业知识。愿意回应别人提出的问题或请求，并以专业的角色传播现有的知识信息；分享的专业知识影响覆盖的范围在 1-3 个同事或客户。
				S2	能够理解别人的需求，并应用自身的专业知识帮忙解决。不仅仅是回应/回答问题，能够应用自身的专业知识帮助解决他人的专业问题；提供技术协助，如同“自由顾问”，提供个人的专业知识以提升绩效，或解决他人的技术问题。
				S3	成为组织内专业知识的传播者。愿意通过各种公开的途径和方式，成为组织内专业知识的传播者，提升组织绩效和技术能力；自身的专业知识影响/覆盖一个项目组或部门或某个特定单元。
				S4	推动分享和传播新知识。犹如专业传教士或变革顾问一般积极地在部门或公司内部传播新专业知识；在专业或技术期刊上，发表介绍新技术或新方法的文章；新技术/新方法影响的范围为整个公司或社会专业领域。

附 录 G
（资料性）
能力培养

应根据本文件要求，实施设计与开发培训，并根据知识、技能和经验的要求确定培训标准学时。

G.1 培养内容

能力培养的内容应包括：

a) 基础知识、专业知识和相关知识培养；
b) 基本技能、专业技能和软技能培养；
c) 基于工作实践的经验积累。

G.2 培养阶段和培养方式

培养分为职前培养和在职培养两个阶段，构成从业人员不同阶段和能力水平的终身教育体系。

a) 职前培养方式
包括：理论教学、理论与实践一体化教学、生产性实训、企业实习等方式。
a) 在职培养方式在职培养方式包括：
1）内部培训或外部培训；
2）在岗培训或脱岗培训；
3）学历提升、课堂培训、项目实践或导师辅导等。

G.3 培养活动

组织或个人应根据从业人员能力要求制定从业人员能力培养计划，确定培养目标、内容、方式和周期，并由符合GB/T 37696-2019要求的培训师实施培养活动。

a) 教育/培训机构培养：符合要求的各级教育机构（普通高校、中等和高等职业院校等）及培训机构应根据从业人员能力要求，制定人才培养方案，为企业培养合格的从业人员，满足个人就业和职业发展需要；
b) 企业培养：企业应有针对性、有计划地实施职业能力培养，满足个人职业发展需要，增强企业竞争力；
c) 个人培养：从业人员应根据个人职业发展计划，融合企业发展目标和从业技能要求，不断积累知识、技能和经验，提升能力水平。