GZB

国 家 职 业 标 准

职业编码：2-02-38-12

数据安全工程技术人员

（2023 年版）

中华人民共和国人力资源和社会保障部
中央网络安全和信息化委员会办公室 制定
中华人民共和国工业和信息化部

说　　明

为贯彻落实《关于深化人才发展体制机制改革的意见》，推动实施新时代人才强国战略，促进专业技术人员提升职业素养、补充新知识新技能，实现人力资源深度开发，推动经济社会全面发展，依据《中华人民共和国劳动法》《中华人民共和国职业教育法》有关规定，人力资源社会保障部联合中央网信办、工业和信息化部组织有关专家，开发制定了《数据安全工程技术人员国家职业标准（2023 年版）》（以下简称《标准》）。

一、本《标准》以《中华人民共和国职业分类大典（2022 年版）》为依据，严格按照《国家职业标准编制技术规程（专业技术类）》有关要求，坚持“以职业活动为导向、以专业能力为核心”的指导思想，在充分考虑产业结构变化、市场需求的发展和科技进步对数据安全工程技术人员专业要求的基础上，以客观反映数据安全发展水平及从业人员的专业能力要求为目标，对数据安全工程从业者的专业活动内容进行规范细致描述，明确了各等级专业技术人员的工作领域、工作内容以及知识水平、专业能力和实践要求。

二、本《标准》为首次制定，依据有关规定将本职业分为初级、中级、高级三个等级，包括职业概况、基本要求、工作要求、权重表和附录五个方面内容。

三、本《标准》的编制工作在人力资源社会保障部专业技术人员管理司、中央网信办干部局、工业和信息化部人事教育司、中国就业培训技术指导中心的指导下，由中国网络空间安全协会具体组织实施。

四、本《标准》主要起草单位有：中国网络空间安全协会、国家计算机网络与信息安全管理中心、北京邮电大学、中国科学院信息工程研究所、公安部第三研究所、中国软件评测中心、国科华盾（北京）科技有限公司、中国联合网络通信集团有限公司、华为技术有限公司、杭州安恒信息技术股份有限公司、山东伏羲智库互联网研究院、中云技术股份有限公司、三六零数字安全科技集团有限公司。主要起草人：李欲晓、崔聪聪、李政、徐倩华、林鹏、卢毓海、潘彭丹、肖佃艳、冯运波、何晓霞、彭博韬、苗春雨、张德馨、杜廷龙、孙艺、李松涛。

五、本《标准》主要审定人员有：杨建军、李凤华、杨伟平、罗海宁、贾成千、陈世翔、郎波、徐国爱、张莉、梅颖、杨韬、王惠莅、洪延青。

六、本《标准》业经人力资源社会保障部、中央网络安全和信息化委员会办公室、工业和信息化部批准，自颁布之日起实施。

数据安全工程技术人员
国家职业标准
（2023 年版）

1. 职业概况

1.1 职业名称

数据安全工程技术人员

1.2 职业编码

2-02-38-12

1.3 职业定义

从事数据安全需求分析挖掘、技术方案设计、项目实施、运营管理等工作的工程技术人员。

1.4 专业技术等级

本职业共设三个等级，分别为：初级、中级、高级。

1.5 职业环境条件

室内，常温。

1.6 职业能力特征

具有较强的学习能力、计算能力、表达能力及分析、推理和判断能力。

1.7 普通受教育程度

大学专科毕业。

1.8 职业培训要求

1.8.1 培训时间

数据安全工程技术人员需要按照本《标准》的职业要求参加有关课程培训，完成规定学时，取得学时证明。初级 128 标准学时，中级 148 标准学时，

高级 168 标准学时。

1.8.2 培训教师

承担初级、中级理论知识或专业能力培训任务的人员，应具有相关职业中级及以上专业技术等级或相关专业中级及以上职称。

承担高级理论知识或专业能力培训任务的人员，应具有相关职业高级专业技术等级或相关专业高级职称。

1.8.3 培训场所设备

理论知识培训在标准教室或线上平台进行；专业能力培训在具有相应软、硬件条件（包括模拟环境）的培训场所进行。

1.9 专业技术考核要求

1.9.1 申报条件

——取得初级培训学时证明，并具备以下条件之一者，可申报初级专业技术等级：

（1）取得技术员职称。

（2）具备相关专业大学本科及以上学历（含在读的应届毕业生）。

（3）具备相关专业大学专科学历，从事本职业技术工作满 1 年。

（4）技工院校毕业生按国家有关规定申报。

——取得中级培训学时证明，并具备以下条件之一者，可申报中级专业技术等级：

（1）取得助理工程师职称后，从事本职业技术工作满 2 年。

（2）具备大学本科学历，或学士学位，或大学专科学历，取得初级专业技术等级后，从事本职业技术工作满 3 年。

（3）具备硕士学位或第二学士学位，取得初级专业技术等级后，从事本职业技术工作满 1 年。

（4）具备相关专业博士学位。

（5）技工院校毕业生按国家有关规定申报。

——取得高级培训学时证明，并具备以下条件之一者，可申报高级专业技术等级：

（1）取得工程师职称后，从事本职业技术工作满 3 年。

（2）具备硕士学位，或第二学士学位，或大学本科学历，或学士学位，取

得中级专业技术等级后，从事本职业技术工作满 4 年。

（3）具备博士学位，取得中级专业技术等级后，从事本职业技术工作满 1 年。

（4）技工院校毕业生按国家有关规定申报。

1.9.2 考核方式

分为理论知识考试以及专业能力考核。理论知识考试、专业能力考核均实行百分制，成绩皆达 60 分（含）以上者为合格，考核合格者获得相应专业技术等级证书。

理论知识考试以闭卷笔试、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；专业能力考核以开卷实操考试、上机实践、模拟环境测试（需有专业人员现场测评记录）等方式为主，主要考核从业人员从事本职业应具备的技术水平。

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，且每个考场不少于 2 名监考人员；专业能力考核中的考评人员与考生配比不低于 1∶5，且考评人员为 3 人（含）以上单数。

1.9.4 考核时间

理论知识考试时间不少于 90 分钟，专业能力考核时间不少于 150 分钟。

1.9.5 考核场所设备

理论知识考试在标准教室进行，专业能力考核在具有相应软、硬件条件（包括模拟环境）的考核场所进行。

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，讲求信誉。
（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）计算机硬件基础知识。
（2）计算机软件基础知识。
（3）操作系统基础知识。
（4）网络基础知识。
（5）数据库基础知识。
（6）数据结构基础知识。

2.2.2 技术基础知识

（1）网络安全知识。
（2）密码技术知识。
（3）数据分类分级知识。
（4）数据质量管理知识。
（5）数据处理活动安全管理知识。
（6）数据采集与数据预处理知识。
（7）数据计算与数据存储知识。
（8）数据运营与技术指导知识。
（9）数据分析与挖掘知识。

（10）软件设计与开发知识。
（11）应急响应管理知识。

2.2.3 相关法律、法规、标准知识

（1）《中华人民共和国劳动法》相关知识。
（2）《中华人民共和国民法典》相关知识。
（3）《中华人民共和国网络安全法》相关知识。
（4）《中华人民共和国数据安全法》相关知识。
（5）《中华人民共和国个人信息保护法》相关知识。
（6）《中华人民共和国密码法》相关知识。
（7）《中华人民共和国保守国家秘密法》相关知识。
（8）《中华人民共和国刑法》相关知识。
（9）《关键信息基础设施安全保护条例》相关知识。
（10）《数据出境安全评估办法》相关知识。
（11）其他数据安全相关法律法规、管理规定、标准相关知识。

2.2.4 其他知识

（1）保密管理知识。
（2）环境保护知识。
（3）文明生产知识。
（4）劳动保护知识。

3. 工作要求

本《标准》对初级、中级、高级的专业能力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 初级

职业功能	工作内容	专业能力要求	相关知识要求
1. 数据安全管理	1.1 数据资产识别	1.1.1 能判断数据资产与业务之间的关系 1.1.2 能按照数据资产管理要求进行数据资产识别 1.1.3 能编制数据资产清单	1.1.1 数据资产和数据业务基础知识 1.1.2 数据资产识别工具与技术 1.1.3 数据资产管理知识
	1.2 数据分类分级	1.2.1 能根据制度或操作规程进行数据分类 1.2.2 能依据操作流程规范或使用工具完成数据分级任务	1.2.1 数据分类分级相关标准
	1.3 数据治理基础工作	1.3.1 能使用工具进行数据收集、存储、使用、加工、传输、提供、公开、销毁等全生命周期管理	1.3.1 数据处理的合法、正当、必要原则和要求 1.3.2 密码技术知识 1.3.3 数据汇聚、分析的风险与管理要求 1.3.4 数据脱敏与匿名化知识
2. 数据安全工程规划设计和建设实施	2.1 数据安全基础保障方案设计	2.1.1 能按照要求设计数据区域边界防护解决方案 2.1.2 能基于已有数据安全基础方案调整输出不同业务的具体实施方案	2.1.1 安全区域边界知识 2.1.2 数据安全行业应用知识
	2.2 数据安全处理活动方案设计	2.2.1 能根据业务场景，设计数据收集安全技术方案 2.2.2 能根据访问控制策略和用户角色权限，制定数据安全的访问控制解决方案 2.2.3 能根据数据存储方式制定数据载体防护策略，设计数据载体安全管理与销毁解决方案	2.2.1 访问控制知识 2.2.2 数据销毁知识 2.2.3 数据载体安全管理知识

续表

职业功能	工作内容	专业能力要求	相关知识要求
2. 数据安全工程规划设计和建设实施	2.3 数据安全工程建设实施	2.3.1 能理解并按照数据安全基础保障、处理活动、网络通信、防护体系等方案有序开展数据安全工程建设实施工作 2.3.2 能熟知数据收集、存储、使用、加工、传输、提供、公开、删除全过程中安全建设技术工具参数标准，按照国家法律法规要求和业务场景制度流程要求实施数据收集、存储、使用、加工、传输、提供、公开、删除全过程中的安全建设	2.3.1 数据收集、存储、使用、加工、传输、提供、公开、删除全过程中安全建设技术工具知识 2.3.2 数据收集、存储、使用、加工、传输、提供、公开、删除全过程中安全建设制度流程及实施操作知识
3. 数据安全技术开发与运维	3.1 开发	3.1.1 能基于数据安全架构方案完成数据处理活动各环节安全防护相关系统、模块、工具的基础开发工作 3.1.2 能根据数据安全防护技术需求适配联调数据安全技术防护产品 3.1.3 能使用开源产品或库开发实现身份认证、访问控制等基础安全防护功能	3.1.1 软件系统开发体系知识 3.1.2 网络安全、数据库安全、主机安全防护知识 3.1.3 数据处理活动各环节安全防护知识
	3.2 测试	3.2.1 能根据测试方案进行数据处理活动各环节风险测试 3.2.2 能根据测试方案对数据安全措施的有效性进行测试 3.2.3 能基于各项测试结果撰写数据安全系统、组件和工具测试报告	3.2.1 数据安全软件测试知识 3.2.2 数据安全风险测试方法应用和工具使用知识 3.2.3 数据安全措施测试方法应用和工具使用知识
	3.3 实施	3.3.1 能根据数据安全技术实施方案安装各类数据安全技术防护系统、组件和工具 3.3.2 能完成常用中间件的搭建及使用，编制数据安全技术防护类交付文档 3.3.3 能根据数据安全技术实施方案使用数据库审计，利用脱敏、数据防泄露、水印、密码学、隐私保护等技术工具实施数据安全基础防护	3.3.1 计算机操作系统、网络、磁盘管理等知识 3.3.2 数据库审计、脱敏技术、数据防泄露技术、水印技术、密码学技术、隐私保护技术等数据安全防护技术工具使用知识 3.3.3 数据安全产品组网部署方法

续表

职业功能	工作内容	专业能力要求	相关知识要求
3. 数据安全技术开发与运维	3.4 运维	3.4.1 能对服务器、网络安全设备和网络信息系统等数据安全基础设施进行日常安全维护、安全巡检 3.4.2 能排查分析常见的数据安全产品故障 3.4.3 能按照部署手册完成系统升级	3.4.1 互联网数据中心相关知识 3.4.2 数据安全产品或设备的安装、配置知识 3.4.3 数据安全产品或设备的故障分析方法 3.4.4 日常数据安全运维工作流程和方法
4. 数据安全监测与应急处置	4.1 数据安全检测与分析	4.1.1 能使用工具发现和检测数据载体的漏洞 4.1.2 能根据安全加固方案对漏洞进行安全加固和修复 4.1.3 能根据漏洞扫描结果形成数据安全漏洞扫描报告	4.1.1 漏洞管理知识 4.1.2 漏洞扫描工具使用方法
	4.2 数据安全异常监测	4.2.1 能使用工具监测数据访问活动，发现异常数据访问行为 4.2.2 能初步确定数据安全事件异常类别 4.2.3 能使用工具审计数据异常行为或状态 4.2.4 能撰写数据安全异常监测日志	4.2.1 常见数据安全异常行为 4.2.2 网络攻击流程及渗透攻击知识 4.2.3 入侵检测技术原理 4.2.4 数据异常行为或状态审计方法和工具 4.2.5 数据安全异常监测日志编写方法
	4.3 数据安全应急响应与处置	4.3.1 能使用工具发现安全事件 4.3.2 能根据数据安全应急响应预案，按照流程开展数据安全应急演练 4.3.3 能根据容灾计划，定期备份和迁移关键数据 4.3.4 能使用工具进行数据备份	4.3.1 数据安全事件检测工具使用方法 4.3.2 数据安全事件应急演练知识 4.3.3 数据容灾备份知识 4.3.4 数据备份、迁移与恢复知识

续表

职业功能	工作内容	专业能力要求	相关知识要求
5. 数据安全评估	5.1 数据安全合规性评估	5.1.1 能依据数据安全合规评估规范确定评估范围 5.1.2. 能采用问卷调查、访谈、资料查阅等方式，对受评估方的人员情况、业务系统等基本信息进行调研 5.1.3 能识别、分析各业务系统的主要数据处理行为 5.1.4 能识别、分析第三方应用接口的个人信息和重要数据采集行为 5.1.5 能使用工具评估检测数据处理行为是否合规	5.1.1 问卷设计和信息检索知识 5.1.2 业务系统数据处理分析方法 5.1.3 接口数据采集行为分析方法 5.1.4 个人信息和重要数据特征提取与识别方法 5.1.5 数据安全合规评估相关技术工具使用方法
	5.2 数据安全风险评估	5.2.1 能识别并梳理数据资产，对资产价值进行定性或者定量分析 5.2.2 能使用评估工具识别数据处理系统的漏洞 5.2.3 能根据风险分析模型，定性或者定量地评定数据安全风险程度	5.2.1 网络和数据安全常见的风险和威胁类型 5.2.2 数据安全风险评估方法 5.2.3 数据系统安全风险评估工具使用方法
	5.3 数据出境安全评估	5.3.1 能界定数据出境的数量、范围、种类、类型和级别 5.3.2 能确定数据跨境和境外接收方处理数据的目的、范围、方式	5.3.1 数据传输方法及原理 5.3.2 组织内部和外部数据收集流程和方法工具 5.3.3 数据安全出境评估的基本要求

3.2 中级

职业功能	工作内容	专业能力要求	相关知识要求
1. 数据安全管理	1.1 数据资产识别	1.1.1 能对数据资产使用部门、角色进行梳理 1.1.2 能对数据资产存储策略进行梳理 1.1.3 能对数据资产使用状况、安全责任人等进行梳理 1.1.4 能使用自动化工具识别数据资产属性	1.1.1 数据资产存储策略 1.1.2 数据属性识别自动化工具
	1.2 数据分类分级	1.2.1 能根据数据所涉及范围设计数据分类分级标准 1.2.2 能基于数据资产清单进行数据分类分级体系设计 1.2.3 能制定数据分类分级流程规范 1.2.4 能编制重要数据目录	1.2.1 数据分类分级方法 1.2.2 数据分类分级自动化软件工具
	1.3 数据安全需求分析	1.3.1 能分析明确数据处理活动各环节安全需求 1.3.2 能从数据安全威胁角度开展数据安全需求分析 1.3.3 能从数据安全风险角度开展数据安全需求分析	1.3.1 数据处理活动各环节安全知识 1.3.2 数据安全威胁建模知识 1.3.3 数据安全框架模型知识
	1.4 数据治理开展工作	1.4.1 能依据政策法规和标准要求，组织数据收集、存储、使用、加工、传输、提供、公开等管理	1.4.1 数据处理合法、正当、必要原则和具体要求 1.4.2 数据对外提供要求 1.4.3 数据安全管理知识
2. 数据安全工程规划设计和建设实施	2.1 数据安全保障方案设计	2.1.1 能针对数据源和目标平台设计数据传输可行身份认证方案 2.1.2 能根据数据分类分级和业务场景进行数据加密传输方案的设计 2.1.3 能根据数据源和数据特点，设计数据完整性校验和防篡改方案 2.1.4 能根据安全需求设计数据通信网络安全验证方案 2.1.5 能梳理数据传输接口，设计传输接口管控与审计方案	2.1.1 网络协议知识 2.1.2 数据通信安全知识 2.1.3 传输通信加密知识 2.1.4 网络安全验证知识 2.1.5 接口调用日志知识 2.1.6 监控审计知识

续表

职业功能	工作内容	专业能力要求	相关知识要求
2. 数据安全工程规划设计和建设实施	2.2 数据安全处理活动方案设计	2.2.1 能根据业务需求设计数据提供和公开安全技术方案 2.2.2 能根据数据分类分级设计数据销毁安全技术方案 2.2.3 能根据数据分类分级制定数据加密策略，设计数据安全存储解决方案 2.2.4 能根据数据特点和业务需求，设计数据防泄漏方案	2.2.1 数据收集策略知识 2.2.2 数据加密技术知识 2.2.3 数据签名技术知识 2.2.4 水印、密钥技术知识 2.2.5 数据丢失防护技术知识 2.2.6 数据内外部共享安全技术知识
	2.3 数据安全专职人员管理方案设计	2.3.1 能进行数据安全专职人员录用、离岗方案的设计 2.3.2 能进行外部人员访问方案的设计 2.3.3 能对数据安全专职人员的行为进行安全审计	2.3.1 人员审计知识 2.3.2 数据安全风险管理知识 2.3.3 数据安全行为状态审计知识
	2.4 数据安全工程建设实施	2.4.1 能按照国家法律法规要求，结合业务场景制定数据处理全过程中的安全建设实施制度流程 2.4.2 能熟练使用数据处理全过程中的安全建设技术工具，并根据业务场景优化技术工具参数、研发技术工具 2.4.3 能理解并按照数据安全基础保障、处理活动、网络通信、防护体系等方案，有序开展数据安全工程建设实施工作和相应的人员及技术管理	2.4.1 数据处理全过程中安全建设实施相关法律法规及行业特点知识 2.4.2 数据处理全过程中安全技术工具研发知识 2.4.3 数据处理全过程中安全建设技术工具知识
3. 数据安全技术开发与运维	3.1 开发	3.1.1 能根据数据安全管理方案开发相应的组织架构体系及外部调用接口 3.1.2 能根据数据安全技术防护建设方案开发相应的技术工具 3.1.3 能根据开发需求和功能要求选择对应的密码技术以及开发基础密码库的功能接口 3.1.4 能调试并修复常见基础编程和网络应用开发漏洞 3.1.5 能根据数据安全防护方案开发身份认证、访问控制等功能接口	3.1.1 软件工程体系知识 3.1.2 开源数据安全产品功能接口知识 3.1.3 编程语言、编程原理以及主流数据安全开发框架等知识 3.1.4 编程漏洞修复方法 3.1.5 密码函数库使用方法 3.1.6 自动化脚本开发知识

续表

职业功能	工作内容	专业能力要求	相关知识要求
3. 数据安全技术开发与运维	3.2 测试	3.2.1 能设计数据安全软件开发和测试工作流程，并使用测试管理工具进行管理 3.2.2 能配置实施风险规避措施 3.2.3 能进行特定业务的逻辑漏洞测试 3.2.4 能使用工具进行数据安全系统漏洞挖掘和代码审计，并给出通用性安全漏洞的修复建议 3.2.5 能使用工具对系统的数据安全防护措施进行白盒或灰盒测试 3.2.6 能编制数据安全测试报告	3.2.1 主流数据安全系统测试方法 3.2.2 安全防御机制绕过方法 3.2.3 测试数据保护措施有效性的策略、方法、原理
	3.3 实施	3.3.1 能面向复杂场景编制实施方案和部署手册 3.3.2 能制定数据库审计、脱敏、数据防泄露、水印、隐私保护、人员审计的安全策略 3.3.3 能根据数据安全技术实施方案部署运行数据安全保护、检测、分析、溯源、评估、审计等数据安全工具 3.3.4 能部署实施数据安全管控策略	3.3.1 数据库、云计算、虚拟化、数据安全保护工具等知识 3.3.2 数据审计、脱敏、防泄漏、水印、隐私保护、加密工具的工作原理
	3.4 运维	3.4.1 能对数据安全系统或应用进行部署、联网配置和调试 3.4.2 能根据数据安全合规性检查结果进行建设整改 3.4.3 能针对数据安全风险、威胁开展数据安全运维工作 3.4.4 能持续改进数据安全运维流程	3.4.1 数据安全产品或设备的调试和故障分析知识 3.4.2 数据访问控制、加密、脱敏、备份和防泄漏等数据安全技术方面的应用知识 3.4.3 数据安全产品的原理和使用方法
4. 数据安全监测与应急处置	4.1 数据安全检测与分析	4.1.1 能开发漏洞检测工具 4.1.2 能根据漏洞测试结果分析数据安全潜在风险 4.1.3 能对数据安全漏洞进行分析、验证，确定安全漏洞的类别和等级 4.1.4 能使用威胁情报系统、工具，收集、发现威胁情报并进行归类分析	4.1.1 安全漏洞的原理及检测方法 4.1.2 漏洞检测工具开发方法 4.1.3 威胁情报收集、检测与分析方法

续表

职业功能	工作内容	专业能力要求	相关知识要求
4. 数据安全监测与应急处置	4.2 数据安全异常监测	4.2.1 能审计异常数据访问活动，并研判、执行对应管控措施 4.2.2 能根据系统日志等分析数据泄露、数据越权操作等异常行为 4.2.3 能判断数据安全异常事件的类别与级别	4.2.1 异常数据访问活动审计与管控方法 4.2.2 访问控制技术原理 4.2.3 数据安全异常事件分类分级知识
	4.3 数据安全应急响应与处置	4.3.1 能对数据安全事件进行应急分析 4.3.2 能制定有效控制数据安全事件影响扩大的措施 4.3.3 能制定消除数据安全事件影响的措施 4.3.4 能根据业务需求选择数据恢复策略进行数据恢复	4.3.1 数据安全应急响应知识 4.3.2 数据安全事件分类分级知识 4.3.3 数据安全事件处置流程和方法 4.3.4 数据恢复管理与策略知识与方法
5. 数据安全评估	5.1 数据安全合规性评估	5.1.1 能收集和分析数据安全合规需求，建立数据安全合规资料库和合规清单 5.1.2 能设计数据安全合规检查的技术流程 5.1.3 能优化完善个人信息保护合规检查脚本、策略，开发个人信息保护合规检查工具 5.1.4 能优化完善重要数据合规检查脚本、策略，开发重要数据合规检查工具 5.1.5 能分析企业数据安全管理现状，识别数据安全合规问题及改进项，提出数据安全合规建议	5.1.1 数据安全合规需求分析方法 5.1.2 数据安全合规检查技术流程设计方法 5.1.3 合规检查脚本、工具开发方法
	5.2 数据安全风险评估	5.2.1 能收集和分析数据安全风险评估需求，组织实施评估活动 5.2.2 能开发数据安全风险自动化分析工具 5.2.3 能识别数据在不同处理环节、不同业务场景面临的安全风险 5.2.4 能根据风险分析模型综合评定数据安全风险程度 5.2.5 能基于风险分析结果，提出数据安全风险应对措施	5.2.1 数据安全风险评估需求分析方法 5.2.2 数据安全风险评估工具开发方法 5.2.3 数据安全威胁场景分析知识 5.2.4 数据安全风险问题差距分析方法 5.2.5 数据安全风险控制方法和措施

续表

职业功能	工作内容	专业能力要求	相关知识要求
5. 数据安全评估	5.3 数据要素流通、交易及出境安全评估	5.3.1 能正确评估境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性 5.3.2 能识别数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险 5.3.3 能评估与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等，是否满足数据安全保护要求 5.3.4 能明确数据境外存储的起止时间及到期后的处理方式，利用技术手段对其处理方式进行验证 5.3.5 能评估境外接收方履行责任义务的管理和技术措施、能力 5.3.6 能通过技术手段分析数据跨境通信链路涉及的国家和地区，研判是否存在由于数据缓存、内容分发等造成的数据跨境安全风险 5.3.7 能评估发生数据跨境安全事件时，采取补救措施的有效性及其对数据主体权益产生的影响 5.3.8 能研判数据安全维护渠道是否通畅 5.3.9 能分析数据流通和交易过程中数据来源，评估安全保护措施的有效性 5.3.10 能根据流通中的数据来源和数据生成特征，分析越权情况和越权风险，界定数据操作权限	5.3.1 数据出境安全评估方法 5.3.2 常见数据加密传输协议 5.3.3 数据流量监测方法 5.3.4 跨境数据安全事件处理方法 5.3.5 数据跨境法律法规知识 5.3.6 数据流通和交易过程和典型应用场景知识 5.3.7 数据流通过程中数据权限管理和风险知识

3.3 高级

职业功能	工作内容	专业能力要求	相关知识要求
1. 数据安全管理	1.1 数据资产管理	1.1.1 能对数据资产全面盘点形成数据资产地图并进行图形化展示 1.1.2 能将数据资产进行标签化处理 1.1.3 能建立一套符合数据安全驱动的组织管理制度	1.1.1 数据资产画图工具和技术 1.1.2 数据资产标签化的工具和技术
	1.2 数据分类分级	1.2.1 能基于行业和业务理解构建数据分类分级框架 1.2.2 能对数据分类分级结果进行评审和完善 1.2.3 能对数据分类分级规则进行优化	1.2.1 数据资产分类分级框架知识 1.2.2 数据分类分级结果评价方法
	1.3 数据安全需求分析与管理	1.3.1 能建立组织业务的数据安全需求分析体系 1.3.2 能开展数据安全需求分析的审计活动 1.3.3 能将数据安全需求分析纳入数据开发的整个生命周期	1.3.1 数据安全风险评估方法 1.3.2 数据安全需求管理知识
	1.4 数据治理方案制定	1.4.1 能按照法律和政策要求制定数据采集管理方案 1.4.2 能按照法律和政策要求制定数据传输管理方案 1.4.3 能按照法律和政策要求制定数据存储管理方案 1.4.4 能按照法律和政策要求制定数据使用管理方案 1.4.5 能按照法律和政策要求制定数据销毁管理方案	1.4.1 数据安全相关法律法规政策标准知识 1.4.2 数据治理框架知识 1.4.3 数据治理流程设计与改进知识

续表

职业功能	工作内容	专业能力要求	相关知识要求
2. 数据安全工程规划设计和建设实施	2.1 数据安全管理框架设计	2.1.1 能根据数据处理活动安全需求制定管理侧安全架构解决方案 2.1.2 能根据数据处理活动安全需求制定终端安全架构解决方案 2.1.3 能根据数据类型和等级设计数据安全风险监测框架	2.1.1 终端防泄漏技术知识 2.1.2 数据库安全技术知识 2.1.3 数据安全风险管理知识
	2.2 数据安全防护体系设计	2.2.1 能制定与优化数据处理活动各环节安全防护方案 2.2.2 能构建涵盖数据处理活动各环节的安全防护技术工具体系 2.2.3 能根据数据应用的业务需求，构建数据安全运营体系	2.2.1 数据处理活动各环节安全防护方法 2.2.2 数据安全威胁风险知识 2.2.3 数据安全技术与工具知识
	2.3 数据安全技术管理方案设计	2.3.1 能根据数据分类分级设计数据资产管理方案 2.3.2 能根据业务需求设计数据安全技术与工具管理方案 2.3.3 能根据组织数据安全策略，制定数据安全管理制度 2.3.4 能根据组织的安全管理策略，进行数据安全机构、人员岗位方案的设计 2.3.5 能制定数据安全相关技术规范，开展数据安全合规培训和宣传	2.3.1 数据安全模型知识 2.3.2 数据安全技术与工具知识 2.3.3 数据安全技术管理知识 2.3.4 数据安全法、个人信息保护法等法律法规知识
	2.4 数据安全工程建设实施	2.4.1 能结合业务场景，指导开展数据处理全过程中的安全建设实施及制度流程制定 2.4.2 能指导数据处理全过程中安全建设技术工具参数标准制定及工具研发、使用 2.4.3 能指导并管理有关人员按照数据安全基础保障、处理活动、网络通信、防护体系等方案有序开展数据安全工程建设实施工作，并统筹进行技术管理	2.4.1 数据处理全过程中安全建设标准知识 2.4.2 数据处理全过程中安全建设技术管理知识

续表

职业功能	工作内容	专业能力要求	相关知识要求
3. 数据安全技术开发与运维	3.1 开发	3.1.1 能完成数据安全技术防护平台、数据传输安全平台、数据共享安全平台架构设计和开发管理 3.1.2 能根据数据安全防护方案，制定详细技术开发方案，编制研发计划和路线图 3.1.3 能基于基础函数库或接口，设计开发数据密码防护、权限管理等基本数据安全防护功能模块 3.1.4 能针对防护方案要求，设计与研发数字水印、密钥管理等数据安全技术	3.1.1 数据传输安全平台、数据共享安全平台、隐私数据保护平台的开发和管理知识 3.1.2 数据安全系统技术选型知识 3.1.3 复杂数据安全系统功能设计与研发
	3.2 测试	3.2.1 能制订和实现合理的自动化验证方案，并设计和实现自动化测试工具，完成数据安全防护类技术工具的测试和验证 3.2.2 能自主编写测试工具，对目标工程源码进行代码分析 3.2.3 能编写用于指导测试实施工作的安全测试计划和安全测试技术指南 3.2.4 能评估数据安全测试工作的安全风险、规避措施，实施风险管控	3.2.1 数据安全系统测试实施组织方法、技术指南编写方法 3.2.2 数据安全系统源代码分析方法 3.2.3 数据安全测试风险评估方法
	3.3 实施	3.3.1 能构建数据安全技术实施框架，组织实施全方位数据安全保护系统、平台 3.3.2 能制定数据安全技术实施的流程规范 3.3.3 能构建数据安全技术系统之间的关联分析策略 3.3.4 能持续改进数据安全技术并组织实施 3.3.5 能识别产品开发及上线运行中处理的重要数据等，并实施安全防护和安全合规策略	3.3.1 数据安全系统联动与分析知识 3.3.2 数据安全技术实施的框架构建方法 3.3.3 数据安全技术实施的流程规范制定方法 3.3.4 数据安全技术系统之间的关联分析策略构建方法 3.3.5 重要数据界定与识别知识
	3.4 运维	3.4.1 能规划建设数据安全运维体系 3.4.2 能评估和验证数据安全运维工作的有效性 3.4.3 能审计数据系统运行日志、数据访问日志、操作日志等，评估系统安全风险 3.4.4 能制定数据安全系统运维方案、流程和规范，编写数据安全技术运行管理手册，以及用户、管理员使用指南	3.4.1 系统日志审计等知识 3.4.2 数据安全运营平台方面的原理和使用方法 3.4.3 数据安全技术运行管理手册、用户手册、管理员手册编写方法

续表

职业功能	工作内容	专业能力要求	相关知识要求
4. 数据安全监测与应急处置	4.1 数据安全检测与分析	4.1.1 能分析数据安全相关漏洞原理和利用方法 4.1.2 能评估数据安全相关漏洞的风险程度，制定加固措施或开发修复补丁 4.1.3 能正确归类、整合安全威胁，形成及时准确的数据安全威胁情报	4.1.1 漏洞利用方法 4.1.2 漏洞风险评估方法 4.1.3 修复补丁开发方法 4.1.4 主要安全事件特征归类和分析方法 4.1.5 数据安全威胁情报分析方法
	4.2 数据安全异常监测	4.2.1 能对数据异常行为进行定位、溯源和关联分析 4.2.2 能针对数据安全风险点制定异常行为监测和临时管控策略 4.2.3 能对数据异常行为出现的关键环节进行加固或修复 4.2.4 能根据数据安全异常行为监测情况编制报告	4.2.1 数据异常活动溯源方法 4.2.2 异常行为建模、关联分析知识 4.2.3 数据异常行为监测和管控策略设计和部署方法 4.2.4 数据安全异常行为监测报告编写方法
	4.3 数据安全应急响应与处置	4.3.1 能制定数据安全应急预案并组织内部演练 4.3.2 能制定数据安全事件处置操作规程 4.3.3 能组织安全处置与业务间的协同联动，以保证业务连续性、数据备份与恢复计划和应急预案的实施 4.3.4 能对数据安全事件进行复盘，编写数据安全事件预防规范 4.3.5 能根据业务特性，制定合适的容灾计划	4.3.1 数据安全应急方案编写规范 4.3.2 数据安全应急响应管理知识 4.3.3 数据安全事件应急处置实施方法 4.3.4 容灾管理知识
	4.4 数据安全溯源与取证	4.4.1 能制定数据安全事件取证溯源的策略和机制 4.4.2 能梳理安全事件相关数据的流转与分布情况，合理推测还原事件的发生过程 4.4.3 能使用工具查找风险源、固定证据 4.4.4 能组织编写数据安全事件溯源取证报告 4.4.5 能根据取证溯源结果对数据服务相关的访问控制、合规性保障等数据处理活动，安全策略及其安全技术机制提出优化建议	4.4.1 数据安全事件溯源取证技术知识 4.4.2 数据安全溯源和取证工具使用方法 4.4.3 数据安全事件溯源取证报告编写方法

续表

职业功能	工作内容	专业能力要求	相关知识要求
5. 数据安全评估	5.1 数据安全合规性评估	5.1.1 能根据具体合规监管要求制定相应的数据安全合规评估工作方案 5.1.2 能依据工作方案，组织协调相关部门人员，开展合规评估 5.1.3 能对数据处理系统进行分析，制定数据处理活动各环节合规性评估的技术方案和实施标准 5.1.4 能对评估对象的数据安全组织架构和管理制度进行合规评估 5.1.5 能对合规评估结果进行综合分析形成评估报告，提供整改建议和优化方案	5.1.1 数据安全合规性评估工作方案编写方法 5.1.2 常见数据处理系统和应用的数据安全策略的执行逻辑 5.1.3 数据安全法律法规要求 5.1.4 数据安全不合规项优化整改措施 5.1.5 合规评估报告编写方法
	5.2 数据安全风险评估	5.2.1 能编制评估方案，制定评估计划，建立数据安全风险评估制度规范、流程策略，并能组织实施评估活动 5.2.2 能根据数据安全风险分析结果，提出风险处置建议，并编制评估报告 5.2.3 能制定数据安全风险评估管理制度，持续优化并改进风险评估管理机制	5.2.1 数据安全风险评估计划和报告编制方法 5.2.2 数据安全风险管理方法
	5.3 数据要素流通、交易及出境安全评估	5.3.1 能制定数据出境安全评估制度、流程和工作方案，组织开展数据出境安全评估活动 5.3.2 能基于数据出境安全风险分析，撰写数据出境安全评估报告 5.3.3 能制定并组织落实数据出境合规整改方案 5.3.4 能制定并组织实施数据流通、交易安全评估方案	5.3.1 数据出境安全评估方案编写方法 5.3.2 数据出境安全风险分析方法 5.3.3 数据出境安全评估报告编写方法 5.3.4 数据流通、交易风险评估知识

4. 权重表

4.1 理论知识权重表

项目 \ 专业技术等级		初级（%）	中级（%）	高级（%）
基本要求	职业道德	5	5	5
	基础知识	20	10	5
相关知识要求	数据安全管理	25	20	10
	数据安全工程规划设计和建设实施	15	20	15
	数据安全技术开发与运维	15	15	15
	数据安全监测与应急处置	10	15	25
	数据安全评估	10	15	25
合计		100	100	100

4.2 专业能力要求权重表

项目 \ 专业技术等级		初级（%）	中级（%）	高级（%）
专业能力要求	数据安全管理	40	25	20
	数据安全工程规划设计和建设实施	15	20	20
	数据安全技术开发与运维	20	20	15
	数据安全监测与应急处置	15	20	20
	数据安全评估	10	15	25
合计		100	100	100

5. 附录

5.1 术语定义

1. 数据资产

被保护的数据。

2. 数据载体

用于存放和传输数据的媒体。

3. 数据处理

包括数据的收集、存储、使用、加工、传输、提供、公开等。

4. 数据安全

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

5. 数据安全评估

针对数据收集、存储、使用、加工、传输、提供、公开等活动，根据相关法规标准要求，按照风险分析的方法，分析数据相关活动存在的安全风险。

5.2 参考文献

［1］GB/T 37973—2019《信息安全技术 大数据安全管理指南》相关知识

［2］GB/T 37988—2019《信息安全技术 数据安全能力成熟度模型》相关知识

［3］GB/T 39725—2020《信息安全技术 健康医疗数据安全指南》相关知识

［4］GB/T 39477—2020《信息安全技术 政务信息共享 数据安全技术要求》相关知识

［5］GB/T 42014—2022《信息安全技术 网上购物服务数据安全要求》相关知识

［6］GB/T 42012—2022《信息安全技术 即时通信服务数据安全要求》相关知识

［7］GB/T 42015—2022《信息安全技术 网络支付服务数据安全要求》相关知识