工业和信息化人才培养工程培训课程标准

数据安全

（试行版）

工业和信息化部教育与考试中心

二〇二二年十二月

说　明

为贯彻落实《关于加强和改进工业和信息化人才队伍建设的实施意见》（工信部人〔2022〕138号），立足新发展阶段、贯彻新发展理念、构建新发展格局，工业和信息化部教育与考试中心依据数字技术、智能制造等行业发展人才实际需要，积极整合行业教育资源优势，组织行业专家、教育专家持续研发《工业和信息化人才培养工程培训课程标准》（以下简称“标准”），用于指导工业和信息化人才培养工程相关培训课程建设，高质量推动工业和信息化人才培养工程发展。

《标准》以客观反映现阶段行业技术发展水平和从业人员能力要求为目标，在充分考虑经济发展、科技进步和产业结构变化的基础上，对课程的等级、模块划分进行定义，对培训内容要求、专业能力要求、知识要求和考核权重进行了详细说明。

《标准》组编遵循了有关技术规程的要求，既保证体例规范，又体现以专业活动为导向、以专业技术技能为核心的特点，模块化的结构使其具有根据技术发展进行调整的灵活性和实用性，符合培训工作的需要。

本《标准》编制工作由工业和信息化部教育与考试中心具体组织实施，参与标准编制单位有北京神州绿盟科技有限公司、北京安维信息技术有限公司、中国软件与技术服务股份有限公司等。参与编制人有龚玉涵、蒋建春、刘伟平、史秋艳、张珊珊、王玉娥、刘永波等。

本《标准》经工业和信息化部教育与考试中心批准，自颁布之日起施行。

工业和信息化人才培养工程

培训课程标准

1　课程概况

1.1　课程名称

数据安全

1.2　课程定义

课程依据数据安全知识框架、数据安全治理工作的核心能力，使学员能建立数据安全管理体系和防护知识体系，具备完成数据安全治理和管理等的技术技能能力。

1.3　课程技能等级

本课程共设两个等级，分别为：初级、中级、高级。

1.4　课程环境条件

室内、常温。

1.5　课程能力要求

具有较强的学习能力、研究能力；具有一定的理解、判断和表达能力；具有一定的分析解决问题的能力和沟通能力。

1.6　普通受教育程度

高中毕业（或同等学历）。

1.7　课程培训要求

1.7.1　培训期限

初级课程不少于线上或线下 64 标准学时；中级课程不少于线上或线下 70 标准学时。

1.7.2　培训教师

承担初级理论知识或专业能力培训任务人员，应具有相关课程培训经验 1 年。

承担中级理论知识或专业能力培训任务人员，应具有相关课程培训经验 2 年以上，或具有相关职业高级专业技术等级、相关专业高级职称二者之一。

承担高级理论知识或专业能力培训任务人员，应具有行业从业经验或相关课程培训经验 3 年以上，或具有相关职业高级专业技术等级、相关专业高级职称二者之一。

1.7.3 培训场所设备

理论知识培训应有可容纳 30 人以上学员的教室，并配有满足教学需要的网络环境和学习软件、设施等。

2 基本要求

2.1 专业道德

2.1.1 专业道德基本知识

2.1.2 专业守则

（1）遵纪守法，爱岗敬业

（2）精益求精，勇于创新

（3）诚实守信，恪守职责

（4）遵守规程，安全操作

（5）认真严谨，忠于职守

2.2 基础知识

2.2.1 基础理论知识

（1）网络安全监管

（2）信息安全管理

（3）网络信息安全评估

（4）数据安全基本概念

（5）数据安全法解读

（6）数据分类分级基本概念

（7）数据生命周期

（8）数据安全隐私概念

2.2.2 实操能力知识

（1）个人信息安全

（2）数据安全基础

（3）数据分类分级

（4）数据安全风险评估

（5）数据安全风险与挑战

（6）行业数据安全管理体系建设实践

（7）数据安全管理

3 课程内容要求

本标准对初级、中级、高级各级别的课程要求依次递进，高级别涵盖低级别的要求。

3.1 初级

数据安全设计方向的课程模块包括数据安全采集、数据安全处理、数据安全评估、数据安全优化、数据安全技术服务咨询；数据安全实施和运营方向的课程模块包括数据安全采集、数据安全技术服务、数据安全防护、数据安全处理、数据安全运营、数据安全管理；数据安全治理方向的课程模块包括数据安全采集、数据安全技术服务、数据安全管理、数据安全评估、数据安全优化、数据安全技术服务咨询。

课程模块	培训内容	专业能力要求	相关知识要求
1.数据安全采集	1.1 数据安全日志收集	1.1.1 能够识别数据系统日志信息 1.1.2 能够使用日志收集工具采集数据系统相关日志	1.1.1 基础数据业务梳理方法及日志工具使用方法
	1.2 数据安全配置收集	1.2.1 能够识别数据系统配置信息 1.2.2 能够使用工具或人工获取到数据系统相关配置	1.2.1 系统配置方法及使用方法
	1.3 数据安全威胁情报收集	1.3.1 能够识别数据安全威胁情报信息 1.3.2 能够收集数据安全事件，提炼形成数据威胁报告 1.3.3 能够采集数据系统安全漏洞信息 1.3.4 能够使用工具或人工获取数据安全威胁情报信息	1.3.1 网络爬虫知识 1.3.2 实时数据采集知识 1.3.3 作业调度知识
	1.4 数据安全法律法规政策收集	1.4.1 能够识别数据安全法律法规政策信息 1.4.2 能够使用工具或人工获取数据安全法律法规政策信息	1.4.1 离线数据采集知识
2.数据安全技	2.1 数据资产梳理	2.1.1 能够理解数据资产梳理要求，识别数据资产 2.2.2 能够使用数据资产梳理工具	2.1.1 数据资产相关知识 2.1.2 数据资产梳理工具使用方法

术服务	2.2 数据资产访问权限梳理	2.2.1 能够识别和收集数据资产访问权限文件 2.2.2 能够数据库访问权限信息 2.2.3 能够使用数据库权限获取工具	2.2.1 权限管理知识 2.2.2 主流数据库安全产品的部署配置原理
	2.3 数据资产使用梳理	2.2.1 能够识别和收集数据资产使用的用户和系统 2.2.3 能够利用工具获取数据资产使用信息	2.2.1 数据资产相关知识 2.2.2 数据资产梳理工具使用方法
	2.4 数据资产存储梳理	2.4.1 能够按照服务要求，识别和收集存储的数据资产 2.4.2 能够人工和工具收集数据资产 2.4.3 能够统计存储的数据资产分布情况	2.4.1 文件系统数据存储知识 2.4.2 关系型数据库安全知识 2.4.3 非关系型数据库安全知识
	2.5APP 应用安全隐私检查	2.5.1 能够按照隐私保护规则，识别隐私保护数据 2.5.2 能够使用工具检查 APP 应用安全隐私合规情况	2.5.1 隐私保护法规知识 2.5.2APP 相关使用知识
	2.6 数据安全合规检查	2.6.1 能够按照数据安全合规检查服务要求，识别数据合规信息 2.6.2 能够使用工具检查数据安全情况	2.6.1 数据安全合规检查规范
	2.7 数据安全风险评估	2.7.1 能够按照数据安全风险服务要求，识别数据风险信息 2.7.2 能够使用安全工具检查数据资产安全状况 2.7.3 能够收集和整理数据资产安全风险信息	2.7.1 数据库扫描工具 2.7.2 基础数据安全知识
	2.8 数据安全设备产品安装	2.8.1 能够部署、配置数据防勒索设备产品 2.8.2 能够部署、配置堡垒机部署和配置设备产品部署、配置 2.8.3 能够部署、配置安全审计与入侵监测设备产品部署、配置 2.8.4 能够部署、配置数据安全态势监测设备产品 2.8.5 能够部署、配置数据防护设备产品	2.8.1 主流数据安全产品的基本概念和功能配置原理 2.8.2 数据安全技术工具基本工作原理
	2.9 数据安全服务运维保障	2.9.1 能够运行维护数据安全证书服务系统 2.9.2 能够运行维护数据存储加密服务系统 2.9.3 能够运行维护数据安全可信隐私计算服务系统	2.9.1 加密技术 2.9.2 隐私计算服务知识
	2.10 数据安全重保服务	2.10.1 能够根据数据安全重保服务方案要求，提供重保服务	2.10.1 重保系统知识

		2.10.2 能够记录数据安全重保服务完成情况	
	2.11 数据安全应急响应	2.11.1 能够按照数据安全应急演练服务方案，实施应急响应	2.11.1 数据安全应急响应操作规则
3.数据安全防护	3.1 数据安全防护方案实施	3.1.1 能够根据数据采集保护方案要求，对数据采集工具或系统进行防护功能相关操作 3.1.2 能够部署、配置和使用数据采集保护产品	3.1.1 主流数据安全产品的基本概念和功能配置原理
	3.2 大数据安全防护方案实施	3.2.1 能对业务系统防护计划进行实施 3.2.2 能对大数据防护计划进行实施 3.2.3 能对业务系统安全防护方案进行测试 3.2.4 能实施大数据测试安全防护方案	3.2.1 数据安全技术工具基本工作原理 3.2.2 大数据技术防护知识
4.数据安全处理	4.1 个人信息隐私保护与核查	4.1.1 能够根据个人信息隐私保护方案要求，配置隐私保护规则 4.1.2 能够根据个人信息隐私保护方案要求，部署和使用隐私保护产品和工具 4.1.3 能够根据个人信息隐私保护方案要求，使用和维护隐私保护平台 4.1.4 能够对个人信息隐私保护实施核查	4.1.1 个人信息保护规定
	4.2 数据脱敏	4.2.1 能够根据个人信息隐私保护方案要求，进行数据脱敏相关操作 4..2.2 能够根据个人信息隐私保护方案要求，部署和使用数据脱敏保护产品和工具	4.2.1 数据脱敏知识
	4.3 数据安全分析处理	4.3.1 能够使用工具进行数据安全分析 4.3.2 能够使用工具进行数据安全导出导入存储 4.3.3 能够根据规范要求在安全环境下进行数据使用	4.3.1 主流数据分析工具
	4.4 数据安全处理策略核查	4.4.1 能够对数据安全处理策略实施核查	4.4.1 数据安全处理策略
5.数据安全运营	5.1 数据安全增强	5.1.1 能够进行操作系统安全增强配置 5.1.2 能够进行数据库安全增强配置 5.1.3 能够进行中间件安全增强配置 5.1.4 能够进行应用安全增强配置 5.1.5 能够进行大数据系统安全增强配置 5.1.6 能够进行数据防勒索设备产品的部署使用	5.1.1 操作系统安装知识及安全机制 5.1.2 云计算及虚拟化部署知识及安全基线配置 5.1.3Linux 系统基础操作知识及安全基线配置
	5.3 数据安全运维	5.3.1 堡垒机部署和配置设备产品使用	5.3.1 数据库堡垒机、跳板机等工具的功能配置原理
	5.4 数据防护	5.4.1 能够对数据防护设备产品进行部署	5.4.1 主流数据防护设备

	监测设备使用	和配置 5.4.2 能够使用安全审计与入侵监测设备产品 5.4．3 能够使用数据安全态势监测设备产品	原理
	5.5 数据安全应急响应	5.5.1 能够按照制定的数据安全应急方案进行响应处理	5.5.1 数据安全应急响应机制
	5.6 数据安全配置核查	5.6.1 能够按照操作系统安全配置基线进行核查操作 5.6.2 能对数据库安全配置基线进行核查操作 5.6.3 能对中间件安全配置基线进行核查操作 5.6.4 能对应用安全配置基线进行核查操作 5.6.5 能对大数据系统安全配置基线进行核查操作	5.6.1 数据组件安装知识及安全基线配置 5.6.2 数据集群配置知识及安全基线配置 5.6.3 数据组件安全基础操作知识
	5.7 数据保护能力核查	5.7.1 能对数据防勒索设备产品有效性进行核查 5.7.2 能对堡垒机部署和配置设备产品有效性进行核查 5.7.3 能对安全审计与入侵监测设备产品有效性进行核查 5.7.4 能对数据安全态势监测设备产品有效性进行核查 5.7.5 能对数据防护设备产品有效性进行核查	5.7.1 数据安全技术工具的工作原理和制度规范编写要求
	5.8 数据应用代码安全审核	5.8.1 能对数据应用安全代码进行审核	OWASP TOP 10 漏洞 CWE TOP
	5.9 数据应用安全测试	5.9.1 能够使用测试工具或人工执行数据应用安全测试用例 5.9.2 能够观测、记录数据安全测试测试执行结果 5.9.3 能够使用端口扫描、数据漏洞扫描、Web 安全应用漏洞扫描、网络协议分析等测试工具	5.9.1 软件测试基础知识 5.9.2 漏洞扫描工具使用方法
6.数据安全管理	6.1 数据安全防泄漏产品的配置使用	6.1.1 能够进行数据安全防泄漏设备产品部署 6.1.2 能够使用数据安全防泄漏产品对业务系统进行保护 6.1.3 能够使用数据安全防泄漏产品对数据进行加密保护 6.1.4 能够使用防护产品对数据流转进行审计	6.1.1 主流数据安全产品的防护原理、部署及使用方法

	6.2 数据安全合规监测	6.2.1 能对日常的数据库进行安全漏洞扫描 6.2.2 能利用测试工具进行数据库安全渗透测试	6.2.1 数据库安全漏洞工具应用知识
7.数据安全评估	7.1 数据库安全风险评估	7.1.1 能够数据库安全风险评估方案进行实施	7.1.1 主流数据库安全产品的部署配置原理
	7.2 大数据系统安全风险评估	7.2.1 能够对大数据系统安全风险评估方案进行实施	7.2.1 大数据安全漏洞基本知识 7.2.2 大数据系统安全漏洞基本知识
	7.3 终端数据安全风险评估	7.3.1 能够对终端数据安全的风险评估方案进行有效实施	7.3.1 数据安全技术工具基本工作原理
	7.4 数据安全管理风险评估	7.4.1 能够编写或者受理评估申请 7.4.2 能依据安全管理规则和组织需求确定评估范围 7.4.3 能够协助企业实施数据安全管理成熟度自评 7.4.4 能够实施数据安全管理风险评估方案	7.4.1 数据管理能力成熟度评估模型知识
	7.5 数据生命周期安全风险评估和合规检查	7.6.1 能够实施数据生命周期安全风险评估方案 7.6.2 能够按照网络安全等级保护合规核查清单列表，对数据系统进行合规检查操作 7.6.3 能够按照商用密码应用合规核查清单列表，对数据系统进行合规检查操作 7.6.4 能够按照网络安全产品审查要求，对数据安全产品进行合规检查操作 7.6.5 能够收集和整理合规检查信息	7.6.1 数据生命周期相关知识 7.6.2 网络安全等级保护标准知识 7.6.3 商用密码合规知识
8.数据安全优化	8.1 数据安全质量指标信息采集	8.1.1 能够按照数据安全质量采集方案，获取数据安全质量指标信息 8.1.2 能够部署和使用数据安全质量采集工具	8.1.1 数据安全度量指标体系 8.1.1 数据安全采集工具的使用
	8.2 数据系统安全基线配置优化	8.2.1 能够按照数据系统安全基线配置优化方案，实施配置优化操作 8.2.2 能够部署和使用数据系统安全基线配置工具 8.2.3 能够观测、收集和对比数据系统安全基线配置优化效果信息 8.2.4 能够记录数据系统安全基线配置优化操作记录	8.2.1 数据安全配置知识
	8.3 数据安全设备产品配置优化	8.3.1 能够按照数据安全设备配置优化方案，实施配置优化操作 8.3.2 能够部署和使用数据安全设备优化	8.3.2 数组安全设备部署配置知识

		工具 8.3.3 能够观测、收集和对比数据安全设备产品配置优化效果信息 8.3.4 能够记录数据安全设备配置优化操作	

3.2 中级

数据安全设计方向的课程模块包括数据安全采集、数据安全处理、数据安全评估、数据安全优化、数据安全技术服务咨询；数据安全实施和运营方向的课程模块包括数据安全采集、数据安全技术服务、数据安全防护、数据安全处理、数据安全运营、数据安全管理；数据安全治理方向的课程模块包括数据安全采集、数据安全技术服务、数据安全管理、数据安全评估、数据安全优化、数据安全技术服务咨询。

课程模块	培训内容	专业能力要求	相关知识要求
1.数据安全采集	1.1 数据资产分类分级	1.1.1 能够对数据资产进行关联性分析，完善数据资产要素丰富度 1.1.2 理解分类分级要求，并对数据资产进行分类分级标注 1.1.3 能够使用工具标注数据资产类型和级别 1.1.4 能够定期更新、维护数据资产分类分级标签	1.1.1 数据分析流程 1.1.2 数据分类分级标准与原理 1.1.3 数据库性能监控方法
	1.2 数据资产信息收集	1.2.1 能够根据数据资产规范，识别数据资产 1.2.2 能够使用工具自动收集数据资产	1.2.1 数据资产规范知识
	1.3 数据分类分级标注	1.3.1 能够理解数据资产分类分级要求，标注网络信息系统的数据资产类型和等级 1.3.2 能够使用工具标注数据资产类型和级别	1．3.1 数据资产分级分类标准知识
	1.4 数据资产梳理	1.4.1 能够准确评估数据资产的价值 1.4.2 能够对数据资产进行整合汇总记录	1.4.1 数据资产的评估方法
	1.5 数据源鉴别及记录	1.5.1 能够识别数据安全威胁情报信息并整理记录 1.5.2 能够收集数据安全事件，提炼形成数据威胁报告 1.5.3 能够采集数据系统安全漏洞信息并形成漏洞报告	1.5.1 漏洞扫描相关知识及工具的使用
	1.6 数据质量跟踪和分析	1.6.1 能够评估现有制度规范、操作流程文件的合理性、有效性 1.6.2 能够基于组织现有的安全建设内容进行数据质量验证 1.6.3 能进行业务系统数据安全措施的有效性测试检查	1.6.1 规范制度、操作流程解读及评估方法 1.6.2 安全建设业务知识 1.6.3 安全攻防技术

		1.6.4 能制定数据安全现状进行分析汇总	基本知识 1.6.4 安全相关技术工具的基本知识
	1.7 数据采集安全控制	1.7.1 能依据用户业务需求明确数据业务边界 1.7.2 能参照业界通用测评方法制定数据安全评估计划 1.7.3 能制定数据业务流程梳理方案和关键信息收集清单	1.7.1 待评估数据基本业务知识 1.7.2 业界通用测评方法 1.7.3 数据访问、操作相关技术工具知识
	1.8 数据安全标准规范符合分析	1.8.1 能够识别数据安全法律法规政策信息 1.8.2 能够使用工具或人工获取数据安全法律法规政策信息	1.8.1 数据安全标准规范
	1.9 数据安全采集审计	1.9.1 能够制定数据采集审计方案 1.9.2 能够规划确定审计工具	1.9.1 数据采集审计方法 1.9.2 主流审计工具
2.数据安全技术服务	2.1 数据安全技术服务方案设计	2.1.1 能够完成数据资产梳理服务设计 2.1.2 能够完成数据资产分类分级服务设计 2.1.3 能够完成数据存储服务方案设计 2.1.4 能够完成数据安全可信隐私计算服务方案设计 2.1.5 能够完成数据安全合规检查服务方案设计 2.1.6 能够完成数据安全风险评估服务方案设计	2.1.1 技术方案设计规范 2.1.2 数据资产分类规范
	2.2 数据安全服务方案推广和组织实施	2.2.1 能够根据数据安全服务方案进行市场推广 2.2.2 能够根据数据安全服务方案组织协调相关厂商进行方案实施	2.2.1 数据安全服务技术方案编写规范
	2.3 数据安全服务支撑工具、系统、平台研发和部署	2.3.1 能够对主流数据安全服务支撑工具进行测评对比 2.3.2 能够编写测评报告，分析优劣，出具分析报告	2.3.1 数据安全服务关键技术知识 2.3.2 数据安全防护方案技术与原理
	2.4 数据安全技术服务规范	2.4.1 能够完成数据安全服务质量评估分析和改进 2.4.2 能够执行数据资产梳理服务流程与规范 2.4.3 能够执行数据资产分类分级服务流程与规范 2.4.4 能够执行数据存储服务流程与规范 2.4.5 能够执行数据安全可信隐私计算服务流程与规范 2.4.6 能够执行数据安全风险评估服务流程与规范	2.4.1 数据安全技术服务规范与流程
3.数	3.1 数据安	3.1.1 能够设计数据安全防护方案，并根据方案	3.1.1 数据安全产品

据安全防护	全防护方案设计与实施	进行防护功能相关协调部署 3.1.2 能够部署、配置和使用数据采集保护产品	的基本概念和功能配置原理
	3.2 业务系统安全防护方案设计与实施	3.2.1 能够设计业务系统防护方案 3.2.2 能够业务系统防护计划进行部署实施，系统评估	3.2.1 数据安全技术工具基本工作原理
	3.3 大数据安全防护方案设计实施	3.3.1 能够设计大数据防护部署方案 3.3.2 能够对大数据防护计划进行实施	3.3.1 大数据技术防护知识
4. 数据安全处理	4.1 个人信息隐私保护方案设计	4.1.1 能够根据个人信息隐私保护方案要求，设计隐私保护规则	4.1.1 个人信息保护规范
	4.2 数据脱敏方案设计	4.2.1 能够根据个人信息隐私保护方案要求，设计数据脱敏方案	4.2.1 数据脱敏原则
	4.3 数据安全分析处理方案设计	4.3.1 能够设计数据安全分析方案	4.3.1 数据安全处理原则
	4.4 数据安全处理方案组织实施监督	4.3.1 能够使用工具进行数据安全方案的实施 4.3.2 能够使用工具进行数据安全导出导入存储，分析出具分析报告 4.3.3 能够根据规范要求在安全环境下进行数据使用，并优化实施方案	4.3.1 主流数据分析工具
5.数据安全运营	5.1 数据安全运营方案设计	5.1.1 能够设计数据安全运营管控技术方案 5.1.2 能够设计数据应用安全开发技术方案 5.1.3 能够设计数据安全运维与监管技术方案 5.1.4 能够设计数据安全应急响应技术方案 5.1.5 能够设计数据备份与业务容灾技术方案	
	5.2 数据安全增强策略制定维护	5.1.1 能够规划操作系统、数据库等安全增强配置策略 5.1.2 能够制定进行大数据系统安全增强配置策略 5.1.3 能够进行数据防勒索设备产品的协调部署使用	5.1.1 操作系统安装知识及安全机制 5.1.2 云计算及虚拟化部署知识及安全基线配置 5.1.3Linux 系统基础操作知识及安全基线配置
	5.3 数据安全运维策略规划	5.3.1 能够完成堡垒机部署和配置设备产品使用 5.3.2 能够根据定期巡检方案进行设备的维护巡检	5.3.1 数据安全产品技术工具场景应用知识 5.3.2 数据安全运营知识
	5.4 数据防护监测设备规划部署	5.4.1 能够规划数据防护设备产品部署方案 5.4.2 能够完成安全审计与入侵监测设备部署方案确定 5.4. 3 能够确定数据安全态势监测设备产品形	5.4.1 数据安全技术工具的工作原理和制度规范编写要求

		态	
	5.5 数据安全应急响应方案制定	5.5.1 能够按照制定的数据安全应急方案进行响应处理	5.5.1 数据安全应急响应规范
	5.6 数据安全配置核查	5.6.1 能够按照操作系统安全配置基线进行核查操作 5.6.2 能够完成数据库安全配置基线进行核查操作 5.6.3 能够完成中间件安全配置基线进行核查操作 5.6.4 能够完成应用安全配置基线进行核查操作 5.6.5 能够完成大数据系统安全配置基线进行核查操作	5.6.1 数据组件安装知识及安全基线配置 5.6.2 数据集群配置知识及安全基线配置 5.6.3 数据组件安全基础操作知识
	5.7 数据保护能力规范制定	5.7.1 能够完成数据防勒索设备产品有效性核查 5.7.2 能够完成堡垒机部署和配置设备产品有效性核查 5.7.3 能够完成安全审计与入侵监测设备产品有效性核查 5.7.4 能够完成数据安全态势监测设备产品有效性核查 5.7.5 能够完成数据防护设备产品有效性核查	5.7.1 组织内现有相关安全建设涉及的业务知识 5.7.2 基础安全攻防技术基本知识 5.7.3 常用安全相关技术工具的基本知识
	5.8 数据应用代码安全规范制定	5.8.1 能够完成数据应用安全代码审核	5.8.1 OWASP TOP 10 漏洞 5.8.2 CWE TOP
	5.9 数据应用安全测试方案制定	5.9.1 能够编写数据安全应用测试用例 5.9.2 能够分析数据安全测试测试执行结果 5.9.3 能够规划端口扫描、数据漏洞扫描、Web 安全应用漏洞扫描、网络协议分析等测试工具	5.9.1 数据库渗透测试基本原理及方法 5.9.2 数据库安全漏洞工具应用知识
6.数据安全管理	6.1 数据安全建设方案设计	6.1.1 能够完成数据管理中心建设方案设计 6.1.2 能够完成数据防泄漏管理建设方案设计 6.1.3 能够完成数据安全合规建设方案设计 6.1.4 能够完成数据流转管理建设方案设计	6.1.1 数据管理中心建设规范
	6.1 数据安全防泄漏产品的选型规划	6.1.1 能够完成数据安全防泄漏设备产品选型方案规划 6.1.2 能够使用数据安全防泄漏产品对业务系统进行防护方案制定 6.1.3 能够使用数据安全防泄漏产品对数据进行加密保护策略制定 6.1.4 能够使用防护产品对数据流转进行审计规划	6.1.1 常用安全相关技术工具
	6.2 数据安全合规策略	6.2.1 能够执行数据分类分级管理策略与规范 6.2.2 能够执行数据防泄漏管理策略与规范	6.2.1 数据安全合规性策略

	与规范	6.2.3 能够执行数据安全合规策略与规范 6.2.4 能够执行数据安全风险管理策略与规范 6.2.5 能够执行网络安全等级保护合规管理策略与规范	
7.数据安全评估	7.1 设计数据安全风险评估方案	7.1.1 能够设计数据库安全风险评估方案 7.1.2 能够设计大数据系统安全风险评估方案 7.1.3 能够设计终端数据安全风险评估方案 7.1.4 能够设计数据安全管理风险评估方案 7.1.5 能够设计数据生命周期安全风险评估方案 7.1.6 能够设计数据安全机制有效性验证评估方案	7.1.1 数据安全评估方案与管理规范
	7.2 数据库安全风险评估	7.2.1 能够完成数据库安全风险评估方案确定	
	7.3 大数据系统安全风险评估	7.3.1 能够完成大数据系统安全风险评估方案确定	7.3.1 大数据系统及组件安全漏洞知识及评估方法 7.3.2 大数据系统及组件安全漏洞修复机制及基本原理
	7.4 终端数据安全风险评估	7.4.1 能够完成终端数据系统安全风险评估方案确定	7.4.1 数据安全风险知识
	7.5 数据安全管理风险评估	7.5.1 能够编写数据安全风险评估申请 7.5.2 能依据安全管理规则和组织需求确定评估方案 7.5.3 能够协助企业制定数据安全管理成熟度自评方案 7.5.4 能够制定数据安全管理风险评估方案	7.5.1 数据管理能力成熟度评估模型知识
	7.6 数据生命周期安全风险评估	7.6.1 能够完成数据生命周期安全风险评估方案制定并实施	7.6.1 数据生命周期知识
	7.7 数据安全合规策略及规范制定	7.7.1 能够按照网络安全等级保护合规核查清单列表对数据系统进行合规策略及规范进行制定 7.7.2 能够按照商用密码应用合规核查清单列表对数据系统进行合规策略及规范制定 7.7.3 能够按照网络安全产品审查要求对数据安全产品进行合规策略及规范制定 7.7.4 能够收集和整理合规检查信息通过分析给出合理建议	7.7.1 网络安全等级保护标准知识 7.7.2 商用密码合规知识
8.数据安	8.1 数据安全优化设计	8.1.1 能够完成数据安全质量指标设计 8.1.2 能够完成数据安全方案调整设计	8.1.1 数据安全检测原理

全优化		8.1.3 能够完成数据安全渗透测试方案设计 8.1.4 能够完成数据安全检查方案设计	
	8.2 数据安全优化方案组织测试实施	8.2.1 能组织实施数据安全渗透测试 8.2.2 能组织实施数据安全检查	8.2.1 数据安全巡检方法 8.2.2 渗透测试知识
	8.3 数据安全质量指标信息采集	8.3.1 能够按照数据安全质量采集方案，获取数据安全质量指标信息 8.3.2 能够部署和使用数据安全质量采集工具 8.3.3 能够整理和汇总数据安全质量指标信息	8.1.1 数据安全度量指标体系 8.1.1 数据安全采集工具的使用
	8.4 数据系统安全基线配置优化	8.4.1 能够按照数据系统安全基线配置优化方案，实施配置优化操作 8.4.2 能够部署和使用数据系统安全基线配置工具 8.4.3 能够观测、收集和对比数据系统安全基线配置优化效果信息 8.4.4 能够记录数据系统安全基线配置优化操作记录	8.2.1 数据安全配置知识
	8.5 数据安全设备产品配置优化	8.5.1 能制定数据安全设备配置优化方案，实施配置优化操作 8.5.2 能够观测、收集和对比数据安全设备产品配置优化效果信息整理汇总 8.5.4 能够记录数据安全设备配置优化操作形成优化报告	8.3.2 数组安全设备部署配置知识
	8.3 数据安全优化策略与规范	8.3.1 能够完成数据安全治理效果质量评估 8.3.2 能够完成定期评审数据安全治理策略与规范 8.3.3 能够完成修订数据安全治理策略与规范	8.3.1 数据安全优化策略
9.数据安全技术服务咨询	9.1 数据安全技术服务咨询方案设计	9.1.1 能够完成数据安全目标分析与理解 9.1.2 能够完成数据安全需求分析与建设规划 9.1.3 能够完成数据安全保护体系框架设计 9.1.4 能够完成网络安全等级保护整改方案设计 9.1.5 能够完成商用密码应用安全整改方案设计	9.1.1 网络安全等级保护规范
	9.2 数据安全技术产品方案对比	9.2.1 能够撰写数据安全技术对比方案	9.2.1 等级保护方案编写规范 9.2.2 评估系统知识 9.2.3 统计分析知识
	9.3 数据安全服务规范	9.3.1 能够完成数据服务系统等级保护定级备案 9.3.2 能够完成数据服务系统等级保护测评 9.3.3 能够完成数据安全合规管理测评 9.3.4 能够完成数据安全管理能力成熟度分析	

		和测评 9.3.5 能够完成数据安全产品审查 9.3.6 能够完成数据安全意识和技术教育培训	

3.3 高级

课程模块	培训内容	专业能力要求	相关知识要求
1.数据安全采集	1.1 数据安全采集策略规范	1.1.1 能够编制、修订数据安全采集策略规范； 1.1.2 能够建立配套工作机制，推进实施数据安全采集策略规范	1.1.1 常用安全相关技术工具的基本知识
	1.2 数据安全采集机制构建	1.2.1 能够建立数据安全采集工作机制，指导、监督、评估数据安全采集工作任务实施 1.2.2 能够理解、分析和利用收集到数据安全，包括数据安全标准规范符合分析、数据安全法律合规要求分析、数据安全脆弱性分析	1.2.1 规范制度、操作流程解读及评估方法 1.2.2 组织内现有相关安全建设涉及的业务知识 1.3.3 基础安全攻防技术基本知识
2.数据安全技术服务	2.1 数据安全技术服务流程规范制定	2.1.1 能够制定数据资产梳理服务流程与规范、数据资产分类分级服务流程与规范、数据安全证书服务流程与规范、数据存储加密服务流程与规范、数据安全可信隐私计算服务流程与规范、APP应用安全隐私检查服务流程与规范、数据安全合规检查服务流程与规范、数据安全风险评估服务流程与规范、数据安全重保服务流程与规范、数据安全应急演练服务流程与规范 2.1.2 能够根据企业数据安全需求实际情况变化，修订数据安全技术服务流程、规范 2.1.3 能够确保数据安全技术服务流程、规范落实行业安全最佳实践	2.1.1 数据安全服务技术方案编写规范
	2.2 数据安全技术服务实施指导和监督	2.2.1 能够识别数据安全技术服务实施过程问题，给出指导解决方案 2.2.2 能够跟踪获取数据安全技术服务实施过程质量，优化改进	2.2.1 数据安全技术服务实施规范
3.数据安全防护	3.1 数据防护策略和规范制定	3.1.1 能够根据企业数据安全防护需求，制定数据采集安全策略与规范、数据传输加密策略与规范、数据存储安全策略与规范、终端数据保护策略与规范、文件服务器保护策略与规范、电子邮件数据保护策略与规范、 数据库保护策略与规范、网站数据保护策略与规范、大数据安全保护策略与规范 3.1.2 能够根据企业数据安全需求实际情况变化，修订数据安全防护策略、规范	3.1.1 主流数据安全产品的基本概念和功能配置原理

		3.1.3 能够确保数据安全防护策略、规范落实行业安全最佳实践	
	3.2 数据防护策略和规范实施指导和监督	3.2.1 能够识别数据安全防护策略、规范实施过程问题，给出指导解决方案 3.2.2 能够跟踪获取数据安全防护策略、规范实施过程质量，优化改进	3.2.1 数据安全技术工具基本工作原理
4. 数据安全处理	4.1 数据安全处理策略和规范制定	4.1.1 能够制定个人信息隐私保护策略与规范 、数据脱敏策略与规范、数据加密策略与规范、数据交换安全策略与规范、数据应用开发安全策略与规范、数据分析安全策略与规范、数据正当使用策略与规范 、数据导入导出安全策略与规范、数据处理环境安全策略与规范 4.1.2 能够根据企业数据安全需求实际情况变化，修订数据安全处理策略、规范 4.1.3 能够确保数据安全处理策略、规范落实行业安全最佳实践	4.1.1 数据安全处理策略
	4.2 数据处理安全策略和规范实施指导和监督	4.2.1 能够识别数据安全处理策略、规范实施过程问题，给出指导解决方案 4.2.2 能够跟踪获取数据安全处理策略、规范实施过程质量，优化改进	4.2.1 数据安全处理规范
5.数据安全运营	5.1 数据安全运营机制构建	5.1.1 能够参照国家、行业网络信息安全标准规范，制定数据安全运营规划 5.1.2 指导、监督、搭建数据安全运营支撑系统、平台 5.1.3 能够建立数据安全运营工作流程，执行数据安全运营策略和规范 5.1.4 能够识别数据安全运营风险，制定应急响应机制、流程、规范，开展数据安全应急演练	5.1.1 数据安全运营机构
	5.2 数据安全运营策略和规范制定	5.2.1 能够按照企业业务数据安全要求，制定数据安全管控风险策略与规范、数据服务平台保护策略、防范恶意攻击策略与规范、数据应用安全开发策略与规范、数据安全内部防范策略与规范、数据安全运维与监管策略与规范、数据外包服务安全策略与规范、数据安全应急响应策略与规范、数据备份与业务容灾策略与规范、数据安全共享开发策略与规范、数据安全使用策略与规范 5.2.2 能够确保数据安全运营策略、规范落实行业安全最佳实践	5.2.1 数据安全运营策略 5.2.2 数据安全运营规范
	5.3 数据运营安全策略、规范实施指导和监	5.3.1 能够识别数据安全运营策略、规范实施过程问题，给出指导解决方案 5.3.2 能够跟踪获取数据安全运营策略、规范实施过程质量，优化改进	5.3.1 数据安全产品技术工具场景应用知识 5.3.2 数据安全运营

	督		知识
6.数据安全管理	6.1 数据安全管理机制构建	6.1.1 能够建立数据安全管理工作流程，执行数据安全管理策略和规范 6.1.2 能够指导、监督、搭建数据安全管理支撑系统、平台 6.1.3 能够识别数据安全运营风险，制定应急响应机制、流程、规范，开展数据安全应急演练	6.1.1 数据安全平台管理规范
	6.2 数据安全管理策略、规范制定	6.2.1 能够按照企业数据安全要求，制定数据分类分级管理策略与规范、数据防泄漏管理策略与规范、文档安全管控策略与规范、数据安全合规策略与规范、 数据流转管理策略与规范、 数据泄露溯源管理策略与规范、数据安全风险管理策略与规范、数据人员安全管理策略与规范、 数据系统建设管理策略与规范、数据系统运维管理策略与规范、数据安全测评管理策略与规范、网络安全等级保护合规管理策略与规范 6.2.2 能够确保数据安全管理策略、规范落实行业安全最佳实践	6.1.1 常用安全相关技术工具
	6.3 数据安全管理策略、规范实施指导和监督	6.3.1 能够识别数据安全运营策略、规范实施过程问题，给出指导解决方案 6.3.2 能够跟踪获取数据安全运营策略、规范实施过程质量，优化改进	
	6.4 数据安全管理体系认证	6.4.1 能够参考信息安全管理标准、数据安全管理成熟度标准，对标数据安全管理差距分析 6.4.2 能够建立第三方评估合作关系，开展数据安全管理体系认证工作	
7.数据安全评估	7.1 数据安全风险评估机制构建	7.1.1 能够建立数据安全评估工作流程，执行数据安全评估策略和规范 7.1.2 能够指导、监督、搭建数据安全评估支撑系统、平台 7.1.3 能够识别数据安全评估风险，制定应急响应机制、流程、规范，开展应急演练	7.1.1 数据安全风险知识
	7.2 数据安全风险评估规范制定和评审	7.2.1 能够按照企业数据安全要求，制定制定网络安全等级保护合规核查规范、商用密码应用安全合规核查规范、数据安全产品合规核查规范、数据安全风险评估规范 7.2.2 能够确保数据安全评估规范落实行业安全最佳实践	7.2.1 数据库备份与恢复基础知识
	7.3 数据安全风险评估规范实施指导和监督	7.3.1 能够识别数据安全评估规范实施过程问题，给出指导解决方案 7.3.2 能够跟踪获取数据安全评估规范实施过程质量，优化改进	7.3.1 大数据系统及组件安全漏洞知识及评估方法 7.3.2 大数据系统及组件安全漏洞修复机

			制及基本原理
8.数据安全优化	8.1 数据安全质量机制构建	8.1.1 能够建立数据安全优化工作流程，指导监督执行数据安全优化策略、规范 8.1.2 能够指导、监督、搭建数据安全质量支撑系统、平台 8.1.3 能够识别数据安全优化风险，制定应急响应机制、流程、规范，开展应急演练	
	8.2 数据安全应用创新	8.2.1 能够组织开展数据安全应用创新活动，掌握数据安全前沿技术发展动态 8.2.2 能够调研、分析数据应用安全问题，结合业务安全应用场景，引入最新解决方案	8.2.1 数据安全巡检方法 8.2.2 渗透测试知识
	8.3 数据安全持续改进	8.3.1 能够正确评估数据安全治理效果质量，提出改进方案 8.3.2 能够定期评审数据安全治理策略与规范 8.3.3 能够修订数据安全治理策略与规范 8.3.4 能够指导、监督、评估组织实施数据安全创新技术方案	8.1.1 数据安全度量指标体系 8.1.1 数据安全采集工具的使用
9.数据安全技术服务咨询	9.1 数据安全评审	9.1.1 能够根据企业单位数据安全需求，独立评审数据安全技术方案、数据安全策略、数据安全规范 9.1.2 能够撰写数据安全评审报告	
	9.2 数据安全攻击调查取证	9.2.1 能够运用工具或人工操作，获取网络攻击相关电子证据 9.2.2 能够阅读查看数据安全运营审计记录，分析数据安全攻击活动 9.2.3 能够协助相关部门，实施数据攻击溯源	9.2.1 等级保护方案编写规范 9.2.2 评估系统知识 9.2.3 统计分析知识
	9.3 数据安全管理建设	9.3.1 能够阅读、理解国内外数据安全管理、技术标准规范和法律法规政策 9.3.2 能够参考相关标准规范，企业数据安全对标差距分析，给出整改建设方案 9.3.3 能够指导企业开展数据安全对标整改建设	9.3.1 商用密码保护方案编写规范 9.3.2 评估系统知识 9.3.3 统计分析知识
	9.4 数据安全审查	9.4.1 能够理解法律法规政策要求，开展数据安全产品、数据服务合规审查工作 9.4.2 能够协助第三方，给出数据安全审查报告	9.4.1 等级保护方案编写规范 9.4.2 评估系统知识 9.4.3 统计分析知识
	9.5 数据安全教育培训	9.5.1 能够指导和开展数据安全管理政策宣贯活动 9.5.2 能够制定、实施数据安全意识、数据安全技术培训方案	

4 权重表

4.1 理论知识权重表

级别 / 课程模块		初级			中级			高级
		数据安全设计方向	数据安全实施运营方向	数据安全治理方向	数据安全设计方向	数据安全实施运营方向	数据安全治理方向	
基本要求	职业道德	5	5	5	5	5	5	5
	基础知识	20	20	25	15	15	25	10
理论知识要求	数据安全采集	10	10	10	10	10	10	5
	数据安全技术服务	--	10	15	--	10	15	5
	数据安全防护	--	15	--	--	15	--	10
	数据安全处理	15	15	--	10	15	--	5
	数据安全运营	--	15	--	--	10	--	5
	数据安全管理	--	10	10	--	15	10	15
	数据安全评估	15	--	10	15	--	10	10
	数据安全优化	20	--	15	20	--	15	15
	数据安全技术服务咨询	15	--	10	20	--	10	15
合计		100	100	100	100	100	100	100

4.2 专业能力要求权重表

级别 / 课程模块		初级			中级			高级
		数据安全设计方向	数据安全实施运营方向	数据安全治理方向	数据安全设计方向	数据安全实施运营方向	数据安全治理方向	
实操能力要求	数据安全采集	15	15	15	15	15	15	10
	数据安全技术服务	--	15	20	--	15	20	10
	数据安全防护	--	15	--	--	15	--	10
	数据安全处理	20	15	--	20	15	--	10
	数据安全运营	--	20	--	--	20	--	5
	数据安全管理	--	20	15	--	20	15	15
	数据安全评估	25	--	15	20	--	15	10
	数据安全优化	20	--	15	25	--	15	15
	数据安全技术服务咨询	20	--	20	20	--	20	15
合计		100	100	100	100	100	100	100