信息安全测试员（个人信息保护合规管理员）

国家职业标准

（征求意见稿）

1 职业概况

1.1 职业(工种)名称

信息安全测试员[1]（个人信息保护合规管理员）

1.2 职业(工种)编码

4-04-04-04-003

1.3 职业(工种)定义

从事个人信息保护合规检测，个人信息收集、存储、使用、加工、传输、提供、公开、删除等环节中的安全保护以及合规管理工作的技术人员。

1.4 职业技能等级

本职业工种共设三个等级，分别为：三级/高级工、二级/技师、一级/高级技师。

1.5 职业环境条件

室内，常温。

1.6 职业能力特征

具有较好的学习、观察、分析、推理和判断、表达、计算、色觉、视觉和行为能力，动作协调，心理健康。

1.7 普通受教育程度

高中毕业（或同等学力）。

1.8 职业培训要求

1.8.1 培训参考时长

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

---

[1]本职业分为渗透测试员、合规测试员、个人信息保护合规管理员三个工种，本标准仅针对个人信息保护合规管理员工种。

1.8.2 培训教师

培训四级/中级工的教师应具有本职业三级/高级工及以上职业资格（职业技能等级）证书或相关专业中级及以上专业技术职务任职资格；培训三级/高级工的教师应具有本职业二级/技师及以上职业资格（职业技能等级）证书或相关专业中级及以上专业技术职务任职资格；培训二级/技师的教师应具有本职业一级/高级技师职业资格（职业技能等级）证书或相关专业高级专业技术职务任职资格；培训一级/高级技师的教师应具有本职业一级/高级技师职业资格（职业技能等级）证书2年以上或相关专业高级专业技术职务任职资格2年以上。

1.8.2 培训场所设备

理论教学教室在标准教室或机房进行。操作技能培训场地在具有必备的安全设备、软硬件、设施设备的场所进行。

1.9 职业技能评价要求

1.9.1 申报条件

具备以下条件之一者，可申报三级/高级工：

（1）累计从事本职业或相关职业工作满10年。

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

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

（4）取得本专业或相关专业的技工院校高级工班及以上毕业证书（含在读应届毕业生）。

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

（6）取得经评估论证的高等职业学校、专科及以上普通高等学校本专业或相

关专业的毕业证书（含在读应届毕业生）。

具备以下条件之一者，可申报二级/技师：

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

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

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

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

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

具备以下条件者，可申报一级/高级技师：

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

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

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

1.9.2 评价方式

评价方式分为理论知识考试、操作技能考核以及综合评审。

理论知识考试以笔试、机考等方式为主，主要考核从业人员从事本职业应掌握的基本要求和相关知识要求。

操作技能考核主要采用实际操作、模拟或仿真操作等方式进行，主要考核从业人员从事本职业应具备的技能水平；

综合评审主要针对二级/技师和一级/高级技师，通常采取审阅申报材料、答辩等方式进行全面评议和审查。

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

1.9.3 监考人员、考评人员与考生配比

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

1.9.4 评价时长

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

1.9.5 评价场所设备

理论知识考试在标准教室或机房进行；操作技能考核在具有必备的安全设备、软硬件、设施设备的场所进行。

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，保密合规。

（2）廉洁自律，可靠可信。

（3）牢记职责，爱岗敬业。

（4）客观严谨，公平公正。

（5）流程规范，操作安全。

（6）认真负责，团结协作。

（7）挑战自我，勇于创新。

2.2 基础知识

2.2.1 计算机相关知识

（1）计算机软硬件基础知识。

（2）操作系统基础知识。

（3）数据库基础知识。

（4）密码学基础知识。

（5）计算机编程基础知识。

（6）应用数据采集原理。

（7）软件测试基础知识。

2.2.2 网络及安全相关知识

（1）网络协议基础知识。

（2）组网设备基础知识。

（3）网络配置、故障排查常用命令和工具。

（4）网络安全基础知识。

（5）数据安全基础知识。

（6）风险评估基础知识。

2.2.3 相关法律、法规、标准知识

（1）《中华人民共和国劳动法》的相关知识。

（2）《中华人民共和国民法典》的相关知识。

（3）《中华人民共和国个人信息保护法》的相关知识。

（4）《中华人民共和国数据安全法》的相关知识。

（5）《中华人民共和国网络安全法》的相关知识。

（6）《中华人民共和国密码法》的相关知识。

（7）GB/T 35273《信息安全技术 个人信息安全规范》的相关知识。

（8）《数据出境安全评估办法》、《个人信息出境标准合同办法》的相关知识。

（9）其它个人信息保护相关法律法规、管理规定、标准的相关知识。

3 工作要求

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

3.1 三级/高级工

职业功能	工作内容	技能要求	相关知识要求
1.个人信息合规检测	1.1 个人信息保护政策文本检测	1.1.1 能对联网应用或设备中隐私政策的独立性、易读性、准确性进行检测 1.1.2 能对联网应用或设备中收集个人信息类型进行检测 1.1.3 能对联网应用或设备中隐私政策等文件的不合理条款进行检测	1.1.1 联网应用或设备中隐私政策相关法律法规和检测方法 1.1.2 个人信息类型知识 1.1.3 联网应用或设备中个人信息处理法律法规相关要求
	1.2 个人信息收集、共享等行为检测	1.2.1 能对联网应用或设备收集个人信息的目的、方式、范围进行检测 1.2.2 能对联网应用或设备中索权程度、捆绑授权行为进行检测或判定 1.2.3 能对联网应用或设备收集的个人信息共享及其合规性进行检测	1.2.1 联网应用或设备收集个人信息检测方法 1.2.2 联网应用或设备收集个人信息合规要点及常见的违法违规行为知识 1.2.3 个人信息共享合法合规性检测知识
	1.3 用户权利保障检测	1.3.1 能对联网应用或设备收集个人信息时告知同意的方式、方法、内容的合规性进行检测 1.3.2 能对联网应用或设备中反馈申诉权利进行检测 1.3.3 能对联网应用或设备使用过程中个人信息主体对其个人信息自主控制范围、权限、方式的合规性检测	1.3.1 联网应用或设备中用户权利相关法律法规相关要求 1.3.2 联网应用或设备中用户权利检测方法
2.个人信息合	2.1 核验分析	2.1.1 能对联网应用或设备的业务功能进行核验 2.1.2 能对联网应用或设备收集使用的个人信息进行核验	2.1.1 联网应用或设备的业务功能核验方法 2.1.2 联网应用或设备的业务个人信息核验方法
	2.2 监控分析	2.2.1 能对联网应用或设备实施监控并分析侵犯个人信息的问题及风险	2.2.1 联网应用或设备监控方法 2.2.2 联网应用或设备侵

规分析		2.2.2 能对联网应用或设备利用的软件开发包（SDK）实施监控并分析侵犯个人信息的问题及风险	犯个人信息风险分析方法 2.2.3 联网应用或设备软件开发包（SDK）利用情况分析方法 2.2.4 联网应用或设备利用的软件开发包（SDK）监控方法
	2.3 代码审计	2.3.1 能对联网应用或设备调用的接口行为代码进行安全性审计 2.3.2 能对联网应用或设备个人权限声明代码进行合规性审计	2.3.1 代码审计知识 2.3.2 个人信息保护代码（重点包括个人信息收集、身份及访问控制、传输及共享、日志、归档及个人信息删除等模块）审计知识
3.个人信息合规管理	3.1 报告编写	3.1.1 能使用工具生成个人信息合规检测报告 3.1.2 能根据国家相关规定编写个人信息合规检测报告	3.1.1 常见的合规报告工具使用方法 3.1.2 个人信息合规检测报告撰写方法
	3.2 合规整改	3.2.1 能根据检测报告提供整改建议 3.2.2 能根据检测报告实施整改 3.2.3 能在整改后实施回归测试，验证整改的有效性	3.2.1 检测报告识读方法 3.2.2 整改建议知识 3.2.3 回归测试知识

3.2 二级/技师

职业功能	工作内容	技能要求	相关知识要求
1.个人信息合规检测	1.1 个人信息收集安全性检测	1.1.1 能对联网应用或设备个人信息收集过程的合法性进行检测 1.1.2 能对联网应用或设备个人信息收集最小必要性进行检测	1.1.1 联网应用或设备个人信息收集过程合规检测方法及要点 1.1.2 个人信息收集最小必要性原则知识 1.1.3 最小必要性检测方法
	1.2 个人信息存储、传输安全性检测	1.2.1 能对联网应用或设备个人信息存储过程的安全性进行检测 1.2.2 能对联网应用或设备个人信息传输过程的安全性进行检测 1.2.3 能对个人信息匿名化、去标识化等措施进行效果评估	1.2.1 联网应用或设备个人信息存储数据识读方法 1.2.2 联网应用或设备个人信息传输过程安全性测试方法 1.2.3 个人信息匿名化、去标识化及效果评估知识
	1.3 个人信息使用安全性检测	1.3.1 能对联网应用或设备个人信息的访问控制安全性进行检测 1.3.2 能对联网应用或设备个人信息的使用限制进行检测 1.3.3 能对个人信息展示进行个人信息安全检测 1.3.4 能对互联网信息服务推荐算法不当使用等违法违规行为进行检测	1.3.1 联网应用或设备个人信息的访问控制规则识读及安全性检测方法 1.3.2 联网应用或设备个人信息的使用限制检测方法 1.3.3 常见的个人信息展示方法及安全性检测方法 1.3.4 互联网信息服务推荐算法合规性及检测相关知识
2.个人信息合规分析	2.1 个人信息安全事件分析	2.1.1 能采用技术手段对个人信息安全事件进行定位 2.1.2 能采用技术手段对个人信息安全事件进行溯源分析	2.1.1 个人信息安全事件定位知识和方法 2.1.3 数据溯源技术知识 2.1.4 个人信息安全事件溯源分析方法
	2.2 个人信息安全性分析	2.2.1 能对联网应用或设备进行个人信息安全性分析 2.2.2 能对联网应用或设备侵犯个人信息过程进行分析 2.2.3 能对个人信息进行差分安全分析 2.2.4 能对个人信息进行关联分析 2.2.5 能对联网应用或设备开发进行个人信息安全需求分析	2.2.1 联网应用或设备安全性分析方法 2.2.2 常见的联网应用或设备侵犯个人信息过程及分析要点 2.2.3 差分攻击知识 2.2.4 个人信息关联分析知识 2.2.5 个人信息安全需求分析方法
3.	3.1 个	3.1.1 能对联网应用或设备进	3.1.1 风险评估知识

个人信息合规管理	人信息保护影响评估	行个人信息保护影响评估，制定个人信息保护影响计划 3.1.2 能编写个人信息保护影响评估报告	3.1.2 个人信息保护影响评估知识 3.1.3 个人信息保护影响评估报告撰写方法 3.1.4 常见的个人信息安全风险
	3.2 安全事件管理	3.2.1 能制定个人信息安全事件应急预案 3.2.2 能根据预案完成应急演练，并对应急预案进行修订 3.2.3 能对恶意软件等造成的个人信息安全事件进行处置	3.2.1 个人信息安全事件应急预案制定方法 3.2.2 应急演练知识 3.2.3 常见个人信息安全事件应急处置和报告相关知识 3.2.4 恶意软件相关知识及处理方法
4.培训指导	4.1 培训实施	4.1.1 能制订培训工作计划 4.1.2 能编制和实施培训方案 4.1.3 能编写本职业培训教材、讲义、课件 4.1.4 能进行本职业培训宣讲	4.1.1 培训工作计划的制订要求、方法 4.1.2 培训方案编制和实施要求、方法 4.1.3 培训教材、讲义、课件编写知识 4.1.4 教学教法知识 4.1.5 培训质量管理体系要求、方法
	4.2 技术指导	4.2.1 能对本职业三级/高级工及以下级别人员进行技能指导 4.2.2 能对本职业三级/高级工及以下级别人员技能水平进行考核	4.2.1 操作经验和技能总结方法 4.2.2 技能和理论基础知识水平考核的要求和方法

3.3 一级/高级技师

职业功能	工作内容	技能要求	相关知识要求
1.个人信息合规检测	1.1 新场景新应用检测	1.1.1 能对新场景新应用提出个人信息合规检测方法 1.1.2 能对新场景新应用进行个人信息安全性测试	1.1.1 物联网、云计算等场景下个人信息合规测试方法 1.1.2 虚拟现实、元宇宙等新应用场景下个人信息合规测试方法
	1.2 安全漏洞检测	1.2.1 能对个人信息相关应用进行安全漏洞测试和合规检测 1.2.2 能对个人信息相关第三方软件开发包（SDK）进行安全漏洞分析 1.2.3 能采取打补丁等技术手段修复个人信息泄露漏洞 1.2.4 能采取技术措施防止个人信息泄露漏洞被利用	1.2.1 渗透测试知识 1.2.2 常用的渗透测试工具及使用方法 1.2.3 软件开发包（SDK）测试方法 1.2.4 常见的个人信息泄露漏洞及修补方法
2.个人信息合规分析	2.1 个人信息安全事件分析	2.1.1 能对侵犯个人信息安全事件的风险等级进行分析 2.1.2 能对侵犯个人信息的违法违规行为进行分析	2.1.1 个人信息安全事件分析方法 2.1.2 常见的个人信息安全事件及违法要点
	2.2 个人信息违法违规行为取证	2.2.1 能对个人信息违法违规行为进行电子数据提取、固定 2.2.2 能根据个人信息违法违规行为电子数据进行违法违规行为仿真复现	2.2.1 个人信息违法违规行为取证方法 2.2.2 数据备份及恢复方法 2.2.3 个人信息违法违规行为数据仿真复现方法
3.个人信息合规管理	3.1 个人信息保护合规体系建设	3.1.1 能根据业务特点和需求建立个人信息保护合规体系 3.1.2 能对个人信息保护能力及违法违规行为进行评审 3.1.3 能针对敏感个人信息、未成年人个人信息设计相应的保护方案 3.1.4 能对个人信息跨境合规性进行自评估 3.1.5 能对个人信息安全的防护策略进行效果分析及优化	3.1.1 个人信息分类分级知识 3.1.2 个人信息保护方案制定方法 3.1.3 敏感个人信息、未成年人个人信息保护相关法律法规知识 3.1.4 数据加密、完整性保护知识 3.1.5 个人信息跨境合规评估知识 3.1.6 隐私计算知识

			3.1.7 常见个人信息安全防护策略
	3.2 个人信息合规咨询	3.2.1 能根据业务需求对个人信息收集、存储、使用、加工、传输、提供、公开、删除等环节提出合规方案 3.2.2 能为不同应用程序和联网设备开发、制造、运营提供个人信息保护咨询	3.2.1 合规咨询的原则 3.2.2 合规咨询的流程、方法 3.2.3 个人信息收集、存储、使用、加工、传输、提供、公开、删除各环节合规要点 3.2.4 典型行业个人信息保护合规要点
4. 培训指导	4.1 培训实施	4.1.1 能对培训需求进行分析 4.1.2 能编制培训规划 4.1.3 能组织编写本职业培训教材、讲义、教案 4.1.4 能进行本职业培训宣讲	4.1.1 培训需求分析要求、方法 4.1.2 培训规划编制要求 4.1.3 培训预算与决算审核方法
	4.2 技术指导	4.2.1 能对本职业各级别人员技能进行指导 4.2.2 能对本职业各级别人员技能水平进行考核 4.2.3 能组织开展技术改造、技术革新活动	4.2.1 指导操作技能、水平考核相关知识 4.2.2 技术改造与革新方法

4 权重表

4.1 理论知识权重表

项目 \ 技能等级		三级/高级工（%）	二级/技师（%）	一级/高级技师（%）
基本要求	职业道德	5	5	5
	基础知识	10	5	5
相关知识要求	个人信息合规检测	35	35	25
	个人信息合规分析	25	25	30
	个人信息合规管理	25	25	30
	培训指导		5	5
合计		100	100	100

4.2 技能要求权重表

项目 \ 技能等级		三级/高级工（%）	二级/技师（%）	一级/高级技师（%）
技能要求	个人信息合规检测	40	35	35
	个人信息合规分析	30	30	25
	个人信息合规管理	30	30	35
	培训指导		5	5
合计		100	100	100