工业信息安全风险评估师

职业能力等级评价标准

（试行稿）

1 项目概况

1.1 项目名称

工业信息安全风险评估师

1.2 项目定义

从事工业环境中信息收集、识别、分析和评价风险的专业人员。

1.3 能力等级

本项目共设三个等级，分别为:初级、中级、高级。

1.4 能力特征

具备工业系统、网络、数据库理论基础；具备使用风险评估方法、风险评估工具，识别工业信息安全潜在风险的能力；具备数据收集与分析，能够从评估过程中提取有效信息，用于风险评估的能力；具备风险评估报告写作，反馈评估结果的能力。

1.5 职业能力等级评价要求

1.5.1 申报条件

工业和信息化部教育与考试中心
EDUCATION & EXAMINATION CENTER OF MINISTRY OF INDUSTRY AND INFORMATION TECHNOLOGY

具备以下条件之一者，可申报初级：

（1） 累计从事相关职业工作1年（含）以上。

（2） 相关专业在校学生。

具备以下条件之一者，可申报中级：

（1） 取得本项目或相关职业初级评价证书（含职业资格证书、职业技能等级证书等）后，相关专业在校学生或累计从事相关职业工作2年（含）以上。

（2） 累计从事相关职业工作4年（含）以上。

具备以下条件之一者，可申报高级：

（1） 取得本项目或相关职业中级评价证书（含职业资格证书、职业技能等级证书等）后，累计从事相关职业工作3年（含）以上。

（2） 累计从事相关职业工作6年（含）以上。

（3） 具有高等职业学校、高级技工学校、技师学院相关专业毕业证书，并取得本项目或相关职业中级评价证书（含职业资格证书、职业技能等级证书等）。

（4） 具有大专及以上相关专业毕业证书，并取得本项目或相关职业中级评价证书（含职业资格证书、职业技能等级证书等）后，累计从事相关职业工作1年（含）以上。

1.5.2 评价方式

职业能力等级评价考试包括理论知识、技能操作两个科目，较高等级必要时可增加综合评审。

理论知识考试以笔试为主，条件成熟时试点开展网络考试，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。技能操作考核主要采用现场操作、模拟操作、面试答辩等方式进行，主要考核从业人员从事本职业应具备的技能水平。综合评审通常采取审阅申报材料、技术答辩等方式进行全面评议和审查。理论知识考试和技能操作考核均采用百分制，成绩达到60分以上者为合格。

1.5.3 监考人员、考评人员与考生配比

理论知识考试和技能操作考核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。技能操作考核中考评人员为3人以上单数。

1.5.4 评价时间

理论知识考试时间不少于90分钟；技能操作考核时间:初级不少于120分钟，中级/高级不少于180分钟。

工业和信息化部教育与考试中心
EDUCATION & EXAMINATION CENTER OF MINISTRY OF INDUSTRY AND INFORMATION TECHNOLOGY

1.5.5 评价场所设备

理论知识考试：在标准教室或标准联网多媒体计算机教室进行。

技能操作考核：在标准联网多媒体计算机教室进行，考生计算机需要按照考核要求安装考试系统客户端及相关应用软件，考试结束后能完成环境的还原。

2 基本要求

2.1 职业道德

（1） 诚实守信，勤勉尽责，谨慎从业。

（2） 坚持独立、客观、公正的原则。

（3） 遵守国家法律法规。

（4） 遵守风险评估行业准则和规范。

2.2 职业守则

（1） 客观公正，保持独立性，不受各方的控制和影响。

（2）对国家秘密、商业秘密和个人隐私予以保密。

（3）遵守职业道德规范，不从事任何损害职业形象的活动。

（4）评估结果公正、合理，反映真实安全状况。

（5）不断学习新的评估方法和技术，提升自己的专业能力。

2.3 基础知识

2.3.1 计算机基础知识

（1）操作系统的原理

（2）Windows命令提示符基础命令

（3）Linux系统基础命令

（4）数据库基本概念

2.3.2 工业网络基础知识

（1）工业网络拓扑结构

（2）工业网络协议原理

（3）工业交换机工作原理

（4）工业路由器工作原理

2.3.3 工业控制系统基础知识

（1）工业系统组成

（2）工业系统运行原理

（3）工业物联网设备基本操作

（4）工业控制系统安全策略基本要求

（5）工业控制系统安全审计基本原则

2.3.4 风险评估基础知识

（1）风险评估的目的

（2）风险评估基本流程

2.3.5 相关法律、法规、标准知识

（1）《中华人民共和国网络安全法》的相关知识。

（2）《中华人民共和国数据安全法》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）《关键信息基础设施安全保护条例》的相关知识。

（5）《信息安全等级保护管理办法》的相关知识。

工业和信息化部教育与考试中心
EDUCATION & EXAMINATION CENTER, MINISTRY OF INDUSTRY AND INFORMATION TECHNOLOGY

（6）其它网络安全相关法律法规、管理规定、标准的相关知识。

3 工作要求

本标准初级、中级、高级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 初级

职业功能	工作内容	技能要求	相关知识要求
1.信息收集	1.1 资产信息收集	1.1.1 能使用资产识别调查问卷，收集评估对象资产信息，填写资产识别清单。 1.1.2 能使用重要资产调查问卷，收集重要资产信息，填写重要资产清单。	1.1.1 调研访谈方法 1.1.2 资产的概念与分类
	1.2 安全现状信息收集	1.2.1 能使用已有安全措施调查问卷，收集评估对象采用的安全措施，填写已有安全措施清单。 1.2.2 能核查重要资产信息，记录核查情况，填写重要资产核查记录。	1.2.1 安全措施分类知识 1.2.2 核查重要资产的流程和方法
2.风险识别	2.1 脆弱性识别	2.1.1 能安装与配置脆弱性扫描、渗透性测试、工控安全测试、机房检测等风险评估工具。 2.1.2 能收集被评组织的安全管理制度信息，填写安全管理制度资料清单。	2.1.1 风险评估工具的安装与配置方法 2.1.2 工业系统的架构和特点
	2.2 威胁识别	2.2.1 能收集以往安全事件人为威胁信息，填写人为威胁历史记录。 2.2.2 能收集以往安全事件环境威胁信息，填写环境威胁历史记录。	2.2.1 人为威胁分类 2.2.2 环境威胁分类
3.风险分析	3.1 信息归纳	3.1.1 能梳理脆弱性识别过程记录的信息，填写脆弱性识别表。 3.1.2 能梳理威胁识别过程记录的信息，填写威胁识别表。	3.1.1 脆弱性的定义及分类 3.1.2 威胁的定义及分类
	3.2 风险分级	3.2.1 能识别威胁利用脆弱性导致安全事件的关联，填写风险识别表。 3.2.2 能识别风险关联的资产，记录风险影响资产范围。	3.2.1 脆弱性与威胁的关系 3.2.2 风险与资产的关系

工业和信息化部教育与考试中心
EDUCATION & EXAMINATION CENTER OF MINISTRY OF INDUSTRY AND INFORMATION TECHNOLOGY

4.风险评价	4.1 风险处置	4.1.1 能指导风险处置计划的实施，记录并提交执行过程中遇到的问题。 4.1.2 能收集风险处置计划执行过程中产生的资料，撰写风险处置进度汇报文档。	4.1.1 风险处置基本流程 4.1.2 风险处置基本原则
	4.2 评估反馈	4.2.1 能汇总资产识别、风险识别、风险处置等过程文档，归档评估材料。 4.2.2 能梳理评估目标、过程、结果等信息，撰写风险评估汇报材料。	4.2.1 风险评估基本流程 4.2.2 风险评估的目的

3.2 中级

职业功能	工作内容	技能要求	相关知识要求
1.信息收集	1.1 资产信息收集	1.1.1 能制作资产识别、重要资产调查问卷。 1.1.2 能分析重要资产的保密性、完整性、可用性、业务承载性，赋值重要资产价值。	1.1.1 设计调查问卷的原则和方法 1.1.2 资产赋值方法 1.1.3 资产分类和识别要点
	1.2 安全现状信息收集	1.2.1 能制作已有安全措施调查问卷。 1.2.2 能分析风险评估方案目标与流程，制定风险评估实施计划。	1.2.1 常见安全措施类型 1.2.2 风险评估的基本流程 1.2.3 安全风险评估实施指南
2.风险识别	2.1 脆弱性识别	2.1.1 能识别并记录工业系统、网络、应用及物理设备的安全隐患。 2.1.2 能识别并记录安全管理制度缺陷。	2.1.1 风险评估工具的操作方法 2.1.2 渗透测试技术 2.1.3 漏洞扫描与挖掘技术 2.1.4 管理制度的缺陷排查方法
	2.2 威胁识别	2.2.1 能识别并记录评估对象面临的恶意及非恶意人为威胁。 2.2.2 能识别并记录评估对象面临的自然灾害及物理环境问题。	2.2.1 人为威胁识别方法 2.2.2 环境威胁识别方法
3.风险分析	3.1 风险赋值	3.1.1 能计算脆弱性被利用导致安全事件发生的损失，记录损失的资产价值。 3.1.2 能计算威胁利用脆弱性导致安全事件发生的可能性，记录威胁发生概率。	3.1.1 安全事件损失的计算方法 3.1.2 安全事件发生可能性的计算方法

工业和信息化部教育与考试中心
EDUCATION & EXAMINATION CENTER OF MINISTRY OF INDUSTRY AND INFORMATION TECHNOLOGY

	3.2 风险分级	3.2.1 能计算系统资产风险值与业务风险值，记录风险值计算结果。 3.2.2 能划分系统资产风险及业务风险等级，记录风险等级信息。	3.2.1 风险计算的原理和方法 3.2.2 风险等级划分的方法和标准
4.风险评价	4.1 风险处置	4.1.1 能分析风险处置过程遇到的问题，给出问题处理建议。 4.1.2 能梳理风险处置过程资料及结果，对比风险处置目标，撰写风险处置报告。	4.1.1 网络安全防护技术 4.1.2 系统安全防护技术 4.1.3 数据安全防护技术
	4.2 评估反馈	4.2.1 能梳理风险评估过程文件，制作关键数据图表，撰写风险评估报告。 4.2.2 能审核风险评估汇报材料的完整性、准确性、规范性，修订汇报材料内容。	4.2.1 风险评估报告的撰写规范和要求 4.2.2 数据图表的类型与适用场景 4.2.3 数据图表的制作方法

3.3 高级

职业功能	工作内容	技能要求	相关知识要求
1.信息收集	1.1 资产信息收集	1.1.1 能分析评估对象业务资产、系统资产、系统组件和单元资产等信息，编制资产识别清单模板。 1.1.2 能分析客户核心业务与资产识别清单内容，编制重要资产清单模板。 1.1.3 能审核重要资产清单，修订赋值结果。	1.1.1 资产识别方法 1.1.2 重要资产识别方法
	1.2 安全现状信息收集	1.2.1 能分析评估对象的技术及管理安全要求，编制已有安全措施清单模板。 1.2.2 能分析重要资产的分布、类型、相关责任人等信息，编制重要资产核查记录模板。 1.2.3 能分析资产识别报告、已有安全措施清单、重要资产核查记录内容，编制风险评估方案。	1.2.1 信息系统安全等级保护基本要求 1.2.2 资产标识与跟踪管理方法
2.风险识别	2.1 脆弱性识别	2.1.1 能分析评估对象的业务类型、组织结构等信息，编制安全管理制度资料清单模板。 2.1.2 能分析脆弱性和已有安全措施，赋值脆弱性被利用的难易程度。	2.1.1 脆弱性分类 2.1.2 脆弱性赋值方法

工业和信息化部教育与考试中心
EDUCATION & EXAMINATION CENTER OF MINISTRY OF INDUSTRY AND INFORMATION TECHNOLOGY

	2.2 威胁识别	2.2.1 能分析评估对象面临的威胁类型，编制人为威胁及环境威胁历史记录模板。 2.2.2 能分析威胁动力、可调动资源及发生频率，赋值威胁行为能力与频率。	2.2.1 人为威胁分析方法 2.2.2 环境威胁分析方法
3.风险分析	3.1 风险赋值	3.1.1 能分析脆弱性识别过程记录的信息，编制脆弱性识别表格模板。 3.1.2 能分析威胁识别过程记录的信息，编制威胁识别表格模板。 3.1.3 能审核脆弱性识别表的真实性、准确性，修订安全事件损失的计算结果。 3.1.4 能审核威胁识别表的真实性、准确性，修订安全事件发生可能性的计算结果。	3.1.1 风险评估方法 3.1.2 风险计算方法
	3.2 风险分级	3.2.1 能分析威胁利用脆弱性导致的风险类型，编制风险识别表格模板。 3.2.2 能审核系统资产风险、业务风险计算结果，修订风险赋值。 3.2.3 能分析风险发生的可能性及后果，编制评估项目中系统资产风险及业务风险等级评价准则。 3.2.4 能审核系统资产风险及业务风险等级划分结果，修订风险等级信息。	3.2.1 系统资产风险计算方法 3.2.2 业务风险计算方法 3.2.3 风险等级划分的标准
4.风险评价	4.1 风险处置	4.1.1 能分析评估对象安全风险，编制风险处置方案。 4.1.2 能分析评估对象安全风险涉及资产，制定风险处置计划。 4.1.3 能审核风险处置报告的真实性、合规性，提交风险处置报告。	4.1.1 风险影响因素 4.1.2 风险处置方法
	4.2 评估反馈	4.2.1 能审核风险评估报告的真实性、合规性，提交风险评估报告。 4.2.2 能汇报评估结果并解答问题，根据反馈意见调整报告内容。	4.2.1 风险评估文档规范 4.2.2 等级保护基础知识 4.2.3 项目沟通技巧

工业和信息化部教育与考试中心
EDUCATION & EXAMINATION CENTER OF MINISTRY OF INDUSTRY AND INFORMATION TECHNOLOGY

4 权重表

4.1 理论知识权重表

项目		技能等级		
		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	信息收集	10	10	15
	风险识别	35	40	35
	风险分析	5	5	20
	风险评价	25	30	20
合计		100	100	100

4.2 技能要求权重表

项目		技能等级		
		初级	中级	高级
		（%）	（%）	（%）
技能要求	信息收集	5	10	15
	风险识别	45	40	30
	风险分析	10	15	25
	风险评价	40	35	30
合计		100	100	100

工业和信息化部教育与考试中心
EDUCATION & EXAMINATION CENTER OF MINISTRY OF INDUSTRY AND INFORMATION TECHNOLOGY