信息安全保障人员认证（CISAW）考试大纲
工业控制系统网络安全方向（基础级/专业级）

第一部分 考核目标与要求

本考试大纲依据《信息安全保障人员认证准则》，确定信息安全保障人员认证（CISAW）工业控制系统网络安全方向的考试目标和要求。

信息安全保障人员认证（CISAW）工业控制系统网络安全方向的考试着重考查考生对工业控制系统网络安全知识与理论在项目建设与安全运营中的综合应用；主要考查考生在工业控制系统网络安全方面的基础知识和基本技能，掌握程度与综合运用所学知识分析、解决工业控制系统网络安全问题的能力。本考试大纲适用于申请信息安全保障人员认证（CISAW）工业控制系统网络安全方向基础级和专业级的考生。

第二部分 对知识考点内容的要求层次

本考试对知识考点层次的要求依次是了解、理解、综合应用三个层次，具体内容要求如下：

了解：要求考生对所列知识的含义有初步的、感性的认识，知道这一知识内容是什么，按照一定的程序和步骤照样模仿，并能（或会）

在有关的问题中识别和认识它。

理解：要求考生对所列知识内容有较深刻的理性认识，知道知识间的逻辑关系，能够对所列知识做正确的描述说明并表达，能够利用所学的知识内容对有关问题进行比较、判别、讨论，具备利用所学知识解决简单问题的能力。

综合应用：要求考生能够对所列的知识内容进行推导证明，能够利用所学知识对问题进行分析、研究、讨论，并且加以解决。

第三部分 能力要求

考生应具有一定的工业控制系统及信息安全相关领域基本知识和项目实施经验，具备工控安全方案设计、安全建设、安全运营及技术服务所需的沟通理解能力、数据处理能力、推理论证能力、实验操作能力、总结分析能力，具体要求如下：

沟通理解能力：用于工控安全工程的需求调研、用户及团队协调沟通的基本能力，能够准确理解工业企业的安全需求与业务痛点。

数据处理能力：用于工控安全风险评估、漏洞扫描、安全监测等过程中的数据记录、分析处理等基本能力，风险识别与评估的专业能力。

推理论证能力：用于工控安全技术方案、实施方案设计、安全防护体系论证、系统安全性验证和确认的综合能力。

实验操作能力：用于工控安全工程实施、安全产品调试、安全测

试、漏洞验证等实验操作能力，熟悉工控安全产品的部署与配置。

总结分析能力：用于工控安全工程、安全运营等需求分析、方案设计、建设实施和安全运维四个阶段的综合分析处理能力。

标准转化能力：用于将现行有效的法律法规、国家标准、行业标准中的要求转化为工控安全工程控制项、检查项和整改项，支撑工控安全工程全过程合规落地。

第四部分 考试内容

知识内容		要求
工控安全基础	工控系统网络安全发展历程	了解
	工业控制网络安全态势	了解
	工业控制系统及网络安全基础与组成	理解
	工业控制系统安全属性（CIA 三性、DAD 三角）	理解
网络安全法律法规与工控安全行业监管要求	国内法律法规：《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《关键信息基础设施安全保护条例》等	理解
	典型行业监管要求（电力、石油石化、烟草、轨道交通等行业）	理解
	国际相关标准（IEC 62443、ISO 27000 系列、NIST SP 800-82 等）	了解
工控安全国内标准解读	国内工控安全标准总览	了解
	综合管理类标准（GB/T 36324-2018《信息安全技术 工业控制系统信息安全分级规范》等）	理解

	工控安全与等级保护工作的融合	理解
	国内标准对国际标准的采纳	了解
	产品类标准	了解
	风险评估与基线检查类标准	理解
	工业互联网安全相关标准	了解
	核心标准要求：《信息安全技术 工业控制系统信息安全防护能力成熟度模型》（GB/T 41400-2024）、《信息安全技术 工业控制系统信息安全防护指南》（GB/T 32919-2016）、《信息安全技术 重要工业控制系统网络安全防护导则》（GB/Z 41288-2022）、《电力监控系统安全防护规定》（2024 版）、《工业控制系统信息安全防护指南》等	综合应用
工业控制系统网络安全风险评估	风险评估基本原理与方法	理解
	工控安全风险评估特点（实时性要求、最小影响原则）	理解
	工控安全风险评估实施（准备、识别、分析、处置四个阶段）	理解
	资产识别、威胁识别、脆弱性识别、保障能力评估	理解
	核心标准要求：《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）等	综合应用
工业控制系统网络安全防御体系	工业控制系统网络安全保障模型	了解
	工业控制系统网络安全架构（纵深防御、安全域划分、边界防护）	理解
	工业控制系统信息安全防护能力成熟度模型	理解
	零信任架构及其在工控环境中的应用	了解

工业控制系统网络安全运营	工业控制系统网络安全管理（机构建设、制度流程、人员能力）	理解
	工业控制系统网络安全运营（资产管理、脆弱性管理、监测预警）	理解
	工业控制系统网络安全运营效果评估	理解
	漏洞管理流程（验证、处置、跟踪）	理解
	应急响应（事前准备、事中处置、事后总结）	理解
	核心标准要求：《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）等	综合应用
工业控制网络安全技术	工业控制环境安全技术特点	理解
	工业控制边界防御技术（工业防火墙、逻辑隔离、网闸、正向隔离装置）	理解
	工业控制安全检测技术（工业安全审计系统、入侵检测、态势感知）	理解
	工业控制终端安全技术（主机防护、白名单机制、移动介质管理）	理解
	工业控制典型安全产品与部署（工业防火墙、安全审计、主机卫士等）	综合应用
	核心标准要求：《信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求》等	综合应用
工业控制网络安全行业实践	典型的行业规范（电力监控系统安全防护规定、烟草行业工控系统安全规范等）	综合应用
	典型行业建设实践（电力、石油石化、轨道交通、智能制造等行业安全解决方案）	综合应用
	工业互联网发展与安全（工业互联网体系架构、安全框架、防护对象）	了解
	车联网信息安全（车联网安全风险类别、车路云一体化安全框架）	了解

	核心标准要求：《工业控制系统信息安全防护能力成熟度模型》（GB/T 41400-2024）等	综合应用

第五部分 试卷满分及考试时间

本考试为笔试试卷，满分 120 分。考试时间为 150 分钟，84 分（含）为合格分。如考生有作弊行为则该考生最终笔试成绩为 0 分，并记入考试诚信名单。

考生笔试成绩为“合格”的，该考生可根据《信息安全保障人员认证准则》相关要求，被授予基础级或专业级认证证书。

第六部分 试卷内容结构

知识内容	所占比例
第 1 章 工控安全基础	10%
第 2 章 网络安全法律法规与工控安全行业监管要求	12%
第 3 章 工控安全国内标准解读	10%
第 4 章 工业控制系统网络安全风险评估	12%
第 5 章 工业控制系统网络安全防御体系	12%
第 6 章 工业控制系统网络安全运营	14%
第 7 章 工业控制网络安全技术	20%
第 8 章 工业控制网络安全行业实践	10%

第七部分 答题方式

笔试，闭卷独立完成。

第八部分 试卷题型结构

1.单选题 40 题，每小题 1 分，共 40 分

1.判断题 10 题，每小题 1 分，共 10 分

3.多选题 10 题，每小题 2 分，共 20 分

4.简答题 4 题，每小题 10 分，共 40 分

5.综合应用题 1 题，共 10 分

第九部分 例题

1.单选题

给出问题描述，要求从给出的四个答案中选择其中最为恰当的一个。

例：下列标准中，主要用于数据分类分级的是（ ）。

A.《数据安全技术 数据分类分级规则》

B.《数据中心设计规范》

C.《信息安全技术 防火墙安全技术要求和测试评价方法》

D.《信息安全技术 系统安全工程能力成熟度模型》

答案：A

说明：本题主要考查标准名称、适用范围与模块知识考点的对应关系。

2.多选题

给出问题描述，要求从给出的四个答案中选择其中恰当的2到4个，多选、少选、漏选或错选均不得分。

例：下列属于“数据安全”相关的标准有（ ）。

A.《信息安全技术 网络数据处理安全要求》

B.《信息安全技术 数据安全能力成熟度模型》

C.《信息安全技术 个人信息安全规范》

D.《数据安全技术 数据分类分级规则》

答案：ABCD

说明：本题主要考查数据安全模块的标准归属和标准名称。

3.判断题

给出判断描述，要求判断其正确或错误。

例：信息系统采用了数据加密技术后，就不需要再进行数据备份和容灾设计。（ ）

答案：错

说明：加密技术主要用于保障数据机密性、完整性和真实性，不能替代备份、容灾和业务连续性设计。对于要求持续运行的重要系统，仍需结合备份、热备、集群等措施保障可用性。

4.简答题

给出问题描述，要求用简练的语言回答问题。

例：简述操作系统加固的定义及基本方法。

参考答案：系统加固技术是保障逻辑环境安全的重要实施技术。从风险的角度出发，加固是降低系统脆弱性和降低威胁利用脆弱性可能性的过程。对操作系统加固的两个方面：

（1）降低脆弱性：封堵端口和服务、删除无用账号、升级软件打补丁以消除漏洞；

（2）降低威胁利用脆弱性的可能性：制定复杂口令；增加防火墙、入侵检测、防病毒等安全措施。

说明：本题考查的是“各类系统集成的建设实施技术和方法”，属于综合应用类知识。

5.综合应用题

例：李某是某大型国有企业的负责人，其负责了该企业内一项重要的信息化项目的开发和建设，信息化系统具备以下特征：（1）系统主要给企业的最终用户提供咨询、查询、业务办理的功能和服务；（2）系统要求24小时不间断的运行并提供相应的功能和服务；（3）企业大约有100万的最终用户，平均在线大于1000人，月均业务量500万左右。为了确保系统的安全性、稳定性和业务连续性，李某考虑将数据加密的技术引入到系统的建设中。请结合安全集成相关的理论和知识回答以下问题：

（1）按密钥方式划分的数据加密的技术有哪两种？

（2）如果你是李某会将数据加密技术运用在系统的哪些方面？

（3）如果你是李某还会考虑哪些措施？

参考答案：

（1）主要考察对数据加密技术的分类：依据密钥方式，密码算法分为对称密码算法和非对称密码算法，都可用于数据加密；

（2）考察密码算法的应用。密码技术能实现数据的机密性、完整性和真实性。可用于数据的加密存储，以保障数据的机密性和完整性；用于用户身份认证、系统完整性保护等方面；

（3）密码技术无法实现对业务连续性和系统可用性的支持。因此，还需从数据可用性、系统可用性和业务连续性角度出发，采用数据备份、系统可用性技术（如备份、热备、集群等）等措施，以确保业务连续性。

说明：本题考查的是“密码算法的作用与应用方法”和“容错容灾技术”两个知识点，属于综合应用的知识。