信息安全保障人员认证（CISAW）考试大纲
安全集成方向（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）安全集成方向的考试目标和要求。

信息安全保障人员认证（CISAW）安全集成方向的考试着重考查考生对信息系统安全集成的知识与理论在项目建设中的综合应用；主要考查考生在信息系统安全集成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、解决安全集成问题的能力。本考试大纲适用于申请信息安全保障人员认证（CISAW）安全集成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：

1.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在有关的问题中识别和认识它。

2.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，能够利用所学知识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。

3.综合应用:考生需能够结合实际应用场景,综合运用专业知识、实操技能及行业标准规范,完成安全集成工程中各类技术与标准的选用、落地映射、贯彻实施、测试验证及问题整改工作,可精准研判工程关键核心问题,具备独立处置复杂工程场景、解决实际工程难题的能力,保障安全集成工程建设目标、运行效果及安全管控目标的适宜性、充分性与有效性。

第三部分 能力要求

考生应具有一定的信息安全及相关领域基本知识和项目实施经验,具备安全集成系统设计、工程建设、项目管理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:

1.沟通理解能力:用于安全集成工程的需求调研、用户及团队协调沟通的基本能力;

2.数据处理能力:用于安全集成工程的需求分析、安全测试、试运行过程的数据记录、分析处理等基本能力,风险识别与评估的专业能力;

3.推理论证能力:用于安全集成工程的技术方案、实施方案设计、完工总结、系统安全性验证和确认的综合能力;

4.实验操作能力:用于安全集成工程的工程实施、设备调试、安全测试等实验操作能力;

5.总结分析能力：用于安全集成工程、项目管理等需求分析、方案设计、建设实施和安全保障四个阶段的综合分析处理能力；

6.标准转化能力：用于将现行有效标准中的要求转化为工程控制项、测试项和整改项，支撑安全集成工程全过程合规落地；

7.终身学习能力：用于对前沿工程技术、法律法规和标准规范不断持续学习，解决工程复杂问题。

8.思政素养能力：具备信息安全行业所需的职业素养与思政品格，坚守网络安全底线、恪守行业职业道德、严守数据保密准则，树立国家安全观和正确的网络安全价值观，在工程实施、项目服务、风险管控全流程中坚守合规守法、诚信履职、责任担当的职业准则，自觉维护网络空间安全与国家信息安全，具备应对行业岗位风险的廉洁自律能力和职业操守。

第四部分 考试内容

知识内容	要求
信息安全基础	
●信息安全基本概念	理解
●风险、威胁和脆弱性的定义与分类	理解
●常见威胁	理解
●信息安全技术发展历程	理解
●信息安全技术发展动态	了解
●相关法律法规与核心标准要求：《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》《中华人民共和国密码法》《信息安全技术 术语》《网络安全技术 信息安全管理体系要求》《网络安全技术 信息安全控制》等	理解/综合应用
数据安全	
●数据安全范畴及基本概念	理解

●密码学的基本概念和原理	理解
●典型密码算法（古典密码算法、对称算法、非对称算法、国密算法）	理解
●密码算法的作用与应用方法（数字认证、数字签名、数字信封）	综合应用
●密钥管理方法和公钥基础设施体系	理解
●容错容灾技术（备份、集群、冗余独立磁盘阵列）	综合应用
●数据安全治理（数据安全分类治理、数据安全审计、敏感数据处理、数据运营）	理解/综合应用
●数据隐私保护的概念和技术（数据匿名化、数据脱敏、零知识证明技术）	理解
●核心标准要求:《数据安全技术 数据分类分级规则》《信息安全技术 网络数据处理安全要求》《信息安全技术 数据安全能力成熟度模型》《信息安全技术 个人信息安全规范》《信息安全技术 信息系统密码应用基本要求》等	理解/综合应用
载体安全	
●载体安全基本概念和安全范畴	理解
●存储和传输介质安全技术	理解
●存储载体的典型安全问题	了解
●传输载体的典型安全问题	了解
●常见传输安全协议	综合应用
●云原生安全的概念和技术（容器、微服务、容器云、开发运维一体化）	理解
●核心标准要求:《信息安全技术 操作系统安全技术要求》《信息安全技术 数据库管理系统安全技术要求》《信息安全技术 服务器安全技术要求和测评准则》《信息安全技术 云计算服务安全指南》《信息安全技术 云计算服务安全能力要求》等	理解/综合应用
环境安全	
●环境安全范畴和基本概念	理解
●机房和数据中心物理环境安全的环境安全要素和设计规范	理解/综合应用
●安全审计技术	综合应用
●安全测试技术	综合应用
●常见安全测试工具	综合应用
●漏洞技术与管理	理解/综合应用
●访问控制基本模型与应用	理解
●入侵检测技术原理和应用	综合应用
●入侵检测防御技术原理和应用	综合应用
●恶意行为及防范（病毒、蠕虫、木马等恶意代码概念、行为机	综合应用

制、生存技术及防范方法、恶意代码的演进）	
●核心标准要求:《数据中心设计规范》《计算机场地通用规范》《信息安全技术 网络安全等级保护测评要求》《信息安全技术 网络安全漏洞管理规范》《信息安全技术 网络入侵检测系统技术要求和测试评价方法》等	理解/综合应用
边界安全	
●边界安全的范畴和基本概念	理解
●物理边界控制的基本知识	理解
●防火墙技术（安全区域、防火墙工作模式、包过滤防火墙、应用代理防火墙、状态检测防火墙、统一威胁管理 UTM、下一代防火墙 NGFW、AI 防火墙）	综合应用
●隔离技术（逻辑隔离技术、网络隔离技术分类、物理隔离技术、网闸）	综合应用
●身份认证技术（鉴别技术、Kerberos 协议、SSL/TLS 协议、口令认证技术、双因素身份认证技术、数字证书的身份认证技术、基于生物特征的身份认证技术、DAC、MAC、RBAC）	综合应用
●零信任技术和零信任架构	理解
●核心标准要求:《信息安全技术 防火墙安全技术要求和测试评价方法》《网络安全技术 网络和终端隔离产品技术规范》《信息技术安全技术网络安全 第 4 部分:使用安全网关的网间通信安全保护》《信息技术安全技术网络安全 第 5 部分: 使用虚拟专用网的跨网通信安全保护》《信息安全技术 网络安全等级保护基本要求》《信息安全技术 网络安全等级保护安全设计技术要求》等	理解/综合应用
安全集成基本概念与模型	
●安全集成的范畴和基本概念	理解
●信息系统安全集成模型	理解
●安全集成两种模式及其相互关系	理解
●安全集成的本质和关键问题	理解
●安全集成的合规性分析	综合应用
●核心标准要求:《信息安全技术 信息安全服务分类与代码》《信息安全技术 网络安全服务能力要求》《信息技术服务 服务安全要求》《网络安全技术 信息安全管理体系要求》《网络安全技术 信息安全控制》等	理解/综合应用
系统安全工程基本理论	
●系统安全工程基本定义与模型	了解/理解
●SSE-CMM 系统安全工程能力成熟度模型的体系架构	理解
●SSE-CMM 系统安全工程能力成熟度模型的工程过程域惯例	综合应用

●SSE-CMM 系统安全工程能力成熟度模型的风险过程域惯例	综合应用
●SSE-CMM 系统安全工程能力成熟度模型的保障过程域惯例	综合应用
●SSE-CMM 系统安全工程能力成熟度模型的理论及方法的综合应用	综合应用
●核心标准要求:《信息安全技术 系统安全工程能力成熟度模型》《信息安全技术 信息系统安全工程管理要求》《网络安全技术 信息技术安全评估准则 第 1 部分: 简介和一般模型》《网络安全技术 信息技术安全评估方法》等	理解/综合应用
系统安全集成工程基础理论	
●安全集成服务阶段	综合应用
●安全集成工程环节及其基本内容	理解
●各个环节的输入与输出	理解
●需求分析技术和方法	综合应用
●方案设计理论和方法	综合应用
●核心标准要求:《信息安全技术 信息系统安全工程管理要求》《信息安全技术 网络安全等级保护安全设计技术要求》《信息安全技术 网络安全等级保护基本要求》《信息安全技术 信息安全风险评估方法》等	综合应用
安全集成工程基础	
●各类系统集成的建设实施技术和方法	综合应用
●安全集成测试技术和方法	综合应用
●系统试运行过程和方法	综合应用
●安全集成理论及方法的综合应用	综合应用
●核心标准要求:《信息安全技术 网络安全等级保护测评要求》《信息安全技术 网络安全等级保护测评过程指南》《信息安全技术 网络安全等级保护测试评估技术指南》《信息安全技术 网络安全漏洞管理规范》《信息技术服务 运行维护 第 1 部分:通用要求》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（%）
信息安全基础	12
数据安全	24
载体安全	8
环境安全	10
边界安全	13
安全集成基本概念与模型	10
系统安全工程基本理论	10
安全集成工程基础	13

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 30 题，每小题 1 分，共 30 分

2.多选题 10 题，每小题 2 分，共 20 分

3.判断题 10 题，每小题 1 分，共 10 分

4.填空题 10 题，每小题 1 分，共 10 分

5.简答题 2 题，每小题 10 分，共 20 分

6.案例分析题 2 题，每小题 10 分，共 20 分

7.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.填空题

给出问题描述，要求填写正确的关键词或术语。

例：按照密钥使用方式，密码算法通常可分为对称密码算法和（__）密码算法。

答案：非对称

说明：本题主要考查密码算法的基本分类。对称密码算法加解密使用相同密钥，非对称密码算法使用公钥和私钥。

5.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。

6.案例分析题

给出案例场景，要求结合知识模块和标准要求进行分析。

例：某单位建设安全集成项目，涉及数据分类分级、云平台部署、边界防护、数据库审计和试运行验收。请说明应分别查阅哪些模块中的标准，并举例说明。

参考答案：数据分类分级应查阅数据安全模块中的《数据安全技术 数据分类分级规则》和《网络数据处理安全要求》；云平台部署应查阅载体安全模块中的《云计算服务安全指南》《云计算服务安全能力要求》和《云计算服务安全能力评估方法》；边界防护应查阅边界安全模块中的《防火墙安全技术要求和测试评价方法》《使用安全网关的网间通信安全保护》和《使用虚拟专用网的跨网通信安全保护》；数据库审计应结合数据安全、载体安全和环境安全相关要求；试运行验收应查阅安全集成工程基础模块中的《网络安全等级保护测评要求》《网络安全等级保护测评过程指南》和《网络安全等级保护测试评估技术指南》。

说明：本题考查标准跨模块综合应用能力。

7.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。