信息安全保障人员认证（CISAW）安全集成方向考试大纲

（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照样模仿，并能(或会)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

用所学的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：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

考生应具备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，以及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和实施方案设计、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。

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与最新进展	了解
● 相关法律法规与标准规范	了解
数据安全	
● 数据安全范畴及基本概念	理解
● 密码学的基本原理	理解
● 典型密码算法	理解
● 密码算法的作用与应用方法	综合应用
● 密钥管理方法	理解
● 容错容灾技术	综合应用
● 反垃圾邮件技术	理解
载体安全	
● 载体安全范畴及基本概念	理解
● 存储介质安全技术	理解
● 传输载体的范畴	理解
● 传输载体的典型安全问题	理解
● 常见安全协议	综合应用
环境安全	
● 环境安全范畴和基本概念	理解
● 机房安全物理环境的基本内容	理解
● 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
● 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
● 恶意代码及防范	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	综合应用
● 隔离技术	综合应用
● 身份认证技术	综合应用
● 恶意行为及防范	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
● CISAW 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
● 常见的网络与信息安全事件	了解
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 体系架构	理解
● SSE-CMM 工程过程域惯例	综合应用
● SSE-CMM 风险过程域惯例	综合应用
● SSE-CMM 保障过程域惯例	综合应用
安全集成工程基础	
● 安全集成服务的四个阶段	综合应用
● 安全集成工程的 8 个环节及其基本内容	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
● 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

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。

考生笔试考试成绩为“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	15
数据安全	20
载体安全	7
环境安全	8
边界安全	15
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	15

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 70 题，每小题 1 分，共 70 分

2. 多选题 10 题，每小题 2 分，共 20 分

3. 简答题 1 题，每小题 6 分，共 6 分

4. 综合应用题 2 题，每小题 12 分，共 24 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：信息安全是指（ ）

A. 保持信息的保密性

B. 保持信息的完整性

C. 保护信息的可用性

D. 以上都不对

答案：D

说明：本题主要考点是信息安全基本概念。信息安全是指保持信息的保密性（机密性）、完整性和可用性等安全属性不会被破坏。选项中 A、B、C 都是其中的一个属性，是片面的，只有 D 是相对全面的，与定义相符。

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，多选或少选不得分。

例：操作系统包含的具体功能有（　　）

A. 作业协调

B. 资源管理

C. I/O 处理

D. 安全功能

答案：A、B、C

说明：本题主要考点是各类系统集成的建设实施技术和方法，属于操作系统的基本知识，是安全实施人员需要掌握的基本知识和技能。从操作系统的定义出发，操作系统是硬件上的软件，负责组织和协调计算机运行、管理软硬件资源并提供系统和用户接口。诚然，目前主流的操作系统都具有安全功能。但从基本定义出发，不包括安全功能。有些操作系统是没有安全功能的。

3. 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。

解答思路与答案：系统加固技术是逻辑环境安全和安全实施技术。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”属于综合应用的知识。

4. 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？

解答思路与答案：

（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、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。