

信息安全保障人员认证（CISAW）考试大纲

风险管理方向（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）风险管理方向的考试目标和要求。

信息安全保障人员认证（CISAW）风险管理方向的考试主要考查考生对信息安全风险管理相关基础知识和基本技能的掌握情况、综合运用所学知识分析和解决实际问题的能力。本考试大纲适用于申请信息安全保障人员认证（CISAW）风险管理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。

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

本考试主要考查考生学习理解能力、逻辑推理能力、实际操作能力、沟通交流能力和综合应用能力。具体能力要求如下:

1.学习理解能力: 考生应具有学习能力,能够理解风险管理的基本概念、基本原则、总体框架和实施过程,并掌握风险预防、风险识别和风险处置的基础知识。

2.逻辑推理能力: 考生应具有风险管理的逻辑推理和逻辑判断能力,能够根据组织面临的风险独立进行调研和分析,并给出合理的解决方案。

3.实际操作能力: 考生应具有风险管理的实操和动手能力,能够熟练使用检测工具实施风险识别;能够针对不同的风险采取适当的处置方式和控制措施进行风险处置。

4.沟通交流能力: 考生应具有风险管理过程中沟通、交流和协调能力,能够挖掘客户需求、寻求管理层支持、反馈阶段性成果,保证风险管理各环节信息沟通的及时和顺畅。

5.综合应用能力: 考生应具有综合运用所学理论知识解决风险管理实际问题的能力,能够制订风险评价准则、管理评估团队、实施风险评估、分析计算和评价风险、撰写风险评估报告;能够制定风险处置计划和方案、实施风险处置并对风险处置效果做出评价,做好风险控制,全面和准确把控风险管理过程。

第四部分 考试内容

表1 考试内容

知识内容		要求
风险管理 基本概念	信息安全	了解
	风险管理	理解
	信息安全风险	理解
	信息安全风险管理	理解
	信息安全风险评估	理解
	风险管理标准化组织及风险管理标准	了解
	风险管理标准 ISO 31000	理解
	信息安全风险管理标准 ISO/IEC27005	理解
	信息安全风险评估标准 GB/T20984	理解
	风险评估技术标准 IEC 31010	了解
项目管理 基础和环 境建立	项目管理相关定义	了解
	项目管理生命周期和知识体系	理解
	环境建立相关定义	了解
	环境建立过程及示例	综合应用
风险识别	风险评估准备和风险识别概述	理解
	发展战略和业务识别	理解
	资产识别	综合应用
	威胁识别	综合应用
	已有安全措施识别	综合应用
	脆弱性识别	理解
	物理脆弱性识别	综合应用
	网络脆弱性识别	综合应用
	系统软件脆弱性识别	综合应用
	应用中间件脆弱性识别	综合应用

知识内容		要求
	应用系统脆弱性识别	综合应用
	管理脆弱性识别	理解
风险分析与计算	风险分析定义和原理	理解
	风险可能性和损失分析	综合应用
	风险计算结果分析	综合应用
	风险要素关联方法	理解
	风险计算过程	理解
	矩阵法及示例	综合应用
	相乘法及示例	综合应用
风险评价和评估输出	风险评价定义和准则	了解
	风险评价过程	综合应用
	风险评价结果	理解
	风险评估文档输出	理解
	风险评估报告	理解
风险处置和风险接受	风险处置概念、原则、方式和流程	理解
	风险处置准备和实施	综合应用
	风险处置效果评价	理解
	残余风险和风险接受	理解
沟通咨询和监视评审	沟通咨询定义、方式	理解
	沟通咨询过程	理解
	监视评审定义、原则	了解
	监视评审内容	理解
	监视评审过程	理解

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 笔试试卷内容结构

表2 笔试试卷内容结构

知识内容	所占比例 (%)
风险管理基本概念	25%
项目管理基础和环境建立	4%
风险识别	45%
风险分析与计算	9%
风险评价和评估输出	5%
风险处置和风险接受	8%
沟通咨询和监视评审	4%

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
2. 多选题 10 题，每小题 2 分，共 20 分
3. 判断题 5 题，每小题 1 分，共 5 分
4. 填空题 5 题，每小题 1 分，共 5 分

- 5. 简答题 2 题, 每小题 8 分, 共 16 分
- 6. 计算题 1 题, 每小题 10 分, 共 10 分
- 7. 综合题 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: 下列关于信息特性描述正确的是 ()。

- A. 信息可以传递和共享, 但是不可以加工和处理
- B. 信息可以传递和共享, 但是在传递过程中会产生损耗
- C. 信息可以传递和共享, 但是不可以脱离它所反映的事物
- D. 信息可以传递和共享, 但是必须依附于信息载体

答案: D

解析: 本题考查的是“风险管理基本概念”中的“信息安全”, 属于需要“了解”的内容。信息可以被加工和处理, 具有增值性; 信息在传递过程中不会产生物质或能量的损耗; 信息可以脱离它所反映的事物被存储和传播; 信息必须依附于信息载体来表达、存储和传播。

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、少选或错选不得分。

例: 下面哪些是信息安全风险的要素 ()。

- A. 威胁
- B. 挑战

C. 脆弱性 D. 资产

答案: A、C、D

解析: 本题考查的是“风险管理基本概念”中的“信息安全风险”, 属于需要“理解”的内容。信息安全风险要素包括: 资产、威胁和脆弱性、安全措施、业务、战略六要素。

3. 判断题

给出一句完整陈述, 要求判断这句话正确或错误, 一般只有两种答案。

例: 信息安全风险管理的核心目标是提高信息系统的运行效率。

答案: 错误。

解析: 本题考查的是“风险管理基本概念”中的“信息安全风险管理”, 属于需要“理解”的内容。信息安全风险管理的核心目标是通过识别、分析、评价和控制风险, 将风险降低至可接受水平, 以保障信息的保密性、完整性和可用性 (CIA), 而非直接提升系统运行效率; 提高运行效率属于性能优化或运维管理范畴。因此该陈述错误。

4. 填空题

题目中给出一处或多处预留的空格, 要求用文字、数字、公式、词语等把缺失的内容填写到空格内, 补全句子、概念或算式。

例: 风险具有一类根本特性: 它存在于一切事物之中, 并且贯穿于每一事物的整个生命周期, 这体现出风险具有 () 的特性。

答案: 普遍性。

解析: 本题考查的是“风险管理基本概念”中的“信息安全风险”, 属于需要“理解”的内容。该特性描述的是风险“无处不在、无时不

在”的属性，即风险广泛存在于各类活动和事物的全生命周期中。这一描述直接对应风险的普遍性特性。

5. 简答题

给出问题描述，要求用简练的语言回答问题。

例：简述信息安全中的“三元组”CIA是什么，并分析它们之间的关系。

答案：

(1) CIA 三元组指信息安全的三项核心属性

- ◇ 保密性：保证信息不会向未授权的人员、实体泄露，严控非授权访问；
- ◇ 完整性：保障信息准确、完备，防止被非法篡改、删除或伪造；
- ◇ 可用性：确保授权用户需要时能及时访问信息和使用系统资源。

(2) CIA 三性的关系

三者相互依存、相互制约，共同构成信息安全的基础。任一属性受损，通常会导致其他属性面临连带风险。例如，保密性措施过严可能影响可用性，完整性校验过繁可能降低系统性能，进而间接影响可用性。信息安全防护需在三者之间取得平衡，兼顾业务需求与安全目标。

解析：本题考查的是“风险管理基本概念”中的“信息安全”，属于需要“理解”的内容。保密性管控访问权限，完整性管控数据变更，可用性保障正常业务使用。三者缺一不可，共同搭建起信息安全的基础。

本框架, 答题既要准确写出三项核心要素, 也要点明三者相互制约、相互支撑的内在联系。

6. 计算题

利用一定的运算法则, 通过运算推导出答案。

例: 在某单位实施的信息安全风险项目, 小张工程师接到任务: 依据风险识别的结果进行风险计算。为此, 小张梳理了风险识别的输出结果如下: 识别业务 B 后的业务重要性赋值为 4; 识别资产 A 后的资产重要等级为 4; 识别威胁 T 后的威胁可能性等级 $L_t(T)$ 为 2; 识别脆弱性 V 后的脆弱性严重程度赋值 I_v 为 3; 识别已有安全措施 C 后的赋值 C 为 1; 脆弱性 V 经安全措施修正的情况下被利用的可能性赋值 $L_v(V, C)$ 为 2。如果小张利用风险计算方法中的相乘法计算威胁 T 利用脆弱性 V 对资产 A 产生的风险值 R (其中相乘法使用的计算公式是: $z = f(x, y) = \sqrt{x \times y}$, 并对 z 的计算值采取四舍五入取整), 请问, 小张通过计算后得到的最终风险值 R 是多少?

答案:

(1) 计算安全事件发生可能性

威胁发生的可能性 $L_t(T) = 2$, 脆弱性被利用的可能性 $L_v(V, C)$
 $= 2$

计算安全事件发生的可能性 $L = \sqrt{2 \times 2} = 2$

(2) 计算资产的重要性

业务重要性 $B = 4$, 资产重要等级 $A = 4$

计算资产的重要性 $I_a = \sqrt{4 \times 4} = 4$

(3) 计算安全事件的损失

资产的重要性 $I_a = 4$, 脆弱性 $I_v = 3$

计算安全事件的损失 $F = \sqrt{4 \times 3} = 2\sqrt{3} = 2 \times 1.732 = 3.464$, 四舍五入取整后为 3

(4) 计算风险值

安全事件发生可能性 $L = 2$, 安全事件的损失 $F = 3$

计算安全事件风险值 $R = \sqrt{2 \times 3} = \sqrt{2} \times \sqrt{3} = 1.414 \times 1.732 = 2.449$, 四舍五入取整后为 2。

解析: 本题考查的是“风险分析与计算”中的“相乘法及示例”, 属于“综合应用”的内容。解题的思路是: 首先计算安全事件发生可能性, 然后计算资产重要性, 接着计算安全事件发生的损失, 最后计算出风险值。计算的步骤为:

$$\text{风险值} = R(B, A, T, V, C) = R(L(L_t(T), L_v(V, C)), F(I_a(B, A), I_v))$$

7. 综合题

利用多个知识点解答给定实际问题。

例: 河北 H-A 会计师事务所在审计工作中发现会计电算化软件的重要性, 委托某研究所开发基于 Windows 平台的计算机辅助审计系统。我公司通过招投标流程承接对该系统的风险评估项目。请你从项目的准备和启动开始, 简述一下整个风险评估的流程。

答案:

(1) 项目准备阶段:

- a) 了解该风险评估项目的背景;

- b) 确定风险评估的目标、对象、范围和边界;
- c) 确定风险评估依据;
- d) 组建团队、制定风险评估技术方案、发出“资产情况调查表”、
准备评估工具;
- e) 得到最高管理者的支持, 召开项目启动会。

(2) 项目执行阶段:

- a) 风险识别阶段:
 - ✧ 发展战略和业务识别, 出具发展战略和业务识别列表;
 - ✧ 资产识别及赋值, 出具资产识别列表;
 - ✧ 威胁识别及赋值, 出具威胁识别列表;
 - ✧ 脆弱性识别及赋值, 出具脆弱性识别列表;
 - ✧ 已有安全措施有效性识别及赋值, 出具已有安全措施识别列表。
- b) 风险分析阶段:
 - ✧ 风险计算, 构建风险计算模型, 并计算风险值;
 - ✧ 风险分析, 根据风险计算结果对系统资产风险进行定级。
- c) 风险评价阶段:
 - ✧ 依据风险分析的结果对整个系统的风险等级进行评价。

(3) 项目结束阶段:

- a) 撰写风险评估报告;
- b) 给出风险处置建议。

解析: 本题考查的是“风险识别”中的“发展战略和业务识别过程、输出及示例”、“资产识别过程、输出及示例”、“威胁识别过程、

输出及示例”、“物理脆弱性识别”、“网络脆弱性识别”、“系统软件脆弱性识别”、“应用系统脆弱性识别”、“管理脆弱性识别”和“已有安全措施识别过程、输出及示例”；“风险分析与计算”中的“风险可能性和损失分析”、“风险计算结果分析”和“风险要素关联分析”；“风险评价和评估输出”中的“风险评估报告”，均属于需要“综合应用”的内容。