

信息安全保障人员认证(CISAW)考试大纲

安全运维方向(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)安全运维方向的考试目标和要求。

信息安全保障人员认证(CISAW)安全运维方向的考试主要考查考生对安全运维相关基础知识和基本技能掌握程度和综合运用所学知识分析、解决问题的能力，本考试大纲适用于申请信息安全保障人员认证(CISAW)安全运维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沟通理解能力、数据处理能力、推理论证能力、实践操作能力和综合应用能力，具体能力要求如下：

1. 沟通理解能力：考生应具有针对安全运维服务项目的需求调研与用户及团队进行协调和沟通的能力。
2. 数据处理能力：考生应具有针对安全运维服务项目的前期需求进行分析、安全测试、运行过程的数据记录、分析处理的能力。
3. 推理论证能力：考生应具有针对安全运维服务项目的技术方案和实施方案开展设计，对安全策略进行制定，建立运维应急处理方案和持续改进机制的能力。
4. 实践操作能力：考生应具有针对安全运维服务项目中工程实施、设备调试、安全测试、策略配置等工作的实际操作能力。
5. 综合应用能力：考生应具有针对安全运维服务项目过程中的前期准备、方案设计、服务实施、评审改进等几个阶段综合应用把控的能力。例如，能够理解安全运维服务体系的流程和方法，具备综合利用管理措施和技术手段实施安全服务，建立信息系统安全运维服务的管理流程和管控方法。

第四部分 考试内容

知识内容	要求
------	----

信息系统安全运维概述	信息和系统的基本概念	理解
	系统运维的定义	理解
	信息系统安全运维模型	综合应用
	信息系统安全运维和运维安全两种模式的内涵及关系	综合应用
安全运维体系	信息系统安全运维框架	理解
	运维安全过程及考虑因素	理解
	信息系统安全运维的合规性要求及评审改进	了解
合规要求	与我国信息安全密切相关的法律法规	了解
	我国信息安全标准发展历程及相关标准	了解
	运维服务标准-ITIL 框架、ISO/IEC 20000 框架、ISO/IEC 27001、COBIT 框架等	了解
安全策略	安全策略的定义、作用	了解
	制定安全策略的方法, 包括原则、要素、步骤等	理解
	各层级安全策略内容, 包括决策层、管理层、执行层	综合应用
运维准备	安全运维服务需求分析	综合应用
	安全运维策划, 包括架构、团队、平台等	综合应用
	安全运维预算编制及管理	理解

	安全运维服务范围, 包括资产梳理、业务梳理	理解
	安全运维服务外包管理, 包括模式、风险等	理解
运维实施	安全运维活动中日常运维的内容	综合应用
	安全运维活动中日常运维的处理原则及流程	综合应用
	安全运维活动中应急响应保障, 包括措施、流程等	综合应用
	安全运维活动中优化改善的内容及流程	综合应用
	安全运维活动中监管评估的实现方式	理解
运维安全	运维安全的活动过程	理解
	运维安全的风险评估, 包括风险识别、风险分析、 风险处置	理解
	安全风险控制策略和措施	综合应用
	人员行为监控、风险过程监控的内容	综合应用
评审及改进	信息系统安全运维过程有效性评估的原则和评估要点, 包括准备、实施等阶段	综合应用
	信息系统安全运维过程有效性评估指标的内容和量化管理	理解
	信息系统安全运维持续改进的内容	理解
	应急管理体系完善的理念及内容应急管	理解

	理体系完善的理念及内容	
--	-------------	--

第五部分 试卷满分及考试时间

满分 120 分， 84 分（含）为合格分。考试时间为 150 分钟。

如考生有作弊行为则该考生最终笔试成绩为 0 分。 考生考试成绩为“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（%）
信息系统安全运维概述	11%
安全运维体系	13%
合规要求	11%
安全策略	13%
运维准备	10%
运维实施	18%
运维安全	16%
评审及改进	8%

第七部分 答题方式

考试有两种方式：

1. 参加线下培训，线下考试，考试形式为笔试，闭卷独立完成。

2. 参加线上培训，线上考试，考试形式为双机位线上机考，考生需要自己准备符合线上考试要求的考试设备、独立安静的考试环境，统一参加线上考试。

学员依据自身情况进行选择。

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 3 题，每小题 10 分，共 30 分
6. 实验题 2 题，每小题 10 分，共 20 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：安全运维的（ ）指的是所有安全运维工作应该符合的法律法规、标准规范、安全管理制度及监管要求等。

- A. 合规要求
- B. 风险分析
- C. 风险评价

D. 过程监控

答案：A

说明：本题考查合规要求的目的和意义。属于了解的知识。信息安全合规要求能够给安全运维一个基本规范，提供信息安全运维相关的标准，保障安全运维工作的合理合规合法。

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：依据安全运维服务的具体情况，可设置（ ）不同的有效性评估要点

- A. 运维事件接收/分析有效性评估要点
- B. 实施阶段的有效性评估要点
- C. 运维策划有效性评估要点
- D. 验收阶段的有效性评估要点

答案：A、B、D

说明：本题考查的是“信息系统安全运维过程有效性评估的原则和评估要点，包括准备、实施等阶段”，属于综合应用的知识。目的是通过对评估要点的设置，将总目标分解为各评估要点的分目标，以便通过对评估要点分目标的控制，来实现对总目标的控制。

3. 判断题

给出问题描述，要求对问题描述判断正误。

例：蠕虫既可以在互联网上传播，也可以在局域网上传播。而且由于局域网本身的特性，蠕虫在局域网上传播速度更快，危害更大。

答案：正确

说明：局域网内的终端处于同一网段，蠕虫可直接对所有终端同时发起暴力破解、共享目录遍历，无需跨广域网进行长距离 IP 扫描，传播延迟极低，甚至能在短时间内完成全网感染，传播效率远高于互联网的随机扫描模式。

4. 填空题

给出问题描述，要求对问题描述中的空格填写正确内容。

安全运维审计，主要是通过各类（）、网络设备、服务器、数据库、（）等日志的收集、分析来实现。

答案：安全设备、业务系统

说明：安全运维审计的日志采集对象，首先覆盖防火墙、IDS/IPS 等安全设备的运行与告警日志，这是网络安全行为审计的核心数据源之一。除网络设备、服务器、数据库外，应用系统的操作日志（如业务系统的用户访问、数据修改记录）是还原全链路操作、识别内部越权等风险的关键补充，覆盖从底层硬件到上层业务的全维度审计范围。

5. 简答题

给出问题描述，要求用简练的语言回答问题。

例：安全运维需求贯穿于整个安全运维的实施过程，是安全运维

管理一部分。请简述安全运维需求管理的主要工作。

答案：需求管理主要包含需求评审、需求变更控制、需求跟踪、需求版本管理等内容。

(1) 需求评审：使信息系统安全运维供、需双方对用户需求内达成共识。

(2) 需求变更控制：通过实施一个需求变更分析和决策的流程,所有的需求变更都要遵循。

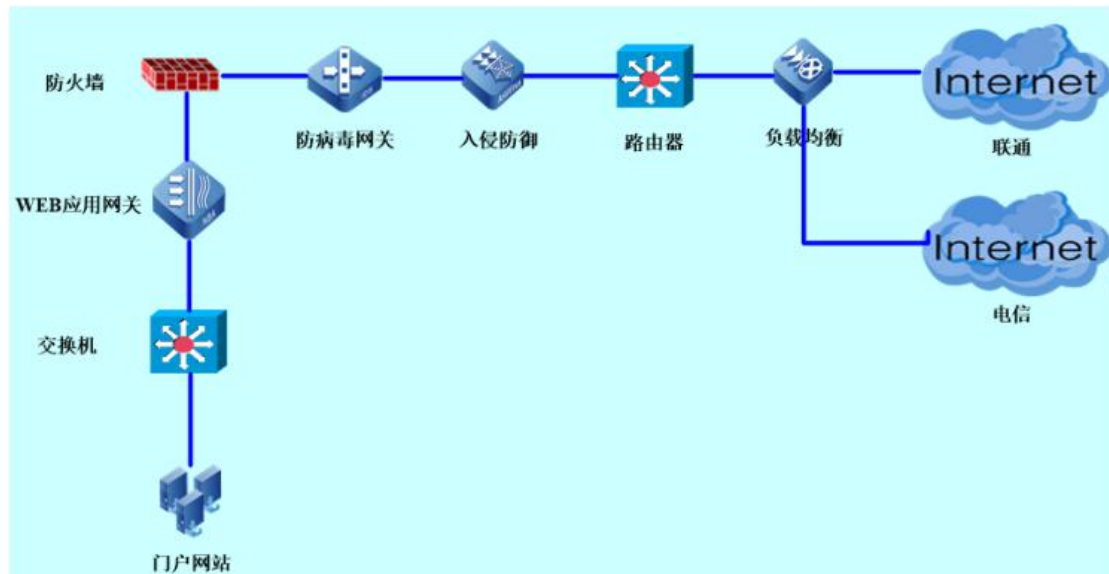
(3) 需求跟踪：记录并维护用户需求中所有项目及项目之间的关系、需求和服务实施之间的关系。

(4) 需求版本管理：以保证每个使用者在任何时候都能得到当前最新版本。对于比较复杂的项目，最好能采用专业的用户需求管理工具，对存储、需求变更管理、需求跟踪等方面进行记录和跟踪。

说明：本题考察的是“安全运维服务需求分析”，属于综合应用的知识。安全需求管理，贯穿于整个安全运维实施过程，包括需求评审，变更控制，跟踪和版本管理。

6. 实验题

例：某机构互联网门户网站区域拓扑如下：



- 1) 在更换入侵防御设备后，接到用户反映网站访问慢，该如何判定该问题
- 2) 针对如上拓扑，提出优化建议

答案：

- 1) (i) 对比网站日常访问速度的基线，如符合基线范围，可认定为正常现象，进入步骤 (iv)，如不符合网站访问速度基线范围，进入步骤 (ii)；
(ii) 对比负载均衡网络接口的带宽使用率基线，如符合基线范围，可认定为正常现象，进入步骤 (iv)，如不符合网站访问速度基线范围，进入步骤 (iii)；
(iii) 检查门户网站至互联网链路上的路由器、交换机、防火墙、入侵防御、web 应用网关等设备的接口的双工状态，尤其是最近更换过的入侵防御设备，以及与入侵防御设备互联的设备的接口状态；如果检测到某个设备的接口状态为非全双工状态，则按照基线标准将接口配置为全双工模式，并重启该接口；如果各

个设备接口状态均正常，则进入步骤 (iv)；

(iv) 与用户联系，排查用户侧网络问题。

2) 链路上设备过多，建议调减，可启用负载均衡的防火墙功能或更换具有防火墙功能的负载均衡，拓扑所描述的网络环境比较简单，不需要使用路由器。

说明：本题考察的是“安全运维活动中日常运维的处理原则及流程”，属于综合应用的知识。通过建立系统中业务量对设备资源使用的基准指标，为今后确认系统是否处于正常状态提供参照依据。