信息安全保障人员认证（CISAW）应急服务方向考试大纲

（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）应急服务方向的考试目标和要求。

信息安全保障人员认证（CISAW）应急服务方向的考试主要从应急响应相关法律法规、网络犯罪过程分析、应急响应体系建立、网络层应急技术与实践、主机层应急技术与实践、应急技术综合演练六个维度进行考核,本考试大纲适用于申请信息安全保障人员认证(CISAW)应急服务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、实验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：用于应急管理工程的需求调研、用户及团队协调沟通的基本能力；

2. 数据处理能力：用于应急管理工程的需求分析、安全测试、业务数据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：用于应急管理工程的技术方案和实施方案设计、对应急预案和安全策略进行制定，建立应急处理方案和持续改进机制的能力；

4. 实验操作能力：用于应急管理工程的安全实施、渗透测试、安全合规检查、安全测试等实验操作能力；

5. 综合应用能力：用于应急管理工程、项目管理等需求分析、应急方案设计、安全保障、系统恢复、入侵分析等综合应用能力，能够建立长久有效的应急与安全管理机制。

第四部分 考试内容

知识域	知识内容	要求
应急响应相关法律法规	《网络安全法》	了解

	《个人信息保护法》	了解
	《数据安全法》	了解
	《关键信息基础设施安全保护条例》	了解
	网络安全等级保护制度	了解
	信息安全事件管理	理解
	应急响应处理流程	理解
网络犯罪过程分析	网络犯罪过程重现	了解
	网络犯罪过程分析	了解
应急响应体系建立	应急响应监控建立	理解
	应急响应流程建立	综合应用
	应急响应预案编写与演练	理解
网络层应急技术与实践	网络层安全技术原理与实践	理解
	网络渗透技术与应急响应实践	综合应用
主机层应急技术与实践	主机层安全技术原理与实践	理解
	主机渗透技术与应急响应实践	综合应用
应急技术综合演练	应急安全技术保障方案	理解
	应急技术综合演练实践	综合应用

第五部分 试卷满分及考试时间

本考试为笔试和上机实验操作，满分 120 分。考试时间为 150 分钟，包含上机实验操作时间 60 分钟，上机实验操作完成后，考生必须关闭电脑，继续完成笔试试题部分。本考试 84 分（含）为合格分。如考生有作弊行为则该考生最终考试成绩为 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（%）
应急响应相关法律法规	8
网络犯罪过程分析	25
应急响应体系建立	27
网络层应急技术与实践	12
主机层应急技术与实践	20
应急技术综合演练	8

第七部分 答题方式

笔试加上机实验操作，闭卷独立完成。

第八部分 试卷题型结构

1. 单选题 60 题，每小题 1 分，共 60 分
2. 实操单选题 10 题，每小题 4 分，共 40 分
3. 简答题 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：某单位网络中仅有一台防火墙，防火墙使用了三个端口，一个端

口是公网接入，一个端口是DMZ口，一个端口是内网接入。单位仅对外开放一个WEB服务器的80端口访问和本单位DNS域名解析服务，对外公网开放的WEB服务器、DNS服务器A在DMZ区域，内网区域有另外一个内部DNS域名解析的内部DNS服务器B。在应急准备阶段，发现防火墙的配置规则如下：

（1）防火墙对外映射端口为Http 80、Tcp 53、Udp 53

（2）防火墙DMZ和内网口间开放了Tcp 53

请问该单位防火墙配置应该如何修正？

A. 将对外映射的Tcp 53、Udp 53关闭

B. 将对外映射的Tcp 53关闭，将DMZ和内网规则改为Udp 53。

C. 将对外映射的Udp 53关闭，将DMZ和内网规则改为Udp 53。

D. 将对外映射的Tcp 53关闭，将DMZ和内网间规则Tcp 53删除。

答案：D

说明：本题知识点属于“网络渗透技术与应急响应实践”，属于综合应用的知识，主要考察网络安全域划分与访问控制。DNS服务器A对外服务端口为Udp53端口，没有对外DNS Zone文件同步的需求，所以对外映射TCP53端口需要关闭。DMZ区和内网是不同的安全域，两个DNS Zone文件作用的安全域不同，不可相互访问，所以需要将防火墙DMZ和内网口间开放的Tcp 53规则删除，因此选择答案D。

2. 实操单选题

给出问题描述，按照给定的实验操作考试环境登录步骤，在指定的实操考试环境的服务器A里，找出四个答案中正确的一个。

例：请分析服务器 A 上的木马进程名字是多少？木马运行在什么目录下？

A. systemr，c:/systemr

B. systemr，c:/windows/system32

C. calc.exe c:/windows/system32

D. calc1.exe c:/windows/system32/manager

答案：D

说明：本题知识点属于“主机渗透技术与应急响应实践”知识域，属于综合应用的知识，主要考察主机木马查杀方法。一般情况下，寻找 Windows 系统的木马进程，需要查找任务管理器中的可疑进程，查找可疑的服务项，查找注册表，也可以通过木马查杀工具查找木马，查找到木马程序后，查看木马程序名称和所在位置，本题通过查看系统服务，发现木马，即可得出答案 D。

3.简答题

给出问题描述，要求用简练的语言回答问题。

例：在某中大型系统中，划分了有多个网络安全域，每个安全域中，存在多个网段，为了保障各个安全域和网段之间的安全，监控域的安全情况，保持业务平稳运行，一般可以做出哪些应急体系建设规划，请列举至少 5 条有效的方法。

解答思路与答案：

1)对各个域和各个网段，在交换机中划分不同的 Vlan，设置 Acl 规则，严格按照业务需求和网络安全相关要求进行实施。对于敏感端

口，如 22、445、3306、3389 等端口进行严格的访问控制。

2)对人员按照职位不同，划分不同的网络访问权限，分配不同的网络资源。

3)对于服务器，及时更新补丁，开展渗透测试，防止出现中高危漏洞，对个人电脑，访问内网需要提出申请，禁止下载非软件白名单的软件。

4)部署防火墙等边界设备，设置异常流量自动报警，设置访问控制规则，严控内部向外部的非法连接。

5)安装抗 DDoS、Waf 等安全设备，实时监控，主动告警。

6)做好日志保存，日志至少保存 6 个月以上。

7)做好数据本地和异地备份，对数据读写、存储异常能够及时告警。

8)定期开展网络应急预案演练与等级保护基线检查。

说明：本题知识点属于“应急响应流程建立”知识域，属于综合应用的知识，主要考察应急响应体系建立思路和路线。