CISSP考试练习(习题卷14)

第1部分：单项选择题，共100题，每题只有一个正确答案,多选或少选均不得分。

1.[单选题]以下哪一个是需要系统重新认证和重新认证的主要原因?
A)协助数据所有者确定未来的敏感性和临 界性
B)向软件开发团队保证所有安全问题 都已 得到解决
C)验证安全保护仍为组织安全政策所接受
D)帮助安全团队接受或拒绝新的实施和生产系统
答案:C
解析:

2.[单选题]以下哪一项 是获得识别和支持时要获得的最佳指标访问管理 (IAM) 解决方案?
A)应用连接成功导致数据 泄露
B)连接故障后恢复系统的管理费用
C)实施错误限制的员工系统超时
D)支持密码重置请求所需的服务台成本
答案:D
解析:

3.[单选题]通常用什么术语来指 通过从受信任的源伪造数据包来将一台机器验证到另一台机器的技术?
A)中间人 (MITM) 攻击
B)蓝精灵
C)会话 重定向
D)欺骗
答案:D
解析:

4.[单选题]在SSD驱动器废弃时,为什么要物理破坏SSD驱动器以防止数据泄露?
A)消磁只能部分擦除SSD上的数据
B)SSD没有数据残留
C)SSD无法进行零填充
D)内置的擦除命令在一些SSD上不是完全有效的
答案:D
解析:研究表明,在SSD 上清除数据的传统方法是不可靠的。SSD 将数据扇区重新映射为损耗均衡的一部分,并且擦除命令在不同品牌SSD 上的执行效果可能不太一样。零填充同样也可用于清除SSD上的文件,但也可能存在像擦除命令那样的情况。消磁对SSD 来说无效,因为SSD 是闪存介质,而不是磁介质。SSD 没有数据剩磁问题。
Research has shown that traditional methods of sanitizing files on SSDs were not reliable.SSDs remap data sectors as part of wear leveling,and erase commands are not consistently effective across multiple SSD brands.

5.[单选题]儿童在线隐私保护法COPPA旨在保护使用互联网的儿童的隐私。在未经父母同意的情况下，公司可从孩子身上手机个人身份信息的最低年龄是
A)13
B)14
C)15
D)16
答案:A

解析:

6.[单选题]在软件开发生命周期 (SDLC)中何时必须定义软件安全功能要求?
A)系统初步设计完成后,数据安全分类已执行d
B)执行业务功能分析和数据安全分类后
C)执行漏洞分析后和系统详细设计开始之前
D)系统初步设计开发后,数据安全分类开始之前
答案:B
解析:

7.[单选题]高级管理层要求数据库管理员对会计系统数据库执行特定更改。系统明确指示管理员不要跟踪或证明票证中的更改。以下哪项是最佳行动方案?
A)一个。忽略该请求,并且不执行更改。
B)根据请求执行更改,并依靠下一次审核来检测和报告情况。
C)执行更改,但无论如何都要创建更改票证,以确保具有完全的可追溯性。
D)使用公司举报人流程直接通知审计委员会或内部审计。
答案:C
解析:

8.[单选题]可信平台模块 (TPM) 的哪些功能会创建系统配置的哈希摘要以验证未进行更改?
A)远程认证
B)绑定
C)密封
D)随机数
答案:A
解析:

9.[单选题]哪种类型的控制与避免风险的发生有关?
A)威慑控制
B)检测控制
C)预防控制
D)补偿控制
答案:C
解析: Preventive controls deals with the avoidance of risk through the diminution of probabilities.
Is like the example we read earlier about the dogs. Just to remember, Since we want to
Prevent something from happening, we can go out and buy some Guard dogs to make the
Job. You are buying them because you want to prevent something from happening. The
Intruder will see the dogs and will maybe go back, this prevents an attack, this dogs are a
Form of preventive control.

10.[单选题]What type of database attack would allow a customer service employee to determine quarterly sales results before they are publically announced? 哪种类型的数据库攻击会允许客户服务员工在公布季度销售结果之前确定季度销售结果?
A)Polyinstantiation多重性问题
B)Inference推断
C)Aggregation汇聚
D)Data mining数据挖掘
答案:A
解析:

11.[单选题]Kailey 正在审查她的组织维护的一组旧记录,并希望安全地处理它们。 她不确定该组织应将记录保留多长时间,因为它们涉及税务数据。 Kailey 如何确定是否可以处置这些记录?
A)查阅组织的记录保留政策。
B)咨询 IRS 要求。
C)保留记录至少七年。
D)永久保留记录。
答案:A
解析:

12.[单选题]下列哪个是把测试和开发环境分离最好的原因?
A)安全访问系统下开发
B)控制测试环境的稳定
C)隔离的用户和开发人员
D)限制访问系统下测试
答案:B
解析: The test environment must be controlled and stable in order to ensure that development projects are tested in a realistic environment which, as far as possible, mirrors the live environment.

13.[单选题]在开发业务影响分析时， 团队应首先创建资产列表。 接下来应该发生什么?
A)Identify vulnerabilities in each asset.
识别每项资产中的漏洞。
B)Determine the risks facing the asset.
确定资产面临的风险。
C)Develop a value for each asset.
为每项资产制定一个价值。
D)Identify threats facing each asset.
识别每项资产面临的威胁。
答案:C
解析:制定资产清单后， 业务影响分析团队应为每项资产分配价值。 此处列出的其他活动仅在为资产分配价值后发生。
章节：模拟考试202201

14.[单选题]下列哪项是为了支持多种协议以及提供登录、密码和纠错功能而开发的?
Which of the following was developed to support multiple protocols as well as provide as well as provide login, password, and error correction capabilities?
A)邮局协议 (POP)
Post Office Protocol (POP)
B)密码认证协议 (PAP)
Password Authentication Protocol (PAP)
C)点对点协议 (PPP)
Point-to-Point Protocol (PPP)
D)质询握手认证协议 (CHAP)
Challenge Handshake Authentication Protocol (CHAP)
答案:D
解析:

15.[单选题]All hosts on the network are sending logs via syslog-ng to the log collector. The log collector is behind its own firewall, The security professional wants to make sure not to put extra load on the firewall due to the amount of traffic that is passing through it. Which of the following types of filtering would MOST likely be used? 网络上的所有主机都通过syslog ng向日志收集器发送日志。日志收集器位于

自己的防火墙后面，安全专业人员希望确保不会由于通过它的流量而给防火墙带来额外的负载。以下哪种类型的过滤最有可能被使用？
A)Uniform Resource Locator（URL）Filtering统一资源定位器（URL）筛选
B)Web Traffic Filtering Web流量过滤
C)Dynamic Packet Filtering动态包过滤
D)Static Packet Filtering静态包过滤
答案:C
解析:

16.[单选题]下列哪个选项是对于物理攻击，加固数据安全最好的答案
A)把计算机藏在一些盒子后面
B)把计算机锁在一个实体上
C)全盘加密
D)设置BIOS密码
答案:B
解析: Physical security of a computer is important but with strong disk encryption the data can be rendered practically useless to an attacker who physically steals a computer or its disk drives.

17.[单选题]Tom 正在调整安全监控工具,以减少管理员收到的警报数量,同时要求不能因此丢失重要的安全事件。他决定将系统配置为只报告以下这种情况:在一小时内访问同一账户有五次登录失败。什么术语最好地描述了Tom使用的技术?
A)域值
B)抽样
C)账户锁定
D)阈值
答案:D
解析:阀值是一种分析技术,只有在超过设定的域值后才发出警报,它是一种特殊的抽样形式,然而“抽样”却是更一般的术语,用来描述任何为了审查目的而对全体记录进行的摘录。域值不是常用术语。管理员可在登录失败后选择配置自动或手动账户锁定,但这与本题无关。
Clipping is an analysis technique that only reports alerts after they exceed a set threshold. It is a specific form of sampling, which is a more general term that describes any attempt to excerpt records for review. Thresholding is not a commonly used term.

18.[单选题]In the "Do" phase of the Plan-Do-Check-Act model, which of the following is performed? 在Plan-Do-Check-Act模型的“Do”阶段，执行以下哪项？
A)Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement. 根据业务连续性政策和目标监控和审查绩效，将结果报告给管理层审查，并确定和授权补救和改进措施。
B)Maintain and improve the Business Continuity Management（BCM）system by taking corrective action, based on the results of management review. 根据管理评审结果，采取纠正措施，维护和改进业务连续性管理（BCM）系统。
C)Ensure the business continuity policy, controls, processes, and procedures have been implemented. 确保已实施业务连续性政策、控制、流程和程序。
D)Ensure that business continuity policy, objectives, targets, controls, processes and procedures relevant to improving business continuity have been established. 确保建立了与改善业务连续性相关的业务连续性政策、目标、指标、控制、流程和程序。
答案:D
解析:

19.[单选题]硬件抽象层 (HAL) 在
A)系统 软件。

B)系统 硬件。
C)应用程序 软件。
D)网络 硬件。
答案:A
解析:

20.[单选题]在评估防护措施时,下列哪项不是需要考虑的有效问题?
Which of the following is not a valid issue to consider when evaluating a safeguard?
A)成本效益分析
Cost/benefit analysis
B)符合现有基线
Compliance with existing baselines
C)法律责任与应尽关注
Legal liability and prudent due care
D)与IT基础架构的兼容性
Compatibility with IT infrastructure
答案:B
解析:

21.[单选题]S/MIME 靠什么交换秘钥?
A)共享
B)证书
C)IKE
D)SHA-1
答案:B
解析:略
章节：模拟考试202201

22.[单选题]什么类型的运动检测器使用高微波频率信号传输来识别入侵者?
A)红外
B)热基
C)波形
D)电容
答案:C
解析:波形运动检测器向监控区域内发送超声波或微波信号,通过观察物体反射回来的信号来检测物体的运动变化。Wave pattern motion detectors transmit ultrasonic or microwave signals into the monitor area, watching for changes in the returned signals bouncing off objects.

23.[单选题]关于值边界分析作为一种功能性软件测试技术,下列哪项陈述是正确的?
A)它用于测试通信协议和图形用户界面。
B)它的特征是在函数中实现的进程的无状态行为.
C)测试输入从给定功能规格的导出阈值获得。
D)只考虑该分区中的一个代表值就可以覆盖整个分区。
答案:C
解析:保护先做分析,确认风险,再考虑其他,先后原则

24.[单选题](04063) An organization is considering implementing a Single Sign-On (SSO) solution using industry best practice for key business applications一个组织在考虑实施一个单点登录（SSO）解决方案，方案采用了业界关键业务应用系统的最佳实践。Which of the following provides the BEST security enforcement for the SSO solution?下面哪项提供了SSO方案的最安全的实施?
A)Policies requiring complex passwords需要复杂密码的策略

B)Policies requiring complex passwords需要复杂密码的策略
C)Policies requiring complex passwords需要复杂密码的策略
D)Policies requiring complex passwords需要复杂密码的策略
答案:D
解析:

25.[单选题]两家企业之间存在纠纷， 准备起诉， 属于什么?
A)刑事
B)民事
C)行政
D)冲突
答案:B
解析:略
章节：模拟考试202201

26.[单选题]在以下哪个灾难恢复测试中,团队成员坐在一起,讨论对场景的响应,但实际上没有激活任何灾难恢复控制?
A)清单审核
B)完全中断测试
C)并行测试
D)桌面练习
答案:D
解析:在桌面练习期间,团队成员会聚在一起讨论,而不对信息系统进行任何更改。清单审核是最少破坏性的灾难恢复测试类型,在清单审核期间,由团队成员自己来审核灾难恢复清单的内容,并对系统是否需要改进给出建议。在并行测试期间,团队实际上激活灾难恢复站点进行测试,但主站点仍然继续保持运行。在完全中断测试期间,团队会清除主站点,并确认灾难恢复站点能够处理常规操作。完全中断测试是最彻底的测试,但也是最具破坏性的。
During a tabletop exercise, team members come together and walk through a scenario without making any hanges to information systems. The checklist
Review is the least disruptive type of disaster recovery
Test.

27.[单选题]以下哪项最能描述如何将对系统的访问权限授予联合用户帐户?
A)基于身份提供者(IdP)定义的标准
B)基于依赖方(RP)确定的标准
C)联邦保证级别
D)具有身份保证级别
答案:A
解析:

28.[单选题]以下哪种内存类型被视为易失性内存?
A)Flash
B)EEPROM
C)EPROM
D)RAM
答案:D
解析:RAM 的内容是易失性的,这意味看它们仅在对存储器芯片施加电源时可用,EPROM、EEPROM 和闪存都是非易失性的,这意味着它们即使在断电时也保留其内容。
The contents of RAM are volatile, meaning that they are only available while power is applied to the memory chips.EPROM,EEPROM,and flash memory are all nonvolatile, meaning that they retain their contents even when powered off.

29.[单选题]作为安全评估计划的一部分,已要求安全专业人员在新网站上使用阴性测试策略。将执行以下哪些操作?

A)使用 Web 扫描仪扫描网站内的漏洞 。
B)通过代码审查来确保数据库引用得到正确 处理。
C)建立与 Web 服务器的安全连接,以验证只有已批准的端口是开放的。
D)仅在 Web 表单中输入数字,并验证网站是否提示用户输入有效输入。
答案:D
解析:

30.[单选题]Which factors MUST be considered when classifying information and supporting assets for risk management, legal discovery, and compliance? 在为风险管理、法律查询和法规遵从性对信息和支持资产进行分类时，必须考虑哪些因素？
A)System owner roles and responsibilities,data handing standards,storage and secure development lifecycle requirements.系统所有者角色和职责、数据处理标准、存储和安全开发生命周期要求。
B)Data stewardship roles, data handing and storage standards,data lifecycle requirements.数据管理角色、数据处理和存储标准、数据生命周期要求。
C)Compliance office roles and responsibilities,classified material handing standards,storage system lifecycle requirements.法规遵从性办公室的角色和职责、机密材料处理标准、存储系统生命周期要求。
D)System authorization roles and responsibilities,cloud computing standards, lifecycle requirements.系统授权角色和职责、云计算标准、生命周期要求。
答案:B
解析:

31.[单选题]以下哪项不被认为是基于异常的入侵防御系统?
A)统计异常型
B)协议异常型
C)暂时基于异常
D)流量异常型
答案:C
解析:c。行为型系统可学习一个环境的“正常"活动。下面列出了3种类型:统计异常型创建一个“正常"活动概述文件,并将各种活动与这个文件相匹配。协议异常型标识在公共边界之外使用的协议。流量异常型标识不正常的网络流量。

32.[单选题]在日志审查期间,Karen发现她收集日志的系统需要具有如图所示的日志设置。Karen 可能遇到什么问题?
A)系统中存储了过多日志数据
B)系统自动清除归档日志
C)日志将不包含所需的信息
D)日志将仅包含最近的20MB日志数据
答案:D
解析:当日志文件达到20MB时,系统将用最新的日志条目替换最旧的日志条目。系统不会清除归档日志,因为它不归档日志。由于只有20MB的日志,此系统将不会存储太多日志数据,并且根据题中的信息来看,没有足够的信息表明是否存在安全问题。The system is set to overwrite the logs and will replace the oldest log entries with new log entries when the file reaches 20 MB.The system is not
Purging archived logs because it is not archiving logs.
Since there can only be 20 MB of logs,this system wil
Not have stored too much log data

33.[单选题]In a quarterly system access review, an active privileged account was discovered that did not exist in the prior review on the production system. The account was created one hour after the previous access review. Which of the following is the BEST option to reduce overall risk in addition to quarterly access reviews? 在每季度的系统访问审查中，发现一个活动的特权帐户，该帐户在先前对生产系统的审查中不存在。该帐户是在上次访问检查后一小时创建的。除了季度访问审查外，以下哪项是降低总体风险的最佳选择？
A)Increase logging levels. 提高日志记录级别。
B)Implement bi-annual reviews. 实施两年一次的审查。

C)Create policies for system access. 创建系统访问策略。
D)Implement and review risk-based alerts. 实施和审查基于风险的警报。
答案:D
解析:

34.[单选题]银行出纳员的访问控制策略是实施下列哪一选项的例子?
A)基于规则的策略
B)基于身份的策略
C)基于用户的策略
D)基于角色的策略
答案:D
解析:

35.[单选题]The type of authorized interactions a subject can have with an object is主体可以与对象进行的授权交互类型为
A)control. 控制
B)permission. 准许
C)procedure. 程序
D)protocol. 协议
答案:B
解析:

36.[单选题]下一个是信息安全策略的一个重要特征?
A)确定信息的主要区域功能
B)信息损失的影响
C)需要识别信息
D)列出支持业务功能的应用程序
答案:A
解析: 信息安全策略是描述程序目标的高级计划。 策略不是指南或标准，也不是程序或控制。政策笼统地描述了安全性，而不是具体的。它们为整体 安全计划提供蓝图，就像规范定义你的下一个产品一样。

37.[单选题]下列哪个陈述正确描述了黑盒测试和白盒测试的区别?
A)白盒和黑盒测试的重点是软件程序逻辑的有效性
B)白盒和黑盒测试侧重于一个信息系统功能运行中的有效性，不考虑任何内部程序结构
C)白盒测试侧重于功能的有效性，而黑盒评估软件程序逻辑的有效性
D)黑盒测试侧重于功能的有效性，而白盒评估软件程序逻辑的有效性
答案:D
解析: White box assesses the effectiveness of software program logic

38.[单选题]While reviewing the financial reporting risks of a third-party application, which of the following Service Organization Control (SOC) reports will be the MOST useful? 在审查第三方应用程序的财务报告风险时，以下哪种服务组织控制（SOC）报告最有用?
A)SOC 1
B)SOC 2
C)SOC 3
D)SOC for cybersecurity网络安全SOC
答案:A
解析:

39.[单选题]The PRIMARY security concern for handheld devices is the手持设备的主要安全问题是
A)strength of the encryption algorithm. 加密算法的强度。

B)spread of malware during synchronization. 同步期间恶意软件的传播。
C)ability to bypass the authentication mechanism. 绕过身份验证机制的能力。
D)strength of the Personal Identification Number（PIN）. 个人识别码（PIN）的强度。
答案:C
解析:

40.[单选题]僵尸网络的定义。
A)一组特殊定义的网络
B)外网和内网之间的区域（ DMZ）
C)因为中毒而不能使用的终端
D)一组被控制的， 用于攻击的电脑集群
答案:D
解析:略
章节：模拟考试202201

41.[单选题]Extensible Authentication Protocol-Message Digest 5（EAP-MD5）only provides which of the following? 可扩展身份验证协议消息摘要5（EAP-MD5）仅提供以下哪项？
A)Mutual authentication相互认证
B)Server authentication服务器认证
C)User authentication用户认证
D)Streaming ciphertext data密文数据流
答案:C
解析:

42.[单选题]组织正在选择一个服务提供商,以帮助整合多个计算站点,包括开发、实施和持续支持各种计算机系统。信息保密部门必须核实以下哪些情况?
A)服务提供商的政策与 ISO/IEC27001 一致,并且有证据表明服务提供商正在遵循这些政策。
B)服务提供商将将数据分离到其系统中,并确保满足每个区域的 policies。
C)服务提供商将实施满足或超过当前系统控制的控制和保护, 并生成审核日志作为 验证。
D)服务提供商的政策即使与组织的当前政策不同,也可以满足新环境的要求。
答案:D
解析:

43.[单选题]主体的身份管理流程在哪些 方面建立?
A)信任
B)供应
C)授权
D)招生
答案:D
解析:

44.[单选题]以下哪些组件最难检测到的漏洞?
A)内核
B)共享库
C)硬件
D)系统 应用
答案:A
解析:

45.[单选题]Cathy 的雇主要求她对第三方供应商的政策和程序进行文件审查。 该供应商只是软件供应链中的最后一环。 他们的组件被用作为高端客户运营的在线服务的关键要素。 Cathy 发现了供应商的几个严重问题,例如没有要求对

所有通信进行加密,并且不需要在管理接口上进行多因素身份验证。 针对这一发现,Cathy 应该怎么做?
A)撰写报告并将其提交给 CIO。
B)作废供应商的 ATO。
C)要求供应商审查他们的条款和条件。
D)让供应商签署保密协议。
答案:B
解析:在这种情况下,Cathy 应取消该供应商的运营授权 (ATO)。
这种情况描述了这样一个事实,即供应商没有满足保护服务及其客户所必需的最低安全要求。写一份报告并不是对这一发现的充分回应。您可能已经假设凯茜有权或没有权力执行任何其他选项,但没有迹象表明凯茜在组织中的职位。 CEO 要求 CISO 进行这样的评估是合理的。无论如何,报告应该提交给 CISO,而不是 CIO,CIO 的重点主要是确保有效地使用信息来实现业务目标,而不是确保这种使用是安全的。在这种情况下,审查条款和条件不会有任何区别,因为这些条款和条件通常适用于客户,而不是内部运营。审查并不一定会导致不安全实践的改变或改进。供应商签署的保密协议与这种情况无关。

46.[单选题]Tom 正在为位于佛罗里达州中部的OrangeBlossoms 开展业务连续性规划工作。在评估过程中,委员会确定该地区存在降雪风险,但没有多余资金来实施控制措施以降低该风险的影响。他们选择不采取任何具体行动来应对风险。OrangeBlossoms 追求什么风险管理策略?
A)风险缓解
B)风险转移
C)风险规避
D)风险接受
答案:D
解析:风险接受策略是将企业自身承受的风险以及生产经营过程中不可避免的财务风险承受下来,并采取必要的措施加以控制。在本题中,组织选择不采取任何行动,很明显属于风险接受策略。
Risk acceptance occurs when an organization determines that the costs involved in pursuing other risk management strategies are not justified and they choose not to pursue any action.

47.[单选题]当Jim进入其组织的数据中心时，他必须使用智能卡和密码进入，先通过第一组门，接着第一组门关闭，然后他必须再次使用他的卡通过第二组门。这是什么类型的控制，它叫什么?
A)物理控制；单向活板门
B)逻辑控制；双刷卡控制
C)指令控制；单向通道走廊
D)预防性访问控制；陷门
答案:D
解析:

48.[单选题]当对策成本超过风险成本时，应如何处理成本风险？
A)拒绝风险
B)执行另一种风险分析
C)接受风险
D)减少风险
答案:C
解析:

49.[单选题]Doolittle Industries 的一名会计员工最近因参与贪污计划而被捕。 该员工将钱转入个人账户， 然后每天在其他账户之间转移资金， 以掩盖欺诈行为长达数月。
Which one of the following controls might have best allowed the earlier detection
Of this fraud?
以下哪一项控制措施可能最有助于及早发现这种欺诈？
A)Separation of duties
职责分离

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/196021054225010050