题目1：James正在为他的组织制定一个灾难恢复计划，并希望确定在组织的系统发生故障后可接受的数据丢失量。James正在确定什么变量？

James is building a disaster recovery plan for his organization and would like to determine the amount of acceptable data loss after an outage. What variable is James determining?

A：SLA

SLA

B：RTO

RTO

C：MTD

MTD

D：RPO

RPO

答案:James正在确定的是 \*\*D：RPO\*\*。

\*\*RPO（Recovery Point Objective，恢复点目标）\*\* 是指在灾难发生后，组织可以接受的数据丢失量。它定义了在系统恢复后，数据可以恢复到的时间点。例如，如果RPO为1小时，意味着在灾难发生后，系统恢复时最多只能丢失1小时的数据。

其他选项的解释：

- \*\*A：SLA（Service Level Agreement，服务级别协议）\*\*：是服务提供商和客户之间的协议，规定了服务的质量和可用性标准。

- \*\*B：RTO（Recovery Time Objective，恢复时间目标）\*\*：是指在灾难发生后，系统或服务必须恢复的时间目标。

- \*\*C：MTD（Maximum Tolerable Downtime，最大可容忍停机时间）\*\*：是指组织可以容忍的系统或服务的最长停机时间。

因此，James正在确定的是 \*\*RPO\*\*。

-------------------

题目2：在他的角色中，Chris应该保护组织的利益，以及他负责保护其信息的客户的利益。什么术语描述了在做出决策和行动之前进行的准备和研究？

In his role, Chris is expected to protect the interests of the organization, and the customers whose information he is charged to protect. What term describes the preparation and research undertaken before decisions and actions are made?

A：应尽关注

Due care

B：合规

Compliance

C：应尽职责

Due diligence

D：监管行动

Regulatory action

答案:题目描述的是在做出决策和行动之前进行的准备和研究，这通常被称为“应尽职责”（Due diligence）。应尽职责是指在采取行动或做出决策之前，进行充分的调查、研究和准备，以确保行动或决策是合理、合法且符合最佳利益的。因此，正确答案是：

C：应尽职责

Due diligence

-------------------

题目3：Alex正在准备对其公司的网络系统进行渗透测试，为此他进行了招标。他想要最大程度地保证测试的有效性，并不关心真实的攻击。请问他在招标过程中需要进行什么类型的渗透测试？

Alex is preparing to solicit bids for a penetration test of his company’s network and systems. He wants to maximize the effectiveness of the testing rather than the realism of the test. What type of penetration test should he require in his bidding process?

A：黑盒

Black box

B：白盒

White box

C：灰盒

Gray box

D：零盒

Zero box

答案:在Alex的情况下，他想要最大程度地保证测试的有效性，而不关心真实的攻击。这意味着他希望测试人员能够尽可能全面地发现系统中的漏洞和弱点，而不需要模拟真实的攻击场景。因此，他应该选择\*\*白盒测试（White box）\*\*。

\*\*白盒测试\*\*是指测试人员在完全了解系统内部结构、代码和配置的情况下进行的测试。这种测试方式允许测试人员深入分析系统的各个方面，从而更有效地发现潜在的安全漏洞。由于测试人员拥有系统的详细信息，他们可以更全面地进行测试，而不需要花费大量时间进行信息收集和侦察。

其他选项的解释如下：

- \*\*黑盒测试（Black box）\*\*：测试人员对系统内部结构一无所知，模拟真实的攻击场景。这种方式更注重测试的真实性，但可能无法全面覆盖所有漏洞。

- \*\*灰盒测试（Gray box）\*\*：介于黑盒和白盒之间，测试人员拥有部分系统信息。这种方式在真实性和有效性之间取得平衡。

- \*\*零盒测试（Zero box）\*\*：这个选项并不是一个常见的测试类型，可能是干扰项。

因此，\*\*B：白盒（White box）\*\*是最适合Alex需求的渗透测试类型。

-------------------

题目4：通常会在渗透测试的什么阶段记录应用程序的标题信息？

Application banner information is typically recorded during what penetration testing phase?

A：计划

Planning

B：攻击

Attack

C：报告

Reporting

D：发现

Discovery

答案:题目4的正确答案是：

D：发现

Discovery

在渗透测试的发现阶段，测试人员会收集尽可能多的关于目标系统的信息，包括应用程序的标题信息（Application banner information）。这些信息有助于识别目标系统的类型、版本和可能的漏洞。

-------------------

题目5：Tony希望为他的组织进行灾难恢复计划测试演练。如果他想让演练成为最现实的事件，并且能够中断其组织的运营以进行演练，他应该进行哪种类型的演练？

Tony wants to conduct a disaster recovery plan test exercise for his organization. What type of exercise should he conduct if he wants it to be the most realistic event possible and is able to disrupt his organization’s operations to conduct the exercise?

A：通读

Read-through

B：完全中断

Full interruption

C：走查

Walk-through

D：模拟

Simulation

答案:题目5的正确答案是：

\*\*B：完全中断 (Full interruption)\*\*

解释：

- \*\*完全中断演练\*\*是最现实的灾难恢复测试类型，因为它会实际中断组织的运营，模拟真实的灾难场景。这种演练允许组织在实际中断的情况下测试其灾难恢复计划的有效性，确保所有系统和流程能够在真实情况下恢复运行。

- 其他选项如通读、走查和模拟虽然也是有效的测试方法，但它们不会实际中断组织的运营，因此不如完全中断演练那样现实。

-------------------

题目6：作为新的BYOD策略的一部分，Jim被要求能够识别员工自行带到公司的设备。这些设备并不会被加入到例如Active Directory这样的集中管理系统，下列哪项将会为Jim提供最佳方法来可靠地识别各个设备？

Jim has been asked to individually identify devices that users are bringing to work as part of a new BYOD policy. The devices will not be joined to a central management system like Active Directory, but he still needs to uniquely identify the systems. Which of the following options will provide Jim with the best means of reliably identifying each unique device?

A：记录各个系统的MAC地址

Record the MAC address of each system.

B：要求用户填写表格为每个系统进行注册

Require users to fill out a form to register each system.

C：利用端口扫描器对每个系统进行扫描

Scan each system using a port scanner.

D：通过Web注册系统采用设备指纹

Use device fingerprinting via a web-based registration system.

答案:在BYOD（Bring Your Own Device）策略中，识别员工自行带到公司的设备是一个重要的任务。由于这些设备不会被加入到集中管理系统（如Active Directory），因此需要一种可靠的方法来唯一地识别每个设备。以下是每个选项的分析：

A：记录各个系统的MAC地址

MAC地址是网络接口的唯一标识符，通常不会改变。记录MAC地址是一种简单且可靠的方法来识别设备。然而，MAC地址可以被伪造或更改，因此这种方法并不是绝对可靠的。

B：要求用户填写表格为每个系统进行注册

这种方法依赖于用户的诚实和准确性。用户可能会填写错误的信息，或者故意提供不准确的信息。因此，这种方法并不可靠。

C：利用端口扫描器对每个系统进行扫描

端口扫描器可以识别设备上开放的端口和服务，但这并不能唯一地识别设备。此外，端口扫描可能会被视为侵入性行为，引起用户的不满或隐私问题。

D：通过Web注册系统采用设备指纹

设备指纹是一种通过收集设备的多种信息（如浏览器类型、操作系统、屏幕分辨率、插件等）来唯一识别设备的技术。这种方法可以可靠地识别设备，并且不需要用户手动输入信息。设备指纹技术通常用于Web应用程序中，可以自动收集设备信息并生成唯一的标识符。

综上所述，\*\*D：通过Web注册系统采用设备指纹\*\* 是最佳的方法，因为它可以自动、可靠地识别每个设备，而不依赖于用户的手动输入或容易伪造的信息。

-------------------

题目7：Ben所在的组织使用正式数据治理计划。他正在与一个员工磋商，该员工参与了某个项目，该项目创建了一个全新的数据类，并希望为该数据类分配一个分类级别。谁负责将信息分配到分类级别？

Ben works in an organization that uses a formal data governance program. He is consulting with an employee working on a project that created an entirely new class of data and wants to work with the appropriate individual to assign a classification level to that information. Who is responsible for the assignment of information to a classification level?

A：数据创建者

Data creator

B：数据所有者

Data owner

C：CISO

CISO

D：数据监管者

Data custodian

答案:在正式的数据治理计划中，数据分类的责任通常由数据所有者（Data Owner）承担。数据所有者是对特定数据集负有最终责任的人，他们负责确定数据的敏感性、重要性以及适当的分类级别。数据所有者通常有权决定谁可以访问数据以及如何使用数据。

因此，正确答案是：

\*\*B：数据所有者\*\*

\*\*Data owner\*\*

-------------------

题目8：James希望确保其公司的备份能够在数据中心遭受灾难时幸免于难。以下哪个选项是解决此问题的最佳方法？

James wants to ensure that his company’s backups will survive a disaster that strikes the data center. Which of the following options is the best solution to this concern?

A：异地备份

Off-site backups

B：祖父/父/子备份分层系统

A grandfather/father/son backup tiering system

C：冗余备份系统

Redundant backup systems

D：SAN或NAS的快照

Snapshots to a SAN or NAS

答案:题目8的正确答案是：

\*\*A：异地备份 (Off-site backups)\*\*

### 解析：

James希望确保其公司的备份能够在数据中心遭受灾难时幸免于难。这意味着备份数据需要存储在远离主数据中心的地方，以防止灾难（如火灾、洪水、地震等）同时摧毁主数据中心和备份数据。

- \*\*A：异地备份 (Off-site backups)\*\*

这是最佳解决方案，因为异地备份将数据存储在远离主数据中心的位置，确保即使主数据中心遭受灾难，备份数据仍然安全可用。

- \*\*B：祖父/父/子备份分层系统 (A grandfather/father/son backup tiering system)\*\*

这是一种备份策略，用于管理不同时间点的备份数据，但它并不能解决数据中心灾难导致的数据丢失问题。

- \*\*C：冗余备份系统 (Redundant backup systems)\*\*

冗余备份系统可以提高数据的可用性和可靠性，但如果备份数据仍然存储在同一数据中心，仍然无法抵御灾难性事件。

- \*\*D：SAN或NAS的快照 (Snapshots to a SAN or NAS)\*\*

快照是一种快速备份技术，但如果快照数据存储在同一数据中心，仍然无法抵御灾难性事件。

因此，\*\*异地备份 (Off-site backups)\*\* 是最佳解决方案。

-------------------

题目9：密码的安全性是Gabe所在组织的信息安全计划的重中之重，她很担心密码的安全性。以下哪一项可通过对用户进行身份验证来帮助Gabe最大限度地保证密码安全？

Gabe is concerned about the security of passwords used as a cornerstone of his organization’s information security program. Which one of the following controls would provide the greatest improvement in Gabe’s ability to authenticate users?

A：更复杂的密码

More complex passwords

B：对用户进行安全教育以防止社会工程学攻击

User education against social engineering

C：多因素身份验证

Multifactor authentication

D：多使用基于个人知识的安全问题

Addition of security questions based on personal knowledge

答案:题目要求选择一种能够最大程度提高Gabe对用户进行身份验证能力的控制措施。我们来逐一分析选项：

A：更复杂的密码

虽然更复杂的密码可以增加密码的安全性，但它仍然依赖于单一的身份验证因素（即密码），因此无法显著提高身份验证的整体安全性。

B：对用户进行安全教育以防止社会工程学攻击

用户教育可以帮助防止社会工程学攻击，但它并不直接提高身份验证的安全性，尤其是在密码泄露或被盗的情况下。

C：多因素身份验证

多因素身份验证（MFA）要求用户提供两种或更多种不同类型的身份验证因素（例如密码和一次性验证码）。这种方法显著提高了身份验证的安全性，因为即使密码被泄露，攻击者仍然需要其他因素才能通过验证。

D：多使用基于个人知识的安全问题

基于个人知识的安全问题通常作为密码恢复的辅助手段，但它们本身并不提供额外的安全性，尤其是在攻击者能够通过社会工程学或其他手段获取这些信息的情况下。

综上所述，\*\*多因素身份验证\*\*（选项C）能够最大程度地提高Gabe对用户进行身份验证的能力，因此是最佳选择。

\*\*正确答案：C：多因素身份验证\*\*

-------------------

题目10：网络基础设施与控制层分离开来，供应商处于中立地位，网络编程设计都是基于标准的，这些概念与以下哪个选项关系最密切？

The separation of network infrastructure from the control layer, combined with the ability to centrally program a network design in a vendor-neutral, standards-based implementation, is an example of what important concept?

A：MPLS，使用较短标签替换长网络地址，支持各种协议

MPLS, a way to replace long network addresses with shorter labels and support a wide range of protocols

B：FCoE，一种在以太网上支持常见应用程序的融合协议

FCoE, a converged protocol that allows common applications over Ethernet

C：SDN，一种支持网络虚拟化的融合协议

SDN, a converged protocol that allows network virtualization

D：CDN，一种访问常见网络设计的融合协议

CDN, a converged protocol that makes common network designs accessible

答案:题目中描述的概念是将网络基础设施与控制层分离，并且网络编程设计是基于标准的、供应商中立的。这些特点最符合软件定义网络（Software-Defined Networking, SDN）的定义。SDN 是一种网络架构，它允许网络管理员通过软件程序来管理网络服务，而无需直接接触底层的硬件设备。这种架构使得网络更加灵活和可编程，同时也支持网络虚拟化。

因此，正确答案是：

C：SDN，一种支持网络虚拟化的融合协议

SDN, a converged protocol that allows network virtualization

-------------------

题目11：Susan准备报废其组织的一些DVD-ROM，这些DVD-ROM包含组织的最高机密数据。她应该怎么做才能确保数据不会暴露？

Susan is preparing to decommission her organization’s archival DVD-ROMs that contain Top Secret data. How should she ensure that the data cannot be exposed?

A：消磁

Degauss

B：零擦除

Zero wipe

C：粉碎

Pulverize

D：安全擦除

Secure erase

答案:在处理包含最高机密数据的DVD-ROM时，确保数据不会被恢复或暴露是至关重要的。对于DVD-ROM这种光学存储介质，消磁（Degauss）和零擦除（Zero wipe）并不适用，因为这些方法主要是针对磁性存储介质（如硬盘）的。安全擦除（Secure erase）通常用于固态硬盘或硬盘驱动器，而不是光学介质。

因此，最合适的方法是粉碎（Pulverize）。通过物理粉碎DVD-ROM，可以确保数据无法被恢复。这种方法能够彻底破坏介质，使得数据无法被读取或恢复。

所以，正确答案是：

C：粉碎

Pulverize

-------------------

题目12：Susan很关心一个复杂的变更，并希望确保如果变更没有按计划进行，组织可以恢复。她在组织的变革咨询委员会（CAB）中的角色应该提出什么要求？

Susan is worried about a complex change and wants to ensure that the organization can recover if the change does not go as planned. What should she require in her role on the organization’s change advisory board (CAB)?

A：由于存在风险，她应该拒绝更改

She should reject the change due to risk.

B：她应该要求进行第二次变更审查

She should require a second change review.

C：她应该确保存在回退计划

She should ensure a backout plan exists.

D：她应该确保存在故障转移计划

She should ensure a failover plan exists.

答案:在Susan的角色中，她需要确保组织能够应对变更过程中可能出现的任何问题，特别是如果变更没有按计划进行时。因此，她应该确保存在一个回退计划（backout plan），这样如果变更失败或导致问题，组织可以恢复到变更前的状态，从而最小化对业务的影响。

选项分析：

- A: 拒绝变更可能不是最佳选择，因为变更可能是必要的，而且拒绝变更可能阻碍组织的进步。

- B: 进行第二次变更审查可能有助于更好地理解变更的风险和影响，但这并不能直接解决变更失败后的恢复问题。

- C: 确保存在回退计划是直接针对Susan的担忧，即如果变更没有按计划进行，组织可以恢复。

- D: 故障转移计划通常用于系统故障时切换到备用系统，这与变更失败后的恢复不完全相同。

因此，最合适的答案是：

C：她应该确保存在回退计划

She should ensure a backout plan exists.

-------------------

题目13：Angie正在她的网络出口处配置监控以增强安全性，这样做会允许什么类型的数据包离开网络进入互联网？

Angie is configuring egress monitoring on her network to provide added security. Which one of the following packet types should Angie allow to leave the network headed for the internet?

A：源地址为Angie公共IP地址的数据包

Packets with a source address from Angie’s public IP address block

B：目的地址为Angie公共IP地址的数据包

Packets with a destination address from Angie’s public IP address block

C：源地址不是Angie地址块的数据包

Packets with a source address outside Angie’s address block

D：源地址为Angie私有地址的数据包

Packets with a source address from Angie’s private address block

答案:在配置网络出口监控（egress monitoring）时，Angie的目的是确保只有合法的数据包能够离开她的网络进入互联网。为了增强安全性，她应该允许以下类型的数据包离开网络：

\*\*A：源地址为Angie公共IP地址的数据包\*\*

- 这些数据包的源地址是Angie网络中的公共IP地址，表明这些数据包是从她的网络中合法发出的。允许这些数据包离开网络是合理的，因为它们代表合法的出站流量。

\*\*B：目的地址为Angie公共IP地址的数据包\*\*

- 这些数据包的目的地址是Angie的公共IP地址，表明这些数据包是进入她的网络的入站流量。这些数据包不应该被允许离开网络，因为它们实际上是进入网络的流量。

\*\*C：源地址不是Angie地址块的数据包\*\*

- 这些数据包的源地址不属于Angie的地址块，表明这些数据包可能是伪造的或来自未经授权的源。这些数据包不应该被允许离开网络，因为它们可能代表潜在的安全威胁。

\*\*D：源地址为Angie私有地址的数据包\*\*

- 这些数据包的源地址是Angie的私有IP地址。私有IP地址不应该出现在互联网上，因为它们只在内部网络中使用。允许这些数据包离开网络可能会导致安全问题，因为它们可能被误认为是合法的出站流量。

因此，\*\*A：源地址为Angie公共IP地址的数据包\*\* 是应该被允许离开网络进入互联网的数据包类型。

-------------------

题目14：Matt正在对Linux服务器进行渗透测试，并成功获得了对管理账户的访问权限。他现在想要获得密码散列用于暴力攻击。他在哪里可能找到散列值(假设系统的配置都是现代安全标准)？

Matt is conducting a penetration test against a Linux server and successfully gained access to an administrative account. He would now like to obtain the password hashes for use in a brute-force attack. Where is he likely to find the hashes, assuming the system is configured to modern security standards?

A：/etc/passwd

/etc/passwd

B：/etc/hash

/etc/hash

C：/etc/secure

/etc/secure

D：/etc/shadow

/etc/shadow

答案:在Linux系统中，密码散列值通常存储在 `/etc/shadow` 文件中。这个文件只有root用户或具有特权的用户才能访问，因为它包含了用户的加密密码散列值以及其他与密码相关的信息。

- \*\*/etc/passwd\*\*：这个文件包含了用户账户的基本信息，如用户名、用户ID、组ID、主目录和默认shell等。在现代Linux系统中，密码散列值不再存储在这个文件中，而是存储在 `/etc/shadow` 文件中。

- \*\*/etc/hash\*\* 和 \*\*/etc/secure\*\*：这些文件在标准的Linux系统中并不存在，因此不是存储密码散列值的地方。

- \*\*/etc/shadow\*\*：这是存储用户密码散列值的文件。它包含了加密后的密码、密码过期时间、密码修改时间等信息。只有root用户或具有特权的用户才能访问这个文件。

因此，正确答案是：

\*\*D：/etc/shadow\*\*

-------------------

题目15：Theresa正在实施一个新的访问控制系统，并希望确保开发人员无法将代码从开发系统移动到生产环境中。她希望确保签入代码的开发人员无法在此过程中批准他们自己的代码。她直接执行什么信息安全原则？

Theresa is implementing a new access control system and wants to ensure that developers do not have the ability to move code from development systems into the production environment. She wants to ensure that a developer who checks in code cannot then approve their own code as part of the process. What information security principle is she most directly enforcing?

A：职责分离

Separation of duties

B：双人控制

Two-person control

C：最小特权

Least privilege

D：工作轮换

Job rotation

答案:Theresa正在实施的安全措施最直接地体现了“职责分离”（Separation of duties）的信息安全原则。职责分离是一种安全措施，旨在通过将关键任务分配给不同的个人或团队来减少错误和欺诈的风险。在这个例子中，Theresa确保开发人员不能将代码从开发环境移动到生产环境，并且不能批准自己提交的代码，这正是一种职责分离的实践。这样做可以防止单个个体拥有过多的控制权，从而减少潜在的安全风险。

A：职责分离

Separation of duties

-------------------

题目16：以下哪种工具可提供不可否认性？

Which one of the following tools may be used to achieve the goal of nonrepudiation?

A：数字签名

Digital signature

B：对称加密

Symmetric encryption

C：防火墙

Firewall

D：IDS

IDS

答案:正确答案是 \*\*A：数字签名\*\*。

\*\*解释：\*\*

- \*\*数字签名\*\*（Digital signature）可以提供不可否认性（Nonrepudiation）。不可否认性是指发送方无法否认其发送过某条消息，接收方也无法否认其接收过某条消息。数字签名通过使用发送方的私钥对消息进行签名，接收方可以使用发送方的公钥验证签名的真实性，从而确保消息的来源和完整性。

- \*\*对称加密\*\*（Symmetric encryption）主要用于数据的保密性，但它无法提供不可否认性，因为加密和解密使用的是同一个密钥，无法区分发送方和接收方。

- \*\*防火墙\*\*（Firewall）主要用于网络安全，控制进出网络的流量，但它与不可否认性无关。

- \*\*IDS\*\*（Intrusion Detection System，入侵检测系统）用于检测网络中的异常行为或攻击，但它也无法提供不可否认性。

因此，\*\*数字签名\*\*是唯一能够提供不可否认性的工具。

-------------------

题目17：在这里的TCP三次握手的图中，系统A在步骤3中应该向系统B发送什么？

In this diagram of the TCP three-way handshake, what should system A send to system B in step 3?

<div style="text-align:center"><img alt="" height="488" src="/file/100000/m/20210825/510e63f3623e41cc9cc5e2edd70a21dc.png" width="638" /></div>

A：ACK

ACK

B：SYN

SYN

C：FIN

FIN

D：RST

RST

答案:在TCP三次握手的第三步中，系统A应该向系统B发送一个ACK（确认）包。这个ACK包用于确认系统B发送的SYN+ACK包，并完成连接的建立。

因此，正确答案是：

A：ACK

-------------------

题目18：什么RADIUS备用方案通常用于思科网络设备并支持双因素身份验证？

What RADIUS alternative is commonly used for Cisco network gear and supports twofactor authentication?

A：RADIUS +

RADIUS +

B：TACACS +

TACACS +

C：XTACACS

XTACACS

D：Kerberos

Kerberos

答案:题目18的正确答案是：

B：TACACS +

TACACS+（Terminal Access Controller Access-Control System Plus）是思科网络设备中常用的RADIUS替代方案，并且支持双因素身份验证。TACACS+提供了更细粒度的访问控制和更强大的安全性，通常用于网络设备的身份验证、授权和审计（AAA）服务。

-------------------

题目19：VoIP呼叫管理器和VoIP电话最容易受到以下哪两种类型的攻击？

What two types of attacks are VoIP call managers and VoIP phones most likely to be susceptible to?

A：DoS和恶意软件

DoS and malware

B：蠕虫和木马

Worms and Trojans

C：DoS和主机操作系统攻击

DoS and host OS attacks

D：主机操作系统攻击和缓冲区溢出

Host OS attacks and buffer overflows

答案:VoIP（Voice over Internet Protocol）呼叫管理器和VoIP电话最容易受到以下两种类型的攻击：

A：DoS和恶意软件

DoS and malware

解释：

1. \*\*DoS（拒绝服务）攻击\*\*：VoIP系统依赖于网络连接，因此容易受到DoS攻击。攻击者可以通过发送大量请求或占用带宽来使VoIP服务不可用，导致通话中断或服务质量下降。

2. \*\*恶意软件\*\*：VoIP设备通常运行在操作系统上，可能会受到恶意软件的攻击。恶意软件可以窃取敏感信息、破坏系统功能或传播到其他设备。

其他选项虽然也可能对VoIP系统构成威胁，但DoS和恶意软件是最常见和最直接的影响VoIP系统的攻击类型。

-------------------

题目20：Vivian为零售连锁商店工作，并且希望销售点的终端设备上只能使用预先批准的软件。Vivian应该使用什么方法？

Vivian works for a chain of retail stores and would like to use a software product that restricts the software used on point-of-sale terminals to those packages on a preapproved list. What approach should Vivian use?

A：反病毒

Antivirus

B：启发式

Heuristic

C：白名单

Whitelist

D：黑名单

Blacklist

答案:Vivian希望销售点的终端设备上只能使用预先批准的软件。这意味着她需要一种方法来限制终端设备上可以运行的软件，只允许那些在预先批准的列表中的软件运行。

- \*\*反病毒（Antivirus）\*\*：反病毒软件主要用于检测和删除恶意软件，但它并不直接限制哪些软件可以在设备上运行。

- \*\*启发式（Heuristic）\*\*：启发式方法通常用于检测未知的恶意软件，但它也不直接限制哪些软件可以在设备上运行。

- \*\*白名单（Whitelist）\*\*：白名单是一种安全机制，它只允许预先批准的软件在设备上运行。这与Vivian的需求完全一致。

- \*\*黑名单（Blacklist）\*\*：黑名单是一种安全机制，它阻止已知的不良软件在设备上运行，但它并不限制其他未列入黑名单的软件。

因此，Vivian应该使用\*\*白名单（Whitelist）\*\*的方法来限制销售点终端设备上只能使用预先批准的软件。

正确答案是 \*\*C：白名单\*\*。

-------------------

题目21-1：参照以下情景，回答3个问题。

Hunter是大数据中心管理公司DataTech的设备经理。公司为一个设备安装防洪系统，他正在评估这件事，该设备和设备中的数据总价值1亿美元，安装新的防洪系统将花费1000万美元。

Hunter咨询了洪水专家，了解到该设备所处的洪泛平原每200年会发一次洪水，一旦洪水发生，它可能导致2000万美元的设备受损。

For questions , please refer to the following scenario:

Hunter is the facilities manager for DataTech, a large data center management firm. He is evaluating the installation of a flood prevention system at one of DataTech’s facilities. The facility and contents are valued at $100 million. Installing the new flood prevention system would cost $10 million.

Hunter consulted with flood experts and determined that the facility lies within a 200-year flood plain and that, if a flood occurred, it would likely cause $20 million in damage to the facility.

根据上述信息，DataTech的数据中心受洪水影响的暴露因子是多少？

Based on the information in this scenario, what is the exposure factor for the effect of a flood on DataTech’s data center?

A：2%

2 percent

B：20%

20 percent

C：100%

100 percent

D：200%

200 percent

答案:暴露因子（Exposure Factor, EF）是指在发生特定风险事件时，资产可能遭受的损失比例。在这个情景中，洪水可能导致2000万美元的设备受损，而设备的总价值是1亿美元。

暴露因子的计算公式是：

\[ \text{暴露因子} = \frac{\text{可能的损失}}{\text{资产总价值}} \]

将数值代入公式：

\[ \text{暴露因子} = \frac{20,000,000}{100,000,000} = 0.2 \]

将0.2转换为百分比：

\[ 0.2 \times 100\% = 20\% \]

因此，DataTech的数据中心受洪水影响的暴露因子是20%。

正确答案是：

B：20%

20 percent

-------------------

题目21-1：参照以下情景，回答3个问题。

Hunter是大数据中心管理公司DataTech的设备经理。公司为一个设备安装防洪系统，他正在评估这件事，该设备和设备中的数据总价值1亿美元，安装新的防洪系统将花费1000万美元。

Hunter咨询了洪水专家，了解到该设备所处的洪泛平原每200年会发一次洪水，一旦洪水发生，它可能导致2000万美元的设备受损。

For questions , please refer to the following scenario:

Hunter is the facilities manager for DataTech, a large data center management firm. He is evaluating the installation of a flood prevention system at one of DataTech’s facilities. The facility and contents are valued at $100 million. Installing the new flood prevention system would cost $10 million.

Hunter consulted with flood experts and determined that the facility lies within a 200-year flood plain and that, if a flood occurred, it would likely cause $20 million in damage to the facility.

根据上述信息，DataTech数据中心的洪水年度发生率是多少？

Based on the information in this scenario, what is the annualized rate of occurrence for a flood at DataTech&rsquo;s data center?

A：0.002

0.002

B：0.005

0.005

C：0.02

0.02

D：0.05

0.05

答案:根据题目描述，DataTech数据中心所处的洪泛平原每200年会发一次洪水。因此，洪水的年度发生率可以通过以下公式计算：

\[ \text{年度发生率} = \frac{1}{\text{洪水发生的年数}} \]

将洪水发生的年数代入公式：

\[ \text{年度发生率} = \frac{1}{200} = 0.005 \]

因此，DataTech数据中心的洪水年度发生率是0.005。

正确答案是 \*\*B：0.005\*\*。

-------------------

题目21-1：参照以下情景，回答3个问题。

Hunter是大数据中心管理公司DataTech的设备经理。公司为一个设备安装防洪系统，他正在评估这件事，该设备和设备中的数据总价值1亿美元，安装新的防洪系统将花费1000万美元。

Hunter咨询了洪水专家，了解到该设备所处的洪泛平原每200年会发一次洪水，一旦洪水发生，它可能导致2000万美元的设备受损。

For questions , please refer to the following scenario:

Hunter is the facilities manager for DataTech, a large data center management firm. He is evaluating the installation of a flood prevention system at one of DataTech’s facilities. The facility and contents are valued at $100 million. Installing the new flood prevention system would cost $10 million.

Hunter consulted with flood experts and determined that the facility lies within a 200-year flood plain and that, if a flood occurred, it would likely cause $20 million in damage to the facility.

根据这种情况下的信息，DataTech数据中心的洪水年化损失预期值是多少？

Based on the information in this scenario, what is the annualized loss expectancy for a flood at DataTech’s data center?

A：40,000美元

$40,000

B：100,000美元

$100,000

C：400,000美元

$400,000

D：1,000,000美元

$1,000,000

答案:要计算DataTech数据中心的洪水年化损失预期值（Annualized Loss Expectancy, ALE），我们需要使用以下公式：

\[

ALE = \text{单次事件损失} \times \text{年发生概率}

\]

根据题目提供的信息：

- 单次洪水事件导致的设备损失为2000万美元（$20,000,000）。

- 洪水发生的频率为每200年一次，因此年发生概率为1/200，即0.005。

将这些数值代入公式：

\[

ALE = 20,000,000 \times 0.005 = 100,000 \text{美元}

\]

因此，DataTech数据中心的洪水年化损失预期值是100,000美元。

正确答案是 \*\*B：100,000美元\*\*。

-------------------

题目22：哪些账户通常在账户管理评估期间进行评估？

Which accounts are typically assessed during an account management assessment?

A：随机样本

A random sample

B：高特权的账户

Highly privileged accounts

C：最近生成的账户

Recently generated accounts

D：长期存在的账户

Accounts that have existed for long periods of time

答案:在账户管理评估期间，通常会评估以下几种类型的账户：

B：高特权的账户（Highly privileged accounts）

这些账户通常拥有对系统或数据的广泛访问权限，因此它们的安全性至关重要。评估这些账户有助于确保它们没有被滥用或受到威胁。

C：最近生成的账户（Recently generated accounts）

新创建的账户可能需要特别关注，以确保它们是根据适当的政策和程序创建的，并且没有被用于未经授权的活动。

D：长期存在的账户（Accounts that have existed for long periods of time）

长期存在的账户可能会积累不必要的权限或成为安全漏洞的来源。评估这些账户有助于识别和纠正潜在的安全问题。

A：随机样本（A random sample）

虽然随机样本也可以用于评估，但它并不是一个特定类型的账户，而是一种评估方法。通过随机抽样，可以确保评估的全面性和代表性。

因此，最合适的答案是 B、C 和 D。

-------------------

题目23：云计算将共享责任模型用于安全方面，其中供应商和客户各自承担一些安全性责任。责任划分取决于所使用的服务模式。从客户承担最小责任的情况到客户承担最大责任的情况，请按这个顺序、依据下列选项排列出云服务产品。

1. IaaS

2. SaaS

3. PaaS

Cloud computing uses a shared responsibility model for security, where the vendor and customer both bear some responsibility for security. The division of responsibility depends upon the type of service used. Place the cloud service offerings listed here in order from the case where the customer bears the least responsibility to where the customer bears the most responsibility.

1.IaaS

2.SaaS

3.PaaS

A：1,2,3

1,2,3

B：2,1,3

2,1,3

C：3,2,1

3,2,1

D：2,3,1

2,3,1

答案:在云计算的安全共享责任模型中，供应商和客户各自承担不同的安全责任，具体取决于所使用的服务模式。通常，客户在SaaS（软件即服务）模式下承担的责任最少，而在IaaS（基础设施即服务）模式下承担的责任最多。PaaS（平台即服务）则介于两者之间。

因此，按照客户承担责任从最小到最大的顺序排列，正确的顺序是：

2. SaaS

3. PaaS

1. IaaS

所以正确答案是：

\*\*D：2,3,1\*\*

-------------------

题目24：当合法的用户使用生物识别器而未被成功验证时，会发生什么类型的错误？

What type of error occurs when a valid subject using a biometric authenticator is not authenticated?

A：类型1错误

A Type1error

B：类型2错误

A Type2error

C：类型3错误

A Type3error

D：类型4错误

A Type4error

答案:在生物识别系统中，错误通常分为两种类型：

- \*\*类型1错误（Type 1 Error）\*\*：也称为“假拒绝率”（False Rejection Rate, FRR），指的是合法用户被系统错误地拒绝访问的情况。也就是说，系统未能识别出合法的用户。

- \*\*类型2错误（Type 2 Error）\*\*：也称为“假接受率”（False Acceptance Rate, FAR），指的是非法用户被系统错误地接受为合法用户的情况。也就是说，系统错误地识别了非法用户。

根据题目描述，当合法的用户使用生物识别器而未被成功验证时，发生的是\*\*类型1错误\*\*。

因此，正确答案是：

\*\*A：类型1错误\*\*

-------------------

题目25：办公桌下的紧急按钮是什么类型的物理安全系统的常见示例？

An emergency button under the desk is a common example of what type of physical security system?

A：气隙按钮

An airgap button

B：键盘记录器

A keylogger

C：按钮锁

A pushbutton lock

D：胁迫系统

A duress system

答案:题目25的正确答案是：

D：胁迫系统

A duress system

办公桌下的紧急按钮是一种胁迫系统的常见示例。胁迫系统是一种物理安全系统，允许用户在紧急情况下（如遭遇威胁或危险）秘密地发出警报，而不引起潜在攻击者的注意。这种系统通常用于银行、办公室和其他需要高安全性的场所。

-------------------

题目26：Henry针对Apache Web服务器运行Nikto并接收此处显示的输出。以下哪项包括在他的报告中的描述最不重要？

Henry runs Nikto against an Apache web server and receives the output shown here. Which of the following statements is the least important to include in his report?

<div style="text-align:center"><img alt="" height="320" src="/file/100000/m/20210825/eb27971c8ed3494f823369ba659dc3ff.png" width="659" /></div>

A：缺少的点击劫持x-frame选项，可用于将输入重定向到恶意站点或框架

The missing clickjacking x-frame options could be used to redirect input to a malicious site or frame.

B：应该启用跨站点脚本保护，但没有启用

Cross-site scripting protections should be enabled, but aren’t.

C：Linux系统的inode信息泄漏是一个严重漏洞，允许使用节点引用直接访问文件系统

Inode information leakage from a Linux system is a critical vulnerability allowing direct access to the filesystem using node references.

D：服务器为Linux服务器

The server is a Linux server.

答案:在Henry的报告中最不重要的描述是：

\*\*D：服务器为Linux服务器\*\*

The server is a Linux server.

\*\*解释：\*\*

- \*\*A\*\* 和 \*\*B\*\* 都涉及到具体的安全漏洞和防护措施，这些信息对于评估服务器的安全性非常重要。

- \*\*C\*\* 提到了一个严重的安全漏洞（inode信息泄漏），这可能会直接影响到系统的安全性。

- \*\*D\*\* 只是说明了服务器的操作系统类型，虽然这可能对某些分析有帮助，但它并不直接涉及到安全漏洞或防护措施，因此在报告中相对不那么重要。

因此，\*\*D\*\* 是最不重要的描述。

-------------------

题目27：George正在协助检察官对一个试图侵入乔治公司计算机系统的黑客提出起诉。他把系统日志交给检察官作为证据，检察官坚持要求乔治在庭上说明他是如何收集日志的。什么证据规则要求乔治的证词？

George is assisting a prosecutor with a case against a hacker who attempted to break into the computer systems at George’s company. He provides system logs to the prosecutor for use as evidence, but the prosecutor insists that George testify in court about how he gathered the logs. What rule of evidence requires George’s testimony?

A：证词证据规则

Testimonial evidence rule

B：口头证据规则

Parol evidence rule

C：最佳证据规则

Best evidence rule

D：传闻证据规则

Hearsay rule

答案:正确答案是：C 最佳证据规则（Best evidence rule）

最佳证据规则要求，当提交书面或电子记录作为证据时，必须提供原始文件或记录，或者提供充分的解释说明为什么无法提供原始文件。在这种情况下，George需要出庭作证，说明他是如何收集系统日志的，以确保这些日志的真实性和完整性。这符合最佳证据规则的要求。

-------------------

题目28：以下哪项不是关键风险指标的有效用途（KRI）？

Which of the following is not a valid use for key risk indicators (KRIs)?

A：在问题发生之前提供警告

Provide warnings before issues occur.

B：提供实时事件响应信息

Provide real-time incident response information.

C：提供过去事件的历史信息

Provide historical views of past incidents.

D：提供组织风险承受力的信息

Provide insight into risk tolerance for the organization.

答案:关键风险指标（KRI）的主要目的是帮助组织识别和监控潜在的风险，以便在问题发生之前采取预防措施。因此，KRI的有效用途包括：

A：在问题发生之前提供警告 - 这是KRI的主要用途之一，通过监控关键指标，组织可以在风险演变为问题之前采取行动。

B：提供实时事件响应信息 - KRI可以帮助组织实时监控风险状况，从而在事件发生时迅速做出响应。

D：提供组织风险承受力的信息 - KRI可以帮助组织了解其风险承受能力，并据此调整风险管理策略。

C：提供过去事件的历史信息 - 虽然历史信息对于分析趋势和模式很有用，但这并不是KRI的主要用途。KRI更关注当前和未来的风险状况，而不是过去的事件。

因此，选项C“提供过去事件的历史信息”不是关键风险指标的有效用途。

正确答案是：C

-------------------

题目29：以下哪种恶意软件针对系统漏洞使用内置的传播机制来传播？

Which one of the following malware types uses built-in propagation mechanisms that exploit system vulnerabilities to spread?

A：特洛伊木马

Trojan horse

B：蠕虫

Worm

C：逻辑炸弹

Logic bomb

D：病毒

Virus

答案:正确答案是 B：蠕虫 (Worm)。

蠕虫是一种恶意软件，它利用系统漏洞和内置的传播机制来自动传播到其他系统。与病毒不同，蠕虫不需要依附于其他程序或文件来传播，它可以通过网络、电子邮件或其他通信渠道独立传播。蠕虫通常利用系统漏洞来感染目标系统，并进一步传播到其他易受攻击的系统。

其他选项的解释：

- A：特洛伊木马 (Trojan horse) 是一种伪装成合法软件的恶意程序，通常不包含自我传播的机制。

- C：逻辑炸弹 (Logic bomb) 是一种在特定条件满足时触发的恶意代码，通常不包含传播机制。

- D：病毒 (Virus) 是一种依附于其他程序或文件的恶意代码，需要用户执行感染的文件或程序才能传播。

因此，蠕虫是利用系统漏洞并通过内置传播机制传播的恶意软件类型。

-------------------

题目30：作为公司安全团队的一员，你被要求就对如何确保介质不会被不恰当使用或存储提出建议。 什么解决方案可以帮助组织中的员工适当地处理介质？

As part of your company’s security team, you have been asked to advise on how to ensure that media is not improperly used or stored. What solution will help staff members in your organization to handle media appropriately?

A：标记敏感级别

Labeling with sensitivity levels

B：加密敏感介质

Encrypting the sensitive media

C：双控介质系统

Dual control media systems

D：明确桌面策略

A clear desk policy

答案:为了确保介质不会被不恰当使用或存储，组织可以采取多种措施。以下是对每个选项的分析：

A：标记敏感级别 (Labeling with sensitivity levels)

- 这种方法可以帮助员工识别哪些介质包含敏感信息，从而在处理这些介质时更加小心。通过明确标记介质的敏感级别，员工可以更容易地遵循相应的安全协议。

B：加密敏感介质 (Encrypting the sensitive media)

- 加密是保护敏感数据的有效方法。即使介质丢失或被盗，加密的数据也难以被未经授权的人员访问。这可以大大降低数据泄露的风险。

C：双控介质系统 (Dual control media systems)

- 双控系统要求两个或多个人员共同操作才能访问或处理介质。这种方法可以增加安全性，防止单个人员滥用或误用介质。

D：明确桌面策略 (A clear desk policy)

- 明确的桌面策略要求员工在离开工作区域时清理桌面，确保敏感介质不会被无意中暴露。这可以减少介质被不当访问或丢失的风险。

综合来看，最全面的解决方案可能是结合以上几种方法。例如，组织可以实施标记敏感级别和加密敏感介质的措施，同时采用双控介质系统和明确的桌面策略，以确保介质的安全使用和存储。

因此，最佳答案是结合多种措施，但单独来看，\*\*B：加密敏感介质 (Encrypting the sensitive media)\*\* 是最直接和有效的解决方案之一，因为它直接保护数据本身，即使介质丢失或被盗，数据仍然安全。

-------------------

题目31：Alaina希望在其组织的威胁情报工作中使用广泛采用的威胁建模框架。如果她想使用现有的工具来帮助她的威胁建模团队整合内部创建的情报和外部威胁源数据，你会建议她采用以下哪项？

Alaina wants to use a broadly adopted threat modeling framework for her organization’s threat intelligence efforts. Which of the following would you advise her to adopt if she wants to use preexisting tools to help her threat modeling team integrate both internally created intelligence and external threat feed data?

A：入侵分析的钻石模型

The Diamond Model of Intrusion Analysis

B：ATT&amp;CK

ATT&amp;CK

C：微软的Threat-JUMP建模系统

Microsoft’s Threat-JUMP modeling system

D：Threat-EN

Threat-EN

答案:在威胁情报工作中，选择合适的威胁建模框架对于整合内部情报和外部威胁源数据至关重要。根据题目描述，Alaina希望使用现有的工具来帮助她的团队进行威胁建模。以下是各个选项的分析：

A. \*\*入侵分析的钻石模型 (The Diamond Model of Intrusion Analysis)\*\*

钻石模型主要用于分析入侵事件，强调攻击者、受害者、基础设施和能力的四个核心要素。它主要用于事件分析和归因，而不是一个全面的威胁建模框架。

B. \*\*ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)\*\*

ATT&CK 是一个广泛采用的威胁建模框架，专注于对手的行为和战术。它提供了详细的战术、技术和程序（TTPs），并且可以很好地整合内部和外部威胁情报数据。ATT&CK 框架有丰富的工具和资源支持，适合用于威胁建模和情报共享。

C. \*\*微软的Threat-JUMP建模系统 (Microsoft's Threat-JUMP modeling system)\*\*

Threat-JUMP 是微软开发的一个威胁建模系统，主要用于内部威胁建模和风险评估。虽然它是一个有效的工具，但它的应用范围相对较窄，且不如 ATT&CK 那样广泛采用。

D. \*\*Threat-EN\*\*

Threat-EN 并不是一个广泛采用或知名的威胁建模框架，因此可能缺乏足够的工具和社区支持。

### 结论：

\*\*B. ATT&CK\*\* 是最合适的选项。它是一个广泛采用的威胁建模框架，能够有效地整合内部和外部威胁情报数据，并且有丰富的工具和资源支持。

\*\*建议答案：B. ATT&CK\*\*

-------------------

题目32：下列哪一项不是软件开发的敏捷方法的原则？

Which one of the following is not a principle of the Agile approach to software development?

A：传递信息的最有效方法是通过网络

The most efficient method of conveying information is electronic.

B：工作软件是进度的主要衡量标准

Working software is the primary measure of progress.

C：简单是至关重要的

Simplicity is essential.

D：业务人员和开发人员必须每天一起工作

Businesspeople and developers must work together daily.

答案:题目32的正确答案是：

A：传递信息的最有效方法是通过网络

The most efficient method of conveying information is electronic.

解释：

敏捷开发方法的原则强调面对面的沟通和协作，认为这是传递信息的最有效方法。敏捷宣言中的原则之一是“个体和互动高于流程和工具”，强调了人与人之间的直接沟通的重要性。因此，选项A中的“传递信息的最有效方法是通过网络”与敏捷方法的原则不符。其他选项B、C和D都是敏捷方法的核心原则。

-------------------

题目33：Harry担心其组织内的会计师会修改数据，以掩盖他们通常访问的账户中的欺诈活动。以下哪种控制最能抵御此类攻击？

Harry is concerned that accountants within his organization will modify data to cover up fraudulent activity in accounts that they normally access. Which one of the following controls would best defend against this type of attack?

A：加密

Encryption

B：访问控制

Access controls

C：完整性验证

Integrity verification

D：防火墙

Firewalls

答案:题目中描述的情况是会计师可能会修改数据以掩盖欺诈活动。这种情况下，最有效的控制措施是能够检测或防止数据被未经授权修改的机制。

- \*\*A：加密\*\* - 加密主要用于保护数据的机密性，防止未经授权的访问者读取数据。然而，加密并不能防止已经有权访问数据的人（如会计师）修改数据。

- \*\*B：访问控制\*\* - 访问控制可以限制谁可以访问特定的数据或系统。然而，如果会计师已经有权访问这些数据，访问控制本身并不能防止他们修改数据。

- \*\*C：完整性验证\*\* - 完整性验证机制（如哈希校验、数字签名等）可以检测数据是否被篡改。如果数据被修改，完整性验证可以检测到这种变化，从而帮助发现潜在的欺诈行为。因此，完整性验证是最能抵御这种攻击的控制措施。

- \*\*D：防火墙\*\* - 防火墙主要用于控制网络流量，防止未经授权的网络访问。它并不能防止已经有权访问系统的人修改数据。

因此，\*\*C：完整性验证\*\* 是最能抵御这种攻击的控制措施。

\*\*答案：C：完整性验证\*\*

-------------------

题目34：Ben希望通过环境设计使用预防犯罪的概念来帮助保护他的设施。以下哪项不是这种设计理念的常见例子？

Ben wants to use the concept of crime prevention through environmental design to help secure his facility. Which of the following is not a common example of this design concept in use?

A：在全视野安装摄像头，起到威慑作用

Mounting cameras in full view to act as a deterrent

B：限制花盆的大小，避免它们被用于隐藏

Limiting the size of planters to avoid having them used to hide behind

C：将数据中心定位在建筑物的边缘以增强安全性

Locating data centers at the edge of the building to enhance security

D：减少公众对送货通道和入口的可见度

Making delivery access driveways and entrances less visible to the public

答案:预防犯罪的环境设计（CPTED，Crime Prevention Through Environmental Design）是一种通过环境设计和建筑布局来减少犯罪机会的策略。这种设计理念通常包括增加自然监控、强化领域感、控制入口和出口、以及维护环境等措施。

让我们逐一分析选项：

A：在全视野安装摄像头，起到威慑作用

- 这是CPTED的常见做法，通过增加监控来威慑潜在的犯罪行为。

B：限制花盆的大小，避免它们被用于隐藏

- 这也是CPTED的常见做法，通过减少潜在的藏身之处来增加安全性。

C：将数据中心定位在建筑物的边缘以增强安全性

- 这不符合CPTED的原则。通常，重要的设施（如数据中心）应该位于建筑物的核心区域，以减少被外部攻击的风险。将数据中心放在建筑物的边缘可能会增加其暴露在外部威胁中的风险。

D：减少公众对送货通道和入口的可见度

- 这也是CPTED的常见做法，通过减少对敏感区域的可见性来降低犯罪机会。

因此，选项C“将数据中心定位在建筑物的边缘以增强安全性”不是预防犯罪的环境设计理念的常见例子。

最终答案是：C

-------------------

题目35：Meena希望确保她的供应链风险得到妥善管理。以下哪项不是她应该包括在供应链风险管理 (SCRM) 计划中的常见做法？

Meena wants to ensure that her supply chain risks are well managed. Which of the following is not a common practice she should include in her supply chain risk management (SCRM) plan?

A：在适当的情况下使用合同控制，例如保险和责任限制

Use contractual controls such as insurance and liability limitations where appropriate.

B：稳定的唯一供应商来源

Sole source to provide vendor stability.

C：确保关键组件存在多个供应商

Ensure multiple suppliers exist for critical components.

D：验证潜在供应商的财务稳定性

Validate the financial stability of potential suppliers.

答案:在供应链风险管理（SCRM）计划中，常见的做法包括：

A：在适当的情况下使用合同控制，例如保险和责任限制。这有助于在发生风险时减少潜在的财务损失。

C：确保关键组件存在多个供应商。这可以减少对单一供应商的依赖，从而降低供应链中断的风险。

D：验证潜在供应商的财务稳定性。这有助于确保供应商在财务上是稳健的，能够持续提供产品和服务。

然而，选项B“稳定的唯一供应商来源”并不是一个常见的供应链风险管理做法。依赖单一供应商会增加供应链的风险，因为如果该供应商出现问题（如生产中断、财务困难等），整个供应链可能会受到严重影响。因此，依赖单一供应商通常被认为是不良的供应链管理实践。

所以，正确答案是：

B：稳定的唯一供应商来源

Sole source to provide vendor stability.

-------------------

题目36-1：使用下表，以及你对审计过程的了解，回答3个问题 。

<div style="text-align:center"><img alt="" height="200" src="/file/100000/m/20210825/8e4e100de88b42158b02df71347db16a.png" width="701" /></div>

Using the following table and your knowledge of the auditing process, answer questions .

<div style="text-align:center"><img alt="" height="256" src="/file/100000/m/20210825/809c2af959984bed938ae85b6834fa2c.png" width="651" /></div>

Susan的公司正在准备将其数据中心迁移到基础架构即服务(IaaS)提供商时，希望了解该新提供商的安全性、完整性和可用性控制的有效性。什么样的SOC报告可以为他们提供最详细的信息，包括审计师对IaaS提供商控制有效性的意见？

As they prepare to migrate their data center to an infrastructure as a service (IaaS) provider, Susan’s company wants to understand the effectiveness of their new provider’s security, integrity, and availability controls. What SOC report would provide them with the most detail, including input from the auditor on the effectiveness of controls at the IaaS provider?

A：SOC 1

SOC 1

B：SOC 2

SOC 2

C：SOC 3

SOC 3

D：没有一份SOC报告适合于此，他们应该要求另一种形式的报告

None of the SOC reports is suited to this, and they should request another form of report.

答案:正确答案是 \*\*B：SOC 2\*\*。

### 解析：

SOC（System and Organization Controls）报告分为三种类型：SOC 1、SOC 2 和 SOC 3。每种报告适用于不同的场景和需求。

- \*\*SOC 1\*\*：主要关注与财务报告相关的内部控制，适用于服务组织对客户财务报告的影响。它不直接涉及安全性、完整性和可用性控制。

- \*\*SOC 2\*\*：专门针对服务组织的安全性、可用性、处理完整性、保密性和隐私性控制。SOC 2 报告提供了详细的审计意见，说明服务组织的控制是否有效，并且可以根据客户的需求定制报告内容。因此，SOC 2 是 Susan 的公司最需要的报告类型，因为它直接涉及 IaaS 提供商的安全性、完整性和可用性控制。

- \*\*SOC 3\*\*：与 SOC 2 类似，但 SOC 3 报告是公开的、简化的版本，不包含详细的审计意见或控制测试结果。因此，SOC 3 不适用于需要详细了解控制有效性的情况。

- \*\*选项 D\*\*：不正确，因为 SOC 2 报告正是为这种情况设计的。

因此，\*\*SOC 2\*\* 是 Susan 的公司应该要求的报告类型。

-------------------

题目36-1：使用下表，以及你对审计过程的了解，回答3个问题 。

<div style="text-align:center"><img alt="" height="200" src="/file/100000/m/20210825/8e4e100de88b42158b02df71347db16a.png" width="701" /></div>

Using the following table and your knowledge of the auditing process, answer questions .

<div style="text-align:center"><img alt="" height="256" src="/file/100000/m/20210825/809c2af959984bed938ae85b6834fa2c.png" width="651" /></div>

Susan希望确保组织需要的审计报告要包括：来自外部审计师的意见和有关一段时间内控制实施的信息。她应该要求什么类型的报告？

Susan wants to ensure that the audit report that her organization requested includes input from an external auditor and information about control implementation over a period of time. What type of report should she request?

A：SOC 2, 类型1

SOC 2, Type 1

B：SOC 3, 类型1

SOC 3, Type 1

C：SOC 2, 类型2

SOC 2, Type 2

D：SOC 3, 类型2

SOC 3, Type 2

答案:根据题目描述，Susan希望确保审计报告包括外部审计师的意见以及一段时间内控制实施的信息。我们需要选择符合这些要求的报告类型。

- \*\*SOC 2, Type 1\*\*：这种报告提供的是在某一特定时间点（通常是审计日）的控制环境的描述和审计师的意见。它不涉及一段时间内的控制实施情况。

- \*\*SOC 2, Type 2\*\*：这种报告不仅提供在某一特定时间点的控制环境描述和审计师的意见，还包括一段时间内（通常是6个月或1年）控制实施的有效性评估。因此，它符合Susan的要求。

- \*\*SOC 3, Type 1\*\* 和 \*\*SOC 3, Type 2\*\*：SOC 3报告是SOC 2报告的简化版本，通常用于公开分发，不包含详细的控制描述和测试结果。因此，它们不符合Susan的要求。

综上所述，Susan应该要求 \*\*SOC 2, Type 2\*\* 报告。

\*\*正确答案：C：SOC 2, 类型2\*\*

-------------------

题目36-1：使用下表，以及你对审计过程的了解，回答3个问题 。

<div style="text-align:center"><img alt="" height="200" src="/file/100000/m/20210825/8e4e100de88b42158b02df71347db16a.png" width="701" /></div>

Using the following table and your knowledge of the auditing process, answer questions .

<div style="text-align:center"><img alt="" height="256" src="/file/100000/m/20210825/809c2af959984bed938ae85b6834fa2c.png" width="651" /></div>

当Susan请求SOC 2报告时，她收到了SOC 1报告。Susan应该提出什么问题？

When Susan requests an SOC 2 report, she receives an SOC 1 report. What issue should Susan raise?

A：SOC 1报告仅披露公开可用的信息

SOC 1 reports only reveal publicly available information.

B：SOC 1报告涵盖财务数据

SOC 1 reports cover financial data.

C：SOC 1报告仅涵盖一个时间点

SOC 1 reports only cover a point in time.

D：SOC 1报告仅使用三个月的时间进行测试

SOC 1 reports only use a three-month period for testing.

答案:Susan请求的是SOC 2报告，但她收到了SOC 1报告。SOC 1和SOC 2报告的主要区别在于它们所涵盖的内容和目的。

- \*\*SOC 1报告\*\*：主要关注与财务报告相关的内部控制，通常用于审计财务报表。它涵盖了与财务数据相关的控制措施。

- \*\*SOC 2报告\*\*：主要关注与安全性、可用性、处理完整性、保密性和隐私性相关的控制措施。它通常用于评估服务组织的非财务控制。

因此，Susan应该提出的问题是SOC 1报告涵盖的是财务数据，而不是她所期望的与安全性、可用性等相关的控制措施。

正确答案是：

\*\*B：SOC 1报告涵盖财务数据\*\*

SOC 1 reports cover financial data.

-------------------

题目37：Brad希望聘请第三方审计师来评估其公司将与之签订合同的供应商。如果Brad希望评估供应商的安全策略、控制以及随着时间的推移实施的这些控制的有效性，他应该要求审计员执行什么SOC级别和类型？

Brad wants to engage third-party auditors to assess a vendor that his company will be signing a contract with. If Brad wants to assess the vendor’s security policies and controls as well as the effectiveness of those controls as implemented over time, what SOC level and type should he request the auditors perform?

A：SOC 1，类型2

A SOC 1, Type 2

B：SOC 2，类型1

A SOC 2, Type 1

C：SOC 1，类型1

A SOC 1, Type 1

D：SOC 2，类型2

A SOC 2, Type 2

答案:Brad希望评估供应商的安全策略、控制以及这些控制随着时间的推移的有效性。在这种情况下，最合适的审计报告是SOC 2，类型2。

- \*\*SOC 2\*\* 报告专门针对与安全性、可用性、处理完整性、机密性和隐私相关的控制。这与Brad的需求直接相关，因为他关注的是供应商的安全策略和控制。

- \*\*类型2\*\* 报告不仅描述控制的设计，还评估这些控制在特定时间段内的运行有效性。这符合Brad希望评估控制随时间推移的有效性的需求。

因此，正确答案是：

\*\*D：SOC 2，类型2\*\*

A SOC 2, Type 2

-------------------

题目38：Bell-LaPadula是什么类型的访问控制模型例子？

Bell-LaPadula is an example of what type of access control model?

A：DAC

DAC

B：RBAC

RBAC

C：MAC

MAC

D：ABAC

ABAC

答案:Bell-LaPadula 是一种强制访问控制（Mandatory Access Control, MAC）模型的例子。因此，正确答案是：

C：MAC

Bell-LaPadula 模型主要用于军事和安全领域，它通过定义安全级别和访问规则来确保信息的机密性。该模型的核心原则包括“简单安全属性”（Simple Security Property）和“星属性”（Star Property），分别用于防止低安全级别的用户读取高安全级别的信息，以及防止高安全级别的用户写入低安全级别的信息。

-------------------

题目39：Martha 是一所学院的信息安全官，负责保护学生记录的隐私。什么法律适用于她的情况？

Martha is the information security officer for a small college and is responsible for safeguarding the privacy of student records. What law most directly applies to her situation?

A：HIPAA

HIPAA

B：HITECH

HITECH

C：COPPA

COPPA

D：FERPA

FERPA

答案:题目39的正确答案是：

D：FERPA

解释：

FERPA（Family Educational Rights and Privacy Act，家庭教育权利和隐私法案）是美国的一项联邦法律，旨在保护学生教育记录的隐私。Martha作为学院的信息安全官，负责保护学生记录的隐私，因此FERPA是直接适用于她情况的法律。

其他选项的解释：

- HIPAA（Health Insurance Portability and Accountability Act，健康保险可携性和责任法案）主要适用于医疗信息的隐私保护。

- HITECH（Health Information Technology for Economic and Clinical Health Act，经济和临床健康信息技术法案）是对HIPAA的补充，主要涉及电子健康记录的安全和隐私。

- COPPA（Children's Online Privacy Protection Act，儿童在线隐私保护法案）主要适用于保护13岁以下儿童的在线隐私。

-------------------

题目40：什么美国联邦法律规定了受保护健康信息的安全？

What U.S. federal law mandates the security of protected health information?

A：FERPA

FERPA

B：SAFE Act

SAFE Act

C：GLBA

GLBA

D：HIPAA

HIPAA

答案:正确答案是 D：HIPAA。

HIPAA（Health Insurance Portability and Accountability Act，健康保险可携性和责任法案）是美国联邦法律，它规定了受保护健康信息（PHI）的安全和隐私。HIPAA 的主要目的是保护患者的健康信息不被未经授权的访问和泄露，同时确保医疗信息的可携性和连续性。

其他选项的解释：

- A：FERPA（Family Educational Rights and Privacy Act，家庭教育权利和隐私法案）主要涉及教育记录的保护，而不是健康信息。

- B：SAFE Act（Secure and Fair Enforcement for Mortgage Licensing Act，抵押贷款许可的安全和公平执行法案）与抵押贷款行业相关，与健康信息无关。

- C：GLBA（Gramm-Leach-Bliley Act，格雷姆-里奇-布莱利法案）主要涉及金融机构的隐私保护，与健康信息无关。

-------------------

题目41：攻击者可以利用下列哪项技术进行TOC/TOU攻击？

Which one of the following techniques can an attacker use to exploit a TOC/TOU vulnerability?

A：文件锁定

File locking

B：异常处理

Exception handling

C：算法复杂度

Algorithmic complexity

D：并发控制

Concurrency control

答案:TOC/TOU（Time-of-Check to Time-of-Use）攻击是一种利用程序在检查资源状态和使用资源之间的时间差来进行攻击的技术。这种攻击通常发生在多线程或多进程环境中，攻击者通过改变资源的状态来利用这个时间差。

选项分析：

A. 文件锁定（File locking）：文件锁定是一种防止多个进程同时访问同一文件的机制。虽然文件锁定可以防止某些并发问题，但它并不能直接防止TOC/TOU攻击。

B. 异常处理（Exception handling）：异常处理是程序处理错误和异常情况的方式。异常处理本身并不能防止TOC/TOU攻击。

C. 算法复杂度（Algorithmic complexity）：算法复杂度是指算法执行所需的时间和空间资源。算法复杂度与TOC/TOU攻击无关。

D. 并发控制（Concurrency control）：并发控制是管理多个线程或进程同时访问共享资源的机制。TOC/TOU攻击正是利用并发控制中的漏洞，因此攻击者可以利用并发控制技术来进行TOC/TOU攻击。

因此，正确答案是：

D：并发控制

Concurrency control

-------------------

题目42：Susan正在配置她的网络设备以使用syslog。她应该设置什么，以确保她收到有关异常问题的通知，但不会收到正常的操作问题消息？

Susan is configuring her network devices to use syslog. What should she set to ensure that she is notified about issues but does not receive normal operational issue messages?

A：设施代码

The facility code

B：日志优先级

The log priority

C：安全级别

The security level

D：严重程度

The severity level

答案:正确答案是 D：严重程度 (The severity level)。

在配置syslog时，Susan需要设置日志的严重程度（severity level）来过滤日志消息。syslog定义了多个严重程度级别，从0（紧急）到7（调试）。通过设置适当的严重程度级别，Susan可以确保只接收那些高于或等于指定严重程度级别的日志消息，从而避免接收正常的操作问题消息。

例如，如果Susan将严重程度设置为4（警告），她将只接收严重程度为4及以上的日志消息（如警告、错误、紧急等），而不会接收严重程度为5（通知）或6（信息）等较低级别的日志消息。

其他选项的解释：

- A：设施代码 (The facility code) 用于标识日志消息的来源（如内核、邮件系统等），但不用于过滤日志消息的严重程度。

- B：日志优先级 (The log priority) 是设施代码和严重程度的组合，但它本身不直接用于过滤日志消息。

- C：安全级别 (The security level) 不是syslog中的标准术语，通常不用于配置日志过滤。

-------------------

题目43：哪种RAID级别也被称为磁盘镜像？

What RAID level is also known as disk mirroring?

A：RAID 0

RAID 0

B：RAID 1

RAID 1

C：RAID 3

RAID 3

D：RAID 5

RAID 5

答案:正确答案是 B：RAID 1。

RAID 1 也被称为磁盘镜像（disk mirroring）。在 RAID 1 中，数据会被同时写入两个或多个磁盘，从而实现数据的冗余。如果一个磁盘发生故障，另一个磁盘仍然可以继续工作，确保数据的安全性和可用性。

-------------------

题目44：Isaac最近从他的交换机供应商那里购买了一台48端口交换机。交换机供应商已告知Isaac购买的交换机型号将于明年到期。这告诉Isaac关于这些设备的什么信息？

Isaac recently purchased a 48 port switch from his switch vendor. The switch vendor has announced that the model of switch that Isaac purchased will reach end of life next year. What does this tell Isaac about the devices?

A：这些设备明年将停止销售

The devices will stop being sold next year.

B：这些设备明年将停止运行

The devices will stop functioning next year.

C：明年将不再支持这些设备

The devices will no longer be supported next year.

D：这些设备将获得至少三年以上的支持

The devices will be supported for a minimum of three more years.

答案:正确答案是：C：明年将不再支持这些设备

The devices will no longer be supported next year.

解析：当供应商宣布某个设备型号将“到期”（end of life）时，这通常意味着该型号将不再生产，并且供应商将停止提供支持服务，如软件更新、安全补丁和技术支持。这并不意味着设备会立即停止工作，但用户可能面临更高的风险，因为不再有官方的支持来修复潜在的漏洞或问题。因此，选项C是正确的，它表明这些设备明年将不再得到支持。选项A、B和D都不准确，因为“到期”并不直接意味着设备会停止销售、停止运行或获得至少三年的支持。

-------------------

题目45：调查、访谈和审计都是衡量组织安全状况哪些重要组成部分的方法？

Surveys, interviews, and audits are all examples of ways to measure what important part of an organization’s security posture?

A：代码质量

Code quality

B：服务漏洞

Service vulnerabilities

C：安全意识

Awareness

D：攻击面

Attack surface

答案:题目45的正确答案是：

C：安全意识

Awareness

调查、访谈和审计都是用来衡量组织安全状况中安全意识的重要方法。这些方法可以帮助评估员工对安全政策的理解、遵守情况以及组织整体的安全文化。

-------------------

题目46：Tom是互联网服务提供商的总顾问，最近他收到了针对该公司的诉讼通知，因为有客户通过提供商的电路来非法传输受版权保护的内容。这种情况下，什么法律能保护Tom的公司？

Tom is the general counsel for an internet service provider, and he recently received notice of a lawsuit against the firm because of copyrighted content illegally transmitted over the provider’s circuits by a customer. What law protects Tom’s company in this case?

A：计算机欺诈和滥用法

Computer Fraud and Abuse Act

B：数字千年版权法

Digital Millennium Copyright Act

C：窃听法

Wiretap Act

D：版权法

Copyright Code

答案:在这种情况下，保护Tom的公司的法律是 \*\*B：数字千年版权法（Digital Millennium Copyright Act, DMCA）\*\*。

### 解释：

- \*\*数字千年版权法（DMCA）\*\* 提供了对互联网服务提供商（ISP）的“安全港”保护。根据DMCA，如果ISP在不知情的情况下传输了受版权保护的内容，并且一旦收到版权持有人的通知后迅速采取行动删除或阻止访问该内容，ISP可以免于承担版权侵权的责任。

- \*\*计算机欺诈和滥用法（A）\*\* 主要针对未经授权访问计算机系统的行为，与此案无关。

- \*\*窃听法（C）\*\* 涉及未经授权的电子通信拦截，与此案无关。

- \*\*版权法（D）\*\* 是保护版权持有人的法律，而不是保护ISP免于责任的法律。

因此，\*\*B：数字千年版权法\*\* 是正确答案。

-------------------

题目47：什么类型的身份验证者方法基于时间或算法的系统生成动态密码的类型2身份验证因素？

A Type 2 authentication factor that generates dynamic passwords based on a time-or algorithm-based system is what type of authenticator?

A：PII

A PII

B：智能卡

A smart card

C：令牌

A token

D：CAC

ACAC

答案:题目47的正确答案是：

C：令牌

A token

解释：基于时间或算法的系统生成动态密码的类型2身份验证因素通常是通过硬件或软件令牌实现的。这些令牌生成一次性密码（OTP），这些密码在一定时间后或基于特定算法变化，以增加安全性。因此，令牌是符合题目描述的身份验证者方法。

-------------------

题目48：Fred在新雇主的公司中负责商业秘密和机密内部数据。如果他选择离开该雇主并在该雇主竞争对手的公司工作，Fred原雇主应该使用什么法律工具来保护他们的数据？

Fred’s new employer has hired him for a position with access to their trade secrets and confidential internal data. What legal tool should they use to help protect their data if he chooses to leave to work at a competitor?

A：停止损失订单

A stop-loss order

B：NDA

An NDA

C：AUP

An AUP

D：加密

Encryption

答案:正确答案是 B：NDA（Non-Disclosure Agreement，保密协议）。

NDA 是一种法律工具，用于保护公司的商业秘密和机密信息。通过签署 NDA，Fred 同意在离开公司后不向竞争对手或任何第三方泄露或使用这些机密信息。这为原雇主提供了一种法律手段，可以在 Fred 违反协议时采取法律行动。

其他选项的解释：

- A：停止损失订单（Stop-loss order）通常用于金融市场，与保护商业秘密无关。

- C：AUP（Acceptable Use Policy，可接受使用政策）通常用于规范员工对公司资源的使用，但不直接涉及离职后的保密问题。

- D：加密（Encryption）是一种技术手段，用于保护数据的安全，但它不是法律工具，无法在法律上约束员工的行为。

-------------------

题目49：Mark的公司卷入了一起民事案件。他可能需要达到什么样的证据标准？

Mark’s company is involved in a civil case. What evidentiary standard is he likely to need to meet?

A：真实证据标准

The real evidence standard

B：排除合理怀疑

Beyond a reasonable doubt

C：优势证据

Preponderance of evidence

D：书面标准

The documentary evidence standard

答案:在民事案件中，通常适用的证据标准是“优势证据”（Preponderance of evidence）。这意味着原告需要证明其主张的事实比被告的反驳更有可能是真实的。换句话说，原告需要证明其主张的真实性超过50%的可能性。

因此，正确答案是：

C：优势证据

Preponderance of evidence

-------------------

题目50：当使用具有8位二进制加密密钥的加密算法时，存在多少种可能的密钥？

How many possible keys exist when using a cryptographic algorithm that has an 8-bit binary encryption key?

A：16

16

B：128

128

C：256

256

D：512

512

答案:当使用具有8位二进制加密密钥的加密算法时，每一位可以是0或1，因此总共有 \(2^8\) 种可能的组合。计算如下：

\[

2^8 = 256

\]

因此，存在256种可能的密钥。

正确答案是：C：256

-------------------

题目51：当你根据IT系统的特定需求应用安全控制，正在执行什么活动？

What activity is being performed when you apply security controls based on the specific needs of the IT system that they will be applied to?

A：标准化

Standardizing

B：基线

Baselining

C：范围

Scoping

D：修订

Editing

答案:正确答案是 \*\*C：范围 (Scoping)\*\*。

\*\*解释：\*\*

当根据IT系统的特定需求应用安全控制时，你正在执行的活动是“范围界定”（Scoping）。范围界定是指根据系统的具体需求、环境和风险，选择和调整安全控制措施，以确保这些措施适用于特定的系统或环境。这一过程涉及确定哪些安全控制是必要的，并根据系统的特定需求进行调整。

其他选项的解释：

- \*\*A：标准化 (Standardizing)\*\*：指的是制定和实施统一的标准或规范，通常不涉及根据特定需求进行调整。

- \*\*B：基线 (Baselining)\*\*：指的是建立一个基准或最低标准，通常用于比较或评估系统的安全状态。

- \*\*D：修订 (Editing)\*\*：指的是对现有内容进行修改或更新，与根据特定需求应用安全控制的活动不完全相关。

因此，最符合题意的选项是 \*\*C：范围 (Scoping)\*\*。

-------------------

题目52：在电子发现过程的哪个阶段，组织对所收集的信息进行粗略剪切，以丢弃不相关的信息？

During what phase of the electronic discovery process does an organization perform a rough cut of the information gathered to discard irrelevant information?

A：保存

Preservation

B：鉴定

Identification

C：收集

Collection

D：处理

Processing

答案:在电子发现过程的哪个阶段，组织对所收集的信息进行粗略剪切，以丢弃不相关的信息？

正确答案是：D：处理 (Processing)

解释：在电子发现过程中，处理阶段（Processing）是指对收集到的数据进行初步整理和筛选，以去除不相关或冗余的信息。这一步骤有助于减少数据量，使得后续的审查和分析更加高效。

-------------------

题目53：Ben的工作是确保数据标有适当的敏感性标签。由于Ben在美国政府工作，他必须将Unclassified、Confidential、Secret和Top Secret这四个标签应用于系统和介质。如果Ben被要求标记一个处理秘密、机密和未分类信息的系统，他应该如何标记？

Ben’s job is to ensure that data is labeled with the appropriate sensitivity label. Since Ben works for the U.S. government, he has to apply the labels Unclassified, Confidential, Secret, and Top Secret to systems and media. If Ben is asked to label a system that handles Secret, Confidential, and Unclassified information, how should he label it?

A：混合分类

Mixed classification

B：机密

Confidential

C：最高机密

Top Secret

D：秘密

Secret

答案:在处理涉及不同敏感级别的信息时，通常需要根据最高级别的敏感信息来标记整个系统或介质。这是因为系统的安全性需要能够保护最高级别的信息，即使系统中也包含较低级别的信息。

在Ben的情况下，系统处理的信息包括秘密（Secret）、机密（Confidential）和未分类（Unclassified）信息。在这三个级别中，秘密（Secret）是最高级别的敏感信息。因此，为了确保系统的安全性，Ben应该将整个系统标记为秘密（Secret）。

所以，正确答案是：

D：秘密

Secret

-------------------

题目54：Susan发现，他们组织使用智能卡的门锁经常不管用，因为工作人员经常把门开着。她在门上贴了一个提醒标志，提醒工作人员一旦把门打开，可能会不安全。另外，她还增加了警报，如果门打开时间超过五分钟，会发出警报声。她实施了什么类型的控制？

Susan has discovered that the smart card-based locks used to keep the facility she works at secure are not effective because staff members are propping the doors open. She places signs on the doors reminding staff that leaving the door open creates a security issue, and she adds alarms that will sound if the doors are left open for more than five minutes. What type of controls has she put into place?

A：物理

Physical

B：行政

Administrative

C：补偿

Compensating

D：恢复

Recovery

答案:Susan在门上贴了提醒标志，并增加了警报系统，这些措施旨在通过改变员工的行为和增加技术手段来增强安全性。这些措施属于不同类型的控制：

1. \*\*提醒标志\*\*：这是一种\*\*行政控制\*\*（Administrative Control），因为它通过政策和程序来影响员工的行为，提醒他们注意安全事项。

2. \*\*警报系统\*\*：这是一种\*\*物理控制\*\*（Physical Control），因为它通过技术手段（警报器）来监控和响应物理环境的变化（门被打开超过五分钟）。

因此，Susan实施的措施包括\*\*行政控制\*\*和\*\*物理控制\*\*。

正确答案是：

A：物理

B：行政

-------------------

题目55：Ben关注他的系统并对系统进行密码破解攻击。他希望实施安全控制，防止攻击者获得这些散列值来破解系统。哪两个控制将最好地实现这一目标？

Ben is concerned about password cracking attacks against his system. He would like to implement controls that prevent an attacker who has obtained those hashes from easily cracking them. What two controls would best meet this objective?

A：更长的密码以及更长的盐

Longer passwords and salting

B：线上加密，并用SHA1替代MD5

Over-the-wire encryption and use of SHA1 instead of MD5

C：使用盐和MD5

Salting and use of MD5

D：使用shadow密码和盐

Using shadow passwords and salting

答案:题目55的正确答案是A：更长的密码以及更长的盐（Longer passwords and salting）。

解析：

- \*\*更长的密码\*\*：增加密码的长度可以显著提高密码的复杂性，使得暴力破解或字典攻击变得更加困难。

- \*\*更长的盐\*\*：盐（salt）是添加到密码中的随机数据，用于增加散列值的唯一性。即使两个用户使用相同的密码，由于盐的不同，他们的散列值也会不同。更长的盐可以进一步提高安全性，使得攻击者更难使用预计算的散列表（如彩虹表）进行攻击。

其他选项的解析：

- \*\*B：线上加密，并用SHA1替代MD5\*\*：虽然线上加密可以保护数据传输过程中的安全，但SHA1已经被认为是不安全的散列算法，不推荐使用。

- \*\*C：使用盐和MD5\*\*：MD5已经被证明是不安全的散列算法，容易受到碰撞攻击，因此不推荐使用。

- \*\*D：使用shadow密码和盐\*\*：Shadow密码是一种保护密码文件的方法，但它本身并不直接增加密码的复杂性或盐的长度，因此不如选项A有效。

因此，选项A是最佳选择。

-------------------

题目56：哪个小组最适合评估组织的行政控制并向第三方提供可靠的报告？

Which group is best suited to evaluate an organization’s administrative controls and provide credible reports to a third party?

A：内部审计师

Internal auditors

B：渗透测试者

Penetration testers

C：外聘审计员

External auditors

D：设计、实施和监控控制的员工

Employees who design, implement, and monitor the controls

答案:正确答案是：C 外聘审计员 (External auditors)

解析：

外聘审计员最适合评估组织的行政控制并向第三方提供可靠的报告。外聘审计员是独立的第三方，他们不受组织内部的影响，能够提供客观、公正的评估和报告。他们的主要职责之一就是评估组织的内部控制体系，包括行政控制，并向外部利益相关者（如股东、监管机构等）提供可信的报告。

其他选项的解析：

- A 内部审计师 (Internal auditors)：虽然内部审计师也评估组织的内部控制，但他们属于组织内部的一部分，可能缺乏外聘审计员的独立性。

- B 渗透测试者 (Penetration testers)：渗透测试者主要关注的是信息系统的安全性，而不是广泛的行政控制。

- D 设计、实施和监控控制的员工 (Employees who design, implement, and monitor the controls)：这些员工虽然参与了控制的设计和实施，但他们缺乏独立性和客观性，不适合向第三方提供报告。

因此，C 选项是最合适的。

-------------------

题目57：Lucca的经理不想为其组织的Web应用程序栈采用开源软件包。在考虑开源软件包时，最重要的软件安全优势是什么？

Lucca’s manager does not want to adopt an open source software package for their organization’s web application stack. What software security advantage is the most important when considering open source software packages?

A：代码未编译的事实

The fact that the code is not compiled

B：代码是免费的事实

The fact the code is free

C：检查代码的能力

The ability to inspect the code

D：更改代码的能力

The ability to change the code

答案:在考虑开源软件包时，最重要的软件安全优势是 \*\*C：检查代码的能力\*\*（The ability to inspect the code）。

### 解析：

- \*\*A：代码未编译的事实\*\*

开源软件的代码通常是未编译的，但这并不是其安全优势的核心。未编译的代码只是意味着你可以查看和修改源代码，但这本身并不直接提供安全优势。

- \*\*B：代码是免费的事实\*\*

虽然开源软件通常是免费的，但这与安全性没有直接关系。免费并不意味着软件更安全或更不安全。

- \*\*C：检查代码的能力\*\*

这是开源软件最重要的安全优势之一。开源代码可以被任何人审查，这意味着安全专家和开发者可以检查代码中是否存在漏洞或恶意代码。这种透明性有助于提高软件的安全性，因为问题可以被及时发现和修复。

- \*\*D：更改代码的能力\*\*

虽然开源软件允许用户修改代码，但这更多是一个灵活性和定制化的优势，而不是直接的安全优势。修改代码的能力可以帮助解决特定的安全问题，但这依赖于用户的技术能力和对代码的理解。

因此，\*\*C：检查代码的能力\*\* 是最重要的软件安全优势。

-------------------

题目58：作为雇用新员工过程的一部分，Kathleen的身份管理团队创建了一个新的用户客体，并确保用户客体在需要它的目录和系统中可用。这个过程叫什么？

As part of hiring a new employee, Kathleen&rsquo;s identity management team creates a new user object and ensures that the user object is available in the directories and systems where it is needed. What is this process called?

A：注册

Registration

B：配置

Provisioning

C：人口

Population

D：身份验证加载

Authenticator loading

答案:正确答案是 B：配置 (Provisioning)。

解释：在身份管理中，配置（Provisioning）是指创建和管理用户账户及其相关权限的过程。这包括在需要的目录和系统中创建用户对象，并确保用户能够访问所需的资源。这个过程通常在新员工入职时进行，以确保他们能够顺利访问公司系统和资源。

其他选项的解释：

- A：注册（Registration）通常是指用户自己创建账户的过程，而不是由管理员或团队创建。

- C：人口（Population）与身份管理无关，通常用于描述数据的填充或统计。

- D：身份验证加载（Authenticator loading）与用户账户的创建和管理无关，通常涉及身份验证机制或设备的加载。

-------------------

题目59：当变更最终确定时，发生了软件变更管理过程的哪个阶段？

What phase of the change management process for software occurs when changes are finalized?

A：请求控制

Request control

B：配置控制

Configuration control

C：发布控制

Release control

D：变更控制

Change control

答案:当变更最终确定时，软件变更管理过程的阶段是 \*\*D：变更控制\*\*（Change control）。

变更控制是变更管理过程中的一个关键阶段，它涉及对变更请求的评估、批准、实施和验证。当变更最终确定时，通常意味着变更已经通过了评估和批准，并且已经准备好实施。这个阶段确保变更在实施前经过了适当的审查和控制，以减少对系统的负面影响。

其他选项的解释：

- \*\*A：请求控制\*\*（Request control）：这是变更管理过程的初始阶段，涉及接收和记录变更请求。

- \*\*B：配置控制\*\*（Configuration control）：这是与配置管理相关的活动，确保系统的配置项在变更过程中得到适当的管理和控制。

- \*\*C：发布控制\*\*（Release control）：这是与软件发布相关的活动，确保软件版本在发布前经过适当的测试和验证。

因此，正确答案是 \*\*D：变更控制\*\*（Change control）。

-------------------

题目60：Alice正在设计能供六个用户使用的密码系统，并希望使用对称加密算法。她想要任何两个用户能够彼此通信而不必担心第三用户的窃听。她需要生成多少个对称加密密钥？

Alice is designing a cryptosystem for use by six users and would like to use a symmetric encryption algorithm. She wants any two users to be able to communicate with each other without worrying about eavesdropping by a third user. How many symmetric encryption keys will she need to generate?

A：6

6

B：12

12

C：15

15

D：30

30

答案:要解决这个问题，我们需要计算在六个用户之间，每两个用户之间都需要一个独立的对称加密密钥，以确保他们的通信不会被其他用户窃听。

### 步骤解析：

1. \*\*理解需求\*\*：

- 有6个用户，每个用户需要与其他5个用户通信。

- 每对用户之间需要一个独立的对称加密密钥。

2. \*\*计算组合数\*\*：

- 我们需要计算从6个用户中选取2个用户的组合数，因为每对用户需要一个密钥。

- 组合数的计算公式是：

\[

C(n, k) = \frac{n!}{k!(n - k)!}

\]

其中，\( n = 6 \)（用户总数），\( k = 2 \)（每对用户）。

3. \*\*代入计算\*\*：

\[

C(6, 2) = \frac{6!}{2!(6 - 2)!} = \frac{6 \times 5}{2 \times 1} = 15

\]

4. \*\*结论\*\*：

- Alice需要生成15个对称加密密钥，以确保每对用户之间的通信安全。

### 最终答案：

C：15

-------------------

题目61：以下哪种知识产权保护机制在美国的持续时间最短？

Which one of the following intellectual property protection mechanisms has the shortest duration in the United States?

A：版权

Copyright

B：专利

Patent

C：商标

Trademark

D：商业秘密

Trade secret

答案:在美国的知识产权保护机制中，持续时间最短的是 \*\*B：专利（Patent）\*\*。

- \*\*版权（Copyright）\*\*：通常持续作者的一生加上70年。

- \*\*专利（Patent）\*\*：通常持续20年（从申请日起计算）。

- \*\*商标（Trademark）\*\*：可以无限期续展，只要商标仍在商业中使用。

- \*\*商业秘密（Trade secret）\*\*：只要信息保持秘密状态，保护可以无限期持续。

因此，专利的保护期限最短。

-------------------

题目62：Gordon正在为某制造公司的IT 运营部门制定业务连续性计划。该公司位于北达科他州，他们正在评估地震风险。他们选择采取风险接受策略。以下哪项操作与该策略一致？

Gordon is developing a business continuity plan for a manufacturing company’s IT operations. The company is located in North Dakota and currently evaluating the risk of earthquake. They choose to pursue a risk acceptance strategy. Which one of the following actions is consistent with that strategy?

A：购买地震保险

Purchasing earthquake insurance

B：将数据中心迁移到更安全的区域

Relocating the data center to a safer area

C：记录决策过程

Documenting the decision-making process

D：重新设计设施以承受地震的冲击

Reengineering the facility to withstand the shock of an earthquake

答案:在制定业务连续性计划时，选择风险接受策略意味着组织决定接受潜在风险，而不是采取避免、转移或减轻风险的策略。风险接受通常基于对风险的评估，认为风险发生的可能性低或影响较小，或者采取其他措施的成本过高。

让我们逐一分析每个选项：

A. 购买地震保险 - 这是风险转移策略的一部分，通过购买保险将风险转移给保险公司。这与风险接受策略不一致。

B. 将数据中心迁移到更安全的区域 - 这是风险避免策略的一部分，通过改变地理位置来避免风险。这与风险接受策略不一致。

C. 记录决策过程 - 这是风险接受策略的一部分，组织决定接受风险并记录这一决策过程，以便在风险发生时能够追溯和审查决策。这与风险接受策略一致。

D. 重新设计设施以承受地震的冲击 - 这是风险减轻策略的一部分，通过改进设施来减少地震带来的影响。这与风险接受策略不一致。

因此，最符合风险接受策略的选项是：

\*\*C：记录决策过程\*\*

\*\*Documenting the decision-making process\*\*

-------------------

题目63：Carol 希望实施一项控制措施，以保护她的组织免受数据中心瞬间断电的影响。哪种控制最能满足她的需要？

Carol would like to implement a control that protects her organization from the momentary loss of power to the data center. Which control is most appropriate for her needs?

A：冗余服务器

Redundant servers

B：RAID

RAID

C：UPS

UPS

D：发电机

Generator

答案:题目63的正确答案是：

C：UPS (不间断电源)

UPS (Uninterruptible Power Supply) 是一种能够在电力中断时立即提供备用电源的设备，以保护数据中心免受瞬间断电的影响。UPS可以在电力中断时提供短时间的电力支持，确保关键系统能够继续运行，直到备用发电机启动或系统能够安全关闭。

其他选项的解释：

- A：冗余服务器 (Redundant servers) 主要用于提高系统的可用性和容错能力，而不是直接解决电力中断问题。

- B：RAID (Redundant Array of Independent Disks) 是一种数据存储技术，用于提高数据存储的可靠性和性能，与电力中断无关。

- D：发电机 (Generator) 可以提供长时间的电力支持，但在电力中断的瞬间，发电机需要时间启动，因此无法立即提供电力支持。

因此，UPS是最适合保护数据中心免受瞬间断电影响的控制措施。

-------------------

题目64：Ben在他的组织中重用密码时遇到了问题(组织要求他每30天更改一次密码)。使用哪种类型的密码设置来帮助防止此问题的发生？

Ben has encountered problems with users in his organization reusing passwords, despite a requirement that they change passwords every 30 days. What type of password setting should Ben employ to help prevent this issue?

A：较长的最短期限

Longer minimum age

B：增加密码复杂程度

Increased password complexity

C：实施密码历史记录

Implement password history

D：实施密码长度要求

Implement password length requirements

答案:正确答案是 \*\*C：实施密码历史记录\*\* (Implement password history)。

\*\*解析：\*\*

- \*\*A：较长的最短期限\*\* (Longer minimum age)：这个选项指的是密码在更改之前必须使用的最短时间。它并不能防止用户重复使用旧密码。

- \*\*B：增加密码复杂程度\*\* (Increased password complexity)：虽然增加密码复杂性可以提高密码的安全性，但它并不能防止用户重复使用旧密码。

- \*\*C：实施密码历史记录\*\* (Implement password history)：通过实施密码历史记录，系统可以记住用户过去使用过的密码，并防止用户在一定时间内重复使用这些密码。这可以有效防止用户重复使用旧密码。

- \*\*D：实施密码长度要求\*\* (Implement password length requirements)：虽然增加密码长度可以提高密码的安全性，但它并不能防止用户重复使用旧密码。

因此，\*\*C：实施密码历史记录\*\* 是最合适的解决方案，可以有效防止用户重复使用旧密码。

-------------------

题目65：Chris正为其组织进行风险评估，并确定单次洪水可能对其设施造成的损害程度。请问这是什么指标？

Chris is conducting a risk assessment for his organization and has determined the amount of damage that a single flood could be expected to cause to his facilities. What metric has Chris identified?

A：ALE

ALE

B：SLE

SLE

C：ARO

ARO

D：AV

AV

答案:Chris正在进行的风险评估中，他确定了一次洪水可能对其设施造成的损害程度。这个指标被称为单次损失预期（Single Loss Expectancy, SLE）。

SLE是指在一次特定事件中，预计会造成的经济损失。它是通过将资产价值（Asset Value, AV）与暴露因子（Exposure Factor, EF）相乘来计算的。公式如下：

\[ SLE = AV \times EF \]

在这个例子中，Chris确定的是单次洪水可能造成的损害程度，因此他计算的是SLE。

所以，正确答案是：

B：SLE

-------------------

题目66：在硬盘驱动器退出使用并作为剩余资产出售之前，从电脑中取出硬盘驱动器是什么类型的操作？

The removal of a hard drive from a PC before it is retired and sold as surplus is an example of what type of action?

A：清洗

Purging

B：净化

Sanitization

C：消磁

Degaussing

D：销毁

Destruction

答案:题目66的正确答案是：

B：净化

Sanitization

解释：在硬盘驱动器退出使用并作为剩余资产出售之前，从电脑中取出硬盘驱动器并进行数据清除的操作被称为“净化”（Sanitization）。净化的目的是确保硬盘上的数据无法被恢复，从而保护敏感信息不被泄露。这一过程可能包括数据擦除、覆盖或物理破坏等方法，以确保数据彻底不可恢复。

-------------------

题目67：在事件响应过程的哪个阶段，组织将考虑是否需要将此事件通知执法官员或其他监管机构？

During which phase of the incident response process would an organization determine whether it is required to notify law enforcement officials or other regulators of the incident?

A：检测

Detection

B：恢复

Recovery

C：补救

Remediation

D：报告

Reporting

答案:在事件响应过程中，组织将在“报告”阶段考虑是否需要将此事件通知执法官员或其他监管机构。因此，正确答案是：

D：报告

Reporting

在这个阶段，组织会评估事件的性质和严重程度，并根据法律、法规或合同要求决定是否需要向外部机构报告。

-------------------

题目68：每90天，Charles所在银行部门的员工就会转化任务，这是组织正常流程的一部分为了确保个人不会滥用他们的特权。他的组织从事着什么安全实践？

Every 90 days, the staff in Charles’s department at his bank switch tasks as part of the organization’s normal processes to ensure that an individual does not exploit their privileges. What security practice is his organization engaging in?

A：双人控制

Dual control

B：工作轮换

Job rotation

C：交叉培训

Cross-training

D：离职

Offboarding

答案:正确答案是 B：工作轮换（Job rotation）。

工作轮换是一种安全实践，通过定期将员工从一个岗位或任务转移到另一个岗位或任务，以减少滥用权限或内部欺诈的风险。这种做法有助于确保没有一个人长期掌握敏感信息或权限，从而降低潜在的安全威胁。在Charles所在的银行部门，每90天进行一次任务转换，正是工作轮换的体现。

-------------------

题目69：Michelle负责其组织的移动设备管理工作，并且需要针对丢失和被盗的设备进行处理。以下哪项建议可以为她的组织提供最大的保证，即如果设备被盗了，但数据不会丢失？

Michelle is in charge of her organization’s mobile device management efforts and handles lost and stolen devices. Which of the following recommendations will provide the most assurance to her organization that data will not be lost if a device is stolen?

A：强制性密码和应用程序管理

Mandatory passcodes and application management

B：完整设备加密和强制密码

Full device encryption and mandatory passcodes

C：远程擦除和GPS跟踪

Remote wipe and GPS tracking

D：启用GPS跟踪和完整设备加密

Enabling GPS tracking and full device encryption

答案:题目69的正确答案是：

\*\*B：完整设备加密和强制密码\*\*

\*\*Full device encryption and mandatory passcodes\*\*

### 解析：

- \*\*A：强制性密码和应用程序管理\*\*

虽然强制性密码和应用程序管理可以提高设备的安全性，但它们并不能完全防止数据在设备被盗时被访问或泄露。

- \*\*B：完整设备加密和强制密码\*\*

完整设备加密可以确保即使设备被盗，数据也无法被未经授权的人访问。强制密码则增加了设备访问的难度。这两者结合提供了最高的数据保护级别。

- \*\*C：远程擦除和GPS跟踪\*\*

远程擦除可以在设备被盗后清除数据，但这需要设备连接到网络。GPS跟踪可以帮助定位设备，但它本身并不能防止数据泄露。

- \*\*D：启用GPS跟踪和完整设备加密\*\*

GPS跟踪可以帮助定位设备，但它并不能直接保护数据。完整设备加密是保护数据的关键措施，但单独使用GPS跟踪并不能提供足够的数据保护。

因此，\*\*B选项\*\*（完整设备加密和强制密码）是最佳选择，因为它直接针对数据保护，确保即使设备被盗，数据也不会丢失。

-------------------

题目70：Susan的SMTP服务器在接受和中继电子邮件之前不验证发件人。这个安全配置问题是什么？

Susan’s SMTP server does not authenticate senders before accepting and relaying email. What is this security configuration issue known as?

A：电子邮件网关

An email gateway

B：SMTP中继

An SMTP relay

C：符合X.400标准的网关

An X.400-compliant gateway

D：开放中继器

An open relay

答案:正确答案是：D：开放中继器 (An open relay)

解释：开放中继器是指SMTP服务器在没有验证发件人身份的情况下，接受并转发来自任何发件人的电子邮件。这种配置问题可能导致服务器被滥用来发送垃圾邮件或恶意邮件，因为任何人都可以利用该服务器来发送邮件，而不需要提供任何身份验证。因此，开放中继器是一个严重的安全问题，应该被避免。

-------------------

题目71-1：根据以下场景，回答3个问题：

Jack工作的大型企业多年来一直采用非集中式日志系统。最近该企业开始实施集中日志系统，但在审查日志时他们发现了一起数据泄露事件，且有可能涉及了一名恶意的内部人员。

For questions, please refer to the following scenario:

The large business that Jack works for has been using noncentralized logging for years. They have recently started to implement centralized logging, however, and as they reviewed logs, they discovered a breach that appeared to have involved a malicious insider.

当发现违规行为并审查日志时，发现攻击者已清除了他们所危及的系统上的日志。如何预防未来？

When the breach was discovered and the logs were reviewed, it was discovered that the attacker had purged the logs on the system that they compromised. How can this be prevented in the future?

A：加密本地日志

Encrypt local logs.

B：需要管理更改日志的访问

Require administrative access to change logs.

C：启用日志轮换

Enable log rotation.

D：将日志发送到堡垒主机

Send logs to a bastion host.

答案:在发现攻击者清除了被攻击系统上的日志后，企业需要采取措施来防止类似事件再次发生。以下是每个选项的分析：

A：加密本地日志

加密本地日志可以防止未经授权的访问和篡改，但它并不能防止攻击者删除日志。因此，加密本地日志虽然有助于保护日志的机密性，但并不能完全解决日志被删除的问题。

B：需要管理更改日志的访问

通过限制对日志的更改权限，只有管理员才能修改或删除日志，这可以有效防止恶意内部人员或攻击者删除日志。这是一个有效的预防措施。

C：启用日志轮换

日志轮换是指定期将日志文件归档并创建新的日志文件。虽然这有助于管理日志文件的大小，但它并不能防止攻击者删除日志。因此，日志轮换并不能解决日志被删除的问题。

D：将日志发送到堡垒主机

将日志实时发送到一个安全的堡垒主机（即集中式日志服务器）可以确保即使本地日志被删除，攻击者也无法删除已经发送到堡垒主机的日志。这是一种非常有效的预防措施，因为它确保了日志的完整性和不可篡改性。

\*\*最佳答案：D\*\*

将日志发送到堡垒主机是最有效的预防措施，因为它确保了日志的完整性和不可篡改性，即使本地日志被删除，攻击者也无法删除已经发送到堡垒主机的日志。

-------------------

题目71-1：根据以下场景，回答3个问题：

Jack工作的大型企业多年来一直采用非集中式日志系统。最近该企业开始实施集中日志系统，但在审查日志时他们发现了一起数据泄露事件，且有可能涉及了一名恶意的内部人员。

For questions, please refer to the following scenario:

The large business that Jack works for has been using noncentralized logging for years. They have recently started to implement centralized logging, however, and as they reviewed logs, they discovered a breach that appeared to have involved a malicious insider.

Jack如何使用其组织新的集中日志记录来检测此类问题？

How can Jack detect issues such as this using his organization’s new centralized logging?

A：部署和使用IDS

Deploy and use an IDS.

B：将日志发送到中央日志记录服务器

Send logs to a central logging server.

C：部署和使用SIEM

Deploy and use a SIEM.

D：使用syslog

Use syslog.

答案:在Jack的组织中，集中日志系统的实施是为了更好地监控和管理日志数据，以便及时发现和响应安全事件。针对检测内部恶意行为和数据泄露事件，最有效的方法是使用SIEM（安全信息和事件管理系统）。

\*\*C：部署和使用SIEM\*\*

SIEM系统能够集中收集、分析和关联来自不同来源的日志数据，帮助识别异常行为和潜在的安全威胁。通过SIEM，Jack可以设置规则和警报，以便在检测到可疑活动时立即采取行动。SIEM还可以提供详细的审计跟踪，帮助识别和调查内部人员的恶意行为。

其他选项的解释：

- \*\*A：部署和使用IDS\*\*

IDS（入侵检测系统）主要用于检测外部攻击，而不是内部人员的恶意行为。

- \*\*B：将日志发送到中央日志记录服务器\*\*

这只是集中日志系统的一部分，虽然有助于日志的集中管理，但缺乏分析和检测功能。

- \*\*D：使用syslog\*\*

Syslog是一种日志传输协议，用于将日志发送到中央服务器，但它本身不具备分析和检测功能。

因此，\*\*C：部署和使用SIEM\*\* 是最佳选择。

-------------------

题目71-1：根据以下场景，回答3个问题：

Jack工作的大型企业多年来一直采用非集中式日志系统。最近该企业开始实施集中日志系统，但在审查日志时他们发现了一起数据泄露事件，且有可能涉及了一名恶意的内部人员。

For questions, please refer to the following scenario:

The large business that Jack works for has been using noncentralized logging for years. They have recently started to implement centralized logging, however, and as they reviewed logs, they discovered a breach that appeared to have involved a malicious insider.

Jack如何最好地确保问责制对其环境中的系统采取行动的？

How can Jack best ensure accountability for actions taken on systems in his environment?

A：记录审查，并要求每个日志的数字签名

Log review and require digital signatures for each log.

B：需要对所有执行的操作进行身份验证，并集中捕获日志

Require authentication for all actions taken and capture logs centrally.

C：记录管理凭据的使用，并加密传输中的日志数据

Log the use of administrative credentials and encrypt log data in transit.

D：要求集中授权和捕获日志

Require authorization and capture logs centrally.

答案:为了确保问责制，Jack需要确保每个在系统中执行的操作都能够被追踪到具体的个人，并且这些操作的记录是安全且不可篡改的。让我们逐一分析每个选项：

A：记录审查，并要求每个日志的数字签名

- 记录审查是必要的，但要求每个日志都有数字签名可能会增加系统的复杂性和管理负担。数字签名主要用于确保数据的完整性和来源的真实性，但对于确保问责制来说，这并不是最直接的方法。

B：需要对所有执行的操作进行身份验证，并集中捕获日志

- 这个选项要求所有操作都需要身份验证，这意味着每个操作都可以追踪到具体的用户。集中捕获日志可以确保所有操作的记录都在一个地方，便于审查和分析。这是一个有效的方法来确保问责制。

C：记录管理凭据的使用，并加密传输中的日志数据

- 记录管理凭据的使用可以帮助追踪谁使用了哪些权限，但这并不直接确保所有操作的问责制。加密传输中的日志数据是保护数据安全的重要措施，但它并不直接解决问责制的问题。

D：要求集中授权和捕获日志

- 集中授权可以确保只有经过授权的用户才能执行特定操作，而集中捕获日志可以确保所有操作的记录都在一个地方。这与选项B类似，也是一个有效的方法来确保问责制。

综合以上分析，选项B和D都是确保问责制的有效方法。然而，选项B更加强调身份验证，这是确保每个操作都能追踪到具体用户的关键步骤。因此，选项B是最佳选择。

最终答案是：$\boxed{B}$。

-------------------

题目72：Ed的组织有5个IP地址由ISP分配给他们，但需要将超过100台计算机和网络设备连接到互联网。他可以使用什么技术通过有限的IP地址连接他的整个网络？

Ed’s organization has 5 IP addresses allocated to them by their ISP but needs to connect more than 100 computers and network devices to the internet. What technology can he use to connect his entire network via the limited set of IP addresses he can use?

A：IPsec

IPsec

B：PAT

PAT

C：SDN

SDN

D：IPX

IPX

答案:Ed的组织可以使用 \*\*PAT（Port Address Translation，端口地址转换）\*\* 技术来通过有限的IP地址连接整个网络。PAT 是 NAT（Network Address Translation，网络地址转换）的一种形式，允许多个设备共享一个公共IP地址，通过使用不同的端口号来区分不同的内部设备。

因此，正确答案是：

\*\*B：PAT\*\*

-------------------

题目73：以下预防措施可有助于防止哪类攻击？

n要求提供身份证明

n针对只有语音的请求，要求回叫授权

n避免通过只基于语音的通信方式更改密码

What type of attack would the following precautions help prevent?

■Requesting proof of identity

■Requiring callback authorizations on voice-only requests

■Not changing passwords via voice communications

A：DOS攻击

DoS attacks

B：蠕虫

Worms

C：社会工程学攻击

Social engineering

D：肩窥

Shoulder surfing

答案:这些预防措施主要是为了防止社会工程学攻击（Social engineering）。

- \*\*要求提供身份证明\*\*：这可以防止攻击者冒充他人进行欺诈行为。

- \*\*针对只有语音的请求，要求回叫授权\*\*：这可以防止攻击者通过电话冒充他人进行欺诈。

- \*\*避免通过只基于语音的通信方式更改密码\*\*：这可以防止攻击者通过电话冒充他人来更改密码。

社会工程学攻击通常依赖于欺骗和操纵人类行为，而不是直接利用技术漏洞。这些措施通过增加身份验证的步骤和限制敏感操作的方式，可以有效减少社会工程学攻击的风险。

因此，正确答案是：

C：社会工程学攻击

Social engineering

-------------------

题目74：CIS基准是哪种合规工具的一个示例？

The CIS benchmarks are an example of what sort of compliance tool?

A：安全基线

A security baseline

B：合规标准

A compliance standard

C：安全配置工具

A secure provisioning tool

D：安全自动化工具

A security automation tool

答案:CIS基准（Center for Internet Security Benchmarks）是一种广泛认可的安全配置指南，旨在帮助组织确保其系统和应用程序的安全配置。这些基准提供了详细的配置建议，以减少系统漏洞和攻击面。

因此，CIS基准是 \*\*安全基线\*\* 的一个示例。

正确答案是：

A：安全基线

A security baseline

-------------------

题目75：剩余数据是在试图清除之后留下的什么类型的数据的另一个术语？

Residual data is another term for what type of data left after attempts have been made to erase it?

A：剩余数据

Leftover data

B：MBR

MBR

C：Bitrot

Bitrot

D：残余数据

Remnant data

答案:题目75的正确答案是：

D：残余数据

Remnant data

解析：残余数据（Remnant data）是指在尝试清除数据后仍然留在存储设备上的数据。这些数据可能由于删除操作不彻底或数据恢复技术而被保留下来。其他选项如MBR（主引导记录）和Bitrot（数据衰减）与题目描述的情况不符。

-------------------

题目76：以下哪种灾难恢复测试类型涉及灾难恢复设施的实际激活？

Which one of the following disaster recovery test types involves the actual activation of the disaster recovery facility?

A：模拟试验

Simulation test

B：桌面练习

Tabletop exercise

C：并行测试

Parallel test

D：清单审查

Checklist review

答案:题目76的正确答案是：

C：并行测试

Parallel test

并行测试（Parallel test）是一种灾难恢复测试类型，它涉及将生产系统和灾难恢复系统同时运行，以验证灾难恢复设施的实际激活和运行能力。这种测试通常不会中断生产系统的运行，但会确保在灾难发生时，恢复系统能够正常工作。

其他选项的解释：

- A：模拟试验（Simulation test）通常是在模拟环境中进行的测试，不涉及实际的生产系统或灾难恢复设施。

- B：桌面练习（Tabletop exercise）是一种讨论和演练灾难恢复计划的会议，不涉及实际的操作或设施激活。

- D：清单审查（Checklist review）是对灾难恢复计划中的步骤和清单进行审查，以确保所有步骤都已准备就绪，但不涉及实际的操作或设施激活。

-------------------

题目77：什么访问控制系统允许所有者决定谁可以访问他们拥有的客体？

What access control system lets owners decide who has access to the objects they own?

A：基于角色的访问控制

Role-based access control

B：基于任务的访问控制

Task-based access control

C：自由访问控制

Discretionary access control

D：基于规则的访问控制

Rule-based access control

答案:正确答案是：

C：自由访问控制 (Discretionary access control)

自由访问控制（Discretionary Access Control, DAC）是一种访问控制机制，它允许资源的所有者（如文件或文件夹的创建者）决定谁可以访问这些资源以及他们可以执行哪些操作。在这种系统中，所有者可以授予或撤销其他用户对资源的访问权限。

-------------------

题目78：使用可信信道和链路加密是防止什么类型的访问控制攻击的方法？

Using a trusted channel and link encryption are both ways to prevent what type of access control attack?

A：暴力

Brute-force

B：欺骗登录屏幕

Spoofed login screens

C：中间人攻击

Man-in-the-middle attacks

D：字典攻击

Dictionary attacks

答案:使用可信信道和链路加密是防止\*\*中间人攻击\*\*（Man-in-the-middle attacks）的方法。

\*\*中间人攻击\*\*是指攻击者在通信双方之间插入自己，窃听或篡改通信内容。通过使用可信信道和链路加密，可以确保通信的机密性和完整性，防止攻击者在通信过程中窃取或篡改数据。

因此，正确答案是：

C：中间人攻击

Man-in-the-middle attacks

-------------------

题目79：以下哪一项不是(ISC)2道德守则的规范之一？

Which one of the following is not one of the canons of the (ISC)2 Code of Ethics?

A：保护社会公共利益和维持必要的公众信任

Protect society, the common good, necessary public trust and confidence, and the infrastructure.

B：正直、诚实、公正、负责任和合法地行事

Act honorably, honestly, justly, responsibly, and legally.

C：为负责人提供高效优质的服务

Provide diligent and competent service to principals.

D：保持所有调查和评估的合格记录

Maintain competent records of all investigations and assessments.

答案:题目79的正确答案是：

D：保持所有调查和评估的合格记录

Maintain competent records of all investigations and assessments.

解释：

(ISC)² 道德守则的规范主要包括以下几点：

1. 保护社会公共利益和维持必要的公众信任（A选项）。

2. 正直、诚实、公正、负责任和合法地行事（B选项）。

3. 为负责人提供高效优质的服务（C选项）。

D选项“保持所有调查和评估的合格记录”并不是(ISC)²道德守则的规范之一。因此，D选项是正确答案。

-------------------

题目80：组织的应急响应准则应包括以下哪个组成部分？

Which one of the following components should be included in an organization&rsquo;s emergency response guidelines?

A：立即反应程序

Immediate response procedures

B：长期业务连续性协议

Long-term business continuity protocols

C：组织的冷站点激活程序

Activation procedures for the organization&rsquo;s cold sites

D：订购设备的联系信息

Contact information for ordering equipment

答案:题目80是关于组织的应急响应准则应该包括哪些组成部分。应急响应准则是一套预先制定的程序和步骤，用于在紧急情况下指导组织如何快速有效地响应，以最小化损失并恢复正常运营。

A选项“立即反应程序”是应急响应准则的核心组成部分，它定义了在紧急情况发生时应立即采取的步骤和措施，以确保人员安全和减少财产损失。

B选项“长期业务连续性协议”虽然对于组织的长期恢复和运营至关重要，但它通常属于业务连续性计划的一部分，而不是应急响应准则的组成部分。

C选项“组织的冷站点激活程序”是指在没有主要设施可用时，启动备用站点以维持业务运营的程序。这通常是灾难恢复计划的一部分，而不是应急响应准则的直接组成部分。

D选项“订购设备的联系信息”虽然在某些情况下可能有用，但它不是应急响应准则的核心组成部分。

因此，最合适的答案是A选项“立即反应程序”。

最终答案是：$\boxed{A}$。

-------------------

题目81：Ben 正努力整合联合身份管理系统，并需要为基于浏览器的单点登录交换身份验证和授权信息。哪项技术是他最好的选择？

Ben is working on integrating a federated identity management system and needs to exchange authentication and authorization information for browser-based single sign-on. What technology is his best option?

A：HTML

HTML

B：XACML

XACML

C：SAML

SAML

D：SPML

SPML

答案:Ben 正在努力整合联合身份管理系统，并需要为基于浏览器的单点登录交换身份验证和授权信息。在这种情况下，最适合的技术是 \*\*SAML\*\*（Security Assertion Markup Language）。

\*\*SAML\*\* 是一种基于 XML 的标准，用于在不同的安全域之间交换身份验证和授权数据。它广泛用于实现单点登录（SSO），允许用户在一个系统中登录后，无需再次登录即可访问其他联合系统中的资源。

其他选项的解释：

- \*\*HTML\*\* 是用于创建网页的标记语言，不涉及身份验证和授权信息的交换。

- \*\*XACML\*\*（eXtensible Access Control Markup Language）是一种用于定义访问控制策略的语言，但不直接用于单点登录。

- \*\*SPML\*\*（Service Provisioning Markup Language）用于在系统之间交换用户资源供应信息，也不直接用于单点登录。

因此，\*\*C：SAML\*\* 是最佳选择。

-------------------

题目82：组织一般隔一段时间就应该为相关人员开展业务连续性计划评估培训，请问培训的最短时间间隔是多少？

What is the minimum interval at which an organization should conduct business continuity plan refresher training for those with specific business continuity roles?

A：每周

Weekly

B：每月

Monthly

C：半年一次

Semiannually

D：每年

Annually

答案:正确答案是：D：每年 (Annually)

业务连续性计划评估培训的目的是确保相关人员能够熟悉和掌握业务连续性计划的更新内容，以及在紧急情况下能够有效地执行计划。通常，这种培训每年进行一次，以确保相关人员对计划的最新变化有充分的了解，并保持其应对突发事件的能力。虽然具体的培训频率可能因组织的需求和行业标准而有所不同，但每年一次是最常见的推荐频率。

-------------------

题目83：在软件测试期间通常测试哪三种类型的接口？

What three types of interfaces are typically tested during software testing?

A：网络、物理、应用程序接口

Network, physical, and application interfaces

B：API、UI、物理接口

APIs, UIs, and physical interfaces

C：网络接口、API、UI

Network interfaces, APIs, and UIs

D：应用程序、程序、用户界面

Application, programmatic, and user interfaces

答案:在软件测试期间，通常会测试以下三种类型的接口：

1. \*\*用户界面（UI）\*\*：这是用户与软件交互的直接界面，测试确保用户界面易于使用且功能正常。

2. \*\*应用程序接口（API）\*\*：这些接口允许不同的软件组件相互通信，测试确保API按预期工作并正确处理数据。

3. \*\*网络接口\*\*：这些接口涉及软件与网络之间的通信，测试确保数据在网络中正确传输。

因此，正确答案是：

\*\*C：网络接口、API、UI\*\*

\*\*Network interfaces, APIs, and UIs\*\*

-------------------

题目84：Amanda希望监控她的LDAP服务器，以便查出导致问题的类型。如果她想要使用生产服务器和实际流量进行测试，她应该使用什么类型的监控？

Amanda wants to monitor her LDAP servers to identify which types of queries are causing problems. What type of monitoring should she use if she wants to be able to use the production servers and actual traffic for her testing?

A：活跃

Active

B：实时

Real-time

C：被动

Passive

D：重放

Replay

答案:Amanda希望监控她的LDAP服务器以识别导致问题的查询类型，并且她希望使用生产服务器和实际流量进行测试。在这种情况下，她应该使用\*\*被动监控\*\*。

\*\*被动监控\*\*（Passive Monitoring）是指在不干扰正常操作的情况下，通过监听和分析实际流量来收集数据。这种方式不会对生产环境产生影响，适合用于监控和分析实际流量，而不会引入额外的负载或干扰。

其他选项的解释：

- \*\*活跃监控\*\*（Active Monitoring）：主动发送测试请求或流量来监控系统，可能会对生产环境产生影响。

- \*\*实时监控\*\*（Real-time Monitoring）：虽然可以实时查看数据，但不一定适合用于分析实际流量，且可能会对系统性能产生影响。

- \*\*重放监控\*\*（Replay Monitoring）：通常是指重新播放之前捕获的流量，而不是直接使用实际流量。

因此，\*\*C：被动监控\*\*（Passive Monitoring）是最合适的选择。

-------------------

题目85：Steve正在开发一个输入验证例程，它将保护支持Web应用程序的数据库免受SQL注入攻击。Steve应在哪里放置输入验证码？

Steve is developing an input validation routine that will protect the database supporting a web application from SQL injection attack. Where should Steve place the input validation code?

A：嵌入在网页中的JavaScript

JavaScript embedded in the web pages

B：Web服务器上的后端代码

Backend code on the web server

C：数据库上的存储过程

Stored procedure on the database

D：用户的Web浏览器上的代码

Code on the user’s web browser

答案:正确答案是 \*\*B：Web服务器上的后端代码\*\*。

### 解析：

SQL注入攻击是通过在用户输入中插入恶意SQL代码来攻击数据库的一种方式。为了防止SQL注入攻击，输入验证和清理应该在Web服务器的后端代码中进行，而不是在前端（如JavaScript或用户的浏览器）或数据库中。

- \*\*A：嵌入在网页中的JavaScript\*\*

JavaScript运行在用户的浏览器中，用户可以禁用或绕过它，因此不能依赖它来防止SQL注入攻击。

- \*\*B：Web服务器上的后端代码\*\*

后端代码（如PHP、Python、Java等）运行在服务器上，可以对用户输入进行严格的验证和清理，确保输入数据是安全的，然后再将其传递给数据库。这是防止SQL注入的最佳实践。

- \*\*C：数据库上的存储过程\*\*

虽然存储过程可以增加安全性，但它们不能完全替代输入验证。输入验证应该在数据到达数据库之前进行。

- \*\*D：用户的Web浏览器上的代码\*\*

与选项A类似，浏览器端的代码（如JavaScript）可以被用户绕过或篡改，因此不能作为防止SQL注入的主要手段。

因此，\*\*B：Web服务器上的后端代码\*\* 是最合适的选择。

-------------------

题目86：Ben 正在选择一种用于拥有10000名员工的组织中的加密算法。他必须促进组织内任何两名员工之间的沟通。以下哪种算法将允许他用最短的时间来实现密钥管理？

Ben is selecting an encryption algorithm for use in an organization with 10,000 employees. He must facilitate communication between any two employees within the organization. Which one of the following algorithms would allow him to meet this goal with the least time dedicated to key management?

A：RSA

RSA

B：IDEA

IDEA

C：3DES

3DES

D：Skipjack

Skipjack

答案:在拥有10000名员工的组织中，Ben需要选择一种加密算法，以便任何两名员工之间能够安全通信，并且密钥管理的时间最短。为了实现这一目标，Ben应该选择一种能够有效管理大量密钥对的算法。

选项分析：

- \*\*A：RSA\*\*

RSA是一种非对称加密算法，每个用户需要一对公钥和私钥。对于10000名员工，每个员工需要与其他9999名员工通信，这意味着需要管理大量的密钥对。虽然RSA在安全性上表现良好，但密钥管理的工作量会非常大。

- \*\*B：IDEA\*\*

IDEA是一种对称加密算法，通常用于加密数据。对称加密算法要求通信双方共享同一个密钥。对于10000名员工，每对员工之间需要一个独立的密钥，这意味着需要管理大约5000万（10000 \* 9999 / 2）个密钥，这在密钥管理上是非常不现实的。

- \*\*C：3DES\*\*

3DES也是一种对称加密算法，与IDEA类似，密钥管理的工作量也会非常大，因为每对员工之间需要一个独立的密钥。

- \*\*D：Skipjack\*\*

Skipjack是一种对称加密算法，与IDEA和3DES类似，密钥管理的工作量也会非常大。

\*\*最佳选择：A：RSA\*\*

虽然RSA的密钥管理在10000名员工的情况下仍然复杂，但相比于对称加密算法（如IDEA、3DES、Skipjack），RSA的非对称特性使得密钥管理更为高效。通过使用公钥基础设施（PKI），可以有效地管理公钥和私钥对，而不需要为每对员工生成和分发独立的密钥。因此，RSA在这种情况下是最佳选择。

-------------------

题目87：Grace正在考虑在其组织中使用新的身份证，用于物理访问控制。她看到下图显示的样品卡，但并不确定该卡使用的技术。请问这是什么类型的卡？

Grace is considering the use of new identification cards in her organization that will be used for physical access control. She comes across the sample card shown here and is unsure of the technology it uses. What type of card is this?

<div style="text-align:center"><img alt="" height="277" src="/file/100000/m/20210825/25796cac434141d29c1e31eb9549ccbc.png" width="572" /></div>

A：智能卡

Smart card

B：相二卡

Phase-two card

C：接近卡

Proximity card

D：磁条卡

Magnetic stripe card

答案:根据题目描述和图像中的卡片特征，Grace所看到的卡片最可能使用的是接近卡（Proximity card）技术。接近卡通常用于物理访问控制系统，用户只需将卡片靠近读卡器即可进行身份验证，无需物理接触。这种卡片通常包含一个射频识别（RFID）芯片，能够在一定距离内与读卡器进行通信。

因此，正确答案是：

C：接近卡

Proximity card

-------------------

题目88：该图显示了什么类型的日志文件？

What type of log file is shown in this figure?

<div style="text-align:center"><img alt="" height="234" src="/file/100000/m/20210825/51e93412d8ff44cabf8dc627438246df.png" width="629" /></div>

A：应用

Application

B：Web 服务器

Web server

C：系统

System

D：防火墙

Firewall

答案:根据题目描述，图中显示的日志文件类型可能是与网络或安全相关的日志。由于选项中有“防火墙”（Firewall），而防火墙日志通常记录网络流量、访问控制、安全事件等信息，因此最有可能的答案是：

D：防火墙

Firewall

当然，具体答案还需要根据图中的内容进一步确认。如果图中显示的日志内容与网络流量、安全事件或访问控制相关，那么选择“防火墙”是最合适的。

-------------------

题目89：下列哪项活动有助于减轻零日漏洞的威胁？

Which one of the following activities transforms a zero-day vulnerability into a less dangerous attack vector?

A：发现漏洞

Discovery of the vulnerability

B：传输层加密的实现

Implementation of transport-layer encryption

C：重新配置防火墙

Reconfiguration of a firewall

D：安全补丁的发布

Release of a security patch

答案:题目89的正确答案是：

D：安全补丁的发布

Release of a security patch

解析：

零日漏洞（Zero-day vulnerability）是指尚未被公开或尚未有补丁修复的安全漏洞。攻击者可以利用这些漏洞在软件开发者或安全研究人员发现并修复之前进行攻击。发布安全补丁是减轻零日漏洞威胁的最有效方法之一，因为补丁可以修复漏洞，使其不再被利用。

其他选项的解析：

A：发现漏洞 - 虽然发现漏洞是第一步，但仅仅发现漏洞并不能减轻威胁，除非采取进一步的措施（如发布补丁）。

B：传输层加密的实现 - 传输层加密可以保护数据在传输过程中的安全，但它不能直接减轻零日漏洞的威胁。

C：重新配置防火墙 - 重新配置防火墙可以增强网络的安全性，但它不能直接修复零日漏洞。

因此，发布安全补丁是减轻零日漏洞威胁的最直接和有效的方法。

-------------------

题目90：Elle的组织不得不转向远程工作。每个员工都需要访问特定的应用程序，并且由于快速切换，员工可能是家庭系统或借来的笔记本电脑系统上工作。 在Elle面临的这种情况下，远程访问的最佳选择是什么？

Elle’s organization has had to shift to remote work. Each staff member needs access to specific applications, and due to the quick shift, staff members are working from systems that may be home systems or borrowed laptops. What is the best option for remote access in a situation like the one that Elle is facing?

A：IPsec VPN

An IPsec VPN

B：在每个远程工作地点使用专用光纤连接

A dedicated fiber connection to each remote work location

C：基于HTML5的VPN

An HTML5-based VPN

D：使用远程桌面连接到公司办公楼现有的工作站

Use of remote desktop to connect to an existing workstation at the company’s office building

答案:在Elle的组织面临的情况下，最佳的远程访问选择是 \*\*A：IPsec VPN\*\*。

### 原因分析：

1. \*\*IPsec VPN\*\*：

- \*\*安全性\*\*：IPsec VPN 提供了强大的加密和认证机制，确保数据在传输过程中的安全性，适合处理敏感信息。

- \*\*灵活性\*\*：员工可以从任何设备（包括家庭系统或借来的笔记本电脑）连接到公司网络，访问所需的应用程序。

- \*\*广泛支持\*\*：大多数操作系统和设备都支持IPsec VPN，易于部署和管理。

2. \*\*专用光纤连接\*\*：

- \*\*不切实际\*\*：为每个远程工作地点安装专用光纤连接成本高昂且不现实，尤其是在员工分布广泛的情况下。

3. \*\*基于HTML5的VPN\*\*：

- \*\*局限性\*\*：HTML5 VPN 通常用于通过浏览器访问特定的应用程序，可能无法提供对所有公司资源的全面访问，且安全性可能不如IPsec VPN。

4. \*\*远程桌面连接到公司办公楼现有的工作站\*\*：

- \*\*依赖性\*\*：这种方法依赖于公司办公楼的工作站，如果办公楼出现问题（如断电或网络故障），远程员工将无法工作。

- \*\*性能问题\*\*：远程桌面连接可能会受到网络延迟和带宽限制的影响，影响工作效率。

因此，\*\*IPsec VPN\*\* 是最适合Elle组织的远程访问解决方案，能够在确保安全性的同时提供灵活性和广泛的设备支持。

-------------------

题目91：Susan想要监视VMWare环境中系统之间的流量。她最好选择什么解决方案来监控流量？

Susan wants to monitor traffic between systems in a VMware environment. What solution would be her best option to monitor that traffic?

A：使用传统的基于硬件的IPS

Use a traditional hardware-based IPS.

B：在每个虚拟系统上安装Wireshark

Install Wireshark on each virtual system.

C：设置虚拟跨接口并使用VM IDS捕获数据

Set up a virtual span port and capture data using a VM IDS.

D：使用netcat捕获VM之间发送的所有流量

Use netcat to capture all traffic sent between VMs.

答案:在VMware环境中监视系统之间的流量，最佳的选择是：

\*\*C：设置虚拟跨接口并使用VM IDS捕获数据\*\*

\*\*Set up a virtual span port and capture data using a VM IDS.\*\*

### 解析：

- \*\*A：使用传统的基于硬件的IPS\*\*

传统的基于硬件的IPS（入侵防御系统）通常用于物理网络环境，无法直接监控虚拟机之间的内部流量，因此不适合VMware环境。

- \*\*B：在每个虚拟系统上安装Wireshark\*\*

虽然Wireshark可以捕获流量，但在每个虚拟系统上安装Wireshark会占用大量资源，并且管理起来非常复杂，不是最佳选择。

- \*\*C：设置虚拟跨接口并使用VM IDS捕获数据\*\*

在VMware环境中，可以通过设置虚拟跨接口（vSphere Distributed Switch的端口镜像功能）来捕获虚拟机之间的流量，并结合虚拟机入侵检测系统（VM IDS）进行分析和监控。这是最有效和高效的方式。

- \*\*D：使用netcat捕获VM之间发送的所有流量\*\*

Netcat是一个网络工具，主要用于数据传输和调试，不适合用于流量监控和分析。

因此，\*\*C选项\*\*是最合适的解决方案。

-------------------

题目92-1：参考以下场景，回答4个问题。

Matthew 和Richard 是位于不同物理位置的朋友，他们开始彼此通信时希望使用加密技术来保障其通信的保密性。他们交换数字证书开始通信，并计划使用非对称加密算法来安全交换电子邮件。

For questions , please refer to the following scenario:

Matthew and Richard are friends located in different physical locations who would like to begin communicating with each other using cryptography to protect the confidentiality of their communications. They exchange digital certificates to begin this process and plan to use an asymmetric encryption algorithm for the secure exchange of email messages.

当Matthew给Richard发消息时，他应该用什么密钥加密消息？

When Matthew sends Richard a message, what key should he use to encrypt the message?

A：Matthew的公钥

Matthew’s public key

B：Matthew的私钥

Matthew’s private key

C：Richard的公钥

Richard’s public key

D：Richard的私钥

Richard’s private key

答案:当Matthew给Richard发消息时，他应该使用Richard的公钥来加密消息。这是因为非对称加密算法的基本原理是使用接收者的公钥加密消息，只有接收者的私钥才能解密该消息。因此，Matthew使用Richard的公钥加密消息后，只有Richard可以使用自己的私钥解密并读取消息内容。

正确答案是：

C：Richard的公钥

Richard's public key

-------------------

题目92-1：参考以下场景，回答4个问题。

Matthew 和Richard 是位于不同物理位置的朋友，他们开始彼此通信时希望使用加密技术来保障其通信的保密性。他们交换数字证书开始通信，并计划使用非对称加密算法来安全交换电子邮件。

For questions , please refer to the following scenario:

Matthew and Richard are friends located in different physical locations who would like to begin communicating with each other using cryptography to protect the confidentiality of their communications. They exchange digital certificates to begin this process and plan to use an asymmetric encryption algorithm for the secure exchange of email messages.

当Richard收到来自马修的消息时，他应该使用什么密钥来解密消息？

When Richard receives the message from Matthew, what key should he use to decrypt the message?

A：Matthew的公钥

Matthew’s public key

B：Matthew的私钥

Matthew’s private key

C：Richard的公钥

Richard’s public key

D：Richard的私钥

Richard’s private key

答案:在非对称加密算法中，每个用户都有一对密钥：公钥和私钥。公钥可以公开分享给任何人，而私钥必须严格保密。当Matthew发送加密消息给Richard时，他会使用Richard的公钥来加密消息。因此，只有Richard的私钥才能解密这条消息。

所以，当Richard收到来自Matthew的消息时，他应该使用自己的私钥来解密消息。

正确答案是：

D：Richard的私钥

Richard's private key

-------------------

题目92-1：参考以下场景，回答4个问题。

Matthew 和Richard 是位于不同物理位置的朋友，他们开始彼此通信时希望使用加密技术来保障其通信的保密性。他们交换数字证书开始通信，并计划使用非对称加密算法来安全交换电子邮件。

For questions , please refer to the following scenario:

Matthew and Richard are friends located in different physical locations who would like to begin communicating with each other using cryptography to protect the confidentiality of their communications. They exchange digital certificates to begin this process and plan to use an asymmetric encryption algorithm for the secure exchange of email messages.

Matthew希望通过给信息添加数字签名来加强通信的安全性。加密的目的是要执行数字签名的哪项特性？

Matthew would like to enhance the security of his communication by adding a digital signature to the message. What goal of cryptography are digital signatures intended to enforce?

A：秘密

Secrecy

B：可用性

Availability

C：机密性

Confidentiality

D：不可否认

Nonrepudiation

答案:数字签名的主要目的是确保信息的不可否认性（Nonrepudiation）。不可否认性意味着发送者不能否认他们已经发送了信息，因为数字签名提供了发送者身份验证和消息完整性的证据。因此，正确答案是：

D：不可否认

Nonrepudiation

-------------------

题目92-1：参考以下场景，回答4个问题。

Matthew 和Richard 是位于不同物理位置的朋友，他们开始彼此通信时希望使用加密技术来保障其通信的保密性。他们交换数字证书开始通信，并计划使用非对称加密算法来安全交换电子邮件。

For questions , please refer to the following scenario:

Matthew and Richard are friends located in different physical locations who would like to begin communicating with each other using cryptography to protect the confidentiality of their communications. They exchange digital certificates to begin this process and plan to use an asymmetric encryption algorithm for the secure exchange of email messages.

当Matthew要向消息中添加数字签名时，他应使用什么加密密钥来创建数字签名？

When Matthew goes to add the digital signature to the message, what encryption key does he use to create the digital signature?

A：Matthew的公钥

Matthew’s public key

B：Matthew的私钥

Matthew’s private key

C：Richard的公钥

Richard’s public key

D：Richard的私钥

Richard’s private key

答案:当Matthew要向消息中添加数字签名时，他应使用自己的私钥来创建数字签名。数字签名的目的是确保消息的完整性和身份验证，即接收方可以确认消息确实来自Matthew，并且在传输过程中没有被篡改。由于私钥只有Matthew自己持有，因此使用私钥签名可以证明消息确实是由Matthew发出的。

因此，正确答案是：

B：Matthew的私钥

Matthew's private key

-------------------

题目93：当Jim 登录到系统时，将其密码与存储在数据库中的散列值进行比较。这个过程是什么？

When Jim logs into a system, his password is compared to a hashed value stored in a data-base. What is this process?

A：鉴定

Identification

B：散列

Hashing

C：令牌化

Tokenization

D：身份验证

Authentication

答案:这个过程是身份验证（Authentication）。身份验证是确认用户提供的凭据（如用户名和密码）是否与系统中存储的凭据匹配的过程。在这个例子中，Jim输入的密码会被散列处理，然后与数据库中存储的散列值进行比较。如果两者匹配，Jim就被验证为合法用户，允许其访问系统。

所以正确答案是：

D：身份验证

Authentication

-------------------

题目94：在考虑设施设计时，安全专业人员的首要任务是什么？

What is the top priority for security professionals when considering facility design?

A：仅限经批准的人员访问

Limiting access to only approved personnel

B：确保结构支持最小权限

Ensuring that the structure supports least privilege

C：确保人员安全

Ensuring the safety of personnel

D：限制天气或其他自然灾害影响运营的可能性

Limiting the potential for weather or other natural disasters to impact operations

答案:在考虑设施设计时，安全专业人员的首要任务是确保人员安全。这是因为无论设施的设计多么先进或高效，如果人员的安全得不到保障，那么其他所有考虑都是次要的。人员安全包括防止物理伤害、确保紧急情况下的安全疏散、以及提供健康的工作环境等。因此，正确答案是：

C：确保人员安全

Ensuring the safety of personnel

-------------------

题目95：下列哪些类型的控制没有描述陷门？

Which of the following types of controls does not describe a mantrap?

A：威慑

Deterrent

B：预防

Preventive

C：补偿

Compensating

D：物理

Physical

答案:题目95的正确答案是：

C：补偿

Compensating

解释：

- \*\*A：威慑 (Deterrent)\*\*：这类控制旨在通过警告或威胁来阻止潜在的攻击者。例如，安全标志或警告标语。

- \*\*B：预防 (Preventive)\*\*：这类控制旨在防止未经授权的访问或行为。例如，密码、防火墙等。

- \*\*C：补偿 (Compensating)\*\*：这类控制是在主要控制失效时使用的备用控制措施。例如，备份系统或应急计划。

- \*\*D：物理 (Physical)\*\*：这类控制涉及物理屏障或设备，用于限制或控制对特定区域的访问。例如，门锁、围栏、保安人员等。

陷门（Mantrap）是一种物理控制措施，通常用于限制对安全区域的访问。它通常由两个门组成，只有在前一个门关闭后，后一个门才能打开。因此，陷门属于物理控制（D），而不是补偿控制（C）。

-------------------

题目96：Sally的组织需要能够证明某些工作人员发送电子邮件，她希望采用能提供该功能的技术，而不必更改其现有的电子邮件系统。Sally作为电子邮件系统的所有者需要实现的功能的技术术语是什么？她可以使用什么工具来做？

Sally’s organization needs to be able to prove that certain staff members sent emails, and she wants to adopt a technology that will provide that capability without changing their existing email system. What is the technical term for the capability Sally needs to implement as the owner of the email system, and what tool could she use to do it?

A：诚信；IMAP

Integrity; IMAP

B：否认；加密

Repudiation; encryption

C：不可否认；数字签名

Nonrepudiation; digital signatures

D：认证；DKIM

Authentication; DKIM

答案:Sally 的组织需要能够证明某些工作人员发送了电子邮件，并且她希望在不更改现有电子邮件系统的情况下实现这一功能。她需要实现的功能是确保发送者不能否认发送过该邮件，这在技术术语中被称为“不可否认性”（Nonrepudiation）。

为了实现这一功能，Sally 可以使用“数字签名”（Digital Signatures）技术。数字签名可以确保电子邮件的发送者身份的真实性，并且发送者无法否认发送过该邮件。

因此，正确答案是：

\*\*C：不可否认；数字签名\*\*

\*\*Nonrepudiation; digital signatures\*\*

-------------------

题目97：在正常的预雇佣活动期间，通常不执行以下哪种背景调查？

Which one of the following background checks is not normally performed during normal prehire activities?

A：信用检查

Credit check

B：参考验证

Reference verification

C：犯罪记录检查

Criminal records check

D：医疗记录检查

Medical records check

答案:在正常的预雇佣活动期间，通常不会执行医疗记录检查。这是因为医疗记录包含了个人的健康信息，这些信息通常受到隐私保护法律的保护，如美国的《健康保险可携性和责任法案》（HIPAA）。雇主在没有得到应聘者明确同意的情况下，通常无法访问这些信息。此外，使用医疗信息作为雇佣决策的一部分可能会违反反歧视法律。

其他选项，如信用检查、参考验证和犯罪记录检查，是许多雇主在预雇佣过程中常见的背景调查步骤。这些检查有助于雇主评估应聘者的财务责任、过往工作表现和是否有犯罪记录，从而做出更全面的雇佣决策。

因此，正确答案是：

D：医疗记录检查

Medical records check

-------------------

题目98：Naomi的组织将数据访问权限限制为仅具有工作需要的角色用户。这描述了哪项关键的安全操作实践？

Naomi’s organization limits data access to only those users with roles that require it for their job. What key security operations practice does this describe?

A：最小特权

Least privilege

B：特权帐户管理

Privileged account management

C：工作轮换

Job rotation

D：权限提升

Privilege escalation

答案:题目描述的是Naomi的组织将数据访问权限限制为仅具有工作需要的角色用户。这种做法是为了确保用户只能访问他们工作所需的数据，而不能访问其他不必要的数据。这种做法符合“最小特权”原则，即用户只能拥有完成其工作所需的最小权限。

因此，正确答案是：

A：最小特权

Least privilege

-------------------

题目99：在OSI模型中，当数据包从数据流更改为数据段或数据报时，它遍历了哪个层？

In the OSI model, when a packet changes from a data stream to a segment or a datagram, what layer has it traversed?

A：传输层

The Transport layer

B：应用层

The Application layer

C：数据链路层

The Data Link layer

D：物理层

The Physical layer

答案:在OSI模型中，当数据包从数据流更改为数据段或数据报时，它遍历了传输层（Transport layer）。传输层负责提供端到端的数据传输服务，确保数据的完整性和顺序。在这一层，数据流被分割成更小的单元，称为数据段（在TCP协议中）或数据报（在UDP协议中），以便在网络中传输。

因此，正确答案是：

A：传输层

The Transport layer

-------------------

题目100：Tommy处理所在组织的访问控制请求。用户接触他并解释说需要访问人力资源数据库，以完成CFO要求的人员分析工作。用户向Tommy成功展示了什么？

Tommy handles access control requests for his organization. A user approaches him and explains that he needs access to the human resources database in order to complete a headcount analysis requested by the CFO. What has the user demonstrated successfully to Tommy?

A：许可

Clearance

B：职责分离

Separation of duties

C：需知

Need to know

D：隔离

Isolation

答案:题目描述了一个用户请求访问人力资源数据库以完成CFO要求的人员分析工作的情况。用户向Tommy展示了他们需要访问数据库的具体原因，即为了完成特定的工作任务。这符合“需知”（Need to know）原则，即用户只有在需要知道某些信息以完成其工作任务时，才能获得访问权限。

因此，正确答案是：

C：需知

Need to know

-------------------

题目101：Kathleen 想要建立一个提供有关其组织的用户和服务信息的系统，该系统使用一个中央的、开放的、供应商中立、基于标准的系统，并且可以很容易地查询。以下哪项技术是她的最佳选择？

Kathleen wants to set up a service to provide information about her organization’s users and services using a central, open, vendor-neutral, standards-based system that can be easily queried. Which of the following technologies is her best choice?

A：RADIUS

RADIUS

B：LDAP

LDAP

C：Kerberos

Kerberos

D：活动目录

Active Directory

答案:Kathleen 想要建立一个提供有关其组织的用户和服务信息的系统，该系统需要满足以下条件：

1. 中央的、开放的、供应商中立、基于标准的系统。

2. 可以很容易地查询。

让我们逐一分析选项：

- \*\*A：RADIUS\*\*

RADIUS（远程认证拨号用户服务）主要用于网络访问控制，如认证、授权和计费（AAA）。它主要用于管理网络访问权限，而不是存储和查询用户和服务信息。因此，RADIUS 不符合 Kathleen 的需求。

- \*\*B：LDAP\*\*

LDAP（轻量级目录访问协议）是一个开放的、供应商中立的、基于标准的协议，专门用于访问和维护分布式目录信息服务。LDAP 非常适合存储和查询用户和服务信息，并且可以轻松集成到各种系统中。因此，LDAP 是 Kathleen 的最佳选择。

- \*\*C：Kerberos\*\*

Kerberos 是一种网络认证协议，主要用于身份验证和单点登录（SSO）。它不适用于存储和查询用户和服务信息，因此不符合 Kathleen 的需求。

- \*\*D：活动目录（Active Directory）\*\*

活动目录是微软开发的目录服务，主要用于 Windows 环境中的用户和资源管理。虽然它可以存储和查询用户信息，但它不是供应商中立的，并且依赖于 Windows 生态系统。因此，活动目录不符合 Kathleen 的需求。

\*\*最佳选择是 B：LDAP\*\*。

-------------------

题目102：在企业中最常使用什么类型的工具，将资产、用户和所有者进行匹配？

What type of tool is most frequently used to match assets to users and owners in enterprises?

A：企业内容管理工具

An enterprise content management tool

B：条形码属性标签

Barcoded property tags

C：基于RFID的资产标签

RFID-based property tags

D：系统库存

A system inventory

答案:在企业中，最常使用的工具类型是将资产、用户和所有者进行匹配的是：

\*\*D：系统库存\*\*

\*\*A system inventory\*\*

系统库存工具通常用于跟踪和管理企业的资产，包括将资产与用户和所有者进行匹配。这种工具可以提供详细的资产信息、位置、使用情况以及与特定用户或所有者的关联。虽然条形码属性标签和基于RFID的资产标签也可以用于资产跟踪，但它们通常作为系统库存的一部分来使用，而不是单独的工具。企业内容管理工具则主要用于管理文档和内容，而不是资产跟踪。

-------------------

题目103：Alice 想要向安全模型添加另一个客体，并授予自己对该客体的权限。Take-Grant保护模型中的哪个规则将允许她完成此操作？

Alice would like to add another object to a security model and grant herself rights to that object. Which one of the rules in the Take-Grant protection model would allow her to complete this operation?

A：采取规则

Take rule

B：授予规则

Grant rule

C：创建规则

Create rule

D：删除规则

Remove rule

答案:在Take-Grant保护模型中，Alice想要添加另一个客体并授予自己对该客体的权限，她需要使用\*\*创建规则（Create rule）\*\*。

\*\*创建规则\*\*允许主体创建一个新的客体，并授予自己对该客体的权限。因此，Alice可以通过创建规则来添加一个新的客体，并授予自己对该客体的权限。

所以，正确答案是：

C：创建规则

Create rule

-------------------

题目104：当渗透测试人员在测试期间使用Metasploit时，Amanda不应该关注哪个潜在问题列表？

Which of the following concerns should not be on Amanda’s list of potential issues when penetration testers suggest using Metasploit during their testing?

A：Metasploit只能测试有相应插件的漏洞

Metasploit can only test vulnerabilities it has plug-ins for.

B：渗透测试只涉及组织安全的时间点视图

Penetration testing only covers a point-in-time view of the organization’s security.

C：Metasploit之类的工具可能导致拒绝服务问题

Tools like Metasploit can cause denial-of-service issues.

D：渗透测试不能测试过程和政策

Penetration testing cannot test process and policy.

答案:正确答案是 \*\*A\*\*。

\*\*解释：\*\*

- \*\*A：Metasploit只能测试有相应插件的漏洞\*\*

这个选项是不正确的。Metasploit 不仅仅依赖于插件来测试漏洞。它还可以通过自定义脚本、模块和手动配置来测试各种漏洞。因此，Amanda 不应该将这个问题列为潜在问题。

- \*\*B：渗透测试只涉及组织安全的时间点视图\*\*

这是正确的。渗透测试通常是在某个特定时间点进行的，只能反映该时间点的安全状况，而不能反映持续的安全状态。

- \*\*C：Metasploit之类的工具可能导致拒绝服务问题\*\*

这也是正确的。使用 Metasploit 等工具时，如果不小心操作，可能会导致目标系统崩溃或拒绝服务（DoS）。

- \*\*D：渗透测试不能测试过程和政策\*\*

这也是正确的。渗透测试主要关注技术层面的漏洞和弱点，而不是组织的过程和政策。

因此，Amanda 不应该关注选项 A 中的问题。

-------------------

题目105：Colin正在审查根据共同标准分配了EAL7评价保证级别的系统。他对系统的最高保证是什么？

Colin is reviewing a system that has been assigned the EAL7 evaluation assurance level under the Common Criteria. What is the highest level of assurance that he may have about the system?

A：已经完成功能测试

It has been functionally tested.

B：已经完成有条理的测试和检查

It has been methodically tested and checked.

C：已经完成设计、测试和审查

It has been methodically designed, tested, and reviewed.

D：已经完成正式验证、设计和测试

It has been formally verified, designed, and tested.

答案:题目105的正确答案是：

D：已经完成正式验证、设计和测试

It has been formally verified, designed, and tested.

解析：

EAL7（Evaluation Assurance Level 7）是共同标准（Common Criteria）中的最高评价保证级别。达到EAL7级别的系统意味着它已经经过了最严格的安全评估和验证过程。这包括正式验证、设计和测试，以确保系统的安全性和可靠性。因此，Colin对系统的最高保证是它已经完成了正式验证、设计和测试。

-------------------

题目106：当Alex 使用他的智能卡向上游认证服务提供证书时，Alex希望使用哪个ITU-T标准？

Which ITU-T standard should Alex expect to see in use when he uses his smart card to provide a certificate to an upstream authentication service?

A：X.500

X.500

B：SPML

SPML

C：X.509

X.509

D：SAML

SAML

答案:当Alex使用他的智能卡向上游认证服务提供证书时，他期望使用的ITU-T标准是 \*\*X.509\*\*。

\*\*X.509\*\* 是一个广泛使用的标准，定义了公钥证书的格式，通常用于在互联网上进行身份验证和加密通信。智能卡通常使用X.509证书来进行身份验证。

其他选项的解释：

- \*\*X.500\*\* 是一个目录服务标准，用于定义目录服务的结构和协议，但它不直接用于证书的格式。

- \*\*SPML\*\*（Service Provisioning Markup Language）是一种用于在系统之间交换用户、资源和服务配置信息的XML框架，与证书格式无关。

- \*\*SAML\*\*（Security Assertion Markup Language）是一种用于在不同安全域之间交换身份验证和授权数据的XML标准，主要用于单点登录（SSO）场景，而不是证书格式。

因此，正确答案是 \*\*C：X.509\*\*。

-------------------

题目107：根据COPPA的条款，哪些类型的网站受到管制？

What type of websites are regulated under the terms of COPPA?

A：不由金融机构经营的金融网站

Financial websites not run by financial institutions

B：收集个人信息的医疗保健网站

Healthcare websites that collect personal information

C：收集儿童信息的网站

Websites that collect information from children

D：金融机构运营的金融网站

Financial websites run by financial institutions

答案:COPPA（儿童在线隐私保护法案，Children's Online Privacy Protection Act）主要针对的是收集13岁以下儿童个人信息的网站和在线服务。因此，根据COPPA的条款，受到管制的网站类型是那些收集儿童信息的网站。

正确答案是：

C：收集儿童信息的网站

Websites that collect information from children

-------------------

题目108：Tracy最近接受了联邦政府机构的一个IT合规职位，该部门与国防部密切合作处理政府机密问题。以下哪项法律最不可能属于Tracy的代理机构？

Tracy recently accepted an IT compliance position at a federal government agency that works very closely with the Defense Department on classified government matters. Which one of the following laws is least likely to pertain to Tracy’s agency?

A：HIPAA

HIPAA

B：FISMA

FISMA

C：HSA

HSA

D：CFAA

CFAA

答案:题目要求我们确定哪项法律最不可能与Tracy的代理机构相关。Tracy的代理机构与国防部密切合作处理政府机密问题，这意味着她需要遵守与信息安全、数据保护和合规性相关的法律。

让我们逐一分析每个选项：

A. \*\*HIPAA\*\*（健康保险可携性和责任法案）：HIPAA主要涉及医疗信息的隐私和安全。由于Tracy的代理机构处理的是政府机密问题，而不是医疗信息，因此HIPAA最不可能与她的工作直接相关。

B. \*\*FISMA\*\*（联邦信息安全管理法案）：FISMA要求联邦机构保护其信息和信息系统免受未经授权的访问、使用、披露、破坏、修改或破坏。这与Tracy的代理机构处理政府机密问题密切相关。

C. \*\*HSA\*\*（国土安全法案）：HSA涉及国土安全部的建立和运作，以及与国家安全相关的法律。由于Tracy的代理机构与国防部合作处理政府机密问题，HSA可能与她的工作相关。

D. \*\*CFAA\*\*（计算机欺诈和滥用法案）：CFAA涉及计算机犯罪和未经授权访问计算机系统的行为。这与Tracy的代理机构处理政府机密信息的安全性相关。

综上所述，\*\*HIPAA\*\*最不可能与Tracy的代理机构相关，因为她的工作主要涉及政府机密信息，而不是医疗信息。

\*\*最终答案：A. HIPAA\*\*

-------------------

题目109：参考这里所示的图， 名称是什么？

Referring to the figure shown here, what is the name of the security control indicated by the arrow?

<div style="text-align:center"><img alt="" height="320" src="/file/100000/m/20210826/09dd9276d47b4f78882b932ff08efeca.png" width="548" /></div>

A：陷门

Mantrap

B：入侵防御系统

Intrusion prevention system

C：旋转门

Turnstile

D：门户

Portal

答案:根据题目描述和选项，箭头所指的安全控制措施最可能是 \*\*A：陷门（Mantrap）\*\*。

\*\*陷门（Mantrap）\*\* 是一种物理安全控制措施，通常用于限制人员进入敏感区域。它通常由两道门组成，一次只允许一个人通过，并且需要身份验证（如刷卡或生物识别）才能进入第二道门。这种设计可以有效防止尾随（piggybacking）等安全威胁。

其他选项：

- \*\*B：入侵防御系统（Intrusion prevention system）\*\* 是一种网络安全设备，与物理安全无关。

- \*\*C：旋转门（Turnstile）\*\* 是一种单向通行设备，通常用于控制人流，但不提供高级的身份验证功能。

- \*\*D：门户（Portal）\*\* 是一个通用术语，通常指入口或通道，不特指某种安全控制措施。

因此，正确答案是 \*\*A：陷门（Mantrap）\*\*。

-------------------

题目110：访问控制的问责制有哪两个重要因素？

What two important factors does accountability for access control rely on?

A：鉴定和授权

Identification and authorization

B：身份验证和授权

Authentication and authorization

C：识别和身份验证

Identification and authentication

D：责任和身份验证

Accountability and authentication

答案:访问控制的问责制主要依赖于两个重要因素：身份验证和授权。身份验证确保用户是他们所声称的那个人，而授权则确保用户有权访问特定的资源或执行特定的操作。这两个因素共同作用，确保只有经过验证并被授权的用户才能访问受保护的资源，从而维护系统的安全性和完整性。

因此，正确答案是：

B：身份验证和授权

Authentication and authorization

-------------------

题目111：校验支持了CIA三元组中哪组？

What part of the CIA triad does a checksum support?

A：可用性

Availability

B：完整性

Integrity

C：机密性

Confidentiality

D：真实性

Authenticity

答案:校验和（checksum）主要用于检测数据在传输或存储过程中是否发生了改变。它通过计算数据的校验和值并与原始校验和值进行比较，来验证数据的完整性。因此，校验和支持的是CIA三元组中的完整性（Integrity）。

正确答案是：

B：完整性

Integrity

-------------------

题目112：Scott 的组织将其外部IP地址配置为192.168.1.25。当流量发送到他们的ISP时，它不会到达其目的地。Scott的组织遇到什么问题？

Scott’s organization has configured their external IP address to be 192.168.1.25. When traffic is sent to their ISP, it never reaches its destination. What problem is Scott’s organization encountering?

A：BGP未正确设置

BGP is not set up properly.

B：他们没有向ISP注册IP

They have not registered their IP with their ISP.

C：IP地址是一个私有的、不可路由的地址

The IP address is a private, nonroutable address.

D：192.168.1.25是家庭路由器的保留地址

192.168.1.25 is a reserved address for home routers.

答案:题目描述的是Scott的组织将其外部IP地址配置为192.168.1.25，但当流量发送到他们的ISP时，它不会到达其目的地。我们需要找出这个问题的原因。

首先，我们需要了解192.168.1.25这个IP地址的性质。在IPv4地址空间中，192.168.x.x是一个私有地址范围，这些地址在互联网上是不可路由的。私有地址主要用于内部网络，如家庭、办公室或企业内部网络，它们不能直接在公共互联网上使用。因此，当Scott的组织尝试使用这个私有地址作为其外部IP地址时，ISP无法识别这个地址并将其路由到正确的目的地。

现在，我们来看一下选项：

A：BGP未正确设置。BGP（边界网关协议）是用于在互联网上交换路由信息的协议。虽然BGP设置不正确可能会影响路由，但这个选项与题目中提到的私有IP地址问题无关。

B：他们没有向ISP注册IP。虽然注册IP地址是必要的，但这个选项没有解释为什么192.168.1.25这个地址会导致问题。

C：IP地址是一个私有的、不可路由的地址。这个选项直接指出了问题的核心，即192.168.1.25是一个私有地址，不能在公共互联网上路由。

D：192.168.1.25是家庭路由器的保留地址。虽然192.168.1.25常用于家庭路由器，但这个选项没有解释为什么这个地址会导致流量无法到达目的地。

综上所述，最合适的答案是C：IP地址是一个私有的、不可路由的地址。

所以，最终答案是 $\boxed{C}$。

-------------------

题目113：Jack的组织每天多次整合更新到主应用程序中，然后将其作为代码部署，这些代码通过他们的软件开发管道进行检入和测试。这是什么类型的模型？

Jack’s organization merges updates to their main application multiple times a day and then deploys it as code that is checked in and tested through their software development pipeline. What type of model is this?

A：瀑布

Waterfall

B：CI/CD

CI/CD

C：SCM

SCM

D：IDE

IDE

答案:正确答案是 B：CI/CD。

CI/CD 代表持续集成（Continuous Integration）和持续交付（Continuous Delivery）或持续部署（Continuous Deployment）。这种模型允许开发团队频繁地将代码更改合并到主分支中，并通过自动化的构建和测试流程来验证这些更改。然后，这些经过验证的代码可以自动部署到生产环境中。这种模型有助于加快开发周期，提高软件质量，并减少手动操作带来的错误。

在题目中描述的 Jack 的组织每天多次整合更新到主应用程序中，并通过软件开发管道进行检入和测试，这正是 CI/CD 模型的典型特征。

-------------------

题目114：Sue的组织最近未通过安全评估，因为他们的网络是单一的平面广播域，并且在不同的功能组之间可能嗅探流量。她应该推荐什么解决方案来防止问题的出现？

Sue’s organization recently failed a security assessment because their network was a single flat broadcast domain, and sniffing traffic was possible between different functional groups. What solution should she recommend to help prevent the issues that were identified?

A：使用VLAN

Use VLANs.

B：更改所有系统的子网掩码

Change the subnet mask for all systems.

C：部署网关

Deploy gateways.

D：打开端口安全

Turn on port security.

答案:题目描述中提到，Sue的组织未能通过安全评估，原因是他们的网络是一个单一的平面广播域，并且不同的功能组之间可能会嗅探流量。这意味着网络中的所有设备都在同一个广播域中，缺乏隔离，导致安全风险增加。

### 选项分析：

- \*\*A：使用VLAN\*\*

VLAN（虚拟局域网）可以将网络划分为多个逻辑子网，从而隔离不同的功能组。通过使用VLAN，可以防止不同组之间的流量被嗅探，提高网络安全性。这是解决单一广播域问题的有效方法。

- \*\*B：更改所有系统的子网掩码\*\*

更改子网掩码可能会重新划分IP地址范围，但并不能解决广播域的问题。单一广播域仍然存在，不同组之间的流量仍然可能被嗅探。

- \*\*C：部署网关\*\*

部署网关可以帮助不同网络之间的通信，但并不能直接解决单一广播域的问题。网关通常用于连接不同的网络，而不是隔离同一网络中的流量。

- \*\*D：打开端口安全\*\*

端口安全可以限制连接到特定端口的设备数量或MAC地址，但它并不能解决广播域的问题。端口安全主要用于防止未经授权的设备接入网络，而不是隔离流量。

### 正确答案：

\*\*A：使用VLAN\*\*

通过使用VLAN，可以将网络划分为多个逻辑子网，隔离不同功能组之间的流量，从而防止流量嗅探，提高网络安全性。

-------------------

题目115：以下哪个术语最能描述IP地址10.14.124.240？

Which of the following terms best describes the IP address 10.14.124.240?

A：公有IP地址

Public IP address

B：私有IP地址

Private IP address

C：APIPA地址

APIPA address

D：环回地址

Loopback address

答案:IP地址10.14.124.240属于私有IP地址范围。私有IP地址用于在私有网络内部进行通信，不会在公共互联网上路由。根据RFC 1918，私有IP地址的范围包括：

- 10.0.0.0 到 10.255.255.255

- 172.16.0.0 到 172.31.255.255

- 192.168.0.0 到 192.168.255.255

因此，10.14.124.240属于10.0.0.0/8这个私有IP地址范围。

选项B：私有IP地址（Private IP address）是正确的。

其他选项的解释：

- A：公有IP地址（Public IP address）是指在互联网上唯一且可路由的IP地址。

- C：APIPA地址（APIPA address）是当设备无法从DHCP服务器获取IP地址时自动分配的地址，范围是169.254.0.0到169.254.255.255。

- D：环回地址（Loopback address）用于测试网络接口，通常是127.0.0.1。

所以，正确答案是B：私有IP地址（Private IP address）。

-------------------

题目116：Jim正在对他的公司进行安全评估，并希望使用测试工具执行Web漏洞扫描。以下哪个工具最适合该需求？

Jim is performing a security assessment of his company and would like to use a testing tool to perform a web vulnerability scan. Which of the following tools is best suited to that need?

A：Nmap

Nmap

B：Hydra

Hydra

C：Metasploit

Metasploit

D：Nikto

Nikto

答案:题目116是关于选择最适合进行Web漏洞扫描的工具。让我们逐一分析每个选项：

A：Nmap

Nmap（网络映射器）是一个网络发现和安全审计工具。它主要用于网络探测和端口扫描，而不是专门用于Web漏洞扫描。

B：Hydra

Hydra是一个网络登录破解工具，主要用于暴力破解登录凭证。它并不用于Web漏洞扫描。

C：Metasploit

Metasploit是一个渗透测试框架，包含了大量的漏洞利用模块。虽然它可以用于漏洞扫描，但它更侧重于漏洞利用和渗透测试，而不是专门的Web漏洞扫描。

D：Nikto

Nikto是一个开源的Web服务器扫描器，专门用于检测Web服务器上的漏洞和配置问题。它能够扫描多种Web服务器软件，并报告已知的安全问题。

综上所述，最适合用于Web漏洞扫描的工具是Nikto。

正确答案是：D：Nikto