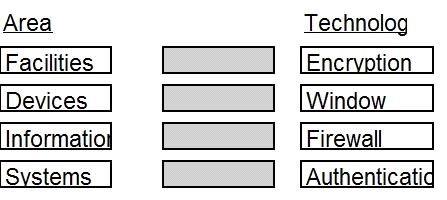
**1. DRAG DROP（拖拽题）**

Given the various means to protect physical and logical assets, match the access management area to the technology.

对以下给定的物理和逻辑资产保护途径，将访问管理领域与技术进行匹配



Answers：

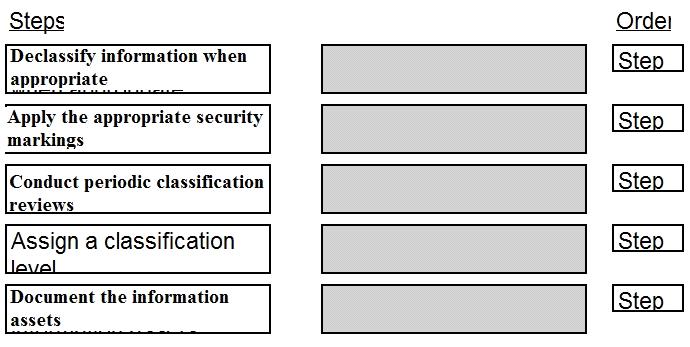


系统—验证；信息—加密；设施—窗锁；设备—防火墙

**2. DRAG DROP（拖拽题）**

Place the following information classification steps in sequential order.

请将以下信息分类步骤排序：



Answers:

步骤1：记录信息资产

步骤2：分配分类级别

步骤3：应用安全标记

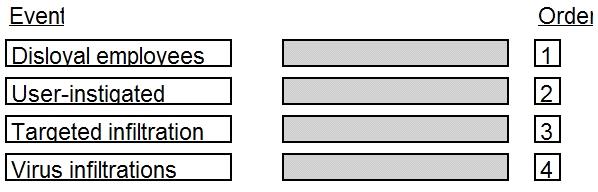
步骤4：定期执行分类审查

步骤5：在适当的时候对信息解密

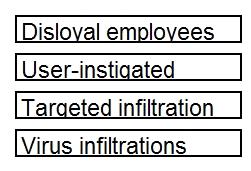
**3. DRAG DROP（拖拽题）**

In which order, from MOST to LEAST impacted, does user awareness training reduce the occurrence of the events below?

用户意识培训以何种程度减少了以下事件的发生？以从最大到最小的顺序排列。



Answers:



不那么忠诚的雇员（仅受自己的意志影响）

被挑唆的用户（受外部故意因素影响）

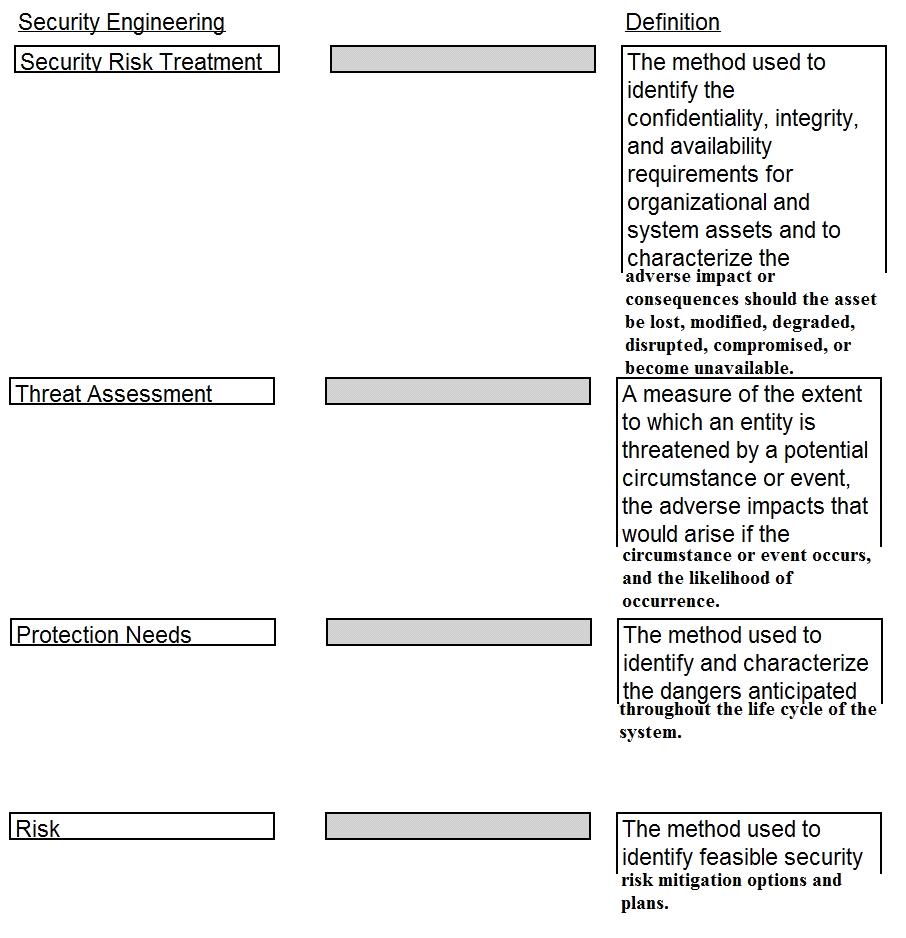
有针对性的渗透（职业黑客/商业间谍）

病毒渗透（非人员因素）

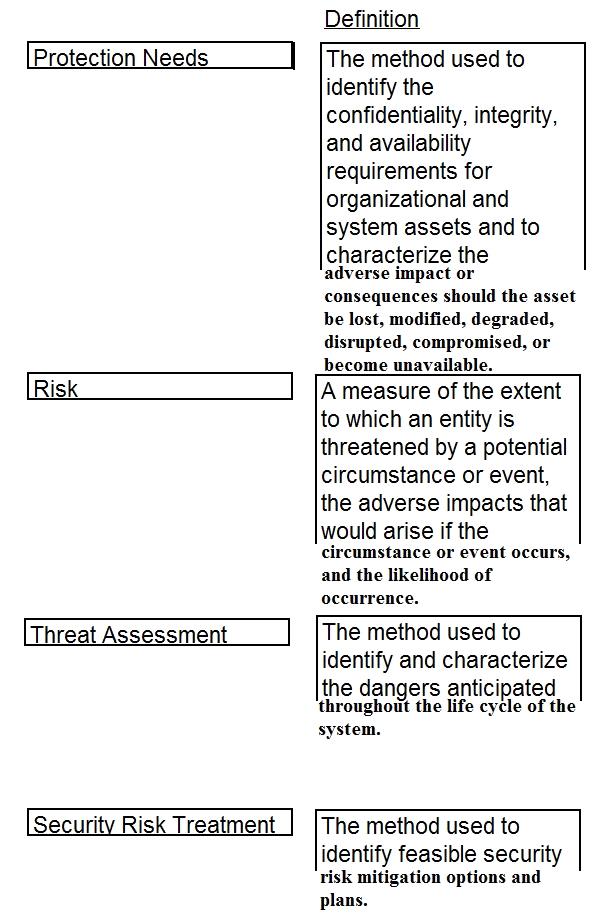
**4. DRAG DROP（拖拽题）**

Drag the following Security Engineering terms on the left to the BEST definition on the right.

将以下左侧的安全工程术语拖至右侧与其最合适的定义匹配。



Answers:



注释：

***Protection Needs*** *保护需求*

The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.

该方法用于识别组织和系统资产的机密性，完整性和可用性要求，并描述资产的丢失，修改，退化，中断，泄露或不可用的不利影响或后果。

***Risk*** *风险*

A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence.

衡量实体受潜在情况或事件威胁的程度，发生情况或事件时将产生的不利影响，以及发生的可能性。

***Threat Assessment*** *威胁评估*

The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.

该方法用于识别和表征系统整个生命周期中预期的危险。

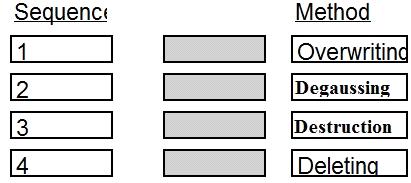
***Security Risk Treatment*** *安全风险处理*

The method used to identify feasible security risk mitigation options and plans.

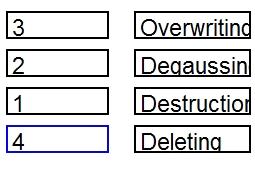
该方法用于识别可行的安全风险缓解方案和计划。

**5. DRAG DROP（拖拽题）**Place in order, from BEST (1) to WORST (4), the following methods to reduce the risk of data remanence on magnetic media.

（1）为最佳，（4）为最差，为右侧的方法按照其降低磁性介质上的数据残留风险的能力匹配序号：

[](http://cdn.aiotestking.com/wp-content/uploads/cissp-v3/15.jpg)

Answers:



Destruction ——销毁

Degaussing——消磁

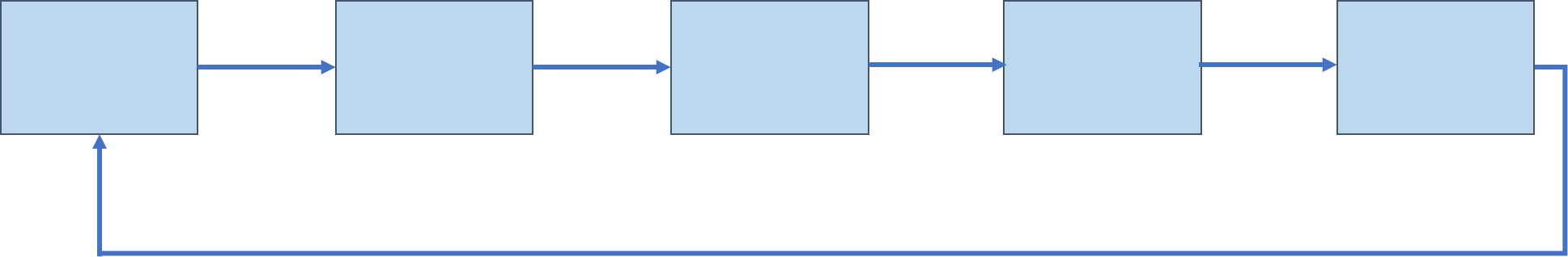
Overwriting——复写

Deleting——删除

**6. DRAG DROP（拖拽题）**

Below are the common phases to creating a Business Continuity/Disaster Recovery (BC/DR) plan. Drag the remaining BC\DR phases to the appropriate corresponding location.

以下是创建业务连续性/灾难恢复（BC / DR）计划的常见阶段。 将剩余的BC \ DR阶段拖到合适的相应位置。



减缓策略开发

业务影响分析

培训，测试和审计

风险评估

BC / DR计划开发

计划维护

Mitigation Strategy Development Business Impact Analysis

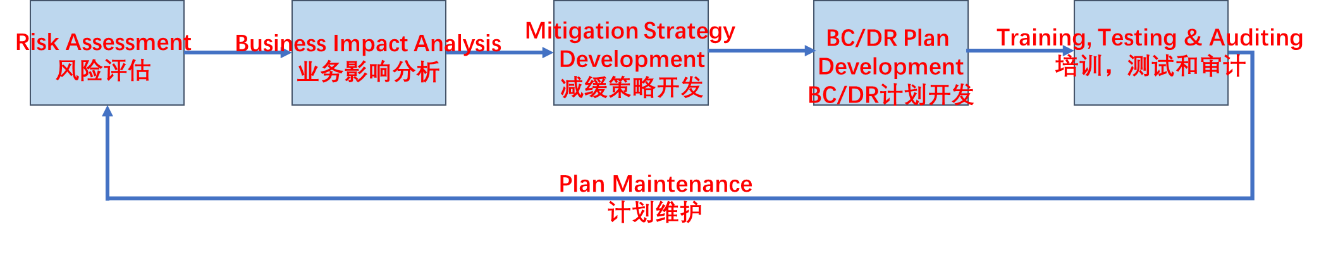
Training, Testing & Auditing

Risk Assessment

BC/DR Plan Development

Plan Maintenance

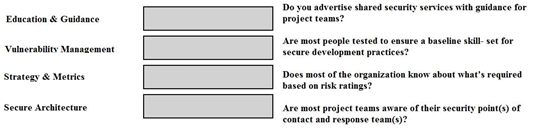
Answer:

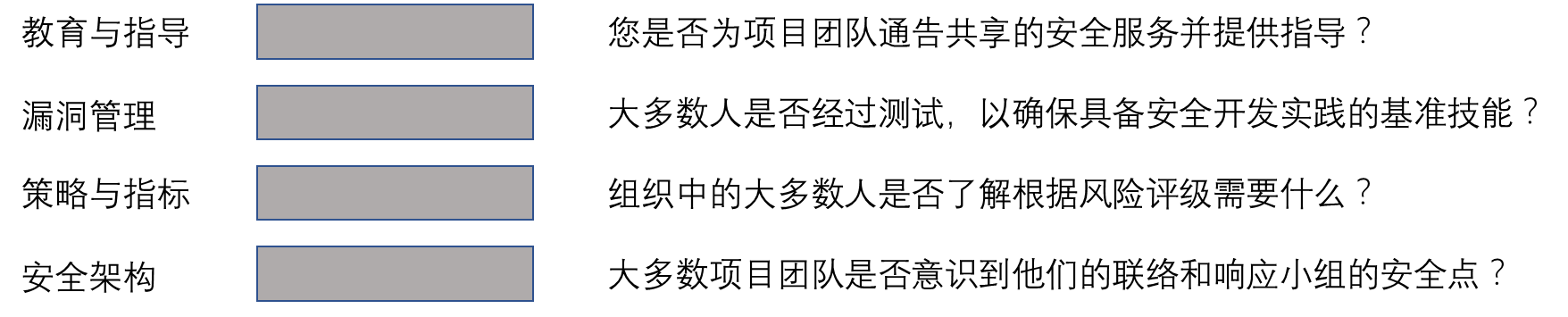


**7. Drag Drop（拖拽题）**

Match the objectives to the assessment questions in the governance domain of Software Assurance Maturity Model (SAMM).

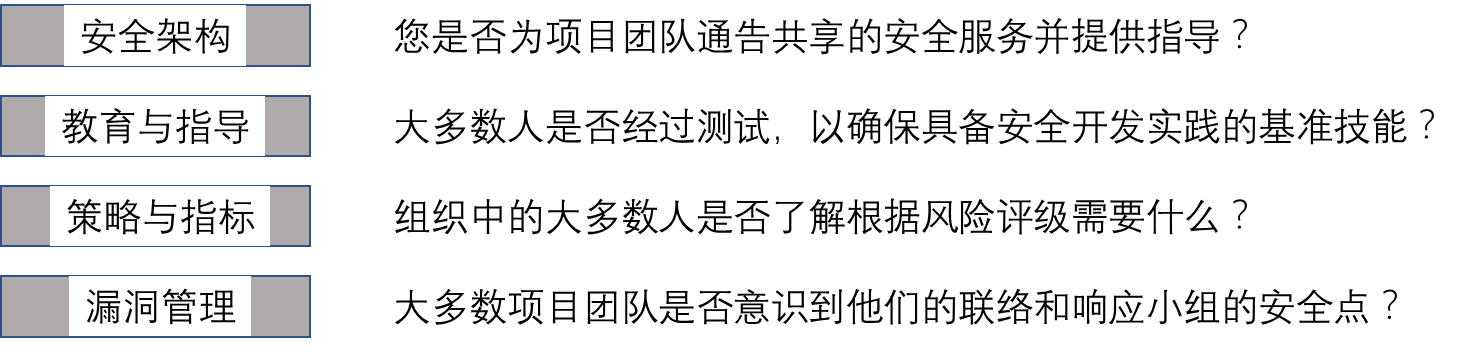
将目标与软件保障成熟度模型（SAMM）治理领域的评估问题相匹配。





Answer:

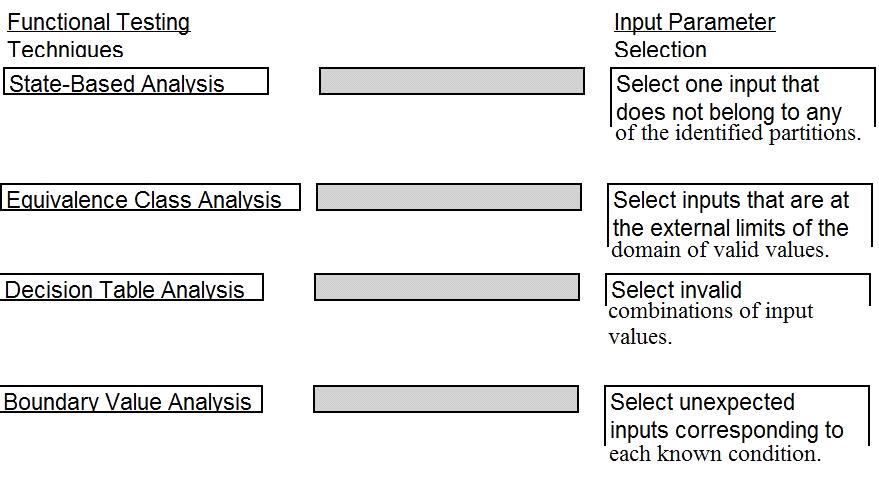


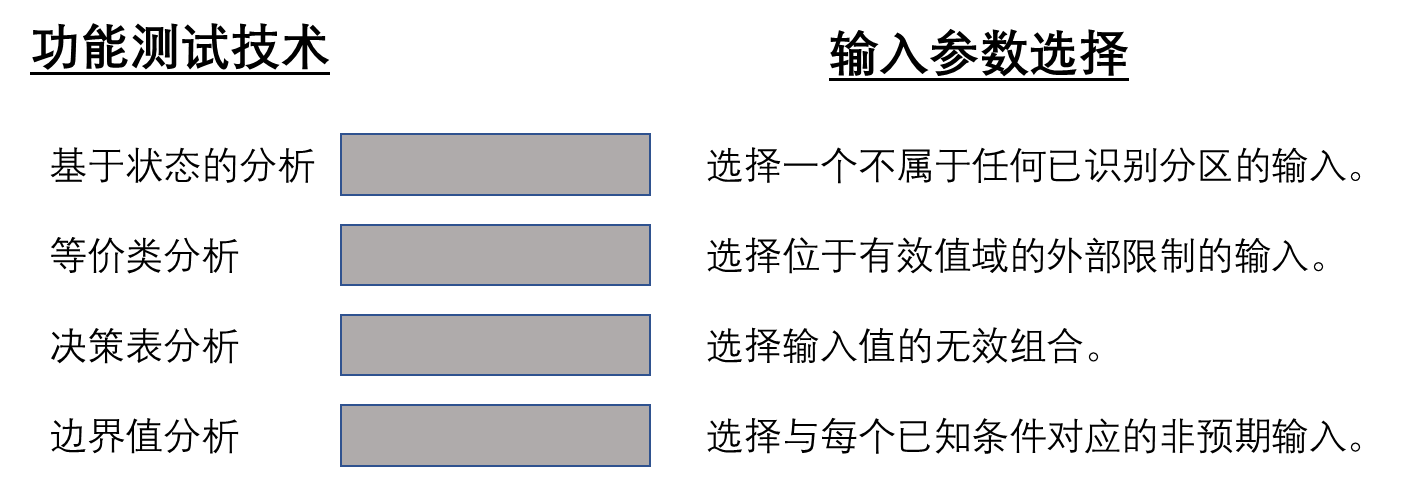


**8. DRAG DROP（拖拽题）**

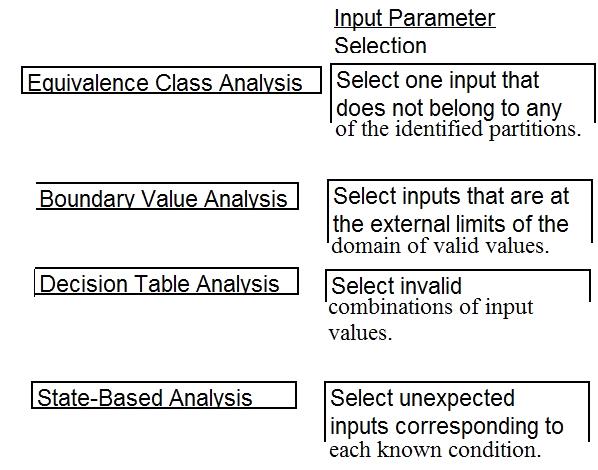
A software security engineer is developing a black box-based test plan that will measure the system’s reaction to incorrect or illegal inputs or unexpected operational errors and situations. Match the functional testing techniques on the left with the correct input parameters on the right.

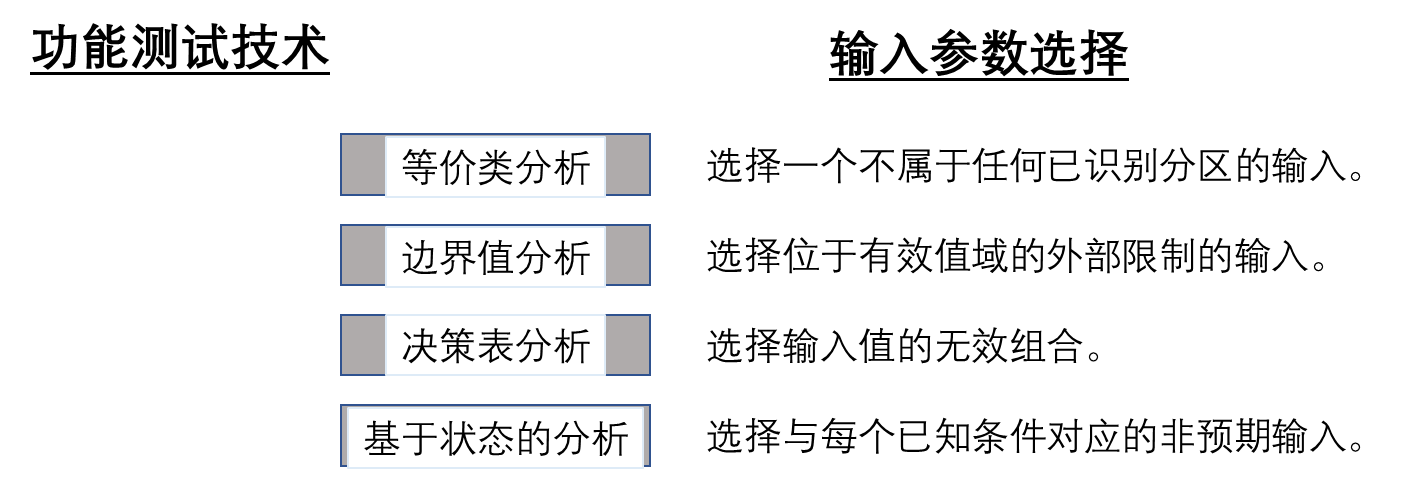
软件安全工程师正在开发基于黑盒的测试计划，该计划将衡量系统对错误或非法输入或意外操作错误和情况的反应。 将功能测试技术与左侧的正确输入参数进行匹配。





Answer:





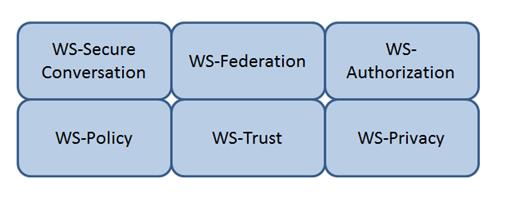
**9. HOTSPOT（热区题，鼠标点中合适的板块即可）**

Which Web Services Security (WS-Security) specification handles the management of security tokens and the underlying policies for granting access?

以下哪一个Web服务安全（WS-Security，Web Services Security）规格处理安全令牌的管理和授权访问的基本策略？

Click on the correct specification in the image below.

请点击下图中的正确规格。



Answer:

WS-Authorization

Java Web Services: Up and Running” By Martin Kalin page 228

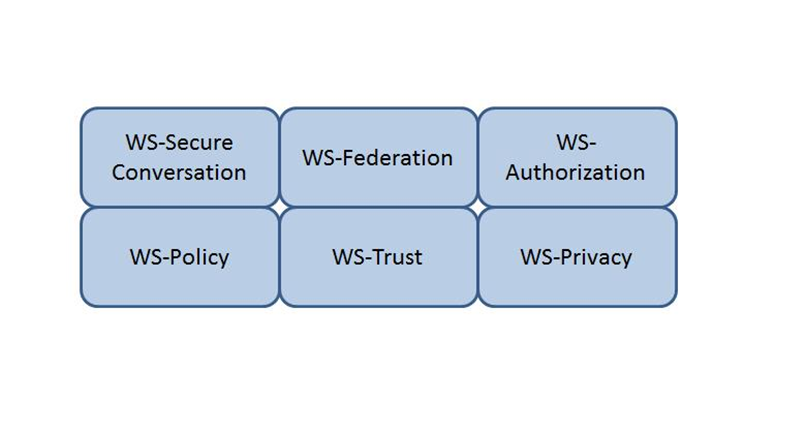
**10. HOTSPOT**

Which Web Services Security (WS-Security) specification negotiates how security tokens will be issued, renewed and validated?

以下哪一个Web服务安全（WS-Security，Web Services Security）规格商定了安全令牌的发布、更新和验证方式？

Click on the correct specification in the image below.

请点击下图中的正确规格。



Answers:

WS-信任（WS-Trust）

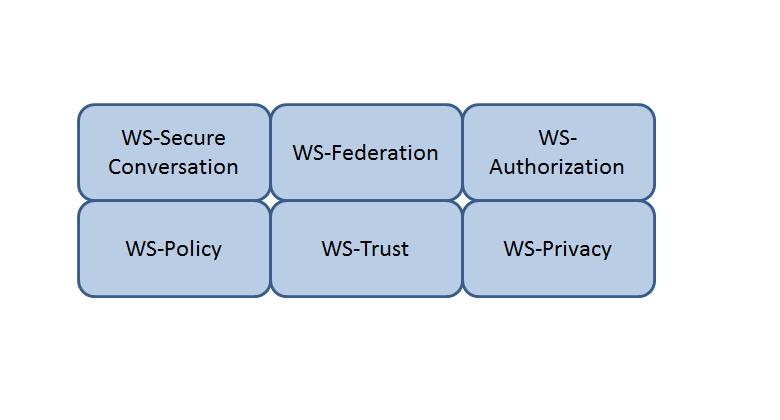
**11. HOTSPOT**

Which Web Services Security (WS-Security) specification maintains a single authenticated identity across multiple dissimilar environments?

以下哪一个Web服务安全（WS-Security，Web Services Security）规格在多个不同的环境中维护单一身份验证标识？

Click on the correct specification in the image below.

请点击下图中的正确规格。



Answer:

WS-Federation

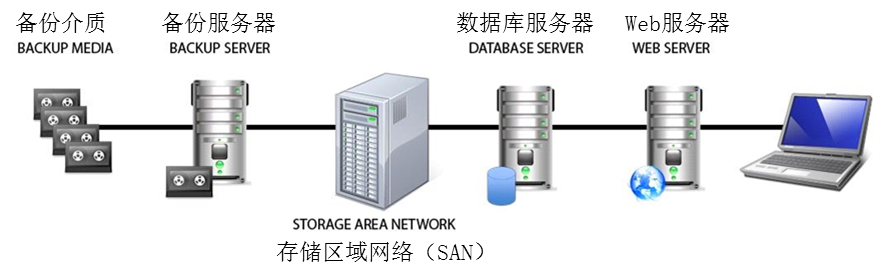
Java Web Services: Up and Running” By Martin Kalin page 228

**12. HOTSPOT**

Identify the component that MOST likely lacks digital accountability related to information access. Click on the correct device in the image below.

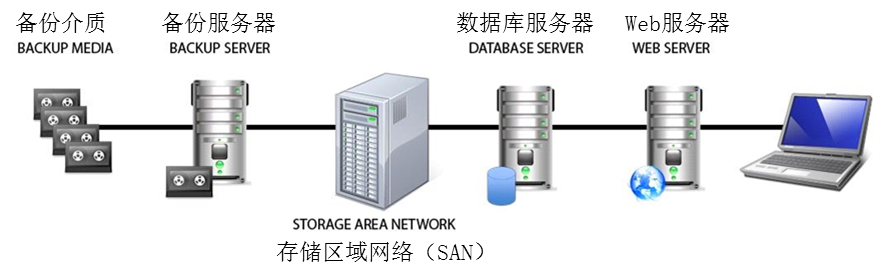
请在以下设备图形中识别出最有可能缺少数字问责性的与信息访问相关的部件。

在如下图形中点击正确的设备。



Answers:

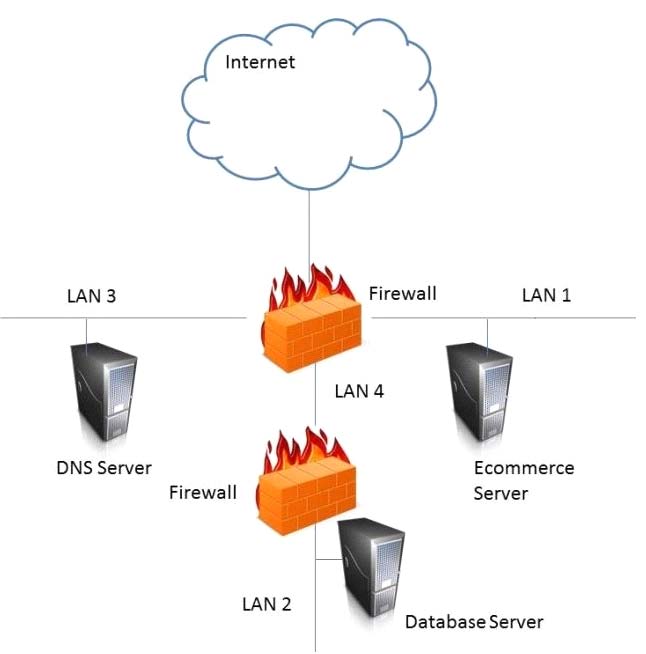
Backup Media（备份介质）



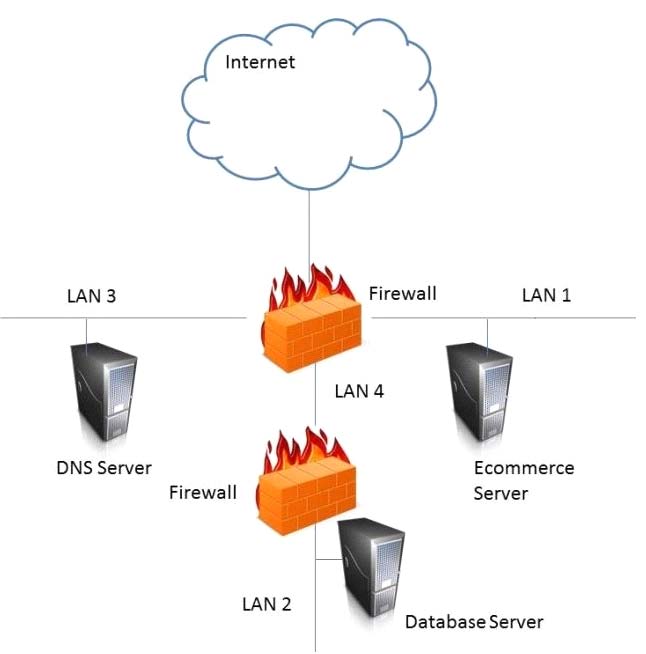
**13. HOTSPOT**

In the network design below, where is the MOST secure Local Area Network (LAN) segment to deploy a Wireless Access Point (WAP) that provides contractors access to the Internet and authorized enterprise services?

需要在下面的网络设计中部署无线接入点（WAP），为承包商提供访问互联网和授权的企业服务，部署在局域网（LAN）的哪一部分最安全？



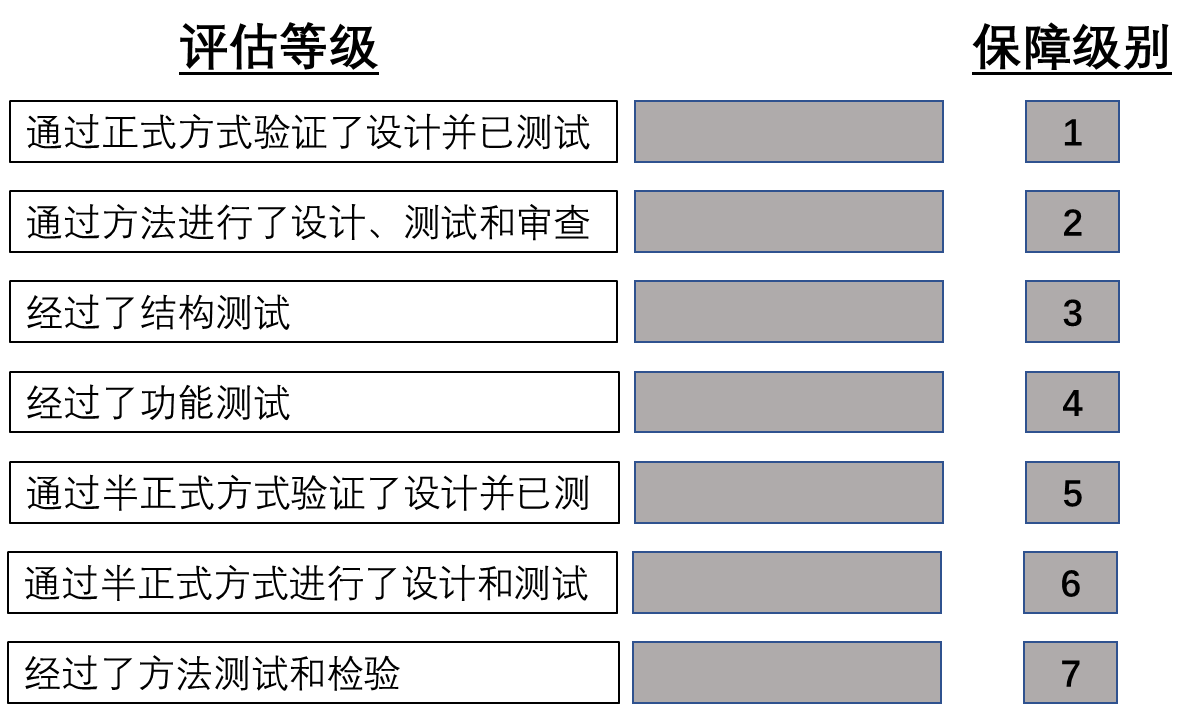
**Answers:** LAN 4



**14. 拖拽题**

将评估等级与其正确的通用准则（CC，Common Criteria）保障级别配对，

将左侧每个评估等级与右侧CC保障级别配对：

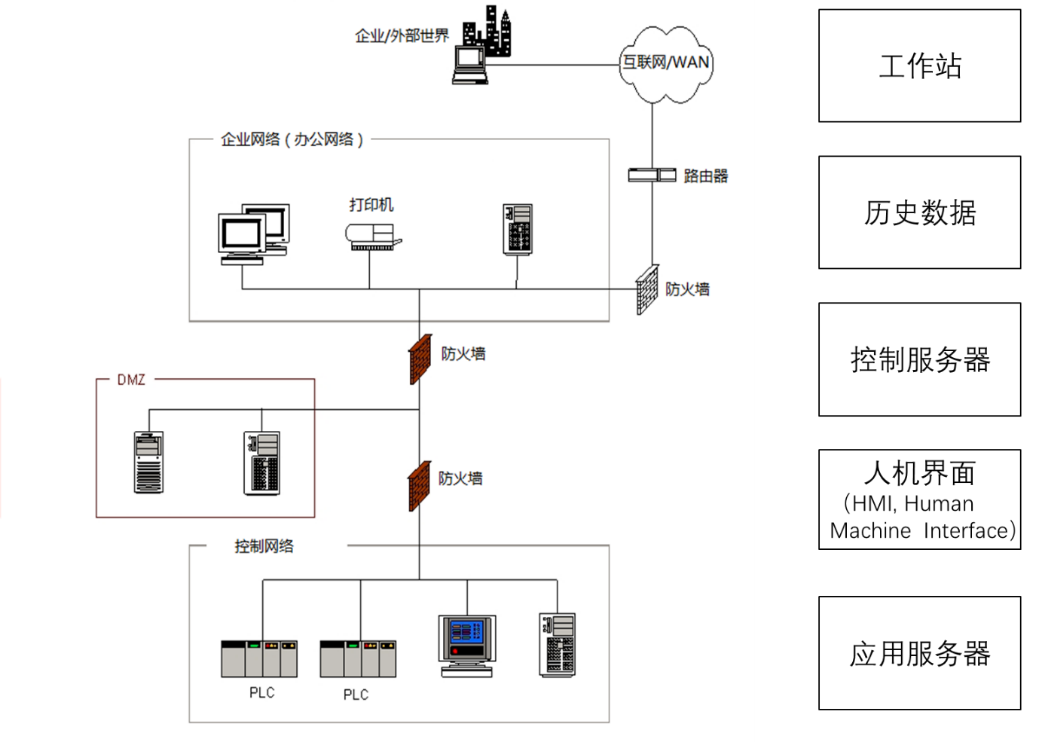


**答案：**

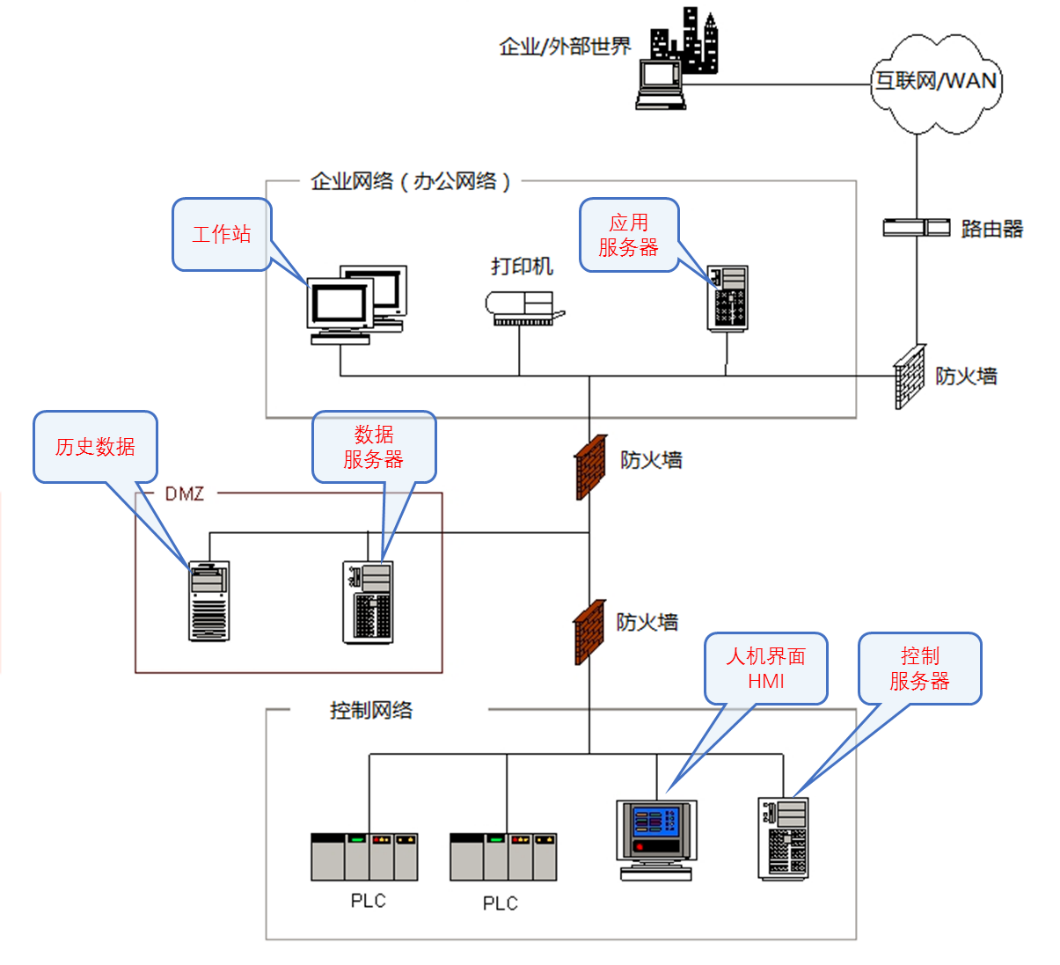
1. 经过了功能测试
2. 经过了结构测试
3. 经过了方法测试和检验
4. 通过方法进行了设计、测试和审查
5. 通过半正式方式进行了设计和测试
6. 通过半正式方式验证了设计并已测
7. 通过正式方式验证了设计并已测试

**15. 拖拽题：**

在国家标准技术研究院(NIST, National Institute Of Standards and Technology)的工业控制系统安全指南中，给定了以下网络安全架构，在合适的位置上放置标签



答案：



**近期有考生回忆说遇到消防相关题目：**

1. 拖拽题：消防材料与着火物质的对应关系



1. 防火门应使用 推杆式的