EXIN

EXIN Information Security Management ISO/IEC 27001

PROFESSIONAL

Certified by EXIN

考试样卷

202309 版本

目录

考试说明

本试卷是 EXIN Information Security Management Professional based on ISO/IEC 27001 (ISMP.CH)模拟考试。 EXIN 考试准则适用于该考试。

本试卷由 30 道单项选择题组成。每道选择题有多个选项，但这些选项中只有一个是正确答案，除非题目中有额外说明。

本试卷的总分是 30 分。每道题的分数是 1 分。您需要获得 20 分或以上通过考试。

考试时间为 90 分钟。

祝您好运!

考试样卷

1 / 30
哪一项是安全战略制定的**关键**要素?

Which is a **key** element of security strategy development?

A) 关于如何支持服务的描述
Description of how the services are being supported

B) 不与组织所在国的法律相冲突的方针
Policy that does not conflict with the law of the organization's country

C) 相关控制目标
Relevant control objectives

D) 投资回报率（ROI）
Return on Investment (ROI)

2 / 30
某组织有多个供应商致力于端到端服务的交付和支持。

该组织应**主要**投资哪项能力，以最大程度地减少源自供应商的信息安全问题?

An organization has several suppliers which contribute to the delivery and support of end-to-end services.

Which capability should the organization invest in **primarily** to minimize the information security issues originating from its suppliers?

A) 审计
Audits

B) 治理
Governance

C) 风险管理
Risk management

D) 培训
Training

3 / 30
安全经理负责确定公司的安全控制。公司正在选择一个供应商来托管面向网络的订购系统。

安全经理应该考量的**最**重要的方面是什么?

The security manager is responsible for defining the security controls for a company. The company is selecting a supplier to host the web-facing ordering system.

What is the **most** important aspect the security manager should look for?

A) 安全关注标准
A standard for due care
B) 尽职调查标准
A standard for due diligence
C) 基准测试
Benchmarking
D) 最佳安全实践
Best security practices

4 / 30
安全控制根据数据元素的安全分级确定。

由谁负责数据元素的安全分级?

Security controls are defined based on the security classification of a data element.

Who is responsible for the security classification of a data element?

A) 负责公司运营的董事会
The board of directors, that runs the company
B) 负责管理数据使用的数据管理员
The data custodian, who manages the use of the data
C) 负责管理流程的流程所有者
The process owner, who governs the process
D) 负责保障信息系统安全的系统所有者
The system owner, who safeguards the information system

5 / 30
某风险经理需要对公司进行完整风险评估。

哪一项是识别公司**大多数**威胁的**最佳**方法?

A risk manager is asked to perform a complete risk assessment for a company.

What is the **best** method to identify **most** of the threats to the company?

A) 与所有利益相关方代表一起集思广益
Have a brainstorm with representatives of all stakeholders

B) 与最高管理层面谈
Interview top management

C) 向所有信息安全相关人员发送威胁识别检查表
Send a checklist for threat identification to all staff involved in information security

6 / 30
目前，一家图书销售公司正在实施信息安全管理。信息安全项目的项目负责人了解到，风险识别过程需要她列出按重要性排列的组织资产清单，她正在与财务经理共同制作这份清单。重要性的权重依据以下标准：对收入的影响（30%）、对利润的影响（40%）、对公众形象的影响（30%）。

财务经理提出了四个重要的信息资产：

- 供应商订单（出货）
- 通过SSL的客户订单（收货）
- 供应商履约建议（收货）
- 通过电子邮件的客户服务请求（收货）

根据影响标准，哪项资产排名最高?

Information security management is currently being implemented in a company that sells books. The project leader for the information security project understands that the risk identification process requires her to list organizational assets arranged in order of importance and she is working with the financial manager to develop this list. The weight of importance is based on the following criteria: impact on revenue (30%), impact on profitability (40%) and impact on public image (30%).

The financial manager has come up with four important information assets:

- Supplier orders (outbound)
- Customer order via SSL (inbound)
- Supplier fulfillment advice (inbound)
- Customer service request via e-mail (inbound)

What asset ranks the highest based on the impact criteria?

A) 供应商订单（出货）
Supplier orders (outbound)

B) 通过SSL的客户订单（收货）
Customer order via SSL (inbound)

C) 供应商履约建议（收货）
Supplier fulfillment advice (inbound)

D) 通过电子邮件的客户服务请求（收货）
Customer service request via e-mail (inbound)

7 / 30
某运营经理希望得到一些关于开设第二个数据中心作为热备份地点的建议。

信息安全官（ISO）会建议该运营经理做什么?

An operations manager wants some advice about opening a second data center as a hot standby location.

What would the information security officer (ISO) advise the operations manager to do?

A) 确保网络和电源有冗余并且由不同的提供商提供
Make sure that network and power supply are made redundant and from different providers
B) 确保物理访问仅授予特定的操作者
Make sure that physical access is only granted to specific operators
C) 确保公司不会成为《爱国者法案》的受害者
Make sure that the company will not be a victim of the Patriot Act legislation
D) 确保该地点具有不同于主地点的物理风险特点
Make sure that the location has a different physical risk profile than the primary location

8 / 30
某大型运输公司采用了信息安全标准，需要针对其将外包的软件开发部门制定控制。公司已经任命了一位外部顾问，确保新的外包情况下，在软件开发的整个供应链上实施符合实施规范的安全控制。

如果供应链中的一个合作伙伴倒闭，应采取什么控制来保证源代码的可用性?

A large transportation company has adopted the standard for information security and needs to set up controls for its software development department, which they will outsource. An external consultant has been appointed to make sure that security controls consistent with the code of practice will be implemented over the complete supply chain for software development in the new outsourced situation.

What control should be put in place to guarantee availability of the source code should one of the partners in the supply chain go out of business?

A) 验收测试
Acceptance testing
B) 有效文档
Effective documentation
C) 托管安排
Escrow arrangements
D) 许可协议
Licensing agreements

9 / 30
风险管理的范围不仅仅局限于组织流程，还应将风险管理嵌入项目管理方法中。例如，应在每个项目的早期阶段进行信息安全风险评估。在实施项目风险管理时，考虑项目的范围十分必要。

标准项目的项目风险管理范围应包括哪些内容?

The scope of risk management is not limited to the organizational processes alone. It should also be embedded in the project management methodology. An information security risk assessment, for example, should be conducted at an early stage of each project. When implementing project risk management, it is necessary to consider the scope of this project.

What should be included in the scope of project risk management for standard projects?

A) 有必要做好最高风险级别的准备，从而实施风险识别、量化、响应制定和响应控制等重要的子流程。
It is necessary to prepare for the maximum risk level and therefore implement important sub-processes like risk identification, quantification, response development and response control.

B) 由于项目组织只是组织的一小部分，因此只需包括针对项目相关威胁和风险的简单识别和评级机制。
It is only necessary to include a simple identification and rating mechanism for the threats and risks specifically related to the project, because a project organization is only a small part of the organization.

C) 范围应包括评估、管理和减少事件影响的必要程序，与信息安全项目一样。
It is should include processes necessary to assess, manage and reduce the impact of occurrences as it would be with an information security project.

10 / 30
当风险评估指出某一特定脆弱性可被利用时，**最好**应实施哪项策略?

Which strategy is **best** to implement when a risk assessment points out that a specific vulnerability can be exploited?

A) 实施风险管理框架
Implementation of a risk management framework

B) 实施信息安全控制
Implementation of an information security control

C) 实施杀毒软件
Implementation of anti-virus software

11 / 30
某组织已说服高级领导层确认需要采用正式的风险管理方法。高级领导层对拟定的风险控制的成本表示了担忧。

哪项说法应包含在实施风险控制的商业论证中?

An organization has convinced its senior leadership of the need for a formal approach to risk management. Senior leadership has raised concerns over the costs of the proposed risk controls.

Which statement should be included in the business case for the implementation of risk controls?

A) 控制是改善组织风险状况的主要手段。
Controls are the primary means of improving the organization’s risk profile.

B) 控制决定组织的风险缓解方案。
Controls determine the organization’s risk mitigation options.

C) 控制帮助组织识别最关键的资产。
Controls help the organization to identify its most critical assets.

D) 控制将为组织提供有关资产脆弱性的信息。
Controls will provide the organization with information about asset vulnerabilities.

12 / 30
某员工曾参与组织风险评估。该评估目的并非实现零残余风险，而是使残余风险符合组织的风险偏好。

风险评估程序何时完成其**主要**目标?

An employee has worked on the organizational risk assessment. The goal of the assessment is not to bring residual risks to zero, but to bring the residual risks in line with an organization’s risk appetite.

When has the risk assessment program accomplished its **primary** goal?

A) 控制实施后
Once the controls are implemented

B) 风险转移完成后
Once the transference of the risk is complete

C) 当决策者获悉存在不受控制的风险，而相关权威团队决定搁置风险时
When decision makers have been informed of uncontrolled risks and proper authority groups decide to leave the risks in place

D) 风险分析完成后
When the risk analysis is completed

13 / 30
信息安全程序的维护是一个持续的过程，需要许多不同的成功影响因素的输入。

哪一种输入影响会要求程序改变?

The maintenance of an information security program requires a continuous process. This requires inputs from the many different factors that will influence its success.

Which is an input influence that would require the process to change?

A) 方针
Policy
B) 风险评估
Risk assessment
C) 安全计划
Security plan

14 / 30
某全球公司的信息安全官（ISO）刚刚接受了信息安全方针的管理评审工作。

评审输出应包括哪些内容?

The information security officer (ISO) for a global company has just received a management review of the information security policy.

What should this output include?

A) 有关各方的反馈
Feedback from interested parties
B) 控制目标和控制的改进情况
Improvement of control objectives and controls
C) 预防和纠正措施的状态
Status of preventive and corrective actions

15 / 30
某组织正在实施信息安全事件处理。该组织已经建立了一个机制，供员工上报发现或怀疑的信息安全事件，但事件上报后并未得到妥善处理。

该组织已经设立了相关的流程、角色和职责，现在正在实施信息安全事件处理所需的其他活动。

哪一项**不是**实施信息安全事件处理的活动?

An organization is implementing information security incident handling. It already has a mechanism for personnel to report observed or suspected information security events, but these are not handled well once they are reported.

The organization has put relevant processes, roles, and responsibilities in place. It is now moving on to implement other activities needed for information security incident handling.

What is **not** an activity to implement information security incident handling?

A) 商定如何通过利用事件中积累的知识来加强和改进信息安全控制，防止发生信息安全事件
Agree how to prevent information security incidents by using knowledge gained from incidents to strengthen and improve information security controls

B) 定义并沟通由有能力的员工执行的信息安全事件响应程序
Define and communicate procedures on information security incident response that should be carried out by competent staff

C) 设计分类和优先级方案，可用于将信息安全事态分类为信息安全事件
Devise a categorization and prioritization scheme that can be used to categorize information security events as information security incidents

D) 实施程序收集和保存与信息安全事件相关的证据，以供任何必要的纪律处分或法律诉讼中使用
Implement procedures to collect and preserve evidence related to information security events for use in any necessary disciplinary or legal actions

E) 建立规则来控制对信息和其他相关资产的物理和逻辑访问，以防止信息安全事件的发生
Set up rules to control physical and logical access to information and other associated assets to prevent information security incidents

16 / 30
安全事件的处理是在信息安全管理指南下，通过事件管理流程完成的。信息安全管理指南要求制定几种类型的缓解计划。

哪项缓解计划涵盖安全事件发生后的短期恢复?

The handling of security incidents is done by the incident management process under guidelines of information security management. These guidelines call for several types of mitigation plans.

Which mitigation plan covers short-term recovery after a security incident has occurred?

A) 业务连续性计划（BCP）
The business continuity plan (BCP)

B) 灾难恢复计划
The disaster recovery plan

C) 事件响应计划
The incident response plan

D) 风险处理计划
The risk treatment plan

17 / 30
协调组织的安全意识活动是谁的责任?

Whose responsibility is it to coordinate an organization’ s security awareness program?

A) 组织的每个人
Everyone in the organization

B) 信息安全管理层
Information security management

C) IT部门
The IT department

D) 首席信息官秘书
The secretary of the CIO

18 / 30
去年，某组织加严对员工的安全控制。在实施额外控制之前，信息安全官（ISO）希望了解员工对信息安全控制的心态。

ISO如何快速获取印象?

Last year an organization became stricter regarding security controls for its employees. Before implementing additional controls, the information security officer (ISO) wants to know the mindset of the employees towards information security controls.

How does the ISO get an impression quickly?

A) 检查互联网数据流
By checking the internet data stream

B) 确定网络是否有病毒
By determining if there are viruses on the network

C) 在正常上班时间后走访办公室
By walking around the office after normal business hours

19 / 30
业务连续性经理要求为应急计划提供意见。

业务连续性经理应**首先**采取什么行动?

The business continuity manager asks for input for the contingency plan.

Which should be the business continuity manager's **first** activity?

A) 界定范围
Define the scope

B) 确定关键业务职能
Identify critical business functions

C) 测试计划
Test the plan

20 / 30
某安全架构师与内部消防小组争论信息安全方针中的表述，即机密区域的门应始终闭锁。应急小组希望在发生火灾时能够进入这些区域。

解决这一难题的**最佳**方案是什么?

A security architect argues with the internal fire prevention team about the statement in the information security policy that doors to confidential areas should be locked at all times. The emergency response team wants access to those areas in case of fire.

What is the **best** solution to this dilemma?

A) 发生火灾时，应保持大门紧闭，防止进入机密区域。
The doors should stay closed in case of fire to prevent access to confidential areas.

B) 发生火灾时门自动打开。
The doors will automatically open in case of fire.

C) 发生火灾时通知安全架构师。
The security architect will be informed when there is a fire.

21 / 30
使用开放设计的安全架构的**主要**优点是什么?

What is the **main** advantage of using an open design of the security architecture?

A) 开放设计易于设置。
Open designs are easy to set up.

B) 开放设计经过多次测试。
Open designs are tested a lot.

C) 开放设计有许多额外功能。
Open designs have a lot of extra features.

22 / 30
关于安全架构的哪项说法是**最**正确的?

Which statement about security architecture is **most** correct?

A) 安全架构完全定义了实施规则。
Security architecture completely defines implementation rules.

B) 安全架构遵循策略。
Security architecture follows strategy.

C) 安全架构是次要的。
Security architecture is secondary.

23 / 30
为什么定义所提供的安全服务很重要?

Why is it important to define which security services will be provided?

A) 更好地协调信息安全要求和客户服务
To better align the information security requirements and the customer service
B) 确定组织的信息安全策略
To determine the information security strategy of an organization
C) 确保组织符合ISO/IEC 27001的要求
To make sure an organization is compliant with the requirements of ISO/IEC 27001
D) 了解信息安全管理体系（ISMS）的范围
To understand the scope of the information security management system (ISMS)

24 / 30
哪个安全项目是为了收集可以表明拒绝服务攻击的大量网络相关流量而设计的?

Which security item is designed to take large collections of network-related traffic that can indicate a denial-of-service attack?

A) 防火墙
Firewall
B) 基于主机的入侵检测防御系统（基于主机的IDPS）
Host-based intrusion detection and prevention system (host-based IDPS)
C) 基于网络的入侵检测防御系统（基于网络的IDPS）
Network-based intrusion detection and prevention system (network-based IDPS)
D) 虚拟专用网络（VPN）
Virtual private network (VPN)

25 / 30
某公司CEO开始使用自己的平板电脑，想要安全经理帮她在平板电脑上使用公司邮箱和日历。安全经理理解这种允许自带设备办公（BYOD）的要求，并组织了有关BYOD的意识培训。

安全经理还应提出哪项控制以防止个人设备被盗或丢失导致数据丢失?

The CEO of a company started using her tablet pc and wants the security manager to facilitate her in using business e-mail and calendar on the tablet. The security manager understands this desire to allow the possibility to Bring Your Own Device (BYOD), and organized an awareness training regarding BYOD.

What other control should the security manager propose to prevent data loss in case of theft or loss of the personal device?

A) 在能够稳定地将企业功能整合到私人设备上之前，不要满足她的需求
Do not grant the wish until stable integration of business functions on private devices is possible

B) 将本地存储和网络连接加密
Encrypt the local storage and network connections

C) 使用一次性密码的令牌实现强身份验证
Implement strong authentication using tokens with one-time passwords

D) 安装反恶意软件和防火墙以防止感染
Install anti-malware and a firewall to prevent infection

26 / 30
为什么IT基础设施中的安全元素很重要?

Why are the security elements in the IT infrastructure important?

A) 实现IT基础设施的业务连续性
To enable business continuity of the IT infrastructure

B) 管理影响IT基础设施的信息安全事件
To manage information security incidents which impact the IT infrastructure

C) 防止对IT基基础设施进行未经授权的物理访问
To prevent unauthorized physical access to the IT infrastructure

D) 保护IT基础设施上的信息资产
To protect the information assets which are on the IT infrastructure

27 / 30
分区是将安全级别不同的物理区域隔离的一种安全控制。安全等级较高的分区可以通过更多的控制来保证安全。某酒店的安全经理负责安全工作，正在考虑为酒店设置分区。

哪些业务功能应合并为一个安全区?

Zoning is a security control to separate physical areas with different security levels. Zones with higher security levels can be secured by more controls. The security manager of a hotel is responsible for security and is considering different zones for the hotel.

What business functions should be combined into one security zone?

A) 会议室和一般办公空间
Boardroom and general office space

B) 健身区和储存设施
Fitness area and storage facility

C) 酒店客房和公共酒吧
Hotel rooms and public bar

D) 公共餐厅和大厅
Public restaurant and lobby

28 / 30
某大公司安全经理的任务是实现对企业数据存储的物理保护。

通过哪项控制可以实现物理保护?

A security manager for a large company has the task to achieve physical protection for corporate data stores.

Through which control can physical protection be achieved?

A) 让访客在企业数据中心签到和签出
Having visitors sign in and out of the corporate datacenter

B) 安装防火墙防止对网络基础设施的访问
Install a firewall to prevent access to the network infrastructure

C) 对需要出入的员工使用钥匙门禁卡控制
Using key access card controls for employees needing access

D) 编写方针来规定可以进入公司的人员
Writing a policy stating who may have access to the company

29 / 30
鉴于物理安全控制是信息安全程序中非常重要的一环，要求信息安全小组为正在建立一些新数据系统的部门设计并实施一个安全边界。

根据ISO/IEC 27001，在建立这个边界时需要考虑的**最**重要准则是什么？

Knowing that physical security controls are a very important part of an information security program, the information security team is asked to design and then implement a security perimeter for a department that is setting up some new data systems.

According to ISO/IEC 27001, which is the **most** important guideline that needs to be considered when establishing this perimeter?

A) 两两支持模式
A two-person support model

B) 安装摄像头和报警器
Installing cameras and alarms

C) 系统记录和监测
System logging and monitoring

D) 边界的强度应与数据值一致
The strength of the perimeter should be in line with the data's value

30 / 30
某组织人力资源经理询问，在雇佣和招聘方面，她如何做才能快速有效地帮助组织按照ISO/IEC 27001加强数据安全程序。

哪一项应作为建议？

The human resource manager for an organization asked what she could do as a quick win in the area of employment and hiring to help strengthen the organization’s data security program according to ISO/IEC 27001.

What should the advice be?

A) 做背景调查
Do background checks

B) 实施安全方针
Implement security policy

C) 在入口处设置旋转门
Place revolving gates at the entrance

答案解析

1 / 30
哪一项是安全战略制定的**关键**要素?

Which is a **key** element of security strategy development?

A) 关于如何支持服务的描述
Description of how the services are being supported

B) 不与组织所在国的法律相冲突的方针
Policy that does not conflict with the law of the organization's country

C) 相关控制目标
Relevant control objectives

D) 投资回报率（ROI）
Return on Investment (ROI)

A) 错误。这个答案与确定总体安全策略无关，更多的是关注服务级别协议（SLA）。
Incorrect. This answer does not pertain to defining an overall security strategy and is more focused on the service level agreement (SLA).

B) 错误。这个答案与确定总体安全策略无关，更多是与方针制定相关。
Incorrect. This answer does not pertain to defining an overall security strategy and is more related to policy development.

C) 正确。制定相关的控制目标是制定安全战略的关键因素。（文献：A，幻灯片第013张）
Correct. Having relevant control objectives is a key element to the development of security strategy. (Literature: A, Slide 013)

D) 错误。这个答案与确定总体安全战略无关，更多是与财务预测和预算编制相关。
Incorrect. This answer does not pertain to defining an overall security strategy and is more related to financial forecasting and budgeting.

2 / 30
某组织有多个供应商致力于端到端服务的交付和支持。

该组织应**主要**投资哪项能力，以最大程度地减少源自供应商的信息安全问题？

An organization has several suppliers which contribute to the delivery and support of end-to-end services.

Which capability should the organization invest in **primarily** to minimize the information security issues originating from its suppliers?

A) 审计
Audits

B) 治理
Governance

C) 风险管理
Risk management

D) 培训
Training

A) 错误。审计对确保已约定的活动得到执行必不可少，但更好的投资是加强治理能力，以确保有方针指导服务提供所涉各方的行为。
Incorrect. Audits are essential to ensure that agreed activities are being performed, but it would be better to invest in governance capabilities to ensure that there are policies which direct the behavior of all parties involved in the service provision.

B) 正确。治理是指导组织的方针和流程（包括供应商的参与）的表层能力。治理负责组织在信息安全等方面的评价、指导和监控。治理工作包括制定方针、接收监控信息、根据组织方针评价信息，并向管理层提供指导以在必要时进行变更。（文献：A，幻灯片第018张）
Correct. Governance is the overlying capability which directs an organization’s policies and processes, including the suppliers’ involvement. Governance handles the evaluation, direction and monitoring of the organization in topics like information security. Governance works on developing policies, receiving monitoring information, evaluating this information based on the policies of the organization, and providing direction to management to make changes where necessary. (Literature: A, Slide 018)

C) 错误。风险管理有许多在本例情况下有用的活动，但加强组织的治理能力将更有可能增强对服务提供所涉各方的活动的总体控制。
Incorrect. Risk management has a number of activities which would be useful in this scenario, but strengthening the organization’s governance capabilities will increase the likelihood of stronger overall control of the activities of all parties involved in service provision.

D) 错误。投资培训很重要，但强大的治理能力将帮助组织制定方针，指导服务提供所涉各方的行为。
Incorrect. It is important to invest in training, but a robust governance capability will help the organization to develop policies which direct the behavior of all parties involved in service provision.

3 / 30
安全经理负责确定公司的安全控制。公司正在选择一个供应商来托管面向网络的订购系统。

安全经理应该考量的**最**重要的方面是什么?

The security manager is responsible for defining the security controls for a company. The company is selecting a supplier to host the web-facing ordering system.

What is the **most** important aspect the security manager should look for?

A) 安全关注标准
A standard for due care
B) 尽职调查标准
A standard for due diligence
C) 基准测试
Benchmarking
D) 最佳安全实践
Best security practices

A) 错误。安全关注标准是最低的安全级别。
Incorrect. A standard for due care symbolizes a minimum level of security.
B) 错误。尽职调查意味着供应商符合标准要求，这不一定是标准。
Incorrect. Due diligence means that the supplier meets a standard requirement. This is not necessarily the standard.
C) 错误。基准测试是一种用于比较业务、成熟度和市场相似的组织的方法。
Incorrect. Benchmarking is a technique used to compare organizations with similar business, maturity and markets.
D) 正确。最佳安全实践是某一行业或工作领域的同类之最，是安全经理对供应商应考量的要求。（文献：A，幻灯片第024张）
Correct. Best security practices are the best in class for a given industry or line of work. This is what the security manager will be looking for in a supplier. (Literature: A, Slide 024)

4 / 30
安全控制根据数据元素的安全分级确定。

由谁负责数据元素的安全分级?

Security controls are defined based on the security classification of a data element.

Who is responsible for the security classification of a data element?

A) 负责公司运营的董事会
The board of directors, that runs the company

B) 负责管理数据使用的数据管理员
The data custodian, who manages the use of the data

C) 负责管理流程的流程所有者
The process owner, who governs the process

D) 负责保障信息系统安全的系统所有者
The system owner, who safeguards the information system

A) 错误。董事会对任何业务流程全面负责，但行使所有职责的责任被下放。
Incorrect. The board is overall accountable for any business process, but the responsibility for exercising all duties is delegated.

B) 错误。管理员负责确定和管理涉及法律法规遵守的任何数据元素的要求，还负责各方和各程序以数据合同形式使用数据。
Incorrect. A custodian is responsible for defining and managing the requirements towards any data element as far as it concerns compliancy to laws and regulations, but also for the use of data by different parties and processes in the form of data contracts.

C) 正确。任何数据元素都是业务流程的控制对象。流程所有者是唯一能确定一个数据元素在组织内是否至关重要的人。（文献：A，幻灯片第045张）
Correct. Any data element is an object of control of a business process. The process owner is the only person who can identify if a data element is critical within the organization. (Literature: A, Slide 045)

D) 错误。系统所有者负责实施所定义的机密性、完整性、可用性（CIA）分级所要求的控制。
Incorrect. The system owner is responsible for implementing the controls as required by the defined confidentiality, integrity, availability (CIA) classification.

5 / 30
某风险经理需要对公司进行完整风险评估。

哪一项是识别公司**大多数**威胁的**最佳**方法?

A risk manager is asked to perform a complete risk assessment for a company.

What is the **best** method to identify **most** of the threats to the company?

A) 与所有利益相关方代表一起集思广益
Have a brainstorm with representatives of all stakeholders

B) 与最高管理层面谈
Interview top management

C) 向所有信息安全相关人员发送威胁识别检查表
Send a checklist for threat identification to all staff involved in information security

A) 正确。与所有利益相关方一起集思广益可确保所有观点都得到体现。（文献：A，幻灯片第030张）
Correct. A brainstorm with all stakeholders makes sure that all perspectives are represented. (Literature: A, Slide 030)

B) 错误。最高管理层可以监督多项威胁，但无法监督全部威胁。识别更多威胁有更好的方法。
Incorrect. Top management can oversee a lot of threats but not all of them. There is a better way to identify more threats.

C) 错误。信息安全相关人员无法监督所有威胁。识别更多威胁有更好的方法。
Incorrect. Staff involved in information security cannot see all the threats. There is a better way to identify more threats.

6 / 30
目前，一家图书销售公司正在实施信息安全管理。信息安全项目的项目负责人了解到，风险识别过程需要她列出按重要性排列的组织资产清单，她正在与财务经理共同制作这份清单。重要性的权重依据以下标准：对收入的影响（30%）、对利润的影响（40%）、对公众形象的影响（30%）。

财务经理提出了四个重要的信息资产：

- 供应商订单（出货）
- 通过SSL的客户订单（收货）
- 供应商履约建议（收货）
- 通过电子邮件的客户服务请求（收货）

根据影响标准，哪项资产排名最高?

Information security management is currently being implemented in a company that sells books. The project leader for the information security project understands that the risk identification process requires her to list organizational assets arranged in order of importance and she is working with the financial manager to develop this list. The weight of importance is based on the following criteria: impact on revenue (30%), impact on profitability (40%) and impact on public image (30%).

The financial manager has come up with four important information assets:

- Supplier orders (outbound)
- Customer order via SSL (inbound)
- Supplier fulfillment advice (inbound)
- Customer service request via e-mail (inbound)

What asset ranks the highest based on the impact criteria?

A) 供应商订单（出货）
Supplier orders (outbound)

B) 通过SSL的客户订单（收货）
Customer order via SSL (inbound)

C) 供应商履约建议（收货）
Supplier fulfillment advice (inbound)

D) 通过电子邮件的客户服务请求（收货）
Customer service request via e-mail (inbound)

（题目未完，接下一页）

A) 错误。当供应商订单发不出去时，将对能否创造收入和利润产生巨大影响。但是，这会导致客户订单延迟。有些客户可能会转向竞争对手求购，这也将影响到利润和公众形象。正常情况下，还是会实现收入和利润。
Incorrect. When supplier orders cannot be sent out, it will have a high impact on the possibility to create revenue and make profit. However, it will cause customer orders to be delayed. Some customers may move their purchase to a competitor. This will also impact on profitability and public image. Normally, revenue and profit will still be realized.

B) 正确。当客户无法在网上下单时，会立即从其他渠道下单，将对收入、利润和公众形象产生极大影响。（文献：A，幻灯片第037张）
Correct. When a customer is not able to order online, they will immediately order from another source. The impact on revenue, profitability and public image will be maximal. (Literature: A, Slide 037)

C) 错误。当供应商通知交货订单发不出去时，将对能否创造收入和实现利润产生巨大影响。此外，这还会导致客户订单延迟。有些客户可能会转向竞争对手求购，这也将影响到利润和公众形象。收入和利润最终会实现。
Incorrect. When supplier delivery on call orders cannot be sent out, it will have a high impact on the possibility to create revenue and make profit. Besides, it will cause customer orders to be delayed. Some customers may move their purchase to a competitor. This will also impact on profitability and public image. Eventually, revenue and profit will be realized.

D) 错误。当客户服务请求不能得到满足时，将对公众形象造成巨大影响。这对收入和利润的影响远低于物流过程出现问题因素所带来的影响。
Incorrect. When customer service requests cannot be fulfilled, it will have a high impact on public image. The impact on revenue and profitability will be significantly lower than compared to elements of the logistics process failing.

7 / 30
某运营经理希望得到一些关于开设第二个数据中心作为热备份地点的建议。

信息安全官（ISO）会建议该运营经理做什么?

An operations manager wants some advice about opening a second data center as a hot standby location.

What would the information security officer (ISO) advise the operations manager to do?

A) 确保网络和电源有冗余并且由不同的提供商提供
Make sure that network and power supply are made redundant and from different providers

B) 确保物理访问仅授予特定的操作者
Make sure that physical access is only granted to specific operators

C) 确保公司不会成为《爱国者法案》的受害者
Make sure that the company will not be a victim of the Patriot Act legislation

D) 确保该地点具有不同于主地点的物理风险特点
Make sure that the location has a different physical risk profile than the primary location

A) 错误。这只是风险特点的一部分。
Incorrect. This is only part of the risk profile.

B) 错误。这是一般安全控制。
Incorrect. This is a general security control.

C) 错误。这不属于物理安全风险，而是一个法律问题。
Incorrect. This is not a physical security risk. It is a legislation problem.

D) 正确。作为备份地点，最好确保有不同的风险特点。（文献：A，幻灯片第050张）
Correct. Since it is a backup location, it is wise to make sure that it has a different risk profile. (Literature: A, Slide 050)

8 / 30
某大型运输公司采用了信息安全标准，需要针对其将外包的软件开发部门制定控制。公司已经任命了一位外部顾问，确保新的外包情况下，在软件开发的整个供应链上实施符合实施规范的安全控制。

如果供应链中的一个合作伙伴倒闭，应采取什么控制来保证源代码的可用性?

A large transportation company has adopted the standard for information security and needs to set up controls for its software development department, which they will outsource. An external consultant has been appointed to make sure that security controls consistent with the code of practice will be implemented over the complete supply chain for software development in the new outsourced situation.

What control should be put in place to guarantee availability of the source code should one of the partners in the supply chain go out of business?

A) 验收测试
Acceptance testing

B) 有效文档
Effective documentation

C) 托管安排
Escrow arrangements

D) 许可协议
Licensing agreements

A) 错误。验收测试是一种确保开发过程中的交付物符合客户质量标准的机制。客户无法获得源代码。
Incorrect. Acceptance testing is a mechanism to ensure that the deliverables of the development process meet the quality criteria of the customer. The customer gets no access to the source code.

B) 错误。有效文档是所有控制的一般要求。源代码不属于客户可访问的文档。
Incorrect. Effective documentation is a general requirement for all controls. Source code is not part of documentation that is accessible to the customer.

C) 正确。托管安排将确保软件源代码存储在一个第三方站点。当满足一定的标准时，例如供应商接受了破产管理，客户可以访问源代码。（文献：A，幻灯片第050张）
Correct. Escrow arrangements will ensure that software source code is stored at a neutral site. The source code is accessible to the customer when certain criteria are met, for example if the supplier goes into receivership. (Literature: A, Slide 050)

D) 错误。许可协议只是确保代码所有权和知识产权。如果供应商倒闭，许可协议不能保证客户获得源代码。
Incorrect. Licensing agreements only ensure code ownership and intellectual property rights. They cannot guarantee access to the source code for the customer should the supplier go out of business.

9 / 30
风险管理的范围不仅仅局限于组织流程，还应将风险管理嵌入项目管理方法中。例如，应在每个项目的早期阶段进行信息安全风险评估。在实施项目风险管理时，考虑项目的范围十分必要。

标准项目的项目风险管理范围应包括哪些内容?

The scope of risk management is not limited to the organizational processes alone. It should also be embedded in the project management methodology. An information security risk assessment, for example, should be conducted at an early stage of each project. When implementing project risk management, it is necessary to consider the scope of this project.

What should be included in the scope of project risk management for standard projects?

A) 有必要做好最高风险级别的准备，从而实施风险识别、量化、响应制定和响应控制等重要的子流程。
It is necessary to prepare for the maximum risk level and therefore implement important sub-processes like risk identification, quantification, response development and response control.

B) 由于项目组织只是组织的一小部分，因此只需包括针对项目相关威胁和风险的简单识别和评级机制。
It is only necessary to include a simple identification and rating mechanism for the threats and risks specifically related to the project, because a project organization is only a small part of the organization.

C) 范围应包括评估、管理和减少事件影响的必要程序，与信息安全项目一样。
It is should include processes necessary to assess, manage and reduce the impact of occurrences as it would be with an information security project.

A) 错误。实施各种可能的子流程只适用于高风险的项目情况，如安全项目或任务关键环境。仅这类环境才适用通用方法。
Incorrect. Implementation of all possible sub-processes is only applicable to high-risk project scenarios like security projects or in mission critical environments. Only in those environments it should be the generic approach.

B) 正确。一般来说，这个范围对大多数项目已经足够。不过，有必要顾及到更大型、更关键的项目，因此，对于更大型/更综合的企业项目，还应有一个程序升级到更细致的风险管理程序。因此，有必要像针对整个组织一样实施通用范围。（文献：A，幻灯片第047张）
Correct. Generally, this scope should be sufficient for most projects. That said, it is necessary to allow for larger and more critical projects, so there should also be a process to escalate to more detailed risk management processes for larger/more comprehensive enterprise projects. Therefore, it is necessary to implement a generic scope like is done for the organization as a whole. (Literature: A, Slide 047)

C) 错误。项目风险管理与一般的风险管理非常相似。相应地，通用范围应是相似的。在许多情况下，只需采取简单的方法，仅识别和评定项目所面临的具体威胁。
Incorrect. Project risk management is very similar to normal risk management. The generic scope should therefore be similar. On many occasions a simple approach will only be necessary, identifying and rating only those threats specifically facing the project.

10 / 30
当风险评估指出某一特定脆弱性可被利用时，**最好**应实施哪项策略？

Which strategy is **best** to implement when a risk assessment points out that a specific vulnerability can be exploited?

A) 实施风险管理框架
Implementation of a risk management framework

B) 实施信息安全控制
Implementation of an information security control

C) 实施杀毒软件
Implementation of anti-virus software

A) 错误。风险管理框架是一种风险方法，而不是策略。
Incorrect. A risk management framework is a risk methodology and not a strategy.

B) 正确。必须实施控制，以尽量减少组织风险。（文献：A，幻灯片第033张）
Correct. Controls must be implemented in order to minimize the organizational risks. (Literature: A, Slide 033)

C) 错误。尽管杀毒软件可以帮助组织抵御病毒和恶意软件，但这并不是解决所有风险的方法。
Incorrect. Although anti-virus software helps organizations to be protected against viruses and malwares, this is not the solution for all the risks.

11 / 30
某组织已说服高级领导层确认需要采用正式的风险管理方法。高级领导层对拟定的风险控制的成本表示了担忧。

哪项说法应包含在实施风险控制的商业论证中?

An organization has convinced its senior leadership of the need for a formal approach to risk management. Senior leadership has raised concerns over the costs of the proposed risk controls.

Which statement should be included in the business case for the implementation of risk controls?

A) 控制是改善组织风险状况的主要手段。
Controls are the primary means of improving the organization’s risk profile.

B) 控制决定组织的风险缓解方案。
Controls determine the organization’s risk mitigation options.

C) 控制帮助组织识别最关键的资产。
Controls help the organization to identify its most critical assets.

D) 控制将为组织提供有关资产脆弱性的信息。
Controls will provide the organization with information about asset vulnerabilities.

A) 正确。信息安全主要可以通过实施控制进行改善。（文献：A，幻灯片第050张和第051张）
Correct. Information security can primarily be improved by implementing controls. (Literature: A, Slide 050 and 051)

B) 错误。这是风险评估的好处，而不是实施控制的好处。
Incorrect. This is a benefit of risk assessment, not implementing controls.

C) 错误。这是风险评估的好处，而不是实施控制的好处。
Incorrect. This is a benefit of risk assessment, not implementing controls.

D) 错误。这是识别威胁的好处，而不是实施控制的好处。
Incorrect. This is a benefit of identifying threats, not implementing controls.

12 / 30
某员工曾参与组织风险评估。该评估目的并非实现零残余风险，而是使残余风险符合组织的风险偏好。

风险评估程序何时完成其**主要**目标?

An employee has worked on the organizational risk assessment. The goal of the assessment is not to bring residual risks to zero, but to bring the residual risks in line with an organization’ s risk appetite.

When has the risk assessment program accomplished its **primary** goal?

A) 控制实施后
Once the controls are implemented

B) 风险转移完成后
Once the transference of the risk is complete

C) 当决策者获悉存在不受控制的风险，而相关权威团队决定搁置风险时
When decision makers have been informed of uncontrolled risks and proper authority groups decide to leave the risks in place

D) 风险分析完成后
When the risk analysis is completed

A) 错误。如无持续监控，控制将随着时间的推移而退化，风险将超出组织的风险偏好。
Incorrect. If there is no ongoing monitoring of the controls, they will deteriorate over time and the risk will exceed the organizational risk appetite.

B) 错误。风险转移只是控制风险的方法之一，本题问的是整个控制结构。
Incorrect. Risk transference is only one of the methods used to control risks. This question is asking about the entirety of the control structure.

C) 正确。信息安全专业人士必须确保残余风险保持在组织风险偏好的范围内，这一点很重要。（文献：A，幻灯片第030张）
Correct. It is important that information security professionals make sure that the remaining risks are maintained within the bounds of the organization's risk appetite. (Literature: A, Slide 030)

D) 错误。当风险分析完成后，真正的风险管理工作才刚刚开始。
Incorrect. When the risk analysis is completed, the real risk management work is just starting.

13 / 30
信息安全程序的维护是一个持续的过程，需要许多不同的成功影响因素的输入。

哪一种输入影响会要求程序改变?

The maintenance of an information security program requires a continuous process. This requires inputs from the many different factors that will influence its success.

Which is an input influence that would require the process to change?

A) 方针
Policy
B) 风险评估
Risk assessment
C) 安全计划
Security plan

A) 错误。方针是程序的输出，不是输入。
Incorrect. Policy is an output of the program. It is not an input.
B) 正确。风险评估是一种需要对过程进行调整的输入改变。（文献：A，幻灯片第033张）
Correct. Risk assessment is a change in input which requires adaption of the process. (Literature: A, Slide 033)
C) 错误。安全计划是程序的输出，不是输入。
Incorrect. The security plan is an output of the program. It is not an input.

14 / 30
某全球公司的信息安全官（ISO）刚刚接受了信息安全方针的管理评审工作。

评审输出应包括哪些内容?

The information security officer (ISO) for a global company has just received a management review of the information security policy.

What should this output include?

A) 有关各方的反馈
Feedback from interested parties
B) 控制目标和控制的改进情况
Improvement of control objectives and controls
C) 预防和纠正措施的状态
Status of preventive and corrective actions

A) 错误。这是信息安全方针管理评审的输入。
Incorrect. This is input to a management review of the information security policy.
B) 正确。这项应包括在输出中。（文献：A，幻灯片第060张）
Correct. This should be included in the output. (Literature: A, Slide 060)
C) 错误。这是信息安全方针管理评审的输入。
Incorrect. This is input to a management review of the information security policy.

15 / 30
某组织正在实施信息安全事件处理。该组织已经建立了一个机制，供员工上报发现或怀疑的信息安全事件，但事件上报后并未得到妥善处理。

该组织已经设立了相关的流程、角色和职责，现在正在实施信息安全事件处理所需的其他活动。

哪一项**不是**实施信息安全事件处理的活动?

An organization is implementing information security incident handling. It already has a mechanism for personnel to report observed or suspected information security events, but these are not handled well once they are reported.

The organization has put relevant processes, roles, and responsibilities in place. It is now moving on to implement other activities needed for information security incident handling.

What is **not** an activity to implement information security incident handling?

A) 商定如何通过利用事件中积累的知识来加强和改进信息安全控制，防止发生信息安全事件
Agree how to prevent information security incidents by using knowledge gained from incidents to strengthen and improve information security controls

B) 定义并沟通由有能力的员工执行的信息安全事件响应程序
Define and communicate procedures on information security incident response that should be carried out by competent staff

C) 设计分类和优先级方案，可用于将信息安全事态分类为信息安全事件
Devise a categorization and prioritization scheme that can be used to categorize information security events as information security incidents

D) 实施程序收集和保存与信息安全事件相关的证据，以供任何必要的纪律处分或法律诉讼中使用
Implement procedures to collect and preserve evidence related to information security events for use in any necessary disciplinary or legal actions

E) 建立规则来控制对信息和其他相关资产的物理和逻辑访问，以防止信息安全事件的发生
Set up rules to control physical and logical access to information and other associated assets to prevent information security incidents

A) 错误。这是实施信息安全事件处理的一环。
Incorrect. This is part of implementing information security incident handling.

B) 错误。这是实施信息安全事件处理的一环。
Incorrect. This is part of implementing information security incident handling.

C) 错误。这是实施信息安全事件处理的一环。
Incorrect. This is part of implementing information security incident handling.

D) 错误。这是实施信息安全事件处理的一环。
Incorrect. This is part of implementing information security incident handling.

E) 正确。实施访问控制可以支持事件的预防，但不是实施信息安全事件处理的一环。（文献：A，幻灯片第085张和第094张）
Correct. Implementing access control can support the prevention of incidents but is not part of implementing information security incident handling. (Literature: A, Slides 085 and 094)

16 / 30
安全事件的处理是在信息安全管理指南下，通过事件管理流程完成的。信息安全管理指南要求制定几种类型的缓解计划。

哪项缓解计划涵盖安全事件发生后的短期恢复?

The handling of security incidents is done by the incident management process under guidelines of information security management. These guidelines call for several types of mitigation plans.

Which mitigation plan covers short-term recovery after a security incident has occurred?

A) 业务连续性计划（BCP）
The business continuity plan (BCP)

B) 灾难恢复计划
The disaster recovery plan

C) 事件响应计划
The incident response plan

D) 风险处理计划
The risk treatment plan

A) 错误。BCP是在确定灾难影响业务运作后部署的，其目标是确保长期组织适当的措施，以确保业务流程的连续性。
Incorrect. The BCP is deployed after the disaster is determined to affect business operation. Its goal is to ensure long-term organization of appropriate measures to ensure the continuity of business processes.

B) 正确。灾难恢复计划涵盖短期恢复，并在事件被标记为灾难后立即执行。（文献：A，幻灯片第081张）
Correct. The disaster recovery plan covers short-term recovery and is executed immediately after the incident is labeled a disaster. (Literature: A, Slide 081)

C) 错误。事件响应计划的时间范围是即时/实时。它在安全事件发生时执行。
Incorrect. The time frame for the incident response plan is immediate/real-time. It is executed when a security incident unfolds.

D) 错误。风险处理计划是信息安全改进计划的一种。改进计划通常每年执行一次。
Incorrect. The risk treatment plan is a type of information security improvement plan. Improvement plans are usually executed on an annual basis.

17 / 30
协调组织的安全意识活动是谁的责任?

Whose responsibility is it to coordinate an organization’ s security awareness program?

A) 组织的每个人
Everyone in the organization

B) 信息安全管理层
Information security management

C) IT部门
The IT department

D) 首席信息官秘书
The secretary of the CIO

A) 错误。虽然组织中的每个人都对组织安全负责，但他们并不负责协调组织的安全意识活动。
Incorrect. While everyone in the organization is responsible for organizational security, they are not responsible for coordinating the organization’ s security awareness program.

B) 正确。信息安全管理层负责协调安全意识活动。（文献：A，幻灯片第095张）
Correct. Information security management is responsible for coordinating the security awareness campaign. (Literature: A, Slide 095)

C) 错误。虽然IT部门需要宣传和了解安全问题，但他们并不负责协调组织的安全意识活动。
Incorrect. While the IT department needs to promote and be aware of security issues and concerns, they are not responsible for coordinating the organization’ s security awareness campaign.

D) 错误。CIO秘书可能负责宣传和倡导意识，但不直接负责协调组织的安全意识活动。
Incorrect.The secretary of the CIO may be responsible for promoting and championing awareness but is not directly responsible for coordinating the organization’ s security awareness program.

18 / 30
去年，某组织加严对员工的安全控制。在实施额外控制之前，信息安全官（ISO）希望了解员工对信息安全控制的心态。

ISO如何快速获取印象?

Last year an organization became stricter regarding security controls for its employees. Before implementing additional controls, the information security officer (ISO) wants to know the mindset of the employees towards information security controls.

How does the ISO get an impression quickly?

A) 检查互联网数据流
By checking the internet data stream

B) 确定网络是否有病毒
By determining if there are viruses on the network

C) 在正常上班时间后走访办公室
By walking around the office after normal business hours

A) 错误。这种做法只提供了关于上网的信息，无法了解到员工的一般心态。
Incorrect. This only gives information about how the internet is being used, not about the general mindset of employees.

B) 错误。这是一种技术措施，并不能提供任何有关员工心态的信息。
Incorrect. This is a technical measure and gives no information about the mindset of the employees.

C) 正确。当ISO在正常上班时间后走访办公室时，可能会看到员工如何处理敏感信息。（文献：A，幻灯片第095张）
Correct. When the ISO walks around the office after normal business hours, it is possible to see how employees handle sensitive information. (Literature: A, Slide 095)

19 / 30
业务连续性经理要求为应急计划提供意见。

业务连续性经理应**首先**采取什么行动?

The business continuity manager asks for input for the contingency plan.

Which should be the business continuity manager's **first** activity?

A) 界定范围
Define the scope

B) 确定关键业务职能
Identify critical business functions

C) 测试计划
Test the plan

A) 错误。范围是项目管理的支柱，而不是应急计划的基石，因为范围是由业务影响分析（BIA）的结果驱动的。
Incorrect. Scope is a pillar of project management and not a cornerstone for contingency planning as the scope is driven by the results of the business impact analysis (BIA).

B) 正确。要制定应急计划，主要是企业必须完成对其关键业务职能和系统的定义，并做好记录。（文献：A，幻灯片第080张）
Correct. The main thing that must be completed in order to have a contingency plan is for the business to define their critical business functions and systems and document these. (Literature: A, Slide 080)

C) 错误。测试应急计划是极其重要的，至少需要每年进行一次，但这不是第一项活动。
Incorrect. Testing of the contingency plan is extremely important and needs to take place at least annually, however it is not the first activity.

20 / 30
某安全架构师与内部消防小组争论信息安全方针中的表述，即机密区域的门应始终闭锁。应急小组希望在发生火灾时能够进入这些区域。

解决这一难题的**最佳**方案是什么?

A security architect argues with the internal fire prevention team about the statement in the information security policy that doors to confidential areas should be locked at all times. The emergency response team wants access to those areas in case of fire.

What is the **best** solution to this dilemma?

A) 发生火灾时，应保持大门紧闭，防止进入机密区域。
The doors should stay closed in case of fire to prevent access to confidential areas.
B) 发生火灾时门自动打开。
The doors will automatically open in case of fire.
C) 发生火灾时通知安全架构师。
The security architect will be informed when there is a fire.

A) 错误。安全优先于保密。
Incorrect. Safety comes before security.
B) 正确。安全优先于保密。（文献：A，幻灯片第091张）
Correct. Safety comes before security. (Literature: A, Slide 091)
C) 错误。尽管通知安全架构师很重要，但应急小组不能等到安全架构师到达现场才开始处理问题。
Incorrect. Although it is good to be informed, the emergency response team cannot wait until the security architect has arrived at the scene.

21 / 30
使用开放设计的安全架构的**主要**优点是什么?

What is the **main** advantage of using an open design of the security architecture?

A) 开放设计易于设置。
Open designs are easy to set up.
B) 开放设计经过多次测试。
Open designs are tested a lot.
C) 开放设计有许多额外功能。
Open designs have a lot of extra features.

A) 错误。开放设计并不比秘密设计更容易设置。
Incorrect. Open designs are not set up easier than secret designs.
B) 正确。开放设计经过广泛测试，而且秘密设计从来不会保持秘密。（文献：A，幻灯片第114张）
Correct. Open designs are tested extensively, and moreover secret designs never stay secret. (Literature: A, Slide 114)
C) 错误。开放设计不一定比秘密设计有更多功能。
Incorrect. Open designs do not necessarily have more features than secret designs.

22 / 30
关于安全架构的哪项说法是**最**正确的?

Which statement about security architecture is **most** correct?

A) 安全架构完全定义了实施规则。
Security architecture completely defines implementation rules.

B) 安全架构遵循策略。
Security architecture follows strategy.

C) 安全架构是次要的。
Security architecture is secondary.

A) 错误。安全架构是比这更高层次的设计，并不能完全定义实施规则。
Incorrect. Security architecture is higher-level design than this and does not completely define the implementation rules.

B) 正确。安全架构遵循信息安全策略。（文献：A，幻灯片第112张）
Correct. Security architecture follows information security strategy. (Literature: A, Slide 112)

C) 错误。安全架构是策略性的，因此不是次要的。
Incorrect. Security architecture is strategic and therefore not secondary.

23 / 30
为什么定义所提供的安全服务很重要?

Why is it important to define which security services will be provided?

A) 更好地协调信息安全要求和客户服务
To better align the information security requirements and the customer service

B) 确定组织的信息安全策略
To determine the information security strategy of an organization

C) 确保组织符合ISO/IEC 27001的要求
To make sure an organization is compliant with the requirements of ISO/IEC 27001

D) 了解信息安全管理体系（ISMS）的范围
To understand the scope of the information security management system (ISMS)

A) 正确。必须定义所提供的安全服务以及采用的架构，以便更好地协调信息安全要求和客户服务。（文献：A，幻灯片第113张）
Correct. The definition of which security services will be provided, and in which architecture, must be defined to better align the information security requirements and the service for the customers. (Literature: A, Slide 113)

B) 错误。信息安全策略在定义包括安全服务的信息安全架构之前确定。
Incorrect. The information security strategy is determined before the information security architecture, which includes security services, is defined.

C) 错误。这不是ISO/IEC 27001的要求。
Incorrect. This is not a requirement of ISO/IEC 27001.

D) 错误。ISMS的范围应在定义安全服务之前了解。
Incorrect. The scope of the ISMS should be understood before the security services are defined.

24 / 30
哪个安全项目是为了收集可以表明拒绝服务攻击的大量网络相关流量而设计的?

Which security item is designed to take large collections of network-related traffic that can indicate a denial-of-service attack?

A) 防火墙
Firewall

B) 基于主机的入侵检测防御系统（基于主机的IDPS）
Host-based intrusion detection and prevention system (host-based IDPS)

C) 基于网络的入侵检测防御系统（基于网络的IDPS）
Network-based intrusion detection and prevention system (network-based IDPS)

D) 虚拟专用网络（VPN）
Virtual private network (VPN)

A) 错误。这是一个安全工具，但不会收集大量网络流量。
Incorrect. This is a security tool but does not collect large amounts of network traffic.

B) 错误。这主要是基于主机的数据流量收集，而不是基于网络的数据流量收集。
Incorrect. This focuses on host-based data traffic collection rather than on network-based data traffic collection.

C) 正确。基于网络的IDPS用于集合和收集组织网络中的数据流，以查看异常事件是否表明存在主动攻击，如拒绝服务。（文献：A，幻灯片第108张）
Correct. The network-based IDPS is used to gather and collect data flows across an organization’s network in order to see if abnormal events are indicative of an active attack such as a denial-of-service would be. (Literature: A, Slide 108)

D) 错误。这是一种网络基础设施接入设备。
Incorrect. This is a network infrastructure access device.

25 / 30
某公司CEO开始使用自己的平板电脑，想要安全经理帮她在平板电脑上使用公司邮箱和日历。安全经理理解这种允许自带设备办公（BYOD）的要求，并组织了有关BYOD的意识培训。

安全经理还应提出哪项控制以防止个人设备被盗或丢失导致数据丢失?

The CEO of a company started using her tablet pc and wants the security manager to facilitate her in using business e-mail and calendar on the tablet. The security manager understands this desire to allow the possibility to Bring Your Own Device (BYOD), and organized an awareness training regarding BYOD.

What other control should the security manager propose to prevent data loss in case of theft or loss of the personal device?

A) 在能够稳定地将企业功能整合到私人设备上之前，不要满足她的需求
Do not grant the wish until stable integration of business functions on private devices is possible
B) 将本地存储和网络连接加密
Encrypt the local storage and network connections
C) 使用一次性密码的令牌实现强身份验证
Implement strong authentication using tokens with one-time passwords
D) 安装反恶意软件和防火墙以防止感染
Install anti-malware and a firewall to prevent infection

A) 错误。这或许是明智之举，但不能被忽视CEO。
Incorrect. It may be wise, but the CEO cannot be overlooked.
B) 正确。万一数据丢失或被盗，至少企业数据是安全的。（文献：A，幻灯片第061张）
Correct. In case of loss or theft at least corporate data are safe. (Literature: A, Slide 061)
C) 错误。这只允许安全登录到企业网络。
Incorrect. This only allows secure login to the corporate network.
D) 错误。万一数据被盗或丢失，数据仍可被第三方访问。
Incorrect. In case of theft or loss the data are still accessible to third parties.

26 / 30
为什么IT基础设施中的安全元素很重要?

Why are the security elements in the IT infrastructure important?

A) 实现IT基础设施的业务连续性
To enable business continuity of the IT infrastructure

B) 管理影响IT基础设施的信息安全事件
To manage information security incidents which impact the IT infrastructure

C) 防止对IT基基础设施进行未经授权的物理访问
To prevent unauthorized physical access to the IT infrastructure

D) 保护IT基础设施上的信息资产
To protect the information assets which are on the IT infrastructure

A) 错误。实现IT基础设施的业务连续性很重要，但此安全元素的目的是保护信息资产。
Incorrect. Enabling business continuity of the IT infrastructure is important, but the purpose of this security element is to protect the information assets.

B) 错误。管理影响IT基础设施的信息安全事件很重要，但此安全元素的目的是保护信息资产。
Incorrect. Managing information security incidents which impact the IT infrastructure is important, but the purpose of this security element is to protect the information assets.

C) 错误。防止对IT基础设施进行未经授权的物理访问很重要，但此安全元素的目的是保护信息资产。
Incorrect. Preventing unauthorized physical access to the IT infrastructure is important, but the purpose of this security element is to protect the information assets.

D) 正确。所有信息安全元素都是为了保护信息。大多数信息驻留在需要保护的IT基础设施中。（文献：A，幻灯片第018张）
Correct. All information security elements are there to protect the information. Most information resides in IT infrastructure which needs to be protected. (Literature: A, Slide 018)

27 / 30
分区是将安全级别不同的物理区域隔离的一种安全控制。安全等级较高的分区可以通过更多的控制来保证安全。某酒店的安全经理负责安全工作，正在考虑为酒店设置分区。

哪些业务功能应合并为一个安全区？

Zoning is a security control to separate physical areas with different security levels. Zones with higher security levels can be secured by more controls. The security manager of a hotel is responsible for security and is considering different zones for the hotel.

What business functions should be combined into one security zone?

A) 会议室和一般办公空间
Boardroom and general office space

B) 健身区和储存设施
Fitness area and storage facility

C) 酒店客房和公共酒吧
Hotel rooms and public bar

D) 公共餐厅和大厅
Public restaurant and lobby

A) 错误。会议室可能包含有价值的战略信息，即普通人员可能无法访问的机密信息。
Incorrect. The boardroom could contain valuable strategic and thus confidential information that may not be accessible to regular personnel.

B) 错误。储存设施应仅限（部分）工作人员使用，而健身区则向所有客人和工作人员开放。
Incorrect. The storage facility should be available for (some) staff only, whereas the fitness area is accessible for all guests and staff.

C) 错误。酒店客房和酒吧必须分开。公共酒吧可供所有人使用，酒店客房仅对付费客人开放。
Incorrect. The hotel rooms and bar must be separated. The public bar can be used by everyone and the hotel rooms are only for paying guests.

D) 正确。这两个地方可供任何人使用。（文献：A，幻灯片第091张）
Correct. Both these locations can be used by anybody. (Literature: A, Slide 091)

28 / 30
某大公司安全经理的任务是实现对企业数据存储的物理保护。

通过哪项控制可以实现物理保护?

A security manager for a large company has the task to achieve physical protection for corporate data stores.

Through which control can physical protection be achieved?

A) 让访客在企业数据中心签到和签出
Having visitors sign in and out of the corporate datacenter

B) 安装防火墙防止对网络基础设施的访问
Install a firewall to prevent access to the network infrastructure

C) 对需要出入的员工使用钥匙门禁卡控制
Using key access card controls for employees needing access

D) 编写方针来规定可以进入公司的人员
Writing a policy stating who may have access to the company

A) 错误。这并不直接提供物理屏障或物理保护，不过却是有效的被动/检测控制和审核点。
Incorrect. This does not directly provide a physical barrier or physical protection. It is a good passive/detective control and audit point.

B) 错误。这不属于物理保护控制，而是逻辑保护控制。
Incorrect. This is not a physical protection control. It is a logical protection control.

C) 正确。钥匙门禁卡是一种有效的物理访问控制，结合某种摄像头/面部识别程序，在验证数据中心进入人员的身份时尤其有用。（文献：A，幻灯片第090张）
Correct. Key cards are a good form of physical access control especially when combined with some sort of camera/facial recognition procedure to verify the identity of someone entering the data center. (Literature: A, Slide 090)

D) 错误。这属于一项组织控制。
Incorrect. This is an organizational control.

29 / 30
鉴于物理安全控制是信息安全程序中非常重要的一环，要求信息安全小组为正在建立一些新数据系统的部门设计并实施一个安全边界。

根据ISO/IEC 27001，在建立这个边界时需要考虑的**最**重要准则是什么？

Knowing that physical security controls are a very important part of an information security program, the information security team is asked to design and then implement a security perimeter for a department that is setting up some new data systems.

According to ISO/IEC 27001, which is the **most** important guideline that needs to be considered when establishing this perimeter?

A) 两两支持模式
A two-person support model
B) 安装摄像头和报警器
Installing cameras and alarms
C) 系统记录和监测
System logging and monitoring
D) 边界的强度应与数据值一致
The strength of the perimeter should be in line with the data's value

A) 错误。这是个不错的物理控制，但并不是最重要的控制，也不是一项准则。
Incorrect. This is a good physical control, but it is not the most important control and it is not a guideline.
B) 错误。这是个不错的物理控制，但并不是最重要的控制，也不是一项准则。
Incorrect. This is a good physical control, but it is not the most important control and it is not a guideline.
C) 错误。这是个不错的控制，但并不是最重要的控制，也不是边界控制。
Incorrect. This is a good control, but it is not the most important control and it is not a perimeter control.
D) 正确。信息安全团队所做的每一个决策都应以数据为中心，决策的依据应是所涉及数据的分类。（文献：A，幻灯片第087张）
Correct. Every decision an information security team makes should be data centric and the decisions should be based on the classification of the data involved. (Literature: A, Slide 087)

30 / 30
某组织人力资源经理询问，在雇佣和招聘方面，她如何做才能快速有效地帮助组织按照ISO/IEC 27001加强数据安全程序。

哪一项应作为建议？

The human resource manager for an organization asked what she could do as a quick win in the area of employment and hiring to help strengthen the organization’ s data security program according to ISO/IEC 27001.

What should the advice be?

A) 做背景调查
Do background checks

B) 实施安全方针
Implement security policy

C) 在入口处设置旋转门
Place revolving gates at the entrance

A) 正确。对潜在员工进行背景调查不失为一个最佳做法。这个简单的步骤大大加强了组织数据的整体安全性。（文献：A，幻灯片第094张和第097张）
Correct. One best practice is to conduct background checks on prospective employees. This simple step greatly strengthens the overall security of organizational data. (Literature: A, Slide 094 and 097)

B) 错误。这是个好主意，但不能快速见效，而是一个长期策略。
Incorrect. This is a good idea but is not a quick win. It would be a long-term strategy.

C) 错误。这是一种物理控制，对雇佣和招聘方面没有帮助。
Incorrect. This is a physical control and does not help in the area of employment and hiring.

试题评分

如下表格为本套样题的正确答案，供参考使用。

问题	答案	问题	答案
1	C	16	B
2	B	17	B
3	D	18	C
4	C	19	B
5	A	20	B
6	B	21	B
7	D	22	B
8	C	23	A
9	B	24	C
10	B	25	B
11	A	26	D
12	C	27	D
13	B	28	C
14	B	29	D
15	E	30	A

Driving Professional Growth

联系 EXIN

www.exinchina.cn

info.china@exin.com

WeChat ID: EXINCH