EXIN

EXIN Information Security Management ISO/IEC 27001

FOUNDATION

Certified by EXIN

考试样卷

202404 版本

目录

考试说明

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

本试卷由 40 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。

本试卷的总分是 40 分。每道题的分数是 1 分。您需要获得 26 分或以上通过考试。

考试时间为 60 分钟。

祝您好运!

考试样卷

1 / 40
某数据库包含了一家电话公司的数百万笔交易。一个客户的发票已生成并发送。

对该客户而言，这份发票包含什么?

A database contains a few million transactions of a phone company. An invoice for a customer has been generated and sent.

What does this invoice contain for the customer?

A) 数据
Data
B) 信息
Information
C) 数据与信息
Data and information

2 / 40
数据和信息有什么区别?

What is the difference between data and information?

A) 数据可以是任何事实或数字。信息是有意义的数据。
Data can be any facts or figures. Information is data that has meaning.
B) 数据由非结构化数字组成。信息由结构化数字组成。
Data consists of unstructured figures. Information consists of structured figures.
C) 数据不需要安全性。信息需要安全性。
Data does not require security. Information requires security.
D) 数据没有价值。信息是经过处理的数据，具有价值。
Data has no value. Information, which is processed data, has value.

3 / 40
哪一项是信息管理的重点?

What is the focus of information management?

A) 允许业务活动和流程不中断地继续进行
Allowing business activities and processes to continue without interruption
B) 确保识别和利用信息的价值
Ensuring that the value of information is identified and exploited
C) 防止未经授权的人访问自动化系统
Preventing unauthorized persons from having access to automated systems
D) 了解信息如何在一个组织中流动
Understanding how information flows through an organization

4 / 40
组织必须了解自身面临的风险，然后才能采取适当的措施。

为确定风险，应该了解什么?

An organization must understand the risks it is facing before it can take appropriate measures.

What should be understood to determine risk?

A) 某事发生的可能性及其对组织的影响
The likelihood of something happening and its consequences to the organization

B) 最佳实践中定义的最常见危险以及如何减轻危险
The most common dangers and how to mitigate these as defined in best practices

C) 组织面临的威胁以及组织面对威胁的脆弱程度
The threats an organization faces and how vulnerable the organization is to them

D) 组织面临的计划外事件以及在发生此类事件时应采取的措施
The unplanned events an organization faces and what to do in case of such an event

5 / 40
除去完整性和机密性，哪一项是信息的第三个可靠性方面?

Besides integrity and confidentiality, what is the third reliability aspect of information?

A) 准确性
Accuracy

B) 可用性
Availability

C) 完全
Completeness

D) 价值
Value

6 / 40
某单位在公司的楼道里放有一台网络打印机。很多员工没有立即拿走打印出来的文件，而是把文件留在打印机上。

这种行为对信息的可靠性有什么影响?

An organization has a network printer in the hallway of the company. Many employees do not pick up their printouts immediately and leave them on the printer.

What is the consequence of this to the reliability of the information?

A) 信息的可用性不再得到保证。
The availability of the information is no longer guaranteed.

B) 信息的机密性不再得到保证。
The confidentiality of the information is no longer guaranteed.

C) 信息的完整性不再得到保证。
The integrity of the information is no longer guaranteed.

7 / 40
问责性和可审计性有什么区别?

What is the difference between accountability and auditability?

A) 问责性是指组织的财务账户管理到位。
可审计性是指组织通过了审计。
Accountability means an organization has their financial accounts well-administered.
Auditability means an organization passed an audit.

B) 问责性是指对组织活动的结果负责。
可审计性是指组织准备好接受独立审查。
Accountability means being liable for the results of an organization's activities.
Auditability refers to an organization's readiness for being independently reviewed.

C) 问责性是指对个人行动负责。
可审计性是指对组织行动负责。
Accountability means having responsibility for an individual's actions.
Auditability means having responsibility for an organization's actions.

D) 问责性是指组织遵守萨班斯-奥克斯利法案（SOX）。
可审计性是指组织遵守ISO/IEC 27001。
Accountability means that an organization complies with Sarbanes-Oxley (SOX).
Auditability refers to an organization complying with ISO/IEC 27001.

8 / 40
哪一项描述**最**符合信息安全方针的目的?

How is the purpose of an information security policy **best** described?

A) 信息安全方针记录了风险分析和寻找适当控制。
An information security policy documents the analysis of risks and the search for appropriate controls.

B) 信息安全方针为组织提供有关信息安全的指导和支持。
An information security policy gives direction and support to the organization regarding information security.

C) 信息安全方针提供必要的细节，使安全计划具体化。
An information security policy makes the security plan concrete by providing it with the necessary details.

D) 信息安全方针可以让人深入了解各种威胁和可能的后果。
An information security policy provides insight into threats and the possible consequences.

9 / 40
Sara的任务是确保组织遵守个人数据保护法规。

她**首先**应该做什么?

Sara has been tasked with ensuring that the organization complies with personal data protection legislation.

What is the **first** thing she should do?

A) 指定专人负责支持管理者遵守该政策
Appoint a person responsible for supporting managers in adhering to the policy
B) 发布禁止收集和存储个人信息的禁令
Issue a ban on collecting and storing personal information
C) 让员工负责提交自己的个人数据
Make employees responsible for submitting their personal data
D) 将个人数据保护法规转化为隐私政策
Translate the personal data protection legislation into a privacy policy

10 / 40
某组织决定将一部分IT工作外包。

与供应商合作时，如何**最好地**确保信息安全?

An organization decides to outsource some of its IT.

How can information security **best** be ensured when working with a supplier?

A) 在供应商组织中任命一名新的信息安全官（ISO）
Appoint a new information security officer (ISO) in the supplier's organization
B) 在协议中正式确定对供应商的信息安全要求
Formalize the information security requirements for the supplier in an agreement
C) 将两个组织完全分离，各自对自己的数据负责
Keep both organizations fully separated to make everyone accountable for their data
D) 要求供应商遵循客户组织的流程和程序
Require the supplier to follow the customer organization's processes and procedures

11 / 40
谁负责将业务策略和目标转化为安全策略和目标?

Who is responsible for the translation of the business strategy and objectives to security strategy and objectives?

A) 首席信息安全官（CISO）
Chief information security officer (CISO)
B) 总经理
General management
C) 信息安全官（ISO）
Information security officer (ISO)
D) 信息安全方针官
Information security policy officer

12 / 40
人为威胁**最好**例子是什么?

Which is the **best** example of a human threat?

A) 漏电导致电源故障。
A leak causes a failure of the electricity supply.

B) U盘将病毒传到网络上。
A USB-stick passes on a virus to a network.

C) 服务器机房内灰尘过多。
There is too much dust in the server room.

13 / 40
某数据库系统因未打上最新的安全补丁，遭到黑客入侵了。黑客能够访问数据和删除数据。

哪个信息安全概念描述了缺失安全补丁程序的情况?

A database system does not have the latest security patches applied to it and was hacked. The hackers were able to access the data and delete it.

What information security concept describes the lack of security patches?

A) 影响
Impact

B) 风险
Risk

C) 威胁
Threat

D) 脆弱性（漏洞）
Vulnerability

14 / 40
一家公司发生火灾。消防部门迅速赶到现场，顺利在火势蔓延而烧毁整个场所前将大火扑灭。但是，服务器却被大火烧毁。保存在另一个房间的备份磁带已经熔化，还有许多文件也丢失了。

此次火灾造成了哪种**间接**损害?

There was a fire in a company. The fire department quickly arrived at the scene and could extinguish the fire before it spread and burned down the entire premises. The server, however, was destroyed in the fire. The backup tapes kept in another room had melted and many other documents were lost.

What **indirect** damage is caused by this fire?

A) 烧毁的计算机系统
Burned computer systems

B) 烧毁的文件
Burned documents

C) 熔化的备份磁带
Melted backup tapes

D) 水渍损害
Water damage

15 / 40
根据业务类型的不同，企业可以采用不同的风险策略。

哪种风险策略**最**适合医院?

Companies can have different risk strategies depending on the type of business.

Which risk strategy is **most** suitable for a hospital?

A) 风险接受
Risk accepting

B) 风险规避
Risk avoiding

C) 风险承受
Risk bearing

D) 风险中立
Risk neutral

16 / 40
执行到位的风险分析可以提供大量有用的信息。风险分析有不同的主要目标。

哪一项**不**属于风险分析的主要目标?

A well-executed risk analysis provides a great deal of useful information. A risk analysis has different main objectives.

What is **not** a main objective of a risk analysis?

A) 在事件成本与控制成本之间建立平衡
Balance the costs of an incident and the costs of a control

B) 确定相关的脆弱性和威胁
Determine relevant vulnerabilities and threats

C) 识别资产及其价值
Identify assets and their value

D) 实施措施和控制
Implement measures and controls

17 / 40
哪一项是发生火灾时的遏制性控制?

What is a repressive control in case of a fire?

A) 在发现火灾后进行扑救
Putting out a fire after it has been detected

B) 修复火灾造成的损害
Repairing damage caused by the fire

C) 投保火灾保险
Taking out a fire insurance

18 / 40
信息分类分级的目的是什么?

What is the goal of classification of information?

A) 贴上标签，使信息更容易识别
Applying labels to make the information easier to recognize

B) 制作关于如何处理移动设备的手册
Creating a manual on how to handle mobile devices

C) 根据信息的敏感度将信息结构化
Structuring information according to its sensitivity

19 / 40
实行职责分离的**最**重要原因是什么?

What is the **most** important reason to apply segregation of duties?

A) 确保员工不在同一时间做同样的工作
Ensuring that employees do not do the same work at the same time
B) 让全体员工共同为自己所犯错误承担责任
Holding all employees jointly responsible for the mistakes they make
C) 明确谁负责哪些任务和活动
Making clear who is responsible for what tasks and activities
D) 最大限度地减少发生未经授权或意外更改的可能
Minimizing the chance of unauthorized or unintended changes

20 / 40
确保信息访问得当的**最佳**方法是什么?

What is the **best** way to ensure appropriate access to information?

A) 自动化工作流
Automate workflows
B) 定义操作规程
Define operating procedures
C) 为所有任务制定作业指导书
Develop work instructions for all tasks
D) 提供培训
Provide training

21 / 40
一家组织的一个办事处发生了火灾。员工被转移到组织的邻近办事处继续工作。

在事件周期的哪个阶段会转向备用安排?

A fire breaks out in an office of an organization. The employees are transferred to neighboring offices of the organization to continue their work.

Where in the incident cycle is moving to a stand-by arrangement found?

A) 损害阶段与恢复阶段之间
Between the damage and recovery stages
B) 事件阶段与损害阶段之间
Between the incident and damage stages
C) 恢复阶段与威胁阶段之间
Between the recovery and threat stages
D) 威胁阶段与事件阶段之间
Between the threat and incident stages

22 / 40
一名员工发现一条方针的到期日在她不知情的情况下被更改，而她是唯一有权执行此操作的人，于是她将此安全事件报告给服务台。

服务台工作人员记录了以下此事件相关信息：
- 日期和时间
- 事件说明
- 事件的可能后果

以上缺少了事件的哪项重要信息?

An employee discovers that the expiration date of a policy has been changed without her knowledge. She is the only person authorized to do this and reports this security incident to the helpdesk.

The helpdesk worker records the following information regarding this incident:
- date and time
- description of the incident
- possible consequences of the incident

What important information about the incident is missing here?

A) 事件报告者的姓名
The name of the person reporting the incident

B) 软件包名称
The name of the software package

C) 电脑（PC）编号
The PC number

23 / 40
为什么定期审计组织的信息安全管理体系（ISMS）很重要?

Why is it important to regularly audit the organization’s information security management system (ISMS)?

A) 审计是客户合同中确保信息安全的常见要求。
Audits are a common requirement in customer contracts to ensure information security.

B) 审计是遵守法律或法规要求的必要要素。
Audits are a required element in order to comply with legal or regulatory requirements.

C) 审计发现达成组织财务目标能力方面的问题。
Audits uncover issues with the ability to meet an organization’s financial targets.

D) 审计发现信息安全控制实施中的弱点。
Audits uncover weaknesses in the implementation of information security controls.

24 / 40
哪份文件会包含禁止使用公司电子邮件进行私人的规定?

Which document would include a rule that forbids the use of company e-mail for private purposes?

A) 品行优良证书
Certificate of good character

B) 行为准则
Code of conduct

C) 《通用数据保护条例》（GDPR）
General Data Protection Regulation (GDPR)

D) 保密协议（NDA）
Non-disclosure agreement (NDA)

25 / 40
当员工发现事件时，通常应**最先**向谁报告?

When an employee detects an incident, to whom should it typically be reported **first**?

A) 服务台
The helpdesk

B) 信息安全经理（ISM）
The information security manager (ISM)

C) 信息安全官（ISO）
The information security officer (ISO)

D) 经理
The manager

26 / 40
培养员工信息安全意识的**最**有效方法是什么?

What is the **most** effective way to create information security awareness among employees?

A) 将意识培训的重点放在管理团队上
Focus awareness training on the management team

B) 让所有员工参加外部信息安全培训
Send all employees to an external information security training

C) 设立针对特定组织的意识计划
Set up an organization-specific awareness program

D) 采取通用的在线信息安全培训课程
Use a generic, online information security training course

27 / 40
哪一项物理控制可以管理对组织信息的访问?

What physical control manages access to an organization’s information?

A) 安装空调
Installing air conditioning

B) 禁止使用U盘
Prohibiting the use of USB sticks

C) 要求用户名和密码
Requiring username and password

D) 使用防碎玻璃
Using unbreakable glass

28 / 40
某数据中心使用电池组，但未配备发电机。

这种配置对数据中心的可用性有什么相关的风险?

A data center uses battery packs but has no power generator.

What is the risk associated with this setup for the availability of the data center?

A) 主电源在恢复后可能不会再自动触发，因为触发主电源需要发电机。
The main power may not come up again automatically when restored, because this needs a power generator.

B) 主电源断电可能超过几分钟或几个小时，这种情况将导致电源不可用。
The main power outage may last for longer than a few minutes or hours, which will cause unavailability of power.

C) 电池组的使用寿命有限，所以可能会在几天后用完柴油而停止工作。
The battery packs’ lifespan is limited, so they may run out of diesel and stop functioning after a couple of days.

D) 电池组必须在几小时后由发电机供电，所以只能提供有限的保护。
The battery packs must be powered by the power generator after a few hours, so they only provide limited protection.

29 / 40
服务器机房内为何要放置空调?

Why is air conditioning placed in the server room?

A) 备用磁带是由无法承受高温的薄塑料制成。因此，如果服务器机房内温度过高，可能会损坏备用磁带。
Back-up tapes are made from thin plastic that cannot withstand high temperatures. Therefore, if it gets too hot in the server room, they may get damaged.

B) 服务器机房内的工作人员不应在高温下工作。高温增加了他们犯错的机会。
Employees that work in the server room should not work in the heat. The heat increases the chance that they make errors.

C) 在服务器机房中，必须对空气进行冷却，同时还要排出设备产生的热量。此外，空调还可以对机房内的空气进行除湿和过滤。
In the server room the air must be cooled, and the heat produced by the equipment must be extracted. It also dehumidifies and filters the air in the room.

D) 服务器机房是给办公室降温的最好方式。不必因大型设备牺牲办公空间。
The server room is the best way to cool the air in the office. No office space must be sacrificed for such a large piece of equipment.

30 / 40
在物理安全中，可以应用多个保护环，并采取不同的措施。

哪一项**不**属于保护环?

In physical security, multiple protection rings can be applied in which different measures can be taken.

What is **not** a protection ring?

A) 建筑环
Building ring

B) 中环
Middle ring

C) 安全室环
Secure room ring

D) 外环
Outer ring

31 / 40
确保资产安全的控制因资产而异。

哪一项是确保资产安全的**最**适当方法?

The control to secure an asset depends on the asset.

What is the **most** appropriate way to secure the asset?

A) 通过填表并签字确保表格安全
Secure a form by having it filled out and signed off

B) 通过分配每个用户一台笔记本电脑，确保笔记本电脑安全
Secure a laptop by assigning it to a single user

C) 通过加密确保U盘安全
Secure a USB-stick with encryption

D) 通过备份确保联网安全
Secure an internet connection with a back-up

32 / 40
哪一项信息安全控制有助于在开发考系统时虑信息安全?

What information security control helps to develop systems with information security in mind?

A) 确保服务器冗余
Ensuring redundancy of the servers

B) 实施物理入口控制
Implementing physical entry controls

C) 对员工进行背景调查
Performing background checks on employees

D) 对信息资产使用数据分类分级
Using data classification on information assets

33 / 40
某组织改变了政策，现在允许员工远程办公。

现在应该采取什么控制?

An organization changes its policy. Employees are now allowed to work remotely.

What control should now be put in place?

A) 创建V-LAN对公司网络进行分段
Create V-LANs to segment the corporate network

B) 对公司网络上的信息进行加密
Encrypt the information on the corporate network

C) 在公司网络上安装防火墙
Install firewalls on the corporate network

D) 使用VPN连接到公司网络
Use a VPN to connect to the corporate network

34 / 40
某组织员工的工作用笔记本电脑经过非对称加密算法保护。为了降低密钥管理的成本，所有顾问都采用相同的密钥对。

如果某些信息被泄露，则应提供新的密钥。

在什么情况下应提供新的密钥?

The employees of an organization work on laptops that are protected by asymmetrical cryptography. To keep the management of the keys cheap, all consultants use the same key pair.

If certain information is compromised, new keys should be supplied.

In what case should new keys be supplied?

A) 当私钥为人所知时
When the private key becomes known
B) 当公钥为人所知时
When the public key becomes known
C) 当公钥基础结构（PKI）为人所知时
When the public key infrastructure (PKI) becomes known

35 / 40
公钥基础结构（PKI）能提供何种安全?

What sort of security does a public key infrastructure (PKI) offer?

A) PKI确保了定期备份公司数据。
A PKI ensures that back-ups of company data are made on a regular basis.
B) PKI向客户表明基于网络的业务是安全的。
A PKI shows customers that a web-based business is secure.
C) PKI验证哪个人或系统属于特定的公钥。
A PKI verifies which person or system belongs to a specific public key.

36 / 40
哪种类型的恶意软件是一种除了执行表面上的功能外，还故意进行辅助活动的程序?

Which type of malware is a program which, in addition to the function that it appears to perform, purposely conducts secondary activities?

A) 逻辑炸弹
Logic bomb
B) 间谍软件
Spyware
C) 木马
Trojan
D) 蠕虫
Worm

37 / 40
哪种类型的恶意软件会通过自我复制来建立一个受污染的计算机网络?

Which type of malware builds a network of contaminated computers by replicating itself?

A) 逻辑炸弹
Logic bomb
B) 间谍软件
Spyware
C) 木马
Trojan
D) 蠕虫
Worm

38 / 40
哪一项与信息安全有关的法律规章可以适用于所有组织?

Which is a legislative or regulatory act related to information security that can be imposed upon all organizations?

A) 《通用数据保护条例》（GDPR）
General Data Protection Regulation (GDPR)
B) 知识产权（IP）
Intellectual property (IP) rights
C) ISO/IEC 27001
ISO/IEC 27001
D) ISO/IEC 27002
ISO/IEC 27002

39 / 40
哪项ISO标准侧重于信息安全控制的实施?

Which ISO standard is focused on the implementation of information security controls?

A) ISO/IEC 27000
ISO/IEC 27000
B) ISO/IEC 27001
ISO/IEC 27001
C) ISO/IEC 27002
ISO/IEC 27002
D) ISO/IEC 27005
ISO/IEC 27005

40 / 40
在欧洲，哪个组织的标准是**最**常用的?

The standards of which organization is **most** commonly used in Europe?

A) 美国国家标准协会（ANSI）
American National Standards Institute (ANSI)

B) 国际标准化组织（ISO）
International Organization for Standardization (ISO)

C) 国家标准技术研究所（NIST）
National Institute of Standards and Technology (NIST)

答案解析

1 / 40
某数据库包含了一家电话公司的数百万笔交易。一个客户的发票已生成并发送。

对该客户而言，这份发票包含什么?

A database contains a few million transactions of a phone company. An invoice for a customer has been generated and sent.

What does this invoice contain for the customer?

A) 数据
Data

B) 信息
Information

C) 数据与信息
Data and information

A) 错误。数据库包含数据，但是当生成发票并发送给接收者时，发票就变成了接收者的信息。
Incorrect. The database contains data. However, when an invoice is generated and sent to a recipient, it is information for the recipient.

B) 正确。信息的价值由接收者决定。发票包含对接收者有价值的数据，所以该发票是一种信息。（文献：A，第4.8.5章）
Correct. The value of information is determined by the recipient. The invoice contains valuable data for the recipient, and therefore it is information. (Literature: A, Chapter 4.8.5)

C) 错误。发票仅包含接收者的信息。
Incorrect. The invoice contains only information for the recipient.

2 / 40
数据和信息有什么区别?

What is the difference between data and information?

A) 数据可以是任何事实或数字。信息是有意义的数据。
Data can be any facts or figures. Information is data that has meaning.

B) 数据由非结构化数字组成。信息由结构化数字组成。
Data consists of unstructured figures. Information consists of structured figures.

C) 数据不需要安全性。信息需要安全性。
Data does not require security. Information requires security.

D) 数据没有价值。信息是经过处理的数据，具有价值。
Data has no value. Information, which is processed data, has value.

A) 正确。信息是通过在特定语境中赋予数据意义而从数据中衍生出来。（文献：A，第3.1章）
Correct. Information is derived from data by giving it meaning in a certain context. (Literature: A, Chapter 3.1)

B) 错误。数据可以是结构化的，也可以是非结构化的。信息通常是结构化的。
Incorrect. Data can be either structured or unstructured. Information is usually structured.

C) 错误。数据和信息都需要安全性。
Incorrect. Both data and information require security.

D) 错误。数据和信息都具有价值。
Incorrect. Both data and information have value.

3 / 40
哪一项是信息管理的重点?

What is the focus of information management?

A) 允许业务活动和流程不中断地继续进行
Allowing business activities and processes to continue without interruption
B) 确保识别和利用信息的价值
Ensuring that the value of information is identified and exploited
C) 防止未经授权的人访问自动化系统
Preventing unauthorized persons from having access to automated systems
D) 了解信息如何在一个组织中流动
Understanding how information flows through an organization

A) 错误。这是业务连续性管理（BCM）的重点。BCM的目的是防止业务活动中断，保护关键流程不受信息系统长久中断的影响，并能迅速恢复。
Incorrect. This is the focus of business continuity management (BCM). The purpose of BCM is to prevent business activities from being disrupted, to protect critical processes against the consequences of far-reaching disruptions in information systems, and to allow for speedy recovery.
B) 正确。信息管理是指一个组织有效地规划、收集、组织、使用、控制、传播和处置其信息的手段，并通过这种手段确保信息的价值得到识别和最大程度的利用。（文献：A，第4.9章）
Correct. Information management describes how an organization efficiently plans, collects, organizes, uses, controls, disseminates, and disposes of its information, and through which it ensures that the value of that information is identified and exploited to the fullest extent. (Literature: A, Chapter 4.9)
C) 错误。这是访问管理的重点，它确保未经授权的人员或进程无法访问自动化系统、数据库和程序。
Incorrect. This is the focus of access management. It ensures that unauthorized persons or processes do not have access to automated systems, databases, and programs.
D) 错误。这是信息分析重点。通过信息分析，可以清楚地了解一个组织如何处理信息以及信息如何在组织中流动。
Incorrect. This is the focus of information analysis. It provides a clear picture of how an organization handles information, and how the information flows through the organization.

4 / 40
组织必须了解自身面临的风险，然后才能采取适当的措施。

为确定风险，应该了解什么?

An organization must understand the risks it is facing before it can take appropriate measures.

What should be understood to determine risk?

A) 某事发生的可能性及其对组织的影响
The likelihood of something happening and its consequences to the organization
B) 最佳实践中定义的最常见危险以及如何减轻危险
The most common dangers and how to mitigate these as defined in best practices
C) 组织面临的威胁以及组织面对威胁的脆弱程度
The threats an organization faces and how vulnerable the organization is to them
D) 组织面临的计划外事件以及在发生此类事件时应采取的措施
The unplanned events an organization faces and what to do in case of such an event

A) 正确。两个高级因素确定风险：某事发生的可能性及其对企业的影响。（文献：A，第3.1章）
Correct. Two high-level factors determine risk: the likelihood of something happening and its impact on the business. (Literature: A, Chapter 3.1)
B) 错误。组织定义自身的风险时，以此为切入点比较不明智。照搬其他组织的实践并不能确保自身安全。
Incorrect. It is unwise to have this as a starting point when an organization defines their risks. Doing what other organizations do does not make this organization safe.
C) 错误。这是对可能性一词的描述。尽管了解可能性很重要，但缺少了一个重要方面：其对企业的影响。
Incorrect. This is a description of the term likelihood. Although it is important to understand likelihood, an important aspect is missing: how it will affect the business.
D) 错误。归根结底需要匹配风险和控制，但这是对风险的应对，而不是首先了解风险的方式。
Incorrect. Eventually, matching risks and controls are needed, but this is rather a response to risk than a way to understand risk in the first place.

5 / 40
除去完整性和机密性，哪一项是信息的第三个可靠性方面?

Besides integrity and confidentiality, what is the third reliability aspect of information?

A) 准确性
Accuracy

B) 可用性
Availability

C) 完全
Completeness

D) 价值
Value

A) 错误。信息的三个可靠性方面分别是可用性、完整性和机密性。准确性是完整性的一部分。
Incorrect. The three reliability aspects of information are availability, integrity, and confidentiality. Accuracy is a part of integrity.

B) 正确。信息的三个可靠性方面分别是可用性、完整性和机密性。（文献：A，第3.4.3章）
Correct. The three reliability aspects of information are availability, integrity, and confidentiality. (Literature: A, Chapter 3.4.3)

C) 错误。信息的三个可靠性方面分别是可用性、完整性和机密性。完全是完整性的一部分。
Incorrect. The three reliability aspects of information are availability, integrity, and confidentiality. Completeness is a part of integrity.

D) 错误。信息的三个可靠性方面分别是可用性、完整性和机密性。
Incorrect. The three reliability aspects of information are availability, integrity, and confidentiality.

6 / 40
某单位在公司的楼道里放有一台网络打印机。很多员工没有立即拿走打印出来的文件，而是把文件留在打印机上。

这种行为对信息的可靠性有什么影响?

An organization has a network printer in the hallway of the company. Many employees do not pick up their printouts immediately and leave them on the printer.

What is the consequence of this to the reliability of the information?

A) 信息的可用性不再得到保证。
The availability of the information is no longer guaranteed.
B) 信息的机密性不再得到保证。
The confidentiality of the information is no longer guaranteed.
C) 信息的完整性不再得到保证。
The integrity of the information is no longer guaranteed.

A) 错误。在创建和打印信息的系统中，信息仍然可以使用。
Incorrect. The information is still available in the system that was used to create and print it.
B) 正确。这些信息可能会落入无权限的人手中或被其阅读。（文献：A，第3.4.1章）
Correct. The information can end up with, or be read by, persons who should not have access to this information. (Literature: A, Chapter 3.4.1)
C) 错误。由于打印文件上的信息是纸面信息，其完整性仍有保证。
Incorrect. The integrity of the information on the prints is still guaranteed since it is on paper.

7 / 40
问责性和可审计性有什么区别?

What is the difference between accountability and auditability?

A) 问责性是指组织的财务账户管理到位。
可审计性是指组织通过了审计。
Accountability means an organization has their financial accounts well-administered.
Auditability means an organization passed an audit.

B) 问责性是指对组织活动的结果负责。
可审计性是指组织准备好接受独立审查。
Accountability means being liable for the results of an organization's activities.
Auditability refers to an organization's readiness for being independently reviewed.

C) 问责性是指对个人行动负责。
可审计性是指对组织行动负责。
Accountability means having responsibility for an individual's actions.
Auditability means having responsibility for an organization's actions.

D) 问责性是指组织遵守萨班斯-奥克斯利法案（SOX）。
可审计性是指组织遵守ISO/IEC 27001。
Accountability means that an organization complies with Sarbanes-Oxley (SOX).
Auditability refers to an organization complying with ISO/IEC 27001.

A) 错误。问责性与财务会计没有直接关系。可审计性与是否通过审计无关。
Incorrect. Accountability has no direct relationship with financial accounting. Auditability has no relationship with having passed an audit.

B) 正确。这是问责性和可审计性的正确定义。（文献：A，第3.4.4章）
Correct. These are the correct definitions of accountability and auditability. (Literature: A, Chapter 3.4.4)

C) 错误。问责性的定义正确，但可审计性的定义错误。可审计性与对组织行动负责无关。
Incorrect. The definition of accountability is correct, but the definition of auditability is not. Auditability has nothing to do with responsibility for the organization's actions.

D) 错误。 问责性和可审计性都不是指符合SOX或ISO/IEC标准。
Incorrect. Neither accountability nor auditability refer to compliance with SOX or ISO/IEC standards.

8 / 40
哪一项描述**最**符合信息安全方针的目的?

How is the purpose of an information security policy **best** described?

A) 信息安全方针记录了风险分析和寻找适当控制。
An information security policy documents the analysis of risks and the search for appropriate controls.

B) 信息安全方针为组织提供有关信息安全的指导和支持。
An information security policy gives direction and support to the organization regarding information security.

C) 信息安全方针提供必要的细节，使安全计划具体化。
An information security policy makes the security plan concrete by providing it with the necessary details.

D) 信息安全方针可以让人深入了解各种威胁和可能的后果。
An information security policy provides insight into threats and the possible consequences.

A) 错误。分析风险和寻找控制是风险分析和风险管理的目的。
Incorrect. The analysis of risks and the search for controls are the purpose of risk analysis and risk management.

B) 正确。通过安全方针，管理层可以提供有关信息安全的指导和支持。（文献：A，第4.2.1章）
Correct. With the security policy, management provides direction and support regarding information security. (Literature: A, Chapter 4.2.1)

C) 错误。安全计划使信息安全方针具体化。安全计划包括选择了哪些控制，谁负责什么，实施控制的指导方针等。
Incorrect. The security plan makes the information security policy concrete. The plan includes which controls have been chosen, who is responsible for what, the guidelines for the implementation of controls, etc.

D) 错误。威胁分析的目的是让人深入了解威胁和可能的后果。
Incorrect. The purpose of a threat analysis is to provide insight into threats and the possible consequences.

9 / 40
Sara的任务是确保组织遵守个人数据保护法规。

她**首先**应该做什么?

Sara has been tasked with ensuring that the organization complies with personal data protection legislation.

What is the **first** thing she should do?

A) 指定专人负责支持管理者遵守该政策
Appoint a person responsible for supporting managers in adhering to the policy
B) 发布禁止收集和存储个人信息的禁令
Issue a ban on collecting and storing personal information
C) 让员工负责提交自己的个人数据
Make employees responsible for submitting their personal data
D) 将个人数据保护法规转化为隐私政策
Translate the personal data protection legislation into a privacy policy

A) 错误。管理者支持人员并不是遵守个人数据保护法规的必要条件。此外，政策应首先与法规相一致。
Incorrect. A person to support managers is not a requirement to become compliant with personal data protection legislation. In addition, the policy should first align with the legislation.
B) 错误。这并不是遵守个人数据保护法规的最好方法。
Incorrect. This is not the best way to comply with personal data protection legislation.
C) 错误。这并不是遵守个人数据保护法规的方法。
Incorrect. This is not a way to become compliant with personal data protection legislation.
D) 正确。遵守法规的第一步是制定组织的内部政策。（文献：A，第5.1章）
Correct. The first step to becoming compliant is to create an internal policy for the organization. (Literature: A, Chapter 5.1)

10 / 40
某组织决定将一部分IT工作外包。

与供应商合作时，如何**最好地**确保信息安全?

An organization decides to outsource some of its IT.

How can information security **best** be ensured when working with a supplier?

A) 在供应商组织中任命一名新的信息安全官（ISO）
Appoint a new information security officer (ISO) in the supplier's organization

B) 在协议中正式确定对供应商的信息安全要求
Formalize the information security requirements for the supplier in an agreement

C) 将两个组织完全分离，各自对自己的数据负责
Keep both organizations fully separated to make everyone accountable for their data

D) 要求供应商遵循客户组织的流程和程序
Require the supplier to follow the customer organization's processes and procedures

A) 错误。如果供应商组织已有ISO，则无必要再在供应商组织任命新的ISO。
Incorrect. It is not necessary to appoint a new ISO in the supplier's organization if the organization already has one.

B) 正确。尽管签订协议这一机制无法万无一失地管理供应商风险，但却是管理供应商风险的最有效方式。（文献：A，第5.20章）
Correct. Although entering into an agreement is not a fail-safe mechanism to manage supplier risk, it is the most effective way of doing so. (Literature: A, Chapter 5.20)

C) 错误。客户组织对所有信息负责。将两个组织完全分离，通常意味着客户组织不知道如何确保或影响供应商组织的信息安全。
Incorrect. The customer organization remains accountable for all information. Keeping the organizations fully separated often implies the customer organization does not know how to ensure or influence information security in the supplier's organization.

D) 错误。这并非最好的方法，因为应允许供应商制定自己的信息安全流程。
Incorrect. This is not the best way because a supplier should be allowed to have their own information security process in place.

11 / 40
谁负责将业务策略和目标转化为安全策略和目标?

Who is responsible for the translation of the business strategy and objectives to security strategy and objectives?

A) 首席信息安全官（CISO）
Chief information security officer (CISO)

B) 总经理
General management

C) 信息安全官（ISO）
Information security officer (ISO)

D) 信息安全方针官
Information security policy officer

A) 正确。CISO属于组织的最高管理层，负责制定整个企业的总体安全策略。（文献：A，第5.2章）
Correct. The CISO is at the highest management level of the organization and develops the general security strategy for the entire business. (Literature: A, Chapter 5.2)

B) 错误。总经理确定策略是CISO确定总体安全策略的输入。
Incorrect. General management defines the strategy that is input for the CISO to define the general security strategy.

C) 错误。ISO负责根据公司的政策制定业务部门的信息安全方针，并确保其得到遵守。
Incorrect. The ISO develops the information security policy of a business unit based on the company policy and ensures that it is observed.

D) 错误。信息安全方针官负责维护由安全策略衍生的方针。
Incorrect. The information security policy officer is responsible for maintaining the policy that is derived from the security strategy.

12 / 40
人为威胁**最好**例子是什么?

Which is the **best** example of a human threat?

A) 漏电导致电源故障。
A leak causes a failure of the electricity supply.

B) U盘将病毒传到网络上。
A USB-stick passes on a virus to a network.

C) 服务器机房内灰尘过多。
There is too much dust in the server room.

A) 错误。漏电不是人为威胁，而是非人为威胁。
Incorrect. A leak is not a human threat, but a non-human threat.

B) 正确。U盘总归是由人插入的。如果插入U盘让病毒进入网络，那就构成人为威胁。（文献：A，第3.9.1章）
Correct. A USB-stick is always inserted by a person. If this causes a virus entering the network, it is a human threat. (Literature: A, Chapter 3.9.1)

C) 错误。灰尘不是人为威胁，而是非人为威胁。
Incorrect. Dust is not a human threat, but a non-human threat.

13 / 40
某数据库系统因未打上最新的安全补丁，遭到黑客入侵了。黑客能够访问数据和删除数据。

哪个信息安全概念描述了缺失安全补丁程序的情况?

A database system does not have the latest security patches applied to it and was hacked. The hackers were able to access the data and delete it.

What information security concept describes the lack of security patches?

A) 影响
Impact

B) 风险
Risk

C) 威胁
Threat

D) 脆弱性（漏洞）
Vulnerability

A) 错误。影响是指某一事件对组织或其信息的影响。
Incorrect. Impact is the effect an event has on the organization or its information.

B) 错误。风险是事件发生的可能性和影响的组合。
Incorrect. A risk is the combination of the likelihood and impact of an event happening.

C) 错误。威胁的一个例子是一个外部实体试图利用一个脆弱性。在这种情况下，黑客构成了威胁。
Incorrect. An example of a threat is an external entity trying to exploit a vulnerability. In this case, the hackers form the threat.

D) 正确。脆弱性（漏洞）的一个例子是缺乏保护。（文献：A，第3.5.3章）
Correct. An example of a vulnerability is a lack of protection. (Literature: A, Chapter 3.5.3)

14 / 40
一家公司发生火灾。消防部门迅速赶到现场，顺利在火势蔓延而烧毁整个场所前将大火扑灭。但是，服务器却被大火烧毁。保存在另一个房间的备份磁带已经熔化，还有许多文件也丢失了。

此次火灾造成了哪种**间接**损害？

There was a fire in a company. The fire department quickly arrived at the scene and could extinguish the fire before it spread and burned down the entire premises. The server, however, was destroyed in the fire. The backup tapes kept in another room had melted and many other documents were lost.

What **indirect** damage is caused by this fire?

A) 烧毁的计算机系统
Burned computer systems
B) 烧毁的文件
Burned documents
C) 熔化的备份磁带
Melted backup tapes
D) 水渍损害
Water damage

A) 错误。烧毁的计算机系统是火灾造成的直接损害。
Incorrect. Burned computer systems are direct damage caused by the fire.
B) 错误。烧毁的文件是火灾造成的直接损害。
Incorrect. Burned documents are direct damage caused by the fire.
C) 错误。熔化的备份磁带是火灾造成的直接损害。
Incorrect. Melted backup tapes are direct damage caused by the fire.
D) 正确。灭火器造成的水渍损害是火灾造成的间接损害。这是救火的一个副作用，目的是将火灾造成的损害降到最低。（文献：A，第3.10章）
Correct. Water damage due to the fire extinguishers is indirect damage caused by the fire. This is a side effect of putting out the fire, which is aimed at minimizing the damage caused by the fire. (Literature: A, Chapter 3.10)

15 / 40
根据业务类型的不同，企业可以采用不同的风险策略。

哪种风险策略**最**适合医院?

Companies can have different risk strategies depending on the type of business.

Which risk strategy is **most** suitable for a hospital?

A) 风险接受
Risk accepting

B) 风险规避
Risk avoiding

C) 风险承受
Risk bearing

D) 风险中立
Risk neutral

A) 错误。医院不能轻易接受因经济损失或濒死患者而产生的风险。
Incorrect. A hospital cannot easily accept risks due to financial losses or dying patients.

B) 正确。医院应尽量规避任何风险。（文献：A，第3.11章）
Correct. Hospitals should try to avoid any risk. (Literature: A, Chapter 3.11)

C) 错误。风险承受是指接受一定的风险。这可能是因为控制的成本超过了可能造成的损害。但这并不是医院应对风险的最佳方式。
Incorrect. Risk bearing means that certain risks are accepted. This could be because the costs of controls exceed the possible damage. In a hospital, this is not the best way to handle risks.

D) 错误。风险中立是指采取安全措施，使威胁不再出现，或即使出现威胁，将造成的损害降至最低。给客户造成损害绝非好事，因此医院应规避风险。
Incorrect. Risk neutral means that security measures are taken such that the threats either no longer manifest themselves or, if they do, the resulting damage is minimized. Damage to clients is never a good idea, so hospitals should be risk avoiding.

16 / 40
执行到位的风险分析可以提供大量有用的信息。风险分析有不同的主要目标。

哪一项**不**属于风险分析的主要目标?

A well-executed risk analysis provides a great deal of useful information. A risk analysis has different main objectives.

What is **not** a main objective of a risk analysis?

A) 在事件成本与控制成本之间建立平衡
Balance the costs of an incident and the costs of a control

B) 确定相关的脆弱性和威胁
Determine relevant vulnerabilities and threats

C) 识别资产及其价值
Identify assets and their value

D) 实施措施和控制
Implement measures and controls

A) 错误。这是风险分析的主要目标之一。
Incorrect. This is one of the main objectives of a risk analysis.

B) 错误。这是风险分析的主要目标之一。
Incorrect. This is one of the main objectives of a risk analysis.

C) 错误。这是风险分析的主要目标之一。
Incorrect. This is one of the main objectives of a risk analysis.

D) 正确。这不是风险分析的目标。（文献：A，第3.7章）
Correct. This is not an objective of a risk analysis. (Literature: A, Chapter 3.7)

17 / 40
哪一项是发生火灾时的遏制性控制?

What is a repressive control in case of a fire?

A) 在发现火灾后进行扑救
Putting out a fire after it has been detected

B) 修复火灾造成的损害
Repairing damage caused by the fire

C) 投保火灾保险
Taking out a fire insurance

A) 正确。这项遏制性控制可以将火灾造成的损害降到最低。（文献：A，第3.8章）
Correct. This repressive control minimizes the damage caused by a fire. (Literature: A, Chapter 3.8)

B) 错误。这不是一项遏制性控制。它并不能将火灾造成的损害降到最低。
Incorrect. This is not a repressive control. It does not minimize the damage caused by the fire.

C) 错误。投保可以避免火灾带来的经济后果，属于风险保险。
Incorrect. Taking out an insurance protects against the financial consequences of a fire and is risk insurance.

18 / 40
信息分类分级的目的是什么?

What is the goal of classification of information?

A) 贴上标签，使信息更容易识别
Applying labels to make the information easier to recognize

B) 制作关于如何处理移动设备的手册
Creating a manual on how to handle mobile devices

C) 根据信息的敏感度将信息结构化
Structuring information according to its sensitivity

A) 错误。给信息贴上标签就是命名，是信息分类的一种特殊形式，在信息分类分级后进行。
Incorrect. Applying labels to information is designation, which is a special form of categorizing information that follows on the classification of information.

B) 错误。制作手册与用户指南有关，并非信息的分类分级。
Incorrect. Creating a manual relates to user guidelines and is not classification of information.

C) 正确。信息分类分级是为了界定信息的不同敏感程度，将信息结构化。（文献：A，第5.12章）
Correct. Classification of information is used to define the different levels of sensitivity into which information can be structured. (Literature: A, Chapter 5.12)

19 / 40
实行职责分离的**最**重要原因是什么?

What is the **most** important reason to apply segregation of duties?

A) 确保员工不在同一时间做同样的工作
Ensuring that employees do not do the same work at the same time

B) 让全体员工共同为自己所犯错误承担责任
Holding all employees jointly responsible for the mistakes they make

C) 明确谁负责哪些任务和活动
Making clear who is responsible for what tasks and activities

D) 最大限度地减少发生未经授权或意外更改的可能
Minimizing the chance of unauthorized or unintended changes

A) 错误。职责分离是为了避免发生未经授权或意外更改，或滥用组织资产，并未规定何时应开展活动。
Incorrect. Segregation of duties is used to avoid the chance of unauthorized or unintended changes, or the misuse of the organization’s assets. It does not define when activities should be performed.

B) 错误。职责分离将任务和责任分开。这没有让一群人共同承担责任。
Incorrect. Segregation of duties separates tasks and responsibilities. It does not make a group of people jointly responsible.

C) 错误。职责分离是为了避免发生未经授权或意外更改，或滥用组织资产的情况，其目的并非为了明确由谁负责什么。
Incorrect. The segregation of duties is used to avoid the chance of unauthorized or unintended changes, or the misuse of the organization's assets. Its objective is not to make clear who is responsible for what.

D) 正确。职责必须分离，以避免发生未经授权或意外更改，或滥用组织资产的情况。（文献：A，第5.3章）
Correct. Duties must be segregated to avoid the chance of unauthorized or unintended changes, or the misuse of the organization's assets. (Literature: A, Chapter 5.3)

20 / 40
确保信息访问得当的**最佳**方法是什么?

What is the **best** way to ensure appropriate access to information?

A) 自动化工作流
Automate workflows

B) 定义操作规程
Define operating procedures

C) 为所有任务制定作业指导书
Develop work instructions for all tasks

D) 提供培训
Provide training

A) 错误。自动化工作流肯定有助于信息安全，但却无助于访问得当。
Incorrect. Automating workflows will certainly contribute to information security, but it does not help appropriate access.

B) 正确。通过规程指导如何以适当、安全和负责任的方式完成工作，是实现有效信息安全的有效途径。（文献：A，第5.36.1章）
Correct. The use of procedures to guide how work is done in an appropriate, safe, and responsible manner is an effective way to achieve effective information security. (Literature: A, Chapter 5.36.1)

C) 错误。这样过于详尽，规定过多，因此不是最佳方法。
Incorrect. This is too detailed and prescriptive, and therefore not the best way.

D) 错误。培训很重要，但不能确保信息访问得当。
Incorrect. Training is important but it does not ensure appropriate access to information.

21 / 40
一家组织的一个办事处发生了火灾。员工被转移到组织的邻近办事处继续工作。

在事件周期的哪个阶段会转向备用安排?

A fire breaks out in an office of an organization. The employees are transferred to neighboring offices of the organization to continue their work.

Where in the incident cycle is moving to a stand-by arrangement found?

A) 损害阶段与恢复阶段之间
Between the damage and recovery stages
B) 事件阶段与损害阶段之间
Between the incident and damage stages
C) 恢复阶段与威胁阶段之间
Between the recovery and threat stages
D) 威胁阶段与事件阶段之间
Between the threat and incident stages

A) 错误。损害阶段和恢复阶段受限于备用安排。
Incorrect. Damage and recovery are limited by the stand-by arrangement.
B) 正确。备用安排是为了限制损害而采取的遏制性措施。（文献：A，第3.8.4章）
Correct. A stand-by arrangement is a repressive measure that is initiated to limit the damage. (Literature: A, Chapter 3.8.4)
C) 错误。恢复阶段是在备用安排实施后进行的。
Incorrect. The recovery stage takes place after putting a stand-by arrangement into operation.
D) 错误。在未发生事件的情况下进行备用安排成本较高。
Incorrect. Carrying out a stand-by arrangement without an incident is very expensive.

22 / 40
一名员工发现一条方针的到期日在她不知情的情况下被更改，而她是唯一有权执行此操作的人，于是她将此安全事件报告给服务台。

服务台工作人员记录了以下此事件相关信息：
- 日期和时间
- 事件说明
- 事件的可能后果

以上缺少了事件的哪项重要信息?

An employee discovers that the expiration date of a policy has been changed without her knowledge. She is the only person authorized to do this and reports this security incident to the helpdesk.

The helpdesk worker records the following information regarding this incident:
- date and time
- description of the incident
- possible consequences of the incident

What important information about the incident is missing here?

A) 事件报告者的姓名
The name of the person reporting the incident

B) 软件包名称
The name of the software package

C) 电脑（PC）编号
The PC number

A) 正确。报告事件时，必须至少记录报告者的姓名。（文献：A，第5.25章）
Correct. When reporting an incident, the name of the reporter must be recorded at a minimum. (Literature: A, Chapter 5.25)

B) 错误。这是后期可添加的补充信息。
Incorrect. This is additional information that may be added later.

C) 错误。这是后期可添加的补充信息。
Incorrect. This is additional information that may be added later.

23 / 40
为什么定期审计组织的信息安全管理体系（ISMS）很重要？

Why is it important to regularly audit the organization’s information security management system (ISMS)?

A) 审计是客户合同中确保信息安全的常见要求。
Audits are a common requirement in customer contracts to ensure information security.

B) 审计是遵守法律或法规要求的必要要素。
Audits are a required element in order to comply with legal or regulatory requirements.

C) 审计发现达成组织财务目标能力方面的问题。
Audits uncover issues with the ability to meet an organization’s financial targets.

D) 审计发现信息安全控制实施中的弱点。
Audits uncover weaknesses in the implementation of information security controls.

A) 错误。客户合同很少包含审计要求。
Incorrect. Customer contracts rarely contain audit requirements.

B) 错误。法律或法规要求通常不需要进行审计。
Incorrect. Legal or regulatory requirements usually do not require audits to be done.

C) 错误。审计通常不用于验证财务绩效。
Incorrect. Audits are not commonly used to verify financial performance.

D) 正确。审计的目的是发现所实施控制中的弱点。（文献：A，第5.35章）
Correct. The purpose of audits is to find weaknesses in implemented controls. (Literature: A, Chapter 5.35)

24 / 40
哪份文件会包含禁止使用公司电子邮件进行私人的规定?

Which document would include a rule that forbids the use of company e-mail for private purposes?

A) 品行优良证书
Certificate of good character

B) 行为准则
Code of conduct

C) 《通用数据保护条例》（GDPR）
General Data Protection Regulation (GDPR)

D) 保密协议（NDA）
Non-disclosure agreement (NDA)

A) 错误。品行优良证书由司法部等组织颁发，表明有关个人未曾犯下刑事罪行。
Incorrect. A certificate of good character is issued by an organization such as the Department of Justice and indicates that no criminal offences were committed by the individual.

B) 正确。行为准则是描述适用于员工的公司政策的文件（通常是员工手册的一部分）。（文献：A，第6.2章）
Correct. The code of conduct is a document (often part of the employee manual) that describes the company policies that are applicable to personnel. (Literature: A, Chapter 6.2)

C) 错误。GDPR是关于个人信息保护。
Incorrect. The GDPR is about the protection of personal information.

D) 错误。NDA是禁止披露某些信息的合同。出于私人目的的公司电子邮件不受此类文件的控制。
Incorrect. An NDA is a contract that forbids the disclosure of certain information. The use of company e-mail for private purposes is not controlled by such a document.

25 / 40
当员工发现事件时，通常应**最先**向谁报告?

When an employee detects an incident, to whom should it typically be reported **first**?

A) 服务台
The helpdesk
B) 信息安全经理（ISM）
The information security manager (ISM)
C) 信息安全官（ISO）
The information security officer (ISO)
D) 经理
The manager

A) 正确。通常情况下，事件应报告给服务台进行评估，办理初始程序，并在需要时升级，而不应立即纵向升级。（文献：A，第6.8章）
Correct. Typically, incidents should be reported to the helpdesk for evaluation, application of initial procedures and escalation if required. They should not be escalated vertically immediately. (Literature: A, Chapter 6.8)
B) 错误。事件不应立即纵向升级。此外，并非每个事件都属于安全事件，因此应首先由服务台评估事件，以确定是否存在安全事件。
Incorrect. Incidents should not be escalated vertically immediately. Also, not every incident is a security incident, so the incident should be assessed by the help desk first to determine if there is a security incident.
C) 错误。事件不应立即纵向升级。此外，并非每个事件都属于安全事件，因此应首先由服务台评估事件，以确定是否存在安全事件。
Incorrect. Incidents should not be escalated vertically immediately. Also, not every incident is a security incident, so the incident should be assessed by the help desk first to determine if there is a security incident.
D) 错误。事件不应立即纵向升级。
Incorrect. Incidents should not be escalated vertically immediately.

26 / 40
培养员工信息安全意识的**最**有效方法是什么?

What is the **most** effective way to create information security awareness among employees?

A) 将意识培训的重点放在管理团队上
Focus awareness training on the management team
B) 让所有员工参加外部信息安全培训
Send all employees to an external information security training
C) 设立针对特定组织的意识计划
Set up an organization-specific awareness program
D) 采取通用的在线信息安全培训课程
Use a generic, online information security training course

A) 错误。所有员工都需要建立信息安全意识，而不仅仅是管理者。
Incorrect. All employees need awareness of information security, not only managers.
B) 错误。外部培训可能不完全适用于特定组织的需求。
Incorrect. External training may not be fully applicable to a specific organization’s needs.
C) 正确。与特定组织需求相适应的安全意识计划是最有效的。（文献：A，第6.3章）
Correct. Adapting a security awareness program to the specific organizational needs is most effective. (Literature: A, Chapter 6.3)
D) 错误。通用信息安全培训可能不完全适用于特定组织的需求。
Incorrect. Generic information security training may not be fully applicable to a specific organization’s needs.

27 / 40
哪一项物理控制可以管理对组织信息的访问?

What physical control manages access to an organization’s information?

A) 安装空调
Installing air conditioning
B) 禁止使用U盘
Prohibiting the use of USB sticks
C) 要求用户名和密码
Requiring username and password
D) 使用防碎玻璃
Using unbreakable glass

A) 错误。空调无法管理对组织信息的访问。
Incorrect. Air conditioning does not manage access to an organization’s information.
B) 错误。这属于组织控制。
Incorrect. This is an organizational control.
C) 错误。这属于技术控制。
Incorrect. This is a technical control.
D) 正确。使用防碎玻璃是物理控制的一个例子，可以防止未经授权的人进入建筑物。（文献：A，第7.4章）
Correct. The use of unbreakable glass is an example of a physical control to prevent unauthorized persons from entering the building. (Literature: A, Chapter 7.4)

28 / 40
某数据中心使用电池组，但未配备发电机。

这种配置对数据中心的可用性有什么相关的风险?

A data center uses battery packs but has no power generator.

What is the risk associated with this setup for the availability of the data center?

A) 主电源在恢复后可能不会再自动触发，因为触发主电源需要发电机。
The main power may not come up again automatically when restored, because this needs a power generator.

B) 主电源断电可能超过几分钟或几个小时，这种情况将导致电源不可用。
The main power outage may last for longer than a few minutes or hours, which will cause unavailability of power.

C) 电池组的使用寿命有限，所以可能会在几天后用完柴油而停止工作。
The battery packs' lifespan is limited, so they may run out of diesel and stop functioning after a couple of days.

D) 电池组必须在几小时后由发电机供电，所以只能提供有限的保护。
The battery packs must be powered by the power generator after a few hours, so they only provide limited protection.

A) 错误。发电机不用于触发主电源。
Incorrect. A power generator is not used to trigger the main power supply.

B) 正确。电池组只能保护临时断电和电涌，而发电机则能保护较长时间的断电。（文献：A，第7.11.1章）
Correct. Battery packs only protect against temporary power outages and surges, whereas a power generator protects for longer-duration outages. (Literature: A, Chapter 7.11.1)

C) 错误。发电机用柴油供电；电池组用电池供电。
Incorrect. Diesel is used to power the generator; a battery pack is powered by batteries.

D) 错误。电池组只能短时间工作，但不由发电机供电。发电机只是接替电池组的工作。
Incorrect. The battery packs will only work for a short period but are not powered by the generator. The generator simply takes over from the battery pack.

29 / 40
服务器机房内为何要放置空调?

Why is air conditioning placed in the server room?

A) 备用磁带是由无法承受高温的薄塑料制成。因此，如果服务器机房内温度过高，可能会损坏备用磁带。
Back-up tapes are made from thin plastic that cannot withstand high temperatures. Therefore, if it gets too hot in the server room, they may get damaged.

B) 服务器机房内的工作人员不应在高温下工作。高温增加了他们犯错的机会。
Employees that work in the server room should not work in the heat. The heat increases the chance that they make errors.

C) 在服务器机房中，必须对空气进行冷却，同时还要排出设备产生的热量。此外，空调还可以对机房内的空气进行除湿和过滤。
In the server room the air must be cooled, and the heat produced by the equipment must be extracted. It also dehumidifies and filters the air in the room.

D) 服务器机房是给办公室降温的最好方式。不必因大型设备牺牲办公空间。
The server room is the best way to cool the air in the office. No office space must be sacrificed for such a large piece of equipment.

A) 错误。备份磁带不应存放在服务器机房中。火灾会毁掉使用中的信息和备份信息。
Incorrect. Back-up tapes should not be stored in the server room. A fire would then destroy both the information in use and the back-up.

B) 错误。这不是要在服务器机房安装空调的原因。
Incorrect. This is not the reason why air conditioning should be installed in the server room.

C) 正确。考虑物理安全时，必须单独处理服务器机房。服务器机房包含易受湿热影响的敏感设备，其本身也会产生热量。（文献：A，第7.11.2章）
Correct. Server rooms must be approached separately when considering physical security. Server rooms contain sensitive equipment that is vulnerable to humidity and warmth and produce heat themselves. (Literature: A, Chapter 7.11.2)

D) 错误。服务器机房不是给整个办公室降温的地方。
Incorrect. The server room is not the place to cool the air in the entire office.

30 / 40
在物理安全中，可以应用多个保护环，并采取不同的措施。

哪一项**不**属于保护环？

In physical security, multiple protection rings can be applied in which different measures can be taken.

What is **not** a protection ring?

A) 建筑环
Building ring
B) 中环
Middle ring
C) 安全室环
Secure room ring
D) 外环
Outer ring

A) 错误。建筑物是关于进入场所的一环。
Incorrect. The building is a ring that deals with access to the premises.
B) 正确。保护环分为四环：外环、建筑物环、工作空间环和安全室环。（文献：A，第7.0.1章）
Correct. There are four protection rings: outer ring, building, workspaces, and secure room. (Literature: A, Chapter 7.0.1)
C) 错误。安全室环是一个有效区域，涉及的是要保护的资产。
Incorrect. The secure room ring is a valid zone and deals with the asset that is to be protected.
D) 错误。外环是一个有效区域，涉及的是场所周边地区。
Incorrect. The outer ring is a valid zone and deals with the area around the premises.

31 / 40
确保资产安全的控制因资产而异。

哪一项是确保资产安全的**最**适当方法?

The control to secure an asset depends on the asset.

What is the **most** appropriate way to secure the asset?

A) 通过填表并签字确保表格安全
Secure a form by having it filled out and signed off

B) 通过分配每个用户一台笔记本电脑，确保笔记本电脑安全
Secure a laptop by assigning it to a single user

C) 通过加密确保U盘安全
Secure a USB-stick with encryption

D) 通过备份确保联网安全
Secure an internet connection with a back-up

A) 错误。将包含信息的一张纸归档并不是一个适当的控制方法。
Incorrect. Filing a piece of paper with information is not an appropriate control.

B) 错误。人手一台笔记本电脑显然会更好，但这不是最合适的选择。用户账号管理和密码控制是更好的控制。
Incorrect. It is obviously better if a single person uses a single laptop, but this is not the most appropriate option. User account management and password control are better controls.

C) 正确。加密是确保U盘安全的有效控制手段。许多组织都采用这种控制方法，不论U盘内所存储信息的级别如何。（文献：A，第8.12章）
Correct. Encryption is a valid control for securing a USB-stick. Many organizations apply this control regardless of the classification of the information stored on the USB-stick. (Literature: A, Chapter 8.12)

D) 错误。使用备份并不是确保联网安全的最好、最直接的方法。
Incorrect. Using a back-up is not the best, direct way to secure the internet connection.

32 / 40
哪一项信息安全控制有助于在开发考系统时虑信息安全?

What information security control helps to develop systems with information security in mind?

A) 确保服务器冗余
Ensuring redundancy of the servers

B) 实施物理入口控制
Implementing physical entry controls

C) 对员工进行背景调查
Performing background checks on employees

D) 对信息资产使用数据分类分级
Using data classification on information assets

A) 正确。服务器冗余是系统开发时应该考虑的控制手段。（文献：A，第8.14章）
Correct. Server redundancy is a control that should be considered during system development. (Literature: A, Chapter 8.14)

B) 错误。这是加强信息安全的有效控制，但与系统开发无关。
Incorrect. This is a valid control to enhance information security but is not related to system development.

C) 错误。这是加强信息安全的有效控制，但与系统开发无关。
Incorrect. This is a valid control to enhance information security but is not related to system development.

D) 错误。这是加强信息安全的有效控制，但与系统开发无关。
Incorrect. This is a valid control to enhance information security but is not related to system development.

33 / 40
某组织改变了政策，现在允许员工远程办公。

现在应该采取什么控制?

An organization changes its policy. Employees are now allowed to work remotely.

What control should now be put in place?

A) 创建V-LAN对公司网络进行分段
Create V-LANs to segment the corporate network

B) 对公司网络上的信息进行加密
Encrypt the information on the corporate network

C) 在公司网络上安装防火墙
Install firewalls on the corporate network

D) 使用VPN连接到公司网络
Use a VPN to connect to the corporate network

A) 错误。确保机密性和职责分离的网络分段应该已经落实到位。这并不特别适用于变更远程办公政策的情况。
Incorrect. Segmenting networks to ensure confidentiality and segregation of duties should already be in place. These do not specifically apply to changing the remote-working policy.

B) 错误。加密是保护信息的重要手段，但并不特别适用于允许员工远程办公的情况。
Incorrect. Encryption is a vital tool to use to protect information, but it does not specifically apply to allowing employees to work remotely.

C) 错误。建立公司网络与外界之间的防火墙很重要，但这一措施应该已经落实到位。此外，防火墙不直接保护远程连接安全。
Incorrect. Firewalls between the corporate network and the outside world are important but these should already be in place. Also, firewalls do not directly secure remote connections.

D) 正确。允许员工远程办公时，使用VPN是一种应落实到位的控制。（文献：A，第8.2章）
Correct. The use of VPNs is a control that should be put in place when employees are allowed to work remotely. (Literature: A, Chapter 8.2)

34 / 40
某组织员工的工作用笔记本电脑经过非对称加密算法保护。为了降低密钥管理的成本，所有顾问都采用相同的密钥对。

如果某些信息被泄露，则应提供新的密钥。

在什么情况下应提供新的密钥?

The employees of an organization work on laptops that are protected by asymmetrical cryptography. To keep the management of the keys cheap, all consultants use the same key pair.

If certain information is compromised, new keys should be supplied.

In what case should new keys be supplied?

A) 当私钥为人所知时
When the private key becomes known
B) 当公钥为人所知时
When the public key becomes known
C) 当公钥基础结构（PKI）为人所知时
When the public key infrastructure (PKI) becomes known

A) 正确。在非对称加密中，对私钥保密非常重要。公钥可能公开。（文献：A，第8.24.5章）
Correct. In asymmetric encryption, it is important to keep the private key private. The public key may be known. (Literature: A, Chapter 8.24.5)
B) 错误。公钥可能对全世界公开。私钥应保密，以确保完整性和可用性。
Incorrect. The public key may be open to the whole world. The private key should be kept secret to ensure integrity and availability.
C) 错误。PKI用于非对称加密系统的密钥交换。
Incorrect. PKI is used for the exchange of keys for asymmetrical encryption systems.

35 / 40
公钥基础结构（PKI）能提供何种安全?

What sort of security does a public key infrastructure (PKI) offer?

A) PKI确保了定期备份公司数据。
A PKI ensures that back-ups of company data are made on a regular basis.
B) PKI向客户表明基于网络的业务是安全的。
A PKI shows customers that a web-based business is secure.
C) PKI验证哪个人或系统属于特定的公钥。
A PKI verifies which person or system belongs to a specific public key.

A) 错误。PKI并不能确保进行备份。
Incorrect. A PKI does not ensure making back-ups.
B) 错误。PKI保证了哪个人或系统属于特定的公钥。
Incorrect. A PKI provides guarantees regarding which person or system belongs to a specific public key.
C) 正确。PKI的一大特点是通过协议、程序和组织结构，为哪个人或系统属于特定的公钥提供保证。（文献：A，第8.24.6章）
Correct. A characteristic of a PKI is that through agreements, procedures, and an organization structure, it provides guarantees regarding which person or system belongs to a specific public key. (Literature: A, Chapter 8.24.6)

36 / 40
哪种类型的恶意软件是一种除了执行表面上的功能外，还故意进行辅助活动的程序？

Which type of malware is a program which, in addition to the function that it appears to perform, purposely conducts secondary activities?

A) 逻辑炸弹
Logic bomb
B) 间谍软件
Spyware
C) 木马
Trojan
D) 蠕虫
Worm

A) 错误。逻辑炸弹是编入软件系统中的一段代码。当满足特定条件时，这段代码将执行一个功能。但逻辑炸弹并不总是用于恶意目的。它并不总是进行辅助活动。
Incorrect. A logic bomb is a piece of code that is built into a software system. This code will then carry out a function when specific conditions are met. This is not always used for malicious purposes. It does not always conduct secondary activities.
B) 错误。间谍软件是一种计算机程序，可收集用户计算机信息并将这些信息发送给另一方。
Incorrect. Spyware is a computer program that collects information on the user's computer and sends this information to another party.
C) 正确。木马程序除了执行表面上的功能外，还故意进行计算机用户未察觉的辅助活动，从而损害受感染系统的完整性。（文献：A，第8.7.2章）
Correct. A trojan is a program which, in addition to the function that it appears to perform, purposely conducts secondary activities, unnoticed by the computer user, which can harm the integrity of the infected system. (Literature: A, Chapter 8.7.2)
D) 错误。蠕虫通过自我复制来构建一个受污染计算机网络。
Incorrect. A worm builds a network of contaminated computers by replicating itself.

37 / 40
哪种类型的恶意软件会通过自我复制来建立一个受污染的计算机网络?

Which type of malware builds a network of contaminated computers by replicating itself?

A) 逻辑炸弹
Logic bomb

B) 间谍软件
Spyware

C) 木马
Trojan

D) 蠕虫
Worm

A) 错误。逻辑炸弹是编入软件系统中的一段代码。当满足特定条件时，这段代码将执行一个功能。但逻辑炸弹并不总是用于恶意目的。
Incorrect. A logic bomb is a piece of code that is built into a software system. This code will then carry out a function when specific conditions are met. This is not always used for malicious purposes.

B) 错误。间谍软件是一种计算机程序，可收集计算机用户信息并将这些信息发送给另一方。
Incorrect. Spyware is a computer program that collects information on the computer user and sends this information to another party.

C) 错误。木马程序除了执行表面上的功能外，还故意进行计算机用户未察觉的辅助活动，从而损害受感染系统的完整性。
Incorrect. A trojan is a program which, in addition to the function that it appears to perform, purposely conducts secondary activities, unnoticed by the computer user, which can harm the integrity of the infected system.

D) 正确。这确实是蠕虫的作用。（文献：A，第8.7章）
Correct. This is what a worm does. (Literature: A, Chapter 8.7)

38 / 40
哪一项与信息安全有关的法律规章可以适用于所有组织?

Which is a legislative or regulatory act related to information security that can be imposed upon all organizations?

A) 《通用数据保护条例》（GDPR）
General Data Protection Regulation (GDPR)

B) 知识产权（IP）
Intellectual property (IP) rights

C) ISO/IEC 27001
ISO/IEC 27001

D) ISO/IEC 27002
ISO/IEC 27002

A) 正确。所有组织都应制定保护个人数据的方针和程序，而负责处理个人数据的每个人都应了解相关方针和程序。（文献：A，第5.33章）
Correct. All organizations should have a policy and procedures for personal data protection, which should be known by everybody who processes personal data. (Literature: A, Chapter 5.33)

B) 错误。该法规与组织的信息安全无关。
Incorrect. This regulation is not related to information security for organizations.

C) 错误。这是一项指导组织如何处理信息安全过程设置的标准。
Incorrect. This is a standard with guidelines for organizations on how to deal with the set-up of an information security process.

D) 错误。该标准又称“信息安全、网络安全和隐私保护——信息安全控制”，包含了信息安全策略和控制的指导方针。
Incorrect. This standard, also known as 'Information security, cybersecurity and privacy protection - Information security controls', contains guidelines for information security policy and controls.

39 / 40
哪项ISO标准侧重于信息安全控制的实施?

Which ISO standard is focused on the implementation of information security controls?

A) ISO/IEC 27000
ISO/IEC 27000
B) ISO/IEC 27001
ISO/IEC 27001
C) ISO/IEC 27002
ISO/IEC 27002
D) ISO/IEC 27005
ISO/IEC 27005

A) 错误。这是对ISO/IEC 27000系列标准的概述。
Incorrect. This is the general introduction to the ISO/IEC 27000 series of standards.
B) 错误。这是包含信息安全管理体系（ISMS）要求的标准。
Incorrect. This is the standard with requirements for an information security management system (ISMS).
C) 正确。这是指定信息安全控制及其实施指南的标准。（文献：A，第4.12章）
Correct. This is the standard specifying information security controls with guidance on their implementation. (Literature A, Chapter 4.12)
D) 错误。ISO/IEC 27005侧重于信息安全风险管理。
Incorrect. ISO/IEC 27005 focuses on information security risk management.

40 / 40
在欧洲，哪个组织的标准是**最**常用的?

The standards of which organization is **most** commonly used in Europe?

A) 美国国家标准协会（ANSI）
American National Standards Institute (ANSI)
B) 国际标准化组织（ISO）
International Organization for Standardization (ISO)
C) 国家标准技术研究所（NIST）
National Institute of Standards and Technology (NIST)

A) 错误。ANSI标准在美国更为常用。
Incorrect. The ANSI standards are more common in the United States of America.
B) 正确。在欧洲，ISO标准最为常用。（文献：A，第5.36章）
Correct. In Europe, the ISO standards are the most common. (Literature: A, Chapter 5.36)
C) 错误。NIST标准在美国更为常用。
Incorrect. The NIST standard is more common in the United States of America.

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	B	**21**	B
2	A	**22**	A
3	B	**23**	D
4	A	**24**	B
5	B	**25**	A
6	B	**26**	C
7	B	**27**	D
8	B	**28**	B
9	D	**29**	C
10	B	**30**	B
11	A	**31**	C
12	B	**32**	A
13	D	**33**	D
14	D	**34**	A
15	B	**35**	C
16	D	**36**	C
17	A	**37**	D
18	C	**38**	A
19	D	**39**	C
20	B	**40**	B

Driving Professional Growth

联系 EXIN

www.exinchina.cn

info.china@exin.com

WeChat ID: EXINCH