考试样题

2018 年 04 九月版

目录

考试说明

本试卷是基于 EXIN Information Security Foundation based on ISO/IEC 27001。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。每答对一题获得 1 分。如果您获得的总分数为 26 分或以上，证明您通过本考试。

考试时间为 60 分钟。

祝您好运!

考试样题

1 / 40
数据和信息之间的关系是什么?

A) 数据是结构化的信息。
B) 信息是具有含义和赋予价值的数据的集合。

2 / 40
为办理火灾保险，行政办公室必须确定其管理的数据的价值。

对组织而言，以下哪个要素对决定数据的价值**不**重要?

A) 数据的内容。
B) 丢失、不完整或不正确数据的可恢复程度。
C) 数据对业务流程的不可或缺性。
D) 使用数据的业务流程的重要性。

3 / 40
黑客获得访问Web服务器，可以读取包含信用卡号码的服务器文件。

信用卡文件的保密性、完整性、可用性（CIA）原则，哪一个被违反了?

A) 可用性
B) 机密性
C) 完整性

4 / 40
在你工作的公司的走廊里有一台网络打印机。许多员工打印后不会立即取回，而是让打印文件留在打印机上。

这样对信息的可靠性上会造成什么影响?

A) 信息的完整性不能得到保障。
B) 信息的可用性不能得到保障。
C) 信息的机密性不能得到保障。

5 / 40
一个执行很好的风险分析可以提供大量有用的信息。风险分析有四个主要目标。

以下哪一个**不**是风险分析的四个主要目标之一?

A) 识别资产和他们的价值
B) 实施适当的措施
C) 建立实施安全措施的成本和事件造成的成本之间的平衡
D) 确定相关的弱点和威胁

6 / 40
一个行政办公室将评估它所暴露的危险。

对信息可靠性产生破坏性影响而言，哪一项是我们对可能的事件的称呼?

A) 依赖性
B) 威胁
C) 弱点
D) 风险

7 / 40
什么是风险管理的目标?

A) 确定某一风险发生的概率。
B) 确定安全事件可能造成的损害。
C) 描述IT资源受到的威胁。
D) 实施措施，降低风险至一个可接受的水平。

8 / 40
几年前你开办公司。你的公司员工人数现在已经从1成长到20。你公司的信息价值也越来越大，你可以自己控制的日子一去不复返了。你知道你需要采取措施，但应该怎么做呢?你聘请了顾问，他建议你从定性风险分析开始。

什么是定性风险分析?

A) 这种分析遵循精确的统计概率计算，以计算由损坏造成的确切损失。
B) 这种分析基于场景和情景，并产生了对可能的威胁的主观看法。

9 / 40
Midwest保险公司发生火灾。消防队很快赶到现场，并在大火蔓延并烧毁整个房舍之前扑灭了大火。然而，服务器毁于火灾之中。保存在另一间屋子里的备份磁带已经融化，许多其他文件都丢失了。

通过这场火灾造成的间接损失的一个例子是什么?

A) 融化的备份磁带
B) 被烧毁的电脑系统
C) 烧毁文件
D) 灭火器引起的水破坏

10 / 40
你是某快递公司的老板。你已经进行了风险分析，现在要确定你的风险策略。你决定对大风险采取措施，但对小风险不采取措施。

这种风险策略叫什么?

A) 风险承受
B) 风险规避
C) 风险中性

11 / 40
以下哪项是人为威胁的实例?

A) USB 记忆棒向网络传播病毒。
B) 服务器机房灰尘太多。
C) 泄漏导致电力供应出现故障。

12 / 40
以下哪项是人为威胁的实例?

A) 雷击
B) 火灾
C) 网络钓鱼

13 / 40
你在一家大公司的办公室工作。你收到一个自称是从服务中心过来的电话。他向您询问您的密码。

这是什么威胁?

A) 自然威胁
B) 组织威胁
C) 社交工程

14 / 40
一个医疗保险公司的分支机构发生了火灾。人员转移到邻近的分支机构继续他们的工作。

在事件周期中，转移到备用场所的安排在哪个阶段？

A) 界于威胁和事件之间
B) 界于恢复和威胁之间
C) 界于损坏和恢复之间
D) 界于事件和损坏之间

15 / 40
信息涉及到很多可靠性的方面。 但是可靠性不断受到各种威胁。威胁的例子有：电缆松动，有人无意中改变信息，数据被私下使用或伪造。

以下例子中哪些是完整性的威胁？

A) 电缆松动
B) 数据无意识修改
C) 数据私下使用

16 / 40
一名工作人员否认发送了某消息。

这影响了信息可靠性的哪个方面？

A) 可用性
B) 正确性
C) 完整性
D) 机密性

17 / 40
以下哪一项**最**恰当地阐述了信息安全策略的目的？

A) 信息安全策略文件包含了风险分析与对策探索。
B) 信息安全策略为管理层提供信息安全方面的指导和支持。
C) 策略用于向安全计划提供必要的细节，使之更加具体。
D) 策略用于深入阐明威胁及其潜在后果。

18 / 40
服务台员工收到关于网络安全事件的报告。他的同事在线且对网络服务器操作系统有更多的经验。他把工单转移到他的同事。

以下哪个属于最好地描述了这种转移？

A) 功能升级
B) 层次升级

19 / 40
保险公司的工作人员发现一个策略的到期日在她未知的情况下改变了。而她是授权唯一可以开展这项工作的人。她向服务台汇报这个安全事件。

服务台人员记录以下信息：
- 日期和时间。
- 事件的描述。
- 以及事件可能的后果。

关于这一事件有关的最重要的信息，有哪些丢失了？

A) 时间报告者的姓名
B) 软件包的名称
C) PC 序号
D) 汇报事件的人名列表

20 / 40
在一个事件周期有四个连续的步骤。

事件阶段之后是哪个步骤？

A) 威胁
B) 损害
C) 恢复

21 / 40
以下哪个措施是预防措施？

A) 安装一个日志系统，确保系统的变化被记录下来。
B) 公司系统受到黑客攻击入侵后，关闭网络通信连接。
C) 把敏感信息放在保险箱里。

22 / 40
在火灾情况下，压制性的措施是什么？

A) 火灾保险
B) 火灾检测发现后灭火
C) 修复火灾造成的损失

23 / 40
信息分级的目的士什么？

A) 为了创建一个处置移动设施的手册。
B) 标签的应用使信息更容易识别。
C) 根据其敏感性构建信息。

24 / 40
谁被授权变更一个分档的级别?

A) 文档作者
B) 文档管理员
C) 文档所有者
D) 文档所有者的经理

25 / 40
机房由一个通行证读卡器进行出入口保护。只有系统管理部门有权限进入。

这是什么类型的安全措施?

A) 纠正类型的安全措施
B) 物理安全措施
C) 逻辑安全措施
D) 压制安全措施

26 / 40
强认证是针对需要高度保护区的访问控制。在强身份验证中，一个人的身份验证需要采用三因素。

需要出具哪些因素进行验证?

A) 你是什么
B) 你有什么
C) 你知道什么

27 / 40
物理安全可以扩展到多个区域（保护环），并采用不同的措施。

什么**不**是保护环?

A) 建筑
B) 中间环
C) 对象
D) 外圈

28 / 40
以下哪一个是物理措施缺乏的威胁结果?

A) 一个用户可以访问属于另一个用户的文件。
B) 因为过热，服务器关机。
C) 打印机上留有机密信息文档。
D) 黑客可以自由访问计算机网络。

29 / 40
以下哪一项是技术措施?

A) 分配信息所有者。
B) 加密文件。
C) 创建策略，明确电子邮件可以发送的范围。
D) 把系统管理密码锁进保险箱中。

30 / 40
中央服务器的备份保存在同一个受保护的服务器机房中。

组织面临什么样的风险?

A) 如果服务器损坏，需要很长时间才能恢复运行。
B) 如果发生火灾，将无法恢复系统到之前的状态。
C) 没有人对备份负责。
D) 未经授权者可轻松取得备份。

31 / 40
以下哪一个恶意软件会造成计算机网络污染?

A) 逻辑炸弹
B) 风暴蠕虫和僵尸网络
C) 木马
D) 间谍软件

32 / 40
组织内，一个安全人员检测某员工的电脑被恶意软件感染。该恶意软件是一个有针对性的钓鱼攻击。

以下哪个行动**最**有利于防止今后发生类似事件?

A) 实施MAC技术
B) 启动安全意识程序
C) 更新防火墙策略
D) 更新垃圾邮件过滤器的签名

33 / 40
你在一家中型企业的IT部门工作。最近多次发生机密信息落入坏人之手。这损害了公司的形象。你被要求提出组织保障措施，来保护你们公司的笔记本电脑。

你**首先**应该采取的步骤是什么?

A) 制定一个关于移动媒体的政策（掌上电脑、笔记本电脑、智能手机、U盘）。
B) 指派安全人员。
C) 加密笔记本电脑的硬盘和USB盘。
D) 设定访问控制策略。

34 / 40
保障组织内信息安全连贯性的系统名称是什么?

A) 信息安全管理体系（ISMS）
B) Rootkit
C) 安全规章，用以保护政府要求的特殊信息

35 / 40
下列哪一选项是“确定一个人的身份是正确的”的术语?

A) 验证
B) 授权
C) 识别

36 / 40
为什么保持一个灾难恢复计划更新和定期测试是必要的?

A) 为了保证对办公场所之外的备份具有访问能力。
B) 为了能够应付日常发生的故障。
C) 否则，当一个偶然发生的事件真的发生时，计划恢复计划和通用程序已经不充分了，或者已经过时。
D) 因为这是个人信息保护法规的要求。

37 / 40
哪部立法，可以允许用户要求检查他/她的注册数据?

A) 公共记录法
B) 个人数据保护法
C) 计算机犯罪法
D) 政府信息（公共访问）法

38 / 40
哪一个是所有组织适用的信息安全立法或监管行动?

A) 知识产权法
B) ISO/IEC 27001
C) ISO/IEC 27002
D) 个人数据保护法

39 / 40
你是某快递公司的老板。你注意到你的雇员，在等待交货时做其他的事情。他们利用这段时间来发送和阅读他们的私人邮件和上网浏览。

在法律方面，在哪些方面你可以用来管理互联网和电子邮件设施的使用?

A) 安装一个应用程序，使得某些网站无法访问和过滤电子邮件附件。
B) 起草一份行为守则，规范雇主和员工互联网和电子邮件使用的权利和义务。
C) 实施隐私规章。
D) 安装病毒扫描系统。

40 / 40
哪种情况下，雇主被允许检查工作场所互联网和电子邮件服务是否被员工用于私人用途?

A) 员工在每次访问被检查后告知。这种情况下，雇主可以检查。
B) 员工被告知，访问可能被检查。这种情况下，雇主可以检查。
C) 当安装了防火墙时，雇主可以检查。

答案解析

1 / 40
数据和信息之间的关系是什么?

A) 数据是结构化的信息。
B) 信息是具有含义和赋予价值的数据的集合。

A) 错误。信息是结构化的数据。
B) 正确。信息对收集者来说，是具有意义的数据。（第3章）

2 / 40
为办理火灾保险，行政办公室必须确定其管理的数据的价值。

对组织而言，以下哪个要素对决定数据的价值**不**重要?

A) 数据的内容。
B) 丢失、不完整或不正确数据的可恢复程度。
C) 数据对业务流程的不可或缺性。
D) 使用数据的业务流程的重要性。

A) 正确。数据的内容不能决定其价值。（第4章）
B) 错误。相比难以或不可能恢复的数据，可轻松恢复的丢失、不完整或不正确的数据价值较低。
C) 错误。数据对业务流程的不可或缺性部分决定价值。
D) 错误。只要对重要业务流程至关重要，数据就很有价值。

3 / 40
黑客获得访问Web服务器，可以读取包含信用卡号码的服务器文件。

信用卡文件的保密性、完整性、可用性（CIA）原则，哪一个被违反了?

A) 可用性
B) 机密性
C) 完整性

A) 错误。黑客没有删除文件或对授权实体拒绝访问攻击。可用性没有被影响。
B) 正确。黑客可以读取文件（机密性）。（第3章）
C) 错误。信用卡文件中没有更改信息，因此没有违反文件的完整性。

4 / 40
在你工作的公司的走廊里有一台网络打印机。许多员工打印后不会立即取回，而是让打印文件留在打印机上。

这样对信息的可靠性上会造成什么影响?

A) 信息的完整性不能得到保障。
B) 信息的可用性不能得到保障。
C) 信息的机密性不能得到保障。

A) 错误。打印信息的完整性依然具备，因为它们是纸质文件。
B) 错误。打印出来后，信息依然是可用的。
C) 正确。信息会被没有访问权限的人员获取并阅读。（第3章）

5 / 40
一个执行很好的风险分析可以提供大量有用的信息。风险分析有四个主要目标。

以下哪一个**不**是风险分析的四个主要目标之一?

A) 识别资产和他们的价值
B) 实施适当的措施
C) 建立实施安全措施的成本和事件造成的成本之间的平衡
D) 确定相关的弱点和威胁

A) 错误。这是风险分析的主要目标。
B) 正确。这不是风险分析的主要目标。当风险分析确定需要安全措施的时候，需要选择合适的措施。（第3章）
C) 错误。这是风险分析的主要目标。
D) 错误。这是风险分析的主要目标。

6 / 40
一个行政办公室将评估它所暴露的危险。

对信息可靠性产生破坏性影响而言，哪一项是我们对可能的事件的称呼?

A) 依赖性
B) 威胁
C) 弱点
D) 风险

A) 错误。依赖性不是一个事件。
B) 正确。威胁是可能对信息的可靠性产生负面影响的潜在事件。（第3章）
C) 错误。弱点是一个对象受到威胁影响的程度。
D) 错误。风险是指由于一个或多个导致中断的威胁在一段时间内的平均预期损失。

7 / 40
什么是风险管理的目标?

A) 确定某一风险发生的概率。
B) 确定安全事件可能造成的损害。
C) 描述IT资源受到的威胁。
D) 实施措施，降低风险至一个可接受的水平。

A) 错误。这是风险分析的一部分。
B) 错误。这是风险分析的一部分。
C) 错误。这是风险分析的一部分。
D) 正确。风险管理的目标就是降低风险至可接受的水平。（第3章）

8 / 40
几年前你开办公司。你的公司员工人数现在已经从1成长到20。你公司的信息价值也越来越大，你可以自己控制的日子一去不复返了。你知道你需要采取措施，但应该怎么做呢？你聘请了顾问，他建议你从定性风险分析开始。

什么是定性风险分析?

A) 这种分析遵循精确的统计概率计算，以计算由损坏造成的确切损失。
B) 这种分析基于场景和情景，并产生了对可能的威胁的主观看法。

A) 错误。对定量风险分析来说，试图计算确定各种事件的概率和每一个特定事件造成损失的可能程度。
B) 正确。定性风险分析包括定义各种威胁，确定漏洞的范围，并制定攻击对策。（第3章）

9 / 40
Midwest保险公司发生火灾。消防队很快赶到现场，并在大火蔓延并烧毁整个房舍之前扑灭了大火。然而，服务器毁于火灾之中。保存在另一间屋子里的备份磁带已经融化，许多其他文件都丢失了。

通过这场火灾造成的间接损失的一个例子是什么?

A) 融化的备份磁带
B) 被烧毁的电脑系统
C) 烧毁文件
D) 灭火器引起的水破坏

A) 错误。磁带融化是火灾造成的直接损失。
B) 错误。燃毁的电脑系统是火灾造成的直接损失。
C) 错误。烧毁的文件是火灾造成的直接损失。
D) 正确。因为消防系统喷水造成的损失是火灾造成的间接损失，这是灭火的副作用，其目的是最大限度地减少火灾造成的损失。（第3章）

10 / 40
你是某快递公司的老板。你已经进行了风险分析，现在要确定你的风险策略。你决定对大风险采取措施，但对小风险不采取措施。

这种风险策略叫什么?

A) 风险承受
B) 风险规避
C) 风险中性

A) 正确。这种措施意味着一定的风险被接受。（第3章）
B) 错误。这意味着采取措施，使威胁得以抵消到不再导致事件发生的程度。
C) 错误。这意味着采取了安全措施，使威胁不再显现，或者，发生后所造成的损害最小化。

11 / 40
以下哪项是人为威胁的实例?

A) USB 记忆棒向网络传播病毒。
B) 服务器机房灰尘太多。
C) 泄漏导致电力供应出现故障。

A) 正确。USB 记忆棒都为人为插入的。因此，如果因为插入记忆棒而使病毒进入网络，则属于人为威胁。（第3章）
B) 错误。灰尘不属于人为威胁。
C) 错误。泄漏不属于人为威胁。

12 / 40
以下哪项是人为威胁的实例?

A) 雷击
B) 火灾
C) 网络钓鱼

A) 错误。雷电属于非人为威胁的实例。
B) 错误。火灾属于非人为威胁的实例。
C) 正确。网络钓鱼（诱使用户访问错误的网站）是人为威胁的一种表现形式。（第3章）

13 / 40
你在一家大公司的办公室工作。你收到一个自称是从服务中心过来的电话。他向您询问您的密码。

这是什么威胁?

A) 自然威胁
B) 组织威胁
C) 社交工程

A) 错误。电话是人类的行为，不是自然威胁。
B) 错误。组织威胁不是一类威胁的通用术语。
C) 正确。使用正确的表达方式或知名人士及其部门的名字给人一种同事试图获取公司和商业秘密的印象。你应该检查你是否实际上真的跟服务台对话。一个服务台员工是不会询问您的密码的。（第3章）

14 / 40
一个医疗保险公司的分支机构发生了火灾。人员转移到邻近的分支机构继续他们的工作。

在事件周期中，转移到备用场所的安排在哪个阶段?

A) 界于威胁和事件之间
B) 界于恢复和威胁之间
C) 界于损坏和恢复之间
D) 界于事件和损坏之间

A) 错误。没有事件发生时，安排备用场所是昂贵的。
B) 错误。恢复是将备用设备投入运行之后发生。
C) 错误。损害和恢复，是受备用安排限制的。
D) 正确。准备备用设施是为了降低损害的纠正措施。（第3章）

15 / 40
信息涉及到很多可靠性的方面。 但是可靠性不断受到各种威胁。威胁的例子有：电缆松动，有人无意中改变信息，数据被私下使用或伪造。

以下例子中哪些是完整性的威胁?

A) 电缆松动
B) 数据无意识修改
C) 数据私下使用

A) 错误。电缆松动是信息可用性的威胁。
B) 正确。数据无意识修改是完整性威胁。（第3章）
C) 错误。数据私下使用是误用导致的，是数据机密性的威胁。

16 / 40
一名工作人员否认发送了某消息。

这影响了信息可靠性的哪个方面?

A) 可用性
B) 正确性
C) 完整性
D) 机密性

A) 错误。基础设施超载运行是可用性威胁的一个例子。
B) 错误。正确性不属于可靠性，而是完整性的一个特征。
C) 正确。否认发送消息是与不可否认性有关，是完整性的一种威胁。（第3章）
D) 错误。误用和/或数据泄密，是机密性的一种威胁。

17 / 40
以下哪一项**最**恰当地阐述了信息安全策略的目的?

A) 信息安全策略文件包含了风险分析与对策探索。
B) 信息安全策略为管理层提供信息安全方面的指导和支持。
C) 策略用于向安全计划提供必要的细节，使之更加具体。
D) 策略用于深入阐明威胁及其潜在后果。

A) 错误。这是风险分析和风险管理的目的。
B) 正确。安全策略用于指导和支持信息安全管理。（第5章）。
C) 错误。是安全计划使信息安全策略具体化。该计划包含应当采取哪些措施、由谁负责哪些事宜以及措施实施细则等内容。
D) 错误。深入阐明威胁及其潜在后果是威胁分析的目的。

18 / 40
服务台员工收到关于网络安全事件的报告。他的同事在线且对网络服务器操作系统有更多的经验。他把工单转移到他的同事。

以下哪个属于最好地描述了这种转移?

A) 功能升级
B) 层次升级

A) 正确。如果服务台员工无法处理事件，事件可以升级到具有更多的专业知识能解决问题的人。这就是所谓的功能（水平）的升级。（第16章）
B) 错误。这就是所谓的功能（水平）的升级。层级升级是指把任务移交给更有权威的人。

19 / 40
保险公司的工作人员发现一个策略的到期日在她未知的情况下改变了。而她是授权唯一可以开展这项工作的人。她向服务台汇报这个安全事件。

服务台人员记录以下信息：
- 日期和时间。
- 事件的描述。
- 以及事件可能的后果。

关于这一事件有关的最重要的信息，有哪些丢失了？

A) 时间报告者的姓名
B) 软件包的名称
C) PC 序号
D) 汇报事件的人名列表

A) 正确。报告事件时，最小需要记录汇报者的姓名。（第16章）
B) 错误。这是可在以后补充的附加信息。
C) 错误。这是可在以后补充的附加信息。
D) 错误。这是可在以后补充的附加信息。

20 / 40
在一个事件周期有四个连续的步骤。

事件阶段之后是哪个步骤?

A) 威胁
B) 损害
C) 恢复

A) 错误。损害是在事件之后，正确的步骤是威胁、事件、损害、恢复。
B) 正确。正确的步骤是威胁、事件、损害、恢复。（第16章）
C) 错误。损害是在事件之后，正确的步骤是威胁、事件、损害、恢复。

21 / 40
以下哪个措施是预防措施?

A) 安装一个日志系统，确保系统的变化被记录下来。
B) 公司系统受到黑客攻击入侵后，关闭网络通信连接。
C) 把敏感信息放在保险箱里。

A) 错误。日志系统只有在事件发生后可以研究发生了什么事。这是一个侦探措施，旨在检测事件发生。
B) 错误。闭所有的互联网流量是一个压制类型的措施，旨在限制事件影响。
C) 正确。保险箱是预防措施，以避免损坏存储的安全敏感信息 。（第3章）

22 / 40
在火灾情况下，压制性的措施是什么？

A) 火灾保险
B) 火灾检测发现后灭火
C) 修复火灾造成的损失

A) 错误。火灾保险，是为了提供火灾后的财务保障。
B) 正确。这是压制措施，最大限度地减少火灾造成的损失。（第3章）
C) 错误。这不是一个压制的措施，它不减少火灾造成的损失。

23 / 40
信息分级的目的士什么？

A) 为了创建一个处置移动设施的手册。
B) 标签的应用使信息更容易识别。
C) 根据其敏感性构建信息。

A) 错误。创建手册是为了用户使用，与信息分级无关。
B) 错误。设计标签，是按照信息分级要求的开展的一种方式。
C) 正确。信息分级是根据信息的敏感程度不同水平来定义的，以便于信息结构化。（第3章和第8章）

24 / 40
谁被授权变更一个分档的级别？

A) 文档作者
B) 文档管理员
C) 文档所有者
D) 文档所有者的经理

A) 错误。作者可以修改内容，不能变更文档级别。
B) 错误。管理员不能变更文档级别。
C) 正确。所有者要确保资产分级或不分级，并被授权根据需求进行文档级别的变更。（第3章和第8章）
D) 错误。所有者的经理没有这个授权。

25 / 40
机房由一个通行证读卡器进行出入口保护。只有系统管理部门有权限进入。

这是什么类型的安全措施?

A) 纠正类型的安全措施
B) 物理安全措施
C) 逻辑安全措施
D) 压制安全措施

A) 错误。纠正安全措施，例如恢复措施。
B) 正确。这是一个物理安全措施。（第3章和第11章）
C) 错误。逻辑安全措施，控制软件和信息的访问权限，不是房间等的物理访问权限。
D) 错误。压制类型的安全措施目的是为了最小化损害的后果。

26 / 40
强认证是针对需要高度保护区的访问控制。在强身份验证中，一个人的身份验证需要采用三因素。

需要出具哪些因素进行验证?

A) 你是什么
B) 你有什么
C) 你知道什么

A) 错误。你是谁，不是通行证验证的例子。
B) 正确。你有什么，是通行证验证的例子。（第11章）
C) 错误。你知道什么，不是通行证验证的例子。

27 / 40
物理安全可以扩展到多个区域（保护环），并采用不同的措施。

什么**不**是保护环?

A) 建筑
B) 中间环
C) 对象
D) 外圈

A) 错误。建筑是一个可以进行边界访问控制的区域。
B) 正确。保护环：外环（在房屋周界保护），建筑（进入处所保护），工作空间（周界内的区域，房间也被称为“内圈”）、对象（资产，是被保护的）。没有中间环这样的说法。（第11章）
C) 错误。对象是被保护的一个资产的范围。
D) 错误。外圈是被周界进行保护的区域。

28 / 40
以下哪一个是物理措施缺乏的威胁结果?

A) 一个用户可以访问属于另一个用户的文件。
B) 因为过热，服务器关机。
C) 打印机上留有机密信息文档。
D) 黑客可以自由访问计算机网络。

A) 错误。逻辑访问控制用来保护文档的访问权限，防止另一个没有权限的用户访问。
B) 正确。物理安全包括设备所属环境的气候条件的保护。（如，空调，湿度）（第11章）
C) 错误。安全策略应该包括如何处理机密文件的规则。所有的员工都应该对此策略有充分的认识。这是一个组织措施。
D) 错误。防止黑客进入计算机或网络是一项技术措施。

29 / 40
以下哪一项是技术措施?

A) 分配信息所有者。
B) 加密文件。
C) 创建策略，明确电子邮件可以发送的范围。
D) 把系统管理密码锁进保险箱中。

A) 错误。分配信息所有者，是一个组织措施。
B) 正确。这是一个技术措施，防止未被授权的人员阅读信息。（第6章）
C) 错误。这是一个组织措施，可以被写进员工合同中的行为守则。
D) 错误。这是一个组织措施。

30 / 40
中央服务器的备份保存在同一个受保护的服务器机房中。

组织面临什么样的风险?

A) 如果服务器损坏，需要很长时间才能恢复运行。
B) 如果发生火灾，将无法恢复系统到之前的状态。
C) 没有人对备份负责。
D) 未经授权者可轻松取得备份。

A) 错误。相反，这样做能够加快系统恢复正常的速度。
B) 正确。备份在火灾中遭损毁的风险非常大。（第11章）
C) 错误。责任与存放位置没有任何关系。
D) 错误。计算机房已上锁。

31 / 40
以下哪一个恶意软件会造成计算机网络污染?

A) 逻辑炸弹
B) 风暴蠕虫和僵尸网络
C) 木马
D) 间谍软件

A) 错误。逻辑炸弹是不是恶意软件。这是一个软件系统中的一段代码。
B) 正确。蠕虫是一个小的计算机程序，故意自我复制，利用其主机的网络设施传播。（第12章）
C) 错误。木马是一种程序，在用户无意识情况下，能执行某种辅助活动。
D) 错误。间谍软件是一种计算机程序，收集计算机用户信息并将此信息发送给另一方。

32 / 40
组织内，一个安全人员检测某员工的电脑被恶意软件感染。该恶意软件是一个有针对性的钓鱼攻击。

以下哪个行动**最**有利于防止今后发生类似事件?

A) 实施MAC技术
B) 启动安全意识程序
C) 更新防火墙策略
D) 更新垃圾邮件过滤器的签名

A) 错误。MAC访问控制；这并不妨碍用户被引诱去执行某些行动，导致针对性的攻击。
B) 正确。这种威胁的脆弱性就是用户的无意识。用户被引诱来执行一些代码导致攻击发生，通常用户违反政策（例如安装可疑软件）。采取安全意识计划，应对在未来将减少此类攻击复发机会。（第12章）
C) 错误。尽管防火墙可以如封锁某些通信，从而避免恶意软件的安装。但是防火墙不能防止此类攻击复发的威胁。
D) 错误。有针对性的攻击，没有必要使用电子邮件。攻击者可能使用社交媒体，甚至手机与受害人接触。

33 / 40
你在一家中型企业的IT部门工作。最近多次发生机密信息落入坏人之手。这损害了公司的形象。你被要求提出组织保障措施，来保护你们公司的笔记本电脑。

你**首先**应该采取的步骤是什么?

A) 制定一个关于移动媒体的政策（掌上电脑、笔记本电脑、智能手机、U盘）。
B) 指派安全人员。
C) 加密笔记本电脑的硬盘和USB盘。
D) 设定访问控制策略。

A) 正确。制定如何利用移动媒体的策略，是一个组织措施和安全措施，可以应用到笔记本电脑上。（第6章）
B) 错误。指定安全人员的技术措施。当有人把一个笔记本电脑带离办公，存在信息泄露的风险。
C) 错误。加密的笔记本电脑和USB硬盘棒是技术措施。这可以在组织内进行实施。
D) 错误。访问控制策略是一个组织措施，可为物理环境访问或IT系统访问控制。

34 / 40
保障组织内信息安全连贯性的系统名称是什么?

A) 信息安全管理体系（ISMS）
B) Rootkit
C) 安全规章，用以保护政府要求的特殊信息

A) 正确。ISMS是ISO/IEC 27001的描述方法。（第3章）
B) 错误。Rootkit是一种恶意的第三方常用软件工具（通常被黑客使用）。
C) 错误。这是属于政府的规章，如何处理特殊信息。

35 / 40
下列哪一选项是“确定一个人的身份是正确的”的术语?

A) 验证
B) 授权
C) 识别

A) 正确。确定一个人的身份是正确的被称为验证。（第9章）
B) 错误。授予给定的计算机或网络的访问权利称为授权。
C) 错误。识别是进行身份已知的过程。

36 / 40
为什么保持一个灾难恢复计划更新和定期测试是必要的?

A) 为了保证对办公场所之外的备份具有访问能力。
B) 为了能够应付日常发生的故障。
C) 否则，当一个偶然发生的事件真的发生时，计划恢复计划和通用程序已经不充分了，或者已经过时。
D) 因为这是个人信息保护法规的要求。

A) 错误。这是恢复系统的一种技术措施。
B) 错误。对一般的中断事件来说，事件程序通常是充分的。
C) 正确。偶然发生的事件需要保持更新的计划和测试的规划。（第17章）
D) 错误。个人信息保护法规包括隐私或个人数据。

37 / 40
哪部立法，可以允许用户要求检查他/她的注册数据？

A) 公共记录法
B) 个人数据保护法
C) 计算机犯罪法
D) 政府信息（公共访问）法

A) 错误。公共档案立法规定了存储和归档文件材料的销毁。
B) 正确。个人数据保护立法规定了这个权力。（第18章）
C) 错误。计算机犯罪立法，从法律上确认通过先进的信息技术犯下的罪行。一种新的犯罪行为的一个例子，是电脑黑客。
D) 错误。政府信息公开访问法，规定了政府文件书面审查的规则。个人数据不是政府文件。

38 / 40
哪一个是所有组织适用的信息安全立法或监管行动？

A) 知识产权法
B) ISO/IEC 27001
C) ISO/IEC 27002
D) 个人数据保护法

A) 错误。这个法规不是组织的信息安全相关。
B) 错误。这个标准是组织建立信息安全流程的准则。
C) 错误。这个标准是组织建立信息安全策略和措施的实践指南。
D) 正确。所有的组织都应该有一个个人数据保护的政策和程序，让每个人都知道谁在处理个人数据。（第18章）

39 / 40
你是某快递公司的老板。你注意到你的雇员，在等待交货时做其他的事情。他们利用这段时间来发送和阅读他们的私人邮件和上网浏览。

在法律方面，在哪些方面你可以用来管理互联网和电子邮件设施的使用？

A) 安装一个应用程序，使得某些网站无法访问和过滤电子邮件附件。
B) 起草一份行为守则，规范雇主和员工互联网和电子邮件使用的权利和义务。
C) 实施隐私规章。
D) 安装病毒扫描系统。

A) 错误。安装这种软件，不能限制互联网和电子邮件用于私人使用。这是一个技术措施。
B) 正确。在行为守则上确定使用互联网和电子邮件的要求， 记录哪些网站可以或不可以访问，被允许的私人使用的范围。这些都是组织内部规定。（第18章）
C) 错误。隐私法规只对员工和客户的个人数据的使用，没有涉及到互联网和电子邮件的使用。
D) 错误。病毒扫描程序检查恶意软件通过电子邮件和互联网连接传入。但它不规范互联网和电子邮件的使用。这是一个技术措施。

40 / 40
哪种情况下，雇主被允许检查工作场所互联网和电子邮件服务是否被员工用于私人用途?

A) 员工在每次访问被检查后告知。这种情况下，雇主可以检查。
B) 员工被告知，访问可能被检查。这种情况下，雇主可以检查。
C) 当安装了防火墙时，雇主可以检查。

A) 错误。每次检查后，员工不需被通知。
B) 正确。员工必须知道，而雇主有权监控使用IT服务。（第3章和第18章）
C) 错误。防火墙用来防止外部入侵，不影响雇主监控服务的使用权。

试题评分

如下表格为套样题的正确答案选项，供参考使用。

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

联系 EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER