认证备考指南

202309 版本

内容

1. 概述

EXIN Information Security Management Professional based on ISO/IEC 27001 (ISMP.CH)

范围

EXIN Information Security Management Professional based on ISO/IEC 27001（ISMP.CH）认证确认专业人员可以管理组织的、人员相关的、物理的以及技术的信息安全风险，与此同时尊重利益相关者的利益。

本认证包括以下主题：
- 信息安全视角
- 风险管理
- 信息安全控制

总结

经济全球化促成信息交流日益频繁。信息交流不仅跨越国界，还跨越私域与商域之间的微妙界线。问责范围随着受管理信息的增加而扩大。信息必须受到保护，防止擅自获取信息或者意外或恶意篡改或破坏信息，需要时必须做到信息可用。

另有一些趋势助推信息安全学科的重要性：
- 合规要求与日俱增。大多数国家制定了多部法律或法规来管理各类数据的使用和保护。这类法律的数量不断增加，其要求也在不断提高。
- 许多行业，尤其是金融界，在政府法规之外补充了其他法规。行业法规的数量和复杂性同样不断增加。
- 各行业、国家和国际安全标准不断制定和完善。
- 有时，组织需要安全认证和可审计的证据来证明组织符合安全标准和/或最佳实践，以作为开展业务的条件。

国际信息安全管理标准 ISO/IEC 27001 是一项广受认可和被广泛引用的标准，为信息安全项目提供了组织及管理的框架。实施基于此标准的程序将有助于组织实现其目标，即满足当今复杂的运营环境中所面临的诸多要求。深刻理解此标准对每个信息安全专业人士的个人发展都很重要。

在 EXIN Information Security Management based on ISO/IEC 27001 项目中，使用了以下定义：信息安全是指维护信息的机密性、完整性和可用性。

背景

EXIN Information Security Management Professional based on ISO/IEC 27001 认证是 EXIN Information Security Management based on ISO/IEC 27001 认证项目的一部分。

目标群体

该认证适用于参与信息安全项目实施、评估和报告的所有安全专业人员，包括以下角色：

- 信息安全经理（ISM）
- 信息安全官（ISO）
- 部门经理
- 流程经理
- 承担安全责任的项目经理

认证要求

- 顺利通过 EXIN Information Security Management Professional based on ISO/IEC 27001 考试。
- 顺利完成 EXIN 授权的 EXIN Information Security Management Professional based on ISO/IEC 27001 培训，包括实践作业。

考试细节

考试类型:	单选题
题目数量:	30
通过分数:	65% (20/30 题)
是否开卷考试:	否
是否记笔记:	否
是否允许携带电子设备/辅助设备:	否
考试时间:	90 分钟

EXIN 的考试规则和规定适用于本次考试。

布鲁姆级别

EXIN Information Security Management Professional based on ISO/IEC 27001 认证根据布鲁姆分类学修订版对考生进行布鲁姆 3 级和 4 级测试。

- 布鲁姆 3 级：应用——表明考生有能力在与学习环境不同的情境下使用所学信息。这类题目旨在证明考生能够以不同的方式或新的方式应用所掌握的知识、实例、方法和规则，在新的情况下解决问题。这类题目通常包含一个简短的场景。
- 布鲁姆 4 级：分析——表明考生有能力将所学信息拆分并加以理解。布鲁姆级别主要通过实践作业进行测试。实践作业是为了证明考生能够辨明动机或原因，作出推断并找到支持归纳的证据，从而检查并拆分信息。

培训

培训时长

本培训课程时长建议 21 小时。该时长包括学员实践作业、考试准备和短暂休息。该时长不包括午餐休息、家庭作业以及考试的时间。

建议个人学习时间

112 小时（4 ECTS），根据现有知识的掌握情况可能有所不同。

培训机构

您可通过 EXIN 官网 www.exin.com 查找该认证的授权培训机构。

2. 考试要求

考试要求详见考试说明。下表列出模块主题（考试要求）和副主题（考试规范）。

考试要求	考试规范	权重
1. 信息安全视角		**10%**
	1.1 信息安全的业务收益	3,3%
	1.2 客户视角的治理	3,3%
	1.3 供应商负有的安全保障责任	3,3%
2. 风险管理		**30%**
	2.1 风险管理的原则	10%
	2.2 控制风险	10%
	2.3 处理残余风险	10%
3. 信息安全控制		**60%**
	3.1 组织控制	20%
	3.2 技术控制	20%
	3.3 物理控制和人员控制	20%
	合计	**100%**

考试规范

1 信息安全视角

1.1 信息安全的业务收益

考生能够...

1.1.1 根据业务价值区分信息类型。

1.1.2 说明信息安全管理体系的特点。

1.2 客户视角的治理

考生能够...

1.2.1 说明外包时信息治理的重要性。

1.2.2 基于安全控制推荐供应商。

1.3 供应商负有的安全保障责任

考生能够...

1.3.1 区分服务管理过程中的安全问题。

1.3.2 支持合规活动。

2 风险管理

2.1 风险管理的原则

考生能够...

2.1.1 解释分析风险的原则。

2.1.2 识别分级资产的风险。

2.1.3 计算分级资产的风险。

2.2 控制风险

考生能够...

2.2.1 根据机密性、完整性和可用性（CIA）对控制进行分类。

2.2.2 根据事件周期阶段选择控制。

2.2.3 选择实施控制的相关指南。

2.3 处理残余风险

考生能够...

2.3.1 区分风险策略。

2.3.2 编制控制的业务案例。

2.3.3 编制风险分析报告。

3 信息安全控制

3.1 组织控制

考生能够...

3.1.1 编写信息安全方针和规程。

3.1.2 实施信息安全事件处理。

3.1.3 在组织内开展意识活动。

3.1.4 落实信息安全的角色和职责。

3.1.5 支持制定和测试业务连续性计划。

3.2 技术控制

考生能够...

3.2.1 说明安全架构的目的。

3.2.2 说明安全服务的目的。

3.2.3 说明安全元素在 IT 基础架构中的重要性。

3.3 物理控制和人员控制

考生能够...

3.3.1 建议针对物理访问的控制。

3.3.2 建议针对聘用生命周期的安全控制。

3. 考试术语表

本章节包含了考生应熟知的术语和缩写。

请注意单独学习术语并不能满足考试要求。学员必须了解其概念，并且能够举例说明。

英文	中文
acceptance	接受
access management	访问管理
asset	资产
attack	攻击
audit	审计
authentication	身份验证
authorization	授权
availability	可用性
avoidance	避免
awareness (campaigns)	意识（活动）
business continuity (plan)	业务连续性（计划）
business impact analysis (BIA)	业务影响分析（BIA）
certificate authority (CA)	认证机构（CA）
cloud computing	云计算
code of practice for information security	信息安全实施规范
compliance	合规性
confidentiality	机密性
controls	控制
cryptography	密码学
defense	防御
disaster recovery plan	灾难恢复计划
encryption	加密
escrow agreement	托管协议
event management	事态管理
firewall	防火墙
host-based intrusion detection and prevention system (host-based IDPS)	基于主机的入侵检测防御系统（基于主机的IDPS）
incident management	事件管理
incident response plan	事件响应计划
information security management system (ISMS)	信息安全管理体系（ISMS）
information security perspectives	信息安全视角
information security program	信息安全程序
integrity	完整性
ISO/IEC 27001	ISO/IEC 27001
ISO/IEC 27002	ISO/IEC 27002
IT strategy	IT 战略
legislation	法规
logical access control	逻辑访问控制
mitigation	缓解
mitigation plan	缓解计划
network content filter	网络内容过滤
network-based intrusion detection and prevention system (network-based IDPS)	基于网络的入侵检测防御系统（基于网络的IDPS）

open design	开放设计
perimeter	边界
physical access control	物理访问控制
Plan-Do-Check-Act (PDCA) cycle	计划-实施-检查-改进（PDCA）循环
policy	方针
private key	私钥
problem management	问题管理
procedure	规程
protocol	协议
public key	公钥
public key infrastructure (PKI)	公钥基础设施（PKI）
Recovery Point Objective (RPO)	恢复点目标（RPO）
Recovery Time Objective (RTO)	恢复时间目标（RTO）
residual risk	残余风险
retention policy	保留方针
risk	风险
risk analysis	风险分析
risk appetite	风险偏好
risk assessment	风险评估
risk management framework	风险管理框架
risk manager	风险经理
risk strategy	风险策略
risk treatment (plan)	风险处理（计划）
security architecture	安全架构
security governance	安全治理
security services	安全服务
Service Oriented Architecture (SOA)	面向服务的架构（SOA）
Statement of Applicability (SoA)	适用性声明（SoA）
third party	第三方
threats	威胁
topic-specific policy	特定主题方针
Total Cost of Ownership (TCO)	总体拥有成本 (TCO)
transference	转移
virtual private network (VPN)	虚拟专用网络（VPN）
vulnerability	脆弱性
zoning	分区

4. 文献

考试文献教材

以下文献包含了考试要求掌握的知识。

A. EXIN
EXIN Information Security Management Professional based on ISO/IEC 27001 Body of Knowledge
EXIN (2023)
免费获取途径：www.exinchina.cn。在"认证教材"页面下载。

可选教材

B. ISO/IEC 27000:2018
Information technology – Security techniques – Information security management systems – Overview and vocabulary
瑞士，ISO/IEC，2018
www.iso.org

C. ISO/IEC 27001:2022
Information security, cybersecurity and privacy protection – Information security management systems – Requirements
瑞士，ISO/IEC，2022
www.iso.org

D. ISO/IEC 27002:2022
Information security, cybersecurity and privacy protection – Information security controls
瑞士，ISO/IEC，2022
www.iso.org

E. ISO/IEC 27005:2022
Information security, cybersecurity and privacy protection – Guidance on managing information security risks
瑞士，ISO/IEC，2022
www.iso.org

备注

可选教材仅作为参考和深度学习使用。

教材考点分布矩阵

考试要求	考试规范	教材参考章节
1. 信息安全视角		
	1.1 信息安全的业务收益	A，幻灯片第 010 – 019 张
	1.2 客户视角的治理	A，幻灯片第 020 – 022 张
	1.3 供应商负有的安全保障责任	A，幻灯片第 023 – 035 张，第 111 – 113 张
2. 风险管理		
	2.1 风险管理的原则	A，幻灯片第 026 – 057 张
	2.2 控制风险	A，幻灯片第 009 – 011 张，第 028 – 068 张，第 115 张
	2.3 处理残余风险	A，幻灯片第 028 – 035 张，第 049 – 052 张
3. 信息安全控制		
	3.1 组织控制	A，幻灯片第 023 – 025 张，第 031 – 034 张，第 052 – 053 张, 第 058 – 085 张，第 091 – 095 张
	3.2 技术控制	A，幻灯片第 058 – 068 张，第 098 – 115 张
	3.3 物理控制和人员控制	A，幻灯片第 058 – 068 张，第 086 – 097 张

联系 EXIN

www.exinchina.cn

info.china@exin.com

WeChat ID: EXINCH