认证备考指南

202404 版本

内容

1. 概述

EXIN Information Security Foundation based on ISO/IEC 27001 (ISFS.CH)

范围

EXIN Information Security Foundation based on ISO/IEC 27001 认证证明专业人员掌握了工作环境中应用的信息安全原则和概念，并清楚如何降低风险。

本认证涵盖内容：
- 信息与安全
- 威胁与风险
- 安全控制
- 法律、规章与标准

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。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，为信息安全计划的组织和管理提供了框架。

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。

EXIN Information Security Foundation based on ISO/IEC 27001 考察了信息安全的基本概念及其关系。该模块的目标是提高对信息的价值和脆弱性的认识，并学习保护信息的必要措施。

背景

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

目标群体

EXIN Information Security Foundation based on ISO/IEC 27001 认证面向组织中的任何信息处理人员。本认证也适用于小型独立企业的企业家，他们需要掌握一些基本的信息安全知识。对新的信息安全专业人士而言，本认证是良好的入门材料。

认证要求

- 顺利通过 EXIN Information Security Foundation based on ISO/IEC 27001 考试。

考试细节

考试类型：	单选题
题目数量：	40
通过分数：	65% (26/40 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：	60 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 Foundation 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 1 级和 2 级测试。

- 布鲁姆 1 级：记忆——依靠对信息的回忆。考生需要对知识吸收、记忆、识别和回忆。
- 布鲁姆 2 级：理解——识记之上的一级。理解表明考生能够理解呈现的内容，并能够评估如何将学习资料应用到实际的环境中。这类题目旨在证明考生能够整理、比较、阐释并选择跟事实和想法有关的正确描述。

培训

培训时长

本培训课程时长建议 14 小时。该时长包括学员分组作业、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

56 小时（2 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. 信息与安全		**27.5%**
	1.1 信息相关概念	10%
	1.2 可靠性方面	7.5%
	1.3 保障组织中的信息安全	10%
2. 威胁与风险		**12.5%**
	2.1 威胁与风险	12.5%
3. 安全控制		**52.5%**
	3.1 概述安全控制	2.5%
	3.2 组织控制	15%
	3.3 人员控制	7.5%
	3.4 物理控制	10%
	3.5 技术控制	17.5
4. 法律、规章与标准		**7.5%**
	4.1 法律与规章	2.5%
	4.2 标准	5%
	合计	**100%**

考试规范

1 信息与安全

1.1 信息相关概念

考生能够...

1.1.1 说明数据与信息之间的区别。

1.1.2 说明信息安全管理概念。

1.2 可靠性方面

考生能够...

1.2.1 说明 CIA 三元组的价值。

1.2.2 描述问责性和可审计性的概念。

1.3 保障组织中的信息安全

考生能够...

1.3.1 概述信息安全方针的目标和内容。

1.3.2 说明与供应商合作时如何确保信息安全。

1.3.3 概述与信息安全相关的角色和职责。

2 威胁与风险

2.1 威胁与风险

考生能够...

2.1.1 说明威胁、风险和风险管理。

2.1.2 描述各类损害。

2.1.3 描述风险策略。

2.1.4 描述风险分析。

3 安全控制

3.1 概述安全控制

考生能够...

3.1.1 举例说明每种类型的安全控制。

3.2 组织控制

考生能够...

3.2.1 说明如何对信息资产进行分类。

3.2.2 描述管理信息访问的控制。

3.2.3 说明信息安全中的威胁和脆弱性管理、项目管理和事件管理。

3.2.4 说明业务连续性的价值。

3.2.5 描述审计和审查的价值。

3.3 人员控制

考生能够...

3.3.1 说明如何通过合同和协议加强信息安全。

3.3.2 说明如何获得信息安全相关意识。

3.4 物理控制

考生能够...

3.4.1 描述物理入口控制。

3.4.2 描述如何保护安全区域内的信息。

3.4.3 说明保护环的工作原理。

3.5 技术控制

考生能够...

3.5.1 概述如何管理信息资产。

3.5.2 描述如何在考虑信息安全的情况下开发系统。

3.5.3 列出确保网络安全的控制。

3.5.4 描述管理访问的技术控制。

3.5.5 描述如何保护信息系统以抵御恶意软件、网络钓鱼和垃圾邮件的侵害。

3.5.6 说明记录和监控如何促进信息安全。

4 法律、规章与标准

4.1 法律与规章

考生能够...

4.1.1 举例说明与信息安全相关的法律规章。

4.2 标准

考生能够...

4.2.1 概述 ISO/IEC 27000、ISO/IEC 27001 和 ISO/IEC 27002 标准。

4.2.2 概述与信息安全相关的其他标准。

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
access control	访问控制
accountability	问责性
annualized loss expectancy (ALE)	年损失预期（ALE）
annualized rate of occurrence (ARO)	年发生率（ARO）
asset	资产
auditability	可审计性
authentication	身份验证
authorization	授权
availability	可用性
backup	备份
biometrics	生物识别
business continuity management (BCM)	业务连续性管理（BCM）
certificate	证书
change management	变更管理
chief information security officer (CISO)	首席信息安全官（CISO）
classification	分类分级
code of conduct	行为准则
compliance	合规性
confidentiality	机密性
controls • corrective • detective • insurance • preventive • reductive • repressive (suppressive)	控制 • 纠正 • 检测 • 保险 • 预防 • 还原 • 遏制（抑制）
cryptography	密码学
cyber crime	网络犯罪
damage • direct damage • indirect damage	损害 • 直接损害 • 间接损害
data	数据
digital signature	数字签名
due care	应有注意
due diligence	尽职调查
escalation	升级
exposure	暴露
(business) impact	（业务）影响
incident cycle	事件周期
information	信息
information analysis	信息分析
information management	信息管理
information security management system (ISMS)	信息安全管理体系（ISMS）

information security manager (ISM)	信息安全经理（ISM）
information security officer (ISO)	信息安全官（ISO）
information security policy	信息安全方针
information security strategy	信息安全战略
information system	信息系统
integrity	完整性
likelihood	可能性
non-disclosure agreement (NDA)	保密协议（NDA）
Plan, Do, Check, Act (PDCA)	计划、执行、检查、行动（PDCA）
personally identifiable information (PII)	个人可识别信息（PII）
phishing	网络钓鱼
privacy	隐私
protection ring	保护环
public key infrastructure (PKI)	公钥基础结构（PKI）
reliability	可靠性
risk	风险
risk analysis • qualitative risk analysis • quantitative risk analysis	风险分析 • 定性风险分析 • 定量风险分析
risk assessment	风险评估
risk management	风险管理
risk strategy • risk avoiding • risk bearing (risk acceptance) • risk neutral	风险策略 • 风险避免 • 风险承受（风险接受） • 风险中立
risk treatment	风险处理
security incident	安全事件
segregation of duties	职责分离
single loss expectancy (SLE)	单次损失预期（SLE）
stand-by arrangement	备用安排
threat • human threat • non-human threat	威胁 • 人为威胁 • 非人为威胁
threat agent	威胁代理
validation	确认
verification	验证
virtual private network (VPN)	虚拟专用网络（VPN）
vulnerability	脆弱性（漏洞）

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. Baars, H., Hintzbergen, J., and Hintzbergen, K.
Foundations of Information Security – Based on ISO 27001 and ISO 27002
Van Haren Publishing: 第四次全面修订版，2023
ISBN: 978 94 018 0958 0（纸质书）
ISBN: 978 94 018 0959 7（电子书）
ISBN: 978 94 018 0960 3（电子出版物）

教材考点分布矩阵

考试要求	考试规范	教材参考章节
1. 信息与安全		
	1.1 信息相关概念	第 3.1 - 3.3, 4.7 - 4.9 章
	1.2 可靠性方面	第 3.4, 4.4 - 4.6 章
	1.3 保障组织中的信息安全	第 4.2, 4.3, 4.11 - 4.14, 5.1 - 5.6, 5.14, 5.19 - 5.23, 5.35, 7.7, 7.9, 7.10, 8.30 章
2. 威胁与风险		
	2.1 威胁与风险	第 3.5, 3.7, 3.9 – 3.11 章
3. 安全控制		
	3.1 概述安全控制	第 3.8 章
	3.2 组织控制	第 3.6.2, 5.3, 5.7 – 5.18, 5.24 – 5.30, 5.35, 5.36, 6.8 章
	3.3 人员控制	第 6 章
	3.4 物理控制	第 7 章
	3.5 技术控制	第 4.10, 8 章
4. 法律、规章与标准		
	4.1 法律与规章	第 5.31 – 5.34 章
	4.2 标准	第 1, 3.6, 3.12, 4.1, 4.12, 5.36 章

联系 EXIN

www.exinchina.cn

info.china@exin.com

WeChat ID: EXINCH