备考指南

2018 年 04 九月版

Copyright © EXIN Holding B.V. 2018. All rights reserved.
EXIN® is a registered trademark.

No part of this publication may be reproduced, stored, utilized or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written permission from EXIN.

目录

1. 概述

EXIN Information Security Foundation based on ISO/IEC 27001（基于 ISO/IEC 27001 的信息安全 基础级）(ISFS.CH)

考察范围

基于 ISO/IEC 27001 的信息安全基础级认证主要考察以下领域：
- 信息与安全：信息的概念和价值，及其信息的可靠性和重要性
- 威胁与风险：威胁和风险的概念，以及与信息的可靠性之间的关系
- 方法与组织：安全策略和安全组织，包括安全组织的构成和（安全）事件管理
- 措施：安全措施及重要性，包括物理、技术和组织措施
- 法律法规：法律法规的重要性及影响

摘要

信息安全是保护信息免受广泛范围的威胁的影响，以实现业务的连续性，最小化业务风险、以及最大化投资回报和业务机会。

信息安全问题正变得越来越重要。随着经济全球化的发展，组织（及其员工、客户和提供商）之间的信息交流日益增多，网络使用日益广泛，联网的计算机和网络设备大量运用，比如公司内部网、接入其他公司的网络和互联网等。

作为广泛认可和运用的国际标准，信息安全管理体系 ISO/IEC 27001 提供了信息安全管理和组织运用的框架和方案。实施这个方案，可以帮助组织很好地满足当前复杂运营环境下的目标要求。深刻理解本标准，对每一个信息安全从业者来说，都是个人发展的必备能力。

EXIN 的信息安全领域采用了如下的定义：信息安全定义、实施、维护、合规，以及一套一致的信息安全控制措施的评价方法，确保（自动和手工的）信息提供过程的可用性、完整性和保密性。

在《基于 ISO/IEC 27001 的信息安全基础级别》模块中，将考察信息安全的基本概念及其关系。这些基础知识将帮助学员们意识到信息是敏感的，因此有必要采取措适当施保护信息。

背景信息

基于 ISO/IEC 27001 的“信息安全基础认证” (Information Security Foundation) 是“信息安全”认证路径的一部分。本模块之后是基于 ISO/IEC 27001 的“信息安全管理高级认证”(Information Security Management Professional) 和基于 ISO/IEC 27001 的“信息安全管理专家级认证”(Information Security Management Expert)。

目标群体

基于 ISO/IEC 27001 的“信息安全基础级别”考试适合在组织内部处理信息的所有人员。本模块还适合有必要掌握某些基础信息安全知识的小型独立业务的企业家。
本模块也可以作为信息安全专业人士的入门课程。

证书要求

- 成功通过 EXIN 信息安全基础级考试。

考试详情

考试类型:	多选题
及格题数:	40
及格分数:	65%
开卷/注意事项:	无
允许使用的电子设备:	无
考试时间安排:	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。这是考生提升到更好的级别的基础。
- 布鲁姆 2 级：理解——比记忆更进一步。理解表明考生能够了解介绍的内容，并能够评估如何将学习资料应用到所在的环境中。

培训

面授课时

培训班面授课时至少 14 小时。本课时含分组、考试准备和短暂的休息时间。不含：家庭作业、考试相关后勤保障、考试及午间休息时间。

建议学习时长

60 小时，根据个人的现有知识而不同

培训机构

授权培训机构的清单请参见 EXIN 网站： http://www.exin.com。

2. 考试要求

考试要求请参见考试规范。下表列举了模块主题（考试要求）和子主题（考试规格）。不同主题在考试中的比重用占总分的百分比表示。

考试要求	考试规格	所占比重
1 信息与安全		**10**
	1.1 信息的概念	2.5
	1.2 信息的价值	2.5
	1.3 可靠性	5
2 威胁与风险		**30**
	2.1 威胁与风险	15
	2.2 威胁、风险及信息的可靠性之间的关系	15
3 方法与组织		**10**
	3.1 安全策略及安全组织	2.5
	3.2 组成部分	2.5
	3.3 事件管理	5
4 措施		**40**
	4.1 措施的重要性	10
	4.2 物理安全措施	10
	4.3 技术措施	10
	4.4 组织措施	10
5 法律法规		**10**
	5.1 法律法规	10
	总分	**100%**

考试规格

1 信息与安全

1.1 信息的概念

考生能够：

1.1.1 解释数据与信息之间的差别。

1.1.2 阐述属于基本基础设施组成部分的存储介质。

1.2 信息的价值

考生能够：

1.2.1 阐述数据/信息对组织的价值。

1.2.2 阐述数据/信息的价值对组织有何影响。

1.2.3 解释如何应用信息安全概念保护数据/信息的价值。

1.3 可靠性

考生能够：

1.3.1 说出信息的可靠性。

1.3.2 阐述信息的可靠性。

2 威胁与风险

2.1 威胁与风险

考生能够：

2.1.1 解释威胁、风险和风险分析的概念。

2.1.2 解释威胁与风险之间的关系。

2.1.3 阐述各种类型的威胁。

2.1.4 阐述各种类型的损害。

2.1.5 阐述各种风险策略。

2.2 威胁、风险及信息的可靠性之间的关系。

考生能够：

2.2.1 识别各类威胁的实例。

2.2.2 阐述各类威胁对信息及信息处理的影响。

3 方法与组织

3.1 安全策略与安全组织

考生能够：

3.1.1 概述安全策略的目标和内容。

3.1.2 概述安全组织的目标和内容。

3.2 组成部分

考生能够：

3.2.1 解释行为守则的重要性。

3.2.2 解释所有权的重要性。

3.2.3 说出信息安全组织中最重要的角色。

3.3 事件管理

考生能够：

3.3.1 概述如何报告安全事件及需要提供哪些信息。

3.3.2 举例说明安全事件。

3.3.3 解释不报告安全事件的后果。

3.3.4 解释升级（职能升级和层次升级）引发的行动。

3.3.5 阐述升级在组织内部带来的影响。

3.3.6 解释事件周期。

4 措施

4.1 措施的重要性

考生能够：

4.1.1 阐述构建或安排安全措施的各种方式。
4.1.2 举例说明每种类型的安全措施。
4.1.3 解释风险与安全措施之间的关系。
4.1.4 解释信息分级的目的。
4.1.5 阐述分级的效果。

4.2 物理安全措施

考生能够：

4.2.1 举例说明物理安全措施。
4.2.2 阐述物理安全措施不足带来的风险。

4.3 技术措施

考生能够：

4.3.1 举例说明技术安全措施。
4.3.2 阐述技术安全措施不足带来的风险。
4.3.3 理解加密、数字签名和证书的概念。
4.3.4 说出网上银行业务的三个步骤（个人电脑、网站和付款）。
4.3.5 说出各种类型的恶意软件。
4.3.6 阐述可用于防范恶意软件的措施。

4.4 组织措施

考生能够：

4.4.1 举例说明组织安全措施。
4.4.2 阐述组织安全措施不足带来的危险和风险。
4.4.3 阐述职责分离和使用密码之类的各种访问安全措施。
4.4.4 阐述访问管理的原则。
4.4.5 阐述身份鉴别、验证和授权的概念。
4.4.6 阐述良好的业务连续性管理对组织的重要性。
4.4.7 阐明进行演练的重要性。

5 法律法规

5.1 法律法规

考生能够：

5.1.1 解释法律法规为何对信息的可靠性具有重要意义。
5.1.2 举例说明与信息安全有关的法律。
5.1.3 举例说明与信息安全有关的法规。
5.1.4 指出可采取哪些措施以遵守法律法规的要求。

3. 基本概念一览表

本列表包含考生应当熟知的术语。术语按字母顺序排列。

请注意，只掌握每个术语的含义是不够的，考生需要具备达到理解概念和举出实例的能力。

英文	中文
Access control	访问控制
Asset	资产
Audit	审计
Authentication	验证
Authenticity	真实性
Authorization	授权
Availability	可用性
Backup	备份
Biometrics	生物识别
Botnet	僵尸网络
Business Continuity Management (BCM)	业务连续性管理 (BCM)
Business Continuity Plan (BCP)	业务连续性计划 (BCP)
Category	类别
Certificate	证书
Change Management	变更管理
Classification (grading)	分类（分级）
Clear desk policy	桌面净空策略
Code of conduct	行为守则
Code of practice for information security (ISO/IEC 27002)	信息安全实施规则 (ISO/IEC 27002)
Completeness	完备性
Compliance	合规性
Computer criminality legislation	计算机犯罪法规
Confidentiality	机密性
Continuity	持续性
Copyright legislation	版权法规
Corrective	纠正
Correctness	正确性
Cryptography	密码学
Cyber crime	网络犯罪
Damage	损害
Data	数据
Detective	探测
Digital signature	数字签名
Direct damage	直接损害
Disaster	灾难
Disaster Recovery Plan (DRP)	灾难恢复计划 (DRP)

Encryption	加密
Escalation • Functional escalation • Hierarchical escalation	升级 • 功能升级 • 层次升级
Exclusivity	排外性
Hacking	黑客
Hoax	骗局
Identification	身份鉴别
Impact	影响
Incident cycle	事件周期
Indirect damage	间接损害
Information	信息
Information analysis	信息分析
Information architecture	信息架构
Information management	信息管理
Information system	信息系统
Infrastructure	基础设施
Integrity	完整性
Interference	干扰
ISO/IEC 27001	ISO/IEC 27001
ISO/IEC 27002	ISO/IEC 27002
Key	密钥
Logical access management	逻辑访问管理
Maintenance door	检修门
Malware	恶意软件
Non-repudiation	不可否认性
Patch	补丁
Personal data protection legislation	个人数据保护法规
Personal firewall	个人防火墙
Phishing	网络钓鱼软件
Precision	准确性
Preventive	预防性
Priority	优先权
Privacy	隐私
Production factor	生产要素
Public Key Infrastructure (PKI)	公钥基础结构 (PKI)
Public records legislation	公共记录法规
Qualitative risk analysis	定性风险分析
Quantitative risk analysis	定量风险分析
Reductive	还原
Reliability of information	信息的可靠性
Repressive	压制的
Risk	风险
Risk analysis	风险分析
Risk assessment (Dependency & Vulnerability analysis)	风险评估（依赖性和脆弱性分析）

Risk avoiding	风险规避
Risk bearing	风险承担
Risk neutral	风险中性
Risk management	风险管理
Risk strategy	风险策略
Robustness	坚固性
Rootkit	Rootkit 后门
Security incident	安全事件
Security measure	安全措施
Security Organization	安全组织
Security Policy	安全策略
Security regulations for the government	政府安全条例
Segregation of duties	职责分离
Social engineering	社交工程
Spam	垃圾邮件
Spyware	间谍软件
Stand-by arrangement	备用安排
Storage medium	存储介质
Threat	威胁
Timeliness	时效性
Trojan	木马
Uninterruptible Power Supply (UPS)	不间断电源 (UPS)
Urgency	紧急
Validation	验证
Verification	确认
Virtual Private Network (VPN)	虚拟专用网络 (VPN)
Virus	病毒
Vulnerability	脆弱性
Worm	蠕虫

4. 文献资料

考试文献资料

A. 作者 Hintzbergen, J., Hintzbergen, K., Smulders, A.和 Baars, H.
《信息安全基础》 - 基于 ISO27001 和 ISO27002
Van Haren Publishing 出版, 2010
ISBN 978 90 8753 568 1

文献概述

考试要求	考试规格	文献资料
1 信息与安全		
	1.1 信息的概念	**A:** 第三章和第四章第 10 节
	1.2 信息的价值	**A:** 第三章和第四章
	1.3 可靠性	**A:** 第三章和第四章
2 威胁与风险		
	2.1 威胁与风险	**A:** 第三 章
	2.2 威胁、风险及信息的可靠性之间的关系	**A:** 第三章和第十一章
3 方法与组织		
	3.1 安全策略及安全组织	**A:** 第三、五、六章
	3.2 组成部分	**A:** 第六、七、八、十三章
	3.3 事件管理	**A:** 第三、五、十六章
4 措施		
	4.1 措施的重要性	**A:** 第三、八、十六章
	4.2 物理安全措施	**A:** 第三、十一章
	4.3 技术措施	**A:** 第六、十、十一、十二章
	4.4 组织措施	**A:** 第三、六、九、十七、十八章
5 法律法规		
	5.1 法律法规	**A:** 第十八章

联系 EXIN

www.exin.com