

信息安全官认证 ISO

【认证机构】

国际信息学考试 (Exam Institute of Information Science) 简称 EXIN, 是一家面向全球 ICT 从业人员的中立考试研发和认证机构。1984 年 EXIN 由荷兰经济事务部创办, 后从荷兰政府部门独立成立了 EXIN 基金会。EXIN 是全球 IT 服务管理最佳实践知识体系 ITIL® 的创始机构之一, 开发并拥有 ITIL® 版本一和版本二全系列试题的知识产权, 目前是 ITIL®和 Prince2®全球最大的认证考试机构。

EXIN 是全球 ICT 领域内的权威认证机构, 个人资质认证体系目前覆盖 IT 服务管理、敏捷开发、数据中心管理、项目管理、DevOps、业务连续性管理、信息安全、云计算、大数据、IT 资产管理、商业分析、绿色 IT、OpenStack、安全编程、软件测试、精益 IT、应用管理、数字营销等类别。目前来自全球 165 多个国家和地区累计近三百万的 ICT 职业人士已经获得了 EXIN 颁发的资格认证, 考试语言多达 25 种。

【谷安天下】

谷安天下始终瞄准世界前沿秉承国际化的视野, 是国内全方面提供中立性安全与风险服务的机构。

咨询业务: 网络安全规划、IT 治理与 IT 规划、ISO27001 和 ISO27701 安全与隐私管理体系、数据安全治理体系、云安全规划、金融科技应用风险评估及管理体系、业务连续性管理体系、信息科技外包管理体系、数字化 IT 审计管理体系咨询等。

审计业务: 信息科技风险全面审计、业务连续性管理专项审计、信息科技外包管理专项审计、数据中心管理专项审计、重要信息系统专项审计、重大项目专项审计、电子银行业务专项审计、数据治理专项审计、非银行 IT 审计等。

培训业务: 包含认证培训、在线教育、安全意识宣贯等人才培养方案。

媒体社区: 安全牛是国内具有影响力的信息安全媒体品牌, 十万安全专业人士关注的社区。

【ISO 课程介绍】

信息安全官认证不是一门单独的考试，而是 EXIN 为已经获得相关认证的专业从业者提供的一种集成认证。考取以下三门认证后（ISO27001 Foundation\ISO27001 Professional\PDF）即可获得 ISO 认证：

- 1、EXIN ISO/IEC 27001 Foundation 基于 ISO27001 信息安全管理基础认证
- 2、EXIN ISO/IEC 27001 Professional 基于 ISO27001 信息安全管理专业认证
- 3、PDF (EXIN Privacy and Data Protection Foundation) 隐私与数据保护基础级认证



【ISO27001 Foundation 课程介绍】

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。

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。

【ISO27001 Foundation 报名须知】

- 报考要求

无学历和工作经验年限的硬性要求。

- **学习对象**

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。还适合有必要掌握基础信息安全知识的小型独立业务的企业家。也可作为信息安全专业人士的入门课程。

- IT 经理、信息中心主任；信息安全经理、资深 IT 人员；信息安全顾问
- 信息安全厂商技术、研发人员；信息安全厂商售前、服务人员
- 风险管理人员、IT 审计人员；信息安全体系建设与维护人员
- 有意学习信息安全管理的人员

- **培训方式**

直播：在线会议平台授课。

- **培训班型及培训周期**

2 天，周末班。

送：精要串讲课程录播视频；送模拟题讲解知识点视频课程

- **培训教材**

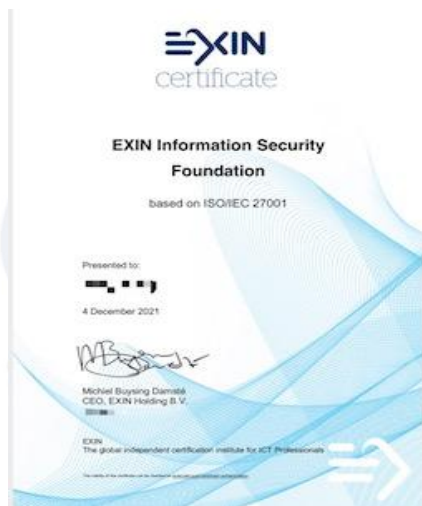
ISO27001 Foundation 学习资料：

- 1、官方认证考试指南一本；
- 2、谷安培训讲义一本、



- **关于考试**

- 1、**考题类型**：40 道单选，考试 1 小时，答对 26 道以上通过考试
- 2、**考试方式**：线上机考
- 3、**考试语言**：中英文对照
- 4、**证书样例**：（证书终身有效，无需维持）



【ISO27001 Foundation 费用与认证价值】

- **ISO27001 Foundation 认证费用**

总计：6500 元（培训费 4500 元、考试费 2000 元）

- **ISO27001 Foundation 认证价值**

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，因此有必要采取措施适当施保护信息。

【ISO27001 Foundation 考试大纲】

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 risk 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

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%

【ISO27001 Professional 课程介绍】

信息对于单个组织及其推动的经济的连续性和正常运行至关重要。此信息必须受到保护，以防止未经授权的人员访问，防止意外或恶意修改或破坏，并且在需要时必须可用。基于 ISO / IEC 27001 的信息安全管理专业人员模块测试对信息安全的组织，物理和技术方面的理解。

【ISO27001 Professional 报名须知】

- **报考要求**

无学历和工作经验年限的硬性要求。

- **学习对象**

该模块适用于参与信息安全计划的实施，评估和报告的每个人，例如信息安全经理（ISM），信息安全官（ISO）或生产线经理，流程经理或项目经理，安全责任。建议使用信息安全的基础知识，例如通过基于 ISO / IEC 27001 认证的 EXIN 信息安全基金会。

- **培训方式**

直播：在线会议平台授课。

- **培训班型及培训周期**

2 天，周末班。

- **培训教材**

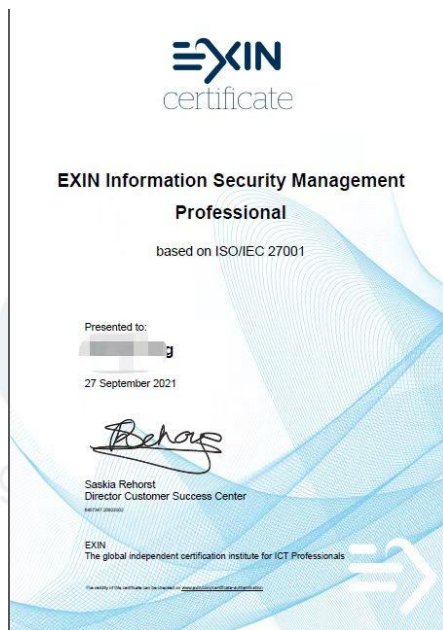
ISO27001 Professional 学习资料：

1、谷安培训讲义一本。



- **关于考试**

- 1、**考题类型**：30 道单选，考试 90 分钟，答对 26 道以上通过考试
- 5、**考试方式**：线上机考
- 6、**考试语言**：中英文对照
- 7、**证书样例**：（证书终身有效，无需维持）



【ISO27001 Professional 费用与认证价值】

- **ISO27001 Professional 认证费用**

总计：8000 元（培训费 5500 元、考试费 2500 元）

- **ISO27001 Professional 认证价值**

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。

【ISO27001 Professional 考试大纲】

- 1、信息安全观点：业务，客户和服务提供商的观点
- 2、风险管理：风险分析，选择控制措施，处理剩余风险
- 3、信息安全控制措施：组织，技术和物理控制

考试要求	
0. Introduction 介绍	
1. Information Security Perspectives 信息安全观点	
	1.1 Business Interest of Information Security 信息安全的商业利益
	1.2 Customer (End User) Perspective on Governance 客户（最终用户）对治理的看法
	1.3 Service Provider/Supplier Responsibilities in Security Assurance 安全保障中的服务提供商/供应商责任
2. Risk Management 风险管理	
	2.1. Risk Management Principles 风险管理原则
	2.2. Controlling the Risks 风险控制
	2.3. Remaining Risks 剩余风险
3. Information Security Controls 信息安全控制	
	3.1. Organizational Controls 组织控制
	3.2. Physical Controls 物理控制
	3.3. Employment Controls 就业控制
	3.4. Continuity Controls 连续性控制
	3.5. Technical Controls 技术控制
	3.6. Network Controls 网络控制

【PDPF 课程介绍】

在欧盟，关于保护数据的规定和标准十分严格。一般数据保护条例 (GDPR, General Data Protection Regulation) 于 2016 年 5 月推出，要求各机构必须在 2018 年 5 月前修改其政策和程序，以保证完全符合 GDPR 的要求。GDPR 要求每个欧盟境内所有公司配备这样一个职位：DPO(Data Protection Officer)。EXIN Privacy & Data Protection 个人认证体系即是基于 GDPR 的专有认证体系。经过两年的过渡，GDPR 已于 2018 年 5 月 28 日正式强制生效。该法规将全面影响所有使用欧盟管辖范围内的个人数据的组织；所有已经或者希望与欧盟境内公司进行交易的组织。

EXIN 发布了一套基于 GDPR 的隐私与数据保护认证体系，共计两个层级：其中 PDPF 为基础级认证。

PDPF (EXIN Privacy and Data Protection Foundation)



PDPF 认证学习项目涵盖了欧盟《通用数据保护条例》GDPR 的所有核心主题。是一门验证专业人员如何保护个人数据，以及对数据保护相关欧盟法规了解程度的认证。

【PDPF 报名须知】

- **报考要求**

无工作经验及学历要求

- **学习对象**

目标群体包括（不限于）

- ◇ 组织内的数据保护官（Data Protection Officer，简称 DPO*）
- ◇ 组织内的数据隐私官 Privacy Officer
- ◇ 组织内的法务人员 / 合规人员 Legal Officer / Compliance Officer
- ◇ 组织内的安全负责人 Security Officer
- ◇ 组织内的业务连续性经理 Business Continuity Manager
- ◇ 组织内的数据管控专家 Data Controller
- ◇ 组织的数据保护审核员（包括内审员和外审员）Data Protection Auditors
- ◇ 人力资源经理 HR Manager

- **培训方式**

直播：在线会议平台授课，2天 周末班；

- **培训教材**

PDF 学习资料：

- 1、官方认证考试指南一本；
- 2、谷安培训讲义一本、



- **关于考试**

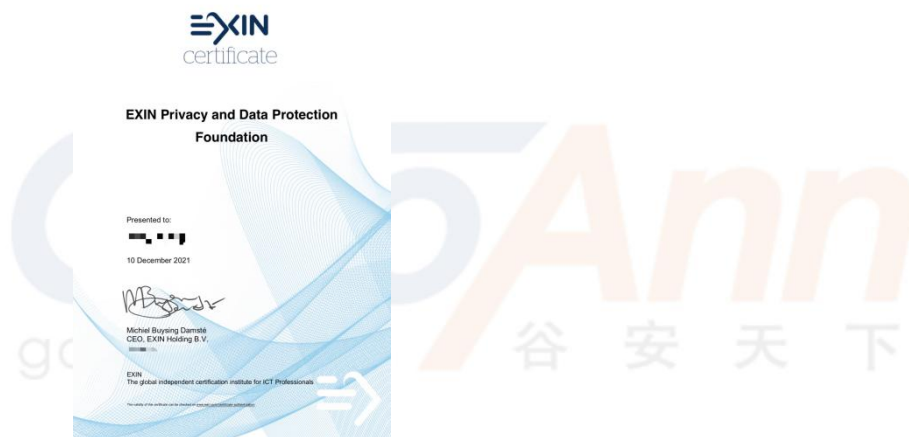
- 1、**考题类型：**

40 道单选，考试 60 分钟，答对 65%以上 (26/40)通过考试)

- 2、**考试方式：**线上机考

- 3、**考试语言：**中英文对照

- 4、**证书样例：**



【认证费用与收益】

- **PDPF 认证费用**

总计：8000 元（培训费：5500 元/人；考试认证费 2500 元/人）

- **ISO 信息安全官认证费用 (ISO2700 Foundation + ISO27001 Professional + PDPF)**

总计：20000 元（培训费：13000 元/人；考试认证费 7000 元/人）

- **谷安天下账户信息**

帐户名称：北京谷安天下科技有限公司

开户银行：北京银行航天支行

帐 号：01090372800120109116339

- **认证收益**

对于企业：

- 1、充分了解最新的数据隐私保护法规 GDPR；

- 2、符合合规以带来业务机会；

3、充分适用于大型企业以及中小型企业。

对于个人：

- 1、 获得一份高需求领域的认证；
- 2、 了解数据隐私保护法规的相关知识，对您的工作和生活均十分有益；
- 3、 使得您在所服务的组织中更具有竞争力。

【PDF 考试大纲】

考试要求	考试明细	比重
1.隐私和数据保护基础和法规		45
	1.1 定义	
	1.2 个人数据	
	1.3 合法理由和目的限制	
	1.4 合法处理个人数据的进一步要求	
	1.5 数据主体权利	
	1.6 数据泄露和相关程序	
2.组织数据保护		35
	2.1 数据保护对组织的重要性	
	2.2 监管机构 ¹	
	2.3 个人数据转移到第三国	
	2.4 有约束力的企业规则和合同中的数据保护	
3.数据保护实践		20
	3.1 与信息安全相关的基于设计的和默认情况下的数据保护	
	3.2 数据保护影响评估 (DPIA)	
	3.3 与数据使用、营销和社交媒介应用相关的实践	
	Total	100%