信息安全管理体系认证 ISO/IEC 27001 Foundation

【认证机构】

APMG 是来自英国的全球知名管理资格鉴定和认证机构，经英国皇家认可委员会（UKAS）授权认可，代表英国商务部（OGC）在全球进行资格认证工作，多年以来一直致力于激励与引导全球项目管理理论与实践发展的前沿，将最权威的标准和概念引入全球各个企业，并逐步深入，在业界获得高度赞誉。

APMG 中国是英国 APM Group(APMG)公司在中国的全资机构及唯一代表机构。APMG 致力于对众多行业及管理领域的组织、过程及人才进行鉴定和认证，业务遍布全球，分别在英国，美国，荷兰，丹麦，澳大利亚和中国设有分支机构。

【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。

【ISO27001 Foundation 课程介绍】

信息安全管理发展至今，越来越多的人认识到安全管理在整个企业运营管理中

的重要性，而作为信息安全管理方面最著名的国际标准—ISO/IEC 27001(简称ISMS)，则成为可以指导我们现实工作的最好的参照。ISO27001 目前作为国际标准，正迅速被全球所接受。依据 ISO27001 标准进行信息安全管理体系建设，是当前各行业组织在推动信息安全保护方面最普遍的思路和正确的先进决策。

信息安全管理 ISO27001 Foundation 认证培训是为了培养并提高信息安全管理体系（ISO 27001）建设者所开设的课程，更注重信息安全管理体系的实施、维护与优化方面。

【ISO27001 Foundation 报名须知】

- **报考要求**

  无工作经验及学历要求

- **学习对象**

IT 经理、信息中心主任、信息安全经理、资深 IT 人员、信息安全厂商技术、研发人员、信息安全厂商售前、服务人员、ISMS 体系审核员、风险管理人员、IT 审计人员、信息安全体系建设与维护人员、ISO27001 内审员、资深 IT 人员、信息安全顾问、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，共 2 天；

- **培训教材**

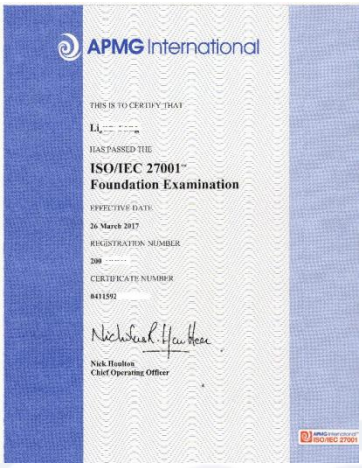
- **关于考试**

  1、**考题类型：5**0 道单选，考试 40 分钟，需答对 25 题以上通过考试；

2、**考试方式：**线上机考

3、**考试语言**：英文试卷

4、**证书样例：**



【ISO27001 Foundation 认证费用及收益】

- **认证费用**

总计：5500 元（培训费：4000 元/人；考试认证费 1500 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**

1、使学员理解信息安全管理相关的核心概念，为学员学习 ISO27001 打下基础。

2、使学员围绕信息安全管理，理解信息安全管理的必要性，迫切性，进而理解风险管理和安全管理的基本方法。

3、使学员站在咨询师的视角，理解不同组织在实施 ISO27001 的思路，需求分析的基本流程。

4、使学员站在咨询师的视角，实施 ISO27001 咨询前，如何实施风险评估，重点理解基本方法和流程。

5.使学员站在咨询师的视角，如何实施 ISO27001 项目，重点理解 ISMS 建立过程。

6、使学员结合前面的知识，深入理解 ISO27001 标准条款，重点理解在不同类型组织在对条款的灵活应用。

7、提升信息安全管理能力同时， 并获得国际权威机构（APMG）颁发的 ISO27001 Foundation 认证证书。

【ISO27001 Foundation 课程大纲】

培训主题	培训目的	培训内容	
一、课程介绍及核心概念	使学员理解信息安全管理相关的核心概念，为学员学习 ISO27001 打下基础	✧ 第一组概念：控制、风险与审计	
		✧ 第二组概念：信息安全的概念及基本属性	
		✧ 第三组概念：信息安全发展的五个阶段及其管理特点	
		✧ 第四组概念：IT 类风险管理、控制与审计相关的方法论	
		✧ 第五组概念：IT 风险管理在企业风险管理中的位置	
		✧ 第六组概念：对 IT 风险的三类控制	
		✧ 第七组概念：三类 IT 风险控制框架	
		✧ 第八组概念：对高层控制的审计内容	
		✧ 第九组概念：对一般控制的审计内容	
		✧ 第十组概念：对应用控制的审计内容	
		✧ ISO27001 课程设计介绍	
二、信息安全管理体系基本概念	使学员围绕信息安全管理，理解信息安全管理管理的必要性，迫切性，进而理解风险管理和安全管理的基本方法	安全形势	✧ 安全事件严重威胁着国家、社会、企业安全及个人隐私 ✧ 漏洞数量持续走高 ✧ 拒绝服务攻击持续活跃 ✧ 恶意代码快速泛滥 ✧ 互联网金融业务安全状况恶化 ✧ 攻击者水平：专业化、规模化、组织化、国际化
		风险特点	✧ 信息安全风险的特点 ✧ 信息安全风险管理难点 ✧ 信息安全事件影响及损失

培训主题	培训目的	培训内容	
		安全管理	✧ 信息安全风险的特点 ✧ 中共中央、国务院对生产安全的要求 ✧ 什么是信息？ ✧ 信息安全管理的目标 ✧ 基本目标完整性、机密性 ✧ 基本目标可用性 ✧ 信息安全目标间关系 ✧ 信息安全管理方式
		ISO 27001 标准内容条款及标准簇讲解	✧ 英国标准协会（BSI） ✧ 国际标准化组织（ISO） ✧ ISO 27001/ISO 27002 标准发展 ✧ ISO Guide 83：国际标准框架 ✧ ISO 27001：2013 标准结构 ✧ 信息安全管理内容框架 ✧ 管理体系框架模型 ✧ ISO 27001:2013 标准结构逻辑关系 ✧ 信息安全管理体系 ✧ ISO/IEC27001:2013 管理体系认证方法 ✧ ISO/IEC27001:2013 管理体系认证流程 ✧ ISO 27001 标准族讲解
三、信息化与信息安全管理思路	使学员站在咨询师的视角，理解不同组织在实施 ISO27001 的思路，需求分析的基本流程	成熟度分析	✧ 企业 IT 风险发展阶段 ✧ 不同行业 IT 风险发展阶段 ✧ 企业 IT 风险发展阶段 – 粗放管理级及特点 ✧ 企业 IT 风险发展阶段 – 规范管理级及特点 ✧ 企业 IT 风险发展阶段 – 优化管理级及特点 ✧ 企业 IT 风险发展阶段 – 融合管理级及特点 ✧ IT 风险管理阶段目标 ✧ 信息安全风险管控内容 ✧ 可管、可控与可信本质区别

培训主题	培训目的	培训内容	
		定位组织	✧ 目前精细化管理程度不够，应逐步实现融合 ✧ 组织的组织架构 VS 大型组织IT 组织架构 ✧ 组织信息安全管理部门与其他部门的职责边界设计 ✧ 信息安全管理的技术背景：管理框架及技术架构 ✧ 信息安全管理的对象：关键信息基础设施与 IT 资产管理 ✧ 信息安全管理与业务连续性管理融合 ✧ 信息安全管理与开发管理的融合 ✧ 信息安全管理与运维管理的融合 ✧ 信息安全管理与数据管理的融合 ✧ 信息安全管理抓手一：建章立制 ✧ 信息安全管理抓手二：安全评估 ✧ 信息安全管理抓手三：风险监测与绩效评价
		定位项目	✧ IT 风险管理与控制框架 ✧ 项目定位 – Step1：完善三道防线工作界面 ✧ 项目定位 – Step2：确定管理重点与落地范围 ✧ 信息安全风险管理思路
		确定目标	✧ 4 大核心目标
		建设思路	✧ 信息安全风险管理思路
四、信息安全风险评估基础知识	使学员站在咨询师的视角，实施 ISO27001 咨询前，如何实施风险评估，重点理解基本方法和流程	ISO27005	✧ 信息安全风险评估定义 ✧ 信息安全风险管理相关概念 ✧ 关键风险要素 ✧ ISO/IEC27005:2018 ISO/IEC 31000:2018 ✧ ISO/IEC27005:2018 风险评估流程
		环境建立	✧ 环境建立的基本活动
		风险评估	✧ ISO/IEC27005 基于资产的风险评估方法 ✧ 风险测量方法：定性分析与定量分析 ✧ 识别资产 ✧ 测量资产价值 ✧ 测量威胁 ✧ 测量弱点 ✧ 与风险可接受准则进行比较

培训主题	培训目的	培训内容	
		风险处置	✧ ISO/IEC27005:2018 风险处置策略选择 ✧ ISO/IEC 27005:2018 四种风险处置策略
		风险接受	✧ 风险接受：批准并持续跟踪
		监视和评审	✧ 风险持续监控与再评估
五、信息安全管理体系实施过程	使学员站在咨询师的视角，如何实施ISO27001项目，重点理解ISMS建立过程	总体方案	✧ 确定本项目4大核心目标 ✧ 总体技术方案与目标的映射
		第一阶段实施方案	✧ 项目启动及现状调研
		第二阶段实施方案	✧ 差距分析与风险评估 ✧ 评估方法1：ISO27001差距分析 ✧ 评估方法2：网络安全法差距评估 ✧ 评估方法3：IT风险管理流程评估 ✧ 评估方法4：IT技术评估 ✧ 评估方法5：风险组合评估
		第三、四阶段实施方案	✧ 体系建设 ✧ 信息安全规划
		认证支持	✧ 体系试运行 ✧ 体系认证 ✧ 增值服务 – 现场培训
		成果展示	✧ 项目交付物 ✧ 信息安全管理的顶层框架设计 ✧ 信息安全管理的二级框架 ✧ 信息安全管理的组织架构设计 ✧ 信息安全管理的制度架构设计 ✧ 信息安全管理的技术架构设计 ✧ 信息安全管理体系有效性测量表设计
六、ISO/IEC27001标准解读	使学员结合前面的知识，深入理解ISO27001标准条款，重点理解在不同类型组织在对条款的灵活应用	✧ ISO/IEC27001:2013标准结构	
		✧ 理解组织环境是差异化实施ISO/IEC27001:2013的关键环节	
		✧ 领导重视是ISMS成功实施的关键因素	
		✧ 目标与规划：风险评估识别IS的风险和机会，并确定ISMS目标	
		✧ 支持ISMS设计	
		✧ 发布运行：试运行 → 发布实施 → 风险评估 → 风险处置	
		✧ 绩效评价：监视→测量→分析→评价，内部审核→管理评审	
		✧ 持续改进：发现不符合项 → 纠正措施 → 持续改进机制	
		✧ ISO27001结构：描绘了ISMS建设的基本过程	

培训主题	培训目的	培训内容
七、ISO/IEC27001 附录解读	使学员结合前面的知识，深入理解 ISO27001 附录部分，重点理解在不同类型组织在对 14 个控制域、35 个控制目标和 114 项控制措施的灵活应用	✧ 信息安全策略
		✧ 信息安全组织
		✧ 人力资源安全
		✧ 资产管理
		✧ 访问控制
		✧ 密码学
		✧ 物理和环境安全
		✧ 运行安全
		✧ 通信安全
		✧ 系统获取、开发和维护
		✧ 供应商关系
		✧ 信息安全事件管理
		✧ 业务连续性管理的信息安全方面
		✧ 符合性
		✧ 解读总结
八、课程回顾与答疑	答疑解惑	✧ 课程总结
		✧ 答疑环节