国际注册信息安全经理认证 CISM

【认证机构】

ISACA（国际信息系统审计协会）是一家成立于 1969 年的非营利组织，总部设在美国芝加哥，是全球公认的提供信息系统鉴证及安全，企业 IT 治理与管理，IT 风险及合规性知识、认证、社区，倡导教育的领导组织。作为享誉全球的信息安全专业机构和学习组织，ISACA 拥有超过 150.000 名成员，分布在信息和网络安全、治理、鉴证、风险和隐私等工作领域，通过技术推动创新。ISACA 在 188 个国家和地区设有 225 多个分会，ISACA 中国办公室成立于 2017 年，是 ISACA 在美国以外唯一的直属机构，旨在服务 ISACA 在中国大陆的持证人员以及 IT 和安全行业的专业人士，引进 ISACA 全球先进的标准、框架体系和知识，并向全球同行输出中国业界的最佳实践。

【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。

【CISM 课程介绍】

注册信息安全经理(CISM)针对信息安全风险在业务应用的管理和相关问题的解

决，CISM 为信息安全经理和信息安全管理职责的专业人员量身定制，提升企业总体的信息系统安全管理水平，向高级管理层确保：拥有 CISM 专业资格认证的人员具有知识和能力提供有效的信息安全管理和咨询，以业务为导向，在应用于业务的管理、设计和技术安全问题时，强调信息风险管理概念。CISM 不适用于信息系统审计人员，但对具有信息系统管理经验和责任的信息系统审计师有帮助。

该认证致力于管理层面，聚焦在信息安全战略、评估系统和政策，自 2002 年推出后，受到了全球资深信息安全经理们的推崇，迄今已有超过 28,000 人获得了这一证书。CISM 注重管理层面，是全球公认的对开发、建立和管理企业信息安全系统的个人能力的认可。CISM 证书的维持率超过 95%。

【CISM 报名须知】

- **报考要求**

  CISM 要求最少要有 5 年信息安全管理的经验(CISA 及 CISSP 认证减免两年).

- **学习对象**

  IT 架构师、安全分析师、数据安全经理、安全和合规主管、信息安全副总裁、首席信息安全官/合规官等。

- **培训方式**

  直播：在线会议平台授课、

- **培训班型及培训周期**

  4 天周末直播班+赠送安全牛课堂 CISM 录播+分章节习题讲解视频课程【1 年有效期】

我们提供 CISM 学员全程备考指导服务：

在您完成第一遍教材精读（4 天公开课）的基础上，外加 4 天分章节录播视频，以题讲解知识点，1000 道试题来自官方复习手册，同时配合各章节思维导图辅助，掌握所有重点和难点；反复加深知识点的理解，反复熟悉，树立考试信心。

- **培训教材**

  1、ISACA 官方正版复习手册中文版（第 15 版）；

  2、官方复习解题手册一本；

  3、谷安培训讲义一本；

- 关于考试

1、考题类型：150 道单选，考试 4 小时，共计 800 分，450 分以上通过考试

2、考试方式：线上机考

3、考试语言：中文\英文等

4、证书样例：

【CISM 费用与认证价值】

- CISM 认证费用

培训费：5500 元、考试费：575 美金（折合人民币 4223 元，包含税发票）。

- 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

- **CISM 认证价值**

1、根据英国政府 2014 年网络安全技能报告，CISM 是企业招聘时看重的证书；

2、CISM 是获得澳大利亚政府 iRAP 认证的先决资格；

3、根据 Foote PartnersIT 技术和证书薪酬指数（ITSCPI）最新发布的季度报告公布的结果，CISM 是薪酬最高的 IT 职业证书之一；

4、CISM 获得美国国家标准学会认可，归入国际标准 ANSI/ISO/IEC 17024；

5、CISM 连续 4 年入选 SC 杂志 “最佳职业认证” 最终提名澳大利亚信号局将 CISM 作为其信息安全注册评估体系的先决资格；

6、德瑞大学在其信息图 “通往安全未来的坦途——信息安全职业之路” 中，鼓励从业人员获取 CISM 证书，这是唯一被提及的证书。

【CISM 课程大纲】

章节主题	章节内容
领域 1—信息安全治理 Information Security Governance (24%)	建立和维护与组织目标相一致的信息安全战略，用于指导信息安全项目的建立和持续管理。 建立和维护信息安全管理框架，用于指导支持信息安全战略的相关活动。 将信息安全治理与公司治理进行整合，以确保信息安全方案可以有效支撑组织的目标和战略。 建立和维护与高级管理层进行沟通的信息安全战略，并给后续的标准，程序和准则的制定提供指南。 开发和建立业务案例用于对信息安全的投资。 确定会对组织产生影响的内外部因素（例如：技术，商业环境，风险承受能力，地理位置，法律和监管要求），确保这些因素在信息安全战略中进行了全面考虑。 获得高级管理层的承诺和其他股东的支持，确保信息安全战略的成功实施。 确定整个组织的信息安全角色和责任，并进行沟通以建立明确的组织结构和权力界限。 建立，监测，评价和报告指标（例如：关键目标指标[KGIs]，关键绩效指标[KPIs]，关键风险指标[KRIs]），向管理层提供关于信息安全战略有效性的准确信息。

领域 2—信息风险管理与合规性 Information Risk Management and Compliance (33%)	建立并维护一个信息资产分类的流程以确保对资产的保护措施与资产的业务价值成正比； 了解各类法律法规、组织及相关的要求，从而将不合规的风险管理在可接受的范围内； 确保周期性地进行风险评估、脆弱性评估和威胁分析，并于所识别的信息风险相对应； 确定适当的风险应对措施来管理风险到可接受的范围内； 评估信息安全控制措施以评估是否适当且有效地将风险降低到可接受的范围内； 识别当前与预期的风险水平之间的差距； 将信息风险管理集成到业务与 I 流程中（例如：开发、采购、项目管理、企业兼并重组等），从而促进在组织内建立一个一致并全面的信息风险管理流程； 对所存在的风险进行监控以确保掌握风险的变化并进行适当的管理； 向不同层面的管理层汇报信息风险方面的不合规情况及其他变化情况，从而有助于风险管理决策的制定。
领域 3—信息安全计划开发与管理 Information Security Program Development and Management (25%)	建立和维护与信息安全策略相符的信息安全程序。 确保信息安全程序和其他业务功能（如人力资源[HR]，财务，采购和 IT）相同步，以支持与业务流程的相容性。 识别、获取、管理、定义用于实施信息安全程序的内外部资源的要求。 建立和维护实施信息安全程序的信息安全架构（人员，流程，技术）。 建立，沟通，维护组织的信息安全标准、流程、指南和其他文件，用于支持信息安全政策，并与其相符。 建立和维护一个强化信息安全意识和人员培训的流程，从而促进和提升组织的安全环境和有效的信息安全文化。 将信息安全要求整合到组织的流程中去（如变更管理，兼并和收购，发展，业务连续性，灾难恢复），从而维护组织的安全基线。 将信息安全要求与第三方合同及相关活动进行整合（如合资企业、外包供应商、商业伙伴、客户），从而维护组织的安全基线。

	建立，监控并周期性的报告程序管理和运行指标，从而评估信息安全程序的有效性及其效率。
领域 4—信息安全事故管理 Information Security Incident Management (18%)	在组织层面上建立并维护一个对信息安全事件进行定义和严重性分级的机制，从而可以对发生的各类事件进行准确的识别和响应。 建立并维护一个事件响应计划来确保对信息安全事件做出有效且及时的响应。 建立并实施相应的流程来确保对信息安全事件进行及时的识别。 建立并维护对信息安全事件进行调查和记录的流程，从而可以依据法律法规和组织的要求进行适当的响应并确定事件的根源。 建立并维护事件升级和通知的流程，从而确保在事件响应管理中适当层级的利益关系人的及时参与。 对响应团队的组织、培训和资源部署，从而可以及时有效地对信息安全事件做出响应。 对事件响应计划进行周期性的测试和检查，从而确保可以对发生的信息安全事件做出有效的响应，以及可以对响应能力进行不断的优化和改进。 建立并维护沟通的计划和流程，用于对内外部各方的沟通进行全面管理。 进行事后检查用于确定引发信息安全事件的根源，从而确定纠正性的措施、对风险进行再评估、评估响应措施的有效性即采取适当的补救行为。 建立和维护确保事件响应计划、灾难恢复计划、业务连续性计划三者一致性的机制。