

请使用 Adobe Reader 填写这份电子申请表。

申请人信息

申请人姓名 _____ ISACA ID _____
 电子邮件 _____ 电话号码 _____

第 1 步 通过考试

CISA 申请人必须在过去五年内通过 CISA 考试。
 如果您尚未通过 CISA 考试，请在线报名：www.isaca.org/examreq

考试通过年份 _____

第 2 步 报告工作经验

要获得 CISA 认证资格，您必须在申请提交日之前的十 (10) 年内拥有至少五 (5) 年的信息系统审计、控制、鉴证或安全工作经验。此经验必须至少符合一个 CISA 工作实务领域（请查看 V-2 页）。如果您不满足 2A 部分的 5 年工作经验要求，可在 2B 部分和/或 2C 部分提交经验豁免申请（最长可抵减 3 年）。

A 部分：信息系统审计、控制、鉴证或安全工作经验（必填）

请在下表列出您的相关工作经验，从当前或最近的职位开始。
 日期不能留空。如目前处于受雇状态，结束日期为今天。

#	公司名称	聘用日期 (年/月)		工作经验时长 执行 CISA 任务		CISA 工作实务领域 (勾选所有适用项)				
		开始日期	结束日期	年数	月数	1	2	3	4	5
1										
2										
3										
4										

(要求至少 2 年) A 部分经验总年数: _____

B 部分：一般工作经验豁免（选填）

要申请通用信息系统或普通审计工作方面的经验豁免，请填写以下详细信息。
 在 A 部分已声明的任职期间不可用于申请此经验豁免。此为 1 年期豁免。

经验豁免类型 (请选择适用的一项) 普通审计 通用信息系统

公司名称 _____ 开始日期 (月/年) _____ 结束日期 (月/年) _____

(最多 1 年) B 部分经验总年数: _____

C 部分：教育经验豁免（选填）

要申请教育经验豁免，请勾选下面相应的方框并输入学校信息（如适用）。

*请随申请表附上您所就读高校的学位证明、成绩单或信函副本。

**请随申请表附上 CIMA 或 ACCA 证书的副本。

- 副学士学位可抵减 1 年
- 任何研究领域的学士、硕士或博士学位可抵减 2 年
- 信息系统或相关领域的硕士学位可抵减 3 年*
- CIMA (皇家特许管理会计师公会) 完全认证可抵减 2 年**
- 特许公认会计师公会的 ACCA 会员身份可抵减 2 年**

学校名称: _____ 学位类型: _____ 研究领域: _____

(最多 3 年) C 部分经验总年数: _____

D 部分：经验总年数

A、B 和 C 部分的经验总年数必须达到 5 年或以上才能申请 CISA 认证

(A 部分 + B 部分 + C 部分) 经验总年数: _____

请使用 Adobe Reader 填写这份电子申请表。

第 3 步 确认工作经验

使用经验证明表（本申请表 V-1 页和 V-2 页）时，请让一位雇主证明步骤 2 中的所有经验。如需多位证明人，可获取更多经验证明表：www.isaca.org/cisaapp。对于 C 部分声明的证书或学位，请提交证书、学位证明或成绩单的副本。

第 4 步 缴纳手续费

申请人必须缴纳 50 美元的手续费，申请流程方可处理。可通过以下方式缴费：www.isaca.org/cisapay

第 5 步 查阅并签署条款和条件协议

继续职业教育 (CPE) 政策

我在此根据国际信息系统审计协会 (ISACA) 的流程和政策向 ISACA 申请获得注册信息系统审计师 (CISA) 认证的资格。我已阅读并同意《认证申请》和继续职业教育 (CPE) 政策中规定的条件（申请之日起生效），包括认证流程和 CPE 政策。

道德规范

我同意：提供符合资格要求的证明；ISACA 可要求对申请表提交的所有信息进行说明或进一步核实，包括但不限于直接联系任何证明人来核实提交的信息；遵守获得和维护认证的要求，包括关于执行 CISA 任务的资格要求，遵守 ISACA 道德规范、标准和政策，以及履行证书更新要求；如果无法遵守认证要求，应立即通知 ISACA 认证部；执行 CISA 的任务；仅在获准认证的范围内作出有关认证的声明；以及不得以误导性或违反 ISACA 准则的方式使用 CISA 证书、徽标或标记。

信息的真实性

我了解并同意，如果我在本申请表中提供的任何陈述或回答是虚假的，或者违反任何考试规定或认证要求，我的认证申请将被拒绝，并且 ISACA 可撤销和没收已授予我的任何证书。我理解，所有认证证书均归 ISACA 所有，如果我被撤销 CISA 认证资格，我将销毁 CISA 证书、停止使用证书并撤销有关本人认证权利的所有声明。我授权 ISACA 进行其认为必要的任何查询和调查，以核实我的资历和专业水准。

第三方信息共享

我同意，如果我获得认证，我的认证状态将被公开，并且 ISACA 可以向提出要求的第三方披露我的认证状态。我明白，如果我的 CISA 认证申请未获批准，可以联系 ISACA 提出申诉。所有上诉由认证考试参加者、认证申请人或已取得认证人士自行决定提出并且负担相关费用。在下面签名即表示我授权 ISACA 披露我的认证状态。此联系信息将用于执行我的认证查询和请求。

联系政策

在下面签名即表示我授权 ISACA 按照提供的地址和电话与我联系，并且我所提供的信息真实准确。如果法律要求或 ISACA 隐私政策有规定，我授权 ISACA 发布机密的认证申请和认证信息。要详细了解我们如何使用您在此表格中所提供的信息，请阅读我们的隐私政策：www.isaca.org/privacy。

使用协议

我在此同意并保证 ISACA 及其官员、主管、监考人员、雇员、代理人及 ISACA 支持组织的人员免受因以下情况而招致的任何申诉、索赔或损失之损害：任何上述人员与我本次申请相关的任何行为或疏漏；申请流程；未能向我颁发任何证书；或任何没收或重新签发此类证书的要求。除以上所述之外，我了解并同意，如果发生与申请有关的诉讼，此诉讼必须提交至美国伊利诺斯州库克县巡回法院，并需依据美国伊利诺斯州的法律。

我理解，ISACA 将拥有决定我是否具备认证资格的最终和唯一权力。

我已阅读并理解本声明，并愿意受其法律约束。

申请人签名：_____ 日期：_____

第 6 步 提交申请

请在线提交您的申请表、其他证明表（如需要）和任何支持文件，网址：<https://support.isaca.org>

请选择“Certifications & Certificate Programs”（认证和证书计划）以及“Submit an Application”（提交申请）。

申请处理时间一般需要两到三周。获得批准后，您将收到电子邮件通知。认证文件包（包括批准函、CISA 证书和金属 CISA 别针）将以邮递形式发送到您 ISACA 档案中的主要地址。一般需要四到八周的时间送达。

请使用 Adobe Reader 填写这份电子申请表。

申请人详细信息

申请人姓名 _____

ISACA ID _____

表格说明

申请人（姓名如上）通过 ISACA 提出 CISA 认证申请。ISACA 要求申请人的工作经验由曾与其共事的主管或经理独立核实。证明人不能为直系或旁系亲属，也不能是人力资源部的员工。

填写此表即表示您证明申请人在随附的申请表（A-1 页）中所述的工作经验是真实的，符合 CISA 工作实务领域和任务说明（V-2 页）。

请将此证明表返回给申请人提交。如有任何问题或疑问，请通过 <https://support.isaca.org> 或拨打 +1.847.660.5505 联系 ISACA。

证明人信息

证明人姓名 _____

公司名称 _____

职位 _____

电子邮件 _____

电话号码 _____

证明人问题

1. 我证明申请人已获得以下工作经验，如 A-1 页所述（选择所有适用项）：

A 部分：公司 1

A 部分：公司 3

A 部分：公司 2

A 部分：公司 4

2. 我证明以下豁免申请情况属实，如 A-1 页 B 和 C 部分所述（选择所有适用项）：

B 部分：工作经验豁免

C 部分：学历

3. 我证明申请人在以下期间的工作经验属实：

开始日期 _____

结束日期 _____

4. 我曾担任申请人的以下角色：

主管

经理

同事

客户

5. 如果我为申请人在 A 部分所述的任何经验作证，则我也可以证明申请人所执行的任务（如本表格 V-2 页所述）据我所知真实无误。

是

否

证明人协议

我在此确认，据我所知，V-1 页和 V-2 页的信息真实无误，没有理由拒绝该申请人的信息系统审计师认证申请。如果需要，我愿意回答 ISACA 关于上述信息的问题。

证明人签名： _____

日期： _____

请使用 Adobe Reader 填写这份电子申请表。

工作实务领域说明

申请人应勾选曾执行部分或全部任务的所有领域，以便证明人确认。

领域 1：信息系统的审计流程

- 规划审计工作，确定信息系统是否得到保护和控制，以及是否为组织创造价值。
- 按照信息系统审计标准和基于风险的信息系统审计战略执行审计。
- 与利益相关方沟通审计进度、发现、结果和建议。
- 对审计进行跟进，以评估是否充分处置了风险。
- 利用数据分析工具简化审计流程。
- 为组织提供咨询服务和指导，以改善信息系统的质量和控制在。

领域 2：IT 治理与管理

- 评估 IT 战略，以便与组织的战略和目标保持一致。
- 评估 IT 治理结构和 IT 组织结构的有效性。
- 评估组织对 IT 政策和实务的管理。
- 评估组织的 IT 政策和实务，确保其符合法规和法律要求。
- 评估 IT 资源和项目组合管理，确保其与组织的战略和目标保持一致。
- 评估组织的风险管理政策和实务。
- 评估 IT 控制管理与监控。
- 评估 IT 关键绩效指标 (KPI) 的监控和报告。
- 评估 IT 供应商选择和合同管理流程是否符合业务要求。
- 确定组织 IT 策略和实务中的流程改进机会。
- 评估与新兴技术、法规和行业惯例相关的潜在机会和威胁。
- 定期审查信息系统和企业架构。
- 评估信息安全计划，确定其有效性以及是否符合组织的战略和目标。
- 评估 IT 服务管理实务是否符合业务要求。

领域 3：信息系统的购置、开发与实施

- 评估对信息系统进行建议的变更的业务案例是否符合业务目标。
- 评估组织的项目管理政策和实务。
- 对在信息系统开发生命周期各个阶段执行的控制进行评估。
- 对信息系统的生产实施和迁移就绪情况进行评估。
- 对系统进行实施后审查，确定其是否满足项目交付成果、控制和要求。

领域 4：信息系统的运营和业务恢复能力

- 评估 IT 运营以确定其是否得到有效控制并持续支持组织的目标。
- 评估 IT 维护实务以确定其是否得到有效控制并持续支持组织的目标。
- 对数据库管理实务进行评估。
- 评估数据治理政策和实务。
- 对问题和事故管理政策和实务进行评估。
- 评估变更、配置、发布和补丁管理策略及实务。
- 评估最终用户计算以确定流程是否得到有效控制。
- 评估组织维持业务运营的能力。
- 评估与资产生命周期管理相关的政策和实务。

领域 5：保护信息资产

- 评估组织的信息安全和隐私政策及实务。
- 评估物理和环境控制，以确定信息资产是否得到充分保护。
- 评估逻辑安全控制以验证信息的机密性、完整性和可用性。
- 评估数据分类实务，以确保其符合组织的政策和适用的外部要求。
- 执行技术安全测试以识别潜在的威胁和漏洞。
- 评估与新兴技术、法规和行业惯例相关的潜在机会和威胁。