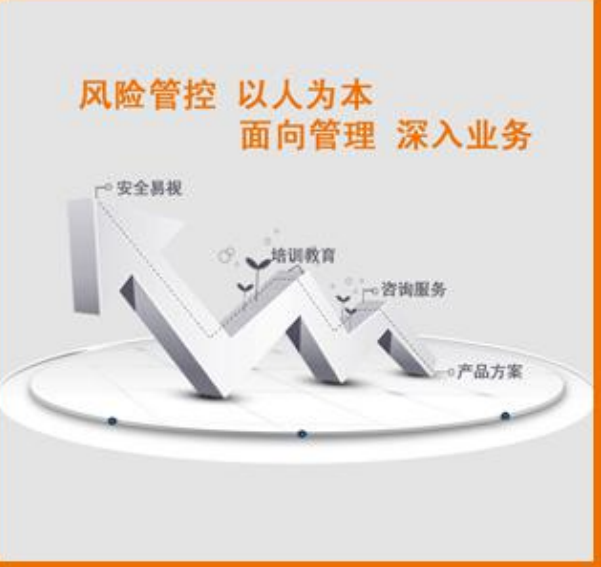


GooAnn
gooann.com 谷安天下

# CISA证书申请指导

谷安天下

2015 ©谷安天下版权所有

# 目录

一、认证申请表填写

二、在线缴费

三、提交申请及申请进度

四、CISA继续职业教育 (CPE) 政策


2015 ©谷安天下版权所有

# 1.进入认证申请页面

**提交认证申请前 需要缴纳50美金的认证费（不缴费 申请是不会处理的）**

https://www.isaca.org/bookstore/pages/product-detail.aspx?product_code=cisa_app **缴纳50美金申请费链接**

http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Apply-for-Certification/Pages/default.aspx

**申请证书链接**

**15年12月之前考试点击此处**

**Individuals taking and passing the CISA exam December 2015 and prior:**

Printable application – Exam passers December 2015 and prior (Best viewed in Internet Explorer) **在线填写点击此处（推荐）**

Download application (881K) **下载手动填写点击此处**

Request an application (sent in postal mail)

**16年6月之后考试点击此处**

**Individuals taking and passing the CISA exam June 2016 and later:**

Printable application – Exam passers June 2016 and later (Best viewed in Internet Explorer) **在线填写点击此处（推荐）**

Download application (512K) **下载手动填写点击此处**

Request an application (sent in postal mail)


2015 ©谷安天下版权所有

CISA Certified Information Systems Auditor™
An ISACA® Certification

Application for CISA Certification

# 1.进入认证申请页面

Requirements to Become a Certified [illegible]
Instructions for Completion of the Ap[illegible]
CISA Certification—Code of Professional Et[illegible]

☐ I have read and understand the above referenced Ethics statements and will adhere to them.

## Application Form

### Applicant Information

申请人资料及目前雇主信息

First Name | Middle Name/Initial | Last/Family | Exam ID

Maiden Name or Former Name:

Preferred Mailing Address: ◯ Home ◯ Business

Home Address | State / Province

Street Address Line 2 | Postal/Zip Code

City | Country

Applicant Home Telephone | Applicant Email Address

### Present Employer Information

Job Title | Business Name

Business Street Address | State / Province

Street Address Line 2 | Postal/Zip Code

City | Country

Business Telephone | Business Fax

Business Email Address

Immediate Supervisor Name: | Supervisor Title

### Work Experience Detail

工作经验信息及豁免

**A. Information Systems Audit, Control or Security Experience**—List your most recent experience first. A candidate must have a minimum of two years of IS audit, control or security experience. Two years of experience is considered 4,000 actual hours, with the exception for full time instructors (see B. Experience Substitution below).

| Employer Name | Dates of employment in IS Audit, Control or Security MM/YY | to | MM/YY | Duration of experience Years | Months |
|---|---|---|---|---|---|
| Employer Name | | to | | | |
| Employer Name | | to | | | |
| Employer Name | | to | | | |
| Total number of years IS auditing, control or security experience (round down to whole year) | | | | Total: | |

**B. Experience Substitution**—A maximum of 1 year IS auditing, control or security experience may be substituted with either **one full year** of auditing experience — or **one full year** of information systems experience.

| Company/ University Name | Dates of Employment MM/YY | to | MM/YY | Type of Experience | Number of Years of Substitution |
|---|---|---|---|---|---|
| | | to | | Non-IS Audit | |
| | | to | | Information Systems | |
| | | to | | University Instructor* | |

*There is no maximum limitation for university instructor experience. However, **two full years** of university instructor experience in a related field is required for each one year of IS auditing, control or security experience substitution.

**C. Educational Experience Waiver**—If you are applying for any experience waivers, please check the appropriate box. To confirm your degree status, please include with your application an original or copy of a transcript or letter from your college or university. Please provide your name as listed on the transcript.

Name on transcript:

☐ Two years experience waiver for a four-year university degree, Masters Degree, or PhD

☐ One year experience waiver for a two-year university degree

☐ Equivalent educational experience to the above, listed here and official verification provided. (list)

☐ One year experience waiver for a university degree that enforces the ISACA sponsored Model Curricula. (Cannot be used if three years substitution or waiver have been claimed.)

**D. Summary of Experience Requirements**

1. Total number of years of information systems audit, control or security experience — enter the total from Section A above (minimum of 2 years)
2. If applying for an experience substitution, enter number of years being substituted in the box and complete Section B above **(maximum of 1 year)**.
3. If applying for an experience waiver, enter 1, 2 or 3 in the box as appropriate and complete Section C above

**Total Work Experience**—add boxes 1, 2 and 3(boxes 2 and 3 cannot exceed 3 years) (must total five years or more to apply for CISA certification)

**E. Individuals Verifying Work Experience Details**—Please record here the names and contact information of the individual(s) that will verify your work experience in sections A and B above:

1. Verifier's Name | Job Title | Company Name
   Company Telephone Number | Company Email Address
2. Verifier's Name | Job Title | Company Name
   Company Telephone Number | Company Email Address
3. Verifier's Name | Job Title | Company Name

Company Telephone Number

Company Email Address

## Verification of Work Experience

I, _____, am applying for certification through ISACA as a Certified Information Systems Auditor. My work experience must be independently verified by my current and/or previous employer(s). The individual verifying the work experience must be an independent verifier and not of any relation to the applicant nor can the verifier verify his/her own work. If I currently or once worked as an independent consultant, I can use a knowledgeable client or an individual certified as a CISA or CISM to perform this role.

I would appreciate your cooperation in completing this form, by verifying my IS auditing, control or security work experience as noted on my application form attached and as described by CISA job practice area and task statements. Please return the complete form to me for my submission to ISACA. If you have any questions concerning this form, please direct them to CISAapplication@isaca.org or +1.847.660.5660. Thank you.

Applicant's Signature

Date

### Employer's Verification Information

雇主的验证信息

Verifier's Name

Company Name

Job Title

Street Address

State / Province

Street Address Line 2

Postal/Zip Code

City

Country

Company Telephone Number

Company Email Address

Name of company relating to candidate's employment from page 2:

**Please answer the six questions below, and then sign and date where indicated on the printed form.**
(The following statements are to be confirmed by the Verifier after printing the application)

1. **Have you functioned in a supervisory position to the applicant such that you can verify his/her work experience?**
2. **How long have you known the applicant?**
3. **Is the categorization and duration of the applicant's work experience, for your organization, as listed on the application for certification form, correct to the best of your knowledge?**
4. **Are you qualified and willing to verify the applicant's work experience prior to his/her affiliation with your company/organization?**
5. **Are you qualified and willing to verify the applicant's educational experience waiver(s) claimed?**
6. **Is there any reason you believe this applicant should not be certified as an information systems auditor?**

## Description of CISA Job Practice Areas

CISA工作实践区的说明

**Please check the boxes that indicate the tasks performed by applicant. Upon review, please sign and date the bottom of this page.**

**Domain 1: The Process of Auditing Information Systems** – Provide audit services in accordance with IT audit standards to assist the organization with protecting and controlling information systems.

**Domain 1 Task Statements**

- ☐ Develop and implement a risk-based IT audit strategy in compliance with IT audit standards to ensure that key areas are included.
- ☐ Plan specific audits to determine whether information systems are protected, controlled and provide value to the organization.
- ☐ Conduct audits in accordance with IT audit standards to achieve planned audit objectives.
- ☐ Report audit findings and make recommendations to key stakeholders to communicate results and effect change when necessary.
- ☐ Conduct follow-ups or prepare status reports to ensure appropriate actions have been taken by management in a timely manner.

**Domain 2: Governance and Management of IT** – Provide assurance that the necessary leadership and organizational structures and processes are in place to achieve objectives and to support the organization's strategy.

**Domain 2 Task Statements**

- ☐ Evaluate the effectiveness of the IT governance structure to ensure adequate board control over the decisions, directions and performance of IT so that it supports the organization's strategies and objectives.
- ☐ Evaluate IT organizational structure and human resources (personnel) management to determine whether they support the organization's strategies and objectives.
- ☐ Evaluate the IT strategy, including the IT direction, and the processes for the strategy's development, approval, implementation and maintenance for alignment with the organization's strategies and objectives.
- ☐ Evaluate the organization's IT policies, standards, and procedures, and the processes for their development, approval, implementation, maintenance, and monitoring, to determine whether they support the IT strategy and comply with regulatory and legal requirements.
- ☐ Evaluate the adequacy of the quality management system to determine whether it supports the organization's strategies and objectives in a cost-effective manner.
- ☐ Evaluate IT management and monitoring of controls (e.g., continuous monitoring, QA) for compliance with the organization's policies, standards and procedures.
- ☐ Evaluate IT resource investment, use and allocation practices, including prioritization criteria, for alignment with the organization's strategies and objectives.
- ☐ Evaluate IT contracting strategies and policies, and contract management practices to determine whether they support the organization's strategies and objectives.
- ☐ Evaluate risk management practices to determine whether the organization's IT-related risks are properly managed.
- ☐ Evaluate monitoring and assurance practices to determine whether the board and executive management receive sufficient and timely information about IT performance.
- ☐ Evaluate the organization's business continuity plan to determine the organization's ability to continue essential business operations during the period of an IT disruption.

**Domain 3: Information Systems Acquisition, Development and Implementation** – Provide assurance that the practices for the acquisition, development, testing, and implementation of information systems meet the organization's strategies and objectives.

**Domain 3 Task Statements**

- ☐ Evaluate the business case for proposed investments in information systems acquisition, development, maintenance and subsequent retirement to determine whether it meets business objectives.
- ☐ Evaluate the project management practices and controls to determine whether business requirements are achieved in a cost-effective manner while managing risks to the organization.
- ☐ Conduct reviews to determine whether a project is progressing in accordance with project plans, is adequately supported by documentation and status reporting is accurate.
- ☐ Evaluate controls for information systems during the requirements, acquisition, development and testing phases for compliance with the organization's policies, standards, procedures and applicable external requirements.
- ☐ Evaluate the readiness of information systems for implementation and migration into production to determine whether project deliverables, controls, and organization's requirements are met.
- ☐ Conduct post-implementation reviews of systems to determine whether project deliverables, controls, and organization's requirements are met.

**Domain 4: Information Systems Operations, Maintenance and Support** – Provide assurance that the processes for information systems operations, maintenance and support meet the organization's strategies and objectives.

**Domain 4 Task Statements**

- ☐ Conduct periodic reviews of information systems to determine whether they continue to meet the organization's objectives.
- ☐ Evaluate service level management practices to determine whether the level of service from internal and external service providers is defined and managed.
- ☐ Evaluate third party management practices to determine whether the levels of controls expected by the organization are being adhered to by the provider.
- ☐ Evaluate operations and end-user procedures to determine whether scheduled and non-scheduled processes are managed to completion.
- ☐ Evaluate the process of information systems maintenance to determine whether they are controlled effectively and continue to support the organization's objectives.
- ☐ Evaluate data administration practices to determine the integrity and optimization of databases.
- ☐ Evaluate the use of capacity and performance monitoring tools and techniques to determine whether IT services meet the organization's objectives.
- ☐ Evaluate problem and incident management practices to determine whether incidents, problems or errors are recorded, analyzed and resolved in a timely manner.
- ☐ Evaluate change, configuration and release management practices to determine whether scheduled and non-scheduled changes made to the organization's production environment are adequately controlled and documented.
- ☐ Evaluate the adequacy of backup and restore provisions to determine the availability of information required to resume processing.
- ☐ Evaluate the organization's disaster recovery plan to determine whether it enables the recovery of IT processing capabilities in the event of a disaster.

**Domain 5: Protection of Information Assets** – Provide assurance that the organization's security policies, standards, procedures and controls ensure the confidentiality, integrity and availability of information assets.

**Domain 5 Task Statements**

- ☐ Evaluate the information security policies, standards and procedures for completeness and alignment with generally accepted practices.
- ☐ Evaluate the design, implementation and monitoring of system and logical security controls to verify the confidentiality, integrity and availability of information.
- ☐ Evaluate the design, implementation, and monitoring of the data classification processes and procedures for alignment with the organization's policies, standards, procedures, and applicable external requirements.
- ☐ Evaluate the design, implementation and monitoring of physical access and environmental controls to determine whether information assets are adequately safeguarded.
- ☐ Evaluate the processes and procedures used to store, retrieve, transport and dispose of information assets (e.g., backup media, offsite storage, hard copy/print data, and softcopy media) to determine whether information assets are adequately safeguarded.

Insert Additional Verification of Work Experience

Clicking the Print button below does not submit your information

# 1.申请人资料及目前雇主信息

Application Form

Applicant Information

姓名

First Name

Middle Name/Initial

Last/Family

准考证号

Exam ID

Maiden Name or Former Name: 曾用名

Preferred Mailing Address: Home Business 地址：家庭或者公司

首选邮寄地址

Home Address

State / Province

Street Address Line 2

Postal/Zip Code

City

家庭地址等

Country

Applicant Home Telephone

Applicant Email Address

Present Employer Information

Job Title

Business Name

Business Street Address

State / Province

Street Address Line 2

现用人单位信息

Postal/Zip Code

City

Country

Business Telephone

Business Fax

Business Email Address

Immediate Supervisor Name:

Supervisor Title



gooann.com 谷 安 天 下
2015 ©谷安天下版权所有

# 2.工作经验信息及豁免

1. **五年的工作经验**才有资格申请 CISA 认证。
2. 必须具备三年**信息系统审计、控制或安全领域工作经验“打底”**；
3. 最多可以抵消两年经验；不够一年的经验不能做为抵消。
4. 非**信息系统审计、控制或安全**的工作经验只能抵消一年经验；
5. 本科及以上学历可以抵消**2年**经验，专科学历可以抵消**1年**经验，需要提交一份大学成绩单或证书的原件或复印件；
6. 经验不够的可以积累工作经验后再申请证，**成绩有效期5年**；

**组合方式：**

五年信息系统审计、控制或安全领域工作经验

三年信息系统审计、控制或安全领域工作经验+本科

四年信息系统审计、控制或安全领域工作经验+专科

四年信息系统审计、控制或安全领域工作经验+非信息系统审计、控制或安全的工作经验

三年信息系统审计、控制或安全领域工作经验+专科+非信息系统审计、控制或安全的工作经验

**特殊情况（大学老师）：**如果用专职大学教师经验来抵减相关领域（例如信息系统、会计、信息系统审计），两“整”年的经验以完成每一年的经验抵减。对于大学教师而言，没有对经验抵减的年限限制。


2015 ©谷安天下版权所有

# 2.工作经验信息及豁免

**A.信息系统审计，控制或安全方面的经验**

先列出你最近期的经验，候选人必须有至少两年的审计，控制或安全方面的经验两年经验被认为是4000实际工时，除全职教师（见下面B.经验抵减）。

1. A 部分 – 信息系统审计、控制或安全经验----对于每一位雇主（从现在的雇主开始），请输入下

列内容：

- 雇主名称
- 从事 IS 审计、控制或安全工作的雇用日期范围（月份和年份）
- 为每一个雇主实施 IS 审计、控制或安全服务的时间以及总计时间（年数和月数）。

Work Experience Detail

A. Information Systems Audit, Control or Security Experience—List your most recent experience first. A candidate must have a minimum of two years of IS audit, control or security experience. Two years of experience is considered 4,000 actual hours, with the exception for full time instructors (see B. Experience Substitution below).

| Employer Name | Dates of employment in IS Audit, Control or Security MM/YY | to | MM/YY | Duration of experience Years | Months |
|---|---|---|---|---|---|
| Employer Name: Beijing GooAnn Technology Co., L | 07/06 | to | 02/12 | 5 | 5 |
| Employer Name: | | to | | | |
| Employer Name: | | to | | | |
| Total number of years IS auditing, control or security experience (round down to whole year) | | | Total: | | |

**信息系统审计、控制或安全经验**


2015 ©谷安天下版权所有

# 2.工作经验信息及豁免

**B.经验抵减**

—A maximum of 1 year IS auditing, control or security experience may be substituted with either **one full year** of auditing experience — or **one full year** of information systems experience. 1年最大可取代任何**一个全年**审计工作经验- **一个**信息系统的经验，**全年的**审计，控制或安全方面的经验。

B 部分 – 经验抵减— 如果要抵减其他审计经验（例如财务审计或营业审计）或其他类型的信息系统工作经验（例如应用程序编程或操作），审计或信息系统工作经验的最大抵减为一“整”年的。如果用专职大学教师经验来抵减相关领域（例如信息系统、会计、信息系统审计），您必须具有两“整”年的经验以完成每一年的经验抵减。对于大学教师而言，没有对经验抵减的年限限制。不够一年的经验不会得到加分。

总结：

1. 非**信息系统审计、控制或安全**的工作经验只能抵消一年，
2. 对于大学老师没有抵消限制

**B. Experience Substitution**—A maximum of 1 year IS auditing, control or security experience may be substituted with either **one full year** of auditing experience — or **one full year** of information systems experience.

| Company/ University Name | Dates of Employment MM/YY | to | MM/YY | Type of Experience | Number of Years of Substitution |
|---|---|---|---|---|---|
| | | to | | Non-IS Audit | |
| | | to | | Information Systems | |
| | | to | | University Instructor* | |

**经验抵减：非审计/信息系统/大学老师**

*There is no maximum limitation for university instructor experience. However, **two full years** of university instructor experience in a related field is required for each one year of IS auditing, control or security experience substitution.


2015 ©谷安天下版权所有

# 2.工作经验信息及豁免

**C.教育经验的豁免**

—If you are applying for any experience waivers, please check the appropriate box.如果您正在寻找任何经验豁免申请，请检查相应的方块。 To confirm your degree status, please include with your application an original or copy of a transcript or letter from your college or university.为了确认您的学籍，请与您的申请书一起附上大专或大学成绩单或信原件或复印件。 Please provide your name as listed on the transcript.，请提供您在成绩单上的姓名。

C 部分 – 教育经验豁免— 选中相应的方框来申请教育经验的豁免。为了确认您的学位水平，请在申请表中附加一份大学成绩单或证书的原件或复印件。为了减少处理时间，请不要单独发送成绩单。

本科及以上学历可以抵消2年经验，专科学历可以抵消1年经验，需要提交一份大学成绩单或证书的原件或复印件

C. Educational Experience Waiver—If you are applying for any experience waivers, please check the appropriate box. To confirm your degree status, please include with your application an original or copy of a transcript or letter from your college or university. Please provide your name as listed on the transcript.

**教育经验的豁免**

Name on transcript:

- ☐ Two years experience waiver for a four-year university degree, Masters Degree, or PhD 为期四年的大学学位，硕士学位或博士学位 **豁免二年经验**
- ☐ One year experience waiver for a two-year university degree 为期二年的大学学位，**豁免1年经验**
- ☐ Equivalent educational experience to the above, listed here and official verification provided. (list) **上述同等教育的经验，在这里列出，并提供官方验证。**
- ☐ One year experience waiver for a university degree that enforces the ISACA sponsored Model Curricula. (Cannot be used if three years substitution or waiver have been claimed.)


2015 ©谷安天下版权所有

# 2.工作经验信息及豁免

**D.总结经验要求 Summary of Experience Requirements**

D 部分 – 经验要求摘要— 记录上述 A-C 部分的总和。标题为“工作经验汇总”（“Total WorkExperience”)的一行应该是在信息系统审计、控制或安全职能部门的工作年限与任何经验抵减或豁免的总和。最少要有五年的工作经验才有资格申请 CISA 认证。

您的五年经验要求中，经验抵减或教育豁免的时间不能超过三年，大学教师的经验抵减除外。

1。 Total number of years of information systems audit, control or security experience — enter the total from Section A above (minimum of 2 years)多年的信息系统审计，控制和安全方面的经验总数 - 从第一个开始进入全部（至少2年以上）

2。 If applying for an experience substitution, enter number of years being substituted in the box and complete Section B above **(maximum of 1 year)** .如果申请的经验替代，输入框和完整的B节**（最多1年）**以上的被取代的年数。

3。 If applying for an experience waiver, enter 1, 2 or 3 in the box as appropriate and complete Section C above如果申请教育经验豁免，在框中输入适当和完整的C节以上1，2或3

D. Summary of Experience Requirements **总结经验要求**

1. Total number of years of information systems audit, control or security experience — enter the total from Section A above (minimum of 2 years)
2. If applying for an experience substitution, enter number of years being substituted in the box and complete Section B above **(maximum of 1 year)**.
3. If applying for an experience waiver, enter 1, 2 or 3 in the box as appropriate and complete Section C above

**Total Work Experience**—add boxes 1, 2 and 3(boxes 2 and 3 cannot exceed 3 years) (must total five years or more to apply for CISA certification)

**Total Work Experience**总的工作经验—add boxes 1, 2 and 3(boxes 2 and 3 cannot exceed 3 years) 1，2，3之和（2，3之和不能超过3年） (must total five years or more to apply for CISA certification) （最少要有五年的工作经验才有资格申请 CISA 认证。）


2015 ©谷安天下版权所有

# 2.工作经验信息及豁免

**E. 验证工作经验的联系人详情**

—Please record here the names and contact information of the individual(s) that will verify your work experience in sections A and B above: - 请在这里记录的姓名和联系人信息，将验证您的工作经验，在A和上文B部分：

**E. Individuals Verifying Work Experience Details**—Please record here the names and contact information of the individual(s) that will verify your work experience in sections A and B above:

| | Verifier's Name | Job Title | Company Name |
|---|---|---|---|
| 1. | Liu Ha | IS auditor | GooAnn |
| | Company Telephone Number: 861051626974 | Company Email Address: liuha@gooann.com | |
| 2. | | | |
| | Company Telephone Number: | Company Email Address: | |
| 3. | | | |
| | Company Telephone Number: | Company Email Address: | |

**验证工作经验的联系人详情**


2015 ©谷安天下版权所有

# 2.工作经验信息及豁免

## 核对工作经验

**Verification of Work Experience**

I, Yi Zheng, am applying for certification through ISACA as a Certified Information Systems Auditor. My work experience must be independently verified by my current and/or previous employer(s). The individual verifying the work experience must be an independent verifier and not of any relation to the applicant nor can the verifier verify his/her own work. If I currently or once worked as an independent consultant, I can use a knowledgeable client or an individual certified as a CISA or CISM to perform this role.

I would appreciate your cooperation in completing this form, by verifying my IS auditing, control or security work experience as noted on my application form attached and as described by CISA job practice area and task statements. Please return the complete form to me for my submission to ISACA. If you have any questions concerning this form, please direct them to CISAapplication@isaca.org or +1.847.660.5660. Thank you.

Applicant's Signature **申请人签名** Date **日期**


2015 ©谷安天下版权所有

# 3.雇主的验证信息和验证

**Employer's Verification Information**

**主管的详细信息**

| | |
|---|---|
| Verifier's Name | [redacted] |
| Job Title | [redacted] |
| Street Address | A-806,Digital Tower,No.2,South Street |
| Street Address Line 2 | ZhongGuanCun,Haidian District,Beijing |
| City | Beijing |
| Company Telephone Number | 861051626974 |
| Company Name | Beijing GooAnn Technology Co., Ltd. |
| State / Province | Beijing |
| Postal/Zip Code | 100086 |
| Country | China |
| Company Email Address | li**@gooann.com |

Name of company relating to candidate's employment from page 2: Beijing GooAnn Technology Co., Ltd.


2015 ©谷安天下版权所有

# 3.雇主的验证信息和验证

1. Have you functioned in a supervisory position to the applicant such that you can verify his/her work experience?你是在一个主管职位，可以验证申请人（他/她）的工作经验？【YES】
2. How long have you known the applicant?您认识申请人有多久？【阿拉伯数字填写年限不要与工作经验冲突】
3. Is the categorization and duration of the applicant‘s work experience, for your organization, as listed on the application for certification form, correct to the best of your knowledge?申请人在您组织的工作经验，申请表上填写的认证信息，是正确的真实的？【YES】
4. Are you qualified and willing to verify the applicant‘s work experience prior to his/her affiliation with your company/organization?你是有资格的，愿意核实申请人的工作经验，之前他/她与贵公司/组织的联系？【YES】
5. Are you qualified and willing to verify the applicant‘s educational experience waiver(s) claimed? 你是有资格的，并愿意以核实申请人的教育经验，减免声名？【YES】或【N/A】
6. Is there any reason you believe this applicant should not be certified as an information systems auditor? 您没有任何理由认为该申请人不应作为一个信息系统审计师认证？【NO】

Please answer the six questions below, and then sign and date where indicated on the printed form.
(The following statements are to be confirmed by the Verifier after printing the application)

1. Have you functioned in a supervisory position to the applicant such that you can verify his/her work experience?
2. How long have you known the applicant?
3. Is the categorization and duration of the applicant's work experience, for your organization, as listed on the application for certification form, correct to the best of your knowledge?
4. Are you qualified and willing to verify the applicant's work experience prior to his/her affiliation with your company/organization?
5. Are you qualified and willing to verify the applicant's educational experience waiver(s) claimed?
6. Is there any reason you believe this applicant should not be certified as an information systems auditor?

请回答下面六个问题，然后打印后签名，并注明日期


2015 ©谷安天下版权所有

# 4. CISA工作实践区的说明

**Domain 1 Task Statements**

- ☐ Develop and implement a risk-based IT audit strategy in compliance with IT audit standards to ensure that key areas are included.
- ☐ Plan specific audits to determine whether information systems are protected, controlled and provide value to the organization.
- ☐ Conduct audits in accordance with IT audit standards to achieve planned audit objectives.
- ☐ Report audit findings and make recommendations to key stakeholders to communicate results and effect change when necessary.
- ☐ Conduct follow-ups or prepare status reports to ensure appropriate actions have been taken by management in a timely manner.

**Domain 2: Governance and Management of IT** – Provide assurance that the necessary leadership and organizational structures and processes are in place to achieve objectives and to support the organization's strategy.

**勾选你工作中会运用到的领域**

**Domain 2 Task Statements**

- ☐ Evaluate the effectiveness of the IT governance structure to ensure adequate board control over the decisions, directions and performance of IT so that it supports the organization's strategies and objectives.
- ☐ Evaluate IT organizational structure and human resources (personnel) management to determine whether they support the organization's strategies and objectives.
- ☐ Evaluate the IT strategy, including the IT direction, and the processes for the strategy's development, approval, implementation and maintenance for alignment with the organization's strategies and objectives.
- ☐ Evaluate the organization's IT policies, standards, and procedures, and the processes for their development, approval, implementation, maintenance, and monitoring, to determine whether they support the IT strategy and comply with regulatory and legal requirements.
- ☐ Evaluate the adequacy of the quality management system to determine whether it supports the organization's strategies and objectives in a cost-effective manner.
- ☐ Evaluate IT management and monitoring of controls (e.g., continuous monitoring, QA) for compliance with the organization's policies, standards and procedures.
- ☐ Evaluate IT resource investment, use and allocation practices, including prioritization criteria, for alignment with the organization's strategies and objectives.
- ☐ Evaluate IT contracting strategies and policies, and contract management practices to determine whether they support the organization's strategies and objectives.
- ☐ Evaluate risk management practices to determine whether the organization's IT-related risks are properly managed.
- ☐ Evaluate monitoring and assurance practices to determine whether the board and executive management receive sufficient and timely information about IT performance.
- ☐ Evaluate the organization's business continuity plan to determine the organization's ability to continue essential business operations during the period of an IT disruption.

**域名1：审计信息系统的过程** -按照IT审计标准，以协助保护和控制信息系统的组织提供审计服务。

**1域任务报表**

- ☐ 在符合IT审计标准制定和实施，以确保关键领域包括以风险为基础的IT审计策略。
- ☐ 计划的具体审核，以确定信息系统是否受到保护，控制和组织提供价值。
- ☐ 按照IT审计标准，以实现审计目标计划进行审核。
- ☐ 报告审计结果和提出建议的关键利益相关者沟通的结果和效果的变化，必要时。
- ☐ 进行跟进或准备状态报告，以确保管理层及时采取适当的行动。

**2域的IT治理和管理** -保证必要的领导和组织结构和流程，实现目标，并支持该组织的战略。

**2域任务报表**

- ☐ 评估IT治理结构的有效性，以确保足够的决定，指示和IT性能，董事会的控制权，所以它支持该组织的战略和目标。
- ☐ 评估IT组织结构和人力资源（人事）管理，以确定他们是否支持该组织的战略和目标。
- ☐ 评估IT战略，包括IT的方向，发展战略，审批，实施和维护与组织的战略和目标相一致的过程。
- ☐ 评估组织的IT政策，标准和程序，并为他们的发展过程中，审批，实施，维护，监控，以确定它们是否支持IT战略和遵守法规和法律要求。
- ☐ 评估的质量管理体系，以确定它是否支持该组织的战略和目标，在成本效益的方式是否足够。
- ☐ 评估IT管理与遵守该组织的政策，标准和程序，监测和控制（例如，连续监测，质量保证）。
- ☐ 评估IT资源的投资，与组织的战略和目标相一致的使用和分配的做法，包括优先级标准，。
- ☐ 评估的IT战略和政策，承包和合同管理的做法，以确定它们是否支持该组织的战略和目标。
- ☐ 评估风险管理的做法，以确定是否组织的IT相关的风险得到妥善管理。
- ☐ 评估监测和保证措施，以确定是否董事会和执行管理IT性能得到充分和及时的信息。
- ☐ 评估组织的业务连续性计划，以确定该组织的能力，继续在一个IT中断期间的基本业务。

GooAnn gooann.com 谷 安 天 下


2015 ©谷安天下版权所有

# 4. CISA工作实践区的说明

**Domain 3: Information Systems Acquisition, Development and Implementation** – Provide assurance that the practices for the acquisition, development, testing, and implementation of information systems meet the organization's strategies and objectives.

**Domain 3 Task Statements**

- ☐ Evaluate the business case for proposed investments in information systems acquisition, development, maintenance and subsequent retirement to determine whether it meets business objectives.
- ☐ Evaluate the project management practices and controls to determine whether business requirements are achieved in a cost-effective manner while managing risks to the organization.
- ☐ Conduct reviews to determine whether a project is progressing in accordance with project plans, is adequately supported by documentation and status reporting is accurate.
- ☐ Evaluate controls for information systems during the requirements, acquisition, development and testing phases for compliance with the organization's policies, standards, procedures and applicable external requirements.
- ☐ Evaluate the readiness of information systems for implementation and migration into production to determine whether project deliverables, controls, and organization's requirements are met.
- ☐ Conduct post-implementation reviews of systems to determine whether project deliverables, controls, and organization's requirements are met.

**Domain 4: Information Systems Operations, Maintenance and Support** – Provide assurance that the processes for information systems operations, maintenance and support meet the organization's strategies and objectives.

**Domain 4 Task Statements**

- ☐ Conduct periodic reviews of information systems to determine whether they continue to meet the organization's objectives.
- ☐ Evaluate service level management practices to determine whether the level of service from internal and external service providers is defined and managed.
- ☐ Evaluate third party management practices to determine whether the levels of controls expected by the organization are being adhered to by the provider.
- ☐ Evaluate operations and end-user procedures to determine whether scheduled and non-scheduled processes are managed to completion.
- ☐ Evaluate the process of information systems maintenance to determine whether they are controlled effectively and continue to support the organization's objectives.
- ☐ Evaluate data administration practices to determine the integrity and optimization of databases.
- ☐ Evaluate the use of capacity and performance monitoring tools and techniques to determine whether IT services meet the organization's objectives.
- ☐ Evaluate problem and incident management practices to determine whether incidents, problems or errors are recorded, analyzed and resolved in a timely manner.
- ☐ Evaluate change, configuration and release management practices to determine whether scheduled and non-scheduled changes made to the organization's production environment are adequately controlled and documented.
- ☐ Evaluate the adequacy of backup and restore provisions to determine the availability of information required to resume processing.
- ☐ Evaluate the organization's disaster recovery plan to determine whether it enables the recovery of IT processing capabilities in the event of a disaster.

**域3：信息系统采集，开发和实施** -收购的做法，信息系统的开发，测试和实施符合该组织的战略和目标提供保证。

**3域任务报表**

- ☐ 评估信息系统采集，开发，维护和后续退休，以确定它是否符合业务目标的拟议投资的商业案例。
- ☐ 评估的项目管理实践和控制，以确定是否风险管理组织的同时，在成本效益的方式实现业务需求。
- ☐ 进行审查，以确定项目是否按照项目计划的进展，充分支持文档和状态报告是准确的。
- ☐ 评估信息系统的控制，在遵守该组织的政策，标准，程序和适用的外部需求的要求，收购，开发和测试阶段。
- ☐ 评估信息系统的实施和迁移到生产准备，以确定是否满足项目交付，控制和组织的要求。
- ☐ 制度实施后进行审查，以确定项目可交付成果，控制和组织的要求是否得到满足。

**勾选你工作中会运用到的领域**

**域4：信息系统操作，维护和支持** -提供保证，信息系统操作流程，维护和支持符合组织的战略和目标。

**4域任务报表**

- ☐ 信息系统进行定期审查，以确定他们是否继续满足该组织的目标。
- ☐ 评估管理服务水平的做法，以确定是否定义和管理，从内部和外部服务提供商的服务水平。
- ☐ 评估第三方管理做法，以确定是否遵守该组织控制的预期水平正在提供商。
- ☐ 评估操作和最终用户的程序，以确定是否定期和不定期的流程管理完成。
- ☐ 评估信息系统的维护过程，以确定它们是否有效控制，并继续支持该组织的目标。
- ☐ 评价数据管理的做法，以确定数据库的完整性和优化。
- ☐ 使用的容量和性能监控工具和技术评估，以确定是否IT服务满足组织的目标。
- ☐ 评估，以确定是否被记录的事件，问题或错误，分析和及时解决问题和事件管理的做法。
- ☐ 评估变更，配置和发布管理的做法，以确定是否定期和不定期组织的生产环境的变化有足够的控制和记录。
- ☐ 评估充足的备份和恢复的条文，以确定恢复处理所需的信息的可用性。
- ☐ 评估组织的灾难恢复计划，以确定它是否能够恢复IT处理能力，在灾难发生时。

GooAnn gooann.com 谷安天下


2015 ©谷安天下版权所有

# 4. CISA工作实践区的说明

**Domain 5: Protection of Information Assets** – Provide assurance that the organization's security policies, standards, procedures and controls ensure the confidentiality, integrity and availability of information assets.

**Domain 5 Task Statements**

- ☐ Evaluate the information security policies, standards and procedures for completeness and alignment with generally accepted practices.
- ☐ Evaluate the design, implementation and monitoring of system and logical security controls to verify the confidentiality, integrity and availability of information.
- ☐ Evaluate the design, implementation, and monitoring of the data classification processes and procedures for alignment with the organization's policies, standards, procedures, and applicable external requirements.
- ☐ Evaluate the design, implementation and monitoring of physical access and environmental controls to determine whether information assets are adequately safeguarded.
- ☐ Evaluate the processes and procedures used to store, retrieve, transport and dispose of information assets (e.g., backup media, offsite storage, hard copy/print data, and softcopy media) to determine whether information assets are adequately safeguarded.

**勾选你工作中会运用到的领域**

**域5：保护信息资产** -保证组织的安全政策，标准，程序和控制，确保信息资产的保密性，完整性和可用性。

**5域任务报表**

- ☐ 评估的信息安全政策，标准和程序的完整性和普遍接受的做法保持一致。
- ☐ 评估，设计，实施和监测系统和逻辑安全控制，以核实信息的保密性，完整性和可用性。
- ☐ 评估的设计，实施和监测的数据进行分类的过程和程序，与该组织的政策，标准，程序，适用的外部需求保持一致。
- ☐ 评估，设计，实施和监控物理访问和环境的控制，以确定是否信息资产得到充分的保障。
- ☐ 评估的过程和程序，用于存储，检索，传输和处理信息资产（例如，备份介质，异地存储，硬拷贝/打印数据和下载版媒体），以确定是否信息资产得到充分的保障。

www.gooann.com
2015 ©谷安天下版权所有

# 5.插入额外需核查的工作经验

如果需要验证的工作经验不止一家公司的话，就要**插入额外需核查的工作经验**

organization's strategies and objectives.

**Domain 3 Task Statements**

- Evaluate the business case for proposed investments in information systems acquisition, development, maintenance and subsequent retirement to determine whether it meets business objectives.
- Evaluate the project management practices and controls to determine whether business requirements are achieved in a cost-effective manner while managing risks to the organization.

confidentiality, integrity and availability of information.

- Evaluate the design, implementation, and monitoring of the data classification processes and procedures for alignment with the organization's policies, standards, procedures, and applicable external requirements.
- Evaluate the design, implementation and monitoring of physical access and environmental controls to determine whether information assets are adequately safeguarded.
- Evaluate the processes and procedures used to store, retrieve, transport and dispose of information assets (e.g., backup media, offsite storage, hard copy/print data, and softcopy media) to determine whether information assets are adequately safeguarded.

Insert Additional Verification of Work Experience

**插入额外需核查的工作经验**

Clicking the Print button below does not submit your information.
Please sign the completed application and either email, fax or postal mail your application to:

**ISACA**
3701 N. Algonquin Rd.
Suite 1010

Print CISA Application


gooann.com 谷 安 天 下
2015 ©谷安天下版权所有

# 6. 申请证书扫描件实例

CISA

Page 1

## Applicant Information

First Name: Yi
Middle Name/Initial:
Last/Family: [redacted]
Exam ID: 117[redacted]
Maiden Name or Former Name:

Preferred Mailing Address: Home / Business
Home Address: A-806,Digital Tower,No.2,South Street
Street Address Line 2: ZhongGuanCun,Haidian District,Beijing
City: Beijing
Applicant Home Telephone: 861051626974
State / Province: Beijing
Postal/Zip Code: 100086
Country: China
Applicant Email Address: [redacted]@126.com

## Present Employer Information

Job Title: Consultant
Business Street Address: A-806,Digital Tower,No.2,South Street
Street Address Line 2: ZhongGuanCun,Haidian District,Beijing
City: Beijing
Business Telephone: 861051626974
Business Email Address: zhengyi@gooann.com
Immediate Supervisor Name: Hua Li
Business Name: Beijing GooAnn Technology Co., Ltd.
State / Province: Beijing
Postal/Zip Code: 100086
Country: China
Business Fax: 861051626975
Supervisor Title: CEO

I hereby apply to ISACA for issuance to me of Certification, as a Certified Information Systems Auditor (CISA) in accordance with and subject to the procedures and regulations of ISACA. I have read and agree to the conditions set forth in the CISA Application for Certification and Continuing Education Policy in effect at the time of my application, covering the Certification process, and Continuing Education policies. I agree to denial of Certification and to forfeiture and redelivery of any certificate or other credential granted me by ISACA in the event that any of the statements or answers made by me in this application are false or in the event that I violate any of the rules or regulations governing such exam. I understand that all certificates are owned by ISACA and if my certificate is granted and then revoked, I will destroy the certificate.

I authorize ISACA to make whatever inquiries and investigations it deems necessary to verify my credentials and my professional standing. If you become a Certified Information Systems Auditor, your certification status will become public, and may be disclosed by ISACA to third parties who inquire. If my application is not approved, I understand that I am able to appeal the decision by contacting certification@isaca.org. By signing below, you authorize ISACA to disclose your certification status. The contact information will be used to fulfill your request, and may also be used by ISACA to send you information about related ISACA goods and services, and other information in which we believe you may be interested. By signing below, you authorize ISACA to contact you at the address and number you have provided, including to provide you with marketing and promotional communications. You further represent that the information you provided is yours and is accurate. To learn more about how we use the information you have provided on this form, please read our Privacy Policy, available at www.isaca.org. If you are already and ISACA member, and /or if you elect to attend one of our events or purchase other ISACA programs or services, information you submit may also be used as described to you at that time.

I hereby agree to hold ISACA, its officers, directors, examiners, employees, and agents, harmless from any complaint, claim, or damage arising out of any action or omission by any of them in connection with this application; the application process; the failure to issue me any certificate; or any demand for forfeiture or redelivery of such certificate.

**I understand that the decision as to whether I qualify for certification rests solely and exclusively with ISACA and that the decision of ISACA is final. I have read and understand these statements and I intend to be legally bound by them.**

Name: [redacted]

Signature: [redacted]

申请人签名

Date: 10-Feb-2012

# 6. 申请证书扫描件实例

CISA Certified Information Systems Auditor — Application for CISA Certification



Applicant Name: [illegible] Exam ID: 1[redacted]

## Work Experience Detail

**A. Information Systems Audit, Control or Security Experience**—List your most recent experience first. A candidate must have a minimum of two years of IS audit, control or security experience. Two years of experience is considered 4,000 actual hours, with the exception for full time instructors (see B. Experience Substitution below).

| Employer Name | Dates of employment in IS Audit, Control or Security MM/YY | to | MM/YY | Duration of experience Years | Months |
|---|---|---|---|---|---|
| Beijing GooAnn Technology Co., Ltd. | 07/06 | to | 02/12 | 5 | 5 |
| Employer Name | | to | | | |
| Employer Name | | to | | | |
| Total number of years IS auditing, control or security experience (round down to whole year) | | | Total: | 5 | 5 |

**B. Experience Substitution**—A maximum of 1 year IS auditing, control or security experience may be substituted with either **one full year** of auditing experience — or **one full year** of information systems experience.

| Company/ University Name | Dates of Employment MM/YY | to | MM/YY | Type of Experience | Number of Years of Substitution |
|---|---|---|---|---|---|
| | | to | | Non-IS Audit | |
| | | to | | Information Systems | |
| | | to | | University Instructor* | |

*There is no maximum limitation for university instructor experience. However, **two full years** of university instructor experience in a related field is required for each one year of IS auditing, control or security experience substitution.

**C. Educational Experience Waiver**—If you are applying for any experience waivers, please check the appropriate box. To confirm your degree status, please include with your application an original or copy of a transcript or letter from your college or university. Please provide your name as listed on the transcript.

Name on transcript:

- ☐ Two years experience waiver for a four-year university degree, Masters Degree, or PhD
- ☐ One year experience waiver for a two-year university degree
- ☐ Equivalent educational experience to the above, listed here and official verification provided. (list)
- ☐ One year experience waiver for a university degree that enforces the ISACA sponsored Model Curricula. (Cannot be used if three years substitution or waiver have been claimed.)

**D. Summary of Experience Requirements**

| | | |
|---|---|---|
| 1. | Total number of years of information systems audit, control or security experience — enter the total from Section A above (minimum of 2 years) | 5 |
| 2. | If applying for an experience substitution, enter number of years being substituted in the box and complete Section B above (**maximum of 1 year**). | |
| 3. | If applying for an experience waiver, enter 1, 2 or 3 in the box as appropriate and complete Section C above | |
| | **Total Work Experience**—add boxes 1, 2 and 3(boxes 2 and 3 cannot exceed 3 years) (must total five years or more to apply for CISA certification) | 5 |

**E. Individuals Verifying Work Experience Details**—Please record here the names and contact information of the individual(s) that will verify your work experience in sections A and B above:

| | Verifier's Name | Job Title | Company Name |
|---|---|---|---|
| 1. | Y[redacted]n | IS auditor | GooAnn |
| | Company Telephone Number: 861051626974 | Company Email Address: hanyu@gooann.com | |
| 2. | Verifier's Name | Job Title | Company Name |
| | Company Telephone Number | Company Email Address | |
| 3. | Verifier's Name | Job Title | Company Name |
| | Company Telephone Number | Company Email Address | |

# 6. 申请证书扫描件实例

Application for CISA Certification

Page 3

Applicant Name: Yi Zheng

Exam ID: [redacted]

## Verification of Work Experience

I, Yi Zheng, am applying for certification through ISACA as a Certified Information Systems Auditor. My work experience must be independently verified by my current and/or previous employer(s). The individual verifying the work experience must be an independent verifier and not of any relation to the applicant nor can the verifier verify his/her own work. If I currently or once worked as an independent consultant, I can use a knowledgeable client or an individual certified as a CISA or CISM to perform this role.

I would appreciate your cooperation in completing this form, by verifying my IS auditing, control or security work experience as noted on my application form attached and as described by CISA job practice area and task statements. Please return the complete form to me for my submission to ISACA. If you have any questions concerning this form, please direct them to CISAapplication@isaca.org or +1.847.660.5660. Thank you.

申请人签名

Applicant's Signature [redacted] Date 2012/2/10

## Employer's Verification Information

Verifier's Name
[redacted]

Company Name
Beijing GooAnn Technology Co., Ltd.

Job Title
CEO

Street Address
A-806,Digital Tower,No.2,South Street

State / Province
Beijing

Street Address Line 2
ZhongGuanCun,Haidian District,Beijing

Postal/Zip Code
100086

City
Beijing

Country
China

Company Telephone Number
861051626974

Company Email Address
[redacted]@gooann.com

Name of company relating to candidate's employment from page 2: Beijing GooAnn Technology Co., Ltd.

回答相关问题

Please answer the six questions below, and then sign and date where indicated on the printed form.
(The following statements are to be confirmed by the Verifier after printing the application)

| | | Yes | No | N/A |
|---|---|---|---|---|
| 1. | Have you functioned in a supervisory position to the applicant such that you can verify his/her work experience? | ✓ | | |
| 2. | How long have you known the applicant? 5 | | | |
| 3. | Is the categorization and duration of the applicant's work experience, for your organization, as listed on the application for certification form, correct to the best of your knowledge? | ✓ | | |
| 4. | Are you qualified and willing to verify the applicant's work experience prior to his/her affiliation with your company/organization? | ✓ | | |
| 5. | Are you qualified and willing to verify the applicant's educational experience waiver(s) claimed? | | | |
| 6. | Is there any reason you believe this applicant should not be certified as an information systems auditor? | | ✓ | |

证明人签名

[redacted] 2012/2/10

# 6. 申请证书扫描件实例

证明人签名

勾选你工作中会运用到的领域

CISA

Page 4

Applicant Name: Yi Zheng

Applicant Exam ID: [redacted]

Verifier Name: Hua Li

[redacted]

Verifier's Signature

2012/2/10

Date

## Description of CISA Job Practice Areas

Please check the boxes that indicate the tasks performed by applicant. Upon review, please sign and date the bottom of this page.

**Domain 1: The Process of Auditing Information Systems** – Provide audit services in accordance with IT audit standards to assist the organization with protecting and controlling information systems.

**Domain 1 Task Statements**

- ✓ Develop and implement a risk-based IT audit strategy in compliance with IT audit standards to ensure that key areas are included.
- ✓ Plan specific audits to determine whether information systems are protected, controlled and provide value to the organization.
- Conduct audits in accordance with IT audit standards to achieve planned audit objectives.
- Report audit results in accordance with IT audit standards including communication of issues and potential impact.
- Conduct follow-up or monitor status reports to ensure identified audit issues have been taken by management in a timely manner.

**Domain 2: Governance and Management of IT** – Provide assurance that the necessary leadership and organizational structures and processes are in place to achieve objectives and to support the organization's strategy.

**Domain 2 Task Statements**

- ✓ Evaluate the effectiveness of the IT governance structure to ensure adequate board control over the decisions, directions and performance of IT so that it supports the organization's strategies and objectives.
- ✓ Evaluate IT organizational structure and human resources (personnel) management to determine whether they support the organization's strategies and objectives.
- Evaluate the IT strategy, including the IT direction, and the processes for the strategy's development, approval, implementation and maintenance for alignment with the organization's strategies and objectives.
- Evaluate the organization's IT policies, standards, and procedures, and the processes for their development, approval, implementation, maintenance and monitoring, to determine whether they support the IT strategy and comply with regulatory and legal requirements.
- Evaluate the adequacy of the quality management system to determine whether it supports the organization's strategies and objectives in a cost-effective manner.
- Evaluate IT management and monitoring of controls (e.g., continuous monitoring, QA) for compliance with the organization's policies, standards and procedures.
- Evaluate IT resource investment, use and allocation practices, including prioritization criteria, for alignment with the organization's strategies and objectives.
- Evaluate IT contracting strategies and policies, and contract management practices to determine whether they support the organization's strategies and objectives.
- ✓ Evaluate risk management practices to determine whether the organization's IT-related risks are properly managed.
- Evaluate monitoring and assurance practices to determine whether the board and executive management receive sufficient and timely information about IT performance.
- ✓ Evaluate the organization's business continuity plan to determine the organization's ability to continue essential business operations during the period of an IT disruption.

**Domain 3: Information Systems Acquisition, Development and Implementation** – Provide assurance that the practices for the acquisition, development, testing, and implementation of information systems meet the organization's strategies and objectives.

**Domain 3 Task Statements**

- Evaluate the business case for proposed investments in information systems acquisition, development, maintenance and subsequent retirement to determine whether it meets business objectives.
- Evaluate the project management practices and controls to determine whether business requirements are achieved in a cost-effective manner while managing risks to the organization.
- Conduct reviews to determine whether a project is progressing in accordance with project plans, is adequately supported by documentation and status reporting is accurate.
- ✓ Evaluate controls for information systems during the requirements, acquisition, development and testing phases for compliance with the organization's policies, standards, procedures and applicable external requirements.
- ✓ Evaluate the readiness of information systems for implementation and migration into production to determine whether project deliverables, controls, and organization's requirements are met.
- ✓ Conduct post-implementation reviews of systems to determine whether project deliverables, controls, and organization's requirements are met.

**Domain 4: Information Systems Operations, Maintenance and Support** – Provide assurance that the processes for information systems operations, maintenance and support meet the organization's strategies and objectives.

**Domain 4 Task Statements**

- Conduct periodic reviews of information systems to determine whether they continue to meet the organization's objectives.
- Evaluate service level management practices to determine whether the level of service from internal and external service providers is defined and managed.
- ✓ Evaluate third party management practices to determine whether the levels of controls expected by the organization are being adhered to by the provider.
- Evaluate operations and end-user procedures to determine whether scheduled and non-scheduled processes are managed to completion.
- Evaluate the process of information systems maintenance to determine whether they are controlled effectively and continue to support the organization's objectives.
- ✓ Evaluate data administration practices to determine the integrity and optimization of databases.
- Evaluate the use of capacity and performance monitoring tools and techniques to determine whether IT services meet the organization's objectives.
- ✓ Evaluate problem and incident management practices to determine whether incidents, problems or errors are recorded, analyzed and resolved in a timely manner.
- ✓ Evaluate change, configuration and release management practices to determine whether scheduled and non-scheduled changes made to the organization's production environment are adequately controlled and documented.
- ✓ Evaluate the adequacy of backup and restore processes to determine the availability of information required to resume processing.
- ✓ Evaluate the organization's disaster recovery plan to determine whether it enables the recovery of IT processing capabilities in the event of a disaster.

**Domain 5: Protection of Information Assets** – Provide assurance that the organization's security policies, standards, procedures and controls ensure the confidentiality, integrity and availability of information assets.

**Domain 5 Task Statements**

- ✓ Evaluate the information security policies, standards and procedures for completeness and alignment with generally accepted practices.
- ✓ Evaluate the design, implementation and monitoring of system and logical security controls to verify the confidentiality, integrity and availability of information.
- ✓ Evaluate the design, implementation, and monitoring of the data classification processes and procedures for alignment with the organization's policies, standards, procedures, and applicable external requirements.
- ✓ Evaluate the design, implementation and monitoring of physical and environmental controls to determine whether information assets are adequately safeguarded.
- ✓ Evaluate the processes and procedures used to store, retrieve, transport and dispose of information assets (e.g., backup media, offsite storage, hard-copy data, and software) media) to determine whether information assets are adequately safeguarded.

# 目录

一、认证申请表填写

二、在线缴费

三、提交申请及申请进度

四、CISA继续职业教育 (CPE) 政策


2015 ©谷安天下版权所有

# 1.加入购物车

## 第一步

**打开：[www.isaca.org/cisapay](http://www.isaca.org/cisapay) 进入购买页面，点击**

2015 ©谷安天下版权所有

# 2.确认信息

## 第二步 确认购物信息

**Global shopping cart**

| Bill To Address | Ship To Address |
|---|---|
| Mr. [redacted]<br>Beijing GooAnn Technology Co., Ltd.<br>A-806, Digital Tower, No 2<br>South Street, Zhongguancun, Haidian<br>Beijing, 100086<br>China | [redacted]A<br>A-806, Digital Tower, No 2<br>South Street, Zhongguancun, Haidian<br>Beijing, 100086<br>China |

Edit Shipping Address

3.修改购物地址

If you purchased books and are shipping to a P.O. Box, please also include the street address to ensure proper delivery.

| Remove | Item # | Type | Description | Qty | Unit Price | Ext. Price |
|---|---|---|---|---|---|---|
| ☐ | CISA_APP | SALES | CISA Application Processing Fee | 1 | $50.00 | $50.00 |

| | |
|---|---|
| **Subtotal:** | **$50.00** |
| Shipping(FEDEX): | $0.00 |
| Total before tax: | |
| Estimated tax: | |
| **Order Total:** | **$50.00** |

4.进行支付

Clear cart | Update cart | Print | Enter Code | Continue shopping | Pay by Check or Bank Transfer | Checkout


2015 ©谷安天下版权所有

# 3.支付

## 第三步 输入信用卡号进行支付

**Payment Details**

| | |
|---|---|
| Payment Method | Credit Card<br>Debit Card (with VISA or MasterCard logo) |
| Card Type * | VISA |
| Card Number<br>*Note: Do not use spaces, non-numeric characters, or dashes.* | |
| Expiration Date (Month, Year) * | 1 2012 |
| Name on card * | [redacted] |
| Credit Card Security Code (CVV) * | •••••••• |
| Payment Amount (US Dollars) | $50.00* |

*** Please note: Upon clicking the "Submit Payment" button, your credit card will be charged the amount shown above.**
If you do not wish to submit payment at this time, you may press Cancel to cancel the payment an
Cart. Cancelling the payment will not remove the items from your cart.

I understand that information I submit will be used as described in the Privacy Policy and that my purcha is subject to the Terms of Use and any additional purchase rules and guidelines in this site.

Submit Payment | Cancel

5.提交支付


2015 ©谷安天下版权所有

# 目录

一、认证申请表填写

二、在线缴费

三、提交申请及申请进度

四、CISA继续职业教育 (CPE) 政策


2015 ©谷安天下版权所有

# 1.向certification@isaca.org发送邮件

收件人：certification@isaca.org；

附　件：2 个（1-2.JPG 等...）查看全部附件

发送状态：发送成功[查看详情]

Dear certification:

I am very honored to have passed the CISA exam,now apply for CISA certification.

Attachment is the application information

Exam ID: [redacted]

Thank you

3. 为了有效处理您的申请表，请收集所有证明文件（工作经验证实表与任何适用的大学成绩单或证书），然后同您完成的 CISA 认证申请表一并邮寄给：
   - 认证协调者
   - ISACA
   - 3701 Algonquin Road, Suite 1010
   - Rolling Meadows, IL 60008-3124 USA
   - 电子邮件：certification@isaca.org cisaapplication@isaca.org
   - *电话号码：+1.847.660.5660 传真号码：*
   - *+1.847.253.1443*


2015 ©谷安天下版权所有

# 2.申请进度

注意：请允许我们利用大概八个星期的时间来处理您完成的“CISA 认证申请表”。审核通过后，您将通过电子邮件收到证书套件，包括认证通知书、您的 CISA 证书以及“CISA 持续教育政策”。

证书申请状态大致时间点：

2015.01.23 提交CISA证书申请

201.01.26 收到ISACA Certification Assistant（认证助理）的确认信，表示收到申请【一周左右】

2015.02.02 收到ISACA Certification Department（认证部）的确认信，表示收到申请【二周左右】

2015.03.15 收到ISACA的邮件表示通过认证【八周左右】

2015.4-6月 ISACA寄来的纸质证书和徽章~~~ 【十二周左右】

关于ISACA 官网上的证书申请状态变化：

2015.01.26 - 03.15 Application Status: Unreviewed

2015.03.16 Application Status: Complete-Under Review

2015.03.17 - 04.11 Application Status: Approved


2015 ©谷安天下版权所有

# 3.CISA证书-实例

CISA Certified Information Systems Auditor

ISACA

CERTIFIED INFORMATION SYSTEMS AUDITOR

ISACA hereby certifies that

[redacted]

has successfully met all requirements and is qualified as a Certified Information Systems Auditor; in witness whereof, we have subscribed our signatures to this certificate.

Requirements include prerequisite professional experience; adherence to the ISACA Code of Professional Ethics and the CISA continuing professional education policy; and passage of the CISA exam.

03 April 2012
Date of Certification

Kenneth L. VanderWal
International President of ISACA and ITG

31 January 2016
Expiration Date

Chair, CISA Certification Committee

[redacted]
Certificate Number

ANSI
ISO/IEC 17024

ISACA
Trust in, and value from, information systems


2015 ©谷安天下版权所有

# 目录

一、认证申请表填写

二、在线缴费

三、提交申请及申请进度

四、CISA继续职业教育 (CPE) 政策


2015 ©谷安天下版权所有

# 1.CISA继续职业教育 (CPE) 政策总体要求

CISA通过后申请到了证书要进行持续再教育，获得学分，简称CPE，ISACA官方的规定三年需要120个学分每年至少20个学分，才能维持证书，如果不能完成学习。那么证书只有三年有效期，三年后学分不足就要重考，只有维持下去才是有效的！第一年不需要

CISA CPE 政策要求在年度和三年认证期都达到 CPE 所要求的学时。CISA 必须符合如下要求才能保持其资格：

1. 每年最低应达到并报告 20 个 CPE 学时。
2. 向 ISACA（国际信息系统审计协会）国际总部全额交付 CPE 维护年费【会员$ 40,非会员$ 85,会员费$ 135】。
3. 在三年报告期间最低应达到并报告 120 个 CPE 学时。
4. 被选中参加年度审查时，必须响应并提交参加 CPE 活动的所需文件记录。
5. 遵守 ISACA 的职业道德规范。


2015 ©谷安天下版权所有

# 2.CPE学分如何获取

1. ISACA 职业教育活动和会议（无限制）
2. 非 ISACA 职业教育活动和会议（无限制）
3. 自学课程（无限制）
4. 经销商的产品推销/营销展示（每年限 10 小时）
5. 教学/演讲/展示（无限制）
6. 发表文章、专题著作和书籍（无限制）
7. 试题编写和审核（无限制）
8. 通过相关的职业考试（无限制）
9. ISACA 理事会/委员会工作（每项 ISACA 认证限每年 20 小时）
10. 对信息系统审计和控制专业的贡献（所有相关活动合计报告的 CISA 学时限每年 20 个小时）
11. 指导他人获得认证（每年限 10 小时）

《CISA继续职业教育 (CPE) 政策》简体中文版下载：
http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Documents/CISA-CPE-ChinSimp.pdf


2015 ©谷安天下版权所有

# 3.CPE填报方法

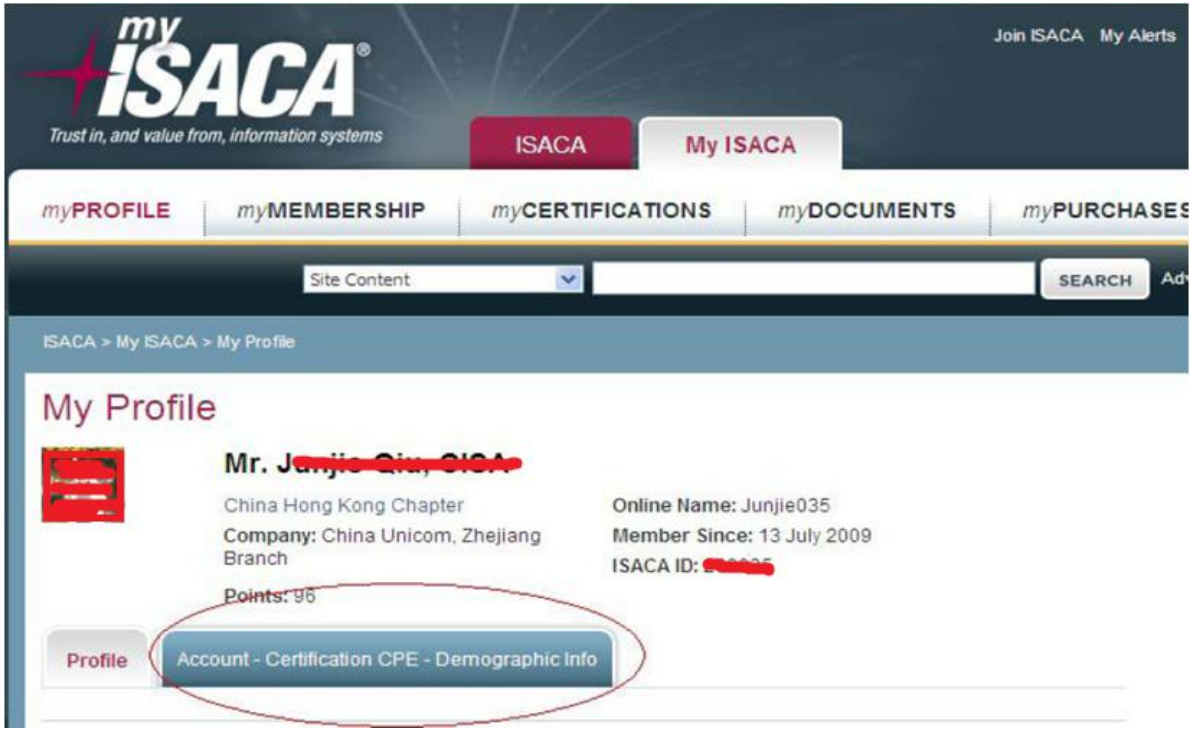
以下以ISACA的会员为例：

1、登陆ISACA网站； http://www.isaca.org 在下图右下角输入相应的“用户名”和“密码”

2015 ©谷安天下版权所有

# 3.CPE填报方法

2、进入“MY ISACA” 》 “MY PROFILE”




3、点击上图红圈内的菜单项： “ACCOUNT-CERTIFICATION CPE-DEMOGRAPHIC INFO”

2015 ©谷安天下版权所有

# 3.CPE填报方法

4、把页面拉到最下面,看到下图:

| CISA | |
|---|---|
| Cycle Year 1 | 2011 |
| Year 1 CPEs Needed | 20.00 |
| Cycle Year 2 | 2012 |
| Year 2 CPEs Needed | 20.00 |
| Cycle Year 3 | 2013 |
| Year 3 CPEs Needed | 20.00 |

Edit

5、然后点击红圈中按纽“EDIT” ，会显示下图的页面：

Profile | Account - Certification CPE - Demographic Info

EDIT this information by clicking the EDIT button at the bottom of the page.

The pre-populated information below is what ISACA currently has on file which may have been collected prior to your coming to this new ISACA web site. This information, and any additional information you provide, will be used as described in our Privacy Policy.

My Contact Information | My Demographic, Certification CPE and Other Information

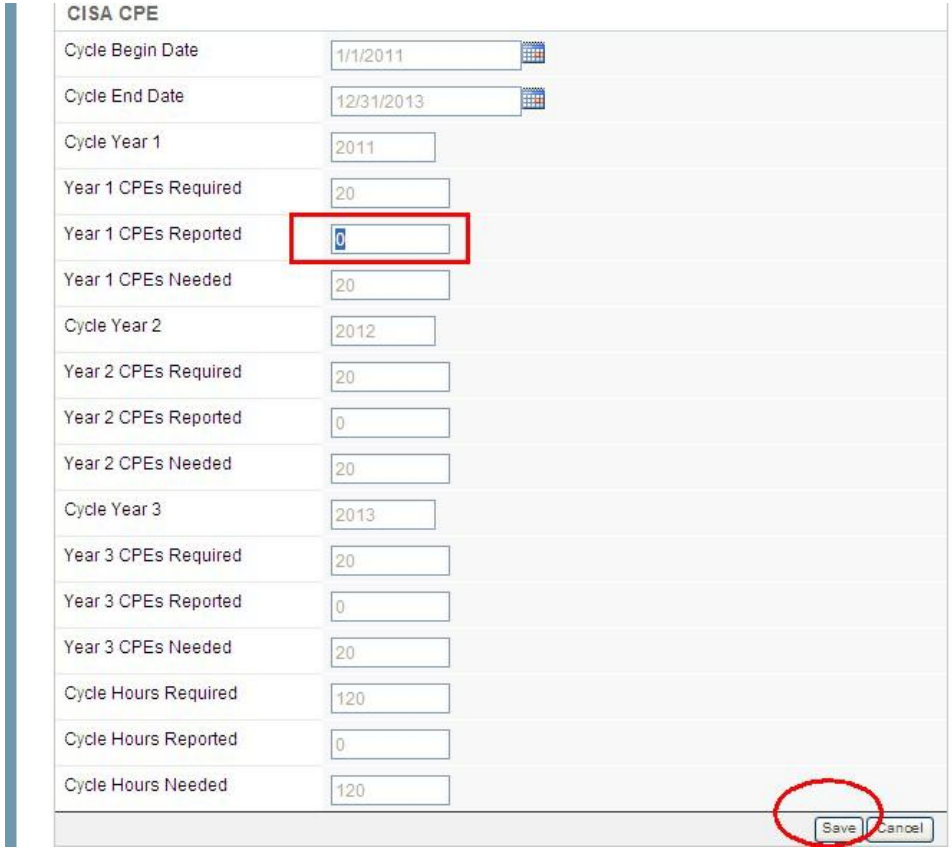
Contact Information

6、再点击上图红圈中的菜单“My Demographic, Certification CPE and Other Information”


2015 ©谷安天下版权所有

# 3.CPE填报方法

7、进入后，把页面拉到最后，显示下图：




8、分别在红框中填入本年的CPE值，确定后，点击右下角的红圈中的“SAVE”按纽，就OK ！建议到12月再进行填写，当然如果截止当前已满足最低CPE要求，可以直接填报。以后每年均按上述方法处理。


2015 ©谷安天下版权所有

# 谢谢观看！

www.gooann.com

2015 ©谷安天下版权所有