CISA Certification Application

Applicants who Passed CISA Exam 2016 and Later

Please use Adobe Reader when filling out this application electronically.

APPLICANT DETAILS

FULL NAME: _____ ISACA ID: _____

EMAIL: _____ PHONE NUMBER: _____

STEP 1. PASS EXAM

CISA applicants are required to have passed the CISA exam in the last five years.
If you have not yet passed the CISA exam, you can register online at www.isaca.org/examreg

EXAM PASS YEAR: _____

STEP 2. REPORT WORK EXPERIENCE

To qualify for CISA, you must have 5 years of information systems auditing, control, assurance or security work experience within the past 10 years of the application submission date. This experience must be in at least one CISA Job Practice Domain Area, available to view on page V-2. If you do not meet the 5-year experience requirements within Section 2A, you may also opt to submit waivers for experience in section 2B and/or 2C (up to a maximum of 3 years).

Section A: Information Systems Audit, Control, Assurance or Security Work Experience *(required)*

Please list related work experience you are claiming below, beginning with your current or most recent position.
Do not leave dates blank. If you are currently employed, please use the current date for the End Date.

		Dates of Employment *(MM/YY)*		Duration of Experience performing CISA tasks		CISA Job Practice Domains *(check all that apply)*				
#	Company Name	Start Date	End Date	Years	Months	1	2	3	4	5
1										
2										
3										
4										

(minimum 2 years required) **SECTION A EXPERIENCE TOTAL:** _____

Section B: General Work Experience Waiver *(optional)*

To apply for a work experience waiver in general information systems or general audit work, please fill out the details below.
This experience can not have been earned during dates of employment already claimed in Section A. This is a 1-year waiver.

Type of Experience Waiver *(Select one if applicable)* ☐ General Audit ☐ General Information Systems

COMPANY: _____ START DATE: _____ END DATE: _____

(maximum 1 year) **SECTION B EXPERIENCE TOTAL:** _____

Section C: Education Experience Waivers *(optional)*

To apply for an education experience waiver, check the appropriate box below and enter the school information, if applicable.
**Attach a copy of your degree, transcript or letter from your college or university with the application.*
***Attach a copy of your CIMA or ACCA certificate with the application.*

- ☐ 1-year waiver for an associate degree
- ☐ 2-year waiver for a bachelor's, master's or doctorate degree in any field of study
- ☐ 3-year waiver for a master's degree in Information Systems or a related field *
- ☐ 2-year waiver for CIMA – Chartered Institute of Management Accountants, full certification **
- ☐ 2-year waiver for ACCA member status from the Association of Chartered Certified Accountants **

SCHOOL NAME: _____ FIELD OF STUDY: _____

(maximum 3 years) **SECTION C EXPERIENCE TOTAL:** _____

Section D: Experience Total

Total experience from Sections A, B & C must be **5** years or more to apply for CISA certification

(Section A + Section B + Section C) **TOTAL EXPERIENCE:** _____

CISA Certification Application

Applicants who Passed CISA Exam 2016 and Later

Please use Adobe Reader when filling out this application electronically.

STEP 3. VERIFY WORK EXPERIENCE

Using the Experience Verification Form (pages V-1 & V-2 of this application), please ask an employer to verify all experience in Step 2. If more than one verifier is needed, you can obtain additional experience verification forms here: *www.isaca.org/cisaapp*. For a certificate or degree claimed in Section C, please submit a copy of the certificate, degree, or transcript.

STEP 4. SUBMIT APPLICATION PROCESSING PAYMENT

All applicants must pay a US $50.00 Application Processing Fee before the application can be fully processed. Payment can be made at: *www.isaca.org/cisapay*

STEP 5. REVIEW AND SIGN TERMS & CONDITIONS AGREEMENT

Continuing Professional Education (CPE) Policy
I hereby apply to ISACA for the Certified Information Systems Auditor (CISA) certification in accordance with and subject to the procedures and policies of ISACA. I have read and agree to the conditions set forth in the Application for Certification and the Continuing Professional Education (CPE) Policy in effect at the time of my application, covering the Certification process and CPE policy.

Code of Ethics
I agree: to provide proof of meeting the eligibility requirements; to permit ISACA to ask for clarification or further verification of all information submitted pursuant to the Application, including but not limited to directly contacting any verifying professional to confirm the information submitted; to comply with the requirements to attain and maintain the certification, including eligibility requirements carrying out the tasks of a CISA, compliance with ISACA's Code of Ethics, standards, and policies and the fulfillment of renewal requirements; to notify the ISACA certification department promptly if I am unable to comply with the certification requirements; to carry out the tasks of a CISA; to make claims regarding certification only with respect to the scope for which certification has been granted; and not use the CISA certificate or logos or marks in a misleading manner or contrary to ISACA guidelines.

Truth in Information
I understand and agree that my Certification application will be denied, and any credential granted me by ISACA will be revoked and forfeited in the event that any of the statements or answers provided by me in this application are false or in the event that I violate any of the examination rules or certification requirements. I understand that all certificates are owned by ISACA and if my certificate is granted and then revoked, I will destroy the certificate, discontinue its use and retract all claims of my entitlement to the Certification. I authorize ISACA to make any and all inquiries and investigations it deems necessary to verify my credentials and my professional standing.

3rd Party Information Sharing
I acknowledge that if I am granted the Certification, my 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 ISACA. Appeals undertaken by a Certification exam taker, Certification applicant or by a certified individual are undertaken at the discretion and cost of the examinee or applicant. By signing below, I authorize ISACA to disclose my Certification status. This contact information will be used to fulfill my Certification inquiries and requests.

Contact Policy
By signing below, I authorize ISACA to contact me at the address and numbers provided and that the information I provided is my own and is accurate. I authorize ISACA to release confidential Certification application and certification information if required by law or as described in ISACA's Privacy Policy. 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/privacy*

Usage Agreement
I hereby agree to hold ISACA, its officers, directors, examiners, employees, agents and those of its supporting organizations 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 re-delivery of such certificate. Notwithstanding the above, I understand and agree that any action arising out of or pertaining to this application must be brought in the Circuit Court of Cook County, Illinois, USA, and shall be governed by the laws of the State of Illinois, USA.

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.

APPLICANT SIGNATURE: _____ DATE: _____

STEP 6. SUBMIT APPLICATION

Please submit your application, additional verification forms (if needed) and any supporting document online at *https://support.isaca.org*

Select **Certifications & Certificate Programs** and **Submit an Application**.

Submitted applications take approximately two-to-three weeks to process. Upon approval, you will be notified via email. A certification packet, including a letter of approval, a CISA Certificate, and a metal CISA pin, will be sent to you via postal mail to the primary address in your ISACA Profile. Please allow four-to-eight weeks for delivery.

CISA Experience Verification Form

Applicants who Passed CISA Exam 2016 and Later

Please use Adobe Reader when filling out this application electronically.

APPLICANT DETAILS

APPLICANT NAME: _____ ISACA ID: _____

FORM INSTRUCTIONS

The applicant (named above) is applying for CISA certification through ISACA. ISACA requires the applicant's work experience to be independently verified by a supervisor or manager with whom they have worked. Verifiers cannot be immediate or extended family, nor can they work in the Human Resources department.

By completing this form, you are attesting to the applicant's work experience as noted on their attached application form (page A-1) and as described by the CISA Job Practice Domains and task statements (page V-2).

Please return this verification form to the applicant for their submission. For any questions, please contact ISACA at https://support.isaca.org or +1.847.660.5505.

VERIFIER DETAILS

VERIFIER NAME: _____

COMPANY NAME: _____ JOB TITLE: _____

EMAIL: _____ PHONE NUMBER: _____

VERIFIER QUESTIONS

1. I am attesting to the following work experience earned by the applicant as indicated on page A-1 (*check all that apply*):

☐ Section A: Company 1 ☐ Section A: Company 3
☐ Section A: Company 2 ☐ Section A: Company 4

2. I am attesting to the following waivers as indicated on page A-1, sections B and C *(check all that apply)*:

☐ Section B: Work Experience Waiver ☐ Section C: Educational Degree

3. I am attesting to the applicant's work experience during the following duration:

START DATE: _____ END DATE: _____

4. I have functioned in the following role(s) to the applicant (*must check at least one to qualify*):

☐ Supervisor ☐ Manager ☐ Colleague ☐ Client

5. If I am attesting to any experience earned in Section A, I can attest that the applicant has completed any or all tasks in the Job Practice Domain(s) indicated on page A-1 and V-2, and that they are correct to the best of my knowledge.

☐ Yes ☐ No

VERIFIER AGREEMENT

I hereby confirm that the information on page V-1 and V-2 is correct to the best of my knowledge and there is no reason this applicant should not be certified as an information systems auditor. I am also willing, if required, to answer questions from ISACA about the above information.

VERIFIER SIGNATURE: _____ DATE: _____

CISA Experience Verification Form

Applicants who Passed CISA Exam 2016 and Later

Please use Adobe Reader when filling out this application electronically.

JOB PRACTICE DOMAIN INSTRUCTIONS

Applicant is required to check any domain in which a minimum of one task has been completed. At least one checked domain is required for certification.

☐ DOMAIN 1 - The Process of Auditing Information Systems

Provide audit services in accordance with IS audit standards to assist the organization in protecting and controlling information systems.

Task Statements:

- Execute a risk-based IS audit strategy in compliance with IS audit standards to ensure that key risk areas are audited.
- Plan specific audits to determine whether information systems are protected, controlled and provide value to the organization.
- Communicate audit results and make recommendations to key stakeholders through meetings and audit reports to promote change when necessary.
- Conduct audit follow-ups to determine whether appropriate actions have been taken by management in a timely manner.
- Conduct audits in accordance with IS audit standards to achieve planned audit objectives.

☐ 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.

Task Statements:

- Evaluate the IT strategy, including 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 effectiveness of the IT governance structure to determine whether IT decisions, directions and performance support 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 risk management practices to determine whether the organization's IT-related risk is identified, assessed, monitored, reported and managed.
- Evaluate IT management and monitoring of controls (e.g., continuous monitoring, quality assurance [QA]) for compliance with the organization's policies, standards and procedures.
- Evaluate the organization's IT policies, standards and procedures, and the processes for their development, approval, release/publishing, implementation and maintenance to determine whether they support the IT strategy and comply with regulatory and legal requirements.
- Evaluate IT resource management, including investment, prioritization, allocation and use, for alignment with the organization's strategies and objectives.
- Evaluate IT portfolio management, including investment, prioritization and allocation, for alignment with the organization's strategies and objectives.
- Evaluate monitoring and reporting of IT key performance indicators (KPIs) to determine whether management receives sufficient and timely information.
- Evaluate the organization's business continuity plan (BCP), including alignment of the IT disaster recovery plan (DRP) with the BCP, 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.

Task Statements:

- Evaluate the business case for the proposed investments in information systems acquisition, development, maintenance and subsequent retirement to determine whether the business case meets business objectives.
- Evaluate IT supplier selection and contract management processes to ensure that the organization's service levels and requisite controls are met.
- Evaluate the project management framework and controls to determine whether business requirements are achieved in a cost-effective manner while managing risk to the organization.
- Conduct postimplementation reviews of systems to determine whether project deliverables, controls and the organization's requirements are met.
- Conduct reviews to determine whether a project is progressing in accordance with project plans, is adequately supported by documentation, and has timely and accurate status reporting.
- 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 the organization's requirements are met.

☐ DOMAIN 4 - Information Systems Operations, Maintenance and Service Management

Provide assurance that the practices for the acquisition, development, testing and implementation of information systems meet the organization's strategies and objectives.

Task Statements:

- Evaluate the IT service management framework and practices (internal or third party) to determine whether the controls and service levels expected by the organization are being adhered to and whether strategic objectives are met.
- Conduct periodic reviews of information systems to determine whether they continue to meet the organization's objectives within the enterprise architecture (EA).
- Evaluate IT operations (e.g., job scheduling, configuration management, capacity and performance management) to determine whether they are controlled effectively and continue to support the organization's objectives.
- Evaluate IT maintenance (patches, upgrades) to determine whether they are controlled effectively and continue to support the organization's objectives.
- Evaluate database management practices to determine the integrity and optimization of databases.
- Evaluate data quality and life cycle management to determine whether they continue to meet strategic objectives.
- Evaluate problem and incident management practices to determine whether problems and incidents are prevented, detected, analyzed, reported and resolved in a timely manner to support the organization´s objectives.
- Evaluate change and release management practices to determine whether changes made to systems and applications are adequately controlled and documented.
- Evaluate end-user computing to determine whether the processes are effectively controlled and support the organization's objectives.
- Evaluate IT continuity and resilience (backups/restores, disaster recovery plan [DRP]) to determine whether they are controlled effectively and continue to support the organization's objectives.

☐ DOMAIN 5 – Protection of Information Assets

Provide assurance that the organization's policies, standards, procedures and controls ensure the confidentiality, integrity and availability of information assets.

Task Statements:

- Evaluate the information security and privacy policies, standards and procedures for completeness, alignment with generally accepted practices and compliance with applicable external requirements.
- Evaluate the design, implementation, maintenance, monitoring and reporting of physical and environmental controls to determine whether information assets are adequately safeguarded.
- Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives.
- Evaluate the design, implementation, maintenance, monitoring and reporting 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 processes and procedures used to store, retrieve, transport and dispose of assets to determine whether information assets are adequately safeguarded.