
CISA[®]

Certified Information Systems Auditor[™]

Application for Certification



Application for CISA Certification

Requirements to Become a Certified Information Systems Auditor

To become a Certified Information Systems Auditor (CISA), an applicant must:

1. *Score a passing grade on the CISA exam.* A passing score on the CISA exam, without completing the required work experience as outlined below, will only be valid for five years. If the applicant does not meet the CISA certification requirements within the five year period, the passing score will be voided.
2. *Submit verified evidence of five years work experience in the fields of Information Systems Auditing, Control or Security.* Work experience must be gained within the ten year period preceding the application date for certification or within five years from the date of initially passing the exam.

Substitutions and waivers of such experience, to a maximum of 3 years, may be obtained as follows:

- A maximum of one year of information systems OR one year of non-IS auditing experience can be substituted for one year of information systems auditing, control, or security experience;
- 60 to 120 completed university semester credit hours (the equivalent of a two-year or four-year degree), not limited by the ten year preceding restriction, can be substituted for one or two years, respectively, of information systems auditing, control or security experience. Even if multiple degrees have been earned, a maximum of 2 years can be claimed.
- A bachelor's or master's degree from a university that enforces the ISACA sponsored Model Curricula can be substituted for one year of information systems auditing, control or security experience. To view a list of these schools, please visit www.isaca.org/modeluniversities. This option cannot be used if three years of experience substitution and educational waiver have already been claimed; and

Exception: Two years as a full-time university instructor in a related field (e.g.; computer science, accounting, information systems auditing) can be substituted for every one year of information systems auditing, control or security experience.

As an example, at a minimum (assuming a two-year waiver of experience by substituting 120 university credits) an applicant must have three years of actual work experience. This experience can be completed by:

- three years information systems audit, control, or security experience;

OR

- two years information systems audit, control, or security experience and one full year non-IS audit or information systems experience or two years as a full-time university instructor.

3. *Agree to abide by the ISACA Code of Professional Ethics.*
4. *Agree to abide with Information Systems Standards as adopted by ISACA, which can be viewed at www.isaca.org/standards.*
5. *Agree to abide by the CISA Continuing Education Policy, which can be viewed at www.isaca.org/cisacpepolicy.*

Application for CISA Certification

ISACA Code of Professional Ethics

ISACA sets forth this Code of Professional Ethics to guide the professional and personal conduct of members of the association and/or its certification holders.

CISAs shall:

1. Support the implementation of, and encourage compliance with, appropriate standards, procedures and controls for information systems
2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices
3. Serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession
4. Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties
5. Maintain competency in their respective fields and agree to undertake only those activities, that they can reasonably expect to complete with professional competence
6. Inform appropriate parties of the results of work performed, revealing all significant facts known to them
7. Support the professional education of stakeholders in enhancing their understanding of information systems security and control

Failure to comply with this Code of Professional Ethics can result in an investigation into a member's and/or certification holder's conduct and, ultimately, in disciplinary measures.

Application for CISA Certification

Instructions for Completion of Forms

1. Complete and return both sides of the Application for CISA Certification. Be sure to sign and date the application. On page 2 complete:

SECTION A – INFORMATION SYSTEMS AUDIT, CONTROL OR SECURITY EXPERIENCE — For each employer (starting with the most current), enter the:

- Company name
- Dates of employment in IS auditing, control or security
- The type of work experience (job process/content areas), by checking the appropriate boxes and entering the total number of years of information systems auditing, control or security experience with each employer. Job process/content areas are defined on page 4 of the application form.

SECTION B – EXPERIENCE SUBSTITUTION — If substituting other audit experience (such as financial or operational auditing) or other types of information systems work experience (such as application programming or operations), there is a maximum limit of one FULL year for the audit or information systems work experience. If substituting full-time university instructor experience in a related field (e.g.; information systems, accounting, information systems auditing) you must have two FULL years experience for each year of experience substitution. There is no limit on the number of year's experience substitution that may be claimed as a university instructor.

No credit will be given for a partial year's experience.

SECTION C – EDUCATIONAL EXPERIENCE WAIVER — Indicate an experience waiver for educational purposes by checking the appropriate box. To confirm your degree status, include an original transcript or letter from your college or university with your application. To reduce processing time, please do not send the transcript separately.

SECTION D – SUMMARY OF EXPERIENCE REQUIREMENTS — Record the totals from sections A-C above. The line titled "Total Work Experience" should be the total number of years spent working in an information systems auditing, control or security function, plus any experience substitution and waivers. A minimum of five years is required for eligibility as a CISA.

No more than three years of experience substitution or educational waivers can be used towards your five year experience requirement, with the exception of those claiming the experience substitution of a university instructor.

2. Complete the top portion of the Verification of Work Experience form. Give the form to the person(s) verifying your work experience; include the descriptions of information systems auditing, control or security job practice areas, on page 4, and a copy of your completed application. This person should be your immediate supervisor or a person of higher rank within the organization. If this person is not qualified or willing to verify all required experience listed in Section A, previous employers must also be asked to complete this form. Please note that if your length of employment with your most recent company is less than three months, verification of work experience is required from previous employers. To reduce processing time, please send the verification forms with your application.
3. In order for your application to be efficiently processed, please collect all supporting documentation (verification of work experience form(s) and any applicable university transcript or letter) and mail your completed Application for CISA Certification to:

Certification Coordinator
ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008-3124 USA

E-mail: certification@isaca.org

Telephone Number: +1.847.253.1545

Fax Number: +1.847.253.1443

NOTE: Please allow approximately eight weeks for the processing of your completed Application for CISA Certification. Upon approval, you will receive a certificate package via mail containing a letter of certification, your CISA certificate and the CISA Continuing Education Policy.

Application for CISA Certification

Name: _____ Exam ID _____
First Middle Initial Last/Family

Maiden Name or Former Name(s) _____ Birth Date: _____ / _____ / _____
M D Y

Preferred Mailing Address: Home () Business () Month and Year of Exam _____

Home Address: _____

City: _____ State/Country: _____ Zip/Postal Code: _____

Home Telephone () _____ Email _____

Present Employer: _____

Your Job Title: _____

Business Name: _____

Business Address: _____

City: _____ State/Country: _____ Zip/Postal Code: _____

Business Telephone () _____ Fax () _____

E-mail _____

Immediate Supervisor: _____ Name _____ Title _____

Person(s) you have requested to verify your work experience (a work experience verification form must be submitted for each person listed):

1. Name _____ Title _____
Company _____ Tel. No. _____
2. Name _____ Title _____
Company _____ Tel. No. _____
3. Name _____ Title _____
Company _____ Tel. No. _____

ISACA reserves the right to contact your verifiers for confirmation of work experience.

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 authorize ISACA to make whatever inquiries and investigations it deems necessary to verify my credentials and my professional standing. I understand that this application and any information or material received or generated by ISACA in connection with my Certification will be kept confidential and will not be released unless I have authorized such release or such release is required by law. However, the fact that I am or am not, or have or have not been, Certified is a matter of public record and may be disclosed. Finally, I allow ISACA to use information from my application for the purpose of statistical analysis, provided that my personal identification with that information has been deleted.

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

Signature

Date

Application for CISA Certification

Work Experience Detail

Exam ID _____ Name _____

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).

Company Name	Dates of Employment in IS Audit, Control or Security		Job Practice Areas Check All That Apply (see page 4)						Number of	
	MM/YY	MM/YY	1	2	3	4	5	6	Years	Months
		To								
		To								
		To								
		To								
Total number of years IS auditing, control or security experience (round down to whole year)										

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		Type of Experience	Number of Years of Substitution
	MM/YY	MM/YY		
		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 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.....
 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 or 2 in the box as appropriate and complete Section C above.....
- TOTAL WORK EXPERIENCE** — add boxes 1, 2 and 3
(must total five years or more to apply for CISA certification).....

Application for CISA Certification

Verification of Work Experience

Exam ID _____

I, _____, am applying for certification through ISACA as a
(Printed Name)

Certified Information Systems Auditor. My work experience must be independently verified by my current (and possibly previous) employer(s). 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 and returning it to me for my submission. If you have any questions concerning this form, please direct them to *certification@isaca.org*. or +1.847.253.1545, x772.

Thank you

Applicant's Signature

Date

Employer's Verification

Please answer all five questions and sign and date the form.

Supervisor's Name: _____

CURRENT CONTACT INFORMATION

Company Name: _____

Job Title: _____

Company Telephone Number: _____ Company E-mail: _____

Name of company being verified on page 2: _____

1. Have you functioned in a supervisory position to the applicant such that you can verify his/her work experience? Yes No
2. How long have you known the applicant? _____ years
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? Yes No
4. Are you qualified and willing to verify the applicant's work experience prior to his/her affiliation with your company/organization? Yes No N/A
5. Is there any reason you believe this applicant should not be certified as an information systems auditor? Yes No

Supervisor's Signature

Date

Application for CISA Certification

Description of CISA Job Practice Areas

1. The IS Audit Process

Provide IS audit services in accordance with IS audit standards, guidelines and best practices to assist the organization in ensuring that its information technology and business systems are protected and controlled.

Tasks

- Develop and implement a risk-based IS audit strategy for the organization in compliance with IS audit standards, guidelines and best practices.
- Plan specific audits to ensure that IT and business systems are protected and controlled.
- Conduct audits in accordance with IS audit standards, guidelines and best practices to meet planned audit objectives.
- Communicate emerging issues, potential risks and audit results to key stakeholders.
- Advise on the implementation of risk management and control practices within the organization, while maintaining independence.

2. IT Governance

Provide assurance that the organization has the structure, policies, accountability, mechanisms and monitoring practices in place to achieve the requirements of corporate governance of IT.

Tasks

- 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 the IT organizational structure and human resources (personnel) management to ensure that they support the organization's strategies and objectives.
- Evaluate the IT strategy and the process for its development, approval, implementation and maintenance to ensure that it supports the organization's strategies and objectives.
- Evaluate the organization's IT policies, standards and procedures and the processes for their development, approval, implementation and maintenance to ensure that they support the IT strategy and comply with regulatory and legal requirements.
- Evaluate management practices to ensure compliance with the organization's IT strategy, policies, standard and procedures.
- Evaluate IT resource investment, use and allocation practices to ensure alignment with the organization's strategies and objectives.
- Evaluate IT contracting strategies and policies and contract management practices to ensure that they support the organization's strategies and objectives.
- Evaluate risk management practices to ensure that the organization's IT-related risks are properly managed.
- Evaluate monitoring and assurance practices to ensure that the board and executive management receive sufficient and timely information about IT performance.

3. Systems and Infrastructure Life Cycle Management

Provide assurance that the management practices for the development/acquisition, testing, implementation, maintenance and disposal of systems and infrastructure will meet the organization's objectives.

Tasks

- Evaluate the business case for the proposed system development/acquisition to ensure that it meets the organization's business goals.
- Evaluate the project management framework and project governance practices to ensure that business objectives are achieved in a cost-effective manner, while managing risks to the organization.
- Perform reviews to ensure that a project is progressing in accordance with project plans, is adequately supported by documentation and its status reporting is accurate.
- Evaluate proposed control mechanisms for systems and/or infrastructure during specification, development/acquisition and testing to ensure that they will provide safeguards and comply with the organization's policies and other requirements.
- Evaluate the processes by which systems and/or infrastructure are developed/acquired and tested to ensure that the deliverables meet the organization's objectives.
- Evaluate the readiness of the system and/or infrastructure for implementation and migration into production.
- Perform postimplementation review of systems and/or infrastructure to ensure that they meet the organization's objectives and are subject to effective internal control.
- Perform periodic reviews of systems and/or infrastructure to ensure that they continue to meet the organization's objectives and are subject to effective internal control.
- Evaluate the process by which systems and/or infrastructure are maintained to ensure the continued support of the organization's objectives and that the systems and/or infrastructure are subject to effective internal control.
- Evaluate the process by which systems and/or infrastructure are disposed of to ensure that they comply with the organization's policies and procedures.

4. IT Service Delivery and Support

Provide assurance that the IT service management practices will ensure the delivery of the level of services required to meet the organization's objectives.

Tasks

- Evaluate service-level management practices to ensure that the level of service from internal and external service providers is defined and managed.
- Evaluate operations management to ensure that IT support functions effectively meet business needs.
- Evaluate data administration practices to ensure the integrity and optimization of databases.
- Evaluate the use of capacity and performance monitoring tools and techniques to ensure that IT services meet the organization's objectives.
- Evaluate change, configuration and release management practices to ensure that changes made to the organization's production environment are adequately controlled and documented.
- Evaluate problem and incident management practices to ensure that incidents, problems and errors are recorded, analyzed and resolved in a timely manner.
- Evaluate the functionality of the IT infrastructure (e.g., network components, hardware and system software) to ensure that it supports the organization's objectives.

5. Protection of Information Assets

Provide assurance that the security architecture (policies, standards, procedures and controls) ensures the confidentiality, integrity and availability of information assets.

Tasks

- Evaluate the design, implementation and monitoring of logical access controls to ensure the confidentiality, integrity, availability and authorized use of information assets.
- Evaluate network infrastructure security to ensure confidentiality, integrity, availability and authorized use of the network and the information transmitted.
- Evaluate the design, implementation and monitoring of environmental controls to prevent or minimize loss.
- Evaluate the design, implementation and monitoring of physical access controls to ensure that information assets are adequately safeguarded.
- Evaluate the processes and procedures used to store, retrieve, transport and dispose of confidential information assets.

6. Business Continuity and Disaster Recovery

Provide assurance that, in the event of a disruption, the business continuity and disaster recovery processes will ensure the timely resumption of IT services, while minimizing the business impact.

Tasks

- Evaluate the adequacy of backup and restore provisions to ensure the availability of information required to resume processing.
- Evaluate the organization's disaster recovery plan to ensure that it enables the recovery of IT processing capabilities in the event of a disaster.
- Evaluate the organization's business continuity plan to ensure its ability to continue essential business operations during the period of an IT disruption.