



**Certified Information
Systems Auditor[®]**

An ISACA[®] Certification

Application for CISA Certification

**For individuals who passed
a CISA exam administered
in 2016 and Later**



Trust in, and value from, information systems

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 apply or meet the CISA certification requirements within the five year period, the passing score will be voided.

Important Note: Your completed CISA application for certification must be submitted within 5 years from the date of initially passing the examination. Retaking and re-passing the examination will be required if the (completed) application for certification is not submitted within five years from the passing date of the examination.

2. Submit payment for the CISA application processing fee of US \$50 online at www.isaca.org/cisapay.
3. Submit verified evidence of *five years work experience in the fields of Information Systems Auditing, Control, Assurance 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, assurance 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, assurance 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
- A master's degree in information security or information technology from an accredited university can be substituted for one year of experience.
- Two year waiver for CIMA (Chartered Institute of Management Accountants) full certification. No waiver is provided for the CIMA Certificate in Business Accounting or the CIMA Advanced Diploma in Management Accounting, both earned en route to becoming fully qualified. (The CIMA full certification waiver is in lieu of the 2-year CISA waiver for a bachelor's degree. Those individuals who have a 2-year CISA waiver for their bachelor's degree cannot also claim the CIMA waiver.) Must provide a copy of CIMA certification as verification.
- Two year waiver for ACCA member status from the Association of Chartered Certified Accountants. Must provide copy of ACCA certification as verification. (Those individuals who have a 2-year CISA waiver for their bachelor's degree cannot also claim the ACCA waiver.)

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, assurance, or security experience;

OR

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

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

Instructions for Completing and Submitting Your Application for CISA Certification

Carefully follow the instructions to complete your application. Be sure to complete all appropriate sections and sign your application. Incomplete or unsigned applications will stall the review process.

1. **Application Page A-1.** Complete with your details on page A-1. Read and review acknowledgement. Print and sign your name with a hand written signature and enter date on form at bottom of page. True digital signatures (those authentically validated) are acceptable. Signatures cut and pasted into the document, imported in a word text box or computer keyed/typed in are **NOT** acceptable.
2. **Payment.** Submit payment for the CISA application processing fee of US \$50 online at www.isaca.org/cisapay.
3. **Application Page A-2.**

SECTION A – INFORMATION SYSTEMS AUDIT, CONTROL, ASSURANCE OR SECURITY EXPERIENCE —

For each employer/company (starting with the most current), enter the:

- **Name of Employer/Company.** Enter your employer/company name.
- **Dates of Employment.** Date range (month and year) of employment with that employer/company. Do not leave dates blank. If currently employed, include a date or current, now, present, etc.
- **Duration of Experience.** Enter number of years and months, by employer and in total, performing IS auditing, control, assurance or security service.

Work experience must be gained within the ten year period preceding the application date for certification or within 5 years from the date of initially passing the exam. Work experience greater than 10 years cannot be claimed on your application.

SECTION B – EXPERIENCE SUBSTITUTION — Non-IS audit/information systems: 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. Partial years do not apply. **University Instructor:** 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 university instructor 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 educational experience waiver by checking the appropriate box. To confirm your degree status, include a copy of your transcript, degree, or letter from your college or university with your application or your verifier can verify this for you. If your verifier has knowledge of your Bachelor's degree and is willing to verify this for you, he may do so by answering the corresponding question on the verification form.

- For those claiming a CIMA or ACCA waiver, a copy of the certification is required for verification
- Those claiming a 3 year waiver for the Master's degree in information security or information technology, a copy of the degree or transcript is required.

Note that with the exception of University Professor, between experience and educational substitutions no more than 3 years may be claimed as waivers/substitutions.

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, assurance or security function, plus any experience substitution and waivers. A minimum of five years is required to qualify for CISA Certification.

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

4. **Application Pages V-1 & V-2.** Complete the top portion on the Verification of Work Experience forms (pages V-1 and V-2) and check the boxes on page V-2 of the verification form that indicate the tasks you performed that are being verified by each verifier. If your verifier is only verifying experience listed in Section B Experience Substitution, only page V-1 is required. Give the form to each person(s) verifying your work experience; and a copy of your completed application. This person should be your immediate supervisor, a person of higher rank within the organization or a person with direct first hand knowledge of your work. The individual verifying the work experience must be an independent verifier and not of any relation to the applicant nor can the applicant verify his/her own work. Human Resource (HR) verifications for work experience are not acceptable unless applicant directly reports to HR function. Letters of Employment are not acceptable as verification for your work experience. If one person cannot verify all required experience for you to become a CISA, previous employers must be asked to complete this form. If you currently or once worked as an independent consultant, you can use a knowledgeable client or an individual certified as a CISA or CISM to perform this role. Two copies of the form are included. If additional copies are required, photocopy the forms. **Verification of Work Experience form page V-1 must be signed and dated by your verifier and submitted along with your application.** To reduce processing time, please send the completed verification forms with your application.

5. **Application Submittal.** In order for your application to be efficiently processed, please collect all supporting documentation (verification of work experience form(s) and any applicable university degree, transcript or letter) and submit your completed Application for CISA Certification via fax, email or mail to:

Certification Coordinator ISACA
3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3124 USA
E-mail: application@isaca.org • Telephone Number: +1.847.660.5660
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 and your CISA certificate.

Frequently Missed Items

Incomplete applications stall the process. In addition to the review of your application, you may want to review the items below to ensure that you have these areas covered in your application.

- Applicant has signed/dated pages A-1 and V-1 of the application in ink?
- Do not leave dates of employment blank. If currently employed, include a date or current, now, present, etc.
- Employment dates do not overlap in any section on page A-2. Years of experience used in Section A cannot be used again in Section B.
- Verifier has answered all questions on page V-1 and signed/dated at the bottom of page V-1.
- Applicant and verification signatures on forms must be manually handwritten or digital (authentically validated) signatures. Signatures cut and pasted into the documents, imported in a word text box or computer keyed/typed in are not acceptable.
- Check to confirm that the verifier listed all the employer/companies that he/she is verifying in the box provided on page V-1.
- The work experience used in your application must be gained within the ten year period preceding the application date for certification or within 5 years from the date of initially passing the exam.
- USD\$50 application processing fee has been paid online at www.isaca.org/cisapay.

Follow Your Application Progress

Once you submit your application, you can follow the progress online at MyISACA > MyCertifications page of the web site.

If status shows:	Comment:
Application Link and Last Date to Apply for Certification	Application has not been received or logged into the record.
Unreviewed	Application has been received but not yet sent through for review.
Complete Under Review	Application is going through the review process. An email message will be sent if any additional information/documents are needed to complete your application.
Complete Pending Audit	Application was selected for a random verifier audit and ISACA is awaiting response from the verifier.
Incomplete	The application is incomplete or has missing documents. Email message is sent to the applicant with details on the incomplete or missing items.
Approved	Application has been tentatively approved and will be certified in the next grouping or certifying batch for that certification unless selected for the random verification audit.

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

Maiden Name or Former Name(s) _____

Preferred Mailing Address: Home () Business ()

Home Address: _____

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

Home Telephone () _____ Email _____

Present Employer/Company Name: _____

Your Job Title: _____

Business Name: _____

Business Address: _____

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

Business Telephone () _____ Fax () _____

E-mail _____

Immediate Supervisor: _____
Name Title

I hereby apply to Information Systems Audit and Control Association, Inc. (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. 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. 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. 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 certification@isaca.org. 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. 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.

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 redelivery 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.

Name _____

Signature _____

Date _____

Work Experience Detail

Exam ID _____ Name _____

SECTION A. INFORMATION SYSTEMS AUDIT, CONTROL, ASSURANCE OR SECURITY EXPERIENCE — List your most recent experience first. A candidate must have a **minimum** of two years of IS audit, control, assurance 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). Work experience must be gained within the ten year period preceding the application date for certification or within 5 years from the date of initially passing the exam. Do not leave dates blank. If currently employed, include a date or current, now, present, etc.

Employer/Company Name	Dates of Employment		Duration of Experience in IS Audit, Control or Security	
	MM/YY	MM/YY	Years	Months
		To		
		To		
		To		
		To		
Total number of years IS auditing, control, assurance or security experience (round down to whole year)				

SECTION B. EXPERIENCE SUBSTITUTION — A maximum of 1 year IS auditing, control, assurance or security experience may be substituted with either one FULL year of auditing experience OR one FULL year of information systems experience. No credit is given for a partial years experience. Experience used in Section A cannot be repeated in Section B.

Company Name Non-IS audit/information systems:	Dates of Employment		Type of Experience	Number of Years of Substitution
	MM/YY	MM/YY		
		To	Non-IS Audit	
		To	Information Systems	
University Name**:				
		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.

SECTION C. EDUCATIONAL EXPERIENCE WAIVER — If you are applying for any experience waivers, please include information on your degree below. Check the appropriate box. To confirm your degree status, include with your application a copy of your degree, transcript or letter from your college or university.

University Name	Educational Degree Awarded	Educational Field of Study

Educational Experience Waiver (Check one which applies to the waiver you are claiming.) *Copy of degree required.

- One year substitution waiver for a 2-Year university degree or equivalent 60 semester credit hours.
- Two years substitution waiver for a Bachelor's, Master's, Ph.D. or equivalent 120 semester credit hours.
- Three years substitution waiver for a Bachelor's degree PLUS Master's in Information Security or Information Technology.*
- Three years substitution waiver for a Bachelor's or Master's degree from a university that enforces the ISACA sponsored Model Curricula.*

OTHER WAIVERS (Must submit certificate as proof for waiver.)

- Two year educational waiver for CIMA – Chartered Institute of Management Accountants, full certification.
- Two year educational waiver for ACCA member status from the Association of Chartered Certified Accountants.

SECTION D. SUMMARY OF EXPERIENCE REQUIREMENTS

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

Verification of Work Experience (page 1 of 2)

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/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 applicant 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, assurance or security work experience as noted on my application form attached and as described by CISA job practice area and task statements (see page V-2). Please return the complete form to me for my submission to ISACA. If you have any questions concerning this form, please direct them to *support.isaca.org*. or +1.847.660.5660.

Thank you

Applicant's Signature

Date

Employer's Verification

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

Verifier's Name: _____

Company Name: _____

Job Title: _____

Address: _____

STREET

CITY

STATE/PROVINCE/COUNTRY

POSTAL CODE

Company Telephone Number: _____ Company E-mail: _____

I am attesting to/verifying the employment experience listed on page A-2. Enter employer/company name(s). List all that apply to this verification. _____

1. Have you functioned in a supervisory position to the applicant or other related position and can verify the experience as listed on page A-2? Yes No
If no, please explain what qualifies you to verify this information? _____
2. I can attest to the duration of the applicant's work experience on this application with my organization. Yes No N/A
If no, I attest to experience from _____ to _____.
3. I can attest to the duration of the applicant's work experience on this application prior to his/her affiliation with my organization. Yes No N/A
4. I can attest that the applicant has performed the tasks in the CISA Job Practice Areas as checked off on verification form page V-2. Yes No
5. Are you qualified and willing to verify the applicant's educational experience waiver(s) claimed? Yes No N/A
6. Is there any reason you believe this applicant **SHOULD NOT** be certified as an information systems auditor? Yes No

Verifier's Signature

Date

Verification of Work Experience (page 2 of 2)

Exam ID _____

Applicant Name: _____

Verifier Name: _____

Applicant required to indicate with an (x) in each box the task they performed to be confirmed by the verifier.

Description of CISA Job Practice Areas

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.
- Conduct audits in accordance with IS audit standards to achieve planned audit objectives.
- 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.

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 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 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 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 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.
- Conduct postimplementation reviews of systems 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 processes for information systems operations, maintenance and service management 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 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.
- Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives.

Verification of Work Experience (page 1 of 2)

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/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 applicant 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, assurance or security work experience as noted on my application form attached and as described by CISA job practice area and task statements (see page V-2). Please return the complete form to me for my submission to ISACA. If you have any questions concerning this form, please direct them to *support.isaca.org*. or +1.847.660.5660.

Thank you

Applicant's Signature

Date

Employer's Verification

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

Verifier's Name: _____

Company Name: _____

Job Title: _____

Address: _____

STREET

CITY

STATE/PROVINCE/COUNTRY

POSTAL CODE

Company Telephone Number: _____ Company E-mail: _____

I am attesting to/verifying the employment experience listed on page A-2. Enter employer/company name(s). List all that apply to this verification. _____

1. Have you functioned in a supervisory position to the applicant or other related position and can verify the experience as listed on page A-2? Yes No
If no, please explain what qualifies you to verify this information? _____
2. I can attest to the duration of the applicant's work experience on this application with my organization. Yes No N/A
If no, I attest to experience from _____ to _____.
3. I can attest to the duration of the applicant's work experience on this application prior to his/her affiliation with my organization. Yes No N/A
4. I can attest that the applicant has performed the tasks in the CISA Job Practice Areas as checked off on verification form page V-2. Yes No
5. Are you qualified and willing to verify the applicant's educational experience waiver(s) claimed? Yes No N/A
6. Is there any reason you believe this applicant **SHOULD NOT** be certified as an information systems auditor? Yes No

Verifier's Signature

Date

Verification of Work Experience (page 2 of 2)

Exam ID _____

Applicant Name: _____

Verifier Name: _____

Applicant required to indicate with an (x) in each box the task they performed to be confirmed by the verifier.

Description of CISA Job Practice Areas

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.
- Conduct audits in accordance with IS audit standards to achieve planned audit objectives.
- 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.

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 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 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 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 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.
- Conduct postimplementation reviews of systems 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 processes for information systems operations, maintenance and service management 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 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.
- Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives.



Telephone: +1.847.253.1545

Fax: +1.847.253.1443

E-mail: *application@isaca.org*

Web site: *www.isaca.org*