CISA®

Certified Information Systems Auditor®

An ISACA® Certification

Application for CISA Certification

✦ISACA®

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.*

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.*

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.

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. The ISACA Code of Professional Ethics can be viewed online at *www.isaca.org/ethics.*

Instructions for Completing and Submitting Your Application and Documentation

Carefully follow the instructions to complete your application. Be sure to complete all appropriate sections and sign your application. Incomplete or unsigned applications will not be accepted.

Instructions for Completion of the Application for CISA Certification Form

1. Application Page A-1. Complete with your details on page A-1. Read and review acknowledgement. Print and sign your name and enter date on form at bottom of page.

2. 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 in IS auditing, control, assurance or security. 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 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 3 years for the Master's degree, a copy of the degree or transctipt 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 waivers 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. 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 or a person of higher rank within the organization. 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 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. Please note that if year length of employment with your most recent company is less than three months, verification of work experience is required from previous employers. Two copies of the form are included. If additional copies are required, photocopy the forms. **All Verification of Work Experience forms pages V-1 and V-2 must be signed by your verifier and submitted along with your application.** To reduce processing time, please send the completed verification forms with your application.

5. 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: *certification@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.

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:

Your Job Title: _____

Business Name:_____

Business Address: _____

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

Business Telephone (   ) _____ Fax (   ) _____

E-mail _____

Immediate Supervisor: _____
                                       Name   Title

Name

_____

Signature

_____

Date

Work Experience Detail

Exam ID _____   Name_____

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 Name	Dates of Employment in IS Audit, Control or Security		Duration of Experience	
	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)				

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 sytems:	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.

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

D. SUMMARY OF EXPERIENCE REQUIREMENTS

1. Total number of years of information systems audit, control, assurance or security experience — enter the total from Section A above (mimimum of 2 years required).. ☐

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 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).. ☐

CISA Certified Information Systems Auditor®
An ISACA® 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 *certification@isaca.org*. or +1.847.660.5660.

Thank you

_____
Applicant's Signature   Date

Employer's Verification

Please answer all five 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 am otherwise qualified to verify the experience as listed on page A-2?   ☐ Yes   ☐ No

   If no, please explain what qualifies you to verify this information? _____

2. 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

3. 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

4. Are you qualified and willing to verify the applicant's educational experience waiver(s) claimed?   ☐ Yes   ☐ No   ☐ N/A

5. Is there any reason you believe this applicant should not be certified as an information systems auditor?   ☐ Yes   ☐ No

_____   _____
Verifier's Signature   Date

CISA Certified Information Systems Auditor®
An ISACA® Certification

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

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.

Tasks
- ☐ 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 that appropriate actions have been taken by management in a timely manner.

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.

Tasks
- ☐ 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 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, quality assurance [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.

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.

Tasks
- ☐ 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 the organization's requirements are met.
- ☐ Conduct postimplementation reviews of systems to determine whether project deliverables, controls and the organization's requirements are met.

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.

Tasks
- ☐ 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 nonscheduled 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 nonscheduled 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.

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.

Tasks
- ☐ 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.

_____   _____
Verifier's Signature   Date

CISA
Certified Information
Systems Auditor®
An ISACA® 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 *certification@isaca.org*. or +1.847.660.5660.

Thank you

_____
Applicant's Signature   Date

Employer's Verification

Please answer all five 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 name(s). List all that apply to this verification. _____

1. Have you functioned in a supervisory position to the applicant or am otherwise qualified to verify the experience as listed on page A-2? ☐ Yes ☐ No

   If no, please explain what qualifies you to verify this information? _____

2. 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

3. 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

4. Are you qualified and willing to verify the applicant's educational experience waiver(s) claimed? ☐ Yes ☐ No ☐ N/A

5. Is there any reason you believe this applicant should not be certified as an information systems auditor? ☐ Yes ☐ No

_____   _____
Verifier's Signature   Date

V-1 (duplicate)

CISA Certified Information
Systems Auditor®
An ISACA® Certification

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

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.

Tasks
☐ 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 that appropriate actions have been taken by management in a timely manner.

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.

Tasks
☐ 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 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, quality assurance [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.

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.

Tasks
☐ 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 the organization's requirements are met.
☐ Conduct postimplementation reviews of systems to determine whether project deliverables, controls and the organization's requirements are met.

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.

Tasks
☐ 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 nonscheduled 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 nonscheduled 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.

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.

Tasks
☐ 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.

_____   _____
Verifier's Signature   Date

CISA
Certified Information
Systems Auditor®

An ISACA® Certification

Telephone: +1.847.253.1545

Fax: +1.847.253.1443

E-mail: *certification@isaca.org*

Web site: *www.isaca.org*