CISM Certification Application

Applicants who Passed CISM Exam in 2017 and Later

Please use Adobe Reader when filling out this application electronically.

APPLICANT INFORMATION

APPLICANT NAME: _____ ISACA ID: _____

EMAIL: _____ PHONE NUMBER: _____

STEP 1. PASS EXAM

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

EXAM PASS YEAR: _____

STEP 2. REPORT WORK EXPERIENCE

To qualify for CISM, you must have 5 years of information security management work experience within the past 10 years of the application submission date. Experience must be earned in three of the four CISM Job Practice Domains to qualify, available on page V-2. If you have not met the 5-year experience requirements within Section A, you may also opt to submit waivers for experience in section B or C.

Section A: Information Security Management Experience *(required)*

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

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

(minimum 3 years of experience in 3 of 4 Job Practice Domains required) **SECTION A EXPERIENCE TOTAL:** _____

Section B: General Information Security Experience Waiver *(optional)*

To apply for a General Information Security Experience Waiver, please fill out the details below. This experience can not have been earned during dates of employment already claimed in Section A. You can claim up to 2 years of experience with this waiver.

		Dates of Employment *(MM/YY)*		Duration of Experience	
#	Company Name	Start Date	End Date	Years	Months
1					
2					

(maximum 2 years) **SECTION B EXPERIENCE TOTAL:** _____

Section C: Substitutions for CISM Work Experience *(optional)*

Applicants are limited to **one** waiver in section C and must submit verification for any waiver claimed.

☐ 2-year waiver for a CISA in good standing ☐ 2-year waiver for a CISSP in good standing
☐ 2-year waiver for an MBA or a master's degree in Information Security/related field
☐ 1-year waiver for a bachelor's degree in Information Security or related field
☐ 1-year waiver for a skill-based or general security certification
☐ 1-year waiver for Information Systems management experience (must be one full year)

COMPANY: _____ START DATE: _____ END DATE: _____

(maximum 2 years) **SECTION C EXPERIENCE TOTAL:** _____

Section D: Experience Total

Total Experience from Sections A, B & C must be **5** Years or More to Apply for Certification

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

STEP 3. VERIFY WORK EXPERIENCE

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

STEP 4. SUBMIT APPLICATION PROCESSING PAYMENT

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

STEP 5. REVIEW AND SIGN TERMS & CONDITIONS AGREEMENT

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

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

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

Third Party Information Sharing
I acknowledge that if I am granted the Certification, my certification status will become public, and may be disclosed by ISACA to third parties who inquire. If my application is not approved, I understand that I am able to appeal the decision by contacting ISACA. Appeals undertaken by a Certification exam taker, Certification applicant or by a certified individual are undertaken at the discretion and cost of the examinee or applicant. By signing below, I authorize ISACA to disclose my Certification status. This contact information will be used to fulfill my Certification inquiries and requests.

Contact Policy
By signing below, I authorize ISACA to contact me at the address and numbers provided and that the information I provided is my own and is accurate. I authorize ISACA to release confidential Certification application and certification information if required by law or as described in ISACA's Privacy Policy. To learn more about how we use the information you have provided on this form, please read our Privacy Policy, available at www.isaca.org/privacy.

Usage Agreement
I hereby agree to hold ISACA, its officers, directors, examiners, employees, agents and those of its supporting organizations harmless from any complaint, claim, or damage arising out of any action or omission by any of them in connection with this application; the application process; the failure to issue me any certificate; or any demand for forfeiture or re-delivery of such certificate. Notwithstanding the above, I understand and agree that any action arising out of, or pertaining to this application must be brought in the Circuit Court of Cook County, Illinois, USA, and shall be governed by the laws of the State of Illinois, USA.

I understand that the decision as to whether I qualify for certification rests solely and exclusively with ISACA and that the decision of ISACA is final.

I have read and understand these statements and I intend to be legally bound by them.

APPLICANT SIGNATURE: _____ DATE: _____

STEP 6. SUBMIT APPLICATION

Please submit your application and verification form(s) online at: *https://support.isaca.org*
Select **Certifications & Certificate Programs** and **Submit an Application**.

Submitted applications take approximately two-to-three weeks to process. Upon approval, you will be notified via email. A certification packet, including a letter of approval, a CISM Certificate, and a metal CISM pin, will be sent to you via postal mail to the primary address in your MyISACA Profile at: *www.isaca.org/myisaca*. Please allow four-to-eight weeks for delivery.

CISM Experience Verification Form

Applicants who Passed CISM Exam in 2017 and Later

Please use Adobe Reader when filling out this application electronically.

APPLICANT DETAILS

APPLICANT NAME: _____ ISACA ID: _____

FORM INSTRUCTIONS FOR VERIFIER

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

You must attest to the applicant's work experience as noted on their attached application form (page A-1) and as described by the CISM Job Practice Domains and task statements (page V-2).

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

VERIFIER INFORMATION

VERIFIER NAME: _____

COMPANY NAME: _____ JOB TITLE: _____

EMAIL: _____ PHONE NUMBER: _____

VERIFIER QUESTIONS

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

☐ Section A: Company 1 ☐ Section A: Company 3

☐ Section A: Company 2 ☐ Section A: Company 4

2. I am attesting to the following general information security experience as indicated on page A-1, section B (*check all that apply*):

☐ Section B: Company 1 ☐ Section B: Company 2

3. I am attesting to experience during the following duration:

START DATE: _____ END DATE: _____

4. I have functioned in the following role(s) to the applicant:

☐ Supervisor ☐ Manager ☐ Colleague ☐ Client

5. If I am attesting to any experience earned in Section A, I can also attest that the tasks performed by the applicant, as listed on page V-2 of this form, are correct to the best of my knowledge.

☐ Yes ☐ No

VERIFIER AGREEMENT

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

VERIFIER SIGNATURE: _____ DATE: _____

CISM Experience Verification Form

Applicants who Passed CISM Exam in 2017 and Later

Please use Adobe Reader when filling out this application electronically.

JOB PRACTICE DOMAIN INSTRUCTIONS

Applicant is required to check any domain in which any or all tasks have been completed.

☐ DOMAIN 1 - Information Security Governance

Establish and/or maintain an information security governance framework and supporting processes to ensure that the information security strategy is aligned with organizational goals and objectives.

Task Statements:

- Establish and/or maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and/or ongoing management of the information security program.
- Establish and/or maintain an information security governance framework to guide activities that support the information security strategy.
- Integrate information security governance into corporate governance to ensure that organizational goals and objectives are supported by the information security program.
- Establish and maintain information security policies to guide the development of standards, procedures and guidelines in alignment with enterprise goals and objectives.
- Develop business cases to support investments in information security.
- Identify internal and external influences to the organization (e.g., emerging technologies, social media, business environment, risk tolerance, regulatory requirements, third-party considerations, threat landscape) to ensure that these factors are continually addressed by the information security strategy.
- Gain ongoing commitment from senior leadership and other stakeholders to support the successful implementation of the information security strategy.
- Define, communicate, and monitor information security responsibilities throughout the organization (e.g., data owners, data custodians, end users, privileged or high-risk users) and lines of authority.
- Establish, monitor, evaluate and report key information security metrics to provide management with accurate and meaningful information regarding the effectiveness of the information security strategy.

☐ DOMAIN 2 - Information Risk Management

Manage information risk to an acceptable level based on risk appetite in order to meet organizational goals and objectives.

Task Statements:

- Establish and/or maintain a process for information asset classification to ensure that measures taken to protect assets are proportional to their business value.
- Identify legal, regulatory, organizational and other applicable requirements to manage the risk of noncompliance to acceptable levels.
- Ensure that risk assessments, vulnerability assessments and threat analyses are conducted consistently, at appropriate times, and to identify and assess risk to the organization's information.
- Identify, recommend or implement appropriate risk treatment/response options to manage risk to acceptable levels based on organizational risk appetite.
- Determine whether information security controls are appropriate and effectively manage risk to an acceptable level.
- Facilitate the integration of information risk management into business and IT processes (e.g., systems development, procurement, project management) to enable a consistent and comprehensive information risk management program across the organization.
- Monitor for internal and external factors (e.g., key risk indicators [KRIs], threat landscape, geopolitical, regulatory change) that may require reassessment of risk to ensure that changes to existing, or new, risk scenarios are identified and managed appropriately.
- Report noncompliance and other changes in information risk to facilitate the risk management decision-making process.
- Ensure that information security risk is reported to senior management to support an understanding of potential impact on the organizational goals and objectives.

☐ DOMAIN 3 - Information Security Program Development and Management

Develop and maintain an information security program that identifies, manages and protects the organization's assets while aligning to information security strategy and business goals, thereby supporting an effective security posture.

Task Statements:

- Establish and/or maintain the information security program in alignment with the information security strategy.
- Align the information security program with the operational objectives of other business functions (e.g., human resources [HR], accounting, procurement and IT) to ensure that the information security program adds value to and protects the business.
- Identify, acquire and manage requirements for internal and external resources to execute the information security program.
- Establish and maintain information security processes and resources (including people and technologies) to execute the information security program in alignment with the organization's business goals.
- Establish, communicate and maintain organizational information security standards, guidelines, procedures and other documentation to guide and enforce compliance with information security policies.
- Establish, promote and maintain a program for information security awareness and training to foster an effective security culture.
- Integrate information security requirements into organizational processes (e.g., change control, mergers and acquisitions, system development, business continuity, disaster recovery) to maintain the organization's security strategy.
- Integrate information security requirements into contracts and activities of third parties (e.g., joint ventures, outsourced providers, business partners, customers) and monitor adherence to established requirements in order to maintain the organization's security strategy.
- Establish, monitor and analyze program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.
- Compile and present reports to key stakeholders on the activities, trends and overall effectiveness of the IS program and the underlying business processes in order to communicate security performance.

☐ DOMAIN 4 - Information Security Incident Management

Plan, establish and manage the capability to detect, investigate, respond to and recover from information security incidents to minimize business impact.

Task Statements:

- Establish and maintain an organizational definition of, and severity hierarchy for, information security incidents to allow accurate classification and categorization of and response to incidents.
- Establish and maintain an incident response plan to ensure an effective and timely response to information security incidents.
- Develop and implement processes to ensure the timely identification of information security incidents that could impact the business.
- Establish and maintain processes to investigate and document information security incidents in order to determine the appropriate response and cause while adhering to legal, regulatory and organizational requirements.
- Establish and maintain incident notification and escalation processes to ensure that the appropriate stakeholders are involved in incident response management.
- Organize, train and equip incident response teams to respond to information security incidents in an effective and timely manner.
- Test, review and revise (as applicable) the incident response plan periodically to ensure an effective response to information security incidents and to improve response capabilities.
- Establish and maintain communication plans and processes to manage communication with internal and external entities.
- Conduct post incident reviews to determine the root cause of information security incidents, develop corrective actions, reassess risk, evaluate response effectiveness and take appropriate remedial actions.
- Establish and maintain integration among the incident response plan, business continuity plan and disaster recovery plan.