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 Certified Information Security Manager® An ISACA® Certification

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.