CISM®

Certified Information Security Manager®

An ISACA® Certification

Application for CISM Certification

ISACA®

Trust in, and value from, information systems

11/2015

Requirements to Become a Certified Information Security Manager

To become a Certified Information Security Manager (CISM), an applicant must:

1. *Score a passing grade on the CISM exam.* A passing score on the CISM exam, without completing the required work experience as outlined below, will only be valid for five years. If the applicant does not meet the CISM certification requirements within the five year period, the passing score will be voided.

   Important Note: Your completed CISM 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 CISM application processing fee of US $50 online at *www.isaca.org/cismpay*.

3. *Submit verified evidence of five (5) years of work experience in the field of information security.* Three (3) of the five (5) years of work experience must be gained performing the role of an information security manager. In addition, this work experience must be broad and gained in three of the four job practice areas (see Verification of Work Experience form). The management portion of this experience must be earned while in an information security management position with responsibility for information security management programs or processes, or while working as an information security management consultant (where the CISM candidate has been actively engaged in the development and/or management of information security programs or processes for the client organization(s). 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 for work performed in the role of an information security manager are not allowed. However, a maximum of two (2) years for general work experience in the field of information security may be substituted as follows:

   - Two years of general work experience may be substituted for currently holding one of the following broad security-related certifications or a post-graduate degree:
     - Certified Information Systems Auditor (CISA) in good standing or
     - Certified Information Systems Security Professional (CISSP) in good standing or
     - Post-graduate degree in information security or a related field (for example: business administration, information systems, information assurance)

   OR

   - A maximum of one year of general information security work experience may be substituted for one of the following:
     - One full year of information systems management experience or
     - One full year of general security management experience
     - Currently holding a skill-based or general security certification [(e.g., SANS Global Information Assurance Certification (GIAC), Microsoft Certified Systems Engineer (MCSE), CompTIA Security+, CompTIA Security+ $_{CE}$, Disaster Recovery Institute Certified Business Continuity Professional (CBCP), ESL IT Security Manager].
     - Completion of an information security management program at an institution aligned with the Model Curriculum.

For example, an applicant holding either a CISA or CISSP will qualify for two years of general information security experience substitution. However, the applicant also must possess a minimum of three years information security management work experience in three of the four job practice areas.

Exception: Two years as a full-time university instructor teaching the management of information security can be substituted for every one year of information security management experience.

4. *Agree to abide by the ISACA Code of Professional Ethics*.

5. *Agree to abide by the CISM Continuing Education Policy which can be viewed at www.isaca.org/cismcpepolicy.*

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. Applications will be randomly selected for audit of the verification forms.

CISM Certified Information Security Manager An ISACA Certification

Application for CISM Certification

Instructions for Completion of the Application for CISM 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 date the application at the bottom of page A-1.

2. Application Page A-2.

Section A—Information Security Management Experience

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

- Name of employer/company where information security management services were performed. This is your work that aligns with the CISM job practice domains.
- Job title held where information security management experience is claimed. If multiple positions were held use one line for each title.
- Date range (month and year) in which information security management services were performed
- Number of years and months, by employer and in total, performing information security management services.

Section B—General Information Security Experience

For each employer/company (starting with the most current), enter information pertaining to experience gained performing general information security services. Experience claimed in Section A cannot also be claimed as general information security experience.

- Name of employer/company where general information security services were performed.
- Position title held where general information security experience is claimed.
- Date range (month and year) in which general information security services were performed
- Number of years and months, by employer and in total, performing general information security services.

Note: If experiences crosses both information security management and general information security manager, duration of experience cannot exceed the total length of employment with each organization.

Section C—Substitution for General Information Security Experience

Two-year substitution—Enter information pertaining to broad security-related certification or graduate degrees earned.

- Certifications held in good standing (include copy of certification or letter indicating good standing).
- Post-graduate degree in information security or related field (for example: business administration, information systems, information assurance) including the name of the institution where earned, the degree title, the date the degree was awarded, and an explanation of the relevancy of this degree to information security management. (copy of a transcript or letter confirming degree status must accompany your application. To reduce processing time, please do not send the transcript separately.)

One-year substitution—Enter information pertaining to information systems management experience, security management, skill-based security-related certifications earned, or information related to completion of a security management program at an institution aligned with the Model Curriculum.

- Information systems management services
  - Name of employer and job title where information systems (non-security) management services were performed
  - Date (month and year) in which information systems management services were performed
- Security Management Experience Gained Outside of Information Security
  - Enter information pertaining to experience gained performing security management activities including physical security, personnel security, risk management, investigations management etc.
  - Name of employer and job title where other security management services were performed
  - Dates during which security management services were performed.
  - Description of security management services performed.
- Skill-based security certification—Enter the certification name and issuing organization (include copy of certification or letter indicating good standing). See page 2 for listing.

Section D—Summary of Work Experience

Record the total number of years and months from sections A, B and C in the appropriate box. The total in box A must be three (3) or more. The total in box C can be no greater than two (2) years, which is the maximum allowable general information security experience substitution allowed. Then add boxes A, B, and C and record the total number of years and months in the box following the line titled "Total Work Experience." This total must be equal to or greater than five (5) years to qualify for CISM certification.

3. Verification page V-1 and V-2.
Complete the top portion on the Verification of Work Experience form (pages V-1 and V-2) and check the boxes on page V-2 that indicate the tasks you performed that are being verified by each verifier. Give the forms 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 CISM, 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 CISM to perform this role. 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.

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

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

Email: *certification@isaca.org*
Telephone Number +1.847.253.1545
Fax Number: +1.847.253.1443

NOTE: Please allow approximately eight weeks for the processing of your completed Application for CISM Certification. Upon approval, you will receive a certificate package via mail containing a letter of certification and your CISM certificate. If you do not receive any communication regarding your application status eight weeks from submittal date, please follow up with an email to *certification@isaca.org*, mark subject, Application Status Request.

CISM® Certified Information Security Manager®
An ISACA® Certification

Application for CISM Certification

Page A-1

Name: ______________________________ Exam ID______________
First Middle Initial/Name 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: ______________________________

Employer/Company Name: ______________________________

Business Address:______________________________

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

Business Telephone ( )______________ Fax ( ) ______________

Email______________________________

Immediate Supervisor: ______________________________ ______________________________
Name Title

I hereby apply to Information Systems Audit and Control Association, Inc. (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. 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, 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. 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. Not withstanding 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

Application for CISM Certification

NAME: ____ Exam ID__________________________

Please use black ink and print in block letters or type

A. Information Security Management Experience—For each employer/company (starting with the most current), enter information pertaining to the positions where you have been responsible for performing information security management activities.

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.

Do not leave dates blank. If currently employed, include a date or current, now, present, etc.

Employer/Company Name	**Job Title**	Dates of employment in general security management	Duration of experience	
		MM/YY MM/YY	Years	Months
		To		
		To		
		To		
		To		
Total years information security management experience (must be 3 or more).				

B. General Information Security Experience—For each employer/company (starting with the most current), enter information pertaining to the positions where you have been responsible for performing general information security services. Duration of work experience claimed in Section A cannot be repeated again in general experience.

Employer/Company Name	**Job Title**	Dates of employment in general security management	Duration of experience	
		MM/YY MM/YY	Years	Months
		To		
		To		
		To		
		To		
Total years general information security experience.				

C. Substitutions for General Information Security Experience

Two-Year Substitution

Current CISA in good standing ? Yes____ Current CISSP in good standing? Yes____ ***Attach a copy of CISSP certificate of certification***

Post-graduate degree? Yes____ ***Send or copy of the transcript or letter confirming degree status to ISACA with your application***

Institution name: ____

Degree name:____ Date awarded: _________ (mo.)/_________(yr.)

Relevancy of degree to information security management____

One-Year Substitution

Information systems management experience? Yes____ Number of years/months_________/_________ ***Must be a minimum of one year to qualify***

Job title: ____________________________________ Employer: ____

Begin date:_________/_________ Left position on: _________/_________

Experience gained in areas of traditional security management including physical security, personnel security, investigations management etc.

Employer ____________________________________ Job Title _________________________________

Begin Date ___________________________ Left Position on ___________________________

Describe areas of security management experience____

____

Skilled-based or general security certification? Yes____ ***Attach a copy of certificate of certification.***

D. Summary of Work Experience

Record the total number of years from sections A, B and C in the appropriate box. The total in box A must be three (3) or more.
The total in box C can be no greater than two (2) years, which is the maximum allowable general information security experience substitution allowed.

		Years	Months
• Total years of information security management experience (Must be 3 or more)	A		
• Total years of general information security experience	B		
• Total number of years being substituted (Must be 2 or less)	C		
Total Work Experience – add boxes A, B and C (Must be 5 or more)	Total		

Verification of Work Experience (page 1 of 2)

Exam ID ______________________________

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

Certified Information Security Manager. As such, my information security 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 CISM to perform this role.

I would appreciate your cooperation in completing this form, by verifying my information security work experience as noted on my application form (page A-2) attached and as described by CISM job practice area and task statements (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

Verifier's Name: ______________________________

Verifier's Certifications and Certification Numbers: ______________________________

Company Name: ______________________________

Job Title: ______________________________

Address: ______________________________
STREET

____
CITY STATE/PROVINCE/COUNTRY POSTAL CODE

Company Telephone Number: ______________________________ Company Email: ______________________________

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. I have functioned in a supervisory or other related position to the applicant and can verify his/her:
   - information security management work experience (see Section A of Application) □ Yes □ No □ N/A
   - general information security work experience (see Section B of Application) □ Yes □ No □ N/A
2. I can attest to the duration of the applicant's:
   - information security management work experience (see Section A of Application) with my organization. If no, I attest to ________ years □ Yes □ No □ N/A
   - general information security work experience (see Section B of Application) with my organization. If no, I attest to ________ years □ Yes □ No □ N/A
3. I am qualified and willing to verify the applicant's:
   - information security management work experience (see Section A of Application) prior to his/her affiliation with my organization. □ Yes □ No □ N/A
   - general information security work experience (see Section B of Application) prior to his/her affiliation with my organization. □ Yes □ No □ N/A
4. If verifying information security management experience:
   - I can attest that according to the CISM job practice areas and task statements, the tasks performed by the applicant with my organization (and/or previous organizations, if applicable) as listed/selected on page V-2 is correct to the best of my knowledge, that the applicant is competent in performing these areas and that I have signed where indicated on page V-2 of the form. □ Yes □ No
5. Is there any reason you believe this applicant should not be certified as an information security manager? □ 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. Verifier to review the items checked and confirm the tasks by signing at the bottom of this page (V-2).

Information Security Governance—Establish and maintain an information security governance framework and supporting processes to ensure that the information security strategy is aligned with organizational goals and objectives, information risk is managed appropriately and program resources are managed responsibly.

☐ Establish and maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and ongoing management of the information security program.
☐ Establish and 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 communicate management's directives and guide the development of standards, procedures and guidelines.
☐ Develop business cases to support investments in information security.
☐ Identify internal and external influences to the organization (for example, technology, business environment, risk tolerance, geographic location, legal and regulatory requirements) to ensure that these factors are addressed by the information security strategy.
☐ Obtain commitment from senior management and support from other stakeholders to maximize the probability of successful implementation of the information security strategy.
☐ Define and communicate the roles and responsibilities of information security throughout the organization to establish clear accountabilities and lines of authority.
☐ Establish, monitor, evaluate and report metrics (for example, key goal indicators [KGIs], key performance indicators [KPIs], key risk indicators [KRIs]) to provide management with accurate information regarding the effectiveness of the information security strategy.

Information Risk Management and Compliance—Manage information risk to an acceptable level to meet the business and compliance requirements of the organization.

☐ Establish and 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 periodically and consistently to identify risk to the organization's information.
☐ Determine appropriate risk treatment options to manage risk to acceptable levels.
☐ Evaluate information security controls to determine whether they are appropriate and effectively mitigate risk to an acceptable level.
☐ Identify the gap between current and desired risk levels to manage risk to an acceptable level.
☐ Integrate information risk management into business and IT processes (for example, development, procurement, project management, mergers and acquisitions) to promote a consistent and comprehensive information risk management process across the organization.
☐ Monitor existing risk to ensure that changes are identified and managed appropriately.
☐ Report noncompliance and other changes in information risk to appropriate management to assist in the risk management decision-making process.

Information Security Program Development and Management—Establish and manage the information security program in alignment with the information security strategy.

☐ Establish and maintain the information security program in alignment with the information security strategy.
☐ Ensure alignment between the information security program and other business functions (for example, human resources [HR], accounting, procurement and IT) to support integration with business processes.
☐ Identify, acquire, manage and define requirements for internal and external resources to execute the information security program.
☐ Establish and maintain information security architectures (people, process, technology) to execute the information security program.
☐ Establish, communicate and maintain organizational information security standards, procedures, guidelines and other documentation to support and guide compliance with information security policies.
☐ Establish and maintain a program for information security awareness and training to promote a secure environment and an effective security culture.
☐ Integrate information security requirements into organizational processes (for example, change control, mergers and acquisitions, development, business continuity, disaster recovery) to maintain the organization's security baseline.
☐ Integrate information security requirements into contracts and activities of third parties (for example, joint ventures, outsourced providers, business partners, customers) to maintain the organization's security baseline.
☐ Establish, monitor and periodically report program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.

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.

☐ Establish and maintain an organizational definition of, and severity hierarchy for, information security incidents to allow accurate identification 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.
☐ Establish and maintain processes to investigate and document information security incidents to be able to respond appropriately and determine their causes while adhering to legal, regulatory and organizational requirements.
☐ Establish and maintain incident escalation and notification processes to ensure that the appropriate stakeholders are involved in incident response management.
☐ Organize, train and equip teams to effectively respond to information security incidents in a timely manner.
☐ Test and review 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 postincident 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, disaster recovery plan and business continuity plan.

____ ______________________

Verifier's Signature Date

CISM® Certified Information Security Manager®
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 Security Manager. As such, my information security 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 CISM to perform this role.

I would appreciate your cooperation in completing this form, by verifying my information security work experience as noted on my application form (page A-2) attached and as described by CISM job practice area and task statements (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

Verifier's Name: ______________________________

Verifier's Certifications and Certification Numbers: ______________________________

Company Name: ______________________________

Job Title: ______________________________

Address: ______________________________
STREET

____
CITY STATE/PROVINCE/COUNTRY POSTAL CODE

Company Telephone Number: ______________________________ Company Email: ______________________________

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. I have functioned in a supervisory or other related position to the applicant and can verify his/her:
   - information security management work experience (see Section A of Application) □ Yes □ No □ N/A
   - general information security work experience (see Section B of Application) □ Yes □ No □ N/A
2. I can attest to the duration of the applicant's:
   - information security management work experience (see Section A of Application) with my organization. If no, I attest to ________ years □ Yes □ No □ N/A
   - general information security work experience (see Section B of Application) with my organization. If no, I attest to ________ years □ Yes □ No □ N/A
3. I am qualified and willing to verify the applicant's:
   - information security management work experience (see Section A of Application) prior to his/her affiliation with my organization. □ Yes □ No □ N/A
   - general information security work experience (see Section B of Application) prior to his/her affiliation with my organization. □ Yes □ No □ N/A
4. If verifying information security management experience:
   - I can attest that according to the CISM job practice areas and task statements, the tasks performed by the applicant with my organization (and/or previous organizations, if applicable) as listed/selected on page V-2 is correct to the best of my knowledge, that the applicant is competent in performing these areas and that I have signed where indicated on page V-2 of the form. □ Yes □ No
5. Is there any reason you believe this applicant should not be certified as an information security manager? □ 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. Verifier to review the items checked and confirm the tasks by signing at the bottom of this page (V-2).

Information Security Governance—Establish and maintain an information security governance framework and supporting processes to ensure that the information security strategy is aligned with organizational goals and objectives, information risk is managed appropriately and program resources are managed responsibly.

☐ Establish and maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and ongoing management of the information security program.
☐ Establish and 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 communicate management's directives and guide the development of standards, procedures and guidelines.
☐ Develop business cases to support investments in information security.
☐ Identify internal and external influences to the organization (for example, technology, business environment, risk tolerance, geographic location, legal and regulatory requirements) to ensure that these factors are addressed by the information security strategy.
☐ Obtain commitment from senior management and support from other stakeholders to maximize the probability of successful implementation of the information security strategy.
☐ Define and communicate the roles and responsibilities of information security throughout the organization to establish clear accountabilities and lines of authority.
☐ Establish, monitor, evaluate and report metrics (for example, key goal indicators [KGIs], key performance indicators [KPIs], key risk indicators [KRIs]) to provide management with accurate information regarding the effectiveness of the information security strategy.

Information Risk Management and Compliance—Manage information risk to an acceptable level to meet the business and compliance requirements of the organization.

☐ Establish and 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 periodically and consistently to identify risk to the organization's information.
☐ Determine appropriate risk treatment options to manage risk to acceptable levels.
☐ Evaluate information security controls to determine whether they are appropriate and effectively mitigate risk to an acceptable level.
☐ Identify the gap between current and desired risk levels to manage risk to an acceptable level.
☐ Integrate information risk management into business and IT processes (for example, development, procurement, project management, mergers and acquisitions) to promote a consistent and comprehensive information risk management process across the organization.
☐ Monitor existing risk to ensure that changes are identified and managed appropriately.
☐ Report noncompliance and other changes in information risk to appropriate management to assist in the risk management decision-making process.

Information Security Program Development and Management—Establish and manage the information security program in alignment with the information security strategy.

☐ Establish and maintain the information security program in alignment with the information security strategy.
☐ Ensure alignment between the information security program and other business functions (for example, human resources [HR], accounting, procurement and IT) to support integration with business processes.
☐ Identify, acquire, manage and define requirements for internal and external resources to execute the information security program.
☐ Establish and maintain information security architectures (people, process, technology) to execute the information security program.
☐ Establish, communicate and maintain organizational information security standards, procedures, guidelines and other documentation to support and guide compliance with information security policies.
☐ Establish and maintain a program for information security awareness and training to promote a secure environment and an effective security culture.
☐ Integrate information security requirements into organizational processes (for example, change control, mergers and acquisitions, development, business continuity, disaster recovery) to maintain the organization's security baseline.
☐ Integrate information security requirements into contracts and activities of third parties (for example, joint ventures, outsourced providers, business partners, customers) to maintain the organization's security baseline.
☐ Establish, monitor and periodically report program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.

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.

☐ Establish and maintain an organizational definition of, and severity hierarchy for, information security incidents to allow accurate identification 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.
☐ Establish and maintain processes to investigate and document information security incidents to be able to respond appropriately and determine their causes while adhering to legal, regulatory and organizational requirements.
☐ Establish and maintain incident escalation and notification processes to ensure that the appropriate stakeholders are involved in incident response management.
☐ Organize, train and equip teams to effectively respond to information security incidents in a timely manner.
☐ Test and review 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 postincident 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, disaster recovery plan and business continuity plan.

____ ____________________
Verifier's Signature Date

CISM® Certified Information Security Manager®

An ISACA® Certification

Telephone: +1.847.253.1545

Fax: +1.847.253.1443

Email: *certification@isaca.org*

Web site: *www.isaca.org*