Application for Certification

Revised 1/2008

Application for CISM Certification

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.

2. *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 five job practice areas (see reverse side of 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). Please note that in most cases work performed while in an IT audit or similar assurance role outside of the information security function **cannot be considered as security management experience**. 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+, Disaster Recovery Institute Certified Business Continuity Professional (CBCP), ESL IT Security Manager].

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 five job practice areas.

     - Completion of an information security management program at an institution aligned with the Model Curriculum.

   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.

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

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

Application for CISM Certification

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.

Members and ISACA certification holders shall:

1. Support the implementation of, and encourage compliance with, appropriate standards, procedures and controls for information systems

2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices

3. Serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession

4. Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties

5. Maintain competency in their respective fields and agree to undertake only those activities, which they can reasonably expect to complete with professional competence

6. Inform appropriate parties of the results of work performed, revealing all significant facts known to them

7. Support the professional education of stakeholders in enhancing their understanding of information systems security and control

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.

Application for CISM Certification

Instructions for Completion of the Application for CISM Certification Form

1. Section A—Information Security Management Experience
For each employer (starting with the most current), enter the following information:

- Name of employer where information security management services were performed
- 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 (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 where general information security services were performed (can be same employer as above)
- 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.

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. (An original transcript or letter confirming degree status must accompany you 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).

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.

Section E—Individuals Verifying Work Experience Details
Please record here the names and contact information of the individual(s) that will verify your work experience in sections A and B.

2. Complete the top portion of the front page of the Verification of Work Experience form and check the boxes on the reverse side 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. If one person cannot verify all required experience for you to become a CISM, previous employers must be asked to complete this form. Two copies of the form are included. If additional copies are required, photocopy the form (both sides). All Verification of Work Experience forms, front and back, 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.

3. 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 mail your completed Application for CISM Certification to:

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

E-mail: *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, your CISM certificate and the CISM Continuing Education Policy.

Application for CISM Certification

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

Maiden Name or Former Name(s) _____ Birth Date: _____/_____ /_____
_____
M D Y

Preferred Mailing Address: Home ( ) Business ( ) Month and Year of Exam_____

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

I hereby apply to ISACA for issuance to me of certification, as a Certified Information Security Manager (CISM) in accordance with and subject to the procedures and regulations of ISACA. I have read and agree to the conditions set forth in the Application for CISM Certification and CISM Continuing Education Policy in effect at the time of my application, covering the certification process; and Continuing Education policies. I agree to denial of certification and to forfeiture and redelivery of any certificate or other credential granted me by ISACA in the event that any of the statements or answers made by me in this application are false or in the event that I violate any of the rules or regulations governing such exam.

I authorize ISACA to make whatever inquiries and investigations it deems necessary to verify my credentials and my professional standing. I understand that this application and any information or material received or generated by ISACA in connection with my certification will be kept confidential and will not be released unless I have authorized such release or such release is required by law. However, the fact that I am or am not, or have or have not been, certified is a matter of public record and may be disclosed. Finally, I allow ISACA to use information from my application for the purpose of statistical analysis and to release my contact information to the ISACA Chapter in my area.

I hereby agree to hold ISACA, its officers, directors, examiners, employees, and agents, 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.

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

Revised 1/2008

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 (starting with the most current), enter information pertaining to the positions where you have been responsible for performing information security management activities.

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

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

Employer Name	Job Title	Dates of employment in general information security		Duration of experience	
		MM/YY	MM/YY	Years	Months
			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 an original 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		

E. Individuals Verifying Work Experience Details

Please record here the names and contact information of the individual(s) that will verify your work experience in sections A and B above:

1. Name_____ Title _____

   Company_____Tel. No._____E-mail _____

2. Name_____ Title _____

   Company_____Tel. No._____E-mail _____

3. Name_____ Title _____

   Company_____Tel. No._____E-mail _____

Application for CISM Certification

Verification of Work Experience (front)

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). 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 attached and as described by CISM job practice area and task statements (see reverse side of form). 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 +1.847.253.1545, x772.

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 E-mail:_____

Name of company relating to candidate's employment from page 2: _____

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 the tasks performed by the applicant with my organization, as listed on the reverse side of this form, is correct to the best of my knowledge. If no, what is incorrect?_____ ☐ Yes ☐ No
   - I can attest to the fact that, according to the CISM job practice areas and task statements, the applicant has worked in, and is competent in, performing tasks in these areas and have signed where indicated on front and back of this 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

Revised 1/2008

Application for CISM Certification

Verification of Work Experience (back)

Exam ID _____

Applicant Name: _____ Verifier Name: _____

Information Security Governance Tasks—Establish and maintain a framework to provide assurance that information security strategies are aligned with the business objectives and consistent with applicable laws and regulations.

☐ Develop an information security strategy aligned with business goals and objectives.
☐ Align information security strategy with corporate governance.
☐ Develop business cases justifying investment in information security.
☐ Identify current and potential legal and regulatory requirements affecting information security.
☐ Identify drivers affecting the organization (e.g., technology, business environment, risk tolerance, geographic location) and their impact on information security.
☐ Obtain senior management commitment to information security.
☐ Define roles and responsibilities for information security throughout the organization.
☐ Establish internal and external reporting and communication channels that support information security.

Information Risk Management Tasks—Identify and manage information security risks to achieve business objectives.

☐ Establish a process for information asset classification and ownership.
☐ Implement a systematic and structured information risk assessment process.
☐ Ensure that business impact assessments are conducted periodically.
☐ Ensure that threat and vulnerability evaluations are performed on an ongoing basis.
☐ Identify and periodically evaluate information security controls and countermeasures to mitigate risk to acceptable levels.
☐ Integrate risk, threat and vulnerability identification and management into lifecycle processes (e.g., development, procurement, and employment lifecycles).
☐ Report significant changes in information risk to appropriate levels of management for acceptance on both a periodic and event-driven basis.

Information Security Program Development Tasks—Create and maintain a program to implement the information security strategy.

☐ Develop and maintain plans to implement the information security strategy.
☐ Specify the activities to be performed within the information security program.
☐ Ensure alignment between the information security program and other assurance functions (e.g., physical, HR, quality, IT).
☐ Identify internal and external resources (e.g., finances, people, equipment, systems) required to execute the information security program.
☐ Ensure the development of information security architectures (e.g., people, processes, technology).
☐ Establish, communicate, and maintain information security policies that support the security strategy.
☐ Design and develop a program for information security awareness, training, and education.
☐ Ensure the development, communication, and maintenance of standards, procedures, and other documentation (e.g., guidelines, baselines, codes of conduct) that support information security policies.
☐ Integrate information security requirements into the organization's processes (e.g., change control, mergers and acquisitions) and life cycle activities (e.g., development, employment, procurement).
☐ Develop a process to integrate information security controls into contracts (e.g., with joint ventures, outsourced providers, business partners, customers, third parties).
☐ Establish metrics to evaluate the effectiveness of the information security program.

Information Security Program Management Tasks—Oversee and direct information security activities to execute the information security program.

☐ Manage internal and external resources (e.g., finances, people, equipment, systems) required to execute the information security program.
☐ Ensure that processes and procedures are performed in compliance with the organization's information security policies and standards.
☐ Ensure that the information security controls agreed to in contracts (e.g., with joint ventures, outsourced providers, business partners, customers, third parties) are performed.
☐ Ensure that information security is an integral part of the systems development process.
☐ Ensure that information security is maintained throughout the organization's processes (e.g., change control, mergers and acquisitions) and life cycle activities (e.g., development, employment, procurement).
☐ Provide information security advice and guidance (e.g., risk analysis, control selection) to the organization.
☐ Provide information security awareness, training and education to stakeholders (e.g., business process owners, users, information technology).
☐ Monitor, measure, test, and report on the effectiveness and efficiency of information security controls and compliance with information security policies.
☐ Ensure that noncompliance issues and other variances are resolved in a timely manner.

Incident Management and Response Tasks—Plan, develop, and manage a capability to detect, respond to, and recover from information security incidents.

☐ Develop and implement processes for detecting, identifying, analyzing, and responding to information security incidents.
☐ Establish escalation and communication processes and lines of authority.
☐ Develop plans to respond to and document information security incidents.
☐ Establish the capability to investigate information security incidents (e.g., forensics, evidence collection and preservation, log analysis, interviewing).
☐ Develop a process to communicate with internal parties and external organizations (e.g., media, law enforcement, customers).
☐ Integrate information security incident response plans with the organization's Disaster Recovery (DR) and Business Continuity Plan (BCP).
☐ Organize, train, and equip teams to respond to information security incidents.
☐ Periodically test and refine information security incident response plans.
☐ Manage the response to information security incidents.
☐ Conduct reviews to identify causes of information security incidents, develop corrective actions, and reassess risk.

Verifier's Signature _____ Date _____

Application for CISM Certification

Verification of Work Experience (front)

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). 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 attached and as described by CISM job practice area and task statements (see reverse side of form). 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 +1.847.253.1545, x772.

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 E-mail:_____

Name of company relating to candidate's employment from page 2: _____

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 the tasks performed by the applicant with my organization, as listed on the reverse side of this form, is correct to the best of my knowledge. If no, what is incorrect?_____ ☐ Yes ☐ No
   - I can attest to the fact that, according to the CISM job practice areas and task statements, the applicant has worked in, and is competent in, performing tasks in these areas and have signed where indicated on front and back of this 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

Application for CISM Certification

Verification of Work Experience (back)

Exam ID _____

Applicant Name: _____ Verifier Name: _____

Information Security Governance Tasks—Establish and maintain a framework to provide assurance that information security strategies are aligned with the business objectives and consistent with applicable laws and regulations.

☐ Develop an information security strategy aligned with business goals and objectives.
☐ Align information security strategy with corporate governance.
☐ Develop business cases justifying investment in information security.
☐ Identify current and potential legal and regulatory requirements affecting information security.
☐ Identify drivers affecting the organization (e.g., technology, business environment, risk tolerance, geographic location) and their impact on information security.
☐ Obtain senior management commitment to information security.
☐ Define roles and responsibilities for information security throughout the organization.
☐ Establish internal and external reporting and communication channels that support information security.

Information Risk Management Tasks—Identify and manage information security risks to achieve business objectives.

☐ Establish a process for information asset classification and ownership.
☐ Implement a systematic and structured information risk assessment process.
☐ Ensure that business impact assessments are conducted periodically.
☐ Ensure that threat and vulnerability evaluations are performed on an ongoing basis.
☐ Identify and periodically evaluate information security controls and countermeasures to mitigate risk to acceptable levels.
☐ Integrate risk, threat and vulnerability identification and management into lifecycle processes (e.g., development, procurement, and employment lifecycles).
☐ Report significant changes in information risk to appropriate levels of management for acceptance on both a periodic and event-driven basis.

Information Security Program Development Tasks—Create and maintain a program to implement the information security strategy.

☐ Develop and maintain plans to implement the information security strategy.
☐ Specify the activities to be performed within the information security program.
☐ Ensure alignment between the information security program and other assurance functions (e.g., physical, HR, quality, IT).
☐ Identify internal and external resources (e.g., finances, people, equipment, systems) required to execute the information security program.
☐ Ensure the development of information security architectures (e.g., people, processes, technology).
☐ Establish, communicate, and maintain information security policies that support the security strategy.
☐ Design and develop a program for information security awareness, training, and education.
☐ Ensure the development, communication, and maintenance of standards, procedures, and other documentation (e.g., guidelines, baselines, codes of conduct) that support information security policies.
☐ Integrate information security requirements into the organization's processes (e.g., change control, mergers and acquisitions) and life cycle activities (e.g., development, employment, procurement).
☐ Develop a process to integrate information security controls into contracts (e.g., with joint ventures, outsourced providers, business partners, customers, third parties).
☐ Establish metrics to evaluate the effectiveness of the information security program.

Information Security Program Management Tasks—Oversee and direct information security activities to execute the information security program.

☐ Manage internal and external resources (e.g., finances, people, equipment, systems) required to execute the information security program.
☐ Ensure that processes and procedures are performed in compliance with the organization's information security policies and standards.
☐ Ensure that the information security controls agreed to in contracts (e.g., with joint ventures, outsourced providers, business partners, customers, third parties) are performed.
☐ Ensure that information security is an integral part of the systems development process.
☐ Ensure that information security is maintained throughout the organization's processes (e.g., change control, mergers and acquisitions) and life cycle activities (e.g., development, employment, procurement).
☐ Provide information security advice and guidance (e.g., risk analysis, control selection) to the organization.
☐ Provide information security awareness, training and education to stakeholders (e.g., business process owners, users, information technology).
☐ Monitor, measure, test, and report on the effectiveness and efficiency of information security controls and compliance with information security policies.
☐ Ensure that noncompliance issues and other variances are resolved in a timely manner.

Incident Management and Response Tasks—Plan, develop, and manage a capability to detect, respond to, and recover from information security incidents.

☐ Develop and implement processes for detecting, identifying, analyzing, and responding to information security incidents.
☐ Establish escalation and communication processes and lines of authority.
☐ Develop plans to respond to and document information security incidents.
☐ Establish the capability to investigate information security incidents (e.g., forensics, evidence collection and preservation, log analysis, interviewing).
☐ Develop a process to communicate with internal parties and external organizations (e.g., media, law enforcement, customers).
☐ Integrate information security incident response plans with the organization's Disaster Recovery (DR) and Business Continuity Plan (BCP).
☐ Organize, train, and equip teams to respond to information security incidents.
☐ Periodically test and refine information security incident response plans.
☐ Manage the response to information security incidents.
☐ Conduct reviews to identify causes of information security incidents, develop corrective actions, and reassess risk.

_____ _____

Verifier's Signature Date

Telephone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: *certification@isaca.org*
Web site: *www.isaca.org*

Revised 1/2008