

INFORMATION SYSTEMS AUDIT
AND CONTROL ASSOCIATION®

CISM

CERTIFIED INFORMATION
SECURITY MANAGER™

CONTINUING PROFESSIONAL
EDUCATION POLICY

The Certified Information Security Manager Continuing Professional Education Policy

Table of Contents

Overview3
CISM Certification Requirements3
General Requirements	
Annual and Three-year Reporting Period	
Payment of CISM Maintenance Fee and Reporting of CPE Hours	
Notification of Annual Compliance	
Audit Of CPE Hours4
Recordkeeping4
Revocation4
Reconsideration and Appeal4
CISM Job Practice Areas4
Qualifying Professional Education Activities5
Formal Training and Learning	
Sharing of Professional Knowledge	
Calculating CPE Hours6
Contact Information6
Code Of Professional Ethics7
Verification Of Attendance Form8

The Certified Information Security Manager Continuing Professional Education Policy

Overview

The goal of the Certified Information Security Manager (CISM) Continuing Professional Education Policy is to ensure that all CISM maintain an adequate level of current knowledge and proficiency. CISM who successfully comply with the CISM Continuing Professional Education Policy will be better equipped to manage, design, oversee and assess an enterprise's information security.

The responsibility for setting the continuing professional education (CPE) requirements rests with the CISM Certification Board. The CISM Certification Board oversees the CPE process and requirements to ensure their applicability.

CISM Certification Requirements

General Requirements

The CISM Continuing Professional Education Policy requires the attainment of CPE hours over an annual and three-year certification period. CISM must comply with the following requirements to retain certification:

- Attain and report an annual minimum of twenty (20) CPE hours.
- Submit annual CPE maintenance fees to ISACA International Headquarters in full.
- Attain and report a minimum of one hundred and twenty (120) CPE hours for a three-year reporting period.
- Submit required documentation of CPE activities if selected for the annual audit.
- Comply with ISACA's Code of Professional Ethics.

Failure to comply with these certification requirements will result in the revocation of an individual's CISM certification.

Annual and Three-Year Certification Period

The annual reporting period begins on 1 January of each year. The three-year certification period varies and is indicated on each annual invoice and on the letter confirming annual compliance.

For newly certified CISM, the annual and three-year certification period begins on 1 January of the year succeeding certification. Reporting CPE hours attained during the year of certification is not required. However, hours attained between the date of certification and 31 December of that year can be used and reported as hours earned in the initial reporting period.

Payment of CISM Maintenance Fee and Reporting of CPE Hours

Payment of the maintenance fee and reporting of CPE hours is required annually. An invoice is mailed each October by ISACA® to all CISM. Payment and reporting of CPE hours is due by 15 January to retain certification.

Notification of Annual Compliance

CISM who report the required number of CPE hours and submit maintenance fees, in full, in a timely manner will receive a confirmation from ISACA. This confirmation will include the number of CPE hours accepted for the annual reporting period, hours reported for past years within the three-year certification period and the number of hours required to qualify for the fixed three-year certification period. It is the responsibility of each CISM to notify ISACA promptly of any errors or omissions in this confirmation.

The Certified Information Security Manager Continuing Professional Education Policy

Audit of CPE Hours

A random sample of CISM's is selected each year for audit. Those CISM's chosen must provide written evidence of previously reported activities that meet the criteria described in the Qualifying Professional Education Activities. The CISM Certification Board will determine the acceptance of hours for specific professional educational activities.

Recordkeeping

A CISM must obtain and maintain documentation supporting reported CPE activities. Documentation must be retained for a minimum of eighteen months following the end of each annual reporting period. Documentation should be in the form of a letter, certificate of completion, payment receipt, attendance roster, Verification of Attendance form (located in this policy) or other independent attestation of completion. At a minimum, each record should include the name of the attendee, name of the sponsoring organization, activity title, activity description, presenter name(s), activity date and location, and the number of CPE hours awarded or claimed.

Revocation

CISM's who fail to comply with the CISM Continuing Professional Education Policy will have their CISM credential revoked and will no longer be allowed to present themselves as a CISM.

Reconsideration and Appeal

CISM's who have had their certification revoked due to non compliance with certification requirements may appeal such revocation by submitting a written request to ISACA. This request must be received no later than sixty (60) days after notice of revocation and include a detailed explanation for the appeal. A copy of the CISM revocation appeal process is available from ISACA upon request.

CISM Job Practice Areas

- **Information Security Governance:** Establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations.
- **Risk Management:** Identify and manage information security risks to achieve business objectives.
- **Information Security Program(me) Management:** Design, develop and manage an information security program(me) to implement the information security governance framework.
- **Information Security Management:** Oversee and direct information security activities to execute the information security program(me).
- **Response Management:** Develop and manage a capability to respond to and recover from disruptive and destructive information security events.

For a description of task and knowledge statements for each area please refer to www.isaca.org/cismcont.htm.

The Certified Information Security Manager Continuing Professional Education Policy

Qualifying Professional Education Activities

The CISM Certification Board believes strongly in continuing education that emphasizes a combination of formal training and learning and the sharing of professional knowledge with other industry professionals. In order to encourage both types of activities, a required minimum number of hours must be acquired annually and during each three-year reporting period. Activities that qualify for CPE must be directly applicable to the management, design or assessment of an enterprise's information security (see CISM Job Practice Areas). CPE hours are not accepted for on-the-job activities unless they fall into a specific qualifying CPE activity. The following categories of qualifying activities and limits have been approved and are acceptable for CPE.

Formal Training and Learning

- **ISACA professional education activities and meetings:** These activities include ISACA conferences, seminars, workshops, programs, meetings and related activities. CISM's earn CPE hours according to the number of hours of active participation. (See Calculating CPE Hours section)
- **Non-ISACA professional education activities and meetings:** These activities include in-house corporate training, university courses, conferences, seminars, workshops, professional meetings and related activities not sponsored by ISACA. In addition, CPE hours can be earned from certification review courses if such courses advance the CISM's information security or managerial knowledge or skills. CISM's earn CPE hours according to the number of hours of active participation. (See Calculating CPE Hours section). However, successfully completed university courses earn 15 CPE hours per semester credit hour and 10 CPE hours per quarter credit hour (Semester = 15 weeks of class; quarter = 10 weeks of class).
- **Self-study courses:** These activities include structured courses designed for self-study that offer CPE hours. These courses will only be accepted if the course provider issues a certificate of completion and the certificate contains the number of CPE hours earned for the course.
- **Vendor sales/marketing presentations (10-hour annual limitation):** These activities include vendor product or system specific sales presentations.

Sharing of Professional Knowledge

- **Teaching/lecturing/presenting/fully accredited university research:** These activities include the development and delivery of professional educational presentations. CPE hours are earned at five times the presentation time for the first delivery (e.g.: two hour presentation earns ten CPE hours) and at the actual presentation time for the second delivery. CPE hours cannot be earned for subsequent presentations of the same material unless the content is substantially modified.
- **Publication of articles, monographs and books:** These activities include the publication or review of material (either hard copy or online) directly related to the management of information security. Submissions must appear in a formal publication or website and a copy of the article or the website address must be available, if requested. For books and monographs, the table of contents and title page must be available. CPE hours are earned for the actual number of hours taken to complete or review the material.

The Certified Information Security Manager Continuing Professional Education Policy

- **CISM exam item development and review:** This activity pertains to the development or review of items for the CISM examination or study aids. One CPE hour is earned for each question accepted by the CISM Certification Board. Actual hours will be given for the formal item review process.
- **Passing related professional examinations:** This activity pertains to the pursuit of other professional examinations. One CPE hour is earned for each examination hour when a passing score is achieved.
- **Participating in professional associations (10-hour annual limitation):** These activities include active participation on an information security professional board, committee or task force. One CPE hour is earned for each hour of active participation.
- **Contributions to the information security profession (10-hour annual limitation):** These activities include work performed for ISACA and other bodies that contribute to the information security profession (i.e. research development, CISM certification review manual development, K-Net development).

Calculating CPE Hours

One CPE hour is earned for each fifty minutes of active participation (excluding lunches and breaks) in a professional educational activity. **Continuing professional education hours are only earned in full-hour increments and rounding must be down.** For example, a CISM who attends an eight-hour presentation (480 minutes) with 90 minutes of breaks will earn seven (7) CPE hours.

Sample Calculation

Educational Activity Schedule	Actual Hours	Minutes
9:00 a.m. – 5:00 p.m.	8.0	480
Less: Two 15-minutes breaks	<.5>	<30>
Less: Lunch – 1 hour	<1.0>	<60>
Total hours of professional education	6.5	390

Calculation of CPE Hours

390 minutes divided by 50 minutes = 7.8 or 7 CE hours (rounded down)

Contact Information

ISACA Certification Department
Information Systems Audit and Control Association
3701 Algonquin Road
Suite 1010
Rolling Meadows, Illinois 60008-3124 USA

Telephone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: certification@isaca.org

The Certified Information Security Manager Continuing Professional Education Policy

Information Systems Audit and Control Association Code of Professional Ethics

The Information Systems Audit and Control Association (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.

CISM

CERTIFIED INFORMATION
SECURITY MANAGER™

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



*Information Systems
Audit and Control
Association®*

3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008 USA