CISM FAQs

Why has ISACA developed an information security certification?
ISACA's name reflects its obligation to offer products, services and benefits not only to the information systems audit profession, but to those who play a vital role in information systems control as well. More than 20 years ago ISACA pioneered the Certified Information Systems Auditor (CISA) credential and has developed and offered training programs to information systems auditors, information security practitioners and those involved in information technology governance. Most recognized in the industry are a series of ISACA conferences that are known as CACS (computer audit, control and security). These programs are held each year worldwide and meet the educational needs of a wide variety of information systems professionals. In recent years, ISACA has undertaken other information security and IT control activities: increased focus on security in the *Information Systems Control Journal*, creation of the IT Governance Institute, and development of research in the privacy area. The maturity of ISACA membership and CISAs and their requested need for an information security credential that goes beyond the practitioner level has led ISACA to the development the CISM credential.

What will the CISM exam cover?
The CISM exam will cover five information security management areas, each of which is further defined and detailed through task and knowledge statements. The five areas are:

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 to implement the information security governance framework.
Information Security Management
Oversee and direct information security activities to execute the information security program.
Response Management
Develop and manage a capability to respond to and recover from disruptive and destructive information security events.

Clicking on the title of any of these five areas will take you to a list of specific task and knowledge statements that represent a current market perspective of what is performed and what should be known by information security managers and provides the basis for the CISM exam.

What is the CISM job practice analysis and how was it developed?
ISACA's philosophy toward certification is to measure individuals' ability and knowledge as it pertains to the performance of their job. As such, ISACA approached the creation of the CISM job practice analysis with the same care and rigor it always has devoted to CISA. To ensure the job practice analysis is reflective of the work performed by information security managers, ISACA appointed a working committee of information security experts to develop and validate a series of task and knowledge statements that properly describe this role. The work included the use of prominent industry leaders, subject matter experts and industry practitioners, all of which played a key role in the development of the CISM job practice analysis.

What are the qualifications to earn the CISM credential?

Qualifying for CISM requires a combination of four "e's": experience, ethics, education and examination. Specifically, the requirements are:

- Successful completion of the Certified Information Security Manager (CISM) exam
- Adherence to a code of professional conduct
- Commitment to continuing professional education
- Submission of verified evidence of a minimum of five years of information security work experience, with a minimum of three years of information security management work experience in three or more of the job practice areas. Waivers for general information security work experience are available, if certain education or certification requirements are met.

For further details, go to www.isaca.org/cismrequire.htm.

Who is eligible to become CISM certified and what makes CISM unique?
CISM is unique in the information security credential marketplace because it is designed specifically and exclusively for individuals who have experience managing an information security program. Experience requirements and the CISM exam are based on the experience required to competently perform the duties and responsibilities of an information security manager. These requirements and the tasks and knowledge that are tested were developed by information security leaders and later validated by subject matter experts and information security managers. The requirements are designed to measure an individual's *management* experience in information security situations, not general practitioner skills.

Will CISAs qualify for CISM?
The CISM certification program recognizes the achievement of the CISA credential as a baseline representation that an individual has gained general information security skill and knowledge. As such, CISAs receive a two-year general information security waiver. However, CISAs will not be eligible to earn a CISM unless they have the required experience and can demonstrate proficiency and practical knowledge in the role of an information security manager.

Go to www.isaca.org/cismrequire.htm#experience to learn how to earn CISM both through exam and through grandfathering.

Will CISSPs and other security credential holders qualify for CISM?
The CISM certification program recognizes the achievement of the CISSP credential as a baseline representation that an individual has gained general information security skill and knowledge, just as it does with individuals who have earned a CISA. As such, CISSPs receive a two-year general information security experience waiver. However, CISSPs will not be eligible to earn a CISM unless they have the required experience and can demonstrate proficiency and practical knowledge in the role of an information security manager. Holders of other, more specialized credentials, such as the SANS Global Information Assurance Certification (GIAC), Microsoft Security Systems Engineer (MCSE), CompTIA Security + Credential and the Disaster Recovery Institute Certified Business Continuity Professional (CBCP) also can receive a one-year general information security experience waiver.

How is CISM different from the other security certifications?
CISM differs from the many other security certifications by virtue of its experience requirements and focus on the job performed by an information security manager. Other security certifications are characterized by a focus on technical skills or platform- or product-specific knowledge, or they are aimed at the practitioner in the earlier years of their career. Only CISM targets the

information security *manager*—the individual who has progressed beyond the practitioner focus, whose emphasis is no longer technical or specialist skills, and who has moved on to the management of an enterprise's information security program. CISM is for the individual who must manage and oversee the enterprise's information security effort, including the practitioners, many of whom may hold other certifications the field offers.

The focus on management that makes CISM unique is demonstrated in its experience requirement, which calls for a minimum of *three* years in information security management, and in its exam focus that is based on the job practices performed by information security managers.

How is CISM different from the Certified Information Systems Security Practitioner (CISSP)?
Although there are many differences between the CISSP common body of knowledge and the CISM job practice areas, the most obvious differences is in the experience requirements. Only CISM requires information security management experience, in addition to general information security experience. CISSP has no such management requirement.

Earning the CISSP and/or the CISA credential is complementary to the attainment of the CISM credential and is encouraged.

What is CISM's grandfathering provision?
The grandfathering provision allows individuals who have an advanced number of years of experience managing an information security program to earn the CISM certification without taking the CISM exam. The grandfathering provision period is available only for a limited time that ends on 31 December 2003. After that, all CISM candidates, regardless of experience level, will be required to pass the CISM exam to qualify for CISM certification. The experience requirements are more stringent than for candidates taking the exam. Whereas the individual taking the exam must have *five* years of information security work experience, with at least *three* of those years in information security management experience in *three* or more of the job practice analysis areas, the grandfathering applicant must have a minimum of *eight* years of information security work experience, with at least *five* of those years in information security management work experience in *four* or more of the job practice analysis areas. Waivers for general information security work experience are available, if certain education or certification requirements are met.

For details, go to www.isaca.org/cismrequire.htm#grandfather.

When will the first CISM exam be held?
The first CISM exam will be in June 2003, at the same time and in the same worldwide locations where the CISA exam is held. The CISM exam will consist of 200 multiple-choice questions that cover the CISM job practice areas. In 2003, the exam will be offered in English only, however, future plans include the translation of the CISM exam into other languages based on demand and interest.

Can I take the CISM exam and CISA exam on the same day?
Since the CISM and CISA exams are geared to information systems professionals at different points in their career, the 2003 CISM and CISA exams will be held simultaneously. This means that an individual will not be able to sit for both exams. Individuals who are not currently practicing as an information security manager, but aspire to in the future, are encouraged first to earn the CISA designation.

What CISM exam study materials will be available and when?
A CISM Review Manual will be available in January 2003 to assist individuals to prepare for the CISM exam. The manual will feature detailed descriptions and explanations of task and knowledge statements and provide applicable information security management principles, practices and strategies with references to where additional guidance can be found. This manual will assist with exam preparation, but since the exam is based on information security management practices it must be used as a guide and not considered as an all-inclusive study source. CISM review courses also will be conducted by ISACA chapters on a limited basis.

What does the CISM continuing professional education program require?
In order to become and remain a CISM an individual must agree to comply with the CISM continuing professional education program. This program requires an individual to earn a minimum of twenty (20) hours annually and one hundred and twenty (120) hours every three years of continuing professional education. Specific activities and requirements are currently under development and will be published in January 2003. In addition, an annual maintenance fee of US $35 ISACA member and US $50 non-member will be required beginning in 2003. Individuals holding both a CISM and a CISA will receive a discount.

What if we as a chapter cooperate locally with the ISSA chapter or promote CISSP?
ISACA chapters are encouraged to maintain their relationships with ISSA/ISC(2). ISACA does not view CISM and CISSP as competitive, but rather complementary. We are all trying to serve the security market, but at different levels and in different ways; therefore it is in the best interests of all concerned to work together.

What are the grandfathering fees to be used for?
The CISM Certification Board determined that the fee charged for application as a CISM under the grandfathering provision should be set at an appropriate level above the cost of exam in order to generate the funds needed to initiate the certification program and to ensure that only serious candidates apply. These funds are, and will continue to be, used to fund the various start-up activities and expenses relating to the certification, including the development and validation of the job practice, program marketing and promotion, hiring administrative personnel to handle applications and inquiries, legal expenses, initial exam item and study guide development and funding CISM Certification Board meetings. Please note, CISM candidates can earn the funds to pay for their application fee by writing items for the CISM exam. By submitting and earning approval for five exam items (US $100 each), ISACA members can both pay for their grandfathering fees and strengthen the exam.