La Faq della certificazione CISM: le domande (e risposte) più frequenti

Questo documento è stato realizzato da Isaca Roma, www.isacaroma.it; questa è la versione del 12 dicembre 2002.
(la versione originale in inglese è disponibile in: http://www.isaca.org/cismfaq.htm , la pagina ISACA su Cism: http://www.isaca.org/cism.htm)

Perché ISACA ha proposto una certificazione di sicurezza informatica?
La missione dell'ISACA, così come è indicato chiaramente dal suo nome (*Information Systems Audit and Control Association*), indica che ci si rivolge non solo ai professionisti dell' IS Auditing ma a tutti coloro che si occupano del controllo dei sistemi informativi. Più di 20 anni fa l'ISACA propose la certificazione CISA (Certified Information Systems Auditor) e da allora ha garantito formazione e informazione di alto livello agli information systems auditor, agli esperti di information security e a coloro che si occupano di information technology governance. Le conferenze ISACA, note come CACS (computer audit, control and security), sono molto apprezzate nel settore. Negli ultimi anni ISACA ha intrapreso ulteriori attività nel campo della Information Security e dell' IT Control: l'Information Systems Control Journal, l'IT Governance Institute e numerose ricerche nell'area della privacy. Da parte di coloro che sono certificati CISA, infine, è giunta la richiesta di creare una nuova certificazione relativa alla Information Security per cui ISACA ha proposto la certificazione CISM.

Su che aree della sicurezza informatica si focalizza CISM?
L'esame CISM si focalizza su cinque aree dell' information security management, aree note come ***job practice areas***, ciascuna delle quali è ulteriormente definita in task e knowledge statement. Le cinque aree sono:

Information Security Governance
Si concentra sul framework che garantisce che le strategie di information security siano in linea con gli obiettivi di business e coerenti con le normative generali e gli standard di settore.
Risk Management
Riguarda l'identificazione e la gestione dei rischi dell' information security al fine di garantire gli obiettivi di business.
Information Security Program(me) Management
Si occupa del disegno, sviluppo e gestione dei programmi di information security al fine di implementare il framework dell'information security governance.

Information Security Management
Riguarda le attività di sicurezza per rendere esecutivo il programma di information security.
Response Management
Sviluppo e gestione delle capacità di rispondere ad eventi distruttivi per la sicurezza informatica in termini di ripristino e recovery.

Maggiori informazioni su ciascuna area sono disponibili (in inglese) selezionando il link del titolo di ciascuna area.

Cosa sono le CISM job practice analysis areas e come sono state sviluppate?
ISACA ha istituito un working committee per proporre e validare una serie di task e knowledge statement che qualificassero il ruolo di Security Manager. Tale comitato ha individuato 5 aree di competenza per la certificazione CISM, aree note come job practice analysis areas.

Che qualifiche sono richieste per ottenere la certificazione CISM?
La certificazione CISM può essere sintetizzata in quattro "e": esperienza, etica, *education* (formazione), esame. Più in particolare i requisiti per la certificazione sono:

- Esperienza pluriennale nell'ambito della sicurezza;
- Superamento dell'esame Certified Information Security Manager (CISM);
- Aderenza al codice di condotta professionale;
- Garanzia di una formazione professionale continua (CPE - *Continuing Professional Education*).

Occorre, in particolare, un'esperienza minima di cinque anni nell'ambito dell' information security, con tre anni specifici in almeno tre delle *job practice areas*.

Maggiori informazioni sui requisiti CISM (in inglese):
http://www.isaca.org/cismrequire.htm

Cosa rende CISM unico?
CISM è unico perché è stato concepito per chi ha maturato un'esperienza significativa nel Security Management. I requisiti richiesti, insieme al corpus delle conoscenze necessarie, qualificano chi è certificato CISM come un Manager piuttosto che come un semplice esperto di sicurezza.

La certificazione CISA qualifica anche per CISM?
Il programma per la certificazione CISM riconosce che l'ottenimento della certificazione CISA rappresenta una base di conoscenza generale per la information security e dunque tale titolo è conteggiato come un'ulteriore esperienza di due anni. La certificazione CISA, da sola, non è però sufficiente per completare i requisiti richiesti: occorre in ogni caso un'esperienza effettiva nel campo del Security Management e superare l'esame.

Maggiori informazioni sull'esperienza richiesta per sostenere CISM (in inglese):
http://www.isaca.org/cismrequire.htm#experience

La certificazione CISSPs o altre certificazioni di sicurezza qualificano anche per CISM?
Il programma per la certificazione CISM riconosce che l'ottenimento della certificazione CISSP rappresenta una base di conoscenza generale per la information security, così come la certificazione CISA, e dunque tale titolo è conteggiato come un'ulteriore esperienza di due anni. La certificazione CISSP, da sola, non è però sufficiente per completare i requisiti richiesti: occorre in ogni caso un'esperienza effettiva nel campo del Security Management e superare l'esame. Altre certificazioni specifiche per la sicurezza quali *SANS Global Information Assurance Certification* (GIAC), *Microsoft Security Systems Engineer* (MCSE), *CompTIA Security + Credential* e *Disaster Recovery*

Institute Certified Business Continuity Professional (CBCP) sono conteggiate come un anno di esperienza.

Cosa rende CISM differente dalle altre certificazioni di sicurezza?
CISM differisce dalle altre certificazioni di sicurezza in virtù dei requisiti richiesti; le altre certificazioni hanno un focus sugli skill tecnologici o sulla conoscenza di particolari piattaforme o prodotti e sono rivolte ai professionisti con pochi anni d'esperienza, generalmente all'inizio della loro carriera. CISM, viceversa, si rivolge a chi ha maturato esperienze manageriali nella sicurezza.

Qual è la differenza fra CISM e CISSP (Certified Information Systems Security Professional)?
Sebbene esistano molte differenze tra il *corpus* delle conoscenze (*Common Body of Knowledge* – CBK) richiesto per sostenere l'esame CISSP e le *job practice areas* di CISM, la vera differenza consiste nei requisiti d'esperienza professionale richiesti. CISM richiede un'esperienza specifica nel security management oltre ad una esperienza generale nella sicurezza. CISSP non ha tale requisito.
In ogni caso, la certificazione CISSP (e/o CISA) è complementare alla certificazione CISM ed il suo ottenimento è incoraggiato.

Cos'è il CISM grandfathering provision?
Il grandfathering provision permette alle persone con un gran numero d'anni d'esperienza nella sicurezza e nel management della sicurezza di ottenere la certificazione CISM senza sostenere l'esame. Il periodo di grandfathering provision si concluderà il 31 Dicembre 2003. Dopo questa data a tutti i candidati CISM, quale che sia il loro livello d'esperienza, sarà richiesto di superare l'esame. I requisiti d'esperienza richiesti per il grandfathering sono più severi rispetto a chi sostiene l'esame. Mentre chi sostiene l'esame deve avere cinque anni d'esperienza nella sicurezza IT, ed almeno tre di questi cinque anni si devono riferire a tre o più job practice analysis areas, chi invece richiede il grandfathering deve avere un minimo di 8 anni di esperienza nel campo della sicurezza ed almeno 5 di questi anni relativi al security management in quattro o più delle aree del job practice analysis. Gli anni di esperienza richiesti possono essere ridotti se si è in possesso di titoli universitari o altre certificazioni di sicurezza.

Maggiori informazioni sul grandfathering (in inglese):
http://www.isaca.org/cismrequire.htm#grandfather

Quando è previsto il primo esame CISM?
Il primo esame Cism avrà luogo nel giugno 2003 contemporaneamente e negli stessi luoghi ove si svolgerà l'esame CISA. L'esame CISM consisterà di 200 domande a risposta multipla che coprono le CISM *job practice areas.* Nel 2003 sarà possibile sostenere l'esame solo in inglese ma in futuro è previsto l'uso anche di altre lingue (se sarà richiesto).

E' possibile sostenere l'esame CISM e l'esame CISA lo stesso giorno?
Si presuppone che gli esami CISM e CISA siano sostenuti in momenti diversi del proprio percorso professionale e dunque nel 2003 gli esami CISM e CISA si terranno in contemporanea per cui non sarà possibile sostenerli entrambi. Si incoraggia chi fosse intenzionato sostenere in futuro l'esame CISM a cominciare con la certificazione CISA.

In che modo e quando sarà disponibile il materiale di studio per l'esame CISM?
Il CISM *Review Manual* sarà disponibile nel gennaio 2003 per assistere chi si prepara per l'esame CISM. Il manuale conterrà le descrizioni dettagliate dei task e knowledge statement delle job practice analysis areas e fornirà i principi dell' information security management, le *practices* e strategie generali con i riferimenti su dove trovare ulteriori materiali di approfondimento. Questo

manuale sarà utile per la preparazione all'esame non deve esser considerato l'unica fonte di preparazione. I capitoli locali ISACA organizzeranno infine corsi di preparazione all'esame CISM.

In che consiste il CISM *Continuing Professional Education Program*?
Al fine di conseguire e e mantenere la certificazione CISM deve essere garantita una formazione professionale continua. Si richiede di effettuare un minimo di venti (20) ore l'anno e di almeno centoventi (120) ore ogni tre anni di formazione professionale nell'ambito della sicurezza. Le caratteristiche di tali attività formative saranno rese note nel gennaio 2003. E' inoltre richiesto una fee annuale di mantenimento di dollari USA 35 per gli associati ISACA e di dollari USA 50 per i non associati a partire dal 2003. E' previsto uno sconto per chi è certificato sia CISA che CISM.

Isaca Roma è il capitolo di Roma dell'ISACA (www.isacaroma.it)