SearchSecurity.com

SearchSecurity.com's IT security certifications guide

Guide to information security certifications

Check out the other guides in this series:

SearchSecurity.com's guide to vendor-neutral security certifications

SearchSecurity.com's guide to vendor-specific security certifications

This special report offers a comprehensive review of information security industry certifications, highlighting which ones can best help you achieve goals specific to your information security career path. It's a companion to two other surveys, which cover the vendor-neutral and vendor-specific security certification landscapes in detail.

For this update to our IT security certifications guide, we made several changes. The following table shows our reporting by the numbers for the previous April 2012 edition as well as this May 2013 edition. The overall numbers for vendor-neutral information security certifications went up by three (in total, we added **five** more credentials to our various lists, but scrubbed **two** old ones, for an **overall net gain of three**).

Counts	2012	2013
General	*49*	*54*
Basic	14	15
Intermediate	7	8
Advanced	28	31
Forensics/Antihacking	*24*	*23*
Basic	10	9
Intermediate	8	8
Advanced	6	6
Specialized	*10*	*9*
TOTALS	**83**	**86**

Since the last revision to this material, there's less change than in any of the five previous such surveys we’ve conducted. We removed two EC-Council credentials – the Certified Secure Application Developer (CSAD) and the ESCP (EC-Council Certified Secure Programmer). To make up for those losses, however, we added the CompTIA Advanced Security Practitioner (CASP) and the Prometric Cyber Security Fundamentals credential, plus three more advanced GIAC credentials (GSSP-JAVA, GREM, and GSE). For the first time ever, this resulted in a small overall delta. It’s starting to look like the information security certification sector is maturing, and may no longer be subject to large-scale entries or defections.

Even so, the sheer number of credentials can make navigating the security certification landscape a dizzying experience. Simply identifying and differentiating among the vast array of offerings can be time-consuming and overwhelming, never mind determining which certification best fits your needs. This SearchSecurity.com guide to information security certifications provides a comprehensive overview of myriad information security certification options. It's intended for anyone looking to get on the information security certification path, whether you're starting up the information security career ladder or already have security experience and wish to hone your skills in some specialized area.

After you have perused the options available to you, visit SearchSecurity.com's CISSP Essentials Security School for resources to help you prepare for the CISSP exam and expand your knowledge of information security practices. If you have feedback on how we can improve this guide to information security certifications, please let us know.

Table of contents

General security -- Basic

Return to Table of Contents

Brainbench Basic Security Certifications
Brainbench offers several basic-level security certifications, each requiring the candidate to pass one exam. Examples of these certifications include:

- Brainbench Firewall Administration Concepts

- Brainbench Internet Security
- Information Technology Security Fundamentals
- ITAA Information Security Awareness
- Brainbench Microsoft Security
- Brainbench Network Authentication
- Brainbench Network Security
- Security Industry Knowledge (U.S.)

Source: Brainbench

CDRE -- Certified Disaster Recovery Engineer
This credential from Iowa-based training company mile2 recognizes individuals with foundational knowledge of disaster recovery (DR) and business continuity (BC) planning methodologies. A CDRE recognizes real-world risks and vulnerabilities to an IT infrastructure, understands how to safeguard assets against threats, and can write DR and BC plans and policies. No prerequisites or classes are required.

Source: mile2

CERT-CCSIH -- CERT-Certified Computer Security Incident Handler
The CERT-CCSIH credential recognizes security professionals who are knowledgeable of and skilled in network monitoring and risk assessments, vulnerability scanning and other infrastructure protection techniques, incident detection and incident response. Candidates must have one or more years of recent experience in incident handling in a technical and/or management role, submit a certification recommendation form signed by a current manager, and pass one exam. The credential is valid for three years.

Source: SEI Carnegie Mellon

CISSO -- Certified Information Systems Security Officer
This credential from mile2 recognizes individuals who can apply risk analysis and mitigation techniques, application security, secure networks and operations, and plan for business continuity and disaster recovery. A CISSO can assess an IT infrastructure for today's threats and risks, and design a security program to mitigate those risks. The CISSO is mile2's alternative to the $(ISC)^2$ CISSP.

Source: mile2

GISF -- GIAC Information Security Fundamentals Certification
This certification is part of the Global Information Assurance Certification Program (described in the "General security – Intermediate" section of this article). The GISF identifies individuals with foundational knowledge of information assurance, such as risk management, defense-in-depth techniques, security policies, disaster recovery and business

continuity. No training or prerequisites are required. Candidates must pass one exam, and the certification is valid for four years.

Source: Global Information Assurance Certification

Prometric **Cyber Security Essentials** (no acronym)
This credential represents a brand-new entrant into the information security fundamentals mix, and is designed to compete directly against the CompTIA Security+ certification (CompTIA abandoned its long-standing test center relationship with Prometric in 2012, and now offers its exams exclusively at VUE testing centers). The areas that this credential covers include general information security, application security, governance and compliance, operational security, network security, physical security, environmental security, and vulnerability management.

Source: Prometric

Security+
This security certification focuses on important security fundamentals related to security concepts and theory, as well as best operational practices. In addition to functioning as a standalone exam for CompTIA, Security+ is part of the requirements for the IBM Certified Advanced Deployment Professional - IBM Service Management Security and Compliance V4 and some Security University certifications.

Source: CompTIA

SSCP -- Systems Security Certified Practitioner
The entry-level precursor to $(ISC)^2$'s CISSP, the SSCP exam covers seven of the 10 domains in the CISSP Common Body of Knowledge (CBK). The exam focuses more on network and administration aspects of information security that are germane to the duties of a day-to-day security administrator, as opposed to the issues of information policy implementation, architecture design and application development security that senior IT security professionals are more likely to handle. Candidates must have at least one year of experience in one or more of the seven domains of the SSCP CBK. $(ISC)^2$ offers the Associate of $(ISC)^2$ credential for candidates who pass the CAP, CISSP, CSSLP or SSCP exam but do not yet meet the experience requirement.

Source: $(ISC)^2$

General security -- Intermediate

Return to Table of Contents

BISA -- Brainbench Information Security Administrator

This certification tests knowledge of networking and Internet security, including authorization, authentication, firewalls, encryption, disaster recovery and more. Candidates must pass eight exams to obtain this certification.

Source: Brainbench

CAP -- Certified Authorization Professional

The CAP aims to identify individuals who can assess and manage the risks that security threats may pose within an organization, particularly in the government and enterprise sectors. This is a credential that lies deals with processes and practices, and works in tandem with emerging compliance requirements (Sarbanes-Oxley and HIPAA, among others) as well as emerging best industry governance standards (Information Technology Infrastructure Library, or ITIL). Candidates must have two years of full-time experience in one or more of the seven domains of the CAP Common Body of Knowledge (CBK). Candidates must also prove experience with Certification & Accreditation while working as a practitioner, an auditor or a contractor. (ISC)^2 offers the Associate of (ISC)^2 credential for candidates who pass the CAP, CISSP, CSSLP or SSCP exam but do not yet meet the experience requirement.

Source: (ISC)^2

CSSLP -- Certified Secure Software Lifecycle Professional

The CSSLP recognizes individuals who specialize in software security across the lifecycle, from conceptualization through design, during coding and testing, and deployment. Candidates must have at least four years of direct experience in the software development lifecycle (SDLC), agree to adhere to a code of ethics, answer questions regarding criminal history and background and pass one exam.

Source: (ISC)^2

CWSP -- Certified Wireless Security Professional

This certification recognizes individuals who can design, implement and manage wireless LAN security. To obtain this credential, candidates must pass two exams.

Source: CWNP

GIAC -- Global Information Assurance Certification Program

This program seeks to identify individuals who can demonstrate both knowledge of and the ability to manage and protect important information systems and networks. The SANS organization is well known for timely, focused and useful security information and certification programs. A beacon on this landscape, GIAC now offers regular online classes and uses such classes to draw attendees to their frequent well-situated week-long conferences. Overall, the GIAC program aims at serious, full-time security professionals responsible for designing, implementing and maintaining a state-of-the-art security infrastructure, which may include incident handling and emergency response team management. Available intermediate-level GIAC credentials include the following:

- GIAC Security Essentials Certification (GSEC)
- GIAC Information Security Professional (GISP)
- GIAC Certified ISO-27000 Specialist (G2700)

General security -- Advanced

Return to Table of Contents

CASP – CompTIA Advanced Security Practitioner
The CASP is one of a few advanced credentials that CompTIA offers, and it has been accredited as a valid credential under the U.S. Department of Defense 8570.01-M Directive designed to prepare the information assurance (government-speak for information security) workforce to prevent and respond to attacks against the agency's and its contractors' information, information systems, and information infrastructures. This exam seeks to cover technical skills and knowledge needed to conceptualize, design, and implement secure solutions across complex enterprise environments (see exam objectives for more info).

Source: CompTIA

CISM -- Certified Information Security Manager
The CISM demonstrates knowledge of information security for IT professionals responsible for handling security matters, issues and technologies. This cert is of primary interest to IT professionals responsible for managing IT systems, networks, policies, practices and procedures to make sure organizational security policies meet governmental and regulatory requirements, conform to best security practices and principles, and meet or exceed requirements stated in an organization's security policy.

Source: Information Systems Audit and Control Association (ISACA)

CISSP -- Certified Information Systems Security Professional
The CISSP demonstrates knowledge of network and system security principles, safeguards and practices. It is of primary interest to full-time IT security professionals who work in internal security positions or who consult with third parties on security matters. CISSPs are capable of analyzing security requirements, auditing security practices and procedures, designing and implementing security policies, and managing and maintaining an ongoing and effective security infrastructure. CISSP candidates must have five years of experience in two or more of the 10 domains of the CISSP CBK (or a college degree plus four years of experience). (ISC)^2 offers the Associate of (ISC)^2 credential for candidates who pass the

CAP, CISSP, CSSLP or SSCP exam but do not yet meet the experience requirement.

Source: (ISC)²

CPP -- Certified Protection Professional
The CPP demonstrates a thorough understanding of physical, human and information security principles and practices. The most senior and prestigious IT security professional certification covered in this article, the CPP requires extensive on-the-job experience (nine years, or seven years with a college degree), as well as a profound knowledge of technical and procedural security topics and technologies. Only those who have worked with and around security for a lengthy portion of their careers are able to qualify for this credential.

Source: ASIS International

CPTE -- Certified Pen Testing Engineer
An offering from mile2, this credential stresses currency on the latest exploits, vulnerabilities and system penetration techniques. It also focuses on business skills, identification of protection opportunities, testing justifications and optimization of security controls to meet business needs and control risks and exposures. The credential is structured around a five-day course that's backed up by the CPT Engineer exam, offered online by mile2.

Source: mile2

GIAC -- Global Information Assurance Certification Program
This SANS cert program (described previously in this article) seeks to identify individuals who can demonstrate both knowledge of and the ability to manage and protect important information systems and networks. Available advanced certifications include the following:

- GIAC Certified Firewall Analyst (GCFW)
- GIAC Certified Intrusion Analyst (GCIA)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified UNIX Security Administrator (GCUX)
- GIAC Certified Windows Security Administrator (GCWN)
- GIAC Certified Enterprise Defender (GCED)
- GIAC Certified Penetration Tester (GPEN)
- GIAC Web Application Penetration Tester (GWAPT)
- GIAC Security Leadership (GSLC)
- GIAC Certified Project Manager (GCPM)
- GIAC Legal Issues (GLEG)
- GIAC Systems and Network Auditor (GSNA)
- GIAC Secure Software Programmer - .NET (GSSP-NET)
- GIAC Secure Software Programmer Java (GSSP-JAVA)

Highly advanced-level certifications include the following:

- GIAC Assessing Wireless Networks (GAWN)
- GIAC Exploit Researcher and Advanced Penetration Tester GXPN
- GREM: GIAC Reverse Engineering Malware

Source: Global Information Assurance Certification and GIAC Certifications Roadmap

The GIAC Security Engineer (GSE) track is the most senior-level certification in that program. To qualify for this certification, candidates must complete three intermediate-level GIAC certifications -- GSEC, GCIA and GCIH -- earning GIAC Gold in at least two of them, pass a proctored multiple-choice exam, and successfully complete a two-day hands-on lab.

GSE Source: Global Information Assurance Certification

ISSAP -- Information Systems Security Architecture Professional
The ISSAP permits CISSPs to concentrate further in information security architecture and stresses the following elements of the CBK:

- Access control systems and methodologies
- Communications and network security
- Cryptography
- Security architecture analysis
- Technology-related business continuity and disaster recovery planning (BCP and DRP)
- Physical security considerations

Source: (ISC)^2

ISSEP -- Information Systems Security Engineering Professional
The ISSEP permits CISSPs who work in areas related to national security to concentrate further in security engineering, in cooperation with the U.S. National Security Agency (NSA). The ISSEP stresses the following elements of the CBK:

- Systems security engineering
- Certification and accreditation (C&A) and risk management framework (RMF)
- Technical management
- U.S. government information assurance governance

Source: (ISC)^2

ISSMP -- Information Systems Security Management Professional

The ISSMP permits CISSPs to concentrate further in security management areas and stresses the following elements of the CBK:

- Enterprise security management practices
- Enterprise-wide system development security
- Overseeing compliance of operations security
- Understanding BCP and DRP
- Law, investigations, forensics and ethics

Source: (ISC) 2

PSP -- Physical Security Professional
Another high-level security certification from ASIS, this program focuses on matters relevant to maintaining security and integrity of the premises, and access controls over the devices and components of an IT infrastructure. Key topics covered include physical security assessment, and selection and implementation of appropriate integrated physical security measures. Requirements include four years of experience in progressive physical security, and a bachelor's degree or higher from an accredited institution of higher education or a high school diploma (or GED) and six years of experience in progressive physical security.

Source: ASIS International

QIAP -- Qualified Information Assurance Professional
Security University's QIAP certification combines coverage of key information security topics, tools and technologies with a hands-on, lab-oriented learning and testing program. To obtain QIAP certification, security professionals must complete three courses on topics such as:

- Access, authentication and public key infrastructure (PKI)
- Network security policy and security-oriented architecture
- Security certification and accreditation

Students must also take and pass three exams, one per course.

Source: Security University

QISP -- Qualified Information Security Professional
Security University's QISP certification combines coverage of key information security topics, tools and technologies with a hands-on, lab-oriented learning and testing program. SU offers the QISP certification with four concentrations: analyst/penetration tester, ethical hacker, forensics and network protection. To obtain the QISP certification, security professionals must complete four courses, according to their concentration. Students must

also take and pass a demanding exam.

Source: Security University

QSSE -- Qualified Software Security Expert
Security University's QSSE certification combines coverage of key software security topics, tools and technologies with a hands-on, lab-oriented learning and testing program. To obtain QSSE certification, security professionals must complete a software security boot camp and seven courses on topics such as:

- Penetration testing
- Breaking and fixing Web applications
- Breaking and fixing software
- Secure software programming
- Software security ethical hacking
- Software security testing best practices
- Reverse engineering

Source: Security University

Forensics/Antihacking -- Basic

Return to Table of Contents

BCF -- Computer Forensics (U.S.)
The Computer Forensics (U.S.) certification is designed for experienced individuals who can analyze and collect evidence, recognize data types, follow proper examination procedures and initial analysis, use forensic tools and prepare for an investigation and report findings.

Source: Brainbench

CCCI -- Certified Computer Crime Investigator (Basic)
The CCCI is one of four computer forensic certifications aimed at law enforcement and private-sector IT professionals seeking to specialize in the investigative side of the field. Basic requirements include three years of experience (law enforcement or corporate), 40 hours of computer crimes training and documented experience from at least 10 case investigations.

Source: High Tech Crime Network

CCFT -- Certified Computer Forensic Technician (Basic)
The CCFT is one of four computer forensic certifications aimed at law enforcement and private IT professionals seeking to specialize in the investigative side of the field. Basic

requirements include three years of experience (law enforcement or corporate), 40 hours of computer forensics training and documented experience from at least 10 case investigations.

Source: High Tech Crime Network

CDFE – Certified Digital Forensics Examiner
The CDFE is aimed at cybercrime investigators who must work with digital evidence and use electronic discovery techniques. Exam topics may include disk storage, seizure and collection techniques, forensic examination, artifact recovery and more. No prerequisites or courses are required, but some hands-on experience will benefit the certification candidate.

Source: mile2

ECIH -- EC-Council Certified Incident Handler
The ECIH is geared toward incident handlers, risk assessment administrators, penetration testers, cyberforensic investigators, vulnerability assessment auditors, system administrators, system engineers, firewall administrators, network managers, IT managers and IT professionals, among others. To obtain ECIH certification, a candidate needs to complete a two-day course and pass one exam.

Source: EC-Council

ECVP -- EC-Council Certified VoIP Professional
The ECVP identifies individuals with experience in VoIP technologies concepts, implementation, deployment and security. To obtain ECVP certification, a candidate needs to pass one exam.

Source: EC-Council

EDRP -- EC-Council Certified Disaster Recovery Professional
The EDRP identifies individuals with experience developing disaster recovery plans in an enterprise environment. This includes creating a secure network by implementing appropriate policies and procedures, and restoring a network in the event of a disaster. To obtain EDRP certification, a candidate must take a two-day course and pass one exam.

Source: EC-Council

ENSA -- EC-Council Network Security Administrator
The NSA identifies individuals who can evaluate internal and external security threats against a network, and develop and implement security policies. One exam is required to obtain this certification.

Source: EC-Council

GCFE -- GIAC Certified Forensic Examiner

This certification is part of the Global Information Assurance Certification Program. The GCFE identifies professionals with the required skills for collecting and analyzing data from Windows computers. The certification is geared toward professionals in the information security profession and legal and law enforcement industries. No training or prerequisites are required. Candidates must pass one exam, and the certification is valid for four years.

Source: Global Information Assurance Certification

Forensics/Antihacking -- Intermediate

Return to Table of Contents

CCE -- Certified Computer Examiner

The CCE, administered by the International Society of Forensic Computer Examiners, seeks to identify individuals with no criminal record who have appropriate computer forensics training or experience, including evidence gathering, handling and storage. In addition, candidates must attend authorized training, have 18 months of experience conducting digital forensic examinations, have documented self-study in digital forensics deemed appropriate by the Certification Board, pass an online examination, have no criminal record and successfully perform a hands-on examination.

Source: International Society of Forensic Computer Examiners

CEH -- Certified Ethical Hacker

The CEH identifies security professionals capable of finding and detecting weaknesses and vulnerabilities in computer systems and networks by using the same tools and applying the same knowledge as a malicious hacker. Candidates must pass a single exam, and take approved training or complete an eligibility form.

Source: EC-Council

CFCE -- Certified Forensic Computer Examiner

The International Association of Computer Investigative Specialists (IACIS) offers this credential to law enforcement and private industry personnel alike. Candidates must have broad knowledge, training or experience in computer forensics, including forensic procedures and standards, as well as ethical, legal and privacy issues. Certification requires an intensive peer review, hands-on performance-based testing, as well as a written exam.

Source: International Association of Computer Investigative Specialists

CHFI -- Computer Hacking Forensic Investigator

The CHFI is geared toward personnel in law enforcement, defense, military, information technology, law, banking and insurance, among others. To obtain CHFI certification, a candidate needs to successfully complete one exam.

Source: EC-Council

CNDA -- Certified Network Defense Architect
The CNDA is geared toward IT personnel who act as penetration testers or legitimate hackers to test the strength and integrity of a network's defense. The CNDA exam is identical to the CEH exam; however, the CNDA program was designed for U.S. government agencies. To obtain CNDA certification, a candidate needs to successfully complete one exam and be employed by the U.S. government.

Source: EC-Council

CSFA -- CyberSecurity Forensic Analyst
The CSFA aims to identify individuals who can perform a comprehensive and sound forensic examination of a computer system and other digital/electronic devices within a limited time frame. Suggested prerequisites include attendance of the CyberSecurity Institute's Computer Forensics Core Competencies course and/or at least one of the following certifications:

- AccessData Certified Examiner (ACE)
- Certified Forensic Computer Examiner (CFCE)
- Certified Computer Examiner (CCE)
- Computer Hacking Forensic Investigator (CHFI)
- EnCase Certified Examiner (EnCE)
- GIAC Certified Forensics Analyst (GCFA)

In addition, candidates should have at least two years of experience performing forensic analysis of Windows FAT and NTFS file systems and writing forensic analysis reports. Candidates must have no criminal record.

Source: CyberSecurity Institute

ECSA -- EC-Council Certified Security Analyst
The ECSA identifies security professionals capable of using advanced methodologies, tools and techniques to analyze and interpret security tests. Candidates must pass a single exam to achieve the certification. The EC-Council recommends candidates take a five-day training course to prepare for the exam.

Source: EC-Council

GCFA -- GIAC Certified Forensics Analyst
This certification is part of the Global Information Assurance Certification Program. The

GCFA identifies professionals with the required skills for collecting and analyzing data from Windows and Linux computers. Professionals holding the GCFA have the ability to conduct formal incident investigations and take a lead role in responding to security incidents. No training or prerequisites are required. Candidates must pass one exam, and the certification is valid for four years.

Source: Global Information Assurance Certification

Forensics/Antihacking -- Advanced

Return to Table of Contents

CCCI -- Certified Computer Crime Investigator (Advanced)

The CCCI is one of four computer forensic certifications aimed at law enforcement and private IT professionals seeking to specialize in the investigative side of the field. Advanced requirements entail five years of experience (law enforcement or corporate), 80 hours of training, involvement as a lead investigator in 20 cases with involvement in over 60 cases overall, and documented experience from at least 15 investigated cases.

Source: High Tech Crime Network

CCFT -- Certified Computer Forensic Technician (Advanced)

The CCFT is one of four computer forensic certifications aimed at law enforcement and private IT professionals seeking to specialize in the investigative side of the field. Basic requirements include five years of experience, 80 hours of computer forensics training, involvement as a lead investigator in 20 cases with involvement in over 60 cases overall, and documented experience from at least 15 investigated cases.

Source: High Tech Crime Network

CPTC -- Certified Pen Testing Consultant

This credential stresses up-to-date knowledge of the latest exploits, vulnerabilities and system penetration techniques. It also focuses on business skills, identification of protection opportunities, testing justifications and optimization of security controls to meet business needs and control risks and exposures. The CPTC covers many of the same topics as the lower-level CPTE certification but in much more depth and breadth. The CPT Consultant credential is structured around a five-day course that's backed up by the CPT Consultant exam, delivered online by mile2.

Source: mile2

GREM -- GIAC Reverse Engineering Malware

This certification is part of the Global Information Assurance Certification Program. The

GREM identifies technologists who are experts in malicious codes and how they affect forensic investigations, incident response and Windows system administration. An individual holding a GREM certification thoroughly understands reverse engineering of malware associated with Microsoft Windows and Web browsers. No training or prerequisites are required. Candidates must pass one exam, and the certification is valid for four years.

Source: Global Information Assurance Certification

LPT -- Licensed Penetration Tester
The LPT identifies security professionals who can thoroughly analyze a network, identify where and how it could be potentially penetrated, and recommend appropriate corrective measures. An LPT must adhere to a strict code of ethics, best practices and appropriate compliance requirements while performing penetration tests. Prerequisites include EC-Council's CEH and ECSA certifications, a valid EC-Council Continuing Education account, submission of the LPT application, proof of a clean background check, detailed resume, an agreement to abide by a code of ethics and payment of a license fee.

Source: EC-Council

PCI -- Professional Certified Investigator
This is a high-level certification from the American Society for Industrial Security (ASIS is also home to the CPP and PSP certifications) for those who specialize in investigating potential cybercrimes. Thus, in addition to technical skills, this certification concentrates on testing individuals' knowledge of legal and evidentiary matters required to present investigations in a court of law: including case management, evidence collection and case presentation. This cert requires five years of investigation experience, with at least two years in case management, a high school diploma (or GED) and a clean criminal record.

Source: ASIS International

Specialized

Return to Table of Contents

CCSA -- Certification in Control Self-Assessment
The CCSA demonstrates knowledge of internal control self-assessment procedures, primarily aimed at financial and records controls. This cert is of primary interest to those professionals who must evaluate IT infrastructures for possible threats to financial integrity, legal requirements for confidentiality, and regulatory requirements for privacy. Candidates must have a four-year college degree or a two-year college degree with one year of control-related business experience, such as: CSA, auditing, quality assurance, risk management or environmental auditing. In addition, CCSA candidates must obtain seven hours of

acceptable facilitation experience or at least 14 hours of acceptable facilitation training, and submit a character reference. To obtain this certification, candidates must pass an exam.

Source: Institute of Internal Auditors

CFE -- Certified Fraud Examiner
The CFE demonstrates ability to detect financial fraud and other white-collar crimes. This cert is of primary interest to full-time security professionals in law, law enforcement or those who work in organizations with legal mandates to audit for possible fraudulent or illegal transactions and activities (such as banking, securities trading or classified operations). The CFE has a long list of qualifications and prerequisites, and eligibility for the credential is based on a point system.

Source: Association of Certified Fraud Examiners

CFSA -- Certified Financial Services Auditor
The CFSA identifies professional auditors with thorough knowledge of auditing principles and practices in the banking, insurance and securities financial services industries. Candidates must have a four-year college degree or a two-year college degree with three years of experience in a financial services environment, submit a character reference and show proof of at least two years of appropriate auditing experience. To obtain this certification, candidates must pass an exam.

Source: The Institute of Internal Auditors

CGAP -- Certified Government Auditing Professional
The CGAP identifies public-sector internal auditors who focus on fund accounting, grants, legislative oversight and confidentiality rights, among other facets of internal auditing. Candidates must have an appropriate four-year college degree or a two-year college degree with five years of experience in a public-sector environment, submit a character reference and show proof of at least two years of direct government auditing experience. To obtain this certification, candidates must pass an exam.

Source: The Institute of Internal Auditors

CIA -- Certified Internal Auditor
The CIA cert demonstrates knowledge of professional financial auditing practices. The cert is of primary interest to financial professionals responsible for auditing IT practices and procedures, as well as standard accounting practices and procedures to ensure the integrity and correctness of financial records, transaction logs and other records relevant to commercial activities. Candidates must have a bachelor’s degree, college degree or approved work equivalent, submit a character reference and show proof of at least two years of direct government auditing experience. To obtain this certification, candidates must

pass a four-part exam.

Source: Institute of Internal Auditors

CISA -- Certified Information Systems Auditor
The CISA demonstrates knowledge of IS auditing for control and security purposes. This cert is of primary interest to IT security professionals responsible for auditing IT systems, practices and procedures to make sure organizational security policies meet governmental and regulatory requirements, conform to best security practices and principles, and meet or exceed requirements stated in an organization's security policy.

Source: Information Systems Audit and Control Association

CRISC -- Certified in Risk and Information Systems Control
The CRISC identifies IT professionals who have hands-on experience with risk identification, assessment evaluation, response, information systems control design and implementation, monitoring and maintenance. Candidates must have at least three years of related work experience and pass one exam.

Source: Information Systems Audit and Control Association

ECSP -- EC-Council Certified Secure Programmer
The ECSP identifies programmers who can design and build relatively bug-free, stable Windows- and Web-based applications with the .NET/Java Framework, greatly reducing exploitation by hackers and the incorporation of malicious code. Candidates must pass a single exam.

Source: EC-Council

Security5
Security5's certification identifies non-IT office workers and home users who understand Internet security terminology, know how to use defense programs such as antivirus and antispyware applications, can implement basic operating system security and follow safe Web and email practices. Candidates must pass an exam.

Source: EC-Council

Additional Resources

Return to Table of Contents

- **Analysis of the security certification landscape**
  Ed Tittel and Kim Lindros offer their insight on the state of the security certification landscape, including a certification plan that individuals can start at any point,

depending on current knowledge, skills and experience.

- **Security School: Training for CISSP certification**
  SearchSecurity.com partners with Shon Harris, CISSP and author of *CISSP All-in-One Exam Guide*, to bring you a series of webcasts and additional study materials on each of the ten domains of the Common Body of Knowledge.
- **Credentials: To be or not to be certified**
  It's a good idea to revisit your career and education goals at least once a year.
- **Does job security for security technology jobs exist?**
  One key to job security in the infosec field is maintaining your education.
- **Guide to vendor-specific security certs**
  Ed Tittel and Kim Lindros provide an overview of vendor-specific security certifications.

About the authors:
Ed Tittel is a 30-plus year veteran of the computing industry, and has contributed to over 100 computing books. Perhaps best known for creating the Exam Cram series of IT cert prep books in the late 1990s, Ed has contributed to 5 editions of the CISSP Study Guide, and numerous other infosec-related titles. These days, Ed blogs regularly for TechTarget, Tom's IT Pro, and PearsonITCertification.com. Visit his website at edtittel.com.

Mary Lemons is a professional writer, editor, and content manager who has worked with Tittel for more than 15 years. She has contributed to books on markup languages and information security, and has edited and managed content for such companies as HP, Sony, Verizon, and Microsoft.

Editor's note: Contributor Kim Lindros contributed to previous versions of this article.

23 May 2013