Security Certifications

- General Security: Basic | Intermediate | Advanced
- Forensics/Anti-Hacking: Basic | Intermediate | Advanced

GENERAL SECURITY - Basic

- **BISA – Brainbench Information Security Administrator**
  This Brainbench certification tests knowledge of networking and Internet security, including authorization, authentication, firewalls, encryption, disaster recovery and more.
  
  *Source: Brainbench*

- **BITSF – Brainbench Information Technology Security Fundamentals**
  This Brainbench certification tests basic knowledge of information security concepts, skills and best practices. Topics covered include:
  - Attack recognition, prevention and response
  - Content security
  - Database infrastructure protection
  - General concepts
  - Network infrastructure protection
  - Perimeter and Internet security
  - Security management systems and security technologies
  
  *Source: Brainbench*

- **GIAC – Global Information Assurance Certification Program**
  This program seeks to identify individuals who can demonstrate knowledge of and the ability to manage and protect important information systems and networks. The SANS organization is well known for its timely, focused, and useful security information and certification program. A shining star on this landscape, the GIAC program aims at serious, full-time security professionals responsible for designing, implementing and maintaining a state-of-the-art security infrastructure that may include incident handling and emergency response team management. Available entry-level certifications include the following:
  - GIAC Information Security Fundamentals (GISF)
  - GIAC Security Essentials Certification (GSEC)
  
  *Source: Global Information Assurance Certification*

- **SCNP – Security Certified Network Professional**
  This entry- to mid-level security certification focuses on two primary topics: firewalls and intrusion detection. Related curriculum and exams cover network security fundamentals,
and network defense and countermeasures. Individuals who attain this certification will be able to work as full-time IT security professionals with an operations focus.

Source: Security Certified Program

- **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, Microsoft accepts the Security+ as an alternative to one of the specialization exams for the MCSA and MCSE Messaging and Security specializations.
  
  Source: CompTIA Security+ Certification Overview

- **SSCP – Systems Security Certified Practitioner**
  The entry-level precursor to ISC²’s CISSP, the SSCP exam covers seven of the 10 domains in the CISSP Common Body of Knowledge. The exam focuses more on operational and administrative issues relevant to information security and less on information policy design, risk assessment details and other business analysis skills that more germane to a senior IT security professional (and less so to a day-to-day security administrator, which is where the SSCP is really focused).

  Source: (ISC)²

- **TICSA – TruSecure ICSA Certified Security Associate**
  TICSA demonstrates basic familiarity with vendor-neutral system- and network-security principles, practices and technologies. It is an entry-level security certification for network or system administrations and for those interested in climbing the first rung in a security certification ladder suitable for full-time IT security work.

  Source: TruSecure ICSA Practitioner Certification

---

**GENERAL SECURITY - Intermediate**

- **BIS – Brainbench Internet Security Certification**
  The BIS seeks to identify individuals with a good working knowledge of Internet security practices, principles and technologies. It is aimed at full-time network or system administrators who must manage systems with Internet connections or access.

  Source: Brainbench

- **BNS – Brainbench Network Security Certification**
  The BNS seeks to identify individuals with a good working knowledge of network security practices, principles and technologies. This cert is aimed at full-time network administrators who must deal with external threats through boundary devices like routers, firewalls or intrusion-detection systems, as well as more typical internal threats.

  Source: Brainbench
• **CIW Security Analyst**

Individuals who take and pass the CIW-Security Professional (CIW-SP) exam, and hold one of the following certifications qualify as a CIW Security Analyst (CIW-SA):

- Microsoft Certified Systems Administrator (MCSA)
- Microsoft Certified Systems Engineer (MCSE) 4
- Microsoft Certified Systems Engineer (MCSE) 2000
- Certified Novell Engineer (CNE) 4
- Certified Novell Engineer (CNE) 5
- Cisco Certified Network Associate (CCNA)
- Cisco Certified Network Professional (CCNP)
- Cisco Certified Internetwork Expert (CCIE)
- Linux Professional Institute (LPI) Level 2

Individuals who hold this credential can carry out security policy, identify and handle security threats, and apply countermeasures using firewalls, intrusion detection and related systems. The program’s Web focus also includes coverage of online payments, transaction processing and related security matters.

*Source:* ProsoftTraining Inc.

• **CIW-SP – Certified Internet Webmaster-Security Professional**

The CIW-SP demonstrates knowledge of Web- and e-commerce-related security principles and practices. It is of primary interest to Web administrators who must implement and manage a secure and working Web presence that may also include e-commerce capabilities.

*Source:* ProsoftTraining Inc.

• **CWSP – Certified Wireless Security Professional**

This certification recognizes individuals who can design, implement and manage wireless LAN security. To obtain this credential, candidates must first acquire CWNA certification and pass one exam. Planet3 Wireless recommends that candidates obtain a Security Certified Program certification or the Security+ certification before taking the CWSP course.

*Source:* Planet3 Wireless

• **EWSCP – Enterprise and Web Security Certified Professional**

This certification recognizes systems administrators, managers and IT support personnel, among others, who are responsible for the security of enterprise-wide networks, VPNs and Web communications. To obtain this cert, candidates must attend three core courses and one elective course, and pass all associated exams.

*Source:* Learning Tree International
• **GIAC – Global Information Assurance Certification Program**

This cert program seeks to identify individuals who can demonstrate knowledge of and the ability to manage and protect important information systems and networks. The SANS organization is well known for its timely, focused, and useful security information and certification program. A shining star on this landscape, the GIAC program aims at serious, full-time security professionals responsible for designing, implementing and maintaining a state-of-the-art security infrastructure that may include incident handling and emergency response team management. Available intermediate certifications include the following:

- GIAC Auditing Wireless Networking (GAWN)
- GIAC Certified Firewall Analyst (GCFW)
- GIAC Certified Intrusion Analyst (GCIA)
- GIAC Certified ISO-17799 Specialist (G7799)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Windows Security Administrator (GCWN)
- GIAC Certified UNIX Security Administrator (GCUX)
- GIAC Security Leadership (GSLC)
- GIAC IT Security Audit Essentials (GSAE)
- GIAC Systems and Network Auditor (GSNA)
- GIAC Certified Security Consultant (GCSC)

*Source: Global Information Assurance Certification*

• **NSCP – Network Security Certified Professional**

The NSCP demonstrates the ability to design and implement organizational security strategies, and secure the network perimeter and component systems. It is an intermediate-level IT security certification aimed at network or systems administrators with heavy security responsibilities or those who work full-time on IT security matters.

*Source: Learning Tree International*

• **SCNA – Security Certified Network Architect**

This is a mid- to senior-level security certification that focuses on concepts, planning and implementation of Private Key Infrastructure and biometric authentication and identification systems. Individuals who attain this certification will be able to implement either or both of these technologies within organizations or as consultants to such organizations.

*Source: Security Certified Program*
GENERAL SECURITY - Advanced

• **AIS – Advanced Information Security Certification**

  Security University’s AIS program combines coverage of key information security topics, tools and technologies with a hands-on, lab-oriented learning and testing program. To obtain AIS certification, security professionals must complete eight courses, including six tools-oriented classes on topics such as:

  o Network penetration testing
  o Firewalls and VPNs
  o Virus analysis, patch management and incident response
  o PKI
  o Intrusion detection and computer forensics
  o Anti-hacking

  Two management classes on network security policy and architecture security are also required. Students must take and pass a demanding exam.

  *Source:* Security University

• **CCISM – Certified Counterespionage and Information Security Manager**

  The purpose of CCISM is to prepare individuals to study potential sources of threat, defeat attacks and manage information security at an organizational level. CCISM is a management-level certification, where CCISMs generally manage, work with or consult IT organizations, technical specialists and other IT security professionals.

  *Source:* Espionage Research Institute

• **CERI-ACSS – Advanced Computer System Security**

  The CERI-ACSS seeks to identify law enforcement officials with advanced computer crime investigation experience and training. Requirements include two years of computer investigation/debugging, three years of Microsoft platform analysis, one year of non-Microsoft platform analysis, 40 hours of approved training, a written exam and successful completion of hands-on exercises.

  *Source:* Cyber Enforcement Resources Inc.

• **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.
• **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 four years of experience (or a college degree plus three years of experience).

*Source: (ISC)^2*

• **CPTS – Certified Penetration Testing Specialist**

An offering from Iowa-based training company, Mile 2, 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, $2,600 course that’s backed up by a Prometric exam.

*Source: Mile2*

• **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 some time are able to qualify for this credential.

*Source: American Society for Industrial Security (ASIS)*

• **CWPSS – Certified Web Professional Security Specialist**

Obtaining this credential requires passing the CIW Security Professional exam and meeting additional work experience requirements. Please see the CIW-SP listing for more information.

*Source: International Webmasters’ Association (IWA)*

• **GIAC – Global Information Assurance Certification Program**

This cert program seeks to identify individuals who can demonstrate knowledge of and the ability to manage and protect important information systems and networks. The SANS organization is well known for its timely, focused, and useful security information and certification program. A shining star on this landscape, the GIAC program aims at serious, full-time security professionals responsible for designing, implementing and maintaining a state-of-the-art security infrastructure that may include incident handling and emergency response team management. The GIAC Security Engineer (GSE) track is
the senior-level certification. All mid-level specializations, as well as additional exams and work, are required.

*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
  - Telecommunications and network security
  - Cryptography
  - Requirements analysis and security standards, guidelines and criteria
  - Technology-related business continuity and disaster recovery planning (BCP and DRP)

  *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 NSA. The ISSEP stresses the following elements of the CBK:
  
  - Systems security engineering
  - Certification and accreditation
  - Technical management

  Plus, it adds profound coverage of U.S. Government information assurance regulations.

  *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, DRP and continuity of operations planning (COOP)
  - 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 five years of experience in physical security, a high school diploma (or GED) and a clean criminal record.

*Source:* ASIS International: Physical Security Professional

**FORENSIC/ANTI-HACKING - Basic**

- **CCCI – Certified Computer Crime Investigator (Basic)**
  
  The CCCI is one of two computer forensic certifications aimed at law enforcement and private IT professionals seeking to specialize in the investigative side of the field. Basic requirements include two years of experience (or a college degree, plus one year of experience), 18 months of investigative experience, 40 hours of computer crimes training and documented experience from at least 10 investigated cases. Advanced requirements bump experience to three years (or a college degree, plus two years of experience), four years of investigations, 80 hours of training and involvement as a lead investigator in 20 cases, with involvement in over 60 cases overall.

  *Source:* High Tech Crime Network certifications

- **CCFT – Certified Computer Forensic Technician (Basic)**
  
  The CCFT is one of two 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 (or a college degree, plus one year of experience), 18 months of forensics experience, 40 hours of computer forensics training and documented experience from at least 10 investigated cases. Advanced requirements include three years of experience (or a college degree, plus two years of experience), four years of investigations, 80 hours of training and involvement as a lead investigator in 20 cases with involvement in over 60 cases overall.

  *Source:* High Tech Crime Network certifications

- **CEECS – Certified Electronic Evidence Collection Specialist Certification**
  
  The CEECS identifies individuals who successfully complete the CEECS certification course. No prerequisites are required to attend the course, which covers the basics of evidence collection in addition to highly technical terminology, theories and techniques.

  *Source:* International Association of Computer Investigative Specialists

- **CERI-CFE – Computer Forensic Examination**
  
  The CERI-CFE seeks to identify law enforcement officials with basic computer crime investigation experience and training. Requirements include two years of computer investigation/debugging, one year of Microsoft platform analysis, six months of non-Microsoft platform analysis, 40 hours of approved training, a written exam and successful completion of hands-on exercises.

  *Source:* Cyber Enforcement Resources Inc.
FORENSIC/ANTI-HACKING - Intermediate

• **CCE – Certified Computer Examiner**
  The CCE, offered by the Southeast Cybercrime Institute at Kennesaw State University in partnership with Key Computer Service, 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 pass an online examination and successfully perform a hands-on examination on three test media.
  
  *Source: Key Computer Service*

• **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 prove knowledge of tools used both by hackers and security professionals.
  
  *Source: EC-Council*

• **CFCE – Computer 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 includes both 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*

• **CIFI – Certified Information Forensics Investigator**
  Obtaining the credential of Certified Information Forensics Investigator requires adherence to a code of ethics, successful completion of a rigorous exam and fulfillment of specific experience requirements. Aimed at full-time professional practitioners, this certification is vendor-neutral and devoid of sponsored training requirements or the use or purchase of specific products.
  
  *Source: International Information Systems Forensics Association*

• **CPTP – Certified Penetration Testing Professional**
  An offering from Iowa-based training company, Mile2, this credential seeks to identify individuals who’ve developed the skills necessary to conduct thorough, painstaking
penetration tests for their employers, or for customers who hire them to conduct such testing independently. The credential is structured around a five-day, $2,600 course, and followed up with a Prometric exam.

Source: Mile2

• **CSFA – CyberSecurity Forensic Analyst**

The CSFA aims to identify individuals who are interested in information technology security issues, especially at the hardware level. Prerequisites include at least one certification in computer and software support, networking or security (such as CompTIA’s A+, Microsoft’s MCSA or MCSE, or Cisco’s CCNA), successful completion of an introductory and an advanced computer forensics course offered through the CyberSecurity Institute and no criminal record.

Source: CyberSecurity Institute

• **FCSS – Field Certified Security Specialist**

This certification permits individuals to specialize in Cisco, Check Point or cross-platform topics (which is why we list it in both the vendor-specific – although the parent organization points out that these certs are "vendor-independent" – and vendor-neutral surveys). Candidates must pass a hands-on, performance-based test to obtain FCSS certification.

Source: Field Certified Professional Association

• **GIAC – Global Information Assurance Certification Program**

This cert program seeks to identify individuals who can demonstrate knowledge of and the ability to manage and protect important information systems and networks. The SANS organization is well known for its timely, focused, and useful security information and certification program. A shining star on this landscape, the GIAC program aims at serious, full-time security professionals responsible for designing, implementing and maintaining a state-of-the-art security infrastructure that may include incident handling and emergency response team management. The program includes one mid-level forensics certification – GIAC Certified Forensic Analyst (GCFA).

Source: Global Information Assurance Certification

• **C3C – Certified Cyber-Crime Expert**

The C3C identifies computer forensics investigators, information technology and security personnel, law enforcement officials, lawyers and others, who must have the knowledge and tools to effectively collect, handle, process and preserve computer forensic evidence. The certification requires successful completion of the Computer Forensic and Cyber Investigation course, and a practical and written exam.

Source: E-business Process Solutions

• **CCCI – Certified Computer Crime Investigator (Advanced)**

The CCCI is one of two computer forensic certifications aimed at law enforcement and private IT professionals seeking to specialize in the investigative side of the field. Basic requirements include two years of experience (or a college degree, plus one year of
experience), 18 months of investigative experience, 40 hours of computer crimes training and documented experience from at least 10 investigated cases. Advanced requirements bump experience to three years (or a college degree, plus two years of experience), four years of investigations, 80 hours of training and involvement as a lead investigator in 20 cases, with involvement in over 60 cases overall.

**Source:** High Tech Crime Network certifications

- **CCFT – Certified Computer Forensic Technician (Advanced)**
  The CCFT is one of two 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 (or a college degree, plus one year of experience), 18 months of forensics experience, 40 hours of computer forensics training and documented experience from at least 10 investigated cases. Advanced requirements include three years of experience (or a college degree, plus two years of experience), four years of investigations, 80 hours of training and involvement as a lead investigator in 20 cases with involvement in over 60 cases overall.

**Source:** High Tech Crime Network certifications

- **CERI-ACFE – Advanced Computer Forensic Examination**
  The CERI-ACFE seeks to identify law enforcement officials with advanced computer crime investigation experience and training. Requirements include two years of computer investigation/debugging, four years of Microsoft platform analysis, two years of non-Microsoft platform analysis, 80 hours of approved training, a written exam and successful completion of hands-on exercises.

**Source:** Cyber Enforcement Resources Inc.

- **CERI-ACSS – Advanced Computer System Security**
  The CERI-ACSS seeks to identify law enforcement officials with advanced computer crime investigation experience and training. Requirements include two years of computer investigation/debugging, three years of Microsoft platform analysis, one year of non-Microsoft platform analysis, 40 hours of approved training, a written exam and successful completion of hands-on exercises.

**Source:** Cyber Enforcement Resources Inc.

- **CPTS – Certified Penetration Testing Specialist**
  An offering from Iowa-based training company, Mile 2, 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, $2,600 course that’s backed up by a Prometric exam.

**Source:** Mile2
• 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 bachelor’s degree or higher counts for up to two years of such experience) and a clean legal record for candidates.

Source: ASIS International

FORENSIC/ANTI-HACKING - Advanced

• Brainbench HIPAA (Security)

The Brainbench HIPAA (Security) cert deals with topics and requirements that drive the Health Insurance Portability and Accountability Act (HIPAA) of 1996, to help IT professionals understand and implement related information handling and processing requirements.

Source: Brainbench

• 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.

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 organization with legal mandates to audit for possible fraudulent or illegal transactions and activities (such as banking, securities trading or classified operations).

Source: Association of Certified Fraud Examiners

• 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 insure the integrity and correctness of financial records, transaction logs and other records relevant to commercial activities.

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*

• **GIAC – Global Information Assurance Certification Program**

This cert program seeks to identify individuals who can demonstrate knowledge of and the ability to manage and protect important information systems and networks. The SANS organization is well known for its timely, focused, and useful security information and certification program. A shining star on this landscape, the GIAC program aims at serious, full-time security professionals responsible for designing, implementing and maintaining a state-of-the-art security infrastructure that may include incident handling and emergency response team management. Available certificates, which indicate successful completion of a relatively short but highly focused course, include the following:

  o GIAC HIPAA Security Certificate (GHSC)
  o GIAC Solaris Gold Standard Certificate (GGSC-0200)
  o GIAC E-Warefare Certificate (GEWF)
  o GIAC Ethics in IT (GEIT)
  o GIAC Cutting Edge Hacking Techniques Certificate (GHTQ)
  o GIAC Reverse Engineering Malware (GREM)
  o GIAC Security Awareness (GSAW)
  o GIAC Cyber Warrior Certificate (GCWY)
  o GIAC Business Law and Computer Security (GBLC)
  o GIAC Legal Issues in Information Technologies (GLIT)
  o GIAC Contracting for Data Security (GCDS)
  o GIAC Law of Fraud (GLFR)
  o GIAC Windows 2000 Gold Standard Certificate (GGSC-0100)
  o GIAC Auditing Cisco Routers Gold Standard Certificate (GGCS-0400)

*Source: Global Information Assurance Certification*