Global Information Assurance Certification (GIAC)

Website:	www.giac.org
E-mail:	info@giac.org
Address:	5401 Westbard Avenue, Suite 1501
	Bethesda, MD 20816, USA
Phone:	+1 540 548 0977
Fax:	+1 540 548 0957

Established in 1999 by the System Administration, Audit, Networking and Security (SANS) Institute (www.sans.org), the Global Information Assurance Certification programme is quickly gaining support and recognition due to its high quality curriculum, training and certifications. Enjoying support of some of the best professionals in the industry and academia the Global Information Assurance Certification is now on par with such long-standing and veteran organisations as the International Information Systems Security Certification Consortium and the Information Systems Audit and Control Association. GIAC offers numerous qualifications at levels ranging from novice to expert in different specialisations such as information security management, UNIX, Windows, audit, incident handling, forensics and others.

One of the certification requirements which sets GIAC qualifications apart from others is the requirement to complete written practical assignments before taking the examinations – which is intended to demonstrate candidates' ability to apply their skills in practice. Other GIAC-specific requirement is the practice of online examinations which are conducted over the Internet – whereas other qualifications require candidates to visit either Prometric or VUE testing centres or attend specially arranged examination sessions to sit their exams.

GIAC qualifications are available as tuition plus exam offerings from the SANS Institute (both online and face to face tuition is available) or as so called "challenge" examinations for those who believe they have the required skills and knowledge to take on the exam without much study.

GIAC qualifications also need to be regularly renewed to ensure that certification holders still meet the certification criteria.

GIAC Security Essentials Certification (GSEC)

The GSEC is a general foundation level certification for anyone responsible for security. GSEC is a practical qualification, like other GIAC qualifications; GSEC holders are expected to have the required skills, knowledge and abilities to understand principles of information security and implement information security solutions. The GIAC Security Essentials Certification covers the following subjects:

- Risk assessment and auditing
- Host and network based intrusion detection
- Honeypots, firewalls and perimeter protection
- Security policy
- Password management
- Security incident handling
- Information warfare
- Web security
- Network fundamentals and IP concepts
- Cisco router filters
- Primary threats for perimeter protection
- PGP, steganography
- Anti-viral tools
- Windows security administration and auditing
- IIS security
- Unix security fundamentals

GIAC costs are as follows:

With SANS online training	US$ 250 + training
With SANS conference training	US$ 250 + training
Challenge (examination only)	US$ 450

For more detailed information on GIAC Security Essentials Certification please visit GIAC at www.giac.org.

GIAC Certified Firewall Analyst (GCFW)

GIAC Certified Firewall Analyst is an intermediate level qualification for those network security professionals who specialise in design, implementation, configuration and monitoring of firewalls. Recertification is required every four years. The following subjects are covered by GCFW training and certification programme:

- IP stimulus/response and fragmentation
- Complex IP transports and services
- Tcpdump, Windump, Ethereal and other sniffers
- Business needs vs. security
- Static packet filtering
- Stateful packet filtering and inspection
- Proxies
- In-depth coverage of popular firewall products
- Implementing security with Cisco routers
- Intrusion detection
- Centralized logging
- Firewall log file analysis
- Log file alerting
- IPSec, SSL, and SSH
- Designing a secure perimeter
- Network and host based auditing

GCFW costs are as follows:

With SANS online training	US$ 250 + training
With SANS conference training	US$ 250 + training
Challenge (examination only)	US$ 450

For more information on GCFW please visit GIAC at www.giac.org.

GIAC Certified Intrusion Analyst (GCIA)

GCIA is an intermediate qualification aimed at intrusion detection specialists who configure, maintain and monitor intrusion detection systems and need to read and analyse network traffic and related logs. GCIA certification needs to be renewed every four years and covers the following subjects:

- TCP/IP fragmentation
- ICMP
- Microsoft networking and security
- Client and server Interaction
- Routing
- IPSec
- Tcpdump
- General network traffic analysis
- Snort
- Snort rules
- Intrusion detection architecture
- Intrusion detection analysis
- Traffic and external analysis

GCIA certification costs are as follows:

With SANS online training	US$ 250 + training
With SANS conference training	US$ 250 + training
Challenge (examination only)	US$ 450

For more information on GCIA certification and training please visit GIAC at www.giac.org.

GIAC Certified Incident Handler (GCIH)

GCIH certification is an intermediate level qualification for those who are responsible for incident handling and response within larger security teams. GCIH certification needs to be renewed every two years and covers the following topics:

- The step-by-step approach used by attackers
- The latest computer attack vectors
- Proactive and reactive defences for each stage of a computer attack
- Scanning for, exploiting and defending systems
- Strategies and tools for detecting each type of attack
- Attacks and defences for Windows, UNIX, switches, routers and other systems
- Application-level vulnerabilities, attacks and defences
- Developing an incident handling process
- Legal issues in incident handling
- Recovering from computer attacks and restoring systems for business

GCIH costs are as follows:

With SANS online training	US$ 250 + training
With SANS conference training	US$ 250 + training
Challenge (examination only)	US$ 450

More details on the GCIH certification is available from www.giac.org.

GIAC Certified Windows Security Administrator (GCWN)

An intermediate qualification, GCWN is specifically targeted at Windows (XP, 2000, and NT) administrators who are responsible for security on Windows networks. This certification must be renewed every two years to keep holders updated on latest challenges and solutions. The following topics are covered in particular:

- Active Directory design
- Delegation of authority
- Dynamic DNS
- Group policy design
- Security templates
- PKI installation and management
- Encrypting file system
- Smart cards and tokens
- IP Security Architecture
- Virtual private networking
- Routing and remote access service
- IIS authentication and authorization
- IIS ISAPI extensions and filters
- Windows scripting
- Scripting: ADSI, CDO, WMI

GCWN costs are as follows:

With SANS online training	US$ 250 + training
With SANS conference training	US$ 250 + training
Challenge (examination only)	US$ 450

For up to date information on GCWN please visit www.giac.org.

GIAC Certified UNIX Security Administrator (GCUX)

GIAC Certified UNIX Security Administrator is an intermediate general UNIX security qualification targeted at UNIX system and network administrators who want better and deeper understanding of UNIX security issues and technologies. GCUX needs to be renewed every two years and covers the following topics:

- Passwords and alternatives
- Memory attacks and overflows
- Trojan horse programs
- Network-based attacks
- Physical security
- Security scanners
- Passwords and privilege
- Network security
- Secure Shell
- UNIX forensics
- Common issues with users and management
- Network Time Protocol
- BIND installation and configuration
- Sendmail security
- Linux specifics
- Solaris specifics
- Logging

GCUX costs are as follows:

With SANS online training	US$ 250 + training
With SANS conference training	US$ 250 + training
Challenge (examination only)	US$ 450

For more information on GCUX training and certification please visit GIAC at www.giac.org.

GIAC Information Security Fundamentals (GISF)

Set at an introductory level the GIAC Information Security Fundamentals certification is aimed at candidates who would like to acquire overall understanding of information security risks, considerations and solutions. To obtain the GISF certification candidates will have to pass two examinations and complete a practical assignment. The GISF designation needs to be renewed every two years and covers the following subjects:

- Understanding information security threats and risks
- Identifying best practices
- Risk management
- Security management
- Access controls, attacks and countermeasures
- Secrecy and privacy
- Auditing concepts
- Internet Protocol
- Routing
- Domain Name Service
- Security considerations
- Basics of cryptography
- Defence in depth

GISF certification costs are as follows:

With SANS online training	US$ 250
With SANS conference training	US$ 250

GISF examination without SANS training is not yet available – please visit www.giac.org for up to date information on availability.

GIAC Systems and Network Auditor (GSNA)

GSNA is an intermediate-level qualification for systems and networks auditors. It must be renewed every two years and covers the following subjects:

- Top 20 vulnerabilities
- Forensic techniques
- Firewall and perimeter auditing
- Audit process
- Time based security
- Blending audit objectives with corporate policy
- Before an incident occurs
- Rootkit pathology
- Uncovering "back doors"
- Building a forensics toolkit
- Detailed audit of a router
- Network security
- Password harvesting
- Nmap
- Network mapping
- Analyzing the results
- Security committees
- Audit tools
- Windows auditing
- UNIX auditing

GSNA costs are as follows:

  With SANS conference training   US$ 250

SANS online training and challenge only examination are not yet available for GSNA; please check www.giac.org for up to date information on availability.

GIAC Certified Forensic Analyst (GCFA)

For information security professionals who are responsible for forensic investigation and/or analysis, advanced incident handling, or formal incident investigation the Global Information Assurance Certification programme offers the GIAC Certified Forensic Analyst intermediate-level qualification which covers the following subjects:

- Incident response
- Forensic preparation
- Windows forensics
- UNIX forensics
- Data recovery and analysis
- Malicious code analysis
- Law enforcement interaction and case law
- Corporate and managerial legal concerns and direction
- The Honeynet project's forensic challenge

GCFA certification must be renewed every four years; GCFA costs are as follows:

   With SANS conference training   US$ 250

SANS online training and challenge only examination are not yet available for GCFA; please visit www.giac.org for up to date information on GCFA training and examination availability.

GIAC IT Security Audit Essentials (GSAE)

The GIAC IT Security Audit Essentials certification is appropriate for those new to IT security audit. It is a foundation level qualification with recertification requirement of every two years and covers the following topics:

- Host- and network-based intrusion detection
- Firewalls and honeypots
- Vulnerability scanners
- Computer security policies
- Password management
- Incident handling
- Information warfare
- Encryption
- Steganography
- Virtual private networks
- Public key infrastructures

GSAE costs are as follows:

With SANS conference training	US$ 250

SANS online training and challenge only examination are not yet available for the GSAE certification; please visit www.giac.org for up to date information on availability.

GIAC Security Leadership Certificate (GSLC)

The GIAC Security Leadership Certificate is the GIAC's certification for managers who would like to learn the essential, up to date knowledge and skills required to manage information security component of IT projects.

- Risk assessment and auditing
- Host and network based intrusion detection
- Honeypots, firewalls and perimeter protection
- Security policy
- Password management
- Security incident handling
- Information warfare
- Web security
- Network fundamentals
- IP concepts and behaviour
- Cisco router filters
- Primary threats for perimeter protection
- PGP, steganography
- Anti-viral tools

GSLC costs are as follows:

   With SANS conference training   US$ 250

GSLC online training and challenge only examination are not available. Please visit www.giac.org for up to date information on training and examination availability.

GIAC Gold Standard Certificate (GGSC)

Two GIAC Gold Standard Certificates are currently available:

- GIAC Solaris Gold Standard Certificate
- GIAC Windows 2000 Gold Standard Certificate

These certificates are for system and network administrators who manage Solaris 8/9 and Windows 2000 systems and networks and are based on "gold standards" defined by the Center for Internet Security (CIS) benchmarks.

These certifications are free of charge when taken with SANS conference training; certification with SANS online training is US$ 100; and only GIAC Solaris Gold Standard Certificate is available as a challenge only examination for US$ 250.

For more information on Gold Standard Certificates and their availability please visit www.giac.org.

GIAC Security Engineer (GSE)

The GIAC Security Engineer certification is the most advanced information security qualification awarded by the Global Information Assurance Certification programme. To earn this highly respected professional designation candidates are required to have five (5) GIAC subject area certifications:

- GIAC Certified Firewall Analyst
- GIAC Certified Intrusion Analyst
- GIAC Certified Incident Handler
- GIAC Certified Windows Security Administrator
- GIAC Certified UNIX Security Administrator

Additionally, other requirements (examination, presentation and an on-site security evaluation) must be met. As of November 2003, only two individuals have earned GIAC's highest professional designation: Mr John Jenkinson, GSE, and Mr Lenny Zeltser, GSE. For up to date information on the GSE designation please visit GIAC at www.giac.org.