



***National Initiative for Cybersecurity Education***

# **Cybersecurity Certification Inventory**

**DRAFT**

Version 1.0

Last Updated: October 19, 2012

## **Cybersecurity Certification Inventory Overview**

The following Cybersecurity Certification Inventory details the professionally recognized certifications available to cybersecurity professionals. The certifications contained within this document supports the National Initiative for Cybersecurity Education (NICE) which aims to increase the national awareness and importance of cybersecurity while also building a technically adept, capable cadre of cybersecurity professionals to protect the nation's cyber infrastructure from foreign and domestic threats.

Each inventory table provides the reader with a clear description of the identified certification and provides supplemental information detailing needed prerequisites and qualifications; examination breakdown and scoring specifics; cost (exam, re-certification, and maintenance); continuing education as well as re-certification requirements; and lastly, applicability to the NICE Framework specialty areas. Due to the current socialization of the recently approved NICE Framework, this section will be completed at a later date.

This document is meant as a useful tool for enhancing and improving cybersecurity professionals' skills across Federal, State, Local, Territorial, Tribal, Non-Profit, Academia, and Private Industry organizations. It is not intended to be inclusive of all known and recognized cybersecurity certifications, but rather a useful starting point for awareness, education, and career development exploration of certifications currently documented as of printing.

This is a working document and is meant to grow as appropriate certifications are identified or existing certification change over time. The existence of a certification in this inventory does not mean it is endorsed or recognized by NICE, but rather it is part of a growing inventory of certifications to evaluate for use in educating and growing the cybersecurity community of professionals.

## Table of Contents

GIAC Information Security Fundamentals .....	4
GIAC Security Leadership Certification.....	4
CompTIA Security+ .....	5
(ISC) <sup>2</sup> Certification and Accreditation Professional .....	5
(ISC) <sup>2</sup> Certified Information Systems Security Professional .....	6
(ISC) <sup>2</sup> Certified Information Systems Security Professional .....	7
(ISC) <sup>2</sup> Systems Security Certified Practitioner .....	7
(ISC) <sup>2</sup> Systems Security Certified Practitioner .....	8
ISACA Certified Information Security Manager .....	8
ISACA Certified Information Systems Auditor .....	9
GIAC Systems and Network Auditor .....	9
Electronic Commerce (EC) Council Certified Ethical Hacker .....	10
CompTIA A+ .....	A10
CompTIA Network+ .....	11
Security Certified Program (SCP) Security Certified Network Professional .....	11
Security Certified Program (SCP) Security Certified Network Architect.....	11
GIAC Security Expert.....	12
GIAC Certified Incident Handler .....	13
DRI Associate Business Continuity Professional.....	13
DRI Certified Functional Continuity Professional .....	14
DRI Certified Business Continuity Professional .....	15
DRI Master Business Continuity Professional.....	16
CERT Certified Computer Security Incident Handler .....	17
GIAC Security Essentials Certification.....	18
Certified Penetration Tester .....	18
Certified Expert Penetration Tester .....	19
Certified Wireless Security Professional.....	19
Certified Hacking Forensic Investigator.....	19

**LIST OF PROFESSIONAL CERTIFICATIONS**

<b>Certification</b>			
<b>GIAC Information Security Fundamentals (GISF)</b>			
<b>Description</b>	Assures the professional holding this certification has the requisite knowledge and skill to perform risk management and defense in depth techniques.		
<b>Qualifications</b>	None		
<b>Prerequisites</b>	None		
<b>Examination</b>	1 proctored exam - 75 questions -2hour time limit – 70.7% minimum passing score		
<b>Cost</b>	<b>Exam Fee Only</b>	<b>Exam Fee if taken with a SANS course</b>	<b>Recertification</b>
	\$999.00	\$549.00 ( <a href="#">SANS Security 301 course</a> fee not included)	\$399.00
<b>Maintenance Fee</b>	\$399 every 4 years		
<b>Continuing Education</b>	36 certification maintenance units (CMUs) obtained in the last 2 years of the 4 year certification cycle and before the expiration of the certification		
<b>Recertification</b>	Two options to qualify for recertification:		
	Earn minimum CMUs required within each 4-year certification cycle period, AND	Pay annual maintenance fees, OR	
	Retake and pass the Certification examination every four years, AND	Pay examination fee	
<b>Framework Specialty Areas*</b>	TBD		
<b>GIAC Security Leadership Certification (GSLC)</b>			
<b>Description</b>	Assures the professional holding this certification has the necessary knowledge and skill to perform managerial or supervisory responsibilities for information security staff.		
<b>Qualifications</b>	None		
<b>Prerequisites</b>	None		
<b>Examination</b>	1 proctored exam - 150 questions - 4hour time limit - 68% minimum passing score		
<b>Cost</b>	<b>Exam Fee Only</b>	<b>Exam Fee if taken with SANS course</b>	<b>Recertification</b>
	\$999.00	\$549.00 ( <a href="#">SANS Management 512 course</a> fee not included)	\$399.00
<b>Maintenance Fee</b>	\$399 every 4 years		
<b>Continuing Education</b>	36 certification maintenance units (CMUs) obtained in the last 2 years and before the expiration of the 4 year certification		
<b>Recertification</b>	Two options to qualify for recertification:		
	Earn minimum CMUs required within each 4-year certification cycle period, AND	Pay annual maintenance fees, OR	
	Retake and pass the Certification examination every four years, AND	Pay examination fee	
<b>Framework Specialty Areas*</b>	TBD		

Certification	CompTIA Security+				
<b>Description</b>	Assures the professional holding this certification has the requisite competency in system security, network infrastructure, access control and organizational security.				
<b>Qualifications</b>	None				
<b>Prerequisites</b>	Recommended:				
	1. CompTIA Network+ certification, AND				
	2. Two years of technical networking experience, with an emphasis on security				
<b>Examination</b>	1 proctored exam - 100 questions – 90 minute time limit - (750 on a scale of 100-900)				
<b>Cost</b>	Exam Voucher Only	Courseware & Exam Voucher	Study Guide	All in One Exam Guide	
	\$276.00	\$341.00	\$49.99	\$60.00	
<b>Maintenance Fee</b>	TBD**				
<b>Continuing Education</b>	Under development**				
<b>Recertification</b>	Every 3 years from the date the candidate is certified				
<b>Framework Specialty Areas*</b>	TBD				
Certification	(ISC) <sup>2</sup> Certification and Accreditation Professional (CAP)				
<b>Description</b>	Assures the professional holding this certification has the appropriate knowledge, skills and abilities required for authorizing and maintaining security of information systems.				
<b>Qualifications</b>	Applies to those responsible for formalizing processes used to assess risk and establish security requirements, and ensuring the information systems possess security commensurate with the level of exposure to potential risk, as well as damage to assets or individuals.				
<b>Prerequisites</b>	Professional experience must be a minimum of two years of direct full-time information systems security certification and accreditation in one or more of these seven (ISC) <sup>2</sup> CAP domains:				
	1. Under the Security Authorization of Information Systems				
	2. Categorize Information Systems				
	3. Establish the Security Control Baseline				
	4. Apply Security Controls				
	5. Assess Security Controls				
	6. Authorize Information System				
	7. Monitor Security Controls				
<b>Examination</b>	1 proctored exam - 125 questions – 3 hour time limit – (700 scaled score out of 1000)				
<b>Cost</b>	<b>Early Registration</b> (payment received 16 days prior to examination date)		<b>Standard Registration</b> (payment received less than 16 days from the examination date)		
	\$419.00		\$469.00		
<b>Maintenance Fee</b>	\$65.00 annually				
<b>Continuing Education</b>	60 continuing professional education (CPE) credits; a minimum of 10 CPEs obtained each year of the 3 year certification cycle				
	<b>Minimum Annual CPE Requirement</b>	<b>Group A Credits</b> - Direct Information Systems Security Activities		<b>Group B Credits</b> - Professional Skills Activities	
	10	40		20	
<b>Recertification</b>	Two options to qualify for recertification:				
	Earn minimum CPE credits required within each 3-year	Pay annual maintenance fees, AND		Abide by the (ISC) <sup>2</sup> Code of Ethics, OR	

	certification cycle period, AND		
	Retake and pass the Certification examination every three years, AND	Pay annual maintenance fees, AND	Abide by the (ISC) <sup>2</sup> Code of Ethics
<b>Framework Specialty Areas*</b>	TBD		
<b>Certification</b>	<b>(ISC)<sup>2</sup> Certified Information Systems Security Professional (CISSP)</b>		
<b>Description</b>	This certification is the leading certification worldwide for information security professionals. The CISSP credential demonstrates competency and knowledge in security concepts and practices.		
<b>Qualifications</b>	The CISSP credential is ideal for mid- and senior-level managers who are working toward or have already attained positions as CISOs, CSOs or Senior Security Engineers.		
<b>Prerequisites</b>	Professionals must have at least five full years of experience in information security in two or more of these 10 (ISC) <sup>2</sup> CISSP domains:		
	1. Access Control		
	2. Software Development Security		
	3. Business Continuity and Disaster Recovery Planning		
	4. Cryptography		
	5. Information Security Governance and Risk Management		
	6. Legal, Regulations, Investigations and Compliance		
	7. Operations Security		
	8. Physical (Environmental) Security		
	9. Security Architecture and Design		
10. Telecommunications and Network Security			
<b>Examination</b>	1 proctored exam - 250 questions – 6 hour time limit – (700 scaled score out of 1000)		
<b>Cost</b>	<b>Early Registration</b> (payment received 16 days prior to examination date)	<b>Standard Registration</b> (payment received less than 16 days from the examination date)	
	\$549.00	\$599.00	
<b>Maintenance Fee</b>	\$85.00 annually		
<b>Continuing Education</b>	120 continuing professional education (CPE) credits; a minimum of 20 CPEs obtained each year of the 3 year certification cycle		
	<b>Minimum Annual CPE Requirement</b>	<b>Group A Credits - Direct Information Systems Security Activities</b>	<b>Group B Credits - Professional Skills Activities</b>
	20	80	40
<b>Recertification</b>	Two options to qualify for recertification:		
	Earn minimum CPE credits required within each 3-year certification cycle period, AND	Pay annual maintenance fees, AND	Abide by the (ISC) <sup>2</sup> Code of Ethics, OR
	Retake and pass the Certification examination every three years, AND	Pay annual maintenance fees, AND	Abide by the (ISC) <sup>2</sup> Code of Ethics
<b>Framework Specialty Areas*</b>	TBD		

<b>Certification</b>			
<b>(ISC)<sup>2</sup> Certified Information Systems Security Professional (CISSP) - Associate</b>			
<b>Description</b>	This certification is available for professionals who lack the years of professional experience but have industry information security knowledge and can pass the CISSP exam.		
<b>Qualifications</b>	Candidates have six years to acquire the required practical work experience for full certification.		
<b>Prerequisites</b>	None		
<b>Examination</b>	1 proctored exam - 250 questions – 6 hour time limit – (700 scaled score out of 1000)		
<b>Cost</b>	<b>Early Registration</b> (payment received 16 days prior to examination date)	<b>Standard Registration</b> (payment received less than 16 days from the examination date)	
	\$549.00	\$599.00	
<b>Maintenance Fee</b>	\$35.00 annually		
<b>Continuing Education</b>	Minimum of 20 continuing professional education (CPE) credits during each year while a CISSP Associate		
<b>Recertification</b>	N/A		
<b>Framework Specialty Areas*</b>	TBD		
<b>Certification</b>			
<b>(ISC)<sup>2</sup> Systems Security Certified Practitioner (SSCP)</b>			
<b>Description</b>	This credential is a technical certification that verifies the educational standard and hands-on practical experience in implementing the plans and enforcing the policies designed, planned and managed by the CISO or CSO.		
<b>Qualifications</b>	This certification is ideal for professionals working towards positions such as Network Security Engineers, Security Systems Analysts or Security Administrators.		
<b>Prerequisites</b>	Professionals must have one year professional experience in one or more in these 7 (ISC) <sup>2</sup> CISSP domains:		
	1. Access Control		
	2. Cryptography		
	3. Malicious code and Activity		
	4. Monitoring and Analysis		
	5. Networks and Communication		
	6. Risk, Response and Recovery		
	7. Security Operations and Administration		
<b>Examination</b>	1 proctored exam - 125 questions – 3 hour time limit – (700 scaled score out of 1000)		
<b>Cost</b>	<b>Early Registration</b> (payment received 16 days prior to examination date)	<b>Standard Registration</b> (payment received less than 16 days from the examination date)	
	\$250.00	\$300.00	
<b>Maintenance Fee</b>	\$65.00 annually		
<b>Continuing Education</b>	60 continuing professional education (CPE) credits; a minimum of 10 CPEs obtained each year of the 3 year certification cycle		
	<b>Minimum Annual CPE Requirement</b>	<b>Group A Credits - Direct Information Systems Security Activities</b>	<b>Group B Credits - Professional Skills Activities</b>
	10	40	20
<b>Recertification</b>	Two options to qualify for recertification:		
	Earn minimum CPE credits required within each 3-year certification cycle period, AND	Pay annual maintenance fees, AND	Abide by the (ISC) <sup>2</sup> Code of Ethics, OR
	Retake and pass the Certification examination every three years, AND	Pay annual maintenance fees, AND	Abide by the (ISC) <sup>2</sup> Code of Ethics

<b>Framework Specialty Areas*</b>	TBD			
<b>Certification</b>	<b>(ISC)<sup>2</sup> Systems Security Certified Practitioner (SSCP) - Associate</b>			
<b>Description</b>	This certification is available for professionals who lack the professional work experience but have industry technical and security knowledge and can pass the SSCP exam.			
<b>Qualifications</b>	Candidates have two years to acquire the required practical work experience for full certification.			
<b>Prerequisites</b>	None			
<b>Requirements</b>	1 proctored exam - 125 questions – 3 hour time limit – (700 scaled score out of 1000)			
<b>Cost</b>	<b>Early Registration</b> (payment received 16 days prior to examination date)		<b>Standard Registration</b> (payment received less than 16 days from the examination date)	
	\$250.00		\$300.00	
<b>Maintenance Fee</b>	\$35.00 annually			
<b>Continuing Education</b>	Minimum of 10 continuing professional education (CPE) credits during each year while a SSCP Associate			
<b>Recertification</b>	N/A			
<b>Framework Specialty Areas*</b>	TBD			
<b>Certification</b>	<b>ISACA Certified Information Security Manager (CISM)</b>			
<b>Description</b>	This certification is specifically for experienced information security managers and those who have information security management responsibilities.			
<b>Qualifications</b>	Professionals who are responsible for managing, designing, overseeing and/or assessing an enterprise's information security program.			
<b>Prerequisites</b>	1. A minimum of five years of information security work experience, AND			
	2. A minimum of three years of information security management work experience in three or more of the job practice analysis areas:			
	a. Information security governance			
	b. Information risk management and compliance			
	c. Information security program development and management			
<b>Examination</b>	1 proctored exam – 200 questions - (450 or higher scaled score to pass the exam)			
	<b>ISACA member</b>		<b>Non-ISACA member</b>	
<b>Cost</b>	Early Online Registration***	Final Mail/Fax Registration***	Early Online Registration***	Final Final/Mail Registration***
	\$395.00	\$495.00	\$545.00	\$645.00
<b>Maintenance Fee</b>	ISACA members		ISACA nonmembers	
	\$40.00		\$85.00	
<b>Continuing Education</b>	120 continuing professional education (CPE) credits; a minimum of 20 CPEs obtained each year of the 3 year certification cycle			
<b>Recertification</b>	Earn minimum CPE credits required within each 3-year certification cycle period, AND	Pay annual maintenance fees, AND	Abide by the ISACA Code of Professional Ethics	
<b>Framework Specialty Areas*</b>	TBD			

<b>Certification</b>	<b>ISACA Certified Information Systems Auditor (CISA)</b>			
<b>Description</b>	This certification demonstrates that the professional has the requisite proficiency and technical skill to perform qualified IS audits based on accepted standards.			
<b>Qualifications</b>	Professionals who have the proven ability to perform reviews to ensure that an enterprise's IT and business systems are adequately controlled, monitored and assessed.			
<b>Prerequisites</b>	A minimum of five years of work experience in the fields of IS auditing, control, assurance or Security.			
<b>Examination</b>	1 proctored exam – 200 questions - (450 or higher scaled score to pass the exam)			
<b>Cost</b>	<b>ISACA member</b>		<b>Non-ISACA member</b>	
	Early Online Registration***	Final Mail/Fax Registration***	Early Online Registration***	Final Final/Mail Registration***
	\$395.00	\$495.00	\$545.00	\$645.00
<b>Maintenance Fee</b>	ISACA members		ISACA nonmembers	
	\$40.00		\$85.00	
<b>Continuing Education</b>	120 continuing professional education (CPE) credits; a minimum of 20 CPEs obtained each year of the 3 year certification cycle			
<b>Recertification</b>	Earn minimum CPE credits required within each 3-year certification cycle period, AND	Pay annual maintenance fees, AND	Abide by the ISACA Code of Professional Ethics	
<b>Framework Specialty Areas*</b>	TBD			
<b>Certification</b>	<b>GIAC Systems and Network Auditor (GSNA)</b>			
<b>Description</b>	Assurance that a certified individual has the appropriate level of knowledge and skill necessary to apply basic risk analysis techniques and to conduct a technical audit of essential information systems.			
<b>Qualifications</b>	Any technical staff involved in securing and auditing information systems; or auditors who wish to demonstrate technical knowledge of the systems they are responsible for auditing.			
<b>Prerequisites</b>	None			
<b>Examination</b>	1 proctored exam - 150 questions - 4 hour time limit - 70% (105 of 150 questions) minimum passing score			
<b>Cost</b>	<b>Exam Fee Only</b>	<b>Exam Fee if taken with a SANS course</b>	<b>Recertification</b>	
	\$999.00	\$549.00 ( <a href="#">SANS Audit 507</a> course fee not included)	\$399.00	
<b>Maintenance Fee</b>	\$399 every 4 years			
<b>Continuing Education</b>	36 CMUs accrued in the last 2 years of the 4 year certification cycle and before the expiration of the certification			
<b>Recertification</b>	Two options to qualify for recertification:			
	Earn minimum CMUs required within each 4-year certification cycle period, AND	Pay annual maintenance fees, OR		
	Retake and pass the Certification examination every four years, AND	Pay examination fee		
<b>Framework Specialty Areas*</b>	TBD			

Certification		Electronic Commerce (EC) Council Certified Ethical Hacker (CEH)			
Description	This certification assures that the professional has the required knowledge and skills to ascertain weaknesses and vulnerabilities in target systems and uses this knowledge and tools as a malicious hacker would.				
Qualifications	The professional will have minimum baseline knowledge of security threats, risks and countermeasures.				
Prerequisites	1. Attended training for the CEH course at any of the accredited training centers, OR				
	2. Self-study in lieu of attending training then must have:				
	a. At least two years of information security related experience and included in application form, AND				
	b. Verification and endorsement of work experience from employer				
Exam	1 proctored exam - 150 questions – 4 hour time limit – 70% minimum score <b>CEH exam 312-50 v7</b>				
Cost	\$500				
Maintenance Fee	None				
Continuing Education	120 EC-Council Continuing Education (ECEs) credits; a minimum of 20 ECE credits obtained each year of the 3 year certification cycle				
Recertification	Continue to accrue the required 120 ECEs during each certification cycle				
Framework Specialty Areas*	TBD				
Certification		CompTIA A+			
Description	This certification assures the professional has the requisite competencies in the areas of installation, preventative maintenance, networking, security and troubleshooting.				
Qualifications	Professionals have excellent customer service and communication skills to work with clients.				
Prerequisites	None				
Examination	2 proctored exams - 100 questions each exam – 90 minute time limit each - (675 for CompTIA A+ Essentials, 700 for CompTIA A+ Practical Application on a scale of 100-900)				
	Two exams are necessary to be certified: CompTIA A+ Essentials, exam code 220-701; and CompTIA A+ Practical Application, exam code 220-702.				
Cost	Exam Voucher Only	Essentials Courseware	Practical Application Courseware & Exam Voucher	Self-Paced eLearning Courseware (6 mos.)	
	\$178.00	\$125.71	\$188.00	\$75.00	
Maintenance Fee	TBD**				
Continuing Education	-20 CEU's for program completion				
Recertification	Every 3 years**				
Framework Specialty Areas*	TBD				

<b>Certification</b>	<b>CompTIA Network+</b>	
<b>Description</b>	This certification assures that the professional has the ability to describe the features and functions of networking components, and manage, maintain, troubleshoot, install, operate, and configure basic network infrastructure.	
<b>Qualifications</b>	None.	
<b>Prerequisites</b>	It is recommended	
	1. At least nine months of experience in network support or administration or adequate academic training, AND	
	2. CompTIA A+ certification	
<b>Examination</b>	1 proctored exam - 100 questions each exam – 90 minute time limit each - (720 on a scale of 100-900)	
<b>Cost</b>	Exam Voucher Only	Courseware & Exam Voucher
	\$253.00	\$295.20
<b>Maintenance Fee</b>	TBD**	
<b>Continuing Education</b>	30 CEU's for program completion.	
<b>Recertification</b>	Every 3 years**	
<b>Framework Specialty Areas*</b>	TBD	
<b>Certification</b>	<b>Security Certified Program (SCP) Security Certified Network Professional (SCNP)</b>	
<b>Description</b>	This certification assures the professional has the appropriate knowledge and skills to perform as a network administrator and has the ability to design and implement firewalls, IDS, wireless security, cryptography, Linux security, and Windows security.	
<b>Qualifications</b>	A knowledge of network security fundamentals.	
<b>Prerequisites</b>	1. Successfully completed the Tactical Perimeter Defense exam ( SC0-451),AND	
	2. Holds a SCNS certification in good standing	
<b>Examination</b>	SC0-471 exam - 60 questions – 90 minutes time limit – 75% minimum score	
<b>Cost</b>	\$179.00	
<b>Maintenance Fee</b>	None	
<b>Continuing Education</b>	None	
<b>Recertification</b>	None	
<b>Roles*</b>	ISSO	
<b>Certification</b>	<b>Security Certified Program (SCP) Security Certified Network Architect (SCNA)</b>	
<b>Description</b>	This certification assures the professional has the necessary knowledge and technical skills to build trusted networks.	
<b>Qualifications</b>	Ability to examine the strategies, components and policies required to implement a trusted network.	
<b>Prerequisites</b>	1. Successfully completed the Strategic Infrastructure Security exam( SC0-471) AND	
	2. Holds an SCNP certification in good standing	
<b>Examination</b>	<b>SC0-501 Exam</b> – covers both the Advanced Security Implementation AND Enterprise Security Solutions courses	<b>SC0-502 Exam</b> - covers all four SCP courses
	60 questions – 90 minutes time limit – 75% minimum score	20 questions – 2 hour time limit – 75% minimum score
<b>Cost</b>	\$199.00	\$199.00
<b>Maintenance Fee</b>	None	

<b>Continuing Education</b>	None	
<b>Recertification</b>	None	
<b>Framework Specialty Areas*</b>	TBD	
<b>Certification</b>	<b>GIAC Security Expert (GSE)</b>	
<b>Description</b>	This certification assures the professional has an in-depth technical proficiency and expertise and is a master in all areas of information security.	
<b>Qualifications</b>	The professional must have the following skills to successfully complete the GSE exam: The skills required to successfully complete the GSE exam can be broken up into three major groups:	
	1. General security skills	
	2. Incident handling skills	
<b>Prerequisites</b>	3. Intrusion detection and analysis skills	
	1. The prerequisite is unique because it includes GIAC Certified Windows Security Administrator (GWSA) and GIAC Certified UNIX Security Administrator (GCUX).	
	2. Candidate must have real world, hands on experience in these subject areas:	
	a. GIAC Security Essentials Certification (GSEC)	
	b. GIAC Certified Intrusion Analyst (GCIA)	
	c. GIAC Certified Incident Handler (GCIH)	
	3. The GSE certification substitution option prerequisite list includes:	
	a. GSEC, GCIH, GCIA with two gold	
	b. GSEC, GCIH, GCIA with one gold and one substitute	
c. GSEC, GCIH, GCIA with no gold and two substitutes		
d. GCWN, GCUX, GCIH, GCIA with one gold		
e. GCWN, GCUX, GCIH, GCIA with no gold and one substitute		
<b>Examination</b>	1 proctored exam - 150 questions - 3-hour time limit - 75% passing score	
<b>Cost</b>	GSE Exam consists of 2 parts. Passage of the multiple-choice exams qualifies to take the lab exam	
	GSE Multiple choice exam	GSE hands-on lab examination
	\$399.00	\$1199
<b>Maintenance Fee</b>	None	
<b>Continuing Education</b>	None	
<b>Recertification</b>	Retake and pass the current certification examination every four years, (benefit of the GSE is that it automatically maintains and renews all other GIAC certifications so long as the GSE itself is maintained) AND	Pay examination fee
<b>Framework Specialty Areas*</b>	TBD	

<b>Certification</b>	<b>GIAC Certified Incident Handler (GCIH)</b>		
<b>Description</b>	Assures the certified professional has the requisite knowledge, skill and abilities to manage incidents; understand common attack techniques and tools; and to defend against and/or respond to such attacks when they occur.		
<b>Qualifications</b>	Professionals who are responsible for incident handling or incident response, or who require an understanding of the current threats to systems and networks, along with effective countermeasures.		
<b>Prerequisite</b>	None		
<b>Examination</b>	1 proctored exam - 150 questions - 4 hour time limit - 72.7% (109 of 150 questions) minimum passing score		
<b>Cost</b>	<b>Exam Fee Only</b>	<b>Exam Fee if taken with a SANS course</b>	<b>Recertification</b>
	\$999.00	\$549.00 ( <a href="#">SANS Security 504</a> course fee not included)	\$399.00
<b>Maintenance Fee</b>	\$399 every 4 years		
<b>Continuing Education</b>	36 certification maintenance units (CMUs) obtained in the last 2 years of the 4 year certification cycle and before the expiration of the certification		
<b>Recertification</b>	Two options to qualify for recertification:		
	Earn minimum CMUs required within each 4-year certification cycle period, AND	Pay annual maintenance fees, OR	
	Retake and pass the Certification examination every four years, AND	Pay examination fee	
<b>Roles*</b>	IR, ISSO, ISSIR		
<b>Certification</b>	<b>DRI Associate Business Continuity Professional (ABCP)</b>		
<b>Description</b>	This certification is for the professional who have some knowledge in business continuity planning, but has not acquired the necessary work experience in business continuity planning.		
<b>Qualifications</b>	None		
<b>Prerequisites</b>	None		
<b>Examination</b>	1 proctored exam - 148 questions – 3.5 hour time limit – 75% minimum score		
<b>Cost</b>	<b>Qualifying Exam</b>	<b>Application Fee</b>	
	\$550.00	\$200.00	
<b>Maintenance Fee</b>	\$125.00 annually		
<b>Continuing Education</b>	None		
<b>Recertification</b>	Pay annual maintenance fees		
<b>Framework Specialty Areas*</b>	TBD		

Certification	DRI Certified Functional Continuity Professional (CFCP)		
<b>Description</b>	This certification is for the continuity specialist responsible for a specific function area or department.		
<b>Qualifications</b>	None.		
<b>Prerequisites</b>	A. Minimum two years' work experience in business continuity planning or disaster recovery planning responsibilities.		
	B. Demonstrate practical experience in three of the core professional practice (PP) areas		
	1. Program Initiation and Management		
	2. Risk Evaluation and Control		
	3. Business Impact Analysis		
	4. Business Continuity Strategies		
	5. Emergency Response and Operations		
	6. Developing and Implementing Business Continuity Plans		
	7. Awareness and Training Programs		
	8. Business Continuity Plan Exercise, Audit and Maintenance		
	9. Crisis Communication		
	10. Coordination With External Agencies		
	C. At least one of the three core PP areas must be from #3, #4, #6 or #8, and occurred within a ten-year period from the application date.		
<b>Examination</b>	1 proctored exam - 148 questions – 4.5 hour time limit – 75% minimum score		
<b>Cost</b>	<b>Qualifying Exam</b>		<b>Application Fee</b>
	\$550.00		\$400.00
<b>Maintenance Fee</b>	\$125.00 annually		
<b>Continuing Education</b>	80 continuing education activity points (CEAPs) are required to be obtained over the 2 year certification cycle		
	<b>Recommended Minimum Annual CEAP Requirement</b>	<b>Group A Credits</b> – Activities directly related to business continuity /disaster recovery planning	<b>Group B Credits</b> - Professional Skills Activities
	40	54	26
<b>Recertification</b>	Three requirements to qualify for recertification:		
	1. Pay all annual maintenance fees		
	2. Obtain the minimum number of CEAPs required for recertification		
	3. Abide by DRI International's Code of Ethics for Business Continuity Professionals		
<b>Framework Specialty Areas*</b>	TBD		

Certification	DRI Certified Business Continuity Professional (CBCP)		
<b>Description</b>	This certification is the basic certification level for professionals responsible for business continuity planning or disaster recovery planning.		
<b>Qualifications</b>	None.		
<b>Prerequisites</b>	A. Minimum of two years' work experience in business continuity planning or disaster recovery planning responsibilities.		
	B. Demonstrate significant and practical experience in five of the ten core professional practice (PP) areas		
	11. Program Initiation and Management		
	12. Risk Evaluation and Control		
	13. Business Impact Analysis		
	14. Business Continuity Strategies		
	15. Emergency Response and Operations		
	16. Business Continuity Plans		
	17. Awareness and Training Programs		
	18. Business Continuity Plan Exercise, Audit and Maintenance		
	19. Crisis Communication		
	20. Coordination With External Agencies		
	C. At least two of the five core PP areas must be from #3, #4, #6 or #8, and occurred within a ten-year period from the application date.		
D. Pass the qualifying exam with at least a C grade. Not required to take this exam if an ABCP certificate has been obtained and is in good standing.			
<b>Examination</b>	1 proctored exam - 148 questions – 4.5 hour time limit – 75% minimum score		
<b>Cost</b>	<b>Qualifying Exam</b>		<b>Application Fee</b>
	\$550.00		\$400.00
<b>Maintenance Fee</b>	\$150.00 annually		
<b>Continuing Education</b>	80 continuing education activity points (CEAPs) are required to be obtained over the 2 year certification cycle		
	<b>Recommended Minimum Annual CEAP Requirement</b>	<b>Group A Credits</b> – Activities directly related to business continuity /disaster recovery planning	<b>Group B Maximum Credits</b> - Professional Skills Activities
	<b>40</b>	<b>54</b>	<b>26</b>
<b>Recertification</b>	Three requirements to qualify for recertification:		
	1. Pay all annual maintenance fees		
	2. Obtain the minimum number of CEAPs required for recertification		
<b>Framework Specialty Areas*</b>	3. Abide by DRI International's Code of Ethics for Business Continuity Professionals		
	TBD		

Certification	DRI Master Business Continuity Professional (MBCP)			
<b>Description</b>	This certification is for professionals who have demonstrated significant knowledge and skill in business continuity planning or disaster recovery planning responsibilities.			
<b>Qualifications</b>	None			
<b>Prerequisites</b>	A. Minimum of five years' of work experience in business continuity planning or disaster recovery planning responsibilities.			
	B. Demonstrate significant and practical experience in 7 of the 10 core professional practice (PP) areas			
	21. Program Initiation and Management			
	22. Risk Evaluation and Control			
	23. Business Impact Analysis			
	24. Business Continuity Strategies			
	25. Emergency Response and Operations			
	26. Business Continuity Plans			
	27. Awareness and Training Programs			
	28. Business Continuity Plan Exercise, Audit and Maintenance			
	29. Crisis Communication			
	30. Coordination With External Agencies			
	C. At least four of the seven core PP areas must be from #3, #4, #6 or #8, and occurred within a ten-year period from the application date.			
<b>Examination</b>	1 proctored exam – Case Study Essay – 4.5 hour time limit – 75% minimum score			
<b>Cost</b>	<b>Master exam</b>		<b>Application Fee</b>	
	\$695.00		\$500.00	
<b>Maintenance Fee</b>	\$200.00 annually			
<b>Continuing Education</b>	80 continuing education activity points (CEAPs) are required to be obtained over the 2 year certification cycle			
	<b>Recommended Minimum Annual CEAP Requirement</b>	<b>Group A Credits – Activities directly related to BCP/DRP</b>	<b>Group B Maximum Credits - Professional Skills Activities</b>	<b>Group C Minimum Credits – Professional Leadership</b>
	40	60	26	10
<b>Recertification</b>	Three requirements to qualify for recertification:			
	1. Pay all annual maintenance fees			
	2. Obtain the minimum number of CEAPs required for recertification			
<b>Framework Specialty Areas*</b>	3. Abide by DRI International's Code of Ethics for Business Continuity Professionals			
	TBD			

Certification		CERT Certified Computer Security Incident Handler (CSIH)			
<b>Description</b>	This certification assures the professional has the requisite knowledge and skills to recognize, analyze, and respond to an incident while adhering to and following the incident process as established by the organization's incident management program.				
<b>Qualifications</b>	Created for incident handling professionals' computer security incident response team (CSIRT) technical staff, system and network administrators with incident handling experience, incident handling trainers and educators, and individuals with some technical training who want to enter the incident handling field.				
<b>Prerequisites</b>	1. It is recommended that the computer security professionals have three or more years of experience in incident handling and/or equivalent security-related experience.				
	2. It is recommended that computer security professionals with one or more years of experience in incident handling and/or equivalent security-related experience take the following 4 SEI courses:				
	a. <a href="#">Fundamentals of Incident Handling</a>				
	b. <a href="#">Advanced Incident Handling</a>				
	c. <a href="#">Information Security for Technical Staff</a>				
<b>Examination</b>	d. <a href="#">Advanced Information Security for Technical Staff</a>				
	1 proctored exam – 3 hour time limit – 80% minimum score, consisting of:				
	1. 46 multiple choice questions (answer 37 questions correctly)				
2. 1 essay, which is reviewed by two subject matter experts who will determine if the test taker's essay has met the required criteria to receive passing credit.					
<b>Cost</b>	\$499.00				
<b>Maintenance Fee</b>	None				
<b>Continuing Education</b>	60 professional development units (PDUs) are required over the 3 year certification cycle				
	Professional activities (maximum PDUs)	Continuing education	Teaching, presentations, and development (maximum PDUs)	Authoring activities (maximum PDUs)	
	40	23	20	30	
<b>Recertification</b>	Three requirements to qualify for recertification				
	Completion of all criteria is to be submitted to the SEI 30 days before the last day of the expiration month.				
	Submission and approval of documentation supporting completion of 60 Professional Development Units (PDU) completed during the renewal cycle				
	Submission of the certification renewal fee of \$150 (US) to the SEI with the renewal application packet. \$150 renewal fee				
<b>Framework Specialty Areas*</b>	TBD				

<b>Certification</b>	<b>GIAC Security Essentials Certification (GSEC)</b>		
<b>Description</b>	Assures the certified professional has the requisite knowledge, skill and abilities to perform hands-on IT system technical responsibilities and information security tasks.		
<b>Qualifications</b>	Professionals who can demonstrate an understanding of essential information security concepts.		
<b>Prerequisites</b>	None		
<b>Examination</b>	1 proctored exam - 180 questions - 5 hour time limit - 73% minimum passing score		
<b>Cost</b>	<b>Exam Fee Only</b>	<b>Exam Fee if taken with a SANS course</b>	<b>Recertification</b>
	\$999.00	\$549.00 ( <a href="#">SANS Security 401</a> course fee not included)	\$399.00
<b>Maintenance Fee</b>	\$399 every 4 years		
<b>Continuing Education</b>	36 certification maintenance units (CMUs) obtained in the last 2 years of the 4 year certification cycle and before the expiration of the certification		
<b>Recertification</b>	Two options to qualify for recertification:		
	Earn minimum CMUs required within each 4-year certification cycle period, AND	Pay annual maintenance fees, OR	
	Retake and pass the Certification examination every four years, AND	Pay examination fee	
<b>Certification</b>	<b>Certified Penetration Tester (CPT)</b>		
<b>Description</b>	The professional has the requisite knowledge and skill in relation to penetration testing.		
<b>Qualifications</b>	Professionals who can demonstrate real world penetration testing skills. Proficiency in network penetration testing, recon, remote/client side exploitation and security best practices.		
<b>Prerequisites</b>	None		
<b>Examination</b>	2 part exam - 1 exam – 50 questions -2 hour time limit - 70% minimum passing score; then take home practical, candidates are tested on their ability with 3 challenges. Completion of the take home must be achieved within 60 days of the exam. 70% is minimum passing score on take home exam.		
<b>Cost</b>	<b>Exam Fee Only</b>	<b>On site proctored exam</b>	
	\$499.00	\$399.99 per voucher	
<b>Maintenance Fee</b>	none		
<b>Continuing Education</b>	4 year certification cycle		
<b>Recertification</b>	Candidates must maintain knowledge and skills over time. Four years certification period. Candidates are notified within a year of expiration. No fees for recertification.		

<b>Certification</b>	<b>Certified Expert Penetration Tester (CEPT)</b>	
<b>Description</b>	The professional has the expert knowledge and skill in relation to penetration testing.	
<b>Qualifications</b>	Professionals who can demonstrate real world penetration testing skills. Proficiency in exploit development, reverse engineering and software security.	
<b>Prerequisites</b>	None	
<b>Examination</b>	2 part exam - 1 exam – 50 questions -2 hour time limit - 70% minimum passing score; then take home practical, candidates are tested on their ability with 3 challenges. Completion of the take home must be achieved within 60 days of the exam. 70% is minimum passing score on take home exam.	
<b>Cost</b>	<b>Exam Fee Only</b>	<b>On site proctored exam</b>
	\$499.00	\$399.99 per voucher
<b>Maintenance Fee</b>	none	
<b>Continuing Education</b>	4 year certification cycle.	
<b>Recertification</b>	Candidates must maintain knowledge and skills over time. Four year certification period. Candidates are notified within a year of expiration. No fees for recertification.	
<b>Certification</b>	<b>Certified Wireless Security Professional (CWSP)</b>	
<b>Description</b>	Assures the certified professional has the requisite knowledge, skill and abilities to secure enterprise Wi-Fi networks from hackers.	
<b>Qualifications</b>	Professionals who can demonstrate an understanding of how to secure Wi-Fi networks.	
<b>Prerequisites</b>	Pass two exams PWO-104 and PWO 105	
<b>Examination</b>	1 proctored exam - 60 questions – 90 minute time limit - 70% minimum passing score	
<b>Cost</b>	<b>Exam Fee Only</b>	
	\$225.00	
<b>Maintenance Fee</b>	N/A	
<b>Continuing Education</b>	N/A	
<b>Recertification</b>	There is no recertification; however, candidates can apply for a higher certification Certified Wireless Network Expert (CWNE) once they have passed four exams PWO 104, 105, 250, 270. Certifications are valid for 3 years.	
<b>Certification</b>	<b>Certified Hacking Forensic Investigator (CHFI)</b>	
<b>Description</b>	The professional has the expert knowledge of law enforcement personnel, system administrators, security officers, defense and military personal, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of the network infrastructure.	
<b>Qualifications</b>	Professionals who can demonstrate experience in computer forensics.	
<b>Prerequisites</b>	Exam ECO-312-49	
<b>Examination</b>	1 exam – 150 questions -4-hour time limit - 70% minimum passing score.	
<b>Cost</b>	Not posted on website	
<b>Maintenance Fee</b>	none	
<b>Continuing Education</b>	3 year certification cycle.	
<b>Recertification</b>	Must receive 120 ECEs over three years.	

NOTES:

\*Each certification will be mapped to the specialty areas of the **National Cybersecurity Workforce Framework** to which they apply.

\*\* Anyone achieving an A+, Network+, or Security+ certification by 12/31/10, is certified for life, and does not require recertification. Effective 1/1/11, all new A+, Network+, or Security+ certifications are valid for 3 years. After 3 years, the certification must be renewed. It is accomplished by either passing the examination or accruing CPUs. This new recertification program is being developed.

\*\*\*Renewal dates are determined by IASCA yearly

DRAFT