State of South Carolina

InfoSec and Privacy Training Framework

Start

Introduction

The development of a training framework is part of the State of South Carolina's (State) initiative to create a Professional Development Program (PDP). The training framework is one of the activities that the State has taken to deploy a PDP that will evolve to provide a career path for Information Security (InfoSec) and Privacy personnel and increase the security posture of the organization. The training framework provides a catalog of coursework for the core InfoSec and Privacy workforce to establish training opportunities.

Clearly defined courses and certifications will encourage growth and ownership of InfoSec and Privacy domains at each State agency, and in turn increase InfoSec and privacy compliance and competency.

Training Framework Layout

InfoSec and Privacy industry authoritative sources were taken into consideration to compile the training framework. The InfoSec and Privacy Competency Model was aligned to the training courses and certifications to increase alignment with the remainder of the PDP and security growth and posture.

InfoSec and Privacy personnel can use the framework in a variety of ways to strategically work toward professional development. All audiences can search training courses by:

- Competency

- Certification

- Position Description

InfoSec and Privacy Training by Competency

InfoSec Governance and Compliance	Risk Strategy and Management	Threat and Vulnerability Management	Privacy	Data Security	IS Acquisition, Development and Maintenance	Physical and Environmental Security	Business Continuity Management and Disaster Recovery	Network and Infrastructure Security	Identity Access Management	Education and Training
InfoSec program management	Risk assessment	Vulnerability management	Privacy program administration	Data management	System development lifecycle	Physical access controls	Business impact assessment	Secure network engineering	Access management	Training needs analysis
InfoSec regulation	Risk acceptance	Security incident and event management	Privacy compliance	Secure data transmission and storage	Secure software development	Environmental security	Business continuity planning	Network defense analysis and control	Identity management	Training curriculum design and development
Policy communication, enforcement and exception management	Risk mitigation	Forensics analysis	Privacy impact assessment	Cryptographic safeguards	Procurement methods	Equipment cleansing and disposal	Data backup and restoration			Training delivery
		Threat identification and categorization	Data classification				Crisis management			
			Privacy incident response							

The InfoSec and Privacy Competency Model is comprised of 11 domains and 35 associated competencies, outlined above. Each competency maps to a selection of training courses and provides a corresponding level of proficiency.

There are further training courses available to strengthen competencies which are not featured under the Position Descriptions.

Click each competency to see associated training courses

CAP	Certified Authorization Professional	CIPM	Certified Information Privacy Manager	CNDA	Certified Network Defense Architect
CASP	CompTIA Advanced Security Professional	CIPP/US	Certified Information Privacy Professional/U.S. Private-Sector	CNFE	Certified Network Forensics Examiner
CBAP	Certified Business Analysis Professional	CIPP/G	Certified Information Privacy Professional/U.S. Government	CPEH	Certified Professional Ethical Hacker
CCFP	Certified Cyber Forensics Professional	CIPT	Certified Information Privacy Technologist	CPTC	Certified Penetration Testing Consultant
CCISO	Certified Chief Information Security Officer	CIRM	Certified Identity Risk Manager	CPTE	Certified Penetration Testing Engineer
CCM	Certified Continuity Manager	CISA	Certified Information Systems Auditor	CRCMP	Certified Risk and Compliance Management Professional
CDFE	Certified Digital Forensics Examiner	CISM	Certified Information Security Manager	CRISC	Certified in Risk and Information Systems Control
CDRE	Certified Disaster Recovery Engineer	CISRCP	Certified Information Systems Risk & Compliance Professional	CSIH	Certified Computer Security Incident Handler
CDRP	Certified Data Recovery Professional	CISSRM	Certified Information Systems Security Risk Manager	CSLO	Certified Security Leadership Officer
CEH	Certified Ethical Hacker	CISSM	Certified Information Systems Security Manager	CSS	Certified Security Sentinel
CGEIT	Certified in the Governance of Enterprise IT	CISSO	Certified Information Systems Security Officer	CSSLP	Certified Secure Software Lifecycle Professional
CHFI	Computer Hacking Forensic Investigator	CISSP	Certified Information Systems Security Professional	CVA	Certified Vulnerability Assessor
CIHE	Certified Incident Handling Engineer	CITAD	Certified IT Asset Disposition	ECSA	EC-Council Certified Security Analyst

Click each certification to see associated competencies and training courses

Go to InfoSec and Privacy Certifications Page 2

Go back to Overview of InfoSec and Privacy Training Framework

InfoSec and Privacy Certifications (2 of 2)

ECSS	EC-Council Certified Security Specialist		GREM	GIAC Certified Reverse Engineering Malware
EDRP	EC-Council Disaster Recovery Professional		GSEC	GIAC Security Essentials
EMCISA	EMC Information Storage Associate		GSLC	GIAC Security Leadership Certification
ENSA	EC-Council Network Security Administrator		GSSP-.NET	GIAC Secure Software Programmer .NET
GAWN	Global Information Assurance Certification (GIAC) Auditing Wireless Networks		GSSP-JAVA	GIAC Secure Software Programmer Java
GCCC	GIAC Critical Controls Certification		GWAPT	GIAC Certified Web Application Penetration Tester
GCED	GIAC Certified Enterprise Defender		GWEB	GIAC Certified Web Application Defender
GCFE	GIAC Certified Forensic Examiner		ISSAP	Information Systems Security Architecture Professional
GCFA	GIAC Certified Forensic Analyst		ISSEP	Information Systems Security Engineering Professional
GCIH	GIAC Certified Incident Handler		ISSMP	Information Systems Security Management Professional
GISF	GIAC Information Security Fundamentals		LPT	Licensed Penetration Tester
GLEG	GIAC Law of Data Security & Investigations		Network+	Network+
GNFA	GIAC Network Forensic Analyst		Security+	Security+
GPEN	GIAC Penetration Tester		SSCP	Systems Security Certified Practitioner

Click each certification to see associated competencies and training courses

InfoSec and Privacy Position Descriptions

Core[1]:

- GRC Manager

- Information Privacy Analyst

- Information Privacy Manager

- InfoSec Analyst

- InfoSec and Privacy Auditor

- InfoSec Architect

- InfoSec Engineer

- InfoSec Manager

Hybrid[2]:

- IT Director

- Network Administrator

- Program Manager (Compliance / Privacy)

- Program Manager (Compliance / Security)

12 Position Descriptions were created to capture the roles and responsibilities necessary to support InfoSec and privacy. Each Position Description maps to a selection of training courses and corresponding position level.

Additional training courses that are not featured in the Position Descriptions may be explored by searching courses by Competency.

Click each position description to see associated training courses

[1] Core employees are defined as employees dedicated full-time to InfoSec and/or Privacy roles and responsibilities
[2] Hybrid employees are defined as staff that have both InfoSec/Privacy and non-InfoSec/Privacy roles and responsibilities

Go back to Overview of InfoSec and Privacy Training Framework

InfoSec and Privacy Position Description
Core: GRC Manager

It is highly recommended that the GRC Manager explore training courses mapped to pertinent competencies for professional development.

Course	Certification	Position Level		
		Level 1	Level 2	Level 3
SANS - SEC401: Security Essentials Bootcamp Style	GSEC	x	x	x
ISACA: Certified in Risk and Information Systems Control (CRISC) Training	CRISC			x
ISACA: Certified Information Security Manager (CISM) Training	CISM		x	x
ISACA: Certified Information Systems Auditor (CISA) Training	CISA		x	x
ISACA: Certified in the Governance of Enterprise IT (CGEIT) Training	CGEIT			x
InfoSec Institute: Certified in the Governance of Enterprise IT (CGEIT) Training (IA-212)	CGEIT			x

InfoSec and Privacy Position Description
Core: Information Privacy Analyst

It is highly recommended that the Information Privacy Analyst explore training courses mapped to pertinent competencies for professional development.

Course	Certification	Position Level		
		Level 1	Level 2	Level 3
ISACA: An Introduction to Privacy and Data Protection Training	N/A	x	x	x
IAPP: Certification Foundation Training*	N/A	x	x	x
IAPP: Certified Information Privacy Professional / U.S. Private-Sector (CIPP/US) Training	CIPP/US		x	x
IAPP: Certified Information Privacy Professional / U.S. Government (CIPP/G) Training	CIPP/G		x	x
IAPP: Certified Information Privacy Technologist (CIPT) Training	CIPT			x

*This course will be retired on July 1st, 2015

InfoSec and Privacy Position Description
Core: Information Privacy Manager

It is highly recommended that the Information Privacy Manager explore training courses mapped to pertinent competencies for professional development.

Course	Certification	Position Level		
		Level 1	Level 2	Level 3
IAPP: Certified Information Privacy Professional / U.S. Private-Sector (CIPP/US) Training	CIPP/US	x	x	x
IAPP: Certified Information Privacy Professional / U.S. Government (CIPP/G) Training	CIPP/G	x	x	x
IAPP: Certified Information Privacy Technologist (CIPT) Training	CIPT	x	x	x
IAPP: Certification Foundation Training*	N/A	x	x	x
IAPP: Certified Information Privacy Manager (CIPM) Training	CIPM		x	x
Privacy Professor – Privacy Impact Assessment Tool Kit	N/A	x	x	x

*This course will be retired on July 1st, 2015

InfoSec and Privacy Position Description
Core: InfoSec Analyst

It is highly recommended that the InfoSec Analyst explore training courses mapped to pertinent competencies for professional development.

Course	Certification	Position Level		
		Level 1	Level 2	Level 3
SANS - SEC301: Intro to Information Security	GISF	x	x	x
SANS - SEC401: Security Essentials Bootcamp Style	GSEC	x	x	x
ISACA: Certified in Risk and Information Systems Control (CRISC) Training	CRISC		x	x
ISACA: Certified Information Security Manager (CISM) Training	CISM			x
ISC2: Certified Information Systems Security Professional (CISSP) Training	CISSP		x	x
CompTIA: Network+ N10-006	Network+	x	x	x
CompTIA: Security+ SY0-401	Security+	x	x	x
EC Council: Certified Ethical Hacker (CEH) Training	CEH			x

InfoSec and Privacy Position Description
Core: InfoSec and Privacy Auditor

It is highly recommended that the InfoSec and Privacy Auditor explore training courses mapped to pertinent competencies for professional development.

Course	Certification	Position Level		
		Level 1	Level 2	Level 3
SANS - SEC401: Security Essentials Bootcamp Style	GSEC	x	x	x
SANS - SEC566: Implementing and Auditing the Critical Security Controls - In-Depth	N/A		x	x
SANS - LEG523: Law of Data Security and Investigations	GLEG	x	x	x
ISACA: Certified Information Systems Auditor (CISA) Training	CISA		x	x
IAPP: Certified Information Privacy Professional / U.S. Private-Sector (CIPP/US) Training	CIPP/US	x	x	x
IAPP: Certified Information Privacy Professional / U.S. Government (CIPP/G) Training	CIPP/G	x	x	x
IAPP: Certified Information Privacy Technologist (CIPT) Training			x	x

InfoSec and Privacy Position Description
Core: InfoSec Architect

It is highly recommended that the InfoSec Architect explore training courses mapped to pertinent competencies for professional development.

Course	Certification	Position Level		
		Level 1	Level 2	Level 3
SANS - MGT305: Technical Communication and Presentation Skills for Security Professionals	N/A	x	x	x
SANS - SEC504: Hacker Techniques, Exploits & Incident Handling	GCIH		x	x
ISC2: Certified Information Systems Security Professional (CISSP)	CISSP		x	x
ISC2: Information Systems Security Architecture Professional (ISSAP) Training	ISSAP	x	x	x
ISACA: Certified Information Security Manager (CISM) Training	CISM			x
InfoSec Institute: Enterprise Security Architecture and Design Online (ONL-212)	N/A	x	x	x
InfoSec Institute: Intrusion Prevention Online (SEC-204)	N/A		x	x
EC Council: Certified Network Defense Architect (CNDA) Training	CNDA		x	x

InfoSec and Privacy Position Description
Core: InfoSec Engineer

It is highly recommended that the InfoSec Engineer explore training courses mapped to pertinent competencies for professional development.

Course	Certification	Position Level		
		Level 1	Level 2	Level 3
SANS - SEC566: Implementing and Auditing the Critical Security Controls - In-Depth	GCCC	x	x	x
SANS - SEC504: Hacker Techniques, Exploits & Incident Handling	GCIH		x	x
ISC2: Certified Information Systems Security Professional (CISSP) Training	CISSP		x	x
ISC2: Information Systems Security Engineering Professional (ISSEP) Training	ISSEP	x	x	x
ISACA: Certified Information Security Manager (CISM) Training	CISM		x	x
Defense Cyber Investigation Training Academy: Introduction to Log Analysis	N/A			x
Global Knowledge: Cybersecurity Investigations and Network Forensics Analysis: Practical Techniques for Analyzing Suspicious Network Traffic	N/A		x	x
EC Council: Certified Security Analyst (ECSA) Training	ECSA	x	x	x
EC Council: Licensed Penetration Tester (LPT) Training	LPT		x	x

Go back to InfoSec and Privacy Training by Position Description

InfoSec and Privacy Position Description
Core: InfoSec Manager

It is highly recommended that the InfoSec Manager explore training courses mapped to pertinent competencies for professional development.

Course	Certification	Position Level		
		Level 1	Level 2	Level 3
SANS - MGT512: Security Leadership Essentials for Manager with Knowledge Compression	GSLC	x	x	x
SANS - MGT514: IT Security Strategic Planning, Policy and Leadership	N/A	x	x	x
SANS - MGT305: Technical Communication and Presentation Skills for Security Professionals	N/A	x	x	x
SANS - SEC504: Hacker Techniques, Exploits & Incident Handling	GCIGH		x	x
ISACA: Certified Information Security Manager (CISM) Training	CISM	x	x	x
ISACA: Certified in Risk and Information Systems Control (CRISC) Training	CRISC		x	x
ISACA: Certified in the Governance of Enterprise IT (CGEIT) Training	CGEIT		x	x
ISC2: Certified Information Systems Security Professional (CISSP) Training	CISSP	x	x	x

InfoSec and Privacy Position Description
Hybrid: IT Director

It is highly recommended that the IT Director explore training courses mapped to pertinent competencies for professional development.

Course	Certification
SANS – SEC301: Intro to Information Security	GISF
SANS - SEC464: CyberSecurity Training for IT Administrators	N/A
SANS – LEG523: Law of Data Security Investigations	N/A
SANS - MGT514: IT Security Strategic Planning, Policy and Leadership	N/A
ISACA: An Introduction to Privacy and Data Protection	N/A
ISC2: Certified Information Systems Security Professional (CISSP) Training	CISSP
ISC2: Information Systems Security Management Professional (ISSMP) Training	ISSMP
SC: Business Practices	N/A

InfoSec and Privacy Position Description
Hybrid: Network Administrator

It is highly recommended that the Network Administrator explore training courses mapped to pertinent competencies for professional development.

Course	Certification
SANS - SEC464: CyberSecurity Training for IT Administrators	N/A
SANS - SEC501: Advanced Security Essentials - Enterprise Defender	GCED
ISC2: System Security Certified Practitioner (SSCP) Training	SSCP
CompTIA: Network+ N10-006	Network+
EMC2: Information Storage and Management v2	N/A

InfoSec and Privacy Position Description
Hybrid: Program Manager (Compliance / Privacy)

It is highly recommended that the Program Manager (Compliance / Privacy) to explore training courses mapped to pertinent competencies for professional development.

Course	Certification
IAPP: Certified Information Privacy Professional / U.S. Government (CIPP/G) Training	CIPP/G
IAPP: Certified Information Privacy Professional / U.S. Private-Sector (CIPP/US) Training	CIPP/US
IAPP: Certified Information Privacy Manager (CIPM) Training	CIPM

InfoSec and Privacy Position Description
Hybrid: Program Manager (Compliance / Security)

It is highly recommended that the Program Manager (Compliance / Security) to explore training courses mapped to pertinent competencies for professional development.

Course	Certification
SANS - MGT535: Incident Response Team Management	N/A
ISACA: Certified Information Security Manager (CISM) Training	CISM
DRII: Program Management Principles in Business Continuity Planning	N/A
SC: Business Practices	N/A
SC: Legal Aspects of Purchasing	N/A
SC: Procurement Code in a Nutshell	N/A

Domain: InfoSec Governance and Compliance
Competency: InfoSec Program Management (Part 1)

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
SANS - MGT512: Security Leadership Essentials for Manager with Knowledge Compression	GSLC			x
SANS - SEC440: Critical Security Controls: Planning, Implementing and Auditing	N/A		x	x
SANS - MGT514: IT Security Strategic Planning, Policy and Leadership	N/A		x	x
SANS - SEC301: Intro to Information Security	GISF	x	x	x
SANS - SEC401: Security Essentials Bootcamp Style	GSEC		x	x
SANS - SEC464: CyberSecurity Training for IT Administrators	N/A		x	x
Mile2: Certified Information Systems Security Officer (CISSO) Training	CISSO		x	x
Mile2: Certified Information Systems Security Risk Manager (CISSRM) Training	CISSRM		x	x
Mile2: Certified Information Systems Security Manager (CISSM) Training	CISSM		x	x
Mile2: Certified Security Leadership Officer (CSLO) Training	CSLO			x
Mile2: Certified Security Sentinel (CSS) Training	CSS	x	x	x

Domain: InfoSec Governance and Compliance
Competency: InfoSec Program Management (Part 2)

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
CompTIA: CompTIA Advanced Security Practitioner (CASP) Training	CASP		x	x
CompTIA: Security+ SY0-401	Security+	x	x	x
EC Council: Certified Chief Information Security Officer (CCISO) Training	CCISO			x
EC Council: Certified Security Specialist (ECSS) Training	ECSS			x
Expanding Security: Secure Software Management 101	N/A	x	x	x
InfoSec Institute: SCADA Security (SEC-325)	N/A		x	x
ISACA: Certified Information Systems Auditor (CISA) Training	CISA		x	x
ISACA: Certified Information Security Manager (CISM) Training	CISM			x
ISACA: Certified in Risk and Information Systems Control (CRISC) Training	CRISC		x	x
ISC2: System Security Certified Practitioner (SSCP) Training	SSCP		x	x
ISC2: Certified Authorization Professional (CAP) Training	CAP		x	x
ISC2: Certified Information Systems Security Professional (CISSP) Training	CISSP		x	x
ISC2: HealthCare Information Security and Privacy Practitioner (HCISPP) Training Note: Course related to healthcare	N/A		x	x

Domain: InfoSec Governance and Compliance
Competency: InfoSec Regulation

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
SANS - LEG523: Law of Data Security and Investigations	GLEG	x	x	x
EC Council: Certified Chief Information Security Officer (CCISO) Training	CCISO			x
EC Council: Certified Security Analyst (ECSA) Training	ECSA	x	x	x
ISACA: Certified Information Systems Auditor (CISA) Training	CISA		x	x
ISACA: Certified Information Security Manager (CISM) Training	CISM			x
ISC2: Certified Authorization Professional (CAP) Training	CAP		x	x
ISC2: Certified Information Systems Security Professional (CISSP) Training	CISSP		x	x
ISC2: HealthCare Information Security and Privacy Practitioner (HCISPP) Training Note: Course related to healthcare	N/A		x	x
Mile2: Certified Information Systems Security Officer (CISSO) Training	CISSO		x	x
Pearson: CISSP Video Course Domain 6 - Law, Investigation and Ethics, Downloadable Version	CISSP		x	x

Go back to InfoSec and Privacy Training by Competency

Domain: InfoSec Governance and Compliance
Competency: Policy communication, enforcement and exception management

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
SANS - MGT514: IT Security Strategic Planning, Policy and Leadership	N/A		x	x
SANS - SEC566: Implementing and Auditing the Critical Security Controls - In-Depth	GCCC		x	x
EC Council: Certified Chief Information Security Officer (CCISO) Training	CCISO			x
InfoSec Institute: Information Security Policy Essentials (SEC-211)	N/A	x	x	x
ISACA: Certified Information Systems Auditor (CISA) Training	CISA		x	x
IAITAM: Policy Management Advanced Study Course	N/A		x	x

Go back to InfoSec and Privacy Training by Competency

Domain: Risk Strategy and Management
Competency: Risk Assessment

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
SANS - MGT415: A Practical Introduction to Risk Assessment	N/A	x	x	x
CompTIA: CompTIA Advanced Security Practitioner (CASP) Training	CASP		x	x
CompTIA: Security+ SY0-401	Security+	x	x	x
Expanding Security: Risk Management 101	N/A	x	x	x
IARCP: Certified Information Systems Risk & Compliance Professional (CISRCP) Training	CISRCP		x	x
IARCP: Certified Risk and Compliance Management Professional (CRCMP) Training	CRCMP		x	x
ISACA: Certified Information Security Manager (CISM) Training	CISM			x
ISACA: Certified in Risk and Information Systems Control (CRISC) Training	CRISC		x	x
ISC2: Certified Authorization Professional (CAP) Training	CAP		x	x
ISC2: HealthCare Information Security and Privacy Practitioner (HCISPP) Training Note: Course related to healthcare	N/A		x	x

Go back to InfoSec and Privacy Training by Competency

Domain: Risk Strategy and Management
Competency: Risk Acceptance

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
InfoSec Institute: CGEIT Training (IA-212)	CGEIT			x
ISACA: Certified in the Governance of Enterprise IT (CGEIT) Training	CGEIT			x
ISACA: Certified Information Security Manager (CISM) Training	CISM			x
ISACA: Certified in Risk and Information Systems Control (CRISC) Training	CRISC		x	x
ISC2: Certified Authorization Professional (CAP) Training	CAP		x	x
IARCP: Certified Information Systems Risk & Compliance Professional (CISRCP) Training	CISRCP		x	x
IARCP: Certified Risk and Compliance Management Professional (CRCMP) Training	CRCMP		x	x

Go back to InfoSec and Privacy Training by Competency

Domain: Risk Strategy and Management
Competency: Risk Mitigation

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
InfoSec Institute: CGEIT Training (IA-212)	CGEIT			x
ISACA: Certified in the Governance of Enterprise IT (CGEIT) Training	CGEIT			x
ISACA: Certified Information Security Manager (CISM) Training	CISM			x
ISACA: Certified in Risk and Information Systems Control (CRISC) Training	CRISC		x	x
ISC2: Certified Authorization Professional (CAP) Training	CAP		x	x

Domain: Threat and Vulnerability Management
Competency: Vulnerability Management (Part 1)

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
SANS - SEC542: Web App Penetration Testing and Ethical Hacking	GWAPT		x	x
SANS - SEC560: Network Penetration Testing and Ethical Hacking	GPEN		x	x
SANS - SEC561: Intense Hands-on Pen Testing Skill Development	N/A			x
SANS - SEC580: Metasploit Kung Fu for Enterprise Pen Testing	N/A			x
SANS - SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses	GAWN		x	x
SANS - SEC642: Advanced Web App Penetration Testing and Ethical Hacking	N/A			x
SANS - SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	N/A			x
SANS - SEC760: Advanced Exploit Development for Penetration Testers	N/A			x
Mile2: Certified Penetration Testing Consultant (CPTC) Training	CPTC			x
Mile2: Certified Penetration Testing Engineer (CPTE) Training	CPTE			x
Mile2: Certified Vulnerability Assessor (CVA) Training	CVA	x	x	x
OpenSecurityTraining.info: Introduction to Vulnerability Assessment	N/A	x	x	x

Continue to *Vulnerability Management (Part 2)*

Go back to *InfoSec and Privacy Training by Competency*

Domain: Threat and Vulnerability Management
Competency: Vulnerability Management (Part 2)

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
CompTIA: Network+ N10-006	Network+	x	x	x
CompTIA: Security+ SY0-401	Security+	x	x	x
EC Council: Certified Ethical Hacker (CEH) Training	CEH		x	x
EC Council: Licensed Penetration Tester (LPT) Training	LPT		x	x
InfoSec Institute: Advanced Ethical Hacking & Advanced Persistent Threat (SEC-300)	N/A			x
InfoSec Institute: Advanced Hacking Online (SEC-300)	N/A			x
InfoSec Institute: Expert Penetration Testing (SEC-209)	N/A			x
InfoSec Institute: Intrusion Prevention Online (SEC-204)	N/A		x	x
InfoSec Institute: Mobile Device Penetration Testing (SEC-556)	N/A		x	x
InfoSec Institute: Penetration Testing Online (ONL-206)	N/A		x	x
InfoSec Institute: Web Application Penetration Testing (SEC-402)	N/A		x	x
Mile2: Certified Professional Ethical Hacker (CPEH) Training	CPEH		x	x

Domain: Threat and Vulnerability Management
Competency: Security Incident and Event Management

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
SANS - FOR508: Advanced Digital Forensic Analysis and Incident Response	GCFA			x
SANS - SEC504: Hacker Techniques, Exploits & Incident Handling	GCIH		x	x
SANS - MGT535: Incident Response Team Management	N/A		x	x
SANS - SEC503: Intrusion Detection In Depth	N/A		x	x
CompTIA: Network+ N10-006	Network+	x	x	x
CompTIA: Security+ SY0-401	Security+	x	x	x
Defense Cyber Investigation Training Academy: Introduction to Log Analysis	N/A	x	x	x
InfoSec Institute: Intrusion Prevention Online (SEC-204)	N/A		x	x
ISACA: Certified Information Security Manager (CISM) Training	CISM			x
Mile2: Certified Incident Handling Engineer (CIHE) Training	CIHE		x	x
Mile2: Certified Information Systems Security Officer (CISSO) Training	CISSO		x	x
Mile2: Certified Security Sentinel (CSS) Training	CSS	x	x	x
SEI Certification: Certified Computer Security Incident Handler (CSIH) Training	CSIH		x	x

Domain: Threat and Vulnerability Management
Competency: Forensics Analysis

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
SANS - FOR408: Windows Forensic Analysis	GCFE		x	x
SANS - FOR508: Advanced Digital Forensic Analysis and Incident Response	GCFA			x
SANS - FOR518: Mac Forensic Analysis	N/A			x
SANS - FOR526: Memory Forensics In-Depth	N/A		x	x
SANS - FOR572: Advanced Network Forensics and Analysis	GNFA			x
SANS - FOR585: Advanced Smartphone Forensics	N/A			x
SANS - FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques	GREM		x	x
EC Council: Computer Hacking Forensic Investigator (CHFI) Training	CHFI		x	x
InfoSec Institute: Computer Forensics Training (SEC-203)	N/A	x	x	x
ISC2: Certified Cyber Forensics Professional (CCFP) Training	CCFP		x	x
Mile2: Certified Digital Forensics Examiner (CDFE) Training	CDFE		x	x
Mile2: Certified Information Systems Security Officer (CISSO) Training	CISSO		x	x
Mile2: Certified Network Forensics Examiner (CNFE) Training	CNFE			x

Go back to InfoSec and Privacy Training by Competency

Domain: Threat and Vulnerability Management
Competency: Threat Identification and Categorization

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
SANS - SEC501: Advanced Security Essentials - Enterprise Defender	GCED		x	x
CompTIA: Network+ N10-006	Network+	x	x	x
CompTIA: Security+ SY0-401	Security+	x	x	x
Defense Cyber Investigation Training Academy: Cyber Insider Threats Analysis Training	N/A		x	x
Defense Cyber Investigation Training Academy: Introduction to Cyber Insider Threat Course	N/A	x	x	x
Global Knowledge: Cybersecurity Investigations and Network Forensics Analysis: Practical Techniques for Analyzing Suspicious Network Traffic	N/A		x	x
Global Knowledge: Cybersecurity Investigations and Network Forensics Analysis: Practical Techniques for Analyzing VoIP Traffic	N/A		x	x
Global Knowledge: Cybersecurity Investigations and Network Forensics Analysis: Practical Techniques for Analyzing WiFi Traffic	N/A		x	x

Go back to InfoSec and Privacy Training by Competency

Domain: Privacy
Competency: Privacy Program Administration

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
IAPP: Certification Foundation Training*	N/A	x	x	x
IAPP: Certified Information Privacy Manager (CIPM) Training	CIPM			x
IAPP: Certified Information Privacy Professional / U.S. Private-Sector (CIPP/US) Training	CIPP/US		x	x
IAPP: Certified Information Privacy Professional / U.S. Government (CIPP/G) Training	CIPP/G		x	x
IAPP: Certified Information Privacy Technologist (CIPT) Training	CIPT		x	x

*This course will be retired on July 1st, 2015

Go back to InfoSec and Privacy Training by Competency

Domain: Privacy
Competency: Privacy Compliance

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
EHRs and HIPAA: Steps for Maintaining the Privacy and Security of Patient Information	N/A		x	x
HHS: Examining Compliance with the HIPAA Privacy Rule	N/A		x	x
HHS: HIPAA and You: Building a Culture of Compliance	N/A		x	x
HHS: Privacy Awareness Training	N/A		x	x
IAPP: Certification Foundation Training*	N/A	x	x	x
IAPP: Certified Information Privacy Manager (CIPM) Training	CIPM			x
IAPP: Certified Information Privacy Professional / U.S. Private-Sector (CIPP/US) Training	CIPP/US		x	x
IAPP: Certified Information Privacy Professional / U.S. Government (CIPP/G) Training	CIPP/G		x	x
IAPP: Certified Information Privacy Technologist (CIPT) Training	CIPT		x	x
ISACA: An Introduction to Privacy and Data Protection	N/A	x	x	x
ISC2: HealthCare Information Security and Privacy Practitioner (HCISPP) Training Note: Course related to healthcare	N/A		x	x

*This course will be retired on July 1st, 2015

Go back to InfoSec and Privacy Training by Competency

Domain: Privacy
Competency: Privacy Impact Assessment

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
IAPP: Certification Foundation Training*	N/A	x	x	x
IAPP: Certified Information Privacy Manager (CIPM) Training	CIPM			x
IAPP: Certified Information Privacy Professional / U.S. Private-Sector (CIPP/US) Training	CIPP/US		x	x
IAPP: Certified Information Privacy Professional / U.S. Government (CIPP/G) Training	CIPP/G		x	x
IAPP: Certified Information Privacy Technologist (CIPT) Training	CIPT		x	x
ISACA: Certified Information Systems Auditor (CISA) Training	CISA		x	x
ISC2: HealthCare Information Security and Privacy Practitioner (HCISPP) Training Note: Course related to healthcare	N/A		x	x
Privacy Professor – Privacy Impact Assessment Tool Kit	N/A	x	x	x

*This course will be retired on July 1st, 2015

Go back to *InfoSec and Privacy Training by Competency*

Domain: Privacy

Competency: Data Classification

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
TechTarget: Data classification Podcast	N/A	x	x	x
State of South Carolina Data Classification Training Note: This is a self-paced training	N/A	x	x	x

Domain: Privacy
Competency: Privacy Incident Response

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
IAPP: Certification Foundation Training*	N/A	x	x	x

*This course will be retired on July 1st, 2015

Domain: Data Security
Competency: Data Management

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
CompTIA: Security+ SY0-401	Security+	x	x	x
Expanding Security: Data Administration 101	N/A	x	x	x
ISACA: An Introduction to Privacy and Data Protection	N/A	x	x	x
UMBC Training: Advanced Data Warehousing	N/A			x
UMBC Training: Foundations of Data Mining	N/A	x	x	x

Go back to InfoSec and Privacy Training by Competency

Domain: Data Security
Competency: Secure Data Transmission and Storage

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
CompTIA: Security+ SY0-401	Security+	x	x	x
EMC2: Proven Professional Information Storage Associate v2	EMCISA		x	x
EMC2: Information Storage and Management v2	N/A	x	x	x
UMBC Training: Advanced Data Warehousing	N/A			x
UMBC Training: Designing the Data Warehouse Workshop	N/A		x	x
Pearson: CISSP Video Course Domain 7 - Telecommunications and Networking, Downloadable Version	CISSP		x	x

Go back to InfoSec and Privacy Training by Competency

Domain: Data Security
Competency: Cryptographic Safeguards

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
CEC-Security LLC: Introduction to Cryptography	N/A	x	x	x
CompTIA: Network+ N10-006	Network+	x	x	x
CompTIA: Security+ SY0-401	Security+	x	x	x
OpenSecurityTraining.info: Understanding Cryptology: Cryptanalysis	N/A		x	x
InfoSec Institute: Cryptography Short Course (CISSP Domain #5)	CISSP		x	x

Go back to InfoSec and Privacy Training by Competency

Domain: IS Acquisition, Development and Maintenance
Competency: System Development Lifecycle

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
CompTIA: CompTIA Advanced Security Practitioner (CASP) Training	CASP		x	x
CompTIA: Security+ SY0-401	Security+	x	x	x
ISACA: Certified Information Systems Auditor (CISA) Training	CISA		x	x
ISC2: Certified Authorization Professional (CAP) Training	CAP		x	x
ISC2: Information Systems Security Architecture Professional (ISSAP) Training	ISSAP	x	x	x
ISC2: Information Systems Security Engineering Professional (ISSEP) Training	ISSEP	x	x	x
ISC2: Information Systems Security Management Professional (ISSMP) Training	ISSMP		x	x

Go back to InfoSec and Privacy Training by Competency

Domain: IS Acquisition, Development and Maintenance
Competency: Secure Software Development

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
SANS - DEV522: Defending Web Applications Security Essentials	GWEB	x	x	x
SANS - DEV541: Secure Coding in Java/JEE: Developing Defensible Applications	GWAPT		x	x
SANS - DEV544: Secure Coding in .NET: Developing Defensible Applications	GSSP-JAVA		x	x
SANS - DEV536: Secure Coding: Developing Defensible Applications	GSSP-.NET		x	x
SANS - DEV543: Secure Coding in C & C++	N/A		x	x
ISACA: Certified Information Systems Auditor (CISA) Training	CISA		x	x
ISC2: Certified Secure Software Lifecycle Professional (CSSLP) Training	CSSLP	x	x	x
Expanding Security: Secure Software Engineering 101	N/A	x	x	x
OpenSecurityTraining.Info: Introduction to Software Exploits	N/A	x	x	x

Go back to InfoSec and Privacy Training by Competency

Domain: IS Acquisition, Development and Maintenance
Competency: Procurement Methods (Part 1)

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
SC: Business Practices	N/A	x	x	x
SC: Compendium Overview	N/A		x	x
SC: Construction Procurement - Written Determinations	N/A			x
SC: Contract Administration	N/A		x	x
SC: Ethics in Public Procurement	N/A	x	x	x
NIGP: Contract Administration	N/A		x	x
NIGP: Ethics A Survival Kit for Public Procurement	N/A	x	x	x
NIGP: Introduction to Public Procurement	N/A	x	x	x
NIGP: Sourcing in the Public Sector	N/A		x	x
NIGP: Specification Writing	N/A		x	x

Domain: IS Acquisition, Development and Maintenance
Competency: Procurement Methods (Part 2)

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
SC: FOIA and Document Requests in SC	N/A			x
SC: FOIA's Meeting Rules & the Evaluation Process	N/A			x
SC: Issues in GMP Contracting	N/A			x
SC: IT Vendor Procurement Training	N/A		x	x
SC: Legal Aspects of Purchasing	N/A		x	x
SC: Procurement Code in a Nutshell	N/A	x	x	x
SC: Procurement of Architect / Engineer Services	N/A			x
SC: RFP Process	N/A		x	x
SC: Standard General Bidding Instructions	N/A	x	x	x
SC: Standard Terms & Conditions	N/A	x	x	x

Domain: Physical and Environmental Security
Competency: Physical Access Control

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
Safari: CISSP Video Course Domain 4 – Physical Security	CISSP		x	x
Pearson: CISSP Video Course Domain 4 - Physical Security, Downloadable Version	CISSP		x	x

Domain: Physical and Environmental Security
Competency: Environmental Security

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
Safari: CISSP Video Course Domain 4 – Physical Security	CISSP		x	x
Pearson: CISSP Video Course Domain 4 - Physical Security, Downloadable Version	CISSP		x	x

Domain: Physical and Environmental Security
Competency: Equipment Cleansing and Disposal

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
IAITAM: Disposal Management Advanced Study Course	N/A		x	x
IAITAM: Certified IT Asset Disposition (CITAD) course	CITAD	x	x	x

Go back to InfoSec and Privacy Training by Competency

Domain: Business Continuity Management and Disaster Recovery
Competency: Business Impact Assessment

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
DRII: BCOE 300 Introduction to Business Impact Analysis	N/A	x	x	x

Domain: Business Continuity Management and Disaster Recovery
Competency: Business Continuity Planning

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
Global Knowledge: CBAP Prep Boot Camp	CBAP			x
IBCT: Effective Business Continuity Management Systems (ECP-601)	CCM			x
DRII: BCOE 600 Business Continuity Plan Implementation	N/A	x	x	x
DRII: BCOE 400 Developing Business Continuity Strategies	N/A	x	x	x
DRII: BCOE 100 Program Management Principles in Business Continuity Planning	N/A	x	x	x
DRII: BCOE 800 Exercising and Maintaining Plans	N/A	x	x	x

Domain: Business Continuity Management and Disaster Recovery
Competency: Data Backup and Restoration

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
EC Council: Disaster Recovery Professional (EDRP) Training	EDRP		x	x
EMC2: Backup Recovery Systems and Architecture	N/A	x	x	x
EMC2: Information Storage and Management v2	EMCISA	x	x	x
InfoSec Institute: Data Recovery Training (SEC-205)	CDRP	x	x	x

Go back to InfoSec and Privacy Training by Competency

Domain: Business Continuity Management and Disaster Recovery
Competency: Crisis Management

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
EC Council: Disaster Recovery Professional (EDRP) Training	EDRP		x	x
DRII: BCOE 900 Crisis Communication and Coordinating with External Agencies	N/A	x	x	x
DRII: BCOE 500 Emergency Preparedness and Response	N/A	x	x	x
Mile2: Certified Disaster Recovery Engineer (CDRE) Training	CDRE		x	x

Domain: Network and Infrastructure Security
Competency: Secure Network Engineering

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
CompTIA: Network+ N10-006	Network+	x	x	x
CompTIA: Security+ SY0-401	Security+	x	x	x
EC Council: Network Security Administrator (ENSA) Training	ENSA		x	x
EC Council: Certified Network Defense Architect (CNDA) Training	CNDA		x	x
Defense Cyber Investigation Training Academy: Introduction to Networks and Computer Hardware	N/A	x	x	x
Global Knowledge: Dell SonicWall Network Security Basic Administration (NS-102)	N/A	x	x	x
InfoSec Institute: Enterprise Security Architecture and Design Online (ONL-212)	N/A	x	x	x

Domain: Network and Infrastructure Security
Competency: Network Defense Analysis and Control

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
SANS - SEC501: Advanced Security Essentials - Enterprise Defender	GCED		x	x
CompTIA: Network+ N10-006	Network+	x	x	x
CompTIA: Security+ SY0-401	Security+	x	x	x
EC Council: Certified Network Defense Architect (CNDA) Training	CNDA		x	x
EC Council: Network Security Administrator (ENSA) Training	ENSA		x	x
Global Knowledge: Cybersecurity Investigations and Network Forensics Analysis: Practical Techniques for Analyzing Suspicious Network Traffic	N/A		x	x
Global Knowledge: Cybersecurity Investigations and Network Forensics Analysis: Practical Techniques for Analyzing VoIP Traffic	N/A		x	x
Global Knowledge: Cybersecurity Investigations and Network Forensics Analysis: Practical Techniques for Analyzing WiFi Traffic	N/A		x	x
Global Knowledge: Enterprise WiFi Fundamentals	N/A		x	x

Go back to InfoSec and Privacy Training by Competency

Domain: Identity Access Management
Competency: Access Management

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
ISACA: Certified Information Security Manager (CISM) Training	CISM			x
CompTIA: Security+ SY0-401	Security+	x	x	x
Identity Management Institute: Certified Identity Risk Manager (CIRM) Training	CIRM	x	x	x
TechTarget: Access Control Models, Administration, IPS/IDS Training Video	CISSP		x	x
TechTarget: Access Control Security Models Training Video	CISSP		x	x
Pearson: CISSP Video Course Domain 2 - Access Control, Downloadable Version	CISSP		x	x

Go back to InfoSec and Privacy Training by Competency

Domain: Identity Access Management
Competency: Identity Management

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
ISACA: Certified Information Security Manager (CISM) Training	CISM			x
CompTIA: Network+ N10-006	Network+	x	x	x
CompTIA: Security+ SY0-401	Security+	x	x	x
OpenSecurityTraining.info: Offensive, Defensive, and Forensic Techniques for Determining Web User Identity	N/A		x	x
TechTarget: Authentication Technologies, Federated Identities Training Video	CISSP		x	x
Pearson: CISSP Video Course Domain 2 - Access Control, Downloadable Version	CISSP		x	x

Domain: Education and Training
Competency: Training Needs Analysis

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
ATD: Evaluating Learning Impact Certificate	N/A		x	x
ATD: Managing Learning Programs Certificate	N/A		x	x
Langevin: Training Needs Analysis	N/A		x	x

Domain: Education and Training
Competency: Training Curriculum Design and Development

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
ATD: Advanced E-Learning Instructional Design Certificate	N/A			x
ATD: Designing Learning Certificate	N/A		x	x
ATD: Master Instructional Designer Program	N/A			x
ATD: Master Trainer Program	N/A		x	x

Go back to InfoSec and Privacy Training by Competency

Domain: Education and Training
Competency: Training Delivery

Course	Certification	Proficiency Level		
		Level 1	Level 2	Level 3
SANS - MGT305: Technical Communication and Presentation Skills for Security Professionals	N/A	x	x	x
ATD: Essentials of Coaching Government Employees on the Job	N/A	x	x	x
ATD: Training Certificate	N/A		x	x
ATD: Master Trainer Program	N/A		x	x
ATD: Introduction to Training Certificate	N/A	x	x	x
ATD: Presentation Skills Certificate	N/A	x	x	x
ATD: Facilitating Synchronous Learning Certificate	N/A	x	x	x

Go back to InfoSec and Privacy Training by Competency

Certification:
Certified Authorization Professional (CAP)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
InfoSec governance and compliance	InfoSec program management	ISC2: Certified Authorization Professional (CAP) Training		x	x
	InfoSec regulation			x	x
Risk strategy and management	Risk acceptance			x	x
	Risk assessment			x	x
IS acquisition, development and maintenance	Risk mitigation			x	x
	System development lifecycle			x	x

Go back to *InfoSec and Privacy Certifications Page 1*

Certification:
CompTIA Advanced Security Professional (CASP)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
InfoSec governance and compliance	InfoSec program management	CompTIA: CompTIA Advanced Security Practitioner (CASP) Training		x	x
Risk strategy and management	Risk assessment			x	x
IS acquisition, development and maintenance	System development lifecycle			x	x

Go back to InfoSec and Privacy Certifications Page 1

Certification:
Certified Business Analysis Professional (CBAP)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Business continuity management and disaster recovery	Business continuity planning	Global Knowledge: CBAP Prep Boot Camp			x

Certification:
Certified Cyber Forensics Professional (CCFP)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and vulnerability management	Forensics analysis	ISC2: Certified Cyber Forensics Professional (CCFP) Training		x	x

Certification:
Certified Chief Information Security Officer (CCISO)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
InfoSec governance and compliance	InfoSec program management	EC Council: Certified Chief Information Security Officer (CCISO) Training			x
	InfoSec regulation				x
	Policy communication, enforcement and exception management				x

Go back to InfoSec and Privacy Certifications Page 1

Certification:
Certified Continuity Manager (CCM)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Business continuity management and disaster recovery	Business continuity planning	IBCT: Effective Business Continuity Management Systems (ECP-601)			x

Certification:
Certified Digital Forensic Examiner (CDFE)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and vulnerability management	Forensics analysis	Mile2: Certified Digital Forensics Examiner (CDFE) Training		x	x

Go back to InfoSec and Privacy Certifications Page 1

Certification:
Certified Disaster Recovery Engineer (CDRE)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Business continuity management and disaster recovery	Crisis management	Mile2: Certified Disaster Recovery Engineer (CDRE) Training		x	x

Go back to InfoSec and Privacy Certifications Page 1

Certification:
Certified Data Recovery Professional (CDRP)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Business continuity management and disaster recovery	Data backup and restoration	InfoSec Institute: Data Recovery Training (SEC-205)	x	x	x

Go back to InfoSec and Privacy Certifications Page 1

Certification:
Certified Ethical Hacker (CEH)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and vulnerability management	Vulnerability management	EC Council: Certified Ethical Hacker (CEH) Training		x	x

Go back to *InfoSec and Privacy Certifications Page 1*

Certification:
GIAC Certified Forensic Examiner (GCFE)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and vulnerability management	Forensics analysis	SANS - FOR408: Windows Forensic Analysis		x	x

Go back to *InfoSec and Privacy Certifications Page 2*

Certification:
Certified in the Governance of Enterprise IT (CGEIT)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Risk strategy and management	Risk acceptance	InfoSec Institute: Certified in the Governance of Enterprise IT (CGEIT) Training (IA-212)			x
	Risk mitigation				x
	Risk acceptance	ISACA: Certified in the Governance of Enterprise IT (CGEIT) Training			x
	Risk mitigation				x

Certification:

Computer Hacking Forensic Investigator (CHFI)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and vulnerability management	Forensics analysis	EC Council: Computer Hacking Forensic Investigator (CHFI) Training		x	x

Go back to InfoSec and Privacy Certifications Page 1

Certification:
Certified Incident Handling Engineer (CIHE)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and vulnerability management	Security incident and event management	Mile2: Certified Incident Handling Engineer (CIHE) Training		x	x

Certification:
Certified Information Privacy Manager (CIPM)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Privacy	Privacy compliance	IAPP: Certified Information Privacy Manager (CIPM) Training			x
	Privacy impact assessment				x
	Privacy program administration				x
	Privacy violation response				x

Go back to *InfoSec and Privacy Certifications Page 1*

Certification:

Certified Information Privacy Professional/U.S. Private-Sector (CIPP/US)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Privacy	Privacy compliance	IAPP: Certified Information Privacy Professional / U.S. Private-Sector (CIPP/US) Training		x	x
	Privacy impact assessment			x	x
	Privacy program administration			x	x
	Privacy violation response			x	x

Go back to InfoSec and Privacy Certifications Page 1

Certification:

Certified Information Privacy Professional/U.S. Government (CIPP/G)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Privacy	Privacy compliance	IAPP: Certified Information Privacy Professional / U.S. Government (CIPP/G) Training		x	x
	Privacy impact assessment			x	x
	Privacy program administration			x	x
	Privacy violation response			x	x

Certification:
Certified Information Privacy Technologist (CIPT)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Privacy	Privacy compliance	IAPP: Certified Information Privacy Technologist (CIPT) Training		x	x
	Privacy impact assessment			x	x
	Privacy program administration			x	x
	Privacy violation response			x	x

Certification:

Certified Identity Risk Manager (CIRM)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Identity access management	Access management	Identity Management Institute: Certified Identity Risk Manager (CIRM) Training	x	x	x

Certification:
Certified Information Systems Auditor (CISA)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
InfoSec governance and compliance	InfoSec program management	ISACA: Certified Information Systems Auditor (CISA) Training		x	x
InfoSec governance and compliance	InfoSec regulation			x	x
Privacy	Policy communication, enforcement and exception management			x	x
Privacy	Privacy impact assessment			x	x
IS acquisition, development and maintenance	Secure software development			x	x
IS acquisition, development and maintenance	System development lifecycle			x	x

Go back to InfoSec and Privacy Certifications Page 1

Certification:
Certified Information Security Manager (CISM)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Identity access management	Access management	ISACA: Certified Information Security Manager (CISM) Training			x
	Identity management				x
InfoSec governance and compliance	InfoSec program management				x
	InfoSec regulation				x
Risk strategy and management	Risk acceptance				x
	Risk assessment				x
	Risk mitigation				x
Threat and vulnerability management	Security incident and event management				x

Go back to InfoSec and Privacy Certifications Page 1

Certification:

Certified Information Systems Risk & Compliance Professional (CISRCP)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Risk strategy and management	Risk acceptance	IARCP: Certified Information Systems Risk & Compliance Professional (CISRCP) Training		x	x
	Risk assessment			x	x

Certification:

Certified Information Systems Security Risk Manager (CISSRM)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
InfoSec governance and compliance	InfoSec program management	Mile2: Certified Information Systems Security Risk Manager (CISSRM) Training		x	x

Certification:

Certified Information Systems Security Manager (CISSM)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
InfoSec governance and compliance	InfoSec program management	Mile2: Certified Information Systems Security Manager (CISSM) Training		x	x

Go back to InfoSec and Privacy Certifications Page 1

Certification:
Certified Information Systems Security Officer (CISSO)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and vulnerability management	Forensics analysis	Mile2: Certified Information Systems Security Officer (CISSO) Training		x	x
InfoSec governance and compliance	InfoSec program management			x	x
InfoSec governance and compliance	InfoSec regulation			x	x
Threat and vulnerability management	Security incident and event management			x	x

Go back to InfoSec and Privacy Certifications Page 1

Certification:
Certified Information Systems Security Professional (CISSP) (Part 1)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Identity access management	Access management	TechTarget: Access control models, administration, IPS/IDS training video		x	x
		TechTarget: Access control security models training video		x	x
		Pearson: CISSP Video Course Domain 2 - Access Control, Downloadable Version		x	x
Physical and environmental security	Environmental security	Safari: CISSP Video Course Domain 4 – Physical Security		x	x
		Pearson: CISSP Video Course Domain 4 - Physical Security, Downloadable Version		x	x
	Physical access controls	Safari: CISSP Video Course Domain 4 – Physical Security		x	x
		Pearson: CISSP Video Course Domain 4 - Physical Security, Downloadable Version		x	x

Certification:
Certified Information Systems Security Professional (CISSP) (Part 2)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Identity access management	Identity management	TechTarget: Authentication technologies, federated identities training video		x	x
		Pearson: CISSP Video Course Domain 2 - Access Control, Downloadable Version		x	x
InfoSec governance and compliance	InfoSec program management	ISC2: CISSP Training		x	x
	InfoSec regulation	Pearson: CISSP Video Course Domain 6 - Law, Investigation and Ethics, Downloadable Version		x	x
Data security	Secure data transmission and storage	Pearson: CISSP Video Course Domain 7 - Telecommunications and Networking, Downloadable Version		x	x
	Cryptographic safeguards	InfoSec Institute: Cryptography Short Course (CISSP Domain #5)		x	x

Certification:
Certified IT Asset Disposition (CITAD)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Physical and environmental security	Equipment cleansing and disposal	IAITAM: Certified IT Asset Disposition (CITAD) course	x	x	x

Go back to InfoSec and Privacy Certifications Page 1

Certification:

Certified Network Defense Architect (CNDA)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Network and infrastructure security	Network defense analysis and control	EC Council: Certified Network Defense Architect (CNDA)Training		x	x
	Secure network engineering			x	x

Go back to InfoSec and Privacy Certifications Page 1

Certification:
Certified Network Forensics Examiner (CNFE)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and vulnerability management	Forensics analysis	Mile2: Certified Network Forensics Examiner (CNFE) Training			x

Go back to InfoSec and Privacy Certifications Page 1

Certification:
Certified Professional Ethical Hacker (CPEH)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and vulnerability management	Vulnerability management	Mile2: Certified Professional Ethical Hacker (CPEH) Training		x	x

Go back to InfoSec and Privacy Certifications Page 1

Certification:
Certified Penetration Testing Consultant (CPTC)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and vulnerability management	Vulnerability management	Mile2: Certified Penetration Testing Consultant (CPTC) Training			x

Go back to *InfoSec and Privacy Certifications Page 1*

Certification:
Certified Penetration Testing Engineer (CPTE)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and vulnerability management	Vulnerability management	Mile2: Certified Penetration Testing Engineer (CPTE) Training			x

Go back to InfoSec and Privacy Certifications Page 1

Certification:

Certified Risk and Compliance Management Professional (CRCMP)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Risk strategy and management	Risk acceptance	IARCP: Certified Risk and Compliance Management Professional (CRCMP) Training		x	x
	Risk assessment			x	x

Go back to InfoSec and Privacy Certifications Page 1

Certification:

Certified in Risk and Information Systems Control (CRISC)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
InfoSec governance and compliance	InfoSec program management	ISACA: Certified in Risk and Information Systems Control (CRISC) Training		x	x
Risk strategy and management	Risk acceptance			x	x
	Risk assessment			x	x
	Risk mitigation			x	x

Go back to InfoSec and Privacy Certifications Page 1

Certification:
Certified Computer Security Incident Handler (CSIH)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and vulnerability management	Security incident and event management	SEI Certification: Certified Computer Security Incident Handler (CSIH) Training		x	x

Go back to InfoSec and Privacy Certifications Page 1

Certification:
Certified Security Leadership Officer (CSLO)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
InfoSec governance and compliance	InfoSec program management	Mile2: Certified Security Leadership Officer (CSLO) Training			x

Go back to InfoSec and Privacy Certifications Page 1

Certification:
Certified Security Sentinel (CSS)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
InfoSec governance and compliance	InfoSec program management	Mile2: Certified Security Sentinel (CSS) Training	x	x	x
Threat and vulnerability management	Security incident and event management		x	x	x

Certification:

Certified Secure Software Lifecycle Professional (CSSLP)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
IS acquisition, development and maintenance	Secure software development	ISC2: Certified Secure Software Lifecycle Professional (CSSLP) Training	x	x	x

Certification:

Certified Vulnerability Assessor (CVA)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and vulnerability management	Vulnerability management	Mile2: Certified Vulnerability Assessor (CVA) Training	x	x	x

Certification:

EC-Council Certified Security Analyst (ECSA)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
InfoSec governance and compliance	InfoSec regulation	EC Council: Certified Security Analyst (ECSA)Training	x	x	x

Certification:
EC-Council Certified Security Specialist (ECSS)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
InfoSec governance and compliance	InfoSec program management	EC Council: Certified Security Specialist (ECSS) Training			x

Certification:
EC-Council Disaster Recovery Professional (EDRP)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Business continuity management and disaster recovery	Crisis management	EC Council: Disaster Recovery Professional (EDRP) Training		x	x
	Data backup and restoration			x	x

Certification:

EMC Information Storage Associate (EMCISA)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Business continuity management and disaster recovery	Data backup and restoration	EMC2: Information Storage and Management v2	x	x	x
Data security	Secure data transmission and storage	EMC2: Proven Professional Information Storage Associate v2		x	x

Go to InfoSec and Privacy Certifications Page 2

Certification:
EC-Council Network Security Administrator (ENSA)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Network and infrastructure security	Network defense analysis and control	EC Council: Network Security Administrator (ENSA) Training		x	x
	Secure network engineering			x	x
				x	x

Go to InfoSec and Privacy Certifications Page 2

Certification:

GIAC Auditing Wireless Networks (GAWN)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and vulnerability management	Vulnerability management	SANS - SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses		x	x

Certification:
GIAC Critical Controls Certification (GCCC)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
InfoSec governance and compliance	Policy communication, enforcement and exception management	SANS - SEC566: Implementing and Auditing the Critical Security Controls - In-Depth		x	x

Certification:
GIAC Certified Enterprise Defender (GCED)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and Vulnerability Management	Threat Identification and Categorization	SANS - SEC501: Advanced Security Essentials - Enterprise Defender		x	x
Network and Infrastructure Security	Network Defense Analysis and Control				

Certification:
GIAC Certified Forensic Analyst (GCFA)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and vulnerability management	Forensic analysis	SANS - FOR508: Advanced Computer Forensic Analysis and Incident Response			x
	Security incident and event management				x

Certification:

GIAC Certified Incident Handler (GCIH)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and vulnerability management	Security incident and event management	SANS - SEC504: Hacker Techniques, Exploits & Incident Handling		x	x

Certification:
GIAC Information Security Fundamentals (GISF)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
InfoSec governance and compliance	InfoSec program management	SANS - SEC301: Intro to Information Security	x	x	x

Go to InfoSec and Privacy Certifications Page 2

Certification:
GIAC Law of Data Security & Investigations (GLEG)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
InfoSec Governance and Compliance	InfoSec Regulation	SANS - LEG523: Law of Data Security and Investigations	x	x	x

Go to InfoSec and Privacy Certifications Page 2

Certification:
GIAC Network Forensic Analyst (GNFA)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and vulnerability management	Forensics analysis	SANS - FOR572: Advanced Network Forensics and Analysis			x

Certification:
GIAC Penetration Tester (GPEN)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and vulnerability management	Vulnerability management	SANS - SEC560: Network Penetration Testing and Ethical Hacking		x	x

Certification:
GIAC Certified Reverse Engineering Malware (GREM)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and vulnerability management	Forensics analysis	SANS - FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques		x	x

Certification:
GIAC Security Essentials (GSEC)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
InfoSec governance and compliance	InfoSec program management	SANS - SEC401: Security Essentials Bootcamp Style		x	x

Certification:
GIAC Security Leadership Certification (GSLC)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
InfoSec governance and compliance	InfoSec program management	SANS - MGT512: Security Leadership Essentials for Manager with Knowledge Compression			x

Certification:
GIAC Secure Software Programmer .NET (GSSP-.NET)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
IS acquisition, development and maintenance	Secure software development	SANS – DEV544: Secure Coding in .NET: Developing Defensible Applications		x	x

Certification:
GIAC Secure Software Programmer Java (GSSP-JAVA)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
IS acquisition, development and maintenance	Secure software development	SANS - DEV541: Secure Coding in Java/JEE: Developing Defensible Applications		x	x

Certification:

GIAC Certified Web Application Penetration Tester (GWAPT)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and vulnerability management	Vulnerability management	SANS - SEC542: Web App Penetration Testing and Ethical Hacking		x	x

Go to InfoSec and Privacy Certifications Page 2

Certification:
GIAC Certified Web Application Defender (GWEB)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
IS acquisition, development and maintenance	Secure software development	SANS - DEV522: Defending Web Applications Security Essentials	x	x	x

Certification:

Information Systems Security Architecture Professional (ISSAP)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
IS acquisition, development and maintenance	System development lifecycle	ISC2: Information Systems Security Architecture Professional Training	x	x	x

Certification:

Information Systems Security Engineering Professional (ISSEP)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
IS acquisition, development and maintenance	System development lifecycle	ISC2: Information Systems Security Engineering Professional Training	x	x	x

Certification:

Information Systems Security Management Professional (ISSMP)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
IS acquisition, development and maintenance	System development lifecycle	ISC2: Information Systems Security Management Professional Training		x	x

Certification:

Licensed Penetration Tester (LPT)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Threat and vulnerability management	Vulnerability management	EC Council: Licensed Penetration Tester (LPT) Training		x	x

Certification:
Network+

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Data security	Cryptographic safeguards	CompTIA: Network+ N10-006	x	x	x
Identity access management	Identity management		x	x	x
Network and infrastructure security	Network defense analysis and control		x	x	x
	Secure network engineering		x	x	x
Threat and vulnerability management	Security incident and event management		x	x	x
	Threat identification and categorization		x	x	x
	Vulnerability management		x	x	x

Certification:
Security+ (Part 1)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Identity access management	Access management		x	x	x
Data security	Cryptographic safeguards		x	x	x
	Data management		x	x	x
Identity access management	Identity management		x	x	x
InfoSec governance and compliance	InfoSec program management	CompTIA: Security+ SY0-401	x	x	x
Network and infrastructure security	Network defense analysis and control		x	x	x
Risk strategy and management	Risk assessment		x	x	x
Data security	Secure data transmission and storage		x	x	x

Certification:
Security+ (Part 2)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
Network and infrastructure security	Secure data transmission and storage	CompTIA: Security+ SY0-401	x	X	x
Threat and vulnerability management	Secure network engineering		x	x	x
IS acquisition, development and maintenance	System development lifecycle		x	x	x
Threat and vulnerability management	Threat identification and categorization		x	x	x
	Vulnerability management		x	x	x

Certification:
Systems Security Certified Practitioner (SSCP)

Domain	Competency	Course	Proficiency Level		
			Level 1	Level 2	Level 3
InfoSec governance and compliance	InfoSec program management	ISC2: System Security Certified Practitioner (SSCP) Training		x	x

Go to InfoSec and Privacy Certifications Page 2

Appendix

Course Description
ATD: Designing Learning Certificate

- Course that provides all of the tools necessary to develop powerful, bottom-line focused training. It provides best practices for conducting a needs assessment, job/task analysis, and course design and development

- Please visit the following website for additional information:

  http://www.ATD.org/Education/Programs/Designing-Learning-Certificate

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
ATD: Advanced E-Learning Instructional Design Certificate

- Course that provides expert techniques vital to design effective e-learning that achieves lasting performance change. The course provides general development guidelines and time requirements for designing a successful e-learning event

- Please visit the following website for additional information:

  http://www.ATD.org/Education/Programs/Advanced-E-Learning-Instructional-Design-Certificate

* ASTD has been renamed as ATD

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
ATD: Essentials of Coaching Government Employees on the Job

- Course that demonstrates how the regular use of a coaching model and supporting language techniques can be lead to measurable development on the job. Throughout the program, participants practice the tools using real government examples and situations, and they leave the program with a coaching approach to foster learning on the job

- Please visit the following website for additional information:

    http://www.ATD.org/Education/Programs/Coaching-Government-Employees-on-the-Job

* ASTD has been renamed as ATD

Go back to *InfoSec and Privacy Training by Competency*

Go back to *InfoSec and Privacy Training by Certification*

Go back to *InfoSec and Privacy Training by Position Description*

Course Description
ATD: Evaluating Learning Impact Certificate

- Course that helps participants to determine the impact of learning programs and develop and implement an evaluation strategy for the organization. Participants will receive a solid foundation in all aspects of the measurement and evaluation of learning and performance solutions

- Please visit the following website for additional information:

  http://www.ATD.org/Education/Programs/Evaluating-Learning-Impact-Certificate

* ASTD has been renamed as ATD

Go back to _InfoSec and Privacy Training by Competency_

Go back to _InfoSec and Privacy Training by Certification_

Go back to _InfoSec and Privacy Training by Position Description_

Course Description
ATD: Facilitating Synchronous Learning Certificate

- This online course provides ten hours of live, online instruction where participants will learn to maximize the engagement of remote participants and manage the logistics of facilitating synchronous learning

- Please visit the following website for additional information:

  https://www.td.org/Education/Programs/Facilitating-Synchronous-Learning-Certificate

* ASTD has been renamed as ATD

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
ATD: Introduction to Training Certificate

- High-level introductory course to gain a foundation in delivering training events. The courses provides proven techniques for facilitating engaging and result-oriented training sessions

- Please visit the following website for additional information:

    http://www.ATD.org/Education/Programs/Introduction-to-Training-Certificate

* ASTD has been renamed as ATD

Go back to *InfoSec and Privacy Training by Competency*

Go back to *InfoSec and Privacy Training by Certification*

Go back to *InfoSec and Privacy Training by Position Description*

Course Description
ATD: Master Instructional Designer Program

- This course covers the entire process of analysis, design, development, implementation, and evaluation of learning programs. In addition, this program explores new design models and techniques that align with emerging needs

- Please visit the following website for additional information:

    http://www.ATD.org/Education/Programs/ATD-Master-Instructional-Designer

* ASTD has been renamed as ATD

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
ATD: Master Trainer Program

- Assessment-based certificate program that provides the opportunity to evaluate real-world projects, and master the skills required to create formal and informal learning

- Please visit the following website for additional information:

  http://www.ATD.org/Education/Programs/ATD-Master-Trainer

* ASTD has been renamed as ATD

Course Description
ATD: Presentation Skills Certificate

- During this program you will learn proven tips and examples that will guide you through the presentation process no matter how large the audience

- Please visit the following website for additional information:

  https://www.td.org/Education/Programs/Presentation-Skills-Certificate

* ASTD has been renamed as ATD

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
ATD: Training Certificate

- Premier train-the-trainer program that provides a practical, how-to overview of the entire training function. New trainers will gain a strong foundation in critical training skills and seasoned trainers will be introduced to new approaches for delivering powerful training

- Please visit the following website for additional information:

    http://www.ATD.org/Education/Programs/Training-Certificate

* ASTD has been renamed as ATD

Course Description
ATD: Managing Learning Programs Certificate

- This three-day program provides the critical leadership necessary to develop the learning function (its people and programs) and have a meaningful impact on the overall strategy in your organization. This interactive program includes self-assessments, small group case study discussion, best-practice review, and feedback on specific challenges participants face

- Please visit the following website for additional information:

  https://www.td.org/Education/Programs/Managing-Learning-Programs-Certificate

* ASTD has been renamed as ATD

Go back to *InfoSec and Privacy Training by Competency*

Go back to *InfoSec and Privacy Training by Certification*

Go back to *InfoSec and Privacy Training by Position Description*

Course Description
CEC-Security LLC: Introduction to Cryptography

- This is a 32 hour course that gives the student a thorough overview of cryptography. It includes classic cryptography, major symmetric algorithms, asymmetric algorithms, hashing algorithms, steganography, and applications of cryptography

- Please visit the following website for additional information:

  http://www.cec-security.com/courses.htm

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
CompTIA: CompTIA Advanced Security Practitioner (CASP) Training

- CompTIA offers multiple training options available to prepare participants to obtain the CompTIA Advanced Security Practitioner (CASP) certification. The CASP exam covers the technical knowledge and skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments

- Please visit the following website for additional information:

  http://certification.comptia.org/getCertied/certifications/comptia-advanced-security-practitioner-(casp)

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
CompTIA: Network+ N10-006

- Multiple training options available to prepare participants to obtain the CompTIA Network+ certification. The exam Network+ N10-006 covers network technologies, installation and configuration, media and topologies, management, and security

- Please visit the following website for additional information:

    http://certification.comptia.org/getCertified/certifications/network.aspx

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
CompTIA: Security+ SY0-401

- Multiple training options available to prepare participants to obtain the CompTIA Security+ certification. The Security+ SY0-401 exam covers the most important foundational principles for securing a network and managing risk

- Please visit the following website for additional information:

    http://certification.comptia.org/getCertified/certifications/security.aspx

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description

Defense Cyber Investigation Training Academy: Cyber Insider Threats Analysis Training

- Course that defines insider threat, examines relevant laws and regulations, and explores motivations and indicators of insider threat agents

- Please visit the following website for additional information:

    https://www.dcita.edu/courses.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
Defense Cyber Investigation Training Academy: Introduction to Cyber Insider Threat Course

- Scenario-based online course that introduces the insider threat and presents methods for investigation and analysis

- Please visit the following website for additional information:

  https://www.dcita.edu/courses.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Course Description

Defense Cyber Investigation Training Academy: Introduction to Networks and Computer Hardware

- Course that teaches basic computer and network component identification and function, along with the foundational theory cyber investigators must understand

- Please visit the following website for additional information:

  https://www.dcita.edu/courses.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description

Defense Cyber Investigation Training Academy: Introduction to Log Analysis

- The course objective is to provide students with a comprehensive understanding of log analysis techniques. Students learn how to process logs from Windows and Linux operating systems, firewalls, intrusion detection systems, and Web and e-mail servers. Students also learn how to assemble evidence found in logs to assist in tasks ranging from building a case to recognizing an intrusion

- Please visit the following website for additional information:

    https://www.dcita.edu/courses.html

Course Description
DRII: BCOE 300 Introduction to Business Impact Analysis

- Learn the purpose, objectives and value of conducting a business impact analysis. The student will understand methodologies, terms, and definitions, such as mission-critical business processes, recovery time objectives (RTO), and acceptable exposure to loss

- Please visit the following website for additional information:

  https://www.drii.org/education/trainings.php

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
DRII: BCOE 500 Emergency Preparedness and Response

- Learn and understand the emergency management structure and the planning necessary to manage a crisis for your organization. This will include identification, escalation, and notification procedures. This course covers the challenges of reviewing and coordinating emergency evacuation programs in place in organizations, or working with the responsible areas to develop or enhance existing programs

- Please visit the following website for additional information:

    https://www.drii.org/education/trainings.php

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Course Description
DRII: BCOE 900 Crisis Communication and Coordinating with External Agencies

- All plans must include communication elements, and this course is designed to assist the student in making All the necessary preparations for managing an emergency. Learn how to develop procedures that will allow you to effectively communicate with All audiences, to identify and train spokespersons, to develop key messages, and to work effectively with the media

- Please visit the following website for additional information:

    https://www.drii.org/education/trainings.php

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
DRII: BCOE 600 Business Continuity Plan Implementation

- Learn the application of skills and information gathered in putting the BCM program into action by identifying the components of the planning process including plan methodology, implementation, organization, and documentation

- Please visit the following website for additional information:

  https://www.drii.org/education/trainings.php

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
DRII: BCOE 400 Developing Business Continuity Strategies

- Learn the challenges of selecting the appropriate strategies for recovery of business processes, critical functions, operations and the supporting information technologies within the specified recovery time objective. It defines alternative strategies, assesses the strengths and weaknesses of strategies and methodologies for presentation to management. We will identify the process steps involved in the analysis and strategy determination. This will be linked directly and supported by the data gathering activities accomplished during the risk assessment and BIA

- Please visit the following website for additional information:

    https://www.drii.org/education/trainings.php

Course Description
DRII: BCOE 800 Exercising and Maintaining Plans

- Identify the components needed to establish an exercise, testing, maintenance and audit program. To continue to be effective, a business continuity management (BCM) program must implement a regular exercise schedule to establish confidence in a predictable and repeatable performance of recovery activities throughout the organization

- Please visit the following website for additional information:

  https://www.drii.org/education/trainings.php

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
DRII: BCOE 100 Program Management Principles in Business Continuity Planning

- Learn how to establish the need for a business continuity program in your organization and how to obtain management support. You will also learn how to organize and manage the process of developing a business continuity program. This course identifies the requirements and imperatives of project management methodologies required to develop an enterprise-wide business continuity program

- Please visit the following website for additional information:

    https://www.drii.org/education/trainings.php

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
EC Council: Certified Chief Information Security Officer (CCISO) Training

- In-person and online training options that provides all fundamental knowledge to obtain Chief Information Security Officer (CCISO) certification. This certification will provide your employers with the assurance that you possess the proven knowledge and experience to plan and oversee Information Security for the entire corporation

- Please visit the following website for additional information:

  https://cert.eccouncil.org/certified-chief-information-security-officer.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
EC Council: Certified Ethical Hacker (CEH) Training

- Ethical hacking course with 19 of the most current security domains any ethical hacker will ever want to know when they are planning to beef up the information security posture of their organization. This course prepares participants for EC-Council Certified Ethical Hacker (CEH) exam 312-50

- Please visit the following website for additional information:

  http://www.eccouncil.org/Certification/certified-ethical-hacker

Course Description

EC Council: Computer Hacking Forensic Investigator (CHFI) Training

- This course presents a detailed methodological approach to computer forensics and evidence analysis. It is a comprehensive course covering major forensic investigation scenarios that enable students to acquire hands-on experience on various forensic investigation techniques and standard tools necessary to successfully carry-out a computer forensic investigation

- Please visit the following website for additional information:

  http://www.eccouncil.org/Certification/professional-series/chfi-course-outline

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Course Description
EC Council: Certified Network Defense Architect (CNDA) Training

- This course has been specially designed for Government Agencies around the world. This course prepares participants to become Certified Network Defense Architect (CNDA). Other than the name the content is exactly the same as the Certified Ethical Hacker (CEH)

- Please visit the following website for additional information:

  http://www.eccouncil.org/Certification/certified-network-defense-architect

Course Description
EC Council: Certified Security Analyst (ECSA) Training

- Training program which teaches information security professionals to conduct real life penetration tests using real time scenarios. It prepares participants to achieve EC-Council Security Analyst (ECSA) certification

- Please visit the following website for additional information:

    https://www.eccouncil.org/about-ec-council-certified-security-analyst

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
EC Council: Certified Security Specialist (ECSS) Training

- This course will benefit the students who are interested in learning fundamentals of information security, network security, and computer forensics. It will prepare students to obtain EC-Council Certified Security Specialist (ECSS) certification

- Please visit the following website for additional information:

    http://www.eccouncil.org/Certification/ec-council-certified-security-specialist

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
EC Council: Disaster Recovery Professional (EDRP) Training

- This course teaches participants the methods in identifying vulnerabilities and taking appropriate countermeasures to prevent and mitigate failure risks for an organization. It prepares students to prepare for the EC-Council Disaster Recovery Professional Training (EDRP) certification

- Please visit the following website for additional information:

   http://www.eccouncil.org/Certification/ec-council-disaster-recovery-professional

Course Description
EC Council: Network Security Administrator (ENSA) Training

- Training program that provides fundamental skills needed to analyze the internal and external security threats against a network, and to develop security policies that will protect an organization's information. It prepares participants to achieve EC-Council Network Security Administrator (ENSA) certification

- Please visit the following website for additional information:

  http://www.eccouncil.org/Certification/ec-council-network-security-administrator

Course Description
EC Council: Licensed Penetration Tester (LPT) Training

- Licensed Penetration Tester (LPT) program teaches the report writing skills of the professional pen tester. The LPT program was also designed to evaluate the student's capabilities of performing penetration tests in real-time scenarios on an active cyber range

- Please visit the following website for additional information:

    http://www.eccouncil.org/about-licensed-penetration-tester

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
EHRs and HIPAA: Steps for Maintaining the Privacy and Security of Patient Information

- The goal of this activity is to summarize steps for incorporating security standards of the Health Insurance Portability and Accountability Act (HIPAA) into an electronic health record

- Please visit the following website for additional information:

  http://www.medscape.org/viewarticle/821650

* User will need to create a free Medscape account to view content

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
EMC2: Backup Recovery Systems and Architecture

- This course provides participants with a solid foundation in Backup and Recovery infrastructure. It teaches participants about backup and recovery theory, including backup methods, planning, and key terminology

- Please visit the following website for additional information:

   https://education.emc.com/academicalliance/documents/EAA_backup_recovery_one-pager.pdf

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
EMC2: Information Storage and Management v2

- This course builds a strong understanding of underlying storage technologies and prepares students to learn advanced concepts, technologies and products. It provides a comprehensive learning on storage technology, which will enable students to make more informed decisions in an increasingly complex IT environment

- Please visit the following website for additional information:

    https://education.emc.com/guest/campaign/InformationStorageandManagement.aspx

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
EMC2: Proven Professional Information Storage Associate v2

- This course covers storage architectures and key data center elements, physical and logical components of a storage infrastructure, storage networking technologies . This course prepares participants to obtain Proven Professional Information Storage Associate v2 certification (EMCISA)

- Please visit the following website for additional information:

  https://education.emc.com/guest/campaign/InformationStorageandManagement.aspx?WT.mc_id=web_emccom_ISMV2_4114

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
Expanding Security: Data Administration 101

- This course is designed to build the functional development of data administration personnel

- Please visit the following website for additional information:

  http://www.expandingsecurity.com/product/niccs-course-data-administration/

Course Description
Expanding Security: Risk Management 101

- This course is designed to build the management development of risk management personnel. It provides the fundamental knowledge to ensure appropriate treatment of risk, compliance, and monitoring assurance from internal perspective

- Please visit the following website for additional information:

  http://www.expandingsecurity.com/product/niccs-risk-management/

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
Expanding Security: Secure Software Management 101

- This course is designed to build functional development of security software engineering personnel

- Please visit the following website for additional information:

  http://www.expandingsecurity.com/product/niccs-course-secure-software-engineering/

Course Description
Expanding Security: Security Program Management 101

- This course teaches individuals the skills to oversee and manage information security program implementation within the organization or other area of responsibility

- Please visit the following website for additional information:

  http://www.expandingsecurity.com/product/niccs-course-security-program-management/

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
Global Knowledge: CBAP Prep Boot Camp

- This boot camp prepares participants for the Certification of Competency in Business Analysis (CBAP) and Certified Business Analysis Professional (CCBA) exams. The CCBA and CBAP designations recognize that practitioners have the knowledge and skills necessary for effectiveness and a professional level of competence in business analysis principles and practices

- Please visit the following website for additional information:

  http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=17609&catid=436&country=United+States

Go back to *InfoSec and Privacy Training by Competency*

Go back to *InfoSec and Privacy Training by Certification*

Go back to *InfoSec and Privacy Training by Position Description*

Course Description

Global Knowledge: Cybersecurity Investigations and Network Forensics Analysis: Practical Techniques for Analyzing Suspicious Network Traffic

- In this course, participants will develop the skills not only to capture suspicious data, but also to discern unusual patterns hidden within seemingly normal network traffic

- Please visit the following website for additional information:

  http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=16842&catid=191&country=United+States

Course Description

Global Knowledge: Cybersecurity Investigations and Network Forensics Analysis: Practical Techniques for Analyzing VoIP Traffic

- VoIP network analysis is a specialized subset of traditional network analysis and encompasses not only the skill of capturing data, but also the ability to discern unusual patterns hidden within seemingly normal network traffic. Through real-world examples and hands-on exercises, participants will gain a set of analysis techniques focusing on the use of vendor-neutral, open source tools

- Please visit the following website for additional information:

    http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=16844&country=United+States

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description

Global Knowledge: Cybersecurity Investigations and Network Forensics Analysis: Practical Techniques for Analyzing WiFi Traffic

- Wi-Fi / WLAN network analysis is a specialized subset of traditional network analysis and encompasses not only the skill of capturing data, but also the ability to discern unusual patterns hidden within seemingly normal network traffic. Through real-world examples and hands-on exercises, participants will gain a set of analysis techniques focused on using vendor-neutral, open source tools

- Please visit the following website for additional information:

    http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=16846&catid=187&country=United+States

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
Global Knowledge: Enterprise WiFi Fundamentals

- The course provides the basic 802.11 wireless networking terminology and functionality. In this Wi-Fi fundamentals course, participants will gain the knowledge needed to enter into or advance within the wireless networking industry

- Please visit the following website for additional information:

  http://www.globalknowledge.co.uk/courses/global_knowledge/wireless/gk3602.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description

Global Knowledge: Dell SonicWALL Network Security Basic Administration (NS-102)

- This course provides students with the background, knowledge, and hands-on experience to begin designing, implementing, and troubleshooting SonicWALL security appliances running SonicOS firmware

- Please visit the following website for additional information:

  http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=11193&catid=191&country=United+States

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description

HHS: Examining Compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule

- Educational program for health care providers on compliance with various aspects of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules

- Please visit the following website for additional information:

    http://www.medscape.org/viewarticle/763251?src=ocr

* User will need to create a free Medscape account to view content

Course Description

HHS: Health Insurance Portability and Accountability Act (HIPAA) and You: Building a Culture of Compliance

- The goals of this program are to outline the responsibilities of covered entities and their business associates under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and provide strategies to build and maintain a culture of compliance with HIPAA

- Please visit the following website for additional information:

  http://www.medscape.org/viewarticle/762170?src=ocr

* User will need to create a free Medscape account to view content

Go back to *InfoSec and Privacy Training by Competency*

Go back to *InfoSec and Privacy Training by Certification*

Go back to *InfoSec and Privacy Training by Position Description*

Course Description
HHS: Privacy Awareness Training

- Training course that teaches students who to define privacy and explain its importance; identify privacy laws, policies, guidance, and principles; define personally identifiable information (PII) and list examples; recognize potential threats to privacy, etc.

- Please visit the following website for additional information:

    http://www.hhs.gov/ocio/securityprivacy/awarenesstraining/privacyawarenesstraining.pdf

Go back to *InfoSec and Privacy Training by Competency*

Go back to *InfoSec and Privacy Training by Certification*

Go back to *InfoSec and Privacy Training by Position Description*

Course Description
IAITAM: Disposal Management Advanced Study Course

- The Disposal Management Advanced Course of Study is based on the information and practices contained in the IAITAM Best Practice Library (IBPL) Disposal Management volume 12 which pertains to the activities and procedures for properly removing assets from an environment

- Please visit the following website for additional information:

  https://www.iaitam.org/eweb/shopping/shopping.aspx?site=iaitam&shopsearch=cas&prd_key=bda31950-6b49-46f9-af05-78ed642007ff

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
IAITAM: Certified IT Asset Disposition (CITAD) Course

- The IAITAM Certification in IT Asset Disposition (CITAD) course prepares individuals to manage the IT asset disposal process within an organization

- Please visit the following website for additional information:

    https://www.iaitam.org/eweb/DynamicPage.aspx?Site=iaitam&WebCode=CITAD

Course Description
IAITAM: Policy Management Advanced Study Course

- The Policy Management Advanced Course of Study is based on the information and practices contained in the IAITAM Best Practice Library (IBPL) Policy Management volume 3, which clearly cites the criticality of this Key Process Area to any IT Asset Management program. Policies need to be clearly defined, understandable and enforced

- Please visit the following website for additional information:

  https://www.iaitam.org/eweb/shopping/shopping.aspx?site=iaitam&shopsearch=cas&prd_key=743cdc8b-fefd-41f1-bc98-69bfa7909d21

Course Description
IAPP: Certified Information Privacy Manager (CIPM) Training

- This program is broken into two segments, the first describing important practices in managing privacy. The second segment is an interactive format in which participants apply these practices to a real-world scenario

- Please visit the following website for additional information:

    https://privacyassociation.org/certify/training/

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
IAPP: Certified Information Privacy Professional / U.S. Private-Sector (CIPP/US) Training

- Training that introduces to the U.S. privacy environment, examines limits on private-sector collection and use of date, includes an introduction to workplace privacy, and introduces privacy law and practice in law enforcement, national security and civil litigation

- Please visit the following website for additional information:

  https://www.privacyassociation.org/media/pdf/certification/course-outlines/USPrivateSectorPrivacyCourseOutline.pdf

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
IAPP: Certified Information Privacy Professional / U.S. Government (CIPP/G) Training

- This training reviews U.S. government privacy definitions and principles and proceeds to review two key laws for federal practice: the Privacy Act and E-Government Act. It also applies information about the laws to privacy program management and organization, records management, and auditing and compliance monitoring

- Please visit the following website for additional information:

  https://www.privacyassociation.org/media/pdf/certification/course-outlines/USGovernmentPrivacyCourseOutline.pdf

Go back to *InfoSec and Privacy Training by Competency*

Go back to *InfoSec and Privacy Training by Certification*

Go back to *InfoSec and Privacy Training by Position Description*

Course Description
IAPP: Certified Information Privacy Technologist (CIPT) Training

- This program is designed to provide students with critical privacy concepts and practices that impact IT, consumer privacy expectations and responsibility, etc.

- Please visit the following website for additional information:

  https://www.privacyassociation.org/media/pdf/certification/course-outlines/CIPTCourseOutline.pdf

Course Description
IARCP: Certified Information Systems Risk and Compliance Professional (CISRCP) Training

- This course has been designed to provide IT and Information Security managers with the knowledge and skills needed to understand and support regulatory compliance and enterprise wide risk management. The course provides with the skills needed to pass the Certified Information Systems Risk and Compliance Professional (CISRCP) exam

- Please visit the following website for additional information:

  http://www.risk-compliance-association.com/CISRCP_Distance_Learning_and_Certification.htm

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
IARCP: Certified Risk and Compliance Management Professional (CRCMP) Training

- This course is intended for professionals that want to understand risk and compliance management and to work as risk and compliance officers. They will prove that they are qualified, when they pass the Certified Risk and Compliance Management Professional (CRCMP) exam

- Please visit the following website for additional information:

  http://www.risk-compliance-association.com/Distance_Learning_and_Certification.htm

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
IBCT: Effective Business Continuity Management Systems (ECP-601)

- This course provides an intensive, hands-on workshop covering all major aspects of effective Business Continuity Management for private sector, public sector, and not-for-profit organization. Completion of this course qualifies participants to sit the certification exam to become a Certified Continuity Manager (CCM). In addition, participants leave this course with our Diploma in Business Continuity Management

- Please visit the following website for additional information:

    http://www.ibct.com/index.php/our-courses/ecp-601

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
Identity Management Institute: Certified Identity Risk Manager (CIRM) Training

- The Certified Identity Risk Manager (CIRM) credential is the only vendor-neutral certification for professionals who manage various identity risks within business operations and information systems. The international CIRM designation is an all encompassing identity management certification which demonstrates an individual's professional capabilities as well as commitment and adherence to identity risk management standards

- Please visit the following website for additional information:

    http://www.identitymanagementinstitute.org/cirm/

Go back to *InfoSec and Privacy Training by Competency*

Go back to *InfoSec and Privacy Training by Certification*

Go back to *InfoSec and Privacy Training by Position Description*

Course Description
InfoSec Institute: Advanced Ethical Hacking & Advanced Persistent Threat (SEC-300)

- This course will teach participants how to successfully attack fully patched and hardened systems, how to circumvent common security controls, and how to get to confidential data. This course prepares participants to become Certified Expert Penetration Tester (CEPT)

- Please visit the following website for additional information:

  http://www.infosecinstitute.com/courses/advanced_ethical_hacking_training.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
InfoSec Institute: Advanced Hacking Online (SEC-300)

- This online course provides participants the skills necessary to identify and prevent the latest complex and complicated attacks. This course consists of 20+ hours of hands-on lab exercises.

- Please visit the following website for additional information:

  http://www.infosecinstitute.com/courses/advanced_hacking_online.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description

InfoSec Institute: Certified in the Governance of Enterprise IT (CGEIT) Training (IA-212)

- This four day seminar will explain the Certified in the Governance of Enterprise IT (CGEIT) examination process. It will help participants prepare for the next CGEIT exam and provide guidance and test participants' readiness through sample questions

- Please visit the following website for additional information:

  http://www.infosecinstitute.com/courses/cgeit-training.html

Course Description
InfoSec Institute: Computer Forensics Training (SEC-203)

- During InfoSec Institute's Computer Forensics Training course participants will see the dark side of how computer crimes are committed, learn how to find traces of illegal or illicit activities left on disk with computer forensics tools and manual techniques, and earn how to recover data intentionally hidden or encrypted by perpetrators

- Please visit the following website for additional information:

  http://www.infosecinstitute.com/courses/computer_forensics_training.html

Course Description
InfoSec Institute: Cryptography Short Course (CISSP Domain #5)

- The cryptography section on the Certified Information Systems Security Professional (CISSP) exam has proven to be one of the most difficult domains for many of our students. This short course takes you through the domain as it relates to the CISSP exam

- Please visit the following website for additional information:

  http://resources.infosecinstitute.com/mini-course/cryptography-cissp-training/

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
InfoSec Institute: Data Recovery Training (SEC-205)

- The InfoSec Institute Data Recovery course provides an in-depth and hands-on exposure to the most hands on and highly technical logical and physical data recovery course available anywhere

- Please visit the following website for additional information:

  http://www.infosecinstitute.com/courses/data_recovery_training.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
InfoSec Institute: Enterprise Security Architecture and Design Online (ONL-212)

- During this course, participants will learn the essentials of Enterprise Security Design for security engineering. This course will bring participants up to speed on the latest security-specific architecture. It will show participants how to implement the myriad of security technologies available on the market today in an effective and cost efficient manner

- Please visit the following website for additional information:

  http://www.infosecinstitute.com/courses/security_architecture_design_online.html

Course Description
InfoSec Institute: Expert Penetration Testing (SEC-209)

- The InfoSec Institute Expert Hacking course provides an in-depth and hands-on review of the most current exploit development strategies and techniques for the Microsoft Windows platform

- Please visit the following website for additional information:

  http://www.infosecinstitute.com/courses/expert_penetration_testing_training.html

Go back to *InfoSec and Privacy Training by Competency*

Go back to *InfoSec and Privacy Training by Certification*

Go back to *InfoSec and Privacy Training by Position Description*

Course Description

InfoSec Institute: Information Security Policy Essentials (SEC-211)

- This two day course provides guidance on critical information security policy elements, communicating the policy organization-wide and executive reporting. This course explores the process of creating security policies, reviews standards and methodologies, and evaluates example policies

- Please visit the following website for additional information:

  http://www.infosecinstitute.com/courses/security-policy-essentials-training.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
InfoSec Institute: Intrusion Prevention Online (SEC-204)

- The Intrusion Prevention training offered by InfoSec Institute covers all areas of intrusion prevention. During this course, participants will learn the technical details that make Intrusion Prevention Systems so effective

- Please visit the following website for additional information:

  http://www.infosecinstitute.com/courses/intrusion_prevention_online.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
InfoSec Institute: Mobile Device Penetration Testing (SEC-556)

- This course covers security risks and controls on both the mobile platform as well as the presentation layer. During this course, participants will get hands-on experience with the top threats that organizations are facing when targeting mobile and BYOD devices

- Please visit the following website for additional information:

  http://www.infosecinstitute.com/courses/mobile-pen-testing-training.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
InfoSec Institute: Penetration Testing Online (ONL-206)

- During this course, participants will learn everything there is to know about penetration testing, from the use of network reconnaissance tools, to the writing of custom zero-day buffer overflow exploits

- Please visit the following website for additional information:

  http://www.infosecinstitute.com/courses/penetration_testing_online.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
InfoSec Institute: SCADA Security (SEC-325)

- This course will provide participants the skills required to direct and manage the appropriate cyber security protection for your SCADA system

- Please visit the following website for additional information:

  http://www.infosecinstitute.com/courses/scada_security_training.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
InfoSec Institute: Web Application Penetration Testing (SEC-402)

- The Web Application Penetration Testing course from InfoSec Institute is a totally hands-on learning experience. From the first day to the last day, participants will learn the ins and outs of Web App Pen Testing by attending thought provoking lectures led by an expert instructor

- Please visit the following website for additional information:

  http://www.infosecinstitute.com/courses/web_application_hacking_training.html

Course Description
ISACA: An Introduction to Privacy and Data Protection

- This course analyzes the risk and value of personal information from different perspectives and outlines the consequences of privacy failures. It explores how organizations can govern, manage, and protect regulated and high value data to manage the risk of non-compliance, information misuse, unauthorized access, and loss

- Please visit the following website for additional information:

  http://www.isaca.org/Education/Training/Pages/An-Introduction-to-Privacy-and-Data-Protection-Miami.aspx

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
ISACA: Certified Information Systems Auditor (CISA) Training

- This course provides an excellent tool for Certified Information Systems Auditor (CISA) certification exam review and continuing professional education. The course features descriptions of the tasks performed by IS auditors and the knowledge required to plan, manage and perform information security audits

- Please visit the following website for additional information:

    http://www.isaca.org/Education/Training/exam-review-courses/Pages/CISA-Online-Review-Course.aspx

Course Description
ISACA: Certified Information Security Manager (CISM) Training

- This training has been developed to assist those who plan to sit for the Certified Information Security Manager (CISM) exam. The 4-day review course focuses on the key points covered in the exam then followed by class practice questions and discussions

- Please visit the following website for additional information:

  http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Prepare-for-the-Exam/Review-Courses/Pages/default.aspx#northamerica

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
ISACA: Certified in Risk and Information Systems Control (CRISC) Training

- The review program has been developed to assist those who plan to sit for the Certified in Risk and Information Systems Control (CRISC) exam. The 4-day review course focuses on the key points covered in the exam then followed by class practice questions and discussions

- Please visit the following website for additional information:

  http://www.isaca.org/Certification/CRISC-Certified-in-Risk-and-Information-Systems-Control/Prepare-for-the-Exam-OLD/Pages/Review-Courses.aspx

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
ISC2: Certified Authorization Professional (CAP) Training

- The Certified Authorization Professional (CAP) course is designed for information security practitioner who champions system security commensurate with an organization's mission and risk tolerance, while meeting legal and regulatory requirements

- Please visit the following website for additional information:

  https://www.isc2.org/cap-training.aspx

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
ISC2: Certified Cyber Forensics Professional (CCFP) Training

- The Certified Cyber Forensics Professional (CCFP) course is designed for intermediate to advanced professionals who possesses at least 3 years of experience in the areas of: forensic techniques and procedures, standards of practice, and legal and ethical principles that assure the accuracy, completeness, and reliability of digital evidence

- Please visit the following website for additional information:

    https://www.isc2.org/CCFP-training/default.aspx

Course Description
ISC2: Certified Information Systems Security Professional (CISSP) Training

- This training course will help candidates review and refresh their information security knowledge and help identify areas they need to study for the CISSP exam. The CISSP exam covers critical topics in security today, including risk management, cloud computing, mobile security, application development security and more

- Please visit the following website for additional information:

    https://www.isc2.org/cissp-training.aspx

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
ISC2: Certified Secure Software Lifecycle Professional (CSSLP) Training

- The Certified Secure Software Lifecycle Professional (CSSLP) course is the largest, most comprehensive, collection of best practices, policies, and procedures, to ensure a security initiative across all phases of application development

- Please visit the following website for additional information:

  https://www.isc2.org/csslpedu/default.aspx

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description

ISC2: HealthCare Information Security and Privacy Practitioner (HCISPP) Training

- The HealthCare Information Security and Privacy Practitioner (HCISPP) training is the most comprehensive review of healthcare security and privacy concepts and industry best practices.

- Please visit the following website for additional information:

    https://www.isc2.org/HCISPP-training/default.aspx

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
ISC2: Information Systems Security Architecture Professional (ISSAP) Training

- This training is the perfect way to assure competence of the six major domains of the Information Systems Security Architecture Professional (ISSAP) Concentration. This course is designed for CISSPs who specialize in designing security solutions and providing management with risk-based guidance to meet organizational needs

- Please visit the following website for additional information:

  https://www.isc2.org/issaprevsem/default.aspx

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
ISC2: Information Systems Security Engineering Professional (ISSEP) Training

- This training is the perfect way to assure competence of the four major domains of the Information Systems Security Engineering Professional (ISSEP) Concentration

- Please visit the following website for additional information:

    https://www.isc2.org/isseprevsem/default.aspx

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
ISC2: Information Systems Security Management Professional (ISSMP) Training

- This training course will help candidates review and refresh their information security knowledge and help identify areas they need to study for the CISSP-ISSMP exam

- Please visit the following website for additional information:

  https://www.isc2.org/issmprevsem/default.aspx

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
ISC2: System Security Certified Practitioner (SSCP) Training

- This training is the key to success in pursuing the System Security Certified Practitioner (SSCP) certification. It is the most comprehensive, complete review of the information systems security concepts and industry best practices covered by the SSCP domains

- Please visit the following website for additional information:

  https://www.isc2.org/sscp-training.aspx

Course Description
Langevin: Training Needs Analysis

- This e-learning module gives you a faster needs analysis approach that is realistic in today's climate. It shows you how to apply a highly effective procedure for determining whether or not training is the solution to a job performance problem. It will help you develop the key skills and confidence to gain acceptance and recognition for your recommendations to management

- Please visit the following website for additional information:

  http://www.langevin.com/workshops/view/training-needs-analysis

Go back to *InfoSec and Privacy Training by Competency*

Go back to *InfoSec and Privacy Training by Certification*

Go back to *InfoSec and Privacy Training by Position Description*

Course Description
Mile2: Certified Digital Forensics Examiner (CDFE) Training

- The Certified Digital Forensics Examiner (CDFE) course will benefit organizations, individuals, government offices, and law enforcement agencies in performing digital forensics and reporting findings

- Please visit the following website for additional information:

  http://mile2.com/digital-forensics-courses/certified-digital-forensics-examiner.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
Mile2: Certified Disaster Recovery Engineer (CDRE) Training

- The Certified Disaster Recovery Engineer (CDRE) course covers disaster recovery and business continuity planning. It is comprised of 11 modules. During the course students will perform different DR/BC exercises including spending all of the fourth day writing their own disaster recovery/business continuity plan

- Please visit the following website for additional information:

    https://www.mile2.com/disaster-recovery-business-continuity-planning.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
Mile2: Certified Incident Handling Engineer (CIHE) Training

- The Certified Incident Handling Engineer (CIHE) 4 day course is designed to help Incident Handlers, System Administrators, and Cyber Security Engineers understand how to plan, create and utilize their systems in order to prevent, detect and respond to attacks

- Please visit the following website for additional information:

    https://mile2.com/mile2-online-estore/classess/cihe-certified-incident-handling-engineer-shop.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
Mile2: Certified Information Systems Security Manager (CISSM) Training

- The Certified Information Systems Security Manager (CISSM) course provides the student with the knowledge and proficiency to prepare for the globally recognized CISSM certification exam. This course will provide the student the tools to build their technical skills to manage, design, oversee and assess an enterprise's information security systems

- Please visit the following website for additional information:

  https://mile2.com/mile2-online-estore/classess/cissm-certified-information-systems-security-manager-shop.html

Course Description
Mile2: Certified Information Systems Security Officer (CISSO) Training

- The Certified Information Systems Security Officer (CISSO) course prepares individuals to analyze an organization's information security threats and risks, and design a security program to mitigate these risks. This course is designed to help students become Certified Information Systems Security Officer

- Please visit the following website for additional information:

  https://www.mile2.com/mile2-online-estore/classess/certified-information-systems-security-officer-shop.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
Mile2: Certified Information Systems Security Risk Manager (CISSRM) Training

- Course that provides fundamental knowledge to become Certified Information Systems Security Risk Manager (CISSRM). Course will be released in fourth quarter of 2015

- Please visit the following website for additional information:

  http://www.mile2.com/mile2-courses.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
Mile2: Certified Network Forensics Examiner (CNFE) Training

- The Certified Network Forensics Examiner (CNFE) course helps students to understand exactly what is going on in a network to ensure its proper use by those instructed with access. It will enhance students' digital forensic competence by adding more advanced network forensics expertise and experience through discussions and practice

- Please visit the following website for additional information:

     http://mile2.com/general-security-courses/certified-network-forensics-examiner.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
Mile2: Certified Professional Ethical Hacker (CPEH) Training

- The Certified Professional Ethical Hacker (CPEH) course helps students gain a valuable skill-set in penetration testing by understand the importance of vulnerability assessments and ethical hacking

- Please visit the following website for additional information:

    http://mile2.com/penetration-testing-ethical-hacking/cpeh.html

Go back to *InfoSec and Privacy Training by Competency*

Go back to *InfoSec and Privacy Training by Certification*

Go back to *InfoSec and Privacy Training by Position Description*

Course Description
Mile2: Certified Penetration Testing Consultant (CPTC) Training

- The Certified Penetration Testing Consultant (CPTC) course provides the knowledge and skills to plan, manage and perform a penetration test

- Please visit the following website for additional information:

    http://www.mile2.com/penetration-testing-ethical-hacking/certified-penetration-testing-expert.html

Course Description
Mile2: Certified Penetration Testing Engineer (CPTE) Training

- The Certified Penetration Testing Engineer (CPTE) course trains students on the 5 key elements of penetration testing: information gathering, scanning, enumeration, exploitation and reporting

- Please visit the following website for additional information:

     http://mile2.com/penetration-testing-ethical-hacking/cpte.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
Mile2: Certified Security Leadership Officer (CSLO) Training

- The Certified Security Leadership Officer (CSLO) course is designed and taught for mid to C level managers as well as any engineers who seek to increase their knowledge in the cyber security arena. The CSLO will give you the ability to better manage IT projects in a secure manner

- Please visit the following website for additional information:

  https://mile2.com/mile2-online-estore/classess/cslo-certified-security-leadership-officer-shop.html

Go back to *InfoSec and Privacy Training by Competency*

Go back to *InfoSec and Privacy Training by Certification*

Go back to *InfoSec and Privacy Training by Position Description*

Course Description
Mile2: Certified Security Sentinel (CSS) Training

- The Certified Security Sentinel (CSS) certification course is intended for anyone that uses a computer on the internet. Attendees will fully understand the security threats that attack daily and countermeasures associated with these attacks

- Please visit the following website for additional information:

  http://www.mile2.com/general-security-courses/certified-security-sentinel.html

Course Description
Mile2: Certified Vulnerability Assessor (CVA) Training

- The Certified Vulnerability Assessor (CVA) training will help students to understand the importance of vulnerability

- Please visit the following website for additional information:

  http://www.mile2.com/general-security-courses/certified-vulnerability-assessor.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
NIGP: Contract Administration

- The Contract Administration in the Public Sector provides essential knowledge for you to better understand and master the world of public procurement

- Please visit the following website for additional information:

  http://www.nigp.org/eweb/StartPage.aspx?Site=NIGP&webcode=pd-05-ep-ot-cd

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
NIGP: Ethics A Survival Kit for Public Procurement

- This course will introduce the student to ethical practices needed during the procurement process. It is designed to offer a practical hands-on approach to ethical decision-making in the public procurement process by engaging in exercises and case studies that reinforce presented concepts

- Please visit the following website for additional information:

  http://www.nigp.org/eweb/StartPage.aspx?Site=NIGP&webcode=pd-13-ep-ot-cd

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
NIGP: Introduction to Public Procurement

- This course provides an overview of fundamental concepts that impact procurement in the public sector

- Please visit the following website for additional information:

  http://www.nigp.org/eweb/DynamicPage.aspx?Site=NIGP&WebCode=InstEvent&Reg_evt_key=a2fdd1a7-d747-45dc-890a-7f352dc04c57

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
NIGP: Sourcing in the Public Sector

- This courses provide essential knowledge for you to better understand and master the world of public procurement. This course is intended for those who want to learn how to navigate the process and increase their understanding of the critical issues that frame the concept of public sector sourcing and discusses future sourcing challenges

- Please visit the following website for additional information:

  http://www.nigp.org/eweb/StartPage.aspx?Site=NIGP&webcode=pd-31-ep-ot-cd

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
NIGP: Specification Writing

- This online course addresses fundamental specification requirements in an applied learning setting

- Please visit the following website for additional information:

  http://www.nigp.org/eweb/DynamicPage.aspx?Site=NIGP&WebCode=InstEvent&Reg_evt_key=d81a1114-d432-48b1-9ee3-b669f0b37d92

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
OpenSecurityTraining.info: Introduction to Software Exploits

- This class will cover both the identification of software vulnerabilities and the techniques attackers use to exploit them. In addition, current techniques that attempt to remediate the threat of software vulnerability exploitation will be discussed

- Please visit the following website for additional information:

  http://opensecuritytraining.info/IntroductionToSoftwareExploits.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
OpenSecurityTraining.info: Introduction to Vulnerability Assessment

- This is a lecture and lab based class giving an introduction to vulnerability assessment of some common computing technologies

- Please visit the following website for additional information:

  http://opensecuritytraining.info/IntroductionToVulnerabilityAssessment.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Course Description
OpenSecurityTraining.info: Offensive, Defensive, and Forensic Techniques for Determining Web User Identity

- This course looks at web users from a few different perspectives. First, we look at identifying techniques to determine web user identities from a server perspective. Second, we will look at obfuscating techniques from a user whom seeks to be anonymous. Finally, we look at forensic techniques, which, when given a hard drive or similar media, we identify users who accessed that server

- Please visit the following website for additional information:

    http://opensecuritytraining.info/WebIdentity.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
OpenSecurityTraining.info: Understanding Cryptology: Cryptanalysis

- This course is a mixture of lecture designed to introduce students to a variety of code-breaking techniques and python labs to solidify those concepts

- Please visit the following website for additional information:

  http://opensecuritytraining.info/Cryptanalysis.html

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description

Pearson: CISSP Video Course Domain 2 - Access Control, Downloadable Version

- This lesson covers Access Control - which is a collection of mechanisms that work together to create security architecture to protect the assets of the information system

- Please visit the following website for additional information:

   http://www.pearsonitcertification.com/store/cissp-video-course-9780789739636

Course Description
Pearson: CISSP Video Course Domain 4 - Physical Security, Downloadable Version

- This lesson covers Physical (Environmental) Security - it addresses the threats, vulnerabilities and countermeasures that can be utilized to physically protect an enterprise's resources and sensitive information

- Please visit the following website for additional information:

  http://www.pearsonitcertification.com/store/cissp-video-course-9780789739636

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
Pearson: CISSP Video Course Domain 7 - Telecommunications and Networking, Downloadable Version

- This lesson covers Telecommunications and Network Security - it discusses network structures, transmission methods, transport formats and security measures used to provide availability, integrity and confidentiality

- Please visit the following website for additional information:

  http://www.pearsonitcertification.com/store/cissp-video-course-9780789739636

Course Description
Pearson: CISSP Video Course Domain 6 - Law, Investigation and Ethics, Downloadable Version

- This lesson covers Legal, Regulations, Investigations and Compliance - it addresses computer crime laws and regulations; the investigative measures and techniques which can be used to determine if a crime has been committed and methods to gather evidence

- Please visit the following website for additional information:

  http://www.pearsonitcertification.com/store/cissp-video-course-9780789739636

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
Privacy Professor – Privacy Impact Assessment (PIA) Tool Kit

- This 1 hour video describes the purposes and benefits of doing Privacy Impact Assessments (PIAs), when to do them, how to scope, key stakeholders to involve. It also provides high level PIA methodology, privacy standards to use for the PIA framework, an in-depth look at PIA questionnaires, documentation to review, in-depth review of a PIA report, PIA corrective action plans (CAPs).

- Please visit the following website for additional information:

    http://hipaaprivacy.org/product/privacy-impact-assessment-training/

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
Safari: CISSP Video Course Domain 4 – Physical Security

- This video course includes realistic labs, scenarios, case studies, and animations designed to build and test your knowledge around physical security

- Please visit the following website for additional information:

  https://www.safaribooksonline.com/library/view/cissp-video-course/9780789740175/

Course Description
SANS - DEV522: Defending Web Applications Security Essentials

- This course will help you to better understand web application vulnerabilities, thus enabling you to properly defend your organization's web assets

- Please visit the following website for additional information:

    http://www.sans.org/course/defending-web-applications-security-essentials

Course Description
SANS - DEV536: Secure Coding: Developing Defensible Applications

- Throughout the course we will look at examples of the types of flaws that secure coding protects against, examine how the flaw might be exploited and then focus on how to correct that code

- Please visit the following website for additional information:

    http://www.sans.org/course/secure-coding-developing-defensible-applications

Course Description
SANS - DEV543: Secure Coding in C & C++

- This course will cover all of the most common programming flaws that affect C and C++ code. Throughout the course students are asked to identify flaws in modern versions of common open-source software to provide hands-on experience identifying these issues in existing code

- Please visit the following website for additional information:

    http://www.sans.org/course/secure-coding-c-plus-plus

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SANS - DEV541: Secure Coding in Java/JEE: Developing Defensible Applications

- This course teaches you the art of modern web defense for Java applications by focusing on foundational defensive techniques, cutting edge protections, and Java EE security features that you can use in your applications as soon as you return to work

- Please visit the following website for additional information:

  http://www.sans.org/selfstudy/course/secure-coding-java-jee-developing-defensible-applications

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SANS - DEV544: Secure Coding in .NET: Developing Defensible Applications

- This course will help students leverage built-in and custom defensive technologies to integrate security into their applications

- Please visit the following website for additional information:

  http://www.sans.org/course/secure-coding-net-developing-defensible-applications

Course Description
SANS - FOR408: Windows Forensic Analysis

- This course focuses on a comprehensive and deep analysis of the latest Microsoft Windows operating systems. In this intermediate course, participants will learn directly how forensic analysts track the second-by-second trail left behind by evildoers used in successful criminal prosecution, incident response, media exploitation or civil litigation

- Please visit the following website for additional information:

  http://www.sans.org/course/windows-forensic-analysis

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SANS - FOR518: Mac Forensic Analysis

- This course will enable Windows-based investigators to broaden their analysis capabilities and have the confidence and knowledge to comfortably analyze any Mac or iOS system

- Please visit the following website for additional information:

  http://www.sans.org/event/for518-mac-forensic-analysis-2014/course/mac-forensic-analysis

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SANS - FOR408: Windows Forensic Analysis

- This course focuses on a comprehensive and deep analysis of the latest Microsoft Windows operating systems. In this intermediate course, participants will learn directly how forensic analysts track the second-by-second trail left behind by evildoers used in successful criminal prosecution, incident response, media exploitation or civil litigation

- Please visit the following website for additional information:

  http://www.sans.org/course/windows-forensic-analysis

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SANS - FOR526: Memory Forensics In-Depth

- This course focuses on best practices and recommendations from experts in the field to guide Digital Forensics and Incident Response (DFIR) professionals through acquisition, validation, and memory analysis with real-world and malware-laden memory images. Having in-depth knowledge of Windows memory internals allows the examiner to access target data

- Please visit the following website for additional information:

    http://www.sans.org/course/memory-forensics-in-depth

FOR THE STATE OF SOUTH CAROLINA INTERNAL USE ONLY

Course Description
SANS - FOR572: Advanced Network Forensics and Analysis

- This course covers the tools, technology and processes required to integrate network evidence sources into the investigations, with a focus on efficiency and effectiveness

- Please visit the following website for additional information:

  http://www.sans.org/course/advanced-network-forensics-analysis

Course Description
SANS - FOR585: Advanced Smartphone Forensics

- This course covers the best tools currently available to conduct smartphone and mobile device forensics, and provide detailed instructions on how to manually decode data that tools sometimes overlook

- Please visit the following website for additional information:

  http://www.sans.org/course/advanced-smartphone-mobile-device-forensics

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SANS - FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques

- This training has helped forensic investigators, incident responders, security engineers, and IT administrators acquire the practical skills to examine malicious programs that target and infect Windows systems

- Please visit the following website for additional information:

  http://www.sans.org/course/reverse-engineering-malware-malware-analysis-tools-techniques

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SANS - LEG523: Law of Data Security and Investigations

- This course provides training and continuing education for many compliance programs under information security and privacy mandates such as GLBA, HIPAA, FISMA, and PCI-DSS. In addition, LEG523 is associated with the coveted GIAC Law of Data Security & Investigations (GLEG) certification, which strengthens the credibility of forensics investigators as witnesses in court and can help a forensics consultant win more business

- Please visit the following website for additional information:

    http://www.sans.org/course/law-data-security-investigations

Course Description
SANS - MGT415: A Practical Introduction to Risk Assessment

- In this course participants will learn the practical skills necessary to perform regular risk assessments for their organizations

- Please visit the following website for additional information:

  http://www.sans.org/course/intro-risk-assessment

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SANS - MGT512: Security Leadership Essentials for Manager with Knowledge Compression

- This course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology

- Please visit the following website for additional information:

  http://www.sans.org/course/security-leadership-essentials-managers-knowledge-compression

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SANS - MGT514: IT Security Strategic Planning, Policy and Leadership

- In this course participants will learn the entire strategic planning process. Topics covered in depth include how to plan the plan, horizon analysis, visioning, environmental scans (SWOT, PEST, Porter's etc.), historical analysis, mission, vision, and value statements

- Please visit the following website for additional information:

  http://www.sans.org/course/security-strategic-planning-policy-leadership

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SANS - MGT535: Incident Response Team Management

- This course will take participants to the next level of managing an incident response team. During this course, students will learn by applying course content through hands-on skill-building exercises

- Please visit the following website for additional information:

  http://www.sans.org/course/incident-response-team-management

Course Description
SANS - SEC301: Intro to Information Security

- This introductory certification course is the fastest way to get up to speed in information security. This entry-level course covers a broad spectrum of security topics and is liberally sprinkled with real life examples

- Please visit the following website for additional information:

    http://www.sans.org/course/intro-information-security

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

FOR THE STATE OF SOUTH CAROLINA INTERNAL USE ONLY

Course Description
SANS - SEC401: Security Essentials Bootcamp Style

- This course teaches participants the essential skills and techniques needed to protect and secure an organization's critical information assets and business systems

- Please visit the following website for additional information:

  https://www.sans.org/community/event/sec401-madison-12may2014-doc-blackburn

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SANS - SEC440: Critical Security Controls: Planning, Implementing and Auditing

- This course helps participants master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Council on CyberSecurity

- Please visit the following website for additional information:

   http://www.sans.org/course/critical-security-controls-planning-implementing-auditing

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SANS - SEC464: CyberSecurity Training for IT Administrators

- Unique training program for IT operations and admins that teaches them how to discover evidence of intruder activity, and demonstrate how to work effectively with their organization's security professionals

- Please visit the following website for additional information:

  http://www.sans.org/course/cyber-security-training-for-it-administrators

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SANS - SEC501: Advanced Security Essentials - Enterprise Defender

- This course builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise. During this course, you will learn core components of building a defensible network infrastructure and how to properly secure routers, switches, and network infrastructure, Methods to detect advanced attacks of systems that are currently compromised, methods to detect advanced attacks of systems that are currently compromised, ways to respond to an incident, among others

- Please visit the following website for additional information:

    http://www.sans.org/course/advanced-security-essentials-enterprise-defender

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SANS - FOR508: Advanced Digital Forensics and Incident Response

- This course will help to determine how the breach occurred, comprised and affected systems, what attackers took or changed, and incident containment and remediation

- Please visit the following website for additional information:

    http://www.sans.org/course/advanced-computer-forensic-analysis-incident-response

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SANS - SEC503: Intrusion Detection In Depth

- This training delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence

- Please visit the following website for additional information:

  http://www.sans.org/course/intrusion-detection-in-depth

Course Description
SANS - SEC504: Hacker Tools, Techniques, Exploits and Incident Handling

- The course is particularly well-suited to individuals who lead or are a part of an incident handling team. General security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks

- Please visit the following website for additional information:

  http://www.sans.org/course/hacker-techniques-exploits-incident-handling

Course Description
SANS - SEC560: Network Penetration Testing and Ethical Hacking

- This course prepares participants to perform detailed reconnaissance by examining a target's infrastructure and mining blogs, search engines, social networking sites and other Internet and intranet infrastructure

- Please visit the following website for additional information:

   http://www.sans.org/course/network-penetration-testing-ethical-hacking

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SANS - SEC542: Web App Penetration Testing and Ethical Hacking

- SEC542 helps students move beyond push-button penetration testing to professional web application penetration testing that finds flaws before the adversaries discover and abuse them

- Please visit the following website for additional information:

  http://www.sans.org/course/web-app-penetration-testing-ethical-hacking

Course Description
SANS - SEC561: Intense Hands-on Pen Testing Skill Development (with SANS NetWars)

- With over 30 hours of intense labs, students experience a leap in their capabilities, as they come out equipped with the practical hands-on skills needed to address today's pen test and vulnerability assessment projects in enterprise environments

- Please visit the following website for additional information:

    http://www.sans.org/event/sans-2014/course/hands-on-penetration-skill-development

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SANS - SEC566: Implementing and Auditing the Critical Security Controls - In-Depth

- The course will teach how to master the specific techniques and tools needed to implement and audit the 'Twenty Critical Security Controls', a prioritized, risk-based approach to security

- Please visit the following website for additional information:

    http://www.sans.org/course/implementing-auditing-critical-security-controls

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SANS - SEC580: Metasploit Kung Fu for Enterprise Pen Testing

- This class will show students how to apply the incredible capabilities of the Metasploit Framework in a comprehensive penetration testing and vulnerability assessment regimen, according to a thorough methodology for performing effective tests

- Please visit the following website for additional information:

  http://www.sans.org/course/metasploit-kung-fu-enterprise-pen-testing

Course Description
SANS - SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses

- This course teaches participants how to identify the threats that expose wireless technology and build on this knowledge to implement defensive techniques that can be used to protect wireless systems. This course prepares participants to obtain GIAC Auditing Wireless Networks (GAWN)

- Please visit the following website for additional information:

  http://www.sans.org/course/wireless-ethical-hacking-penetration-testing-defenses

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SANS - SEC642: Advanced Web App Penetration Testing and Ethical Hacking

- This advanced pen testing course uses a combination of lecture, real-world experiences, and hands-on exercises to teach the techniques used to test the security of enterprise applications

- Please visit the following website for additional information:

  http://www.sans.org/course/advanced-web-app-penetration-testing-ethical-hacking

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SANS - SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

- This course shows penetration testers how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws

- Please visit the following website for additional information:

    http://www.sans.org/course/advanced-penetration-testing-exploits-ethical-hacking

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Course Description
SANS - SEC760: Advanced Exploit Development for Penetration Testers

- This course teaches the skills required to reverse engineer 32-bit and 64-bit applications, perform remote user application and kernel debugging, analyze patches for 1-day exploits, and write complex exploits, such as use-after-free attacks, against modern software and operating systems

- Please visit the following website for additional information:

    http://www.sans.org/course/advance-exploit-development-pentetration-testers

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SC: Business Practices

- Half-day course provides information on how agencies do business with MMO

- Please visit the following website for additional information:

    http://procurement.sc.gov/PS/training/PS-training-classes.phtm?number=MMO-3

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SC: Compendium Overview

- This course provides a practical overview of the new compendium, with a focus on the overall structure, the guidance, the forms, and all parts of the compendium other than Parts II.A. and Part VII

- Please visit the following website for additional information:

  http://procurement.sc.gov/PS/training/PS-training-classes.phtm?number=MMO-4-B

Course Description
SC: Construction Procurement - Written Determinations

- This course provides an understanding of requirements for and purposes of written determinations required by the Procurement Code, and how to write a determination meeting the requirements of law

- Please visit the following website for additional information:

  http://procurement.sc.gov/PS/training/PS-training-classes.phtm?number=OSE-1

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SC: Contract Administration

- This full one-day course provides guidelines for a South Carolina State Government standardized approach to Contract Administration

- Please visit the following website for additional information:

    http://procurement.sc.gov/PS/training/PS-training-classes.phtm?number=MMO-1

Go back to *InfoSec and Privacy Training by Competency*

Go back to *InfoSec and Privacy Training by Certification*

Go back to *InfoSec and Privacy Training by Position Description*

Course Description
SC: Ethics in Public Procurement

- This course gives a greater understanding of Ethics and how it impacts the day to day operations of public procurement

- Please visit the following website for additional information:

  http://procurement.sc.gov/PS/training/PS-training-classes.phtm?number=MMO-8

Go back to *InfoSec and Privacy Training by Competency*

Go back to *InfoSec and Privacy Training by Certification*

Go back to *InfoSec and Privacy Training by Position Description*

Course Description
SC: FOIA and Document Requests in SC

- This course is designed to help participants navigate the Freedom of Information Act, Procurement Code, and Trade Secrets Act and balance the need for disclosure with the need for maintaining integrity in the procurement process

- Please visit the following website for additional information:

  http://procurement.sc.gov/PS/training/PS-training-classes.phtm?number=MMO-7

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SC: FOIA's Meeting Rules & the Evaluation Process

- This course is designed to help participants conduct a competitive sealed proposal, including the evaluation process, in compliance with FOIA's meeting rules

- Please visit the following website for additional information:

  http://procurement.sc.gov/PS/training/PS-training-classes.phtm?number=MMO-6

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SC: Issues in Guaranteed Maximum Price (GMP) Contracting

- During this course, students will learn about the components of a Guaranteed Maximum Price (GMP), pitfalls in GMP contracting and other issues related to the administration of GMP type contracts such as Construction Management at-Risk

- Please visit the following website for additional information:

  http://procurement.sc.gov/PS/training/PS-training-classes.phtm?number=OSE-3

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SC: IT Vendor Procurement Training

- One-day training program for vendors that provide information technology products and services to governmental entities within the State of South Carolina. This course is designed to help businesses be more successful doing business with government

- Please visit the following website for additional information:

   http://procurement.sc.gov/PS/training/PS-training-classes.phtm?number=ITMO-1

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SC: Legal Aspects of Purchasing

- This course will provide information that is critical to ensuring all procurements have a solid legal foundation and legal issues that you may face on a day-to-day basis

- Please visit the following website for additional information:

    http://procurement.sc.gov/PS/training/PS-training-classes.phtm?number=MMO-4-A

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Course Description
SC: Procurement Code in a Nutshell

- Half-day course focuses on demystifying the code and identifying the requirements most Procurement Officers need to know

- Please visit the following website for additional information:

  http://procurement.sc.gov/PS/training/PS-training-classes.phtm?number=MMO-2

Course Description
SC: Procurement of Architect / Engineer Services

- During this course, students will learn what services qualify as professional design services and the steps and procedures for procuring professional design services in compliance with the requirements of the Procurement Code

- Please visit the following website for additional information:

  http://procurement.sc.gov/PS/training/PS-training-classes.phtm?number=OSE-2

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
SC: Request for Proposal (RFP) Process

- During this course, participants will be taken through the processes from beginning to end and also learn the common pitfalls associated with Request for Proposal (RFP)

- Please visit the following website for additional information:

  http://procurement.sc.gov/PS/training/PS-training-classes.phtm?number=MMO-5

Course Description
SC: Standard General Bidding Instructions

- This training provides a better understanding of the information necessary to publish good bidding documents

- Please visit the following website for additional information:

  http://procurement.sc.gov/PS/training/PS-training-classes.phtm?number=MMO-4-C

Course Description
SC: Standard Terms & Conditions

- This course will focus on the standard terms and conditions of the "Uniform State Provisions & Clauses" a/k/a/ the "Compendium"

- Please visit the following website for additional information:

    http://procurement.sc.gov/PS/training/PS-training-classes.phtm?number=MMO-4-D

Course Description
SEI Certification: Certified Computer Security Incident Handler (CSIH)

- The CERT-Certified Computer Security Incident Handler (CSIH) certification and Clearmodel training program to support the needs of military, civilian, and contract personnel who handle information systems

- Please visit the following website for additional information:

    http://seicertification.clearmodel.com/get-certified/computer-security/cert-certified-computer-security-incident-handler/

Course Description
State of South Carolina Data Classification Training

- This self-paced training explains the State of South Carolina data classification model created to categorize the State's data for efficient use and protection

- Please visit the following website for additional information:

  http://dis.sc.gov/resources/Documents/Data_Classification_Training_Deck_Abbreviated.pdf

  http://dis.sc.gov/PoliciesAndProcedures/Pages/default.aspx

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Course Description
TechTarget: Access Control Models, Administration, IPS/IDS Training Video

- In this special multimedia presentation from SearchSecurity's CISSP Essentials Security School, expert exam trainer Shon Harris, CEO and founder of Logical Security, discusses different access control models -- how subjects access objects -- including discretionary, mandatory and role-based access control

- Please visit the following website for additional information:

  http://searchsecurity.techtarget.com/feature/CISSP-training-video-Access-control-models-administration-IPS-IDS

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
TechTarget: Access Control Security Models Training Video

- In this special multimedia presentation from SearchSecurity's CISSP Essentials Security School, expert CISSP exam trainer Shon Harris, CEO and founder of Logical Security, offers a detailed review of security controls, assurance evaluation and certification/accreditation

- Please visit the following website for additional information:

  http://searchsecurity.techtarget.com/feature/CISSP-training-video-Access-control-security-models

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
TechTarget: Authentication Technologies, Federated Identities Training Video

- The CISSP training presentation delves into what identity management systems are and their goals, and also touches upon the topics of digital identity and federated identity

- Please visit the following website for additional information:

  http://searchsecurity.techtarget.com/feature/CISSP-training-video-Authentication-technologies-federated-identities

Course Description
TechTarget: Data Classification Podcast

- In this podcast, John Merryman of GlassHouse Technologies will help you figure out why unstructured data is so difficult to classify, whose responsibility data classification should be and what the trends in the data classification market will be in the future

- Please visit the following website for additional information:

  http://searchstorage.techtarget.com/report/Data-classification-podcast

Go back to <u>InfoSec and Privacy Training by Competency</u>

Go back to <u>InfoSec and Privacy Training by Certification</u>

Go back to <u>InfoSec and Privacy Training by Position Description</u>

Course Description
UMBC Training: Advanced Data Warehousing

- This 3-day course introduces experienced students to best industry practices for dealing with difficult data warehouse data structures, databases and processes

- Please visit the following website for additional information:

  http://umbctraining.com/Courses/catalog/IT-4838C

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
UMBC Training: Designing the Data Warehouse Workshop

- This 3-day workshop focuses on the full end-to-end process of the data warehouse, namely, Gather, Store and Deliver

- Please visit the following website for additional information:

  http://umbctraining.com/Courses/catalog/IT-4837C

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
UMBC Training: Foundations of Data Mining

- The course will provide a comprehensive introduction to the data mining process steps using practical applications. The emphasis will be on the foundation of the data mining techniques

- Please visit the following website for additional information:

    http://umbctraining.com/Courses/catalog/IT-4832C

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
IAPP: Certification Foundation Training

- The course explains common principles and approaches to Privacy, introduces the major privacy models employed around the globe, and provides an overview of privacy and data protection regulation by jurisdictions and by industry sector

- Please visit the following website for additional information:

  https://privacyassociation.org/media/pdf/certification/course-outlines/FoundationCourseOutline.pdf

*This course will be retired on July 1st, 2015

Course Description
SANS - MGT305: Technical Communication and Presentation Skills for Security Professionals

- This course is designed for every IT professional in your organization. In this course we cover the top techniques that will show any attendee how to research and write professional quality reports, and how to create outstanding presentation materials. Attendees will also get a crash course on advanced public speaking skills

- Please visit the following website for additional information:

  http://www.sans.org/course/technical-communication-presentation-skills-security-professionals

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description

Course Description
ISACA: Certified in the Governance of Enterprise IT (CGEIT) Training

- ISACA provides Certified in the Governance of Enterprise IT (CGEIT) exam preparation workshops in various cities throughout the year. These workshops focus on IT governance, key points covered in the CGEIT exam, and class practice questions and discussion

- ISACA additionally provides CGEIT exam study materials including the CGEIT Review Manual 2015 and CGEIT Review Questions, Answers & Explanations Manual 2015. These materials can be accessed at the website below

- Please visit the following website for additional information:

  http://www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Pages/default.aspx

Go back to InfoSec and Privacy Training by Competency

Go back to InfoSec and Privacy Training by Certification

Go back to InfoSec and Privacy Training by Position Description