



InfoSec Academy Information Systems Leadership Track

Fundamental Courses	Foundational Courses	Specialized Courses	Advanced Courses	Certification Preparation Courses
Texas Security & Policy Assurance Soft Skills	Certified Security Sentinel	Certified Information Systems Security Officer	Top 20 Information Systems Controls	Certified Information Systems Security Professional (CISSP) Certified Information Security Manager (CISM) Certified Information Systems Auditor (CISA) Certified Ethical Hacker (CEH)



InfoSec Academy

Information Systems Leadership Track

Course Details

Course Name	Description	Professional Roles	Modules
Texas Security Policy & Assurance Course	Upon successful completion of this course, the participant will be prepared to apply the state rules regarding information security in the state of Texas within their agency.	ISOs & CISOs	Module 1: Texas Rules and Legislation Modules 2: Data Classification Module 3: Security Framework Module 4: Agency Security Plans Modules 5: Reports Modules 6: Security Services
Soft Skills Course (examples): Team Building Without Time Wasting Helping Employees Use Their Time Wisely Everybody Wins: How to Turn Conflict into Collaboration	A variety of soft skills courses are available covering a wide range of topics.	Dependent on the course	N/A



InfoSec Academy

Information Systems Leadership Track

Course Details

Course Name	Description	Professional Roles	Modules
Certified Security Sentinel - C)SS	<p>The Certified Security Sentinel certification course is intended for anyone that uses a computer on the internet. Attendees will not only understand security threats and attacks but also be prepared with countermeasures for these attacks. The weakest link in any companies' security program is a poorly trained employee. Once a student understands what can happen, they will know what to look for. And with that understanding, be able to keep the information they have been entrusted with as safe as possible.</p> <p>The social engineering portion of the class is designed to teach the participants the skills used by social engineers to facilitate the extraction of information from an organization using technical and non-technical methods. Computer fraud, black-hat hacking, and cyber-terrorism are all phrases that describe crimes that use over-the-wire technology to attack, steal, and terrorize their victims. The key to most of these over-the-wire attacks being successful is information they receive through social engineering. Does it work? Can smart people be easily deceived? Kevin Mitnick, who served five years in prison for repeated hacking said in testimony before Congress on the subject of Social Engineering: "I was so successful with that attack that I rarely had to resort to a technical attack." If you're afraid of having your identity, credit card credentials, or business information compromised, then this is the training you have been looking for.</p> <p>The Certified Security Sentinel certification course trains students on how attacks are performed, how to identify an attack, and how to secure information. One of the most valuable skill sets of a C)SS is that they understand how to train others on security as well.</p>	Employees who need to learn the basics of security.	Module 1: Basic Computer Security Module 2: User Awareness Module 3: Implementation Countermeasures Module 4: Essential Security Awareness Module 5: Using the Internet at Work Module 6: Accessing the Network Locally Module 7: Accessing the Network Remotely Module 8: Social Engineering Module 9: Understanding and Interacting with our Target Module 10: Researching Our Target Module 11: Methods of Deception



InfoSec Academy

Information Systems Leadership Track

Course Details

Course Name	Description	Professional Roles	Modules
Certified Information Systems Security Officer - C)ISSO	<p>The Certified Information Systems Security Officer course is designed for forward-thinking security professionals that want the advanced skillset necessary to manage and consult businesses on information security.</p> <p>The C)ISSO addresses the broad range of industry best practices, knowledge and skills expected of a security leader. The candidate will learn both the theory and the requirements for practical implementation of core security concepts, practices, monitoring and compliance. Through the use of a risk-based approach, a C)ISSO is able to implement and maintain cost-effective security controls that are aligned with business requirements.</p> <p>Whether you are responsible for the management of a Cyber Security team, a Security Officer, an IT auditor or a Business Analyst, the C)ISSO course is the ideal way to increase your knowledge, expertise, skill, and credibility.</p> <p>The C)ISSO program standards are closely aligned with those of the ISO27001, NIST, CISM® and the CISSP® CBK® exam objectives. The C)ISSO excels by providing a well-rounded, comprehensive overview of essential security topics.</p>		Module 1: Risk Management Module 2: Security Management Module 3: Identification and Authentication Module 4: Access Control Module 5: Security Models and Evaluation Criteria Module 6: Operations Security Module 7: Symmetric Cryptography and Hashing Module 8: Asymmetric Cryptography and PKI Module 9: Network Connections Module 10: Network Protocols and Devices Module 11: Telephony, VPNs and Wireless Module 12: Security Architecture and Attacks Module 13: Software Development Security Module 14: Database Security and Development Module 15: Malware and Software Attacks Module 16: Business Continuity Module 17: Disaster Recovery Module 18: Incident Management, Law, and Ethics Module 19: Physical Security



InfoSec Academy

Information Systems Leadership Track

Course Details

Course Name	Description	Professional Roles	Modules
Certified Information Systems Security Manager - C)ISSM	<p>The Certified Information Systems Security Manager certification course is was designed to teach towards and certify a information systems professional's high standard of excellence in following areas:</p> <ol style="list-style-type: none"> 1. Information Security Governance 2. Information Risk Management and Compliance 3. Information Security Program Development and Management 4. Information Security Incident Management <p>While we provide thorough training in these 4 critical areas of information systems security management, most who take the C)ISSM have professional experience in all four of these areas. A gap of experience in some of these fields can be bridged by achieving our C)ISSO: Certified Information Systems Security Officer Certification available at mile2.com.</p>	IT Auditor IT Consultant Security Consultant Chief Information Officer	Module 1 - Introduction Module 2 - Information Security Governance Module 3 - Information Risk Management and Compliance Module 4 - Information Security Program Development and Management Module 5 - Information Security Incident Management



InfoSec Academy

Information Systems Leadership Track

Course Details

Course Name	Description	Professional Roles	Modules
<p>Top 20 Information Systems Controls</p>	<p>The Information Systems 20 Controls certification course covers understanding and implementing the 20 most important security controls. These controls were chosen by leading government and private organizations who are experts on how attacks work and what can be done to prevent them from happening. The controls were selected as the best way to block known attacks as well as help search for and alleviate any damage from the attacks that are successful. This course allows the security professional to see how to implement controls in your existing network though highly effective and economical automation. For management, this training is the best way to distinguish how you will assess whether these security controls are effectively being administered.</p> <p>Our instructors have real-world experience and will show you the value of what you are learning in proprietary case studies. As a result of this course and exam, attentive students are prepared to be leaders of future security projects, because they will have a plan for exactly what needs to be done in securing a network.</p>	<p>Information Systems Professional Security Consultant Chief Information Officer IT Professional</p>	<p>Introduction Critical Control 1: Inventory of Authorized and Unauthorized Devices Critical Control 2: Inventory of Authorized and Unauthorized Software Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers Critical Control 4: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches Critical Control 5: Boundary Defense Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs Critical Control 7: Application Software Security Critical Control 8: Controlled Use of Administrative Privileges Critical Control 9: Controlled Access Based on Need to Know Critical Control 10: Continuous Vulnerability Assessment and Remediation Critical Control 11: Account Monitoring and Control Critical Control 12: Malware Defenses Critical Control 13: Limitation and Control of Network Ports, Protocols, and Services Critical Control 14: Wireless Device Control Critical Control 15: Data Loss Prevention Critical Control 16: Secure Network Engineering Critical Control 17: Penetration Tests and Red Team Exercises Critical Control 18: Incident Response Capability Critical Control 19: Data Recovery Capability Critical Control 20: Security Skills Assessment</p>



InfoSec Academy

Information Systems Leadership Track

Course Details

Course Name	Description	Professional Roles	Modules
Certified Security Leadership Officer - C)SLO	<p>The Certified Security Leadership Officer course is designed to give management an essential understanding of current security issues, best practices, and technology. Because a C)SLO understands security, he or she is prepared to manage the security component of a business and its information technology security projects. A C)SLO can be seen as the bridge between those who understand security and those who don't. These skills can be put to use the day the a C)SLO returns to work.</p> <p>Essentials topics covered in this management track include: Network Fundamentals and Applications, Hardware Architecture, Information Assurance Foundations, Computer Security Policies, Contingency and Continuity Planning, Business Impact Analysis, Incident Handling, Architectural Approaches to Defense in Depth, Cyber Attacks, Vulnerability Assessment and Management, Security Policies, Web Security, Offensive and Defensive Information Warfare, culminating with Management Practicum.</p>	<p>Information Systems Professional Security Consultant Chief Information Officer IT Professional</p>	<p>Module 1: Wireless Networks—802.11 Module 2: Access Control Module 3: Computer Forensics and Legalities Module 4: Cryptography Applications Module 5: Cryptography Algorithms and Concepts Module 6: Key Management Module 7: Cryptosystems Module 8: Digital Acquisition Module 9: DNS Module 10: Disaster Recovery and Business Continuity Planning Module 11: Endpoint Security Module 12: Honey pots, Honeynets, Honeytokens, Tarpits, oh my Module 13: IP Terms and Concepts Module 14: Logging Module 15: Malicious Software Module 16: Managing Security Policy Module 17: Methods of Attack Module 18: Mitnick-Shimomura Module 19: Physical Security Module 20: Risk Management & Security Module 21: Security and Organizational Structure Module 22: Security Awareness Module 23: Steganography Module 24: The Intelligent Network - Unified Threat Management (UTM) Module 25: Network Infrastructure Module 26: Vulnerability Assessment – Outside View Module 27: Vulnerability Management – inside view</p>