

COURSE CATALOG - LINE MANAGER

JOB FUNCTIONS	COURSES						
<u>Laws, Regulations and Policies:</u> Understand government-wide and organization-specific published documents governing mandated requirements and standards for the management and protection of information technology resources.	SANS Track 9						
Explain and be aware of national and DOE cyber security laws, regulations and procedures							
Ability to lead the effort to ensure security awareness by users and line managers	✓						
Enforce your organization's cyber security policies	✓						
Describe organizational cyber security policies	✓						
Recognize and investigate potential violations	✓						
Evaluate conflicting functional requirements and select those requirements that will provide the highest level of security at the minimum cost							
<u>Security Program Management:</u> Understand IT security program elements and administrative policies to ensure an effective IT security program.							
Understand the cyber security roles of various organizational personnel	✓						
Describe:							
- your organization's internet security procedures	✓						
- WAN/LAN security procedures	✓						
Understand change control policies							
Define system threats	✓						
Define system vulnerabilities	✓						
Define the services on his/her systems that are vulnerable and determine whether those services can be turned off							
Describe security inspections/reviews/assessments	✓						
Understand system and database integrity	✓						
Explain concepts of confidentiality, integrity and accountability	✓						
Give examples of alarms, signals and reports							
Describe disaster recovery procedures							
Describe system protection measures:							
- discuss your responsibility for system protection	✓						
- describe responsibilities with software copyrights							
- describe protection on software							
- describe approaches used to prevent software piracy							
- describe approaches for e-mail privacy							
- describe the use of caller ID							

JOB FUNCTIONS	COURSES						
	SANS Track 9						
Security Program Management (continued)							
- describe different types of network security software	✓						
- define network firewalls	✓						
- define methods of intrusion detection	✓						
Describe continuity planning							
Describe electronic records management	✓						
Explain information ownership principles							
Explain how to avoid the five most common social engineering attacks							
Describe authentication mechanisms, discretionary and mandatory access controls, one-time passwords							
Describe password management policy							
Describe configuration management							
Discuss privileges							
Explain the benefits of auditing and monitoring							
Explain risk management concepts	✓						
Define categories of risk to an organization and define your organization's risk management process	✓						
Design of Security Systems, Processes and Procedures: Provide guidance to ensure safeguards are incorporated in the design of information systems.							
Describe the Project Management Processes							
Participate in the identification of system confidentiality, integrity and availability in relation to user needs and risk management	✓						
Draft security concept of operations document for proposed system	✓						
Development of Security Systems, Processes and Procedures: Ensure that security requirements are considered, resolved and incorporated as information systems and technologies are developed or changed.							
Participate in the development and modification of approaches to correct vulnerabilities identified during system implementation	✓						
Operation of Security Systems: Implement and maintain systems and their safeguards, identify departures from plans and new vulnerabilities, or make operational and procedural changes, to ensure that appropriate safeguards are within acceptable levels of risk.							
Use network access controls as designed	✓						
Perform backups							
Perform risk management	✓						

JOB FUNCTIONS	COURSES						
	SANS Track 9						
Operation of Security Systems (continued)							
Use protection measures	✓						
Perform corrective actions	✓						
Implement intrusion detection procedures	✓						
Use alarms, signals and reports in accordance with existing policies and procedures							
Implement disaster recovery procedures							
Implement storage media protection and controls							
Install virus detection and update virus datasets							
Terminate Security Systems: Implement the system security termination plan, including the security requirements for archiving and disposing of resources.							
Identify and explain disposition of media and data policies and procedures							
Comply with termination procedures and report any incident or breaches							