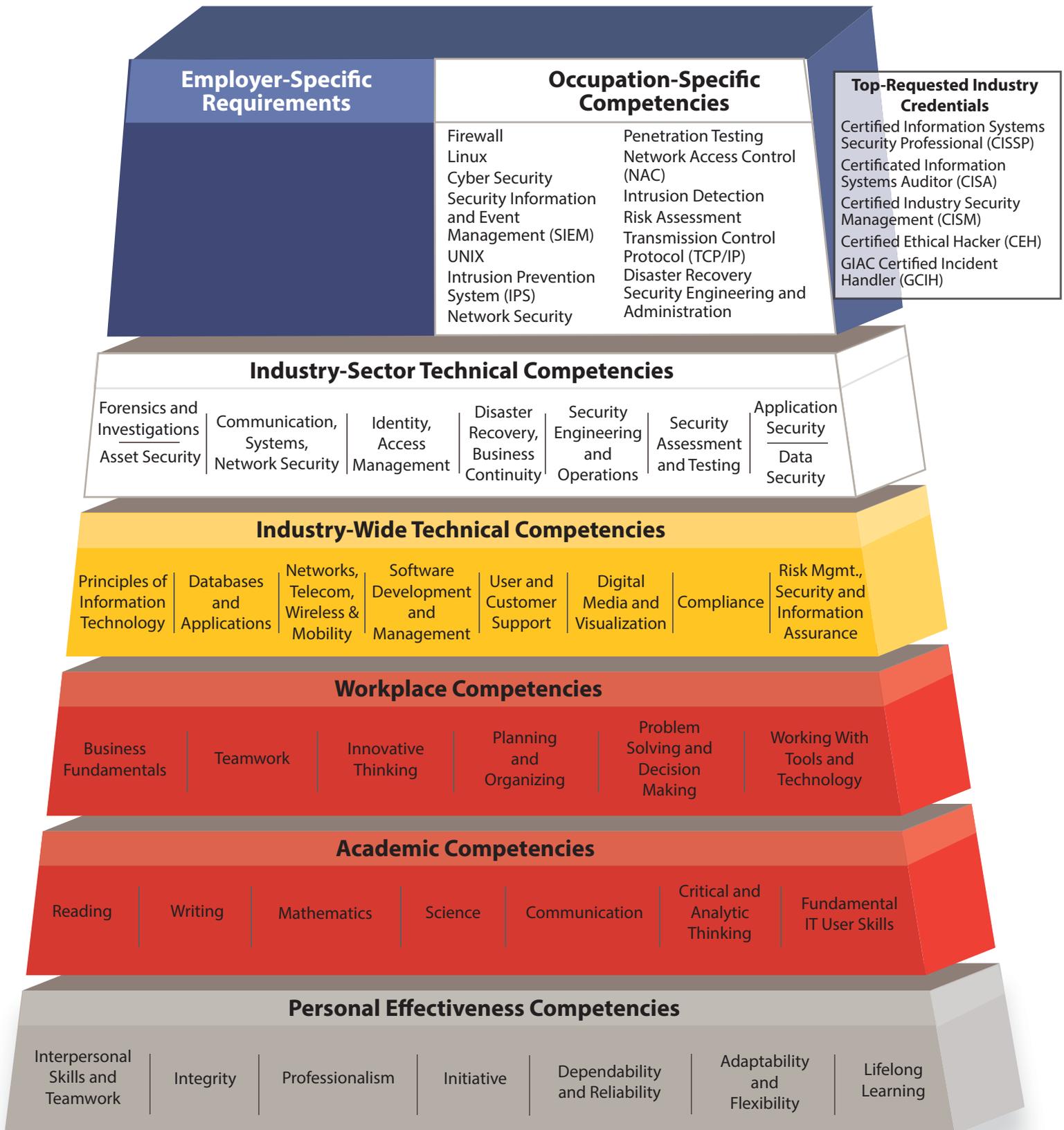


Minnesota Dual-Training Pipeline

Competency Model for Information Technology

Occupation: Security Analyst



Based on: Information Technology Competency Model Employment and Training Administration, United States Department of Labor, September 2012.

Competency Model for Security Analyst

Security Analyst - A security analyst is responsible for maintaining the security and integrity of data. They must have knowledge of every aspect of information security within the company. Their main job is to analyze the security measures of a company and determine how effective they are.

Industry-Sector Technical Competencies

- Communication, Systems, Network Security – Training in keeping communications, systems and networks secure.
- Forensics and Investigations – Knowledge of IT forensics to recover information and investigate network security breaches.
- Asset Security – Understanding of procedures to inventory IT assets and securely manage IT resources.
- Identity, Access Management – Training in granting users appropriate access to IT resources and preventing access by non-authorized users.
- Disaster Recovery, Business Continuity – Understand the importance of keeping business functions and computing processes on-going and how to recover from an outage or equipment failure. Strategic contingency planning for catastrophic system failure.
- Security Engineering and Operations – Training in managing security environments and able to resolve technical issues.
- Security Assessment and Testing – Understanding of how to secure internal and external applications/systems and applying techniques to test asset security.
- Application Security – Knowledge of measures taken to prevent gaps (vulnerabilities) in the security policy of an application or the underlying system through flaws in the design, development, deployment, upgrade, or maintenance of the application.
- Data Security – Training in protecting data from destructive and unwanted actions of unauthorized and/or careless users.

Occupation-Specific Competencies, typically address in on-the-job training

- Firewall – Able to maintain and update the security system controlling the incoming and outgoing network traffic.
- Linux/ UNIX – Demonstrate knowledge of Linux/UNIX operating systems and the underlying source codes.
- Cyber Security – Demonstrate knowledge of processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access.
- Security Information and Event Management (SIEM) – Ability to use the principles of real-time monitoring, correlation of events, notifications and console views (security event management -SEM) as well as providing long-term storage as well as analysis and reporting of log data (security information management-SIM).
- Intrusion Prevention System (IPS) – Maintain network security appliances that monitor network and/or system activities for malicious activity.
- Network Security – Ability to monitor authorized access, prevent misuse and un-authorized modification, or denial to computer network and network-accessible resources.
- Penetration Testing – Use appropriate methods to attack a computer system to look for security weaknesses, potentially gaining access to the computer's features and data.
- Network Access Control (NAC) – Implement and monitor protocols to secure access to network through tools such as antivirus, host intrusion prevention, and vulnerability assessment, user or system authentication and network security enforcement.
- Intrusion Detection – Demonstrate ability to monitor network or system activities for malicious activities or policy violations.
- Risk Assessment – Ability to identify vulnerabilities and threats to the information resources used and deciding what countermeasures, if any, to take to reduce risk.
- Application Security – Ability to identify and/or implement sound coding and testing practices for enterprise applications and software systems.
- Transmission Control Protocol (TCP/IP) – Understand and use protocol to provide reliable, ordered, and error-checked delivery of information between applications running on hosts communicating over an IP network.
- Disaster Recovery – Show competency in rapid restoration of data, systems, and services in the event of significant incidents and disasters using well-designed backups, system redundancies and role management.
- Security Engineering and Administration – Demonstrate ability to implement secure computing environments, controls and countermeasures.

Possible Security Analyst Certifications

- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Industry Security Management (CISM)
- Certified Ethical Hacker (CEH)
- GIAC Certified Incident Handler (GCIH)

Security Analyst Occupational Training Plan

	List Course/Training Name and Title	Description of Courses and/or Training Program	List Responsible Provider: Company, College, Trainer, or other	Anticipated Completion Date
<i>Related Instruction Competencies</i>				
Forensics and Investigations				
Asset Security				
Communication, Systems, Network Security				
Identity, Access Management				
Disaster Recovery/Business Continuity				
Security Engineering and Operations				
Security Assessment and Testing				
Application Security				
Data Security				
<i>On-The-Job Training Competencies</i>				
Firewall				

Linux				
Cyber Security				
Security Information and Event Management (SIEM)				
UNIX				
Intrusion Prevention System (IPS)				
Network Security				
Penetration Testing				
Network Access Control (NAC)				
Intrusion Detection				
Risk Assessment				
Transmission Control Protocol (TCP/IP)				
Disaster Recovery				
Security Engineering and Administration				