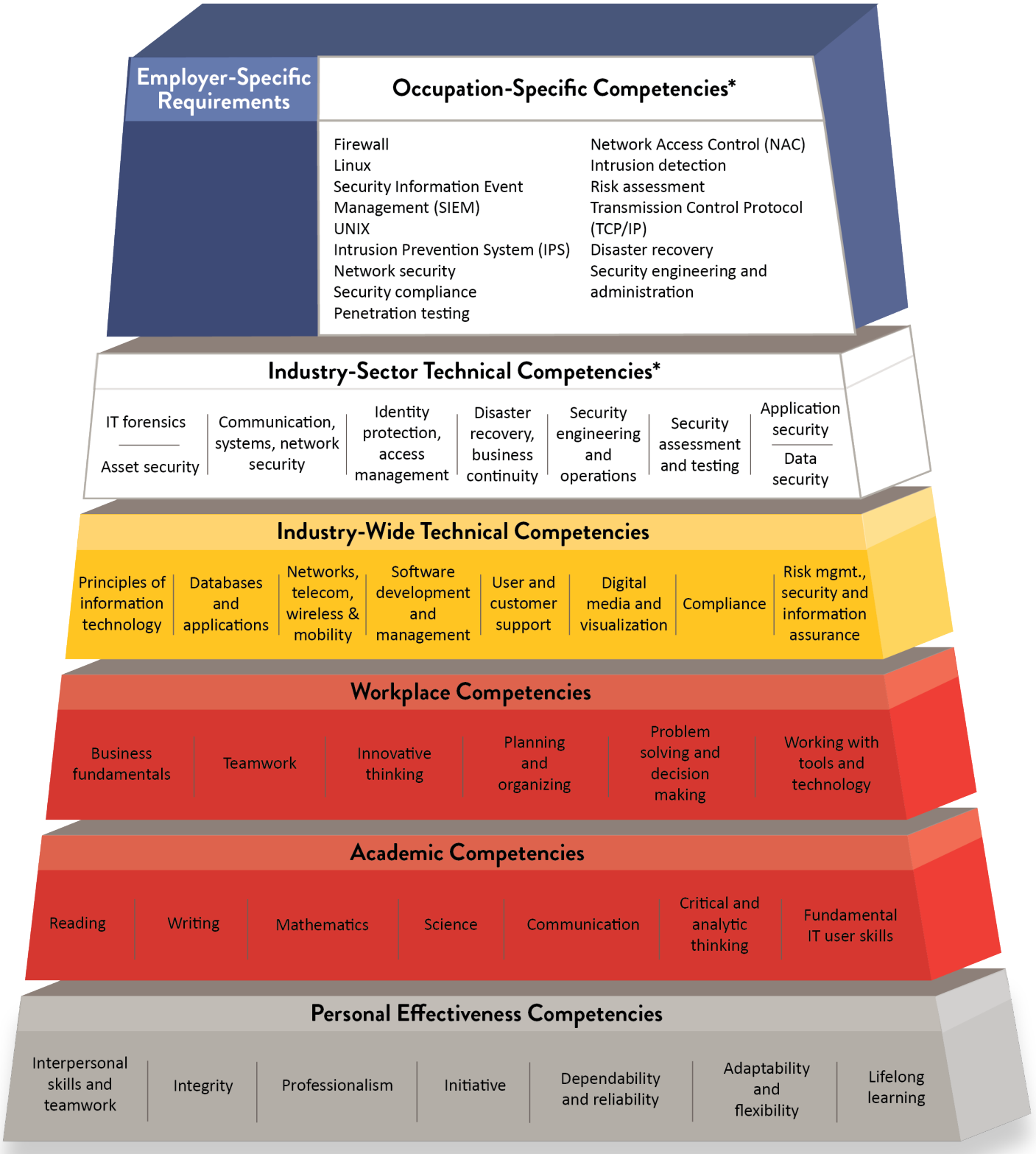
Minnesota Dual-Training Pipeline

Competency Model for Information Technology
Occupation: Information Security Analyst/Specialist



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

*Pipeline recommends the Industry-Sector Technical Competencies as formal training opportunities (provided through related instruction) and the Occupation-Specific Competencies as on-the-job training opportunities.

Competency Model for Information Security Analyst/ Specialist

Information Security Analyst/ Specialist – An information security analyst/ specialist 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 anddetermine how effective they are at preventing threats to the company's data.

Industry-Sector Technical Competencies

Related Instruction for dual training means the organized and systematic form of education resulting in the enhancement of skills and competencies related to the dual trainee's current or intended occupation.

- **Communication, systems, network security** – Know how to keep communications, systems, and networks secure.
- **IT forensics** – Knowledge of IT forensics best practices and how to recover information and investigate network security breaches.
- **Asset security** – Understanding of procedures to inventory IT assets and securely manage IT resources.
- **Identity protection, 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. Know how to do strategic contingency planning for catastrophic system failure.
- **Security engineering and operations** – Understand how to manage security environments and be able to resolve technical problems.
- **Security assessment and testing** – Understanding of how to assess secure internal and external applications/systems and how to apply techniques to test the effectiveness of asset security.

- **Application security** – Knowledge of measures taken to identify and prevent gaps (vulnerabilities) in the security policy of an enterprise application or the underlying software 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

On-the-Job Training (OJT) is hands-on instruction completed at work to learn the core competencies necessary to succeed in an occupation. Common types of OJT include job shadowing, mentorship, cohort-based training, assignment-based project evaluation and discussion-based training.

- **Firewall** – Know how to maintain and update the security system controlling the incoming and outgoing network traffic.

- **UNIX** – Demonstrate knowledge of UNIX operating systems and the underlying source codes that relate to these systems.

- **Linux** – Demonstrate knowledge of Linux operating systems and the underlying source codes that relate to these systems.

- **Security information 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)** – Know how to 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** – Know how to use appropriate methods to attack a computer system to look for security weaknesses, potentially gaining access to the computer's features and data in order to prevent future attacks.

- **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** – Know how to identify vulnerabilities and threats to the information resources used and decide what counter measures, if any, to take to reduce risk.

- **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 compliance** – Know how to create reports and validation to prove how your organization's IT security measures are meeting a set of standards and complying with those standards. This reporting may be kept internally or shared with outside companies to illustrate a level of security inworking with the company.

- **Security engineering and administration** – Know how to create, implement and oversee secure computing environments, controls and counter measures.

Updated July 2022