**Senior Management**

* Is ultimately responsible for security
* Sets strategic direction and expectations for security policy
* Assigns responsibility to the necessary resources to ensure the creation of security policy
* Understands the risks facing the organization

**IT Management**

* Supports all information assets
* Is responsible for designing, writing, and executing security policy
* Ensures that security is a priority
* Makes decisions on the balance of security versus usability, in conjunction with the business
* Is ultimately responsible for confidentiality, integrity, and availability (CIA) of systems

**IT Security Staff**

* Includes IT security program managers and computer security managers
* Is responsible for design, execution, and maintenance of security
* Manages assets that are pertinent to defense
* Manages vulnerabilities and threats
* Implements countermeasures to ensure CIA

**Non-IT Manager**

* Ensures employees have the tools necessary to accomplish their job
* Is responsible for employees' training, understanding, and adherence to security policy
* Must adhere to and support security policy

**Network Administrator**

* Manages computer resources
* Is responsible for changes to resources
* Ensures that resources adhere to the principles of CIA
* Implements technical controls as mandated by security policy

**User**

* Is the consumer of IT resources
* Performs duties determined by job description
* Understands and complies with security policy
* Must be aware of security issues

**Auditor**

* Monitors for compliance
* Tests to ensure controls are in place and effective
* Partners with IT staff to create more effective security policy and controls
* Understands the risks and threats facing an organization