



Security and Personnel

Chapter 11



Positioning & Staffing Security Function

- Location of IS function within organization function
 - IT function as a peer or other IT functions (help desk)
 - Physical security
 - Administrative services function – peer to HR
 - Insurance and risk management function
 - Legal department
- Balance between access and security



Staffing IS Function

- Demand
 - More openings than qualified candidates
- Needs of organization for better hiring practices
 - Knowledge of skills and qualification needed
 - Knowledge of budgetary needs of IS function and associated positions
 - Appropriate level of influence and prestige necessary to perform function



What Security Personnel Should Know

- How an organization operates at all levels.
- That IS security is usually a mgmt problem & seldom exclusively technical problem
- How to work with people
- The role of policy in guiding security functions
- Most IT technologies (not as expert but as generalist)
- Terminology of IT and IS
- How to protect an org's assets from security attacks
- How business solutions can be applied to solve problems
- Strong communications and writing skills



Entry in the IS Professional

- IT technical people
 - Networking experts
 - Programmers
 - Database administrators
 - System Administrators
- Non technical
 - Ex-law enforcement
 - Military personnel



Classification of positions

- Definers
 - Provide policies, guidelines and standards
 - Do consulting and risk assessment
 - Develop the product and technical architectures
 - Senior people with broad knowledge (not depth)
- Builders
 - Techies
 - Create and install security solutions
- Administrators
 - Operate and administer the security tools
 - Monitor
 - Day-to-day work

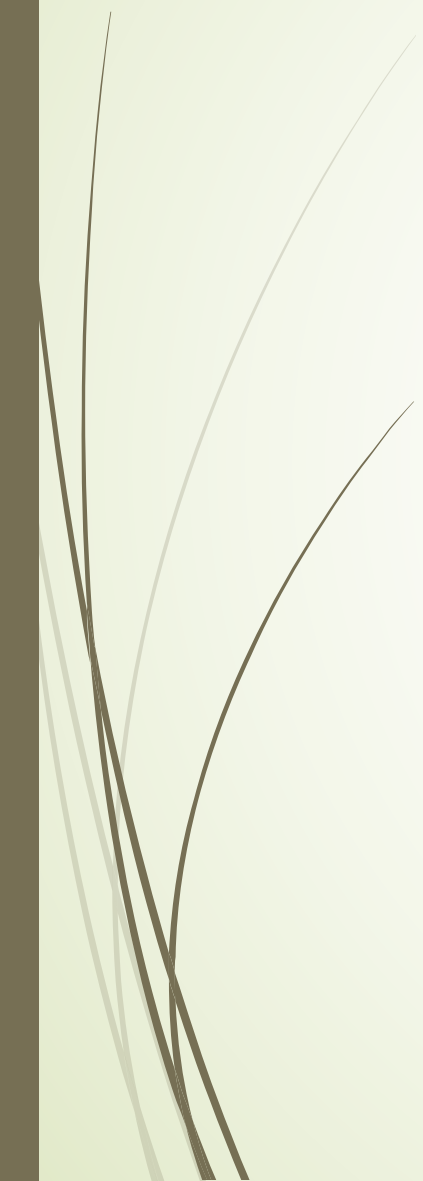


Chief Information Security Officer

- Manages overall info security program
- Drafts or approves info security policies
- Works with CIO with strategic plans
- Develops tactical plans
- Works with security mgmt on operational plans
- Budgeting
- Sets priorities for purchase & implementation on security projects
- Security personnel hiring and firing
- Spokesperson for the info security team



Security Manager

- Develop and manage info security programs & control systems
 - Monitor performance of info security & control system for alignment w/policy
 - Prepare & communicate risk assessment
 - Represent management in change management process
 - Incident response
 - Disaster recovery
 - Supervision
- 

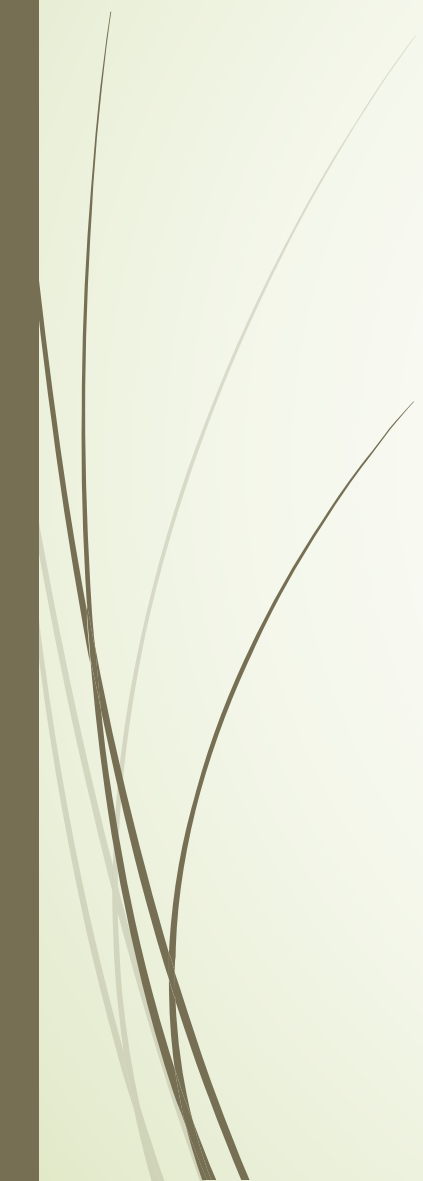


IT Security Compliance Manager

- Develop & manage IT security compliance pgm
- Develop security standards in line with industry standards
- Identify IT related business risk
- Manage and conduct IT security compliance reviews
- Conduct investigation



Security Technician

- Technically qualified
 - Able to configure IDS, firewalls etc
 - Able to implement security measures
 - Entry level
 - Generally must have experience
 - Tend to be specialized in one technical area
- 



Certifications



- ▶ Certified Information Systems Security Professional (CISSP)
 - ▶ Must possess 3 full-time security professional work
 - ▶ Considered most prestigious
 - ▶ Covers 10 domains
 - ▶ Access control
 - ▶ Application security
 - ▶ Business continuity and disaster recovery planning
 - ▶ Cryptography
 - ▶ Information security and risk management
 - ▶ Legal, regulations, compliance and investigations
 - ▶ Operations security
 - ▶ Physical security
 - ▶ Security architecture and design
 - ▶ Telecommunications and network security



Certifications

- Systems Security Certified Practitioner
 - Recognizes mastery of an international standard and body of knowledge
 - Oriented toward the security administrator
 - Focuses on practices, roles and responsibilities
 - 7 domains
 - Access controls
 - Cryptography
 - Malicious code and activity
 - Monitoring and analysis
 - Networks and communications
 - Risks, response and recovery
 - Security operations and administration



Certificates

➤ Associate of (ISC)²

- Geared toward those wanting to take CISSP or SSCP
- Lack requisite experience
- Test required

➤ Certification and Accreditation Professional (CAP)

- Minimum of 2 years experience in 1+ of areas of common body of knowledge domains
- Pass the CAP exam
- Agree to Code of Ethics
- Provide background and criminal history



Certifications

- ▶ Certified Information Systems Auditor (CISA)
 - ▶ Pass exam
 - ▶ Areas
 - ▶ IS auditing process
 - ▶ IT governance
 - ▶ Systems and Infrastructure lifecycle
 - ▶ IT service delivery and support
 - ▶ Protection of information assets
 - ▶ Business and disaster recovery

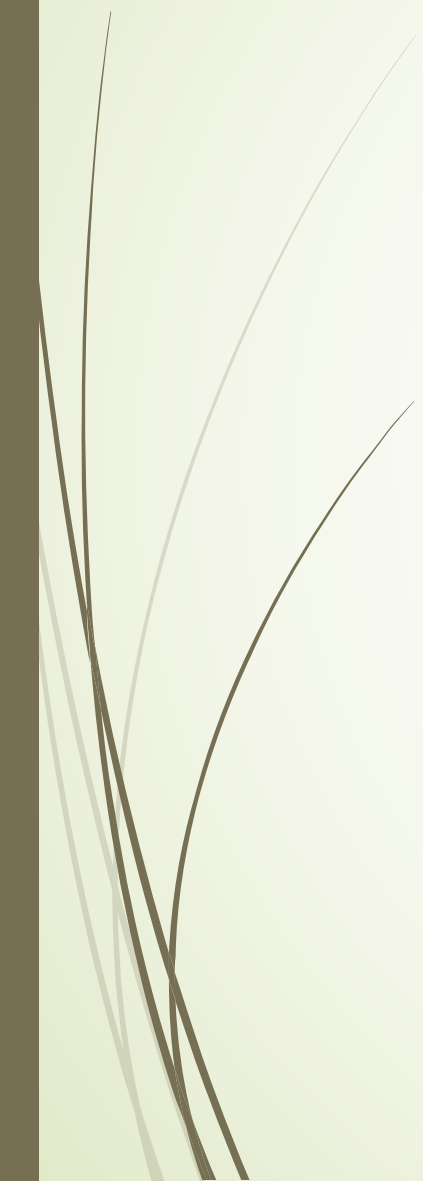


Certifications

- ▶ Certified Information Systems Manager (CISM)
 - ▶ Information Security governance
 - ▶ Information risk management
 - ▶ Information security program development
 - ▶ Information security program management
 - ▶ Incident management and response

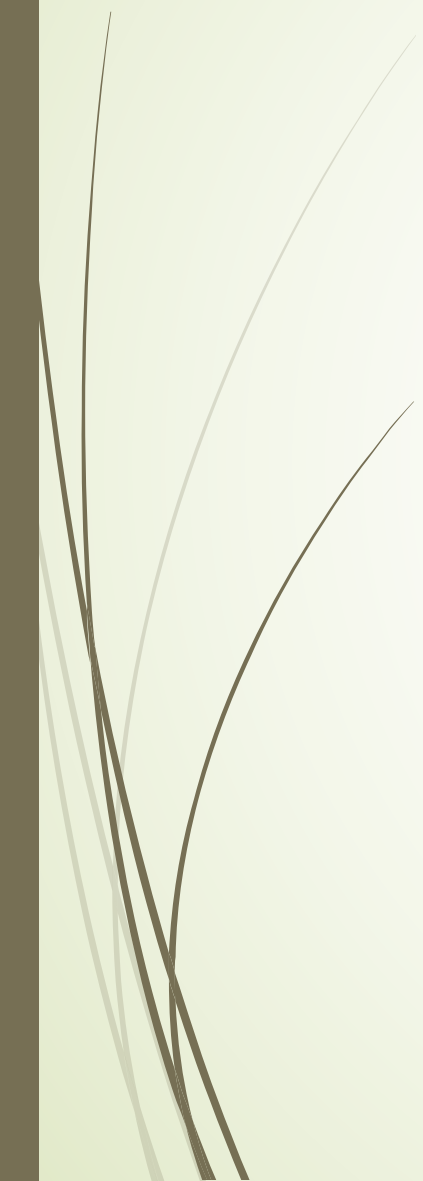


Certifications

- Global Information Assurance Certification (GIAC)
 - Security Certified Professional (SCP)
 - Security+
 - Certified Information Forensic Investigator
 - Various company certifications
- 



Advice for IS Professionals

- ▶ Business before technology
 - ▶ When evaluating a problem
 - ▶ Look at source of problem first
 - ▶ Determine factors impacting problem
 - ▶ Check organizational policy for direction
 - ▶ Use technology to deploy necessary controls
 - ▶ Your job is to protect the orgs information assets
 - ▶ Be heard and not seen
 - ▶ Know more than you say and be more skillful than you let on
 - ▶ Speak to users not at them
 - ▶ Your education is never complete
- 



Personnel Precautions

- Background investigations
 - Conducted for all employees prior to hiring
 - Scope varies with position
 - Extremely sensitive positions – conduct periodically
 - Require written permission as terms of employment



Personnel Precautions

- ▶ Monitoring of employee activity
 - ▶ Internet usage
 - ▶ Surveillance cameras in sensitive areas
 - ▶ Recording telephone conversations
 - ▶ Mandatory vacations
 - ▶ Exit procedures for employees leaving company