SENG 460

Practice of Information Security and Privacy

Information Security Governance and Risk Management

Overview

- Functionality vs. Security
- Security Development
  - Security Program Development
  - Enterprise Security Architecture Development
  - Security Controls Development
  - Process Management Development
- Security Management
  - Security Governance Responsibilities and Roles
  - Security Governance Components
  - Information Value Assessment, Classification & Controls
  - Risk Assessment and Analysis
  - Personnel Security

Functionality vs. Security

- Functionality improvements tends to open more access to end users, while security improvements tend to restrict access to end users (trade-off relationship)
- Functionality is well understood (easy to implement it right), while security is not in most of the cases (easy to implement it wrong)
- Functionality is favored by users, while security is not

To avoid wasting time and money, security development and functionality development have to be balanced, so that productivity is not affected.

Security Program Development

- **Security Through Obscurity**
  - Rely on confusion to provide security, assuming that your enemies are not as smart as you are and that they cannot figure out something that you feel is very tricky
  - Develop security in an ad hoc manner
- **Security Through Framework**
  - Develop security program using a framework made up of many entities: logical, administrative, and physical protection mechanisms, procedures, business processes, and people that all work together to provide a protection level for an environment
  - Develop security in a holistic manner

Security Program Development - British Standard 7799 (BS7799)

- Developed in 1995 by the United Kingdom government's Department of Trade and Industry and published by the British Standards Institution.
  - Outlines how an information security management system (ISMS) (aka security program) should be built and maintained
  - Provide guidance to organizations on how to design, implement, and maintain policies, processes, and technologies to manage risks to its sensitive information assets

• **Information security policy for the organization** Map of business objectives to security, management's support, security goals, and responsibilities.
• **Creation of information security infrastructure** Create and maintain an organizational security structure through the use of a security forum, a security officer, defining security responsibilities, authorization processes, outsourcing, and independent reviews.
• **Asset classification and control** Develop a security infrastructure to protect organizational assets through accountability and inventory, classification, and handling procedures.
• **Personnel security** Reduce risks that are inherent in human interaction by screening employees, defining roles and responsibilities, training employees properly, and documenting the ramifications of not meeting expectations.

• **Physical and environmental security** Protect the organization's assets by properly choosing a facility location, erecting and maintaining a security perimeter, implementing access control, and protecting equipment.
• **Communications and operations management** Carry out operations security through operational procedures, proper change control, incident handling, separation of duties, capacity planning, network management, and media handling.
• **Access control** Control access to assets based on business requirements, user management, authentication methods, and monitoring.
• **System development and maintenance** Implement security in all phases of a system's lifetime through development of security requirements, cryptography, integrity protection, and software development procedures.
• **Business continuity management** Counter disruptions of normal operations by using continuity planning and testing.
• **Compliance** Comply with regulatory, contractual, and statutory requirements by using technical controls, system audits, and legal awareness.

Security Program Development -ISO/IEC 27000 Series:

- International Organization for Standardization (ISO) and the International Electro technical Commission (IEC) worked together to build on top of what was provided by BS7799 and launch the new version as a global standard, known as the ISO/IEC 27000 series.
  - serves as industry best practices for the management of security controls in a holistic manner within organizations around the world.
  - It is common for organizations to seek an ISO/IEC 27001 certification by an accredited third party.

• **ISO/IEC 27000** Overview and vocabulary
• **ISO/IEC 27001** ISMS requirements
• **ISO/IEC 27002** Code of practice for information security management
• **ISO/IEC 27003** Guideline for ISMS implementation
• **ISO/IEC 27004** Guideline for information security management measurement and metrics framework
• **ISO/IEC 27005** Guideline for information security risk management
• **ISO/IEC 27006** Guidelines for bodies providing audit and certification of information security management systems
• **ISO/IEC 27011** Information security management guidelines for telecommunications organizations
• **ISO/IEC 27031** Guideline for information and communications technology readiness for business continuity
• **ISO/IEC 27033-1** Guideline for network security
• **ISO 27799** Guideline for information security management in health organizations

• **ISO/IEC 27007** Guideline for information security management systems auditing
• **ISO/IEC 27013** Guideline on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001
• **ISO/IEC 27014** Guideline for information security governance
• **ISO/IEC 27015** Information security management guidelines for the finance and insurance sectors
• **ISO/IEC 27032** Guideline for cybersecurity
• **ISO/IEC 27033** Guideline for IT network security, a multipart standard based on ISO/IEC 18028:2006
• **ISO/IEC 27034** Guideline for application security
• **ISO/IEC 27035** Guideline for security incident management
• **ISO/IEC 27036** Guideline for security of outsourcing
• **ISO/IEC 27037** Guideline for identification, collection, and/or acquisition and preservation of digital evidence

Enterprise Security Architecture Development

- **An enterprise security architecture is a subset of an enterprise architecture, which**
  - Define the information security strategy that consists of layers of solutions, processes, and procedures and the way they are linked across an enterprise strategically, tactically, and operationally
  - Describe the structure and behavior of all the components that make up a holistic information security management system (ISMS).
  - Ensure that security efforts align with business practices in a standardized and cost-effective manner.

Enterprise Security Architecture Development

- Sherwood Applied Business Security Architecture (SABSA)

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The business	Business risk model	Business process model	Business organization and relationships	Business geography	Business time dependencies
Conceptual	Business attributes profile	Control objectives	Security strategies and architectural layering	Security entity model and trust framework	Security domain model	Security-related lifetimes and deadlines
Logical	Business information model	Security policies	Security services	Entity schema and privilege profiles	Security domain definitions and associations	Security processing cycle
Physical	Business data model	Security rules, practices, and procedures	Security mechanisms	Users, applications, and user interface	Platform and network infrastructure	Control structure execution
Component	Detailed data structures	Security standards	Security products and tools	Identities, functions, actions, and ACLs	Processes, nodes, addresses, and protocols	Security step timing and sequencing
Operational	Assurance of operation continuity	Operation risk management	Security service management and support	Application and user management and support	Security of sites, networks, and platforms	Security operations schedule

Security Program vs. Enterprise Security Architecture

- The security program specifies the pieces and parts that need to be put into place to provide a holistic security for the organization overall and how to properly take care of those pieces and parts.
- The enterprise security architecture illustrates how these components are to be integrated into the different layers of the current business environment.

As another example, the security program could dictate that data protection needs to be put into place. The architecture can show how this happens at the infrastructure, application, component, and business level.

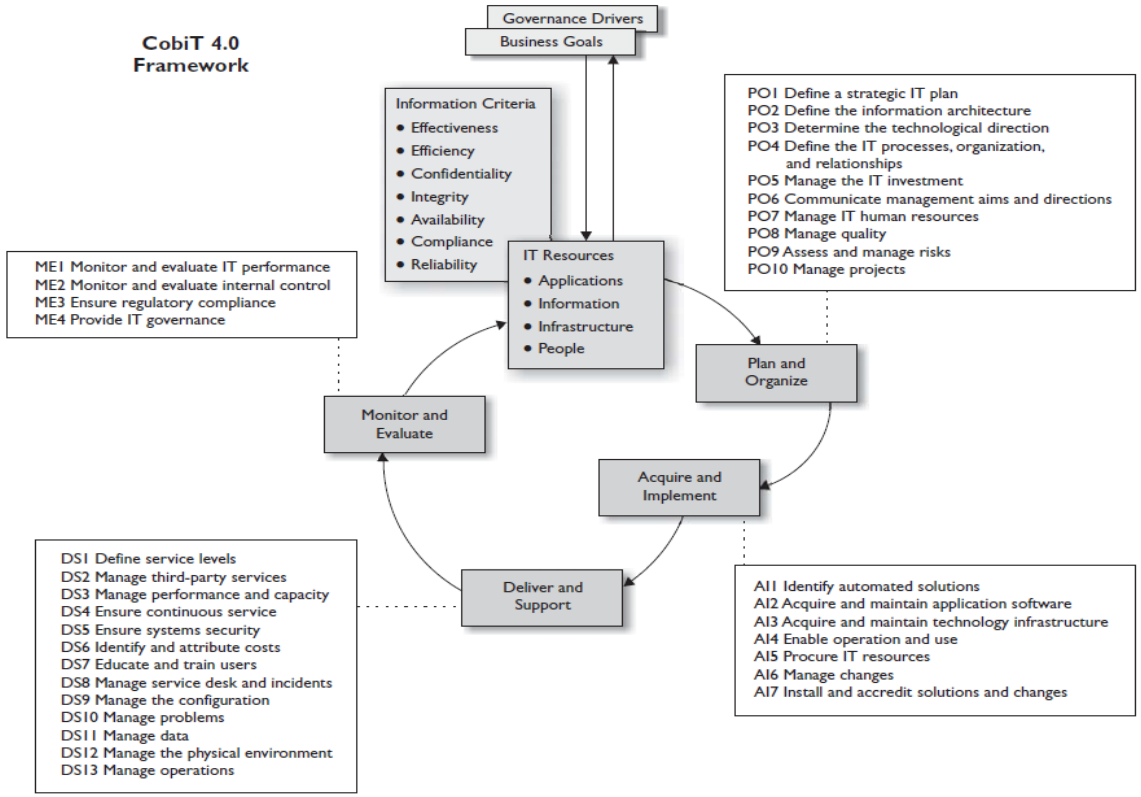
Security Controls Development

- CobiT

Control Objectives for Information and related Technology (CobiT) is a framework which contains set of control objectives developed by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI)

Sample CobiT objectives for user account management control:

- Using unique user IDs to enable users to be linked to and held accountable for their actions
- A procedure to require users to understand and acknowledge their access rights and the conditions of such access



Security Controls Development

- NIST SP 800-55

CobiT contains control objectives used within the private sector; the U.S. government has its own set of requirements. The National Institute of Standards and Technology (NIST) SP 800-53 outlines controls that agencies need to put into place to be compliant with the Federal Information Security Management Act of 2002.

Identifier	Family	Class
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PM	Program Management	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational

Process Management Development

Security controls needs to be used effectively and efficiently by proper process. The security controls can be considered the “things,” and processes are how we use these things.

- ***The Information Technology Infrastructure Library (ITIL)***
  - A set of best practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business.
  - 26 processes are listed in ITIL 2011 edition and described in 5 volumes that are ITIL Service Strategy, ITIL Service Design, ITIL Service Transition, ITIL Service Operation, ITIL Continual Service Improvement.
- ***Six Sigma***
  - A set of techniques and tools (quality management methods, mainly empirical, statistical methods) for process improvement.
  - Six Sigma seeks to improve the quality of process outputs by identifying and removing the causes of defects (errors) and minimizing variability in manufacturing and business processes.

Security Governance Responsibilities and Roles

- Security Steering Committee

A security steering committee is responsible for making decisions on tactical and strategic security issues within the enterprise as a whole. This committee should meet at least quarterly and have a well-defined agenda. Some of the group's responsibilities are as follows:

- Define the acceptable risk level for the organization.
- Develop security objectives and strategies.
- Determine priorities of security initiatives based on business needs.
- Review risk assessment and auditing reports.
- Monitor the business impact of security risks.
- Review major security breaches and incidents.
- Approve any major change to the security policy and program.

The CEO should head security steering committee , and the CFO, CIO, department managers, and Chief Internal Auditor should all be on it.

Security Governance Responsibilities and Roles

- Audit Committee

The audit committee reviews and evaluates the company's internal operations, internal audit system, and the transparency and accuracy of financial reporting so the company's investors, customers, and creditors have continued confidence in the organization. This committee is usually responsible for at least the following items:

- The integrity of the company's financial statements and other financial information provided to stockholders and others
- The company's system of internal controls
- The engagement and performance of the independent auditors
- The performance of the internal audit function
- Compliance with legal requirements, regulations, and company policies regarding ethical conduct

*The audit committee should be appointed by the **Board of Directors***

Security Governance Responsibilities and Roles

- Other Security Related Roles and Responsibilities

Data Owner (information owner): usually a member of management who is in charge of a specific business unit, and who is ultimately responsible for the protection and use of a specific subset of information.

Data Custodian: responsible for maintaining and protecting the data.

System Owner: responsible for one or more systems, each of which may hold and process data owned by different data owners.

Application Owner: usually the business unit managers, are responsible for dictating who can and cannot access their business specific applications.

Security Administrator: responsible for implementing and maintaining specific security net work devices and software in the enterprise.

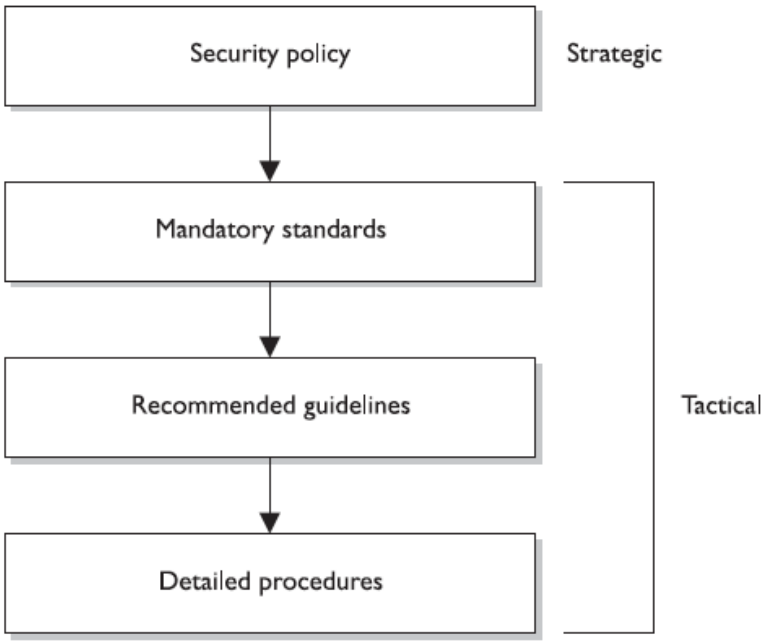
Security Analyst (Consultant): The security analyst role works at a higher, more strategic level than the previously described roles and helps develop policies, standards, and guidelines, as well as set various baselines.

Process Owner: responsible for properly defining, improving upon, and monitoring these processes.

Security Governance Components

For a company's security governance to be successful, it must start at the top level and be useful and functional at every single level within the organization. Accordingly. Information security governance components are defined for different organization levels, which includes:

- Policies
- Standards
- Guidelines
- Procedures
- Baselines

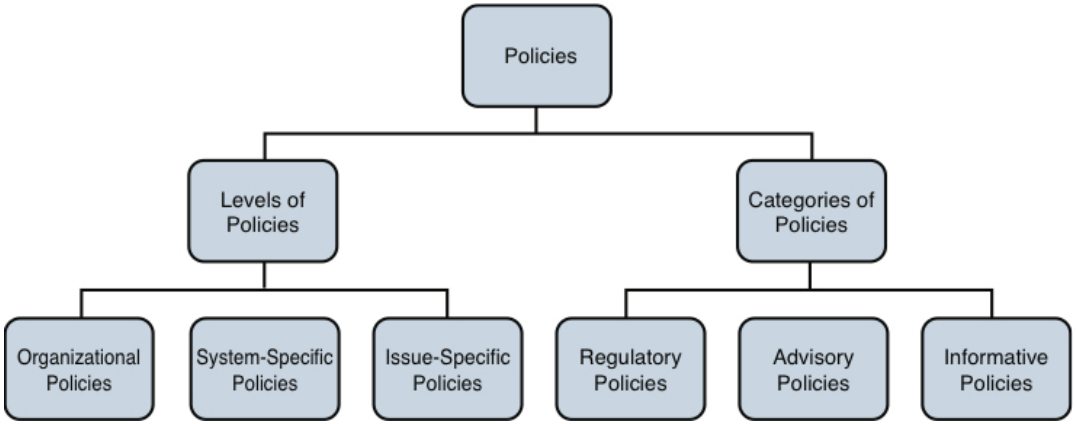


Security Governance Components

- Policies

A ***security policy*** is an overall general statement produced by senior management (or a selected policy board or committee) that dictates what role security plays within the organization. An organization will have many policies, and they should be set up in a hierarchical manner.

- **Organizational Policies** are also referred to as master security policies, which is at the highest level.
- **Issue-specific policies**, also called a functional policy, addresses specific security issues that management feels need more detailed explanation and attention to make sure a comprehensive structure is built and all employees understand how they are to comply with these security issues.
- ***system-specific policy*** presents the management's decisions that are specific to the actual computers, networks, and applications.



Security Governance Components

- Standards & Guidelines

- **Standards** refer to mandatory activities, actions, or rules. Standards can give a policy its support and reinforcement in direction.

An organization may have an issue-specific data classification policy that states "All confidential data must be properly protected." It would need a supporting data protection standard outlining how this protection should be implemented and followed, as in "Confidential information must be protected with AES256 at rest and in transit."

- ***Guidelines*** are recommended actions and operational guides to users, IT staff, operations staff, and others when a specific standard does not apply.

A policy might state that access to confidential data must be audited. A supporting guideline could further explain that audits should contain sufficient information to allow for reconciliation with prior reviews.

Security Governance Components

- Procedures

Procedures are detailed step-by-step tasks that should be performed to achieve a certain goal. The steps can apply to users, IT staff, operations staff, security members, and others who may need to carry out specific tasks.

- Procedures are considered the lowest level in the documentation chain, which spells out how the policy, standards, and guidelines will actually be implemented in an operating environment.

If a policy states that all individuals who access confidential information must be properly authenticated, the supporting procedures will explain the steps for this to happen by defining the access criteria for authorization, how access control mechanisms are implemented and configured, and how access activities are audited.

Security Governance Components

- Baselines

The term ***baseline*** refers to a point in time that is used as a comparison for future changes. Once a baseline is formally reviewed and agreed upon, after which all further comparisons and development are measured against it.

- A baseline results in a consistent reference point.
- Baselines are also used to define the minimum level of protection required.
- Specific baselines can be defined per system type, which indicates the necessary settings and the level of protection being provided.

Information Value Assessment, Classification & Controls

- The actual value of an information is determined by the importance it has to the organization as a whole, which should reflect all identifiable costs that would arise if the asset were actually impaired.

  - *Cost to acquire or develop the asset*
  - Price others are willing to pay for the asset
  - Cost to replace the asset if lost
  - *Liability issues if the asset is compromised*
  - Operational and production activities affected if the asset is unavailable

- Data classification helps ensure data is protected in the most cost-effective manner.

  Common Classification for commercial business:

  - *Confidential*
  - *Private*
  - *Sensitive*
  - *Public*

  Common Classification for military business:

  - *Top secret*
  - *Secret*
  - *Confidential*
  - *Sensitive*
  - *Unclassified*

- Each classification should have separate handling requirements and procedures pertaining to how that data is accessed, used, and destroyed.

  - *Strict and granular access control for all levels of sensitive data and programs*
  - Encryption of data while stored and while in transmission
  - Auditing and monitoring
  - Backup and recovery procedures

Risk Assessment and Analysis

A risk assessment identifies vulnerabilities and threats, assesses the impact of those vulnerabilities and threats, and determines which controls to implement. Risk assessment or analysis has four main goals:

- Identify assets and asset value.
- Identify vulnerabilities and threats.
- Calculate threat probability and business impact.
- Balance threat impact with countermeasure cost.

Risk Assessment and Analysis

- The Value of Information and Assets

The actual value of an asset is determined by the importance it has to the organization as a whole. The value of an asset should reflect all identifiable costs that would arise if the asset were actually impaired. The following issues should be considered when assigning values to assets:

- Cost to acquire or develop the asset
- Cost to maintain and protect the asset
- Value of the asset to owners and users
- Value of the asset to adversaries
- Price others are willing to pay for the asset
- Cost to replace the asset if lost
- Operational and production activities affected if the asset is unavailable
- Liability issues if the asset is compromised
- Usefulness and role of the asset in the organization

Risk Assessment and Analysis

- Identifying Vulnerabilities and Threats

Threat Agent	Can Exploit This Vulnerability	Resulting in This Threat
Malware	Lack of antivirus software	Virus infection
Hacker	Powerful services running on a server	Unauthorized access to confidential information
Users	Misconfigured parameter in the operating system	System malfunction
Fire	Lack of fire extinguishers	Facility and computer damage, and possibly loss of life
Employee	Lack of training or standards enforcement Lack of auditing	Sharing mission-critical information Altering data inputs and outputs from data processing applications
Contractor	Lax access control mechanisms	Stealing trade secrets
Attacker	Poorly written application Lack of stringent firewall settings	Conducting a buffer overflow Conducting a denial-of-service attack
Intruder	Lack of security guard	Breaking windows and stealing computers and devices

Risk Assessment and Analysis

- Quantitative Risk Analysis Approaches

A **Quantitative** risk analysis assign monetary and numeric values to all elements of the risk analysis process. The most commonly used equations used for this purpose are the ***single loss expectancy (SLE)*** and the ***annual loss expectancy (ALE).***

Asset Value × Exposure Factor (EF) = SLE

SLE × Annualized Rate of Occurrence (ARO) = ALE

The ***exposure factor (EF)*** represents the percentage of loss a realized threat could have on a certain asset.

The ***annualized rate of occurrence (ARO)*** is the value that represents the estimated frequency of a specific threat taking place within a 12-month timeframe.

Risk Assessment and Analysis

- Qualitative Risk Analysis Approaches

A **Qualitative** risk analysis does not use calculations. Instead, it is more opinion- and scenario-based and uses a rating system to relay the risk criticality levels.

Likelihood	Consequences				
	Insignificant	Minor	Moderate	Major	Severe
Almost certain	M	H	H	E	E
Likely	M	M	H	H	E
Possible	L	M	M	H	E
Unlikely	L	M	M	M	H
Rare	L	L	M	M	H

Risk Assessment and Analysis

- Qualitative Approaches vs. Quantitative Approaches

Attribute	Quantitative	Qualitative
Requires no calculations		X
Requires more complex calculations	X	
Involves high degree of guesswork		X
Provides general areas and indications of risk		X
Is easier to automate and evaluate	X	
Used in risk management performance tracking	X	
Allows for cost/benefit analysis	X	
Uses independently verifiable and objective metrics	X	
Provides the opinions of the individuals who know the processes best		X
Shows clear-cut losses that can be accrued within one year's time	X	

Risk Assessment and Analysis

- Control Selection

A security control must make good business sense, meaning it is cost-effective (its benefit outweighs its cost). This requires another type of analysis: a cost/benefit analysis. A commonly used cost/benefit calculation for a given safeguard (control) is:

(ALE before implementing safeguard)
– (ALE after implementing safeguard)
– (annual cost of safeguard) = value of safeguard to the company

Cost of Safeguard:

- Design/planning costs
- Implementation costs
- Environment modifications
- Compatibility with other countermeasures
- Maintenance requirements
- Testing requirements
- Repair, replacement, or update costs
- Operating and support costs
- Effects on productivity
- Subscription costs
- Extra man-hours for monitoring and responding to alerts
- Beer for the headaches that this new tool will bring about

Risk Assessment and Analysis

- Total Risk vs. Residual Risk

Total Risk is the risk a company faces if it chooses not to implement any type of safeguard.

Residual risk is the risk left over to deal with after some safeguard is applied.

Total risk – Countermeasures = Residual risk

Risk Assessment and Analysis

- Risk Handling

Once a company knows the amount of total and residual risk it is faced with, it must decide how to handle it. Risk can be dealt with in four basic ways:

- ***Transfer the Risk:*** Many types of insurance are available to companies to protect their assets.
- ***Avoid the Risk:*** Company can decides to terminate the activity that is introducing the risk.
- ***Mitigate the Risk:*** Implement some countermeasure to reduce the risk to a level considered acceptable enough to continue conducting business.
- ***Accept the Risk:*** the company understands the level of risk it is faced with, as well as the potential cost of damage, and decides to just live with it and not implement the countermeasure

Personnel Security

- Hiring & Termination Practices

- Organizations should have personnel security policies in place that include screening, hiring, and termination policies.
- Personnel screening should occur prior to the offer of employment.
- Personnel hiring procedures should include signing all the appropriate documents, including government-required documentation, no expectation of privacy statements, and non-disclosure agreements (**NDAs**).
- Personnel termination must be handled differently based on whether the termination is friendly or unfriendly.
- Some management controls that some organizations use include ***mandatory vacations***, ***Rotation of duties, etc***.

Personnel Security

- Security Training

- Security Awareness training reinforces the fact that valuable resources must be protected by implementing security measures.
  - Security awareness training should be developed based on the audience.
  - Personnel should sign a document that indicates they have completed the training and understand all the topics.
  - Although the initial training should occur when personnel is hired, security awareness training should be considered a continuous process, with future training sessions occurring annually at a minimum.

- Security Training teaches personnel the skills to enable them to perform their jobs in a secure manner.
- Security education is more independent and is targeted at security professionals who require security expertise to act as in-house experts for managing the security programs.