Mississippi State UNIVERSITY

J. A. "Drew" Hamilton, Jr., Ph.D.

Director, Distributed Analytics & Security Institute
Director, Center for Cyber Innovation
Professor, Computer Science & Engineering

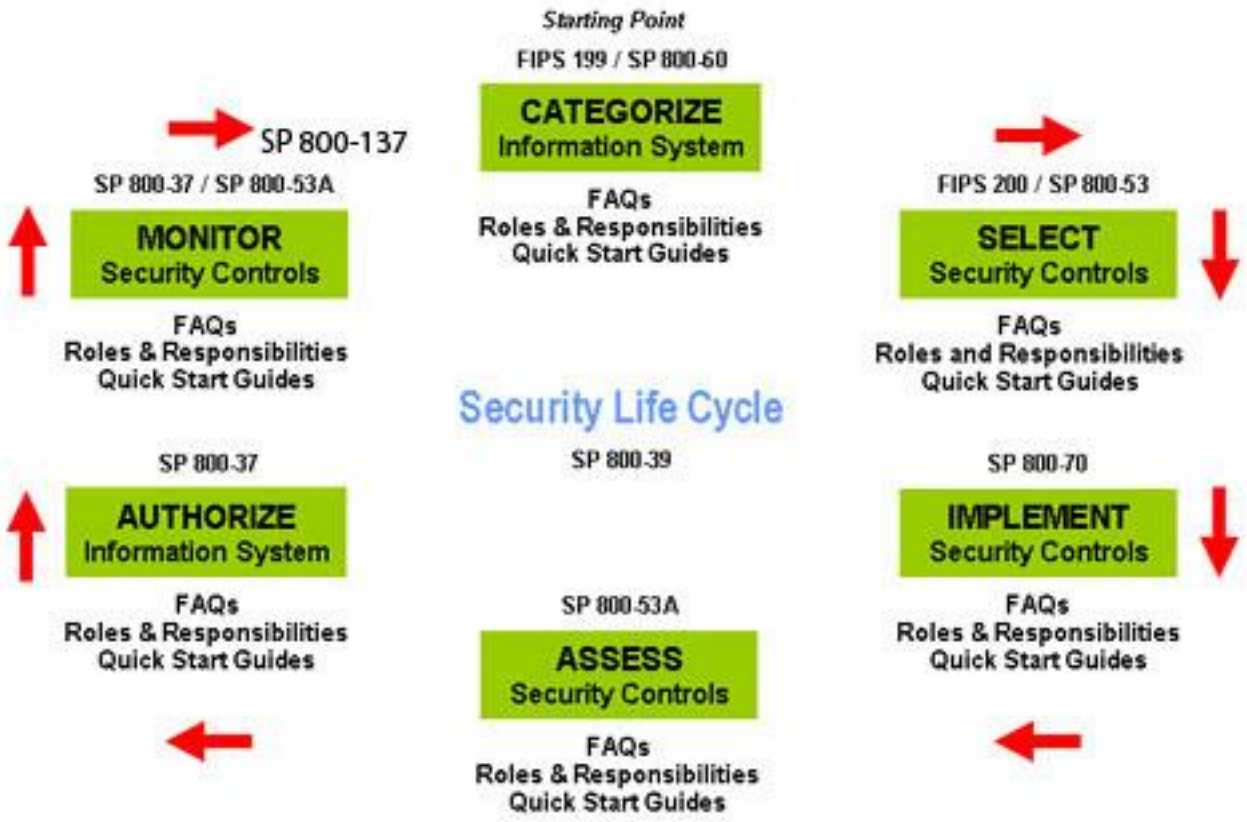
CCI
Post Office Box 9627
Mississippi State, MS 39762

Voice: (662) 325-2294
Fax: (662) 325-7692
hamilton@cci.msstate.edu

Outline 15% (Security, Risk, Compliance, Law, Regulations, and Business Continuity)

- Confidentiality, integrity and availability concepts
- Security governance
- Compliance
- Legal and Regulatory Issues
- Professional Ethics
- Security policies, standards and procedure

NIST Risk Management Framework



Confidentiality, integrity and availability concepts

Dr. Drew Hamilton

Understand and Apply Concepts of Confidentiality, Integrity & Availability

- **Confidentiality: protecting information from unauthorized disclosure;**
- **Integrity: protecting information from unauthorized modifications, and ensure that information is accurate and complete;**
- **Availability: ensuring information is available when needed;**

Virus researchers owe this man a debt of gratitude

(ISC)2 CBK Notes on "CIA"

- **Confidentiality**
  - **Principle of least privilege**
  - **Data Classification**
  - **Controls**
- **Integrity**
  - **Limiting updates**
  - **Verifying changes**
- **Availability**
  - **Denial of service**
  - **Disaster recovery**

1. Not really an equilateral triangle
2. Dependencies exist between confidentiality & integrity
3. Integrity does not get enough attention

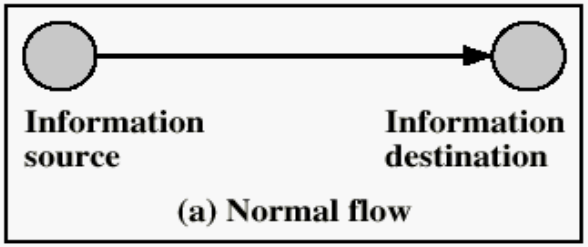
CIA Key Terms

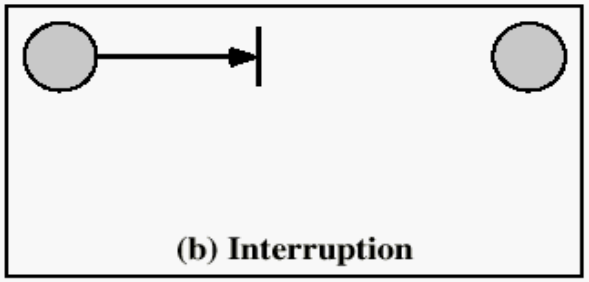
- **Confidentiality**
  - Sensitivity, Discretion, Criticality, Concealment, Secrecy, Privacy, Seclusion, Isolation
- **Integrity**
  - Modifications, Errors, Consistency, Verification, Validation, Accountability, Responsibility, Completeness, Comprehensiveness
- **Availability**
  - Redundancy, Device Failure, Software Errors, Usability, Accessibility, Timeliness

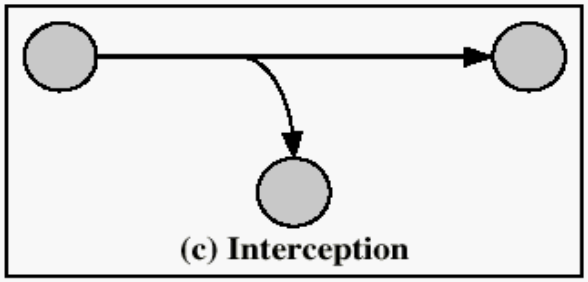
Attacks, Services and Mechanisms

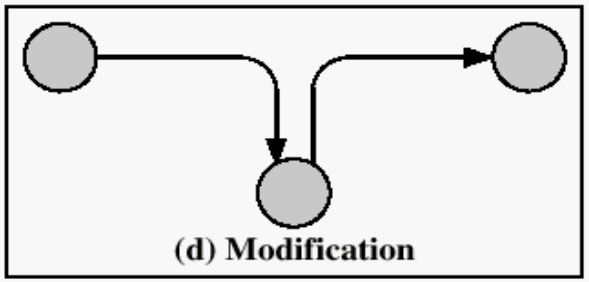
- **Security Attack:** Any action that compromises the security of information.
- **Security Mechanism:** A mechanism that is designed to detect, prevent, or recover from a security attack.
- **Security Service:** A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

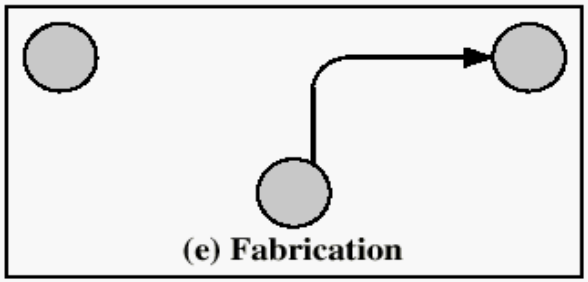
Security Attacks











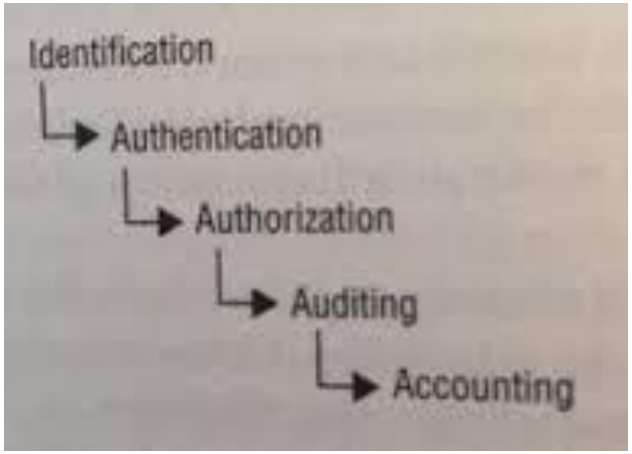
Stallings' Taxonomy

Security Attacks

- **Interruption:** This is an attack on availability
- **Interception:** This is an attack on confidentiality
- **Modification:** This is an attack on integrity
- **Fabrication:** This is an attack on authenticity

Five Elements of AAA Services

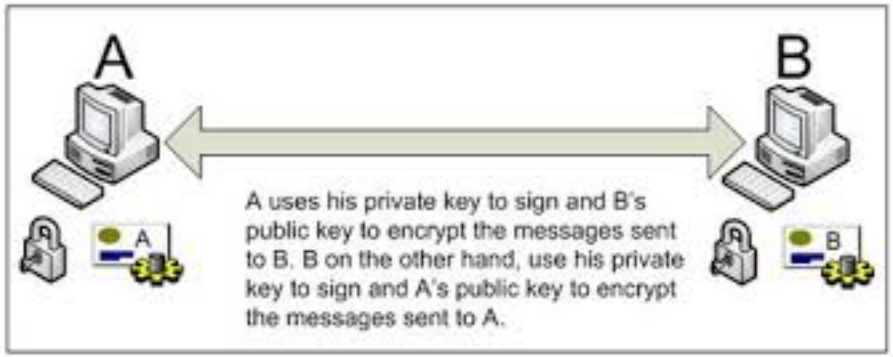
- Identify subject and initiate accountability
- Authenticate the identity of subject
- Authorize access of authenticated subject
- Audit subject's actions to provide accountability
- Accountability ties a subject to their actions



Five Diamond Award

Non-repudiation

- **“The order is final”**
- **Nonrepudiation is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.**



Protection Mechanisms

- **Layering**
  - **Defense in depth**
- **Abstraction**
  - **Abstraction simplifies security by enabling you to assign security controls to a group of objects collected by type or function**
- **Data Hiding**
  - **Hiding subjects of data**
  - **Preventing direct access of hardware**
- **Encryption**
  - **Hiding the meaning of a communication**

Sensitive Data (U.S. Government)

- Unclassified
- Sensitive but Unclassified (SBU)
- FOUO
- Confidential
- Secret
- Top Secret
- Top Secret Compartmented
- So secret that the classification itself is classified
  - Other countries have other designations
    - →secret discreet
    - →NOFORN

Commercial business/private sector classification levels

- **Confidential / Private**
  - **Confidential is company data**
  - **Private is related to individuals**
- **Sensitive**
- **Public**

Security governance

Dr. Drew Hamilton

Master Sergeant Alex Applegate, USAF (ret.)

Shon Harris

Overview

- Administrative Management Responsibilities
- Operations Department Responsibilities
- Configuration Management
- Trusted Recovery States

Information Security Environment

- Organizations must contend with complex laws, regulations, requirements, technology, competitors and partners while pursuing their business objectives.
- Management must take many things into account including moral, labor relations, productivity, cost, etc.
- Must develop an effective security program

- Overarching Organizational Policy
- Management's Security Statement

- Regulations
- Competition
- Organizational Objectives
- Organizational Goals
- Laws
- Shareholders' Interests

Roles and Responsibilities

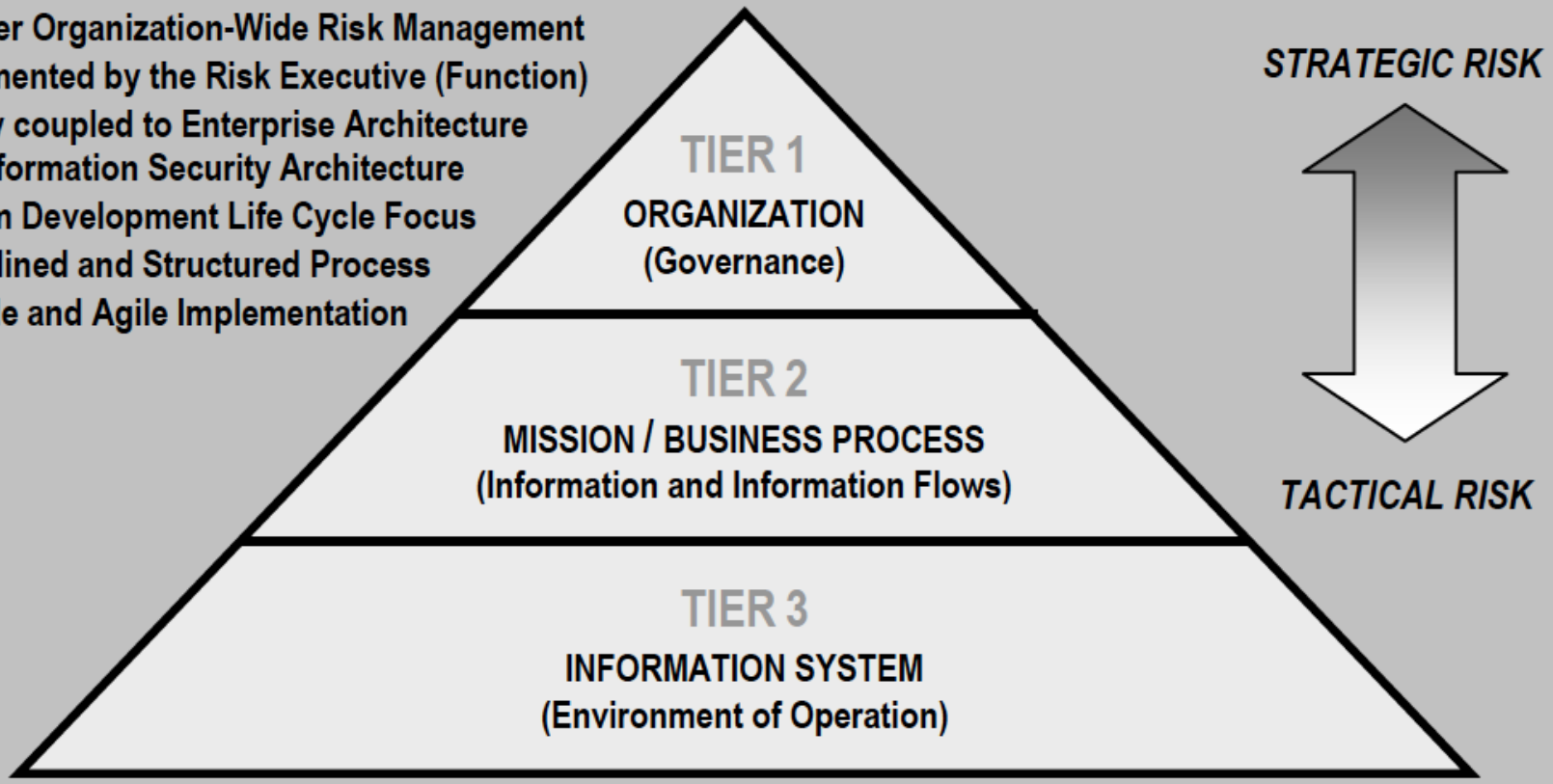
- Specific
  - Delegate certain responsibilities for security to individuals
  - Define acceptable and unacceptable behavior
- General
  - Rules that let everyone know they are responsible for security
- Communicated at hiring
  - Tell new hires the rules and consider annual review
- Verified capabilities and limitations
  - Access to resources defined by job
- Third-party considerations
  - Brief vendors, temps, contract staff on security requirements
- Good practices
  - Keep it simple, relevant, understandable and communicate
- Reinforced via training
  - Annual security training

Organizational Processes

- Acquisitions and mergers
- Divestitures and spinoffs
- Governance Committees

NIST 800-37 Risk Management

- Multitier Organization-Wide Risk Management
- Implemented by the Risk Executive (Function)
- Tightly coupled to Enterprise Architecture and Information Security Architecture
- System Development Life Cycle Focus
- Disciplined and Structured Process
- Flexible and Agile Implementation



NIST Risk Management Framework

	Title	Role	Responsibilities
Executive Responsibilities	Risk Executive (Function)	Overseer	• Define the organization's risk management strategy with respect to the selection of security controls • Promote the use of common controls to more effectively use organizational resources • Promote collaboration and cooperation among organizational entities
	CIO	Leader	• Establish expectations for the security control selection and ongoing monitoring processes to provide a more consistent identification of security controls throughout the organization • Provide resources as needed to support information system owners when selecting security controls • Ensure the organization's risk management strategy is integrated into the enterprise architecture • Participate in the selection and approval of organizational level common security controls • Maintain organizational relationships and connections
Organizational Responsibilities	Senior Information Security Officer/ Information Security Program Office	Coordinator	• Develop organization-wide security control selection guidance consistent with the organization's risk management strategy • Assign responsibility for common controls to individuals or organizations • Establish and maintain a catalog of the organization's common security controls • Review the common security controls periodically and, when necessary, update the common security control selections • Define and disseminate organization-defined parameter values for relevant security controls • Acquire/develop and maintain tools, templates, or checklists to support the security control selection process and the development of system security plans • Develop an organization-wide continuous monitoring strategy • Provide training on selecting security controls and documenting them in the security plan • Lead the organization's process for selecting security controls consistent with the organizational guidance
	Common Control Provider	Selector	• Tailor and supplement the common security controls following organizational guidance • Document the assigned common security controls for the organization in sufficient detail to enable a compliant implementation of the control and maintain the documentation • Disseminate the security documentation associated with the common controls to information system owners that employ the common control in their information system • Define the continuous monitoring strategy for the common controls

NIST Risk Management Framework

System Responsibilities	Title	Role	Responsibilities
	Authorizing Official	Approver	• Review the security plan to determine if the plan is complete, consistent, and satisfies the stated security requirements for the information system • Determine if the security plan correctly identifies the potential risk to organizational operations, assets, individuals, other organizations, and the Nation and recommend changes to the plan if it is insufficient • Approve the selected set of security controls, including all tailoring and supplementation decisions, any use restrictions, and the minimum assurance requirements
	Information Owner/ Steward/Information System Owner	Selector	• Select, tailor, and supplement the security controls following organizational guidance, documenting the decisions in the security plan with appropriate rationale for the decisions • Determine the suitability of common controls for use in the information system • Determine the need for use restrictions in the information system • Determine the assurance measures that meet the NIST SP 800-53 minimum assurance requirements selected for the system • Document the tailored and supplemented set of security controls in the security plan in sufficient detail to enable a compliant implementation of the control • Define the continuous monitoring strategy for the information system • Obtain approval for the tailored and supplemented security controls, common controls, compensating controls, use restrictions, and assurance requirements prior to their implementation • Review the security controls periodically and, when necessary, update the security control selections • Maintain and update the system security plan
	ISSO	Supporter	• Support the information system owner in selecting security controls for the information system • Participate in the selection of the organization's common security controls and in determining their suitability for use in the information system • Review the security controls regarding their adequacy in protecting the information and information system
	Information System Security Engineer	Advisor	• Provide advice in describing the system and its functions, information types, operating environments, and security requirements • Review the adequacy of the security controls and their ability to protect the information system and its information • Assist in tailoring the security controls • Assist in determining the assurance measures that can be used to meet the minimum assurance requirements
	Information Security Architect	Advisor	• Ensure the selection of security controls is consistent with the enterprise architecture, including reference models and segment and solution architectures
	User	Advisor	• Identify mission, business, or operational security requirements • Report any weaknesses in, or new requirements for, current system operations
	Security Control Assessor/Assessment Team	Assessor	• Not involved in selecting security controls

Who is an ISSO?

- ISSO – Information Systems Security Officer
- Reports to the Chief Information Officer (CIO), who reports to the CEO.
- Leader of the Information Security (InfoSec) organization.
- Qualifications
  - Manage and organize people
  - Communicate to upper management without much technical details
  - Have enough technical expertise to understand systems and make decisions

ISSO Reporting Models

- **Report as high in the organization as possible**
  - **Business relationships**
  - **Reporting to the CEO**
  - **Reporting to the IT Department**
  - **Reporting to Corporate Security**
  - **Reporting to the Administrative Services Department**
  - **Reporting to the Insurance and Risk Management Dept.**
  - **Reporting to the Internal Audit Department**
  - **Reporting to the Legal Department**

Administrative Management Responsibilities

- The objective of separation of duties is to ensure that one person acting alone cannot compromise the company's security in any way
- Separation of duties also helps prevent mistakes and minimize conflicts of interest that may take place if one person is performing a task from beginning to end.

Administrative Management Responsibilities

Roles and Associated Responsibilities

- **Control Group – Obtains and validates information obtained from analysts, administrators, and users and passes it to various user groups**
- **Systems Analyst – Designs data flow of systems based on operational and user requirements**
- **Application Programmer – Develops and maintains production software**
- **Help Desk – Resolves end-user and system technical or operations problems**
- **IT Engineer – Performs the day-to-day operational duties on systems and applications**
- **Database Administrator – Creates new database tables and manages the database**
- **Network Administrator – Installs and maintains the LAN/WAN environment**
- **Security Administrator – Defines, configures, and maintains the security mechanisms protecting the organization**
- **Tape Librarian – Receives, records, releases, and protects system and application files backed up on media such as tapes or disks**
- **Quality Assurance – Can consist of both Quality Assurance (QA) and Quality Control (QC). QA ensures that activities meet the prescribed standards regarding supporting documentation and nomenclature. QC ensures that the activities, services, equipment, and personnel operate within the accepted standards.**

Administrative Management Responsibilities

- **Job rotation means that, over time, more than one person fulfills the tasks of one position within the company**
- **Least privilege means an individual should have just enough permissions and rights to fulfill his role in the company and no more**
- **Mandatory vacations are used to force individuals to leave the office for some period of time in order to allow for the identification of fraudulent activity and to facilitate job rotation**

Administrative Management Responsibilities

- **Security administrators should not report to the network administrator**
- **Security administrators should be responsible for:**
  - **Security devices and software**
  - **Performing security assessments**
  - **Establishing user profiles and mandatory access controls**
  - **Security labels in mandatory access control environments**
  - **Setting initial passwords for users**
  - **Reviewing audit logs**

Administrative Management Responsibilities

- **Important questions to ask as a security administrator**
  - **Are users accessing information and performing tasks that are not necessary for their job description?**
  - **Are repetitive mistakes being made?**
  - **Do too many users have rights and privileges to sensitive or restricted data or resources?**

Administrative Management Responsibilities

- **Clipping level – a predefined threshold (or set of thresholds) for the number of certain types of errors that will be allowed before an activity is considered suspicious**
- **The goal using of clipping levels, auditing, and monitoring is to discover problems before major damage occurs and, at times, to be alerted if a possible attack is underway within the network**

Administrative Management Responsibilities

- **Highlighted Note: The security controls and mechanisms that are in place must have a degree of transparency. This enables the user to perform tasks and duties without having to go through extra steps because of the presence of the security controls. Transparency also does not let the user know too much about the controls, which helps prevent him from figuring out how to circumvent them. If the controls are too obvious, an attacker can figure out how to compromise them more easily.**

Administrative Management Responsibilities

- **Operational Assurance concentrates on the product's architecture, embedded features, and functionality that enable a customer to continually obtain the necessary level of protection when using the product.**
- **Life-Cycle Assurance pertains to how the product was developed and maintained with regard to the standards and expectations associated with each stage of the life cycle such that it can be deemed a highly trusted product.**

Event Management

- **Highlighted Note: Event management means that a product is being used to collect various logs throughout the network. The product identifies patterns and potentially malicious activities that a human would most likely miss because of the amount of data in the various logs.**

Operations Department Responsibilities

- Unusual or unexplained occurrences
- Deviations from standards
- Unscheduled initial program loads (reboots)
- Asset identification and management
- System controls

Operations Department Responsibilities

- **Initial program load (IPL) is a mainframe term for loading the operating system's kernel into main memory**
- **Asset management encompasses knowing everything – hardware, firmware, operating system, language runtime environments, applications, and individual libraries – for the overall environment**

Trusted Recovery States

- An operating system's response to a type of failure can defined as one of the following:
  - System reboot: the system shuts itself down in a controlled manner in response to a kernel failure
  - Emergency system restart: system failure happens in an uncontrolled manner
  - System cold start: an unexpected kernel or media failure happens and the regular recovery procedure cannot recover the system to a more consistant state
- It is important to ensure that the system does not enter an insecure state when it is affected by any of these types of problems, and that it shuts down and recovers properly to a secure and stable state

Trusted Recovery States

- **After a system crash:**
  1. **Enter into single-user or safe mode**
  2. **Fix issue and recover files**
  3. **Validate critical files and operations**
- **Security Concerns**
  - **Bootup sequence should not be available to reconfigure**
  - **Writing actions to system logs should not be able to be bypassed**
  - **System forced shutdowns should not be allowed**
  - **Output should not be able to be rerouted**

Trusted Recovery States

- **Input and Output Controls**
  - **Online transactions must be recorded and timestamped**
  - **Data entered into a system should be in the correct format and validated to ensure such data are not malicious**
  - **Ensure output reaches the proper destinations securely**
    - **A signed receipt should always be required before releasing sensitive output**
    - **A heading and trailing banner should indicate who the intended receiver is**
    - **Once the output is created, it must have the proper access controls implemented**
    - **If a report has no information, it should contain the phrase "no output"**

Trusted Recovery States

- **System Hardening**
  - **Wiring closets should be locked**
  - **Network switches and hubs, when it is not practical to place them in locked wiring closets, should be inside locked cabinets**
  - **Network ports in public places should be made physically inaccessible**
- **<u>Highlighted note:</u> Locked down systems are referred to as bastion hosts**

Trusted Recovery States

- Companies have an ethical responsibility to use only legitimately purchased software
- Applications for which no valid business need can be found should be removed
- Companies should have an acceptable use policy, which indicates what software users can install and informs users that the environment will be surveyed from time to time to verify compliance

Trusted Recovery States

- **Remote Administration**
  - **Commands and data should not take place in cleartext**
  - **Truly critical systems should be administered locally instead of remotely**
  - **Only a small number of administrators should be in place for any administration activities**
  - **Strong authentication should be in place for any administration activities**

Configuration Management

Change control process

1. **Request for a change to take place**
2. **Approval of the change**
3. **Documentation of the change**
4. **Testing and presentation**
5. **Implementation**
6. **Report the change to management**

It is critical that the operations department create approved backout plans before implementing changes to systems or the network

Configuration Management

- **Numerous changes can take place in a company:**
  - **New computers installed**
  - **New applications installed**
  - **Different configurations implemented**
  - **Patches and updates installed**
  - **New technologies integrated**
  - **Policies, procedures, and standards updated**
  - **New regulations and requirements implemented**
  - **Network or system problems identified and fixes implemented**
  - **Different network configuration implemented**
  - **New networking devices integrated into the network**
  - **Company can be acquired by, or merged with, another company**

Data Deletion

- **Sanitized: media is erased/cleared of content**
  - **Zeroization: Overwriting with a pattern**
  - **Degaussing: magnetic scrambling**
  - **Destruction: shredding, crushing, burning**
- **Purging: making information unrecoverable even with extraordinary effort such as a forensics laboratory**
- **Data remanence: the residual physical representation of information that was saved and then erased**

Media Management

- **Media Management attributes**
  - **Tracking (audit logging)**
  - **Effectively implemented access controls**
    - **Physical**
    - **Technical**
    - **Administrative**
  - **Tracking the number and location of backup versions**
  - **Documented history of changes to media**
  - **Ensures environmental conditions do not endanger media**
  - **Ensures media integrity**
  - **Inventories the media on a scheduled basis**
  - **Carries out secure disposal activities**
  - **Internal and external labeling**

Mainframes

- **Mainframes**
  - **Still in use**
  - **Designed from the standpoint of massive I/O**
  - **Not maintenance intensive**
  - **Usually perform batch processing rather than interactive**
  - **Can be configured to load into a different type of system at IPL**
  - **May include supercomputers**

Contingency Planning and Business Continuity Planning

- **Know the difference between Contingency Planning and Business Continuity Planning**
  - **BCP addresses how to keep the organization in business after a disaster takes place**
  - **Contingency plans address how to deal with small incidents that do not qualify as disasters, as in power surges, server failures, a down communication link to the Internet, or the corruption of software**

ISC2 continuum of controls relative to the timeline of a security incident

- **Directive**
  - Controls designed to specify acceptable rules of behavior within an organization
- **Deterrent**
  - Controls designed to discourage people from violating security
- **Preventive**
  - Controls implemented to prevent a security incident or information breach
- **Compensating**
  - Controls implemented to substitute for the loss of primary controls and mitigate risk down to an acceptable level
- **Detective**
  - Controls designed to signal a warning when a security control has been breached
- **Corrective**
  - Controls implemented to remedy circumstance, mitigate damage, or restore controls
- **Recovery**
  - Controls implemented to restore conditions to normal after a security incident

IA Controls (Enclosure 4, DoDI 8500.2)

- **IA Control Subject Area. One of eight groups indicating the major subject or focus area to which an individual IA Control is assigned. (Next Slide)**
- **IA Control Number. A unique identifier comprised of four letters, a dash, and a number. The first two letters are an abbreviation for the subject area name and the second two letters are an abbreviation for the individual IA Control name. The number represents a level of robustness in ascending order that is relative to each IA Control. (Next Slide)**
- **IA Control Name. A brief title phrase that describes the individual IA Control.**
- **IA Control Text. One or more sentences that describe the IA condition or state that the IA Control is intended to achieve.**

IA Control Subject Area: Enclave and Computing Environment.

IA Control Number: ECCT-1.

IA Control Name: Encryption for Confidentiality (Data in Transit).

IA Control Text: Unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using NIST-certified cryptography.

Another IA Control Example

IA Service: Availability **Control Subject Area:** Continuity
Control Number: CODB **Control Name:** Data Backup Procedures

CODB-1 Data backup is performed at least weekly.

CODB-2 Data backup is performed daily, and recovery media are stored off-site at a location that affords protection of the data in accordance with its mission assurance category and confidentiality level.

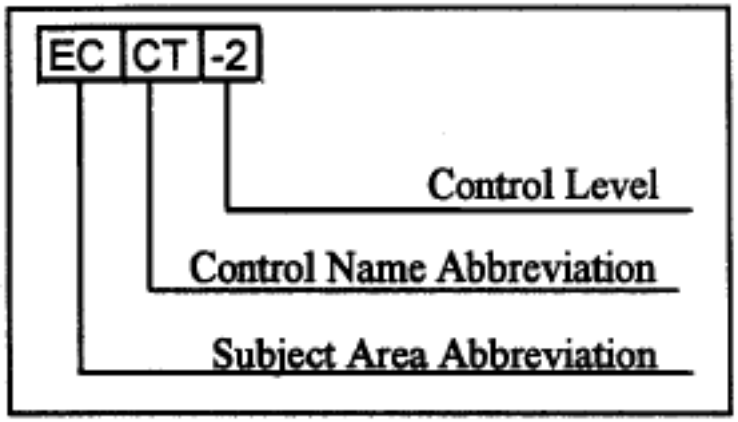
CODB-3 Data backup is accomplished by maintaining a redundant secondary system, not collocated, that can be activated without loss of data or disruption to the operation.

IA Control Subject Areas

Enclosure 4, DoDI 8500.2

Abbreviation	Subject Area Name	Number of Controls in Subject Area
DC	Security Design & Configuration	31
IA	Identification and Authentication	9
EC	Enclave and Computing Environment	48
EB	Enclave Boundary Defense	8
PE	Physical and Environmental	27
PR	Personnel	7
CO	Continuity	24
VI	Vulnerability and Incident Management	3

- **In the example to the right --> the control level is two (2), which means there is a related IA Control, ECCT-1, that provides less robustness. There may also be an IA Control, ECCT-3, that provides greater robustness.**



Mission Assurance Category Summary DoDI 8500.2 Enclosure 3

- **The baseline sets of IA controls are pre-defined based on the determination of the Mission Assurance Category (MAC) and Confidentiality Levels as specified in the formal requirements documentation or by the info owner.**
- **IA Controls addressing availability, confidentiality, integrity, authentication and non-repudiation requirements are keyed to the system's MAC based on the importance of the information to the mission, particularly the warfighters' combat mission, and on the sensitivity or classification of the information.**

MISSION ASSURANCE CATEGORY			
	DEFINITION	Integrity	Availability
1	These systems handle information that is determined to be **vital to the operational readiness or mission effectiveness of deployed and contingency forces** in terms of both content and timeliness.	HIGH	HIGH
2	These systems **handle information that is important to the support of deployed and contingency forces** .	HIGH	MEDIUM
3	These systems handle information that is necessary for the conduct of day-to-day business, but **does not materially affect support to deployed or contingency forces in the short-term** .	BASIC	BASIC

Mission Assurance Category Levels for IA Controls

CONFIDENTIALITY LEVEL	DEFINITION
Classified	Systems processing classified information
Sensitive	Systems processing sensitive information as defined in DoDD 8500.1, to include any unclassified information not cleared for public release
Public	Systems processing publicly releasable information as defined in DoDD 8500.1 (i.e., information that has undergone a security review and been cleared for public release)

- **IA Controls addressing confidentiality requirements are based on the sensitivity or classification of the information. There are three MAC levels and three confidentiality levels with each level representing increasingly stringent information assurance requirements.**

Determining Baseline IA Controls

Combination	Mission Assurance Category	Confidentiality Level	DoDI 8500.2 Enclosure 4 Attachments
1	MAC 1	Classified	1 and 4
2	MAC 1	Sensitive	1 and 5
3	MAC 1	Public	1 and 6
4	MAC 2	Classified	2 and 4
5	MAC 2	Sensitive	2 and 5
6	MAC 2	Public	2 and 6
7	MAC 3	Classified	3 and 4
8	MAC 3	Sensitive	3 and 5
9	MAC 3	Public	3 and 6

NIST SP 800-53r4

TABLE D-1: SECURITY CONTROL PRIORITIZATION CODES

Priority Code	Sequencing	Action
Priority Code 1 **(P1)**	FIRST	Implement P1 security controls first.
Priority Code 2 **(P2)**	NEXT	Implement P2 security controls after implementation of P1 controls.
Priority Code 3 **(P3)**	LAST	Implement P3 security controls after implementation of P1 and P2 controls.
Unspecified Priority Code **(P0)**	NONE	Security control not selected in any baseline.

TABLE D-8: SUMMARY — CONTINGENCY PLANNING CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CP-1	**Contingency Planning Policy and Procedures**		X	X	X	X
CP-2	**Contingency Plan**			X	X	X
CP-2(1)	*CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*				X	X
CP-2(2)	*CONTINGENCY PLAN | CAPACITY PLANNING*					X

NIST SP 800-53r4

TABLE D-2: SECURITY CONTROL BASELINES[92]

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P3	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	**Withdrawn**	—	—	—	—
AC-14	Permitted Actions without Identification or Authentication	P3	AC-14	AC-14	AC-14
AC-15	**Withdrawn**	—	—	—	—

Summary

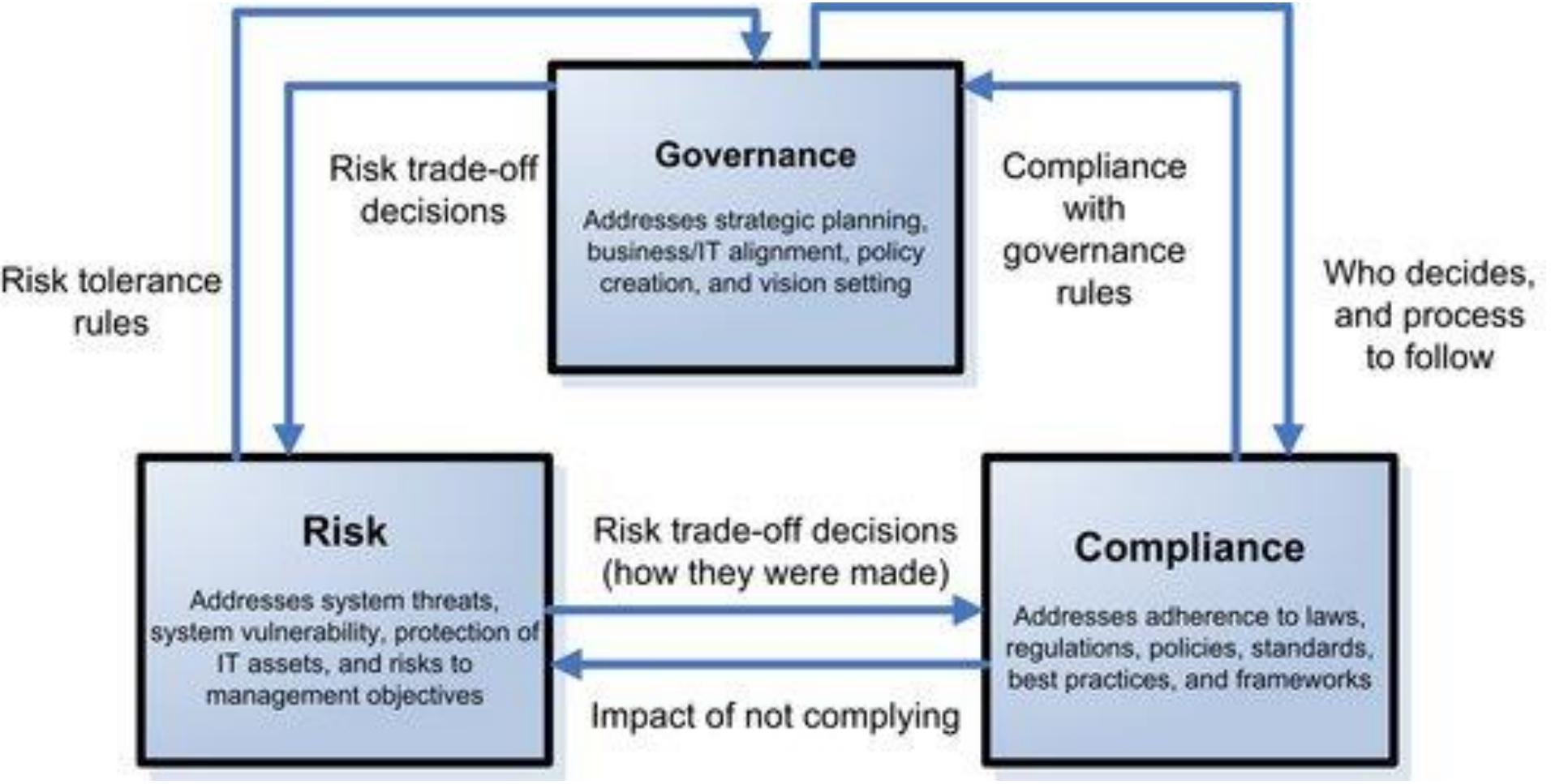
- Administrative Management Responsibilities
- Operations Department Responsibilities
- Configuration Management
- Trusted Recovery States

Compliance

Compliance

Dr. Drew Hamilton

GRC Overview



Verify Compliance

- ***Verify Compliance***
  - **Laws Related to Information Assurance(IA) and Security**
  - **Policy Direction**
  - **Security Requirements**

Verify Compliance Continued

- ***Laws related to information assurance(IA) and Security***
  - **Copyright Protection and Licensing**
  - **Criminal Prosecution**
  - **Due Diligence**
  - **Evidence Collection and Preservation**
  - **Fraud, Waste, and Abuse**
  - **Laws related to information assurance (IA) and Security**
  - **Legal and Liability Issues**
  - **Ethics**

Verify Compliance Continued

- ***Policy Direction***
  - **Access Control Policies**
  - **Administrative Security Policies And Procedures**
  - **Audit trails and Logging Policies**
  - **Documentation Policies**
  - **Evidence Collection and Preservation Policies**

Verify Compliance Continued

- ***Security Requirements***
  - **Access Authorization**
  - **Auditable Events**
  - **Authentication**
  - **Background Investigations**
  - **Countermeasures**
  - **Delegation of Authority**
  - **Education, Training, and awareness**
  - **Electronic Records Management**
  - **Electronic-Mail Security**

Verify Compliance Continued

- Information Classification
- Investigative Authorities
- Key Management Infrastructure
- Information Marking (see domain 2)
- Non-Repudiation
- Public key Infrastructure(PKI)

Copyright Protection and Licensing

- **Copyright Protection**
- **Copyright Protection gives the author of an original work exclusive right for a certain time period in relation to that work, including its publication, distribution and adaptation, after which time the work is said to enter the public domain.**
- **It also allows the creator to derive a benefit from their creation.**

Copyright Protection and Licensing

- **Public works include:**
  - Non-copyrightable items(ideas, facts, schedules, names, etc..)
  - Copyrightable items whose copyrights have expired
  - Copyrightable works put in public domain by the author
- **Duration of copyrights:**
  - Depends on country
  - In U.S.(before 1978, 75 years from date of issue, after 1978 lifetime of author plus 50 years)
  - Patents – protection of inventions and discoveries

Copyright Protection and Licensing

- **Licensing**
- **A license is "an authorization (by the licensor) to use the licensed material (by the licensee).“**
- **Licensing laws required proper licensing purchases balanced with number of machinery it is use on.**

Criminal Prosecution

- **Importance of Criminal Prosecution**

- **Criminal prosecution is the institution and conduct of legal proceedings against a defendant for criminal behavior.**

- **Criminal Prosecution Policy To prosecute individuals who violate law by the misuse or theft of information, assets, or resources from the organization's information system.**

Due Diligence

- **Importance of Due Diligence**
- **The demonstration that the organization is diligent in ensuring that the implemented standards continue to provide the required level of protection**
- **Due diligence is exercised and an organization uses reasonable but not necessarily exhaustive efforts to secure the information they have stewardship over.**
- **It is illustrated by the process advisors use to determine investment recommendations to clients.**

Evidence Collection and Preservation

- Importance of Evidence Collection and Preservation
- Evidence Collection techniques vary by the evidence type and location. The main purpose of evidence collection is to retrieve the evidence "as-is" and without damaging the evidence. To test the hypothesis.
- In the ordinary course of business an organization is not required to save all documents and data within the company. However, once the duty to preserve has been triggered, information must be preserved and must be collected in a manner that is useful and compliant with the Federal Rules.

Legal and regulatory issues

Compliance

Dr. Drew Hamilton

Fraud, Waste, and Abuse

- **Fraud**
  - Fraud is understood to mean a dishonest and deliberate course of action which results in the obtaining of money, property or an advantage to which the recipient would not normally be entitled. This would include, inter alia, theft of government property, or the submission of artificially inflated invoices by a contractor.
- **Waste**
  - Waste entails the expenditure or allocation of resources significantly in excess of need. Waste need not necessarily involve an element of private use nor of personal gain, but invariably signifies poor management.
- **Abuse**
  - Abuse, defined here as a subset of waste, entails the exploitation of "loopholes" to the limits of the law, primarily for personal advantage.

Laws and Mandates

- Congressional IT Security Mandates
- There are five principal pieces of computer security legislation that provide direct mandates of Congressional intent for system security. These laws were enacted in response to developing threats to U.S. information systems, and are a framework to guide security activities by DoD and other Federal Government information assurance professionals.
- The five acts are:
  1. Computer Fraud and Abuse Act
  2. Computer Security Act of 1987
  3. Information Technology Management Reform Act of 1996
  4. Government Information Security Reform Act
  5. Federal Information Security Management Act
- We'll learn the details about each one.

Computer Fraud and Abuse Act Public Law 99-474, 1986

- The Computer Fraud and Abuse Act was first signed as Public Law 98-473 in 1984, but was enhanced and strengthened in 1986 and issued as Public Law 99-474. This act was the first piece of legislation focused on computer crime and has been used to successfully prosecute persons with unauthorized possession of user IDs and passwords from government systems.
- The Computer Fraud and Abuse Act:
- Prohibits intentional, unauthorized or fraudulent access to government systems and certain financial systems (i.e., financial institutions with federally-insured deposits or credits)
- Protects computers used in interstate or foreign commerce or communication
- Crime is committed when unauthorized personnel accesses a system to acquire national defense information, obtain financial information, deny the use of a computer, effect a fraud, or traffic in stolen passwords

Computer Security Act of 1987
Public Law 100-235, 1987

- The Computer Security Act of 1987 mandates a computer security program at all federal agencies. This act assigned numerous responsibilities to NIST, including developing guidelines for mandatory periodic personnel training in computer security awareness and accepted computer security practice.
- The Computer Security Act of 1987:
- Is designed to improve the security and privacy of sensitive information in Federal systems.
- Identifies NIST as the national agency responsible for assessing the vulnerability of federal computer systems, developing standards, and providing technical assistance and training.
- Identifies NSA as a support agency for NIST.
- Mandates that federal agencies establish standards and guidelines for cost-effective security and privacy of systems.
- Requires any federal system that processes sensitive information to have a customized security plan.

Information Technology Management Reform Act of 1996
Title 18 U.S. Code, 1452, 1996

- When combined with the Federal Acquisition Reform Act of 1996, the Information Technology Management Reform Act is commonly referred to as the Clinger-Cohen Act.
- The Clinger-Cohen Act:
- Defined a national security system in public law as any telecommunication or information system operated by the U.S. which is critical to the direct fulfillment of military or intelligence missions or which involves intelligence agencies, cryptologic activities related to national security, command and control of military forces, or equipment that is an integral part of a weapon or weapon system.
- Intended to streamline IT acquisition and emphasize life cycle management of IT.
- Links security to federal agency capital planning and budget processes.

Information Technology Management Reform Act of 1996
Title 18 U.S. Code, 1452, 1996

- Requires each agency to establish the position of Chief Information Officer (CIO).
- Key information technology acquisition actions were to give IT procurement authority back to federal agencies, encourage incremental acquisition of IT systems, and encourage acquisition of commercial off-the-shelf products.
- Key IT management actions were to implement an IT management process for maximizing value and managing risks of acquisitions; establish goals for improving the efficiency of agency operations; and ensure adequate information security policies, procedures, and practices.

Government Information Security Reform Act (GISRA) Included in Public Law 106-398, 2000

- The Government Information Security Reform Act (GISRA)created the same management framework for both unclassified and national security systems. However, at the policy level, guidance for these two types of systems remained separate.
- GISRA:
- Addressed program management and evaluation aspects of information security.
- Required annual agency program reviews and annual inspector general evaluations.
- Required agency to report results of evaluations and audits to the Office of Management and Budget (OMB).
- Mandated an annual OMB report to Congress summarizing materials received from agencies.
- The GISRA expired in Nov. 2002; however, GISRA requirements were extended and updated by the Federal Information Security Management Act (FISMA) of 2002.

Federal Information Security Management Act of 2002 (FISMA)
Title III of the E-Government Act of 2002, 2002

- The President, when signing the Federal Information Security Management Act (FISMA) stated that the Executive Branch should implement the act in a manner that preserves the authority of the Secretary of Defense, the Director of Central Intelligence, and other agency heads with regard to the operation, control, and management of national security systems.
- FISMA:
- Streamlined GISRA's provisions and gave Congress permanent oversight of agency security matters
- Expanded the information that agencies must submit to Congress, including plans for fixing security problems
- Required that agencies utilize information security best practices
- Required agencies to identify risk levels associated with their systems and implement the appropriate level of protections accordingly
- Strengthened the role played by the National Institute of Standards and Technology (NIST) in developing and maintaining standards and guidelines for minimum information security controls

MORE Laws

- **In addition to the five primary pieces of legislation that were just presented, there are five acts that have an immediate impact on providing information system security.**

These are:

  - **Fair Credit Reporting Act**
  - **Privacy Act**
  - **Copyright Act**
  - **Electronic Communications Privacy Act**
  - **Digital Millennium Copyright Act**

Fair Credit Reporting Act
Public Law 91-508, 1970

- The Fair Credit Reporting Act assures individuals access to personal information stored on computer systems and was enacted in response to complaints that citizens were being denied credit due to incorrect information in their credit histories.
- The Fair Credit Reporting Act:
- Places restrictions on agencies and services that hold financial information on citizens
- Gives individuals rights to have inaccurate financial information corrected.
- Specifies process for consumers to obtain credit reports and to challenge information.

Privacy Act
Public Law 93-579, 1974

- The Privacy Act includes several provisions that affect IT security. IT security professionals must ensure that personal data is protected and that physical security, management practices, and computer network controls are as specified for information systems containing information covered under the act.
- U.S. Government must safeguard personal data processed by federal agency computer systems.
- Individuals must be able to find out what personal information is being recorded and to correct inaccurate information.

Copyright Act
Title 18 U.S. Code, 2319, 1980

- The Copyright Act was amended in 1980 to explicitly include computer programs. This act allows for large civil and criminal penalties for copyright infringement.
- Section 506A has a criminal penalty at $250,000 and up to 5 years in prison for more than 10 copies of a single program, or a total retail value over $2500 for all copies.
- Section 504C lists civil penalty at $100,000 per product infringement.

Electronic Communications Privacy Act Public Law 99-508, 1986

- The Electronic Communications Privacy Act updated the federal privacy clause in the Omnibus Crime Control and Safe Streets Act of 1968. The act made it legal to intercept electronic communications readily accessible to the general public and provided for civil damages for illegal interception.
- The Electronic Communications Privacy Act:
- Made unlawful access or divulgence of data illegal, to include data intercepted or retrieved from electronically stored communications, communication servers, and remote computing devices and services.
- Prohibited the communication service providers from divulging contents of communications stored, carried, or maintained by that service.

Digital Millennium Copyright Act Public Law 105-304, 1998

- The Digital Millennium Copyright Act was designed to implement the treaties signed in 1996 at the World Intellectual Property Organization Geneva Conference. The act, which addresses many perceived threats to digital copyrighted material and intellectual property, is supported by the software and entertainment industries.
- The act includes provisions that make it a crime to circumvent anti-piracy measures built into most commercial software and outlaws the manufacture, sale, or distribution of code-cracking devices used to illegally copy software.

Digital Millennium Copyright Act Public Law 105-304, 1998

- **The Digital Millennium Copyright Act:**
  - **Gives Internet Service Providers the responsibility for removing material from users' websites that constitutes copyright infringement.**
  - **Requires webcasters to pay licensing fees to record companies.**
  - **Includes exemptions for cracking of copyright protection devices to conduct encryption research, assess product interoperability, and test computer security systems.**
  - **Provides exemptions from anti-circumvention provisions for non-profit libraries, archives, and educational institutions under certain circumstances.**
  - **States explicitly that nothing should affect the rights, remedies, limitations, or defenses to copyright infringement, including fair use.**

Federal Statutes

- There are five additional statutes affecting information technology security. These are:
  - Freedom of Information Act (FOIA)
  - Child Pornography Prevention Act of 1996
  - Electronic Funds Transfer Act
  - Federal Managers Financial Integrity Act
  - Economic Espionage Act of 1996
- Familiarize yourself with these laws and the requirements they impose on information systems security.

Freedom of Information Act (FOIA)

- **Any person has the right to request access to federal agency records or information.**
- **All U.S. Government agencies are required to disclose records (except those protected by exemptions) upon receiving a written request for them.**

Child Pornography Prevention Act of 1996

- Prohibits the transmission of child pornography.
- Makes it a crime to create, produce, depict, collect, or sell child pornography using a computer, and mandates reporting to law enforcement if discovered.
- Prohibits the use of computer technology to depict child pornography.
- Identifies penalties for failure to report discovery

Electronic Funds Transfer Act

- Makes it a crime to fraudulently obtain and use electronic funds for interstate or foreign commerce. Electronic funds have the same protections as paper currency.
- Prohibits the use, transfer, or sale of debit instruments that have been stolen, counterfeited, altered, lost, or fraudulently obtained in interstate or foreign commerce.

Electronic Funds Transfer Act

- **Holds federal entities accountable to Congress for financial expenditures.**
- **Requires federal entities to disclose financial expenditures to Congress, including computer security and information assurance budgets.**

Economic Espionage Act of 1996

- **Prohibits the gathering of trade secrets for the purpose of providing them to a foreign entity.**
- **Provides criminal penalties for obtaining trade secrets to benefit a government or private foreign entity.**

USA Patriot Act, GPEA, and Paperwork Reduction Acts

- **USA Patriot Act**

  -Focused on counterterrorism

  -Computer trespassers

- **Government Paperwork Elimination Act(GPEA)**
  - **Provides procedures and guidance to implement the Government Paperwork Elimination Act (GPEA).**

  - GPEA requires Federal agencies, by October 21, 2003, to allow individuals or entities that deal with the agencies the option to submit information or transact with the agency electronically, when practicable, and to maintain records electronically, when practicable.
  - **The Act specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form, and encourages Federal government use of a range of electronic signature alternatives.**

USA Patriot Act, GPEA, and Paperwork Reduction Acts

- **Paperwork Reduction Acts**

  •The collection of certain information to the Office of Management and Budget(OMB).

  • establish with specific authority to regulate matters regarding federal information and to establish information policies. These information policies were intended to reduce the total amount of paperwork handled by the United States government and the general public.

Importance of Implications of Legal Issues Which can Affect Information Assurance (IA)

- Legal issues

(1) explain the legal responsibilities of the DAA;

(2) discuss the Computer Fraud and Abuse Act, P.L. 99-474, 18 U.S. Code 1030;

(3) discuss Copyright Protection and License, Copyright Act of 1976, Title 17 U.S. Code, P.L. 102- 307, amended the Copyright Act of 1976, 1990;

(4) discuss the Freedom of Information Act;

(5) discuss the purpose and history of NSD 42;

(6) discuss implications of the Privacy Act;

(7) list and discuss the issues of Computer Security Act of 1987(P.L. 100-235); and

(8) list international legal issues which can affect INFOSEC.

National Archives and Records Act

- The National Archives and Records Act monitors and assists Federal agencies follow guidelines for disposal of public records.

- Federal records can only be destroyed under the procedures described in statues of the NARA.

Computer Fraud and Abuse Act, P.L. 99-474, 18 U.S. Code 1030

- **Computer Fraud and Abuse Act**
  - Computer Fraud and Abuse Act, (Public Law (PL) 99-474) was written in 1986.
  - This law prohibits unauthorized or fraudulent access to government computers and establishment penalties for such access.
  - The act prohibits access with the intent to defraud, as well as international trespassing

Public Law 107-347, E-Government Act 0f 2002, Title III, Federal Information Security Management Act (FISMA), 17 Dec 02 Act

- **Federal Information Security Management Act (FISMA)**
  - **Federal Information Security Management Act (FISMA 107-347)was created in 2002.**
  - **Requires that the Chief Information Officer (CIO) of each Federal agency to create a security program that meets the guidelines of the FISMA.**
  - **This law encompasses all information stored at all Federal agencies.**

Export Control

Commerce Department	State Department	Treasury Department
Export Administration Act	Arms Export Control Act	Trading with the Enemy Act, Int'l Emergency Economic Powers Act, & Others
Export Administration Regulations ("EAR") 15 C.F.R. Parts 700-799	International Traffic in Arms Regulations ("ITAR") 22 C.F.R. Parts 120-130	Iraq Sanctions Regulations, Terrorism Sanctions Regulations, & Others 31 C.F.R. Parts 500-599
Commerce Control List	U.S. Munitions List	List of Specially Designated Nationals & Blocked Persons

Export Control (Encryption)

- **Strong encryption restrictions**
  - **Previously anything over 40 bits was considered strong encryption**
  - **U.S. companies can now export any encryption software to individuals, commercial firms or other non-government end users in any country**
- **No enemy states**
  - **Many countries require the importer of equipment containing strong cryptography to provide the government or law enforcement with a copy of their private keys.**
  - **Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria**
- **Controls on dual-use goods**
  - **Cryptography has long been considered a munition or weapon of war. Can be used for commercial or military purposes, therefor considered dual-use and protected as a military weapon**
- **Wassenaar Arrangement**
  - **39 countries are parties to the agreement which specifies all controlled dual-use goods, including encryption products and products that use encryption**

VERIS Community Database

- The purpose of the VERIS Community Database (VCDB) is to promote data-driven decision making and evidence-based risk management in the information security community by creating a public repository of breach data in an open format.
- The data is free for anyone to take and use as they see fit, and contributing incident data is highly encouraged.

Legal Responsibilities of Senior Systems Managers

- **Legal Responsibilities of Senior Systems Managers**
  1. Security Management
     - Requirements
     - Standards
     - Procedures
     - Security modes
     - Protocols
  2. Risk management program
  3. ISSOs report to ISSM

Implications of the Privacy Act

- Many laws guarantee the right to privacy, the Fourth Amendment, the Federal Wiretap Act, and the Electronic Communications Privacy Act all outline specific details and policy in regards to protecting the privacy of US citizens
- The Fourth Amendment to the Constitution guarantees all individuals fundamental protections of privacy for their personal property.
  - there has been some controversy in how this right should be interpreted when the office and the computers in question belong to the government.
- In the court case of O'Connor vs. Ortega, the government searched the desk of an employee without his permission and was sued for violating his privacy.
  - As a result, the court refined the *Reasonableness Standard*.
  - This standard protects individuals from searches that are unreasonable in scope or justification, but does not require government officials to obtain a search warrant each time they have to access a person's desk or files at work.

Public Law 107-347 Regarding C&A

- Public Law 107-347 regarding certification and accreditation
- Certification and Accreditation is required by the Federal Information Security Management Act (FISMA) of 2002
- FISMA, also known as Title III of the E-Government Act (Public Law 107-347), mandates that all U.S. federal agencies develop and implement an agency-wide information security program that explains its security requirements, security policies, security controls, and risks to the agency

Legal and Liability Issues

- **Legal and Liability Issues**
- **National Security Interests**
- **Loss of life**
- **Financial risks**
- **Privacy Law**
- **Personal Jail Time**

Organisation for Economic Co-operation and Development (OECD) Guidelines

- **The OECD is an international organization that helps different governments come together and tackle the economic, social, and governance challenges of a globalized economy.**

The seven core principles defined by the OECD are:

- Collection of personal data should be limited, obtained by lawful and fair means, and with the knowledge of the subject.
- Personal data should be kept complete and current, and be relevant to the purposes for which it is being used.
- Subjects should be notified of the reason for the collection of their personal information at the time that it is collected, and organizations should only use it for that stated purpose.
- Only with the consent of the subject or by the authority of law should personal data be disclosed, made available, or used for purposes other than those previously stated.
- Reasonable safeguards should be put in place to protect personal data against risks such as loss, unauthorized access, modification, and disclosure.
- Developments, practices, and policies regarding personal data should be openly communicated. In addition, subjects should be able to easily establish the existence and nature of personal data, its use, and the identity and usual residence of the organization in possession of that data.
- Subjects should be able to find out whether an organization has their personal information and what that information is, to correct erroneous data, and to challenge denied requests to do so.
- Organizations should be accountable for complying with measures that support the previous principles.

NOTE Information on OECD Guidelines can be found at www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

Expansion

- Europe is usually stricter than the U.S., and to expand we would need to comply
- *Safe Harbor* requirements...a provision or statute that reduces or eliminates a party's legal liability, usually to encourage desirable practices.
- *European Union Principles on Privacy* - set of principles with six areas that address using and transmitting information considered sensitive in nature. All states in Europe must abide by these six principles to be in compliance.

Types of Laws (Civil)

- Civil (Code) Law System of law used in continental European countries such as France and Spain.
- Different from the common law used in the United Kingdom and United States.
- Civil law is rule-based law not precedence based.
- For the most part, a civil law system is focused on codified law—or written laws. However, some countries follow an “uncodified” civil law legal system.
- The history of civil laws dates to the sixth century when the Byzantine emperor Justinian codified the laws of Rome.
- Civil law was reborn due to the work of Italian legal scholars and spread throughout Europe, as exemplified by the Napoleonic Code of France and the French Civil Code of 1804.
- Civil legal systems should not be confused with the civil (or tort) laws found in the U.S.
- Civil law was established by states or nations for self-regulation; thus, civil law can be divided into subdivisions such as French civil law, German civil law, and so on.
- It is the most widespread legal system in the world and the most common legal system in Europe.
- Under civil law, lower courts are not compelled to follow the decisions made by higher courts.

Types of Law (Common)

- Developed in England.
- Based on previous interpretations of laws:
- In the past, judges would walk throughout the country enforcing laws and settling disputes.
- They did not have a written set of laws, so they based their laws on custom and precedent.
- In the twelfth century, the King of England imposed a unified legal system that was “common” to the entire country.
- Reflects the community’s morals and expectations.
- Led to the creation of barristers, or lawyers, who actively participate in the litigation process through the presentation of evidence and arguments.
- Today, common law uses judges and juries of peers. If the jury trial is waived, the judge decides the facts.
- Typical systems consist of a higher court, several intermediate appellate courts, and many local trial courts.
- Precedent flows down through this system.
- Tradition also allows for “Magistrate’s Courts,” which address administrative decisions.

Types of Law (Common...continued)

- **Common law is broken into the following:**
  - **Criminal**
  - **Civil/tort**
  - **Customary Law**
  - **Religious Law Systems**
  - **Mixed Law Systems**

Types of Common Law

Criminal

- **Based on common law, statutory law, or a combination of both.**
- **Addresses behavior that is considered harmful to society.**
- **Punishment usually involves a loss of freedom, such as incarceration, or monetary fines.**

Type of Common Law (continued)

- Civil/tort
- Offshoot of criminal law.
- Under civil law, the defendant owes a legal duty to the victim. In other words, the defendant is of conduct, usually set by what a “reasonable man of ordinary prudence” would do to prevent foreseeable injury to the victim.
- The defendant’s breach of that duty causes injury to the victim; usually physical or financial.

Categories of civil law

Intentional: Examples include assault, intentional infliction of emotional distress, or false imprisonment.

Wrongs against Property: An example is nuisance against landowner.

Wrongs against a Person: Examples include car accidents, dog bites, and a slip and fall.

Negligence Wrongful death.

Nuisance Trespassing.

Dignitary Wrongs: Include invasion of privacy and civil rights violations.

Economic Wrongs: Examples include patent, copyright, and trademark infringement.

Strict Liability: Examples include a failure to warn of risks and defects in product manufacturing or design.

Administrative (regulatory)

Laws and legal principles created by administrative agencies to address a number of areas, including international trade, manufacturing, environment, and immigration

Responsibility is on the prosecution to prove guilt beyond a reasonable doubt (innocent until proven guilty). Used in Canada, United Kingdom, Australia, United States, and New Zealand.

Type of Common Law (continued)

- Customary Law
- Deals mainly with personal conduct and patterns of behavior.
- Based on traditions and customs of the region.
- Emerged when cooperation of individuals became necessary as communities merged.
- Not many countries work under a purely customary law system, but instead use a mixed system where customary law is an integrated component. (Codified civil law systems emerged from customary law.)
- Mainly used in regions of the world that have mixed legal systems (for example, China and India).
- Restitution is commonly in the form of a monetary fine or service.

Type of Common Law (continued)

Religious Law Systems

- Based on religious beliefs of the region
- In Islamic countries, the law is based on the rules of the Koran.
- The law, however, is different in every Islamic country.
- Jurists and clerics have a high degree of authority.
- Cover all aspects of human life, but commonly divided into: Responsibilities and obligations to others
- Religious duties
- Knowledge and rules as revealed by God, which define and govern human affairs.
- Rather than create laws, law makers and scholars attempt to discover the truth of law.
- Law, in the religious sense, also includes codes of ethics and morality, which are upheld and required by God. For example, Hindu law, Sharia (Islamic law), Halakha (Jewish law), and so on.

Type of Common Law (continued)

Mixed Law Systems

- **Two or more legal systems are used together and apply cumulatively or interactively.**
- **Most often mixed law systems consist of civil and common**
- **A combination of systems is used as a result of more or less clearly defined fields of application.**
- **Civil law may apply to certain types of crimes, while religious law may apply to other types within the same region.**
- **Examples of mixed law systems include Holland, Canada, and South Africa.**


CIVIL LAW
COMMON LAW
MUSLIM LAW
CUSTOMARY LAW
MIXED SYSTEM
NORTH
AMERICA
EUROPE
ASIA
MIDDLE EAST
WEST INDIES
CENTRAL
AMERICA
AFRICA
SOUTH
AMERICA
SOUTH
EAST ASIA
OCEANIA

Civil Law

Civil law deals with wrongs against individuals or companies that result in dam- ages or loss. This is referred to as tort law.

Examples include trespassing, battery, negligence, and products liability.

A civil lawsuit would result in financial restitution and/or community service instead of a jail sentence.

When someone sues another person in civil court, the jury decides upon liability instead of innocence or guilt.

If the jury determines the defendant is liable for the act, then the jury decides upon the punitive damages of the case.

Criminal Law

Criminal law is used when an individual's conduct violates the government laws, which have been developed to protect the public.

Jail sentences are commonly the punishment for criminal law cases, whereas in civil law cases the punishment is usually an amount of money that the liable individual must pay the victim.

For example, in the O.J. Simpson case, he was first tried and found not guilty in the criminal law case, but then was found liable in the civil law case.

This seeming contradiction can happen because the burden of proof is lower in civil cases than in criminal cases.

Administrative Law

- Administrative/regulatory law deals with regulatory standards that regulate performance and conduct.
- Government agencies create these standards, which are usually applied to companies and individuals within those specific industries.
- Some examples of administrative laws could be that every building used for business must have a fire detection and suppression system, must have easily seen exit signs, and cannot have blocked doors, in case of a fire.
- Companies that produce and package food and drug products are regulated by many standards so the public is protected and aware of their actions.
- If a case was made that specific standards were not abided by, high officials in the companies could be held accountable, as in a company that makes tires that shred after a couple of years of use.
- The people who held high positions in this company were most likely aware of these conditions but chose to ignore them to keep profits up. Under administrative, criminal, and civil law, they may have to pay dearly for these decisions.

Intellectual Property Law

Several laws to protect your work including CISSP Study Guides

Intellectual Property Law

A *trade secret* is something that is proprietary to a company and important for its survival and profitability. An example of a trade secret is the formula used for a soft drink, such as Coke or Pepsi.

Intellectual Property Law

Copyright law **protects the right of an author to control the public distribution, reproduction, display, and adaptation of his original work.**

The law covers many categories of work: pictorial, graphic, musical, dramatic, literary, pantomime, motion picture, sculptural, sound recording, and architectural.

Copyright law does not cover the specific resource, as does trade secret law.

Intellectual Property Law

A *trademark* is slightly different from a copyright in that it is used to protect a word, name, symbol, sound, shape, color, or combination of these. The reason a company would trademark one of these, or a combination, is that it represents their company (brand identity) to a group of people or to the world.

Intellectual Property Law

What?

NOTE In 1883, international harmonization of trademark laws began with the Paris Convention, which in turn prompted the Madrid Agreement of 1891. Today, international trademark law efforts and international registration are overseen by the World Intellectual Property Organization (WIPO), an agency of the United Nations.

Intellectual Property Law

- ***Patents*** **are given to individuals or companies to grant them legal ownership of, and enable them to exclude others from using or copying, the invention covered by the patent.**
- **The invention must be novel, useful, and not obvious—which means, for example, that a company could not patent air.**
  - **Thank goodness. If a company figured out how to patent air, we would have to pay for each and every breath we took!**

Algorithms...hmmmm...

NOTE A patent is the strongest form of intellectual property protection.

Internal Protection of Intellectual Property

- The resources protected by one of the previously mentioned laws need to be identified and integrated into the company's data classification scheme. This should be directed by management and carried out by the IT staff.
- Once the individuals who are allowed to have access are identified, their level of access and interaction with the resource should be defined in a granular method.
- Employees must be informed of the level of secrecy or confidentiality of the re- source, and of their expected behavior pertaining to that resource.
- If a company fails in one or all of these steps, it may not be covered by the laws described previously, because it may have failed to practice due care and properly pro- tect the resource that it has claimed to be so important to the survival and competitive- ness of the company.

Software Piracy

- Software piracy occurs when the intellectual or creative work of an author is used or duplicated without permission or compensation to the author. It is an act of infringement on ownership rights, and if the pirate is caught, he could be sued civilly for damages, be criminally prosecuted, or both. HANG HIM FROM A YARD ARM!

- When a vendor develops an application, it usually licenses the program rather than sells it outright. The license agreement contains provisions relating to the use and security of the software and the corresponding manuals. If an individual or company fails to observe and abide by those requirements, the license may be terminated and, depending on the actions, criminal charges may be leveled.

Licenses...ARRRRRRGGH!

- ***Freeware*** **is software that is publicly available free of charge and can be used, copied, studied, modified, and redistributed without restriction.**
- ***Shareware*****, or *trialware*****, is used by vendors to market their software. Users obtain a free, trial version of the software. Once the user tries out the program, the user is asked to purchase a copy of it.**
- ***Commercial software*** **is, quite simply, software that is sold for or serves commercial purposes.**
- ***Academic software*** **is software that is provided for academic purposes at a reduced cost. It can be open source, freeware, or commercial software.**
- ***End User Licensing Agreement (EULA)*** **specifies more granular conditions and restrictions than a master agreement.**

Let me throw some numbers at you...

- A study by the Business Software Alliance (BSA) and International Data Corporation (IDC) found that the frequency of illegal software is 36 percent worldwide.
- This means that for every two dollars' worth of legal software that is purchased, one dollar's worth is pirated.
- Software developers often use these numbers to calculate losses resulting from pirated copies.
- The assumption is that if the pirated copy had not been available, then everyone who is using a pirated copy would have instead purchased it legally.

Digital Millennium Copyright Act

- **the new Digital Millennium Copyright Act (DMCA) makes it illegal to create products that circumvent copyright protection mechanisms**

Privacy

- Seeking to protect Personally Identifiable Information (PII) .
- In response, countries have enacted privacy laws.
  - For example, although the United States already had the Federal Privacy Act of 1974, it has enacted new laws, such as the Gramm-Leach-Bliley Act of 1999 and the Health Insurance Portability and Account-ability Act (HIPAA), in response to an increased need to protect personal privacy information.
- These are examples of a vertical approach to addressing privacy, whereas Canada's Personal Information Protection and Electronic Documents Act and New Zealand's Privacy Act of 1993 are horizontal approaches.

Privacy

The Increasing Need for Privacy Laws

The following issues have increased the need for more privacy laws and governance:

- **Data aggregation and retrieval technologies advancement**
  - Large data warehouses are continually being created full of private information.
- **Loss of borders (globalization)**
  - Private data flows from country to country for many different reasons.
  - Business globalization.
- **Convergent technologies advancements**
  - Gathering, mining, distributing sensitive information.

Sarbanes-Oxley Act (SOX)

- SOX provides requirements for how companies must track, manage, and report on financial information. This includes safeguarding the data and guaranteeing its integrity and authenticity. Most companies rely on computer equipment and electronic storage for transacting and archiving data; therefore, processes and controls must be in place to protect the data.
- Failure to comply with the Sarbanes-Oxley Act can lead to stiff penalties and potentially significant jail time for company executives, including the Chief Executive Officer (CEO), the Chief Financial Officer (CFO), and others.

The Health Insurance Portability and Accountability Act (HIPAA)

- HIPAA outlines how security should be managed for any facility that creates, accesses, shares, or destroys medical information.
- HIPAA mandates steep federal penalties for noncompliance. If medical information is used in a way that violates the privacy standards dictated by HIPAA, even by mistake, monetary penalties of $100 per violation are enforced, up to $25,000 per year, per standard.
- If protected health information is obtained or disclosed knowingly, the fines can be as much as $50,000 and one year in prison.
- If the information is obtained or disclosed under false pretenses, the cost can go up to $250,000 with ten years in prison if there is intent to sell or use the information for commercial advantage, personal gain, or malicious harm.

The Gramm-Leach-Bliley Act of 1999 (GLBA)

- The Gramm-Leach-Bliley Act of 1999 (GLBA) requires financial institutions to develop privacy notices and give their customers the option to prohibit financial institutions from sharing their information with nonaffiliated third parties.
- It also requires these institutions to have a written security policy in place.

The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act, written in 1986 and amended in 1996, is the primary U.S. federal anti-hacking statute. It prohibits seven forms of activity and makes them federal crimes:

- **The knowing access of computers of the federal government to obtain classified information without authorization or in excess of authorization**
- **The intentional access of a computer to obtain information from a financial institution, the federal government, or any protected computer involved in interstate or foreign communications without authorization or through the use of excess of authorization**
- **The intentional and unauthorized access of computers of the federal government, or computers used by or for the government when the access affects the government's use of that computer**
- **The knowing access of a protected computer without authorization or in excess of authorization with the intent to defraud**
- **Knowingly causing the transmission of a program, information, code, or command and, as a result of such conduct, intentionally causing damage without authorization to a protected computer**
- **The knowing trafficking of computer passwords with the intent to defraud**
- **The transmission of communications containing threats to cause damage to a protected computer**

The Federal Privacy Act of 1974

- To keep the government in check on gathering information on U.S. citizens and other matters, a majority of its files are considered open to the public.
  - Government files are open to the public unless specific issues enacted by the legislature deem certain files unavailable.
  - This is what is explained in the Freedom of Information Act.
  - This is different from what the Privacy Act outlines and protects.
- The Privacy Act applies to records and documents developed and maintained by specific branches of the federal government, such as executive departments, government corporations, independent regulatory agencies, and government-controlled corporations.
  - It does not apply to congressional, judiciary, or territorial subdivisions.
- You can gather information, but you must have a need for it, and they cannot disclose your information without your written permission.

Basel II

- **Basel II is built on three main components, called "Pillars."**
  1. **Minimum Capital Requirements measures the risk and spells out the calculation for determining the minimum capital.**
  2. **Supervision provides a framework for oversight and review to continually analyze risk and improve security measures.**
  3. **Market Discipline requires member institutions to disclose their exposure to risk and validate adequate market capital.**
- **Information security is integral to Basel II. Member institutions seeking to reduce the amount of capital they must have on hand must continually assess their exposure to risk and implement security controls or mitigations to protect their data.**

Payment Card Industry Data Security Standards (PCI DSS)

- The PCI DSS applies to any entity that processes, transmits, stores, or accepts credit card data.
- The control objectives are implemented via 12 requirements, as stated at https:// www.pcisecuritystandards.org/security_standards/pci_dss.shtml:

1. Use and maintain a firewall.
2. Reset vendor defaults for system passwords and other security parameters.
3. Protect cardholder data at rest.
4. Encrypt cardholder data when it is transmitted across public networks.
5. Use and update antivirus software.
6. Systems and applications must be developed with security in mind.
7. Access to cardholder data must be restricted by business “need to know.”
8. Each person with computer access must be assigned a unique ID.
9. Physical access to cardholder data should be restricted.
10. All access to network resources and cardholder data must be tracked and monitored.
11. Security systems and processes must be regularly tested.
12. A policy must be maintained that addresses information security.

The Computer Security Act of 1987

- The Computer Security Act of 1987 requires U.S. federal agencies to identify computer systems that contain sensitive information.
- The agency must develop a security policy and plan for each of these systems and conduct periodic training for individuals who operate, manage, or use these systems.
- Federal agency employees must be provided with security-awareness training and be informed of how the agency defines acceptable computer use and practices.

The Economic Espionage Act of 1996

- Prior to 1996, industry and corporate espionage was taking place with no real guidelines for who could properly investigate the events.
- The Economic Espionage Act of 1996 provides the necessary structure when dealing with these types of cases and further defines trade secrets to be technical, business, engineering, scientific, or financial.
- This means that an asset does not necessarily need to be tangible to be protected or be stolen.
- Thus, this act enables the FBI to investigate industrial and corporate espionage cases.

Employee Privacy Issues

- If a company has learned that the state the facility is located in permits keyboard, e-mail, and surveillance monitoring, it must take the proper steps to ensure that the employees know that these types of monitoring may be put into place. This is the best way for a company to protect itself, make sure it has a legal leg to stand on if necessary, and not present the employees with any surprises.
- The monitoring must be work related, meaning that a manager may have the right to listen in on his employees' conversations with customers, but he does not have the right to listen in on personal conversations that are not work related. Monitoring also must happen in a consistent way, such that all employees are subjected to monitoring, not just one or two people.

Review

Review on Ways of Dealing with Privacy

Current methods of privacy protection and examples are listed next:

- **Government regulations** SOX, HIPAA, GLBA, BASEL
- **Self-regulation** Payment Card Industry (PCI)
- **Individual user** Passwords, encryption, awareness

Reasonable Expectation of Privacy (REP)

- If a company feels it may be necessary to monitor e-mail messages and usage, this must be explained to the employees, first through a security policy and then through a constant reminder such as a computer banner or regular training. It is best to have an employee read a document describing what type of monitoring they could be subjected to, what is considered acceptable behavior, and what the consequences of not meeting those expectations are. The employees should sign this document, which can later be treated as a legally admissible document if necessary. This document is referred to as a waiver of reasonable expectation of privacy (REP). By signing the waiver, employees waive their expectation to privacy.

Personal Privacy Protection

End users are also responsible for their own privacy, especially as it relates to protecting the data that is on their own systems. End users should be encouraged to use common sense and best practices. This includes the use of encryption to protect sensitive personal information, as well as firewalls, antivirus software, and patches to protect computers from becoming infected with malware. Documents containing personal information, such as credit card statements, should also be shredded. Also, it's important for end users to understand that when data is given to a third party, it is no longer under their control.

Liability and Its Ramifications

- The company is responsible for providing fire detection and suppression systems, fire-resistant construction material in certain areas, alarms, exits, fire extinguishers, and backups of all the important information that could be affected by a fire.
- If a fire burns a company's building to the ground and consumes all the records (customer data, inventory records, and similar information that is necessary to rebuild the business), then the company did not exercise due care to ensure it was protected from such loss (by backing up to an offsite location, for example).
  - In this case, the employees, shareholders, customers, and everyone affected could successfully sue the company.
  - However, if the company did everything expected of it in the previously listed respects, it could not be successfully sued for failure to practice due care (negligence).

Due Care and Due Diligence

- ***Due care*** **- means that a company did all it could have reasonably done, under the circumstances, to prevent security breaches, and also took reasonable steps to ensure that if a security breach did take place, proper controls or countermeasures were in place to mitigate the damages.**

- ***Due diligence*** **- means that the company properly investigated all of its possible weaknesses and vulnerabilities.**

Figure 10-1 One example of the consequences of corporate fraud in 2002

Downstream Liability

- **Let's say company A and company B have constructed an extranet.**
- **Company A does not put in controls to detect and deal with viruses. Company A gets infected with a destructive virus and it is spread to company B through the extranet.**
- **The virus corrupts critical data and causes a massive disruption to company B's production.**
- **Therefore, company B can sue company A for being negligent. Both companies need to make sure they are doing their part to ensure their activities, or the lack of them, will not negatively affect another company, which is referred to as *downstream liability*.**

NOTE Responsibility generally refers to the obligations and expected actions and behaviors of a particular party. An obligation may have a defined set of specific actions that are required, or a more general and open approach, which enables the party to decide how it will fulfill the particular obligation. Accountability refers to the ability to hold a party responsible for certain actions or inaction.

Due care responsibilities

- To prove negligence in court, the plaintiff must establish that the defendant had a ***legally recognized obligation***, or duty, to protect the plaintiff from unreasonable risks and that the defendant's failure to protect the plaintiff from an unreasonable risk (breach of duty) was the ***proximate cause*** of the plaintiff's damages.

Access Control Policies

- **Access control policies is permitting access to certain facilities, information, and information systems only to authorized individuals.**
- **To understand access control policies you need to understand four main concepts:**
  1. **users**
  2. **actions**
  3. **resources**
  4. **relationships**

Administrative Security Policies And Procedures

- Administrative security policies describe the intended behavior rules for people.
- Serving as a guide for both end-users and management, administrative policies should spell out the roles and responsibilities for all users of technology systems in the organization.
- It is very important to inform end-users and other management team members of administrative security policies.
- Users cannot be expected to follow policies if they do not know what they are.
- After reviewing the administrative policies, it is a good idea to get the user to sign the policy document attesting to the fact that they have read it, understand it and will abide by it.

Audit Trails and Logging Policies

- **Audit Trails**
- **Keep logs of traffic patterns and noting any deviations from normal behavior found. Such deviations are the first clues to security problems**
- **The data to be collected in the logs should include the following:**
  - **User name**
  - **Host name**
  - **Source and destination IP addresses**
  - **Source and destination port numbers**
  - **Timestamp**

Audit Trails and Logging Policies (2)

- This collected data should be kept local to the resource until an event is finished upon which it may be taken to a secure location.
- Make sure that the paths (Channels) from the collection points to the storage location are secure.
- Audit data should be one of the most secured data on location and in back ups.

Audit Trails and Logging Policies (3)

Audit Trail Policy

- The [ORGANIZATION] must maintain audit trail records in compliance with various regulatory laws, rules, and guidelines.
- This policy sets internal controls and audit requirements to include: individual accountability, reconstructing event, problem monitoring, and intrusion detection tools to monitor sensitive systems.

Audit Trails and Logging Policies (4)

- **Logging Policies: All access to networked systems must be logged.**
  - **When determined to be critical to the [ORGANIZATION], the logging of transactions must be included regardless of the operating platform. Log data must be classified as sensitive.**
  - **These logs must be retrievable through clearly defined procedures and must be maintained for time periods prescribed for audit, legal, and recovery purposes.**
  - **As new applications, platforms, mediums, or other technical changes to system operations are made; consideration of logging requirements and availability must be made.**
  - **Requirements for logging data must be clearly established as system, architectural, technical, or network designs.**

Documentation Policies (1)

- Many of the controls and safeguards discussed fall into the traditional categories of detective and reactive controls.
- With the increased public and governmental focus on the protection of personal information, and the passing in several countries of privacy laws and regulations, the focus is now shifting to preventative and proactive approaches.
- It is no longer reasonable to have strictly reactive information security posture; businesses must demonstrate that they have put sufficient forethought into how to prevent system compromises or the unauthorized access to data, and if theses are detected, how to disclose the incident to affected parties.

Documentation Policies (2)

- Most seasoned computer forensics investigators have mixed emotions regarding detailed policies for dealing with an investigation.
- The common concern is that too much detail and formalism will lead to rigid checklists and negatively impact the creative aspects of the analysis and examination.
- Too little formalism an methodology leads to sloppiness, difficulty in recreating the investigative process, and the lack of an auditable process that can be examined by the courts.

Documentation Policies (3)

- In response to this issue, several international entities have devised general guidelines that are based on the International Organization of Computer Evidence (IOCE) /Group of 8 Nations (G8) principles for computer forensics and digital/electronic evidence:
  - When dealing with digital evidence, all of the general forensic and procedural principles must be applied.
  - Upon seizing digital evidence, actions taken should not change that evidence.
  - When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.
  - All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.

Documentation Policies (4)

- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in his possession.
- Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

Evidence Collection and Preservation Policies

- **Definition:**
  - **Preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis using well-defined methodologies and procedures.**
- **Methodology:**
  - **Acquire the evidence without altering or damaging the original.**
  - **Authenticate that the recovered evidence is the same as the original seized.**
  - **Analyze the data without modifying it.**

Evidence Collection and Preservation Policies

- The exact requirements for the admissibility of evidence vary across legal systems and between different classes.
- At a more generic level, evidence should have some probative value, be relevant to the case at hand, and meet the following criteria:
  - Be authentic
  - Be accurate
  - Be complete
  - Be convincing
  - Be admissible

Security Policy

- **Information security policy**

  Information security policy is a set of rules that protects an organization's information assets

- **Two categories**
  - **General Issue-specific**
  - **System-specific**
- **Three types**
  - **Regulatory**
  - **Advisory**
  - **Informative**

Information Security Policy

Importance of Information security policy

- Information security policies provide a framework for best practice that can be followed by all employees. They help to ensure risk is minimized and that any security incidents are effectively responded to.
- Information security policies will also help turn staff into participants in the company's efforts to secure its information assets, and the process of developing these policies will help to define a company's information assets

National IA Certification & Accreditation (C&A) Process Policy

- National Information Assurance Certification and Accreditation Process (NIACAP)" was developed to provide minimum standards for the certification and accreditation of national security systems.
- Federal departments and agencies shall refer to the NIACAP, or a C&A process that is consistent with the NIACAP, when developing their C&A programs.

Personnel Security Policies & Guidance

- **The greatest harm/disruption to a system comes from the actions of individuals, both intentional and unintentional.**
- **Users, designers, implementers, and managers are involved in many important issues in securing the information in an information system.**
- **Users of the systems must meet the personnel requirements contained in the organizations published security policies and guidance**

Personnel Security Policies & Guidance

- As outlined in NIST guidance it is important that organizations, develops, disseminates, and periodically reviews/updates:
- (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.
- The personnel security policy and procedures must be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general, and for a particular information system, when required.
- NIST Special Publication 800-12 provides guidance on security policies and procedures.

Personnel Security Policies & Guidance

- **Policies and guidance should cover:**
  - **Roles and Responsibilities of all personnel**
    - **CIO, CISO, CEO, ISSO**
    - **Supervisors**
    - **Security officers**
    - **Users**
  - **Organization wide policies**
  - **Issues for Compliance, inspection and ramifications of non-compliance.**

Access Authorization

- This is the determination of whether a user has permission to access, read, modify, insert, or delete certain data, or to execute certain programs.
- Authorization is also commonly referred to as access permissions and it determines the privileges a user has on a system and what the user should be allowed to do to the resource.
- Access permissions are normally specified by a list of possibilities. For example, UNIX allows the list { read, write, execute} as the list of possibilities for a user or group of users on a UNIX file.

Auditable Events

- An auditable event represents a single action (either a command or system call) that may affect the security of the system. There are two classifications of events: fixed and selectable.
- Fixed events
- Selectable events

Authentication

- Authentication is the process of validating the identity of someone or something.
- Generally authentication requires the presentation of credentials or items of value to really prove the claim of who you are.
- The items of value or credential are based on several unique factors that show something you know, something you have, or something you are
- Authentication is the validation of a user's identity, in other words, "Are you whom you claim to be"
- In general authentication takes one of the following three forms:
  - Basic authentication
  - Challenge-response
  - Centralized authentication

Background Investigation

- Background checks by employers have proved to be a valuable investment for government agencies and corporations due to the repercussions costs, such as law suits or liability insurance.
- The current cost of processing paperwork of new hired employees, corporations are reassuring themselves the hired individual is worthy of the effort and cost by conducting background check as part of the initial application process.

Countermeasures

- **Countermeasures are defined as an action, device, procedure, technique, or other measure that reduces the vulnerability of an information systems.**

- **Countermeasures that alter the electromagnetic, acoustic or other signature(s) of a target thereby altering the tracking and sensing behavior of an incoming threat (e.g., guided missile) are designated soft kill measures.**

Delegation of Authority

- **Ultimately the managers are responsible for security of the information.**
- **They can transfer their authority to other individuals to secure the organizations information systems and the should not transfer their responsibility to other individuals**

Education, Training, and Awareness

- **Once the information Security program's place in the organization is established, planning for security education, training, and awareness (SETA) program is the responsibility of the CISO and is designed to reduce the incidence of accidental security branches by members of the organization, including employees, contractors, consultants, vendors, and business partners who come into contact with its information assets**

Education, Training, and Awareness

- **Awareness, training, and education programs offer two major benefits:**
  - **They can improve employee behavior.**
  - **They enable the organization to hold employees accountable for their actions.**

Electronic Records Management

- Electronic Records Management
  - E-Government Act
  - National Archives and Records Administration (NARA)
- Importance of Electronic Records Management
  - Common state government business process with laws, policies, procedures and protocols in place and operational within the public sector domain.
  - This activity touches almost all the business activities of state government from routine email to financial transactions, human resources, procurement, justice information, vital records, licenses, geographic information systems, project management, litigation, and collaborative information exchange

Electronic-Mail Security

- A number of encryption cryptosystems have been adapted to add security to e-mail, a notoriously insecure method of communication. Some of the more popular adoptions include
  - Secure Multipurpose Internet Mail Extensions
  - Privacy Enhanced Mail
  - Pretty Good Privacy

Information Classification

- Control for the protection of information
- Important facet of policy
- Least
  - "for internal use only"
- Clean desk policy
  - Information is classified based on the amount of damage it could cause if disclosed to the wrong parties.

Investigative Authorities

- The entities that are delegated authority to investigate incidents on the information system must have support from management.
- The power the investigative authority has needs to be clearly outlined

Key Management Infrastructure

- **Key Management: Generation, Transportation, and Distribution**
- **The Key Exchange Problem**
  - **Although symmetric encryption is commonly used due to its historical position in the cryptography and its speed, it suffers from a serious problem of how to safely and secretly deliver a secret key from the sender to the recipient.**
  - **This problem forms the basis for the *key exchange problem*.**
- **The *key exchange problem* involves:**
  - **ensuring that keys are exchanged so that the sender and receiver can perform encryption and decryption,**
  - **ensuring that an eavesdropper or outside party cannot break the code,**
  - **ensuring the receiver that a message was encrypted by the sender.**

Non-repudiation

- Non-Repudiation is the property that a valid signature is arbitrarily hard to forge and therefore the owner of the key cannot deny the legitimacy of one.
- Non-repudiation has mathematical merit. It is indeed extremely difficult to create a valid digital signature without possession of the private key.
- However operationally this is not so simple.

Public Key Infrastructure (PKI)

- **Importance and role of Public Key Infrastructure (PKI)**
  - **Integrated system of software, encryption methodologies, protocols, legal agreements, and 3rd part services**
  - **Based on public key**
  - **Include digital certificates and certificate authorities**

PKI Continued

- Public key container files that allow computer program to validate the key and identify to whom it belongs.
- Allows integration of key characteristics to be integrated into business practices
  - Authentication
  - Integrity
  - Privacy
  - Authorization
  - Nonrepudiation

Summary

- Copyright Protection and Licensing
- Criminal Prosecution
- Due Diligence
- Evidence Collection and Preservation
- Fraud, Waste, and Abuse

Summary

- **Laws Related To Information Assurance and Security**
  - Electronic Records Management and Federal Records Act
  - Federal Managers Financial Integrity Act of 1982
  - Federal Property and Administration Service Act
  - Patriot Act, GPEA
  - Paperwork Reduction Acts
  - National Archives and Records Act
  - Computer Fraud and Abuse Act
  - Freedom of Information Act and Electronic Freedom of Information Act
  - E-Government Act Of 2002, Title III
  - Federal Information Security Management ACT (FISMA)
  - Privacy Act

Summary

- Ethics
- Policies –
  - Access control
  - Logging and audits
  - Documentation
  - Information security
  - Personnel security
- Certification & Accreditation (C&A) Process Policy
- Countermeasures
- Delegation of Authority
- Education, Training, and Awareness
- Electronic Records Management

Summary

- Electronic-Mail Security
- Information Classification
- Investigative policy and procedures
- Key Management Infrastructure
- Information Marking
- Non-repudiation
- Public Key Infrastructure (PKI)

Ethics

Dr. Drew Hamilton

Ethics

- As an IAO, you have access to a great deal of proprietary information. The systems you oversee store private information, such as medical records, social security numbers, and other personal data.
- Your responsibility is to protect all proprietary data from unauthorized disclosure and to prevent system users from viewing the personal data of other users.

Ethics

- While you perform your duties to safeguard systems, always keep in mind that you serve as an ethical model to other system users. Encourage users to behave in an honest, respectful manner toward the company, the software industry, and their fellow users.
- Make sure users are aware of the policies for using the system responsibly.
- Don't allow others to use computers for anything other than official or authorized usage.
- Encourage responsible use of the system by making users aware of ethics policies, enforcing the policies, and setting a good example yourself!

Ethics

- Read this https://www.isc2.org/cgi-bin/content.cgi?category=12

- Act honorably, honestly, justly, responsibly, and legally, and protect society.
- Work diligently, provide competent services, and advance the security profession.
- Encourage the growth of research—teach, mentor, and value the certification.
- Discourage unnecessary fear or doubt, and do not consent to bad practices.
- Discourage unsafe practices, and preserve and strengthen the integrity of public infrastructures.
- Observe and abide by all contracts, expressed or implied, and give prudent advice.
- Avoid any conflict of interest, respect the trust that others put in you, and take on only those jobs you are fully qualified to perform.
- Stay current on skills, and do not become involved with activities that could injure the reputation of other security professionals.

Ethical Fallacies

The following are examples of these ethical fallacies:

- **Hackers only want to learn and improve their skills. Many of them are not making a profit off of their deeds; therefore, their activities should not be seen as illegal or unethical.**
- **The First Amendment protects and provides the right for U.S. citizens to write viruses.**
- **Information should be shared freely and openly; therefore, sharing confidential information and trade secrets should be legal and ethical.**
- **Hacking does not actually hurt anyone.**

Computer Ethics Institute
10 Commandments

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Internet Architecture Board

The Internet Architecture Board (IAB) is the coordinating committee for Internet de- sign, engineering, and management.

It is responsible for the architectural oversight of the Internet Engineering Task Force (IETF) activities, Internet Standards Process oversight and appeal, and editor of Request for Comments (RFCs)

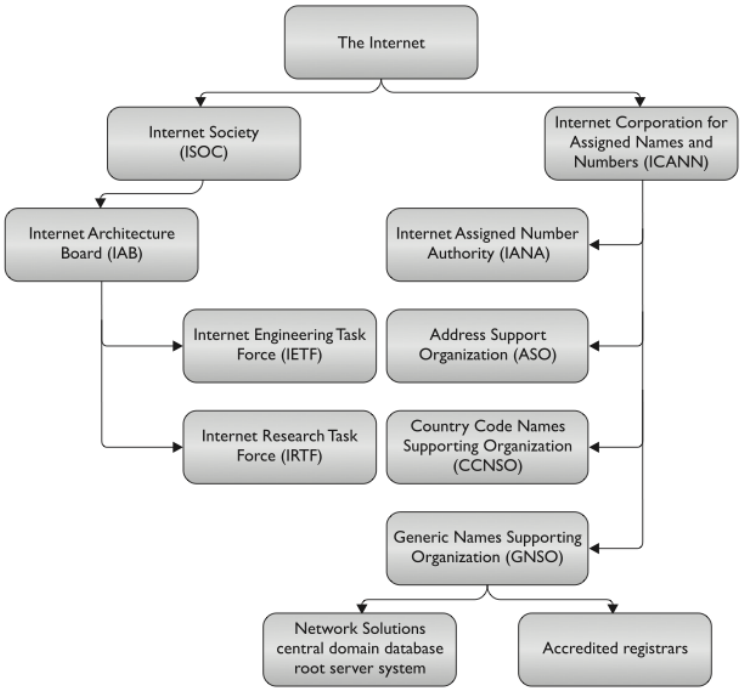


Figure 10-3 Agencies responsible for maintaining order for the components of the Internet

IAB Ethics

The IAB considers the following acts as unethical and unacceptable behavior:

- **Purposely seeking to gain unauthorized access to Internet resources**
- **Disrupting the intended use of the Internet**
- **Wasting resources (people, capacity, and computers) through purposeful actions**
- **Destroying the integrity of computer-based information**
- **Compromising the privacy of others**
- **Conducting Internet-wide experiments in a negligent manner**

Corporate Ethics Programs

- **Why this ethics stuff really matters...**
- **The Federal Sentencing Guidelines for Organizations (FSGO) created an outline for ethical requirements, and in some cases will reduce the criminal sentencing and liability if ethical programs are put in place.**
- **This was updated with requirements that made it much more important for the senior executives and board members of an organization to actively participate and be aware of the ethics program in an organization.**

Security policy, standards, procedures and guidelines

Dr. Drew Hamilton

Agenda

- General Countermeasure/Risk Management Information
- Analyze Potential Countermeasures
- Determine Countermeasures
- Identify Potential Countermeasures
- Determine Cost/Benefit of Countermeasures

General Countermeasure/Risk Management Information

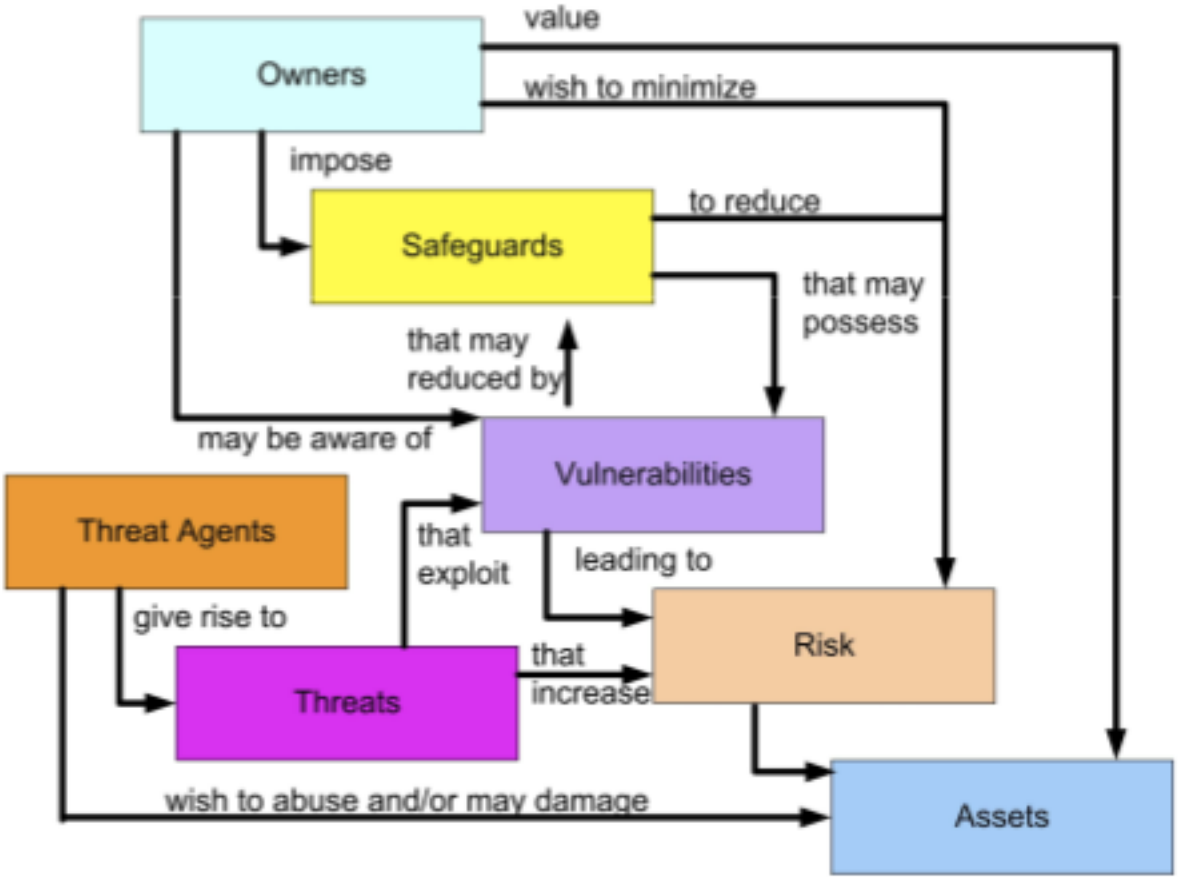
Countermeasure Process

- Identify Systems and Threats to Systems
  - How much risk is present?
- Identify Countermeasures
  - How can we mitigate the risk?
  - Which COTS product should we use?
  - Which OS? How do we lock down the OS?
- Implement Countermeasures
  - Protection Profiles, Network Access Control (NAC), etc
- Assess Effectiveness of Countermeasures
  - How well is the risk mitigated?
    - Qualitative Assessment
    - Quantitative Assessment
    - Certification and Accreditation (C&A Process)
  - Cost/Benefit Analysis
    - Time vs. Money vs. Effort vs. Risk

Definitions

- Asset - a resource (physical or logical) that is valued by the organization.
- Threat - any potential danger to information or an information system.
- Threat Agent – the source that has the potential of causing a threat.
- Exposure - instance of being exposed to losses from a threat.
- Vulnerability - an information system weakness that could be exploited.
- Attack – an action intending harm by exploiting a vulnerability.
- Countermeasures and Safeguards - an entity that mitigates the potential risk.
- Risk-likelihood of an unwanted event occurring.
- Residual Risk-the portion of risk that remains.

Risk Management Information Security Concept Flow



Risk Management Definitions

A discipline for living with the possibility that future events may cause harm.

Risk Management reduces risk by defining and controlling threats and vulnerabilities.

(Threats, Vulnerability, & Asset Value) = Total Risk

Concept of mitigating controls:

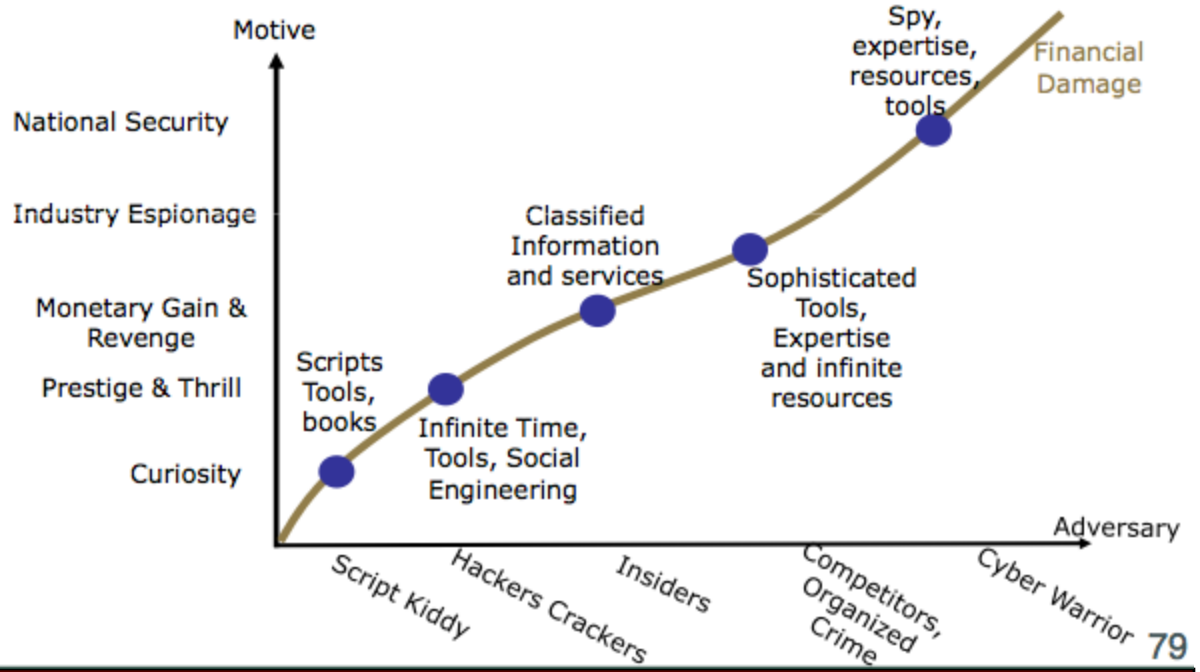
Total Risk -Countermeasures = Residual Risk

Identify System Components and Risks

- **Identify all systems in a network**
  - **Automated tools may be used to assist**
- **Identify risks inherent to systems within enterprise boundary**

Determine countermeasures

- **Countermeasures based on threat capabilities and motivations**
  - **What is the threat?**
  - **How sophisticated is the threat?**
  - **Given the threat level, is it worth implementing a specific countermeasure?**



Security In Systems Engineering

- **Design Phase**
  - **Cheapest phase to add security and risk mitigation efforts**
- **Implementation Phase**
  - **Risk may arise from design issues**
  - **More expensive than design phase to manage risk**
- **Testing Phase**
  - **Add countermeasures to mitigate/reduce risk**
  - **Countermeasures must be tested as well**

Mitigating Risk

- **Risk Reduction: Provide countermeasures to reduce the risk and strengthen the security posture**
  - ***Most common course of action to risk***
- **Risk Transference: Transfer risk to another party.**
  - ***Example: Insurance***
- **Risk Acceptance: Accepting the risk and absorbing the cost when and if occurs**
- **Risk Avoidance: Decide not to continue with the activity or not to support the situation that causes the risk**

Defense vs. Prob. of Attack

	Consequence:				
	Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*
Likelihood:	*1*	*2*	*3*	*4*	*5*
A (almost certain)	H	H	E	E	E
B (likely)	M	H	H	E	E
C (possible)	L	M	H	E	E
D (unlikely)	L	L	M	H	E
E (rare)	L	L	M	H	H

E	Extreme Risk: Immediate action required to mitigate the risk or decide to not proceed
H	High Risk: Action should be taken to compensate for the risk
M	Moderate Risk: Action should be taken to monitor the risk
L	Low Risk: Routine acceptance of the risk

Security Test and Evaluation

- **Procedures**
  - Customized testing procedures for a system
  - Testing procedures written by team to include: management, engineers, and users
- **Tools**
  - Network Scanners
  - Vulnerability Scanners
- **Techniques**
  - Penetration Testing
  - Denial-of-Service Testing

Evaluate Potential Countermeasures

- **Cost**
  - **Initial, Maintenance, Update Cost**
  - **User annoyance level**
- **Level of Risk Mitigated**
  - **Probability of threat occurring**
  - **Scope of the risk**
- **Effectiveness of the countermeasure**
  - **How well does the security control work?**

Organizational Security Needs vs. Countermeasures

- Consider value of information
- Determine cost and value of assets
  - Cost to acquire, develop, and maintain.
  - Value to owners, custodians, users, or adversaries.
  - Recognize cost and value in the real world.
    - Price others are willing to pay (published references, mailing lists, etc.)..
    - Value of intellectual property (trade secrets, classified information, patents, copyrights, etc.).

Testing Roles and Responsibilities

- **All countermeasures must be testable**
- **Roles:**
  - **Usability Tester**
  - **Security Tester**
- **Responsibilities:**
  - **Determine level of risk**
  - **Determine adequacy of security controls**

Testing Tools

- Network Scanners
- Vulnerability Scanners
- Scanners help in penetration testing
- Level of effort in testing should be level with threat level/risk level
- Apply appropriate testing tools to appropriate threat

Testing: Penetration Testing

- **Application Penetration**
  - **Can an unauthenticated user gain access to a restricted application?**
  - **Exploits specific to an OS or application**
- **Network Penetration**
  - **Can an unauthenticated computer gain access to the network?**
  - **Security tools can aid in this kind of testing to include port scanners and network vulnerability scanners**

Determine Underlying State of System

- How to determine state of system?
- What operating system is being used?
  - Every piece of software contains inherent security risks
  - Most risks are documented, others are not (zero-day exploits)
- Base Profiles help keep the same system state across an enterprise
  - Every system runs the same security hardened configuration

Interpreting Test Results

- Deductive reasoning is used to analyze test results
  - For example, “exploit X succeeded in compromising the network, what is the resulting impact to network resources?”
- Static and variable factors should be taken into consideration
  - Many unknowns still exist
- Penetration testing reports should contain the testing methodology

Joint System Usage Acceptance

- Joint System Accreditation
- Apply discriminate approach variables and constants based on test procedures to gain acceptance for joint system usage
- System usage helps develop a usage profile for an intrusion detection system
- Networking intrusion detection should detect outliers in network usage and detect a possible attack

Possible Network Tools

- Password Cracker
- War Dialing
- War Driving
- Log Review
- Virus Scanner
- File Integrity Checking
- Network Mapper (nmap)

Countermeasure Models, Tools, Techniques

- Test Results inform management of next course of action and steps to take
- Models
  - Create spanning tree of threats
    - Map each threat to a specific countermeasure for full threat coverage
- Tools
  - Automated tools such as vulnerability scanners detect vulnerabilities
  - Configuration control tool to evaluate system compliance with security policies
- Techniques
  - Implement countermeasures at various levels
  - Defense in Depth
    - Countermeasures at system, LAN, WAN

Confirm Validity of a Transmission

- **Confirming transmissions is a very effective way to counter a network-based attack**
- **Link-layer encryption (P2P) protects traffic in small network**
- **Public Key Infrastructure (PKI)**
  - **Allows users and systems to exchange digitally signed and encrypted information**
    - **Provides integrity and confidentiality**

Enforcing "Need to Know" Automatically

- **Automated tools can verify an individual's eligibility to receive specific categories of information**
  - **Requires a form of identity/user management at Enterprise level (Role-based access control)**
  - **Can use message-level classification marking**
    - **XML-based message well-suited**
  - **PKI helps control and audit access**
  - **Fine-grained access control provided by many COTS access control solutions**

Methods to Evaluate Security Safeguards

- **Penetration Testing**
  - Most Common Technique
  - Requires a dedicated penetration testing team
- **Enterprise Vulnerability Scanners**
  - Vulnerabilities detected using specific vulnerability profiles
  - Virus Scanners rely on Virus Signatures
- **Enterprise Configuration Validators**
  - Validates Base Profile is implemented properly
  - Integrity Checking

Protection Profiles

- Used by IA engineer as baseline for countermeasure to a threat
- States a security problem rigorously for a system or group of systems (the Target of Evaluation – TOE)
- Specifies security requirements that address the problem
  - Does not address implementation methods
- Used in Common Criteria Evaluation/Certification

Determine Cost/Benefit of Countermeasures

Cost Benefit Analysis

- The organization will need to assess the benefits of the controls in terms of maintaining an acceptable mission posture for the organization.
- Just as there is a cost for implementing a needed control, there is a cost for not implementing it.
- By relating the result of not implementing the control to the mission, organizations can determine whether it is feasible to delay its implementation.

Cost/Benefit: IA Countermeasure Plans

- **Cost of Implementing Countermeasure versus Level of Risk Mitigated (Benefit)**
- **Cost Relating to:**
  - **Personnel**
  - **Implementation**
  - **Deployment**
  - **Maintenance**

Cost/Benefit: Personnel Supporting Access Control Policies

- Information System Security
- IT & Operations management
- System and network administrators
- Internal audit
- Physical security
- Business process and information owners
- Advisors
  (Human Resources, Legal, Emergency Measures Coordinator, Safety Officers)

IA Plans: Aggregation of Risk

- Three primary steps to quantitative risk analysis are:
  1. Estimate potential losses
  2. Conduct a threat analysis
  3. Determine annual loss expectancy
- Aggregate the risk within the organization by comparing countermeasure metrics to quantitative risk scores
- Information Assurance plans should detail how risk is identified, quantified, and tracked
- As mitigation efforts proceed, total risk should decrease in a tangible way

Standard Certification Tools

- Certification tools can help track risk and countermeasures for top-down visibility
- Automated tools act as a tracking mechanism
- Must weigh cost of tool versus value added

Certification Tools

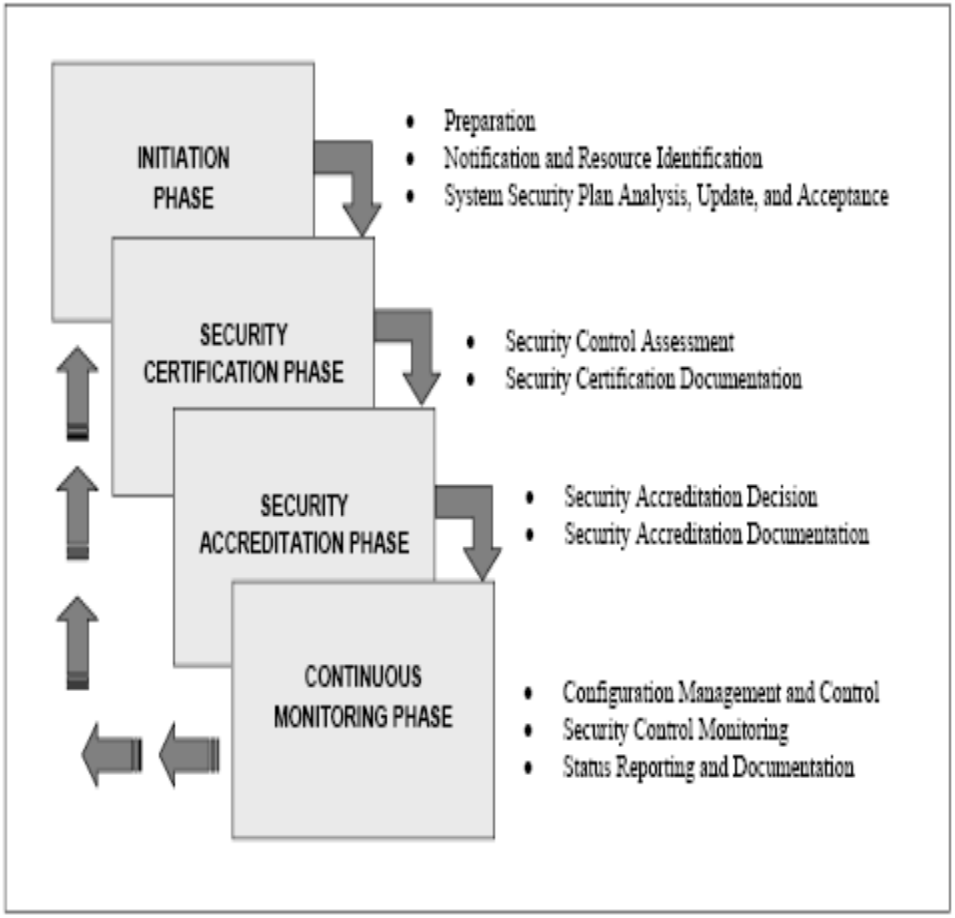


FIGURE 3.1 SECURITY CERTIFICATION AND ACCREDITATION PROCESS

- **The security certification and accreditation process consists of four distinct phases:**
1. **Initiation Phase**
2. **Security Certification Phase**
3. **Security Accreditation Phase**
4. **Continuous Monitoring Phase.**
- **Both technical and non-technical features are evaluated**

Understand and apply threat modeling

Dr. Drew Hamilton

Vulnerability and Attack Avenues Duties

- General
- Developing Attack Avenues
- Characterizing Vulnerabilities
- Researching Vulnerability Report
- Collecting and Reviewing Vulnerabilities
- Comparing and Contrasting Attack Avenues
- Risk of Detection and Response
- Technology Necessary to Mount Attack

Key References

- NIST SP800-30: Risk Management Guide for IT
- NIST SP800-42: Guideline on Network Security Testing
- NIST SP800-53: Recommended Security Controls for Federal Information Systems
- SP800-61: Computer Security Incident Handling Guide
- FIPS-PUB-199: Standards for Security Categorization of Federal Information and Information Systems

Section A - E: Risk Assessments, Avenues of Attack, and Vulnerabilities

- Risk assessment is the first process in the risk management methodology.
- Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its SDLC.
- The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process, as discussed later.
- *Risk* is a function of the *likelihood* of a given *threat-source's* exercising a particular potential *vulnerability*, and the resulting *impact* of that adverse event on the organization.
- To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system.
- Impact refers to the magnitude of harm that could be caused by a threat's exercise of a vulnerability.
- The level of impact is governed by the potential mission impacts and in turn produces a relative value for the IT assets and resources affected (e.g., the criticality and sensitivity of the IT system components and data).

- **The risk assessment methodology encompasses nine primary steps:**
  - **Step 1: System Characterization**
  - **Step 2: Threat Identification**
  - **Step 3: Vulnerability Identification**
  - **Step 4: Control Analysis**
  - **Step 5: Likelihood Determination**
  - **Step 6: Impact Analysis**
  - **Step 7: Risk Determination**
  - **Step 8: Control Recommendations**
  - **Step 9: Results Documentation**

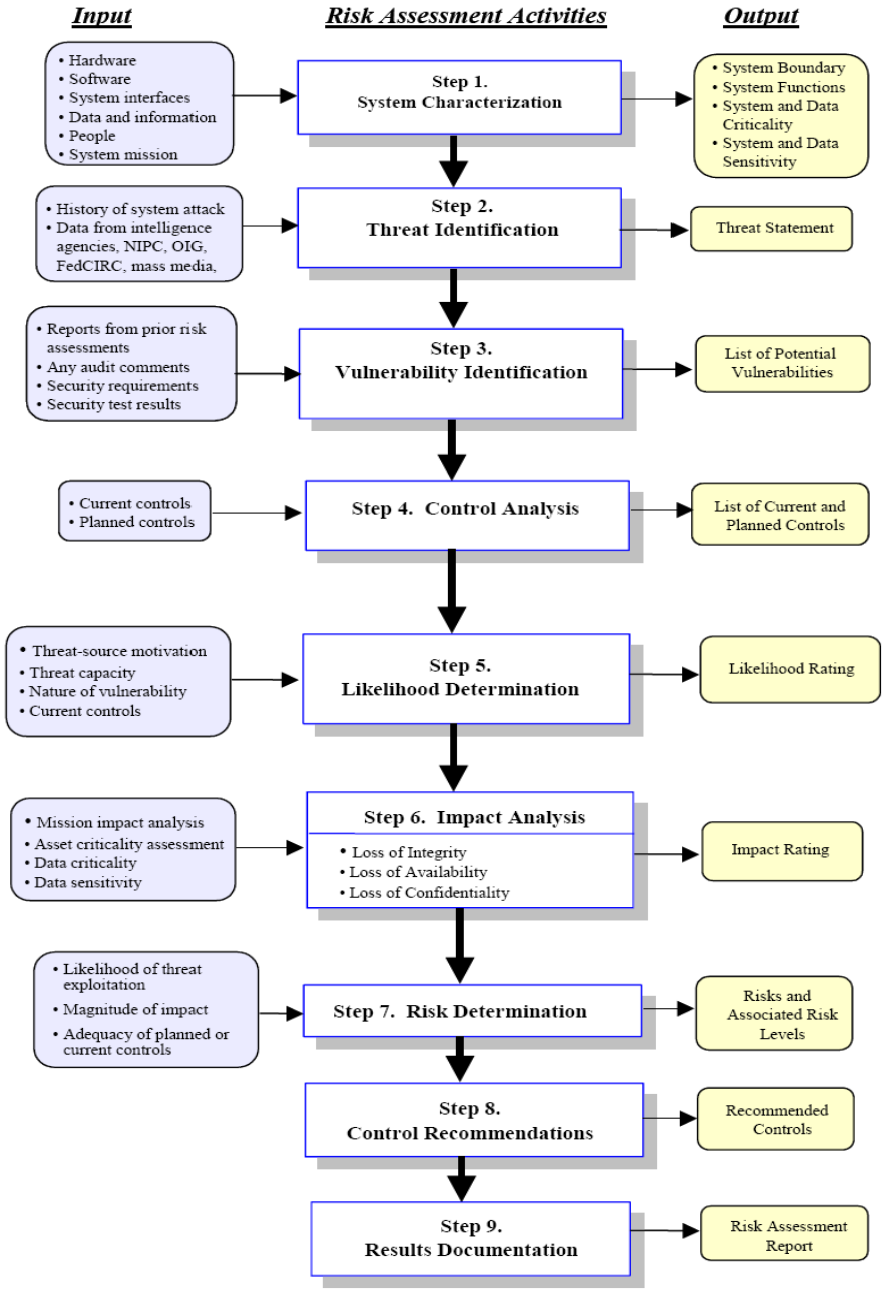


Figure 3-1. Risk Assessment Methodology Flowchart

Risk Assessment/Boundary Definition

- In assessing risks for an IT system, the first step is to define the scope of the effort. In this step, the boundaries of the IT system are identified, along with the resources and the information that constitute the system.
- Characterizing an IT system establishes the scope of the risk assessment effort, delineates the operational authorization (or accreditation) boundaries, and provides information (e.g., hardware, software, system connectivity, and responsible division or support personnel) essential to defining the risk.
- The methodology described can be applied to assessments of single or multiple, interrelated systems. In the latter case, it is important that the domain of interest and all interfaces and dependencies be well defined prior to applying the methodology.

Risk Assessment

- Identifying risk for an IT system requires a keen understanding of the system's processing environment. The person or persons who conduct the risk assessment must therefore first collect system-related information, which is usually classified as follows:
  - Hardware
  - Software
  - System interfaces
    - (e.g., internal and external connectivity)
  - Data and information
  - Persons who support and use the IT system
  - System mission
    - (e.g., the processes performed by the IT system)
  - System and data criticality
    - (e.g., the system's value or importance to an organization)
  - System and data sensitivity.

Risk Assessment

- **Additional information related to the operational environmental of the IT system and its data includes, but is not limited to, the following:**
- **The functional requirements of the IT system**
- **Users of the system (system users providing technical support to the IT system; application users who use the IT system to perform business functions)**
- **System security policies governing the IT system (organizational policies, federal requirements, laws, industry practices)**
- **System security architecture**
- **Current network topology (e.g., network diagram)**
- **Information storage protection that safeguards system and data availability, integrity, and confidentiality**
- **Flow of information pertaining to the IT system (e.g., system interfaces, system input and output flowchart)**

Risk Assessment

- Technical controls used for the IT system (e.g., built-in or add-on security product that supports identification and authentication, discretionary or mandatory access control, audit, residual information protection, encryption methods)
- Management controls used for the IT system (e.g., rules of behavior, security planning)Operational controls used for the IT system (e.g., personnel security, backup, contingency, and resumption and recovery operations; system maintenance; off-site storage; user account establishment and deletion procedures; controls for segregation of user functions, such as privileged user access versus standard user access)
- Physical security environment of the IT system (e.g., facility security, data center policies)
- Environmental security implemented for the IT system processing environment (e.g., controls for humidity, water, power, pollution, temperature, and chemicals).

IT System Security

- For a system that is in the initiation or design phase, system information can be derived from the design or requirements document.
- For an IT system under development, it is necessary to define key security rules and attributes planned for the future IT system.
- System design documents and the system security plan can provide useful information about the security of an IT system that is in development.
- For an operational IT system, data is collected about the IT system in its production environment, including data on system configuration, connectivity, and documented and undocumented procedures and practices.
- Therefore, the system description can be based on the security provided by the underlying infrastructure or on future security plans for the IT system.

IT Information-Gathering Techniques

- Any, or a combination, of the following techniques can be used in gathering information relevant to the IT system within its operational boundary:
- **Questionnaire.** To collect relevant information, risk assessment personnel can develop a questionnaire concerning the management and operational controls planned or used for the IT system.
  - This questionnaire should be distributed to the applicable technical and nontechnical management personnel who are designing or supporting the IT system. The questionnaire could also be used during on-site visits and interviews.
- **On-site Interviews.** Interviews with IT system support and management personnel can enable risk assessment personnel to collect useful information about the IT system (e.g., how the system is operated and managed).
  - On-site visits also allow risk assessment personnel to observe and gather information about the physical, environmental, and operational security of the IT system

IT Information-Gathering Techniques (2)

- **Document Review.** Policy documents (e.g., legislative documentation, directives), system documentation (e.g., system user guide, system administrative manual, system design and requirement document, acquisition document), and security-related documentation (e.g., previous audit report, risk assessment report, system test results, system security plan, security policies) can provide good information about the security controls used by and planned for the IT system.
  - An organization's mission impact analysis or asset criticality assessment provides information regarding system and data criticality and sensitivity.
- **Use of Automated Scanning Tool.** Proactive technical methods can be used to collect system information efficiently.
  - For example, a network mapping tool can identify the services that run on a large group of hosts and provide a quick way of building individual profiles of the target IT system(s).

Threat Identification

- **Threat: The potential for a threat source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.**
- **Threat-Source: Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.**
- **The goal of this step is to identify the potential threat-sources and compile a threat statement listing potential threat-sources that are applicable to the IT system being evaluated.**

Threat-Source Identification (2)

- In assessing threat-sources, it is important to consider all potential threat-sources that could cause harm to an IT system and its processing environment. For example, although the threat statement for an IT system located in a desert may not include "natural flood" because of the low likelihood of such an event's occurring, environmental threats such as a bursting pipe can quickly flood a computer room and cause damage to an organization's IT assets and resources. Humans can be threat-sources through intentional acts, such as deliberate attacks by malicious persons or disgruntled employees, or unintentional acts, such as negligence and errors.
- A deliberate attack can be either (1) a malicious attempt to gain unauthorized access to an IT system (e.g., via password guessing) in order to compromise system and data integrity, availability, or confidentiality or (2) a benign, but nonetheless purposeful, attempt to circumvent system security. One example of the latter type of deliberate attack is a programmer's writing a Trojan horse program to bypass system security in order to "get the job done."

Threat Sources

Table 3-1. Human Threats: Threat-Source, Motivation, and Threat Actions

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Threat-Sources (2)

- An estimate of the motivation, resources, and capabilities that may be required to carry out a successful attack should be developed after the potential threat-sources have been identified, in order to determine the likelihood of a threat's exercising a system vulnerability, as described later.
- The threat statement, or the list of potential threat-sources, should be tailored to the individual organization and its processing environment (e.g., end-user computing habits).
- In general, information on natural threats (e.g., floods, earthquakes, storms) should be readily available.
- Known threats have been identified by many government and private sector organizations.

Threat-sources (3)

- Intrusion detection tools also are becoming more prevalent, and government and industry organizations continually collect data on security events, thereby improving the ability to realistically assess threats. Sources of information include, but are not limited to, the following:
- Intelligence agencies (for example, the Federal Bureau of Investigation's National Infrastructure Protection Center)
- Federal Computer Incident Response Center (FedCIRC)
- Mass media, particularly Web-based resources such as SecurityFocus.com, SecurityWatch.com, SecurityPortal.com, and SANS.org.

Output from Step 2: A threat statement containing a list of threat-sources that could exploit system vulnerabilities

Vulnerabilities

- **Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.**
- **The analysis of the threat to an IT system must include an analysis of the vulnerabilities associated with the system environment.**
- **The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources.**

Vulnerabilities (2)

Vulnerability	Threat-Source	Threat Action
Terminated employees' system identifiers (ID) are not removed from the system	Terminated employees	Dialing into the company's network and accessing company proprietary data
Company firewall allows inbound telnet, and *guest* ID is enabled on XYZ server	Unauthorized users (e.g., hackers, terminated employees, computer criminals, terrorists)	Using telnet to XYZ server and browsing system files with the *guest* ID
The vendor has identified flaws in the security design of the system; however, new patches have not been applied to the system	Unauthorized users (e.g., hackers, disgruntled employees, computer criminals, terrorists)	Obtaining unauthorized access to sensitive system files based on known system vulnerabilities
Data center uses water sprinklers to suppress fire; tarpaulins to protect hardware and equipment from water damage are not in place	Fire, negligent persons	Water sprinklers being turned on in the data center

Vulnerabilities (3)

- Recommended methods for identifying system vulnerabilities are the use of vulnerability sources, the performance of system security testing, and the development of a security requirements checklist.
- It should be noted that the types of vulnerabilities that will exist, and the methodology needed to determine whether the vulnerabilities are present, will usually vary depending on the nature of the IT system and the phase it is in, in the SDLC:
- If the IT system has not yet been designed, the search for vulnerabilities should focus on the organization's security policies, planned security procedures, and system requirement definitions, and the vendors' or developers' security product analyses (e.g., white papers).
- If the IT system is being implemented, the identification of vulnerabilities should be expanded to include more specific information, such as the planned security features described in the security design documentation and the results of system certification test and evaluation.
- If the IT system is operational, the process of identifying vulnerabilities should include an analysis of the IT system security features and the security controls, technical and procedural, used to protect the system.

Vulnerability Sources

- The technical and nontechnical vulnerabilities associated with an IT system's processing environment can be identified via the information-gathering techniques.
- A review of other industry sources (e.g., vendor Web pages that identify system bugs and flaws) will be useful in preparing for the interviews and in developing effective questionnaires to identify vulnerabilities that may be applicable to specific IT systems (e.g., a specific version of a specific operating system).
- The Internet is another source of information on known system vulnerabilities posted by vendors, along with hot fixes, service packs, patches, and other remedial measures that may be applied to eliminate or mitigate vulnerabilities.
- Documented vulnerability sources that should be considered in a thorough vulnerability analysis include, but are not limited to, the following (next slide):

Vulnerability Sources (2)

- Previous risk assessment documentation of the IT system assessed the IT system's audit reports, system anomaly reports, security review reports, and system test and evaluation reports
- Vulnerability lists, such as the NIST I-CAT vulnerability database (http://icat.nist.gov)
- Security advisories, such as FedCIRC and the Department of Energy's Computer Incident Advisory Capability bulletins
- Vendor advisories
- Commercial computer incident/emergency response teams and post lists (e.g., SecurityFocus.com forum mailings)
- Information Assurance Vulnerability Alerts and bulletins for military systems
- System software security analyses.

System Security Testing

- Proactive methods, employing system testing, can be used to identify system vulnerabilities efficiently, depending on the criticality of the IT system and available resources (e.g., allocated funds, available technology, persons with the expertise to conduct the test). Test methods include
    1. Automated vulnerability scanning tool
    2. Security test and evaluation (ST&E)
    3. Penetration testing.
- The automated vulnerability scanning tool is used to scan a group of hosts or a network for known vulnerable services (e.g., system allows anonymous File Transfer Protocol [FTP], sendmail relaying).
- However, it should be noted that some of the *potential* vulnerabilities identified by the automated scanning tool may not represent real vulnerabilities in the context of the system environment.
- For example, some of these scanning tools rate potential vulnerabilities without considering the site's environment and requirements.
- Some of the "vulnerabilities" flagged by the automated scanning software may actually not be vulnerable for a particular site but may be configured that way because their environment requires it.
- Thus, this test method may produce false positives.

System Security Testing (2)

- ST&E is another technique that can be used in identifying IT system vulnerabilities during the risk assessment process. It includes the development and execution of a test plan (e.g., test script, test procedures, and expected test results).
- The purpose of system security testing is to test the effectiveness of the security controls of an IT system as they have been applied in an operational environment.
- The objective is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standards.
- Penetration testing can be used to complement the review of security controls and ensure that different facets of the IT system are secured.
- Penetration testing, when employed in the risk assessment process, can be used to assess an IT system's ability to withstand intentional attempts to circumvent system security. Its objective is to test the IT system from the viewpoint of a threat-source and to identify potential failures in the IT system protection schemes.
- The results of these types of optional security testing will help identify a system's vulnerabilities.

(Note: SP800-42 provides additional information on vulnerability testing using automated tools).

Development of Security Requirements Checklist

Step 3:

- During this step, the risk assessment personnel determine whether the security requirements stipulated for the IT system and collected during system characterization are being met by existing or planned security controls.
- Typically, the system security requirements can be presented in table form, with each requirement accompanied by an explanation of how the system's design or implementation does or does not satisfy that security control requirement.
- A security requirements checklist contains the basic security standards that can be used to systematically evaluate and identify the vulnerabilities of the assets (personnel, hardware, software, information), non-automated procedures, processes, and information transfers associated with a given IT system in the following security areas:
  - Management
  - Operational
  - Technical.

Table 3-3 lists security criteria suggested for use in identifying an IT system's vulnerabilities in each security area.

Additional Security Guidance can be obtained from NIST-SP-800-53.

Table 3-3. Security Criteria

Security Area	Security Criteria
Management Security	• Assignment of responsibilities • Continuity of support • Incident response capability • Periodic review of security controls • Personnel clearance and background investigations • Risk assessment • Security and technical training • Separation of duties • System authorization and reauthorization • System or application security plan
Operational Security	• Control of air-borne contaminants (smoke, dust, chemicals) • Controls to ensure the quality of the electrical power supply • Data media access and disposal • External data distribution and labeling • Facility protection (e.g., computer room, data center, office) • Humidity control • Temperature control • Workstations, laptops, and stand-alone personal computers
Technical Security	• Communications (e.g., dial-in, system interconnection, routers) • Cryptography • Discretionary access control • Identification and authentication • Intrusion detection • Object reuse • System audit

Development of Security Requirements Checklist (2)

The outcome of this process is the security requirements checklist. Sources that can be used in compiling such a checklist include, but are not limited to, the following government regulatory and security directives and sources applicable to the IT system processing environment:

- CSA of 1987
- Federal Information Processing Standards Publications
- OMB November 2000 Circular A-130
- Privacy Act of 1974
- System security plan of the IT system assessed
- The organization's security policies, guidelines, and standards
- Industry practices.

The NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*, provides an extensive questionnaire containing specific control objectives against which a system or group of interconnected systems can be tested and measured.

The control objectives are abstracted directly from long-standing requirements found in statute, policy, and guidance on security and privacy.

The results of the checklist (or questionnaire) can be used as input for an evaluation of compliance and noncompliance. This process identifies system, process, and procedural weaknesses that represent potential vulnerabilities.

Output from Step 3: A list of the system vulnerabilities (observations)7 that could be exercised by the potential threat-sources.

Control Analysis

Step 4:

- **The goal of this step is to analyze the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability.**

- **To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the implementation of current or planned controls must be considered.**

- **For example, a vulnerability (e.g., system or procedural weakness) is not likely to be exercised or the likelihood is low if there is a low level of threat-source interest or capability or if there are effective security controls that can eliminate, or reduce the magnitude of, harm.**

Control Analysis (2)

- Control Methods
  - Security controls encompass the use of technical and non-technical methods.
  - Technical controls are safeguards that are incorporated into computer hardware, software, or firmware (e.g., access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software).
  - Non-technical controls are management and operational controls, such as security policies; operational procedures; and personnel, physical, and environmental security.
- Control Categories

The control categories for both technical and non-technical control methods can be further classified as either preventive or detective. These two subcategories are explained as follows:

- Preventive controls inhibit attempts to violate security policy and include such controls as access control enforcement, encryption, and authentication.
- Detective controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums.

The implementation of such controls during the risk mitigation process is the direct result of the identification of deficiencies in current or planned controls during the risk assessment process (e.g., controls are not in place or controls are not properly implemented).

Control Analysis (3)

Control Analysis Technique

- **As discussed, development of a security requirements checklist or use of an available checklist will be helpful in analyzing controls in an efficient and systematic manner.**
- **The security requirements checklist can be used to validate security noncompliance as well as compliance.**
- **Therefore, it is essential to update such checklists to reflect changes in an organization's control environment (e.g., changes in security policies, methods, and requirements) to ensure the checklist's validity.**

Output from Step 4: List of current or planned controls used for the IT system to mitigate the likelihood of a vulnerability's being exercised and reduce the impact of such an adverse event.

Likelihood Determination

Step 5:

- **To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered:**
  - **Threat-source motivation and capability**
  - **Nature of the vulnerability**
  - **Existence and effectiveness of current controls.**
- **The likelihood that a potential vulnerability could be exercised by a given threat-source can be described as high, medium, or low.**

Output from Step 5: Likelihood rating (High, Medium, Low)

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Impact Analysis

Step 6:

- **The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of a vulnerability. Before beginning the impact analysis, it is necessary to obtain the following information as discussed previously:**
  - **1. System mission (e.g., the processes performed by the IT system)**
  - **2. System and data criticality (e.g., the system's value or importance to an organization)**
  - **3. System and data sensitivity.**
- **This information can be obtained from existing organizational documentation, such as the mission impact analysis report or asset criticality assessment report. A mission impact analysis (also known as business impact analysis [BIA] for some organizations) prioritizes the impact levels associated with the compromise of an organization's information assets based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets.**
- **An asset criticality assessment identifies and prioritizes the sensitive and critical organization information assets (e.g., hardware, software, systems, services, and related technology assets) that support the organization's critical missions.**

Impact Analysis (2)

- If this documentation does not exist or such assessments for the organization's IT assets have not been performed, the system and data sensitivity can be determined based on the level of protection required to maintain the system and data's availability, integrity, and confidentiality.
- Regardless of the method used to determine how sensitive an IT system and its data are, the system and information owners are the ones responsible for determining the impact level for their own system and information. Consequently, in analyzing impact, the appropriate approach is to interview the system and information owner(s).
- Therefore, the adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals: integrity, availability, and confidentiality. The following list provides a brief description of each security goal and the consequence (or impact) of its not being met:

1. **Loss of Integrity.** System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.
2. **Loss of Availability.** If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.
3. **Loss of Confidentiality**. System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

Impact Analysis (3)

- **Some tangible impacts can be measured quantitatively in lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action.**

- **Other impacts (e.g., loss of public confidence, loss of credibility, damage to an organization's interest) cannot be measured in specific units but can be qualified or described in terms of high, medium, and low impacts.**

Table 3-5. Magnitude of Impact Definitions

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Impact Analysis (4)

Quantitative versus Qualitative Assessment

- **In conducting the impact analysis, consideration should be given to the advantages and disadvantages of quantitative versus qualitative assessments.**
- **The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.**
- **The disadvantage of the qualitative analysis is that it does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-benefit analysis of any recommended controls difficult.**
- **The major advantage of a quantitative impact analysis is that it provides a measurement of the impacts' magnitude, which can be used in the cost-benefit analysis of recommended controls.**
- **The disadvantage is that, depending on the numerical ranges used to express the measurement, the meaning of the quantitative impact analysis may be unclear, requiring the result to be interpreted in a qualitative manner.**
- **Additional factors often must be considered to determine the magnitude of impact. These may include, but are not limited to— An estimation of the frequency of the threat-source's exercise of the vulnerability over a specified time period (e.g., 1 year)**
- **An approximate cost for each occurrence of the threat-source's exercise of the vulnerability**
- **A weighted factor based on a subjective analysis of the relative impact of a specific threat's exercising a specific vulnerability.**

Output from Step 6: Magnitude of impact (High, Medium, or Low)

Risk Determination

Step 7:

The purpose of this step is to assess the level of risk to the IT system. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of:

- **The likelihood of a given threat-source's attempting to exercise a given vulnerability**
- **The magnitude of the impact should a threat-source successfully exercise the vulnerability**
- **The adequacy of planned or existing security controls for reducing or eliminating risk.**

To measure risk, a risk scale and a risk-level matrix must be developed.

Risk Determination (2)

- **The sample matrix in Table 3-6 shows how the overall risk levels of High, Medium, and Low are derived. The determination of these risk levels or ratings may be subjective. The rationale for this justification can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level. For example, The probability assigned for each threat likelihood level is 1.0 for High, 0.5 for Medium, 0.1 for Low The value assigned for each impact level is 100 for High, 50 for Medium, and 10 for Low.**

Table 3-6. Risk-Level Matrix

Threat Likelihood	Impact		
	Low (10)	***Medium*** (50)	***High*** (100)
High (1.0)	**Low** 10 X 1.0 = 10	**Medium** 50 X 1.0 = 50	**High** 100 X 1.0 = 100
Medium (0.5)	**Low** 10 X 0.5 = 5	**Medium** 50 X 0.5 = 25	**Medium** 100 X 0.5 = 50
Low (0.1)	**Low** 10 X 0.1 = 1	**Low** 50 X 0.1 = 5	**Low** 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

Risk Determination (3)

Description of Risk Level

Table 3-7 describes the risk levels shown in the above matrix. This risk scale, with its ratings of High, Medium, and Low, represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk scale also presents actions that senior management, the mission owners, must take for each risk level.

Output from Step 7: Risk level (High, Medium, Low)

Table 3-7. Risk Scale and Necessary Actions

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.

Control Recommendations

Step 8:

- During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, are provided. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:
  - Effectiveness of recommended options (e.g., system compatibility)
  - Legislation and regulation
  - Organizational policy
  - Operational impact
  - Safety and reliability
- The control recommendations are the results of the risk assessment process and provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.
- It should be noted that not all possible recommended controls can be implemented to reduce loss.
- To determine which ones are required and appropriate for a specific organization, a cost-benefit analysis, as discussed later, should be conducted for the proposed recommended controls, to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. In addition, the operational impact (e.g., effect on system performance) and feasibility (e.g., technical requirements, user acceptance) of introducing the recommended option should be evaluated carefully during the risk mitigation process.
- *Output from Step 8: Recommendation of control(s) and alternative solutions to mitigate risk*

Results Documentation

Step 9:

- **Once the risk assessment has been completed (threat-sources and vulnerabilities identified, risks assessed, and recommended controls provided), the results should be documented in an official report or briefing.**
- **A risk assessment report is a management report that helps senior management, the mission owners, make decisions on policy, procedural, budget, and system operational and management changes.**
- **Unlike an audit or investigation report, which looks for wrongdoing, a risk assessment report should not be presented in an accusatory manner but as a systematic and analytical approach to assessing risk so that senior management will understand the risks and allocate resources to reduce and correct potential losses. For this reason, some people prefer to address the threat/vulnerability pairs as observations instead of findings in the risk assessment report.**
- **Appendix B provides a suggested outline for the risk assessment report.**
- ***Output from Step 9*: *Risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation***

Cost/Benefit Analysis

- Cost analysis of data protection versus cost of data loss or compromise
- SP800-30: Risk Management Guide for IT Systems, pgs. 37-39

- Annualized Rate of Occurrence (ARO)
- Single Loss Expectancy (SLE) =
  SLE = Asset Value in $ X Exposure Factor
- Annualize Loss Expectancy (ALE) =
  ALE = SLE X ARO

Security Objectives

- **The FISMA defines three security objectives for information and information systems:**

1. **CONFIDENTIALITY**

   "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]

   A loss of *confidentiality* is the unauthorized disclosure of information.

2. **INTEGRITY**

   "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

   A loss of *integrity* is the unauthorized modification or destruction of information.

3. **AVAILABILITY**

   "Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]

   A loss of *availability* is the disruption of access to or use of information or an information system. [FIPS-PUB-199]

Potential Impact (Low)

FIPS Publication 199 defines three levels of *potential impact* on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organization and the overall national interest.

The *potential impact* is LOW if—

− The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

Potential Impact (Moderate)

The *potential impact* is MODERATE if—

- **The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.**

AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

[FIPS-PUB-199]

Potential Impact (High)

The *potential impact* is HIGH if—

- **The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.**

AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

[FIPS-PUB-199]

Potential Impact Definitions for Security Objectives

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Cost/Benefit Analysis (1)

- To allocate resources and implement cost-effective controls, organizations, after identifying all possible controls and evaluating their feasibility and effectiveness, should conduct a cost-benefit analysis for each proposed control to determine which controls are required and appropriate for their circumstances.
- The cost-benefit analysis can be qualitative or quantitative. Its purpose is to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk.
- For example, the organization may not want to spend $1,000 on a control to reduce a $200 risk.
- A cost-benefit analysis for proposed new controls or enhanced controls encompasses the following:
  - Determining the impact of implementing the new or enhanced controls
  - Determining the impact of *not* implementing the new or enhanced controls
  - Estimating the costs of the implementation.– Hardware and software purchases
    - – Reduced operational effectiveness if system performance or functionality is
    - reduced for increased security
    - – Cost of implementing additional policies and procedures
    - – Cost of hiring additional personnel to implement proposed policies, procedures, or
    - services
    - – Training costs
    - – Maintenance costs

[SP 800-30 Page 38]

Cost/Benefit Analysis (2)

- Assessing the implementation costs and benefits against system and data criticality to determine the importance to the organization of implementing the new controls, given their costs and relative impact.
- The organization will need to assess the benefits of the controls in terms of maintaining an acceptable mission posture for the organization. Just as there is a cost for implementing a needed control, there is a cost for not implementing it. By relating the result of not implementing the control to the mission, organizations can determine whether it is feasible to forgo its implementation.

Cost-Benefit Analysis Example: System X stores and processes mission-critical and sensitive employee privacy information; however, auditing has not been enabled for the system. A cost/benefit analysis is conducted to determine whether the audit feature should be enabled for System X.

- Items (1) and (2) address the intangible impact (e.g., deterrence factors) for implementing or not implementing the new control.
- Item (3) lists the tangibles (e.g., actual cost).

(1) Impact of enabling system audit feature: The system audit feature allows the system security administrator to monitor users' system activities but will slow down system performance and therefore affect user productivity. Also the implementation will require additional resources, as described in Item 3.

(2) Impact of not enabling system audit feature: User system activities and violations cannot be monitored and tracked if the system audit function is disabled, and security cannot be maximized to protect the organization's confidential data and mission.

[SP 800-30 Page 39]

Cost/Benefit Analysis (3)

(3) Cost estimation for enabling the system audit feature:

- Cost for enabling system audit feature—No cost, built-in feature $ 0
- Additional staff to perform audit review and archive, per year $ XX,XXX
- Training (e.g., system audit configuration, report generation) $ X,XXX
- Add-on audit reporting software $ X,XXX
- Audit data maintenance (e.g., storage, archiving), per year $ X,XXX
- Total Estimated Costs $ XX,XXX

- The organization's managers must determine what constitutes an acceptable level of mission risk.
- The impact of a control may then be assessed, and the control either included or excluded, after the organization determines a range of feasible risk levels. This range will vary among organizations; however, the following rules apply in determining the use of new controls:
  - If control would reduce risk more than needed, then see whether a less expensive alternative exists
  - If control would cost more than the risk reduction provided, then find something else
  - If control does not reduce risk sufficiently, then look for more controls or a different control
  - If control provides enough risk reduction and is cost-effective, then use it.
- Frequently the cost of implementing a control is more tangible than the cost of not implementing it.
- As a result, senior management plays a critical role in decisions concerning the implementation of control measures to protect the organizational mission.

Jamming

- DoS and DDoS attacks cause in the loss of network availability and “usability upon demand” for authorized users and devices.
- DoS attacks block authorized user access to system resources and network applications.
- Besides the typical DoS attacks (e.g., those involving flooding techniques) directed against LANs and Internet services, Bluetooth devices are also susceptible to signal jamming. Bluetooth devices share bandwidth with microwave ovens, cordless phones, and other wireless networks and thus are vulnerable to interference.
- Malicious users can interfere with the flow of information (i.e., disrupt the routing protocol by feeding the network inaccurate information) by using devices that transmit in the 2.4 GHz ISM band.
- Disrupting the routing protocol prevents ad hoc network devices from negotiating the network’s dynamic topologies. Remote users may encounter jamming more frequently than on-site users.
- Remote users must contend with the same interference that users experience in the office. Further, since the remote environment is uncontrolled, remote devices are more likely to be in close proximity to devices (e.g., other Bluetooth and ISM band devices) that are intentionally or unintentionally jamming their signals.
- Another threat associated with ad hoc devices is a battery exhaustion attack. This attack attempts to disable a device by draining its battery. A malicious user continually sends requests to the device asking for data transfers (assuming the user is part of the network topology) or asking the device to create a network
- Although this type of attack does not compromise network security, it ultimately prevents the user from gaining access to the network, because the device cannot function.

[SP-800-48]

Risk Management Methodology

- Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions.
- This process is not unique to the IT environment; indeed it pervades decision-making in all areas of our daily lives.
- Take the case of home security, for example. Many people decide to have home security systems installed and pay a monthly fee to a service provider to have these systems monitored for the better protection of their property. Presumably, the homeowners have weighed the cost of system installation and monitoring against the value of their household goods and their family's safety, a fundamental "mission" need.
- The head of an organizational unit must ensure that the organization has the capabilities needed to accomplish its mission.
- These mission owners must determine the security capabilities that their IT systems must have to provide the desired level of mission support in the face of real world threats.
- Most organizations have tight budgets for IT security; therefore, IT security spending must be reviewed as thoroughly as other management decisions.
- A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities.

Avenues of Attacks

Avenues of Attacks:

+ Denial of Service—an attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources

+ Malicious Code—a virus, worm, Trojan horse, or other code-based malicious entity that infects a host

+ Unauthorized Access—a person gains logical or physical access without permission to a network, system, application, data, or other resource

+ Inappropriate Usage—a person violates acceptable computing use policies

+ Multiple Component—a single incident that encompasses two or more incidents.

- **[sp800-61]**

Preventing Denial of Service Attacks

- Configure firewall rule sets to prevent reflector attacks. Most reflector attacks can be stopped through network-based and host-based firewall rule sets that reject suspicious combinations of source and destination ports.
- Configure border routers to prevent amplifier attacks. Amplifier attacks can be blocked by configuring border routers not to forward directed broadcasts.
- Determine how the organization's ISPs and second-tier providers can assist in handling network-based DoS attacks. ISPs can often filter or limit certain types of traffic, slowing or halting a DoS attack. They can also provide logs of DoS traffic and may be able to assist in tracing the source of the attack. The organization should meet with the ISPs in advance to establish procedures for requesting such assistance.
- Configure security software to detect DoS attacks. Intrusion detection software can detect many types of DoS activity. Establishing network and system activity baselines, and monitoring for significant deviations from those baselines, can also be useful in detecting attacks.
- Configure the network perimeter to deny all incoming and outgoing traffic that is not expressly permitted. By restricting the types of traffic that can enter and leave the environment, the organization will limit the methods that attackers can use to perform DoS attacks.
- Create a containment strategy that includes several solutions in sequence.
- The decision-making process for containing DoS incidents is easier if recommended solutions are predetermined. Because the effectiveness of each possible solution will vary among incidents, organizations should select several solutions and determine in which order the solutions should be attempted.

Preventing Malicious Code Issues

- Make users aware of malicious code issues. Users should be familiar with the methods that malicious code uses to propagate and the symptoms of infections. Holding regular user education sessions helps to ensure that users are aware of the risks that malicious code poses. Teaching users how to safely handle e-mail attachments should reduce the number of infections that occur.
- Read antivirus bulletins. Bulletins regarding new malicious code threats provide timely information to incident handlers.
- Deploy host-based intrusion detection systems, including file integrity checkers, to critical hosts. Host-based IDS software, particularly file integrity checkers, can detect signs of malicious code incidents, such as configuration changes and modifications to executables.
- Use antivirus software, and keep it updated with the latest virus signatures. Antivirus software should be deployed to all hosts and all applications that may be used to transfer malicious code. The software should be configured to detect and disinfect or quarantine malicious code infections. All antivirus software should be kept current.
- Configure software to block suspicious files. Files that are very likely to be malicious should be blocked from the environment, such as those with file extensions that are usually associated with malicious code, as well as files with suspicious combinations of file extensions.
- Eliminate open Windows shares. Many worms spread through unsecured shares on hosts running Windows. A single infection may rapidly spread to hundreds or thousands of hosts through unsecured shares.
- Contain malicious code incidents as quickly as possible. Because malicious code works surreptitiously and can propagate to other systems rapidly, early containment of a malicious code incident is needed to stop it from spreading and causing further damage. Infected systems should be disconnected from the network immediately. Organizations may need to block malicious code at the e-mail server level, or even temporarily suspend e-mail services to gain control over serious e-mail-borne malicious code incidents.

Preventing Unauthorized Access

- Configure intrusion detection software to alert on attempts to gain unauthorized access. Network and host-based intrusion detection software (including file integrity checking software) is valuable for detecting attempts to gain unauthorized access. Each type of software may detect incidents that the other types of software cannot, so the use of multiple types of computer security software is highly recommended.
- Configure all hosts to use centralized logging. Incidents are easier to detect if data from all hosts across the organization is stored in a centralized, secured location.
- Establish procedures for having all users change their passwords. A password compromise may force the organization to require all users of an application, system, or trust domain—or perhaps the entire organization—to change their passwords.
- Configure the network perimeter to deny all incoming traffic that is not expressly permitted. By limiting the types of incoming traffic, attackers should be able to reach fewer targets and should be able to reach the targets using designated protocols only. This should reduce the number of unauthorized access incidents.
- Secure all remote access methods, including modems and VPNs. Unsecured modems provide easily attainable unauthorized access to internal systems and networks. Remote access clients are often outside the organization's control, so granting them access to resources increases risk.
- Put all publicly accessible services on secured DMZ network segments. This permits the organization to allow external hosts to initiate connections to hosts on the DMZ segments only, not to hosts on internal network segments. This should reduce the number of unauthorized access incidents.

Preventing Inappropriate Usage

- Processes for monitoring and logging user activities should comply with the organization's policies and all applicable laws. Procedures for handling incidents that directly involve employees should incorporate discretion and confidentiality.
- Liability issues may arise during inappropriate usage incidents, particularly for incidents that are targeted at outside parties. Incident handlers should understand when they should discuss incidents with the allegedly attacked party and what information they should reveal.
- Intrusion detection software has built-in capabilities to detect certain inappropriate usage incidents, such as the use of unauthorized services, outbound reconnaissance activity and attacks, and improper e-mail relay usage (e.g., sending spam).
- Basic information on user activities (e.g., FTP commands, Web requests, and e-mail headers) may be valuable for investigative and evidentiary purposes.
- Configure all e-mail servers so they cannot be used for unauthorized mail relaying. Mail relaying is commonly used to send spam.
- Spam filtering software can block much of the spam sent by external parties to the organization's users, as well as spam sent by internal users.
- URL filtering software prevents access to many inappropriate Web sites. Users should be required to use the software, typically by preventing access to external Web sites unless the traffic passes through a server that performs URL filtering.

Preventing Multiple Component Compromise

- Use centralized logging and event correlation software. Incident handlers should identify an incident as having multiple components more quickly if all precursors and indications are accessible from a single point of view.
- Contain the initial incident and then search for signs of other incident components. It can take an extended period of time for a handler to authoritatively determine that an incident has only a single component; meanwhile, the initial incident has not been contained. It is usually better to contain the initial incident first.
- Separately prioritize the handling of each incident component. Resources are probably too limited to handle all incident components simultaneously. Components should be prioritized based on response guidelines for each component and how current each component is.

Attacker Payoff for an Incident

Prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process. Incidents should not be handled on a first-come, first-served basis as a result of resource limitations. Instead, handling should be prioritized based on two factors:

- **+ Current and Potential Technical Effect of the Incident. Incident handlers should consider not only the current negative technical effect of the incident (e.g., unauthorized user-level access to data), but also the likely future technical effect of the incident if it is not immediately contained (e.g., root compromise). For example, a worm spreading among workstations may currently cause a minor impact, but within a few hours the worm traffic may cause a major network outage.**
- **+ Criticality of the Affected Resources. Resources affected by an incident (e.g., firewalls, Web servers, Internet connectivity, user workstations, and applications) have different significance to the organization. The criticality of a resource is based primarily on its data or services, users, trust relationships and interdependencies with other resources, and visibility (e.g., a public Web server versus an internal department Web server). Many organizations have already determined resource criticality through their business continuity planning efforts or their Service Level Agreements (SLA), which state the maximum time for restoring each key resource. When possible, the incident response team should acquire and reuse existing valid data on resource criticality.**

[SP800-61]

Attacker Liability for an Incident: Evidence Gathering

- During incident handling, system owners and others typically want to identify the attacker. Although this information can be important, particularly if the organization wants to prosecute the attacker, incident handlers should stay focused on containment, eradication, and recovery. Identifying the attacker can be a time-consuming and futile process that can prevent a team from achieving its primary goal—minimizing the business impact. The following items describe the most commonly performed activities for attacker identification:
  - + Validating the Attacker's IP Address. New incident handlers often focus on the attacker's IP address. The handler may attempt to validate that the address was not spoofed by using pings, traceroutes, or other methods of verifying connectivity. However, this is not helpful because at best it indicates that a host at that address responds to the requests. A failure to respond does not mean the address is not real—for example, a host may be configured to ignore pings and traceroutes. The attacker may have received a dynamic address (e.g., from a dialup modem pool) that has already been reassigned to someone else. More importantly, if the IP address is real and the team pings it, the attacker may be tipped off that the organization has detected the activity. If this occurs before the incident has been fully contained, the attacker could cause additional damage, such as wiping out hard drives with evidence of the attack. The team should consider acquiring and using IP addresses from another organization (e.g., an ISP) when performing actions such as address validation so that the true origin of the activity is concealed from the attacker.
- Scanning the Attacker's System. Some incident handlers do more than perform pings and traceroutes to check an attacking IP address—they may run port scanners, vulnerability scanners, and other tools to attempt to gather more information on the attacker. For example, the scans may indicate that Trojan horses are listening on the system, implying that the attacking host itself has been compromised. Incident handlers should discuss this issue with legal representatives before performing such scans because the scans may violate organization policies or even break the law.
- [SP-800-61]

Attacker Liability for an Incident: Evidence Gathering (2)

- Researching the Attacker Through Search Engines. In most attacks, incident handlers will have at least a few pieces of data regarding the possible identity of the attacker, such as a source IP address, an e-mail address, or an Internet relay chat (IRC) nickname. Performing an Internet search using this data may lead to more information on the attacker—for example, a mailing list message regarding a similar attack, or even the attacker's Web site. Research such as this generally does not need to be performed before the incident has been fully contained.
- Using Incident Databases. Several groups collect and consolidate intrusion detection and firewall log data from various organizations into incident databases. Some of these databases allow people to search for records corresponding to a particular IP address. Incident handlers could use the databases to see if other organizations are reporting suspicious activity from the same source. The organization can also check its own incident tracking system or database for related activity.
- Monitoring Possible Attacker Communication Channels. Another method that some incident handlers use to identify an attacker is to monitor communication channels that may be used by an attacker. For example, attackers may congregate on certain IRC channels to brag about Web sites that they have defaced. However, incident handlers should treat any such information that they acquire only as a potential lead to be further investigated and verified, not as fact.

[SP-800-61]

Security Countermeasures: Technical Controls

- **Identification. This control provides the ability to uniquely identify users, processes,and information resources. To implement other security controls (e.g., discretionary access control [DAC], mandatory access control [MAC], accountability), it is essential that both subjects and objects be identifiable.**

- **Cryptographic Key Management. Cryptographic keys must be securely managed when cryptographic functions are implemented in various other controls. Cryptographic key management includes key generation, distribution, storage, and maintenance.**

- **Security Administration. The security features of an IT system must be configured (e.g., enabled or disabled) to meet the needs of a specific installation and to account for changes in the operational environment. System security can be built into operating system security or the application. Commercial off-the-shelf add-on security products are available.**

- **System Protections. Underlying a system's various security functional capabilities is a base of confidence in the technical implementation. This represents the quality of the implementation from the perspective both of the design processes used and of the manner in which the implementation was accomplished. Some examples of system protections are residual information protection (also known as object reuse), least privilege (or "need to know"), process separation, modularity, layering, and minimization of what needs to be trusted. [SP800-30]**

Security Countermeasures: Preventative Technical Controls

- **Authentication. The authentication control provides the means of verifying the identity of a subject to ensure that a claimed identity is valid. Authentication mechanisms include passwords, personal identification numbers, or PINs, and emerging authentication technology that provides strong authentication (e.g., token, smart card, digital certificate, Kerberos).**

- **Authorization. The authorization control enables specification and subsequent management of the allowed actions for a given system (e.g., the information owner or the database administrator determines who can update a shared file accessed by a group of online users).**

- **Access Control Enforcement. Data integrity and confidentiality are enforced by access controls. When the subject requesting access has been authorized to access particular processes, it is necessary to enforce the defined security policy (e.g., MAC or DAC). These policy-based controls are enforced via access control mechanisms distributed throughout the system (e.g., MAC sensitivity labels; DAC file permission sets, access control lists, roles, user profiles). The effectiveness and the strength of access control depend on the correctness of the access control decisions (e.g., how the security rules are configured) and the strength of access control enforcement (e.g., the design of software or hardware security).**
[SP800-30]

Security Countermeasures: Preventative Technical Controls (2)

- **Nonrepudiation. System accountability depends on the ability to ensure that senders cannot deny sending information and that receivers cannot deny receiving it. Nonrepudiation spans both prevention and detection. It has been placed in the prevention category in this guide because the mechanisms implemented prevent the successful repudiation of an action (e.g., the digital certificate that contains the owner's private key is known only to the owner). As a result, this control is typically applied at the point of transmission or reception.**

- **Protected Communications. In a distributed system, the ability to accomplish security objectives is highly dependent on trustworthy communications. The protected communications control ensures the integrity, availability, and confidentiality of sensitive and critical information while it is in transit. Protected communications use data encryption methods (e.g., virtual private network, Internet Protocol Security [IPSEC] Protocol), and deployment of cryptographic technologies (e.g., Data Encryption Standard [DES], Triple DES, RAS, MD4, MD5, secure hash standard, and escrowed encryption algorithms such as Clipper) to minimize network threats such as replay, interception, packet sniffing, wiretapping, or eavesdropping. [SP800-30]**

Security Countermeasures: Preventative Technical Controls (2)

Transaction Privacy. Both government and private sector systems are increasingly required to maintain the privacy of individuals.

Transaction privacy controls (e.g., Secure Sockets Layer, secure shell) protect against loss of privacy with respect to transactions performed by an individual.

[SP800-30]

Detection and Recovery Technical Controls

Detection controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums. Recovery controls can be used to restore lost computing resources. They are needed as a complement to the supporting and preventive technical measures, because none of the measures in these other areas is perfect.

Detection and recovery controls include—

• **Audit.** The auditing of security-relevant events and the monitoring and tracking of system abnormalities are key elements in the after-the-fact detection of, and recovery from, security breaches.

• **Intrusion Detection and Containment.** It is essential to detect security breaches (e.g., network break-ins, suspicious activities) so that a response can occur in a timely manner. It is also of little use to detect a security breach if no effective response can be initiated. The intrusion detection and containment control provides these two capabilities.

• **Proof of Wholeness.** The proof-of-wholeness control (e.g., system integrity tool) analyzes system integrity and irregularities and identifies exposures and potential threats. This control does not prevent violations of security policy but detects violations and helps determine the type of corrective action needed.

• **Restore Secure State.** This service enables a system to return to a state that is known to be secure, after a security breach occurs.

• **Virus Detection and Eradication.** Virus detection and eradication software installed on servers and user workstations detects, identifies, and removes software viruses to ensure system and data integrity.

[SP800-30]

Integrate security risk considerations into acquisition strategy and practice

Dr. Drew Hamilton

Based on CNSS 4016

Documentation Outline

- Synthesis of Components and Overall Risks
- Analyze Vulnerabilities and Attacks
- Aspects of Security
- Assessment Methodology
- Associate Threat Probabilities to Vulnerability
- Conducting Risk Analysis
- Countermeasure Analysis
- Critical Thinking
- Deductive Reasoning
- Detailed Residual Risk
- Effect of Countermeasures on Risk
- Effects of Mitigation
- All Risk Variables
- Risk Assessment (Environment & Threat Description)
- Risk Management Methodology
- Security Countermeasures
- Technical Vulnerability
- Threat Analysis
- Threat Description
- Threat/Risk Assessment
- Mission
- Vulnerabilities
- Vulnerability Analysis

Synthesis of Components and Overall Risks

- Every system within the Enterprise comes with inherent risks
  - Base Profiles can provide a consistent level of risk for each system
  - Configuration Management is a essential task to manage risk across the entire domain
- Risk is quantified using two methods:
  - Qualitative Assessment – Uses subjective assessment of risk
  - Quantitative Assessment – Applies useful metrics to risk
- Overall Risk is the totality of risk within the Enterprise
  - Risk is reduced with countermeasures

Analyse Vulnerabilities and Attacks

Process of analysing paired interactions of system threats and vulnerabilities

- **The analysis of the threat to an IT system must include an analysis of the vulnerabilities associated with the system environment. The goal is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources.**
- **Table below presents examples of vulnerability/threat pairs.**

Vulnerability	Threat-Source	Threat Action
Terminated employees' system identifiers (ID) are not removed from the system	Terminated employees	Dialing into the company's network and accessing company proprietary data
Company firewall allows inbound telnet, and *guest* ID is enabled on XYZ server	Unauthorized users (e.g., hackers, terminated employees, computer criminals, terrorists)	Using telnet to XYZ server and browsing system files with the *guest* ID
The vendor has identified flaws in the security design of the system; however, new patches have not been applied to the system	Unauthorized users (e.g., hackers, disgruntled employees, computer criminals, terrorists)	Obtaining unauthorized access to sensitive system files based on known system vulnerabilities

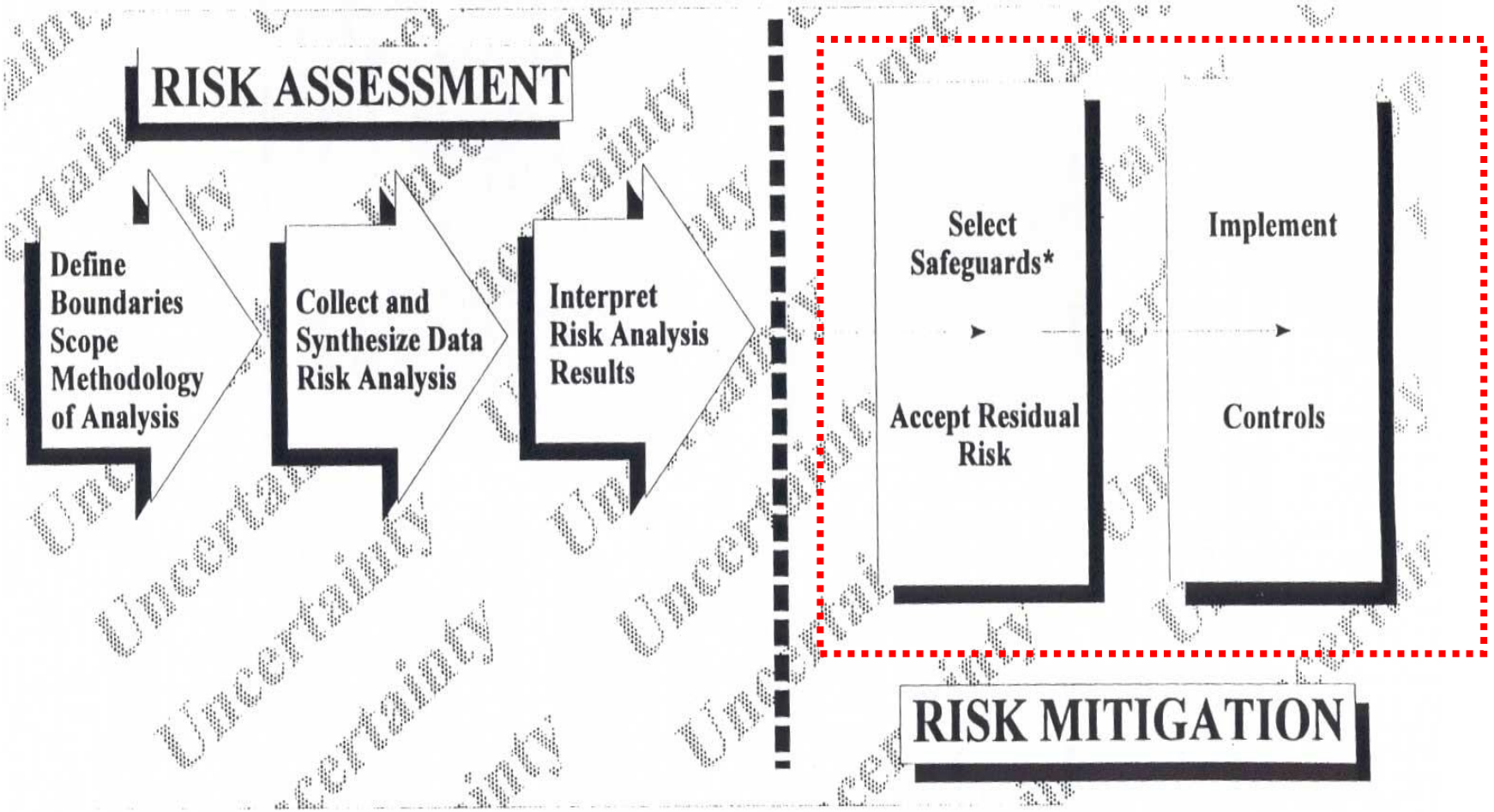
Aspects of Security

- **Confidentiality**
  - [44 U.S.C., Sec. 3542] Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **Integrity**
  - [44 U.S.C., Sec. 3542] Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- **Authentication**
  - [FIPS 200] Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
- **Availability**
  - [44 U.S.C., Sec. 3542] Ensuring timely and reliable access to and use of information.
- **Non-repudiation**
  - [CNSS Inst. 4009] Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

Assessment Methodology

- [44 U.S.C., Sec. 3502] Information Resources - Information and related resources, such as personnel, equipment, funds, and information technology.
- Organizations should use discretion in applying the security controls to information systems, giving consideration to the scalability factors in particular environments. This approach facilitates a cost-effective, risk-based approach to security control implementation that expends no more resources than necessary, yet achieves sufficient risk mitigation and adequate security.
- Scalability is guided by FIPS 199

Conducting Risk Analysis



Countermeasure Analysis

- Impact Analysis – Part of the CM and control process
- Before the system security plan can be developed, the information system be categorized based on a FIPS 199 impact analysis.
- A proper overall impact analysis considers the following factors: impact to the systems, data, and the organization's mission.
- Additionally, this analysis should also consider the criticality and sensitivity of the system and its data.
- While impact can be described in either a quantitative or qualitative approach, impact is generally described in qualitative terms.
- Magnitude of Impact can be:
  - High
  - Medium
  - Low

Mitigating Vulnerabilities

- Control Recommendations – 4th step of risk management
- This step is designed to identify and select controls that could mitigate or eliminate the risks identified in the preceding steps.
- Factors for recommending controls:
  - Effectiveness of recommended options (e.g., system compatibility);
  - Legislation and regulation;
  - Organizational policy
  - Operational impact
  - Safety and reliability
- The Internet is another source of information on known system vulnerabilities posted by vendors, along with hot fixes, service packs, patches, and other remedial measures that may be applied to eliminate or mitigate vulnerabilities.

Further defined in NIST SP 800-53

Critical Thinking

- **Known Variables:**
  - **Architecture**
  - **Risk**
  - **Threats**
- **Hypothetical Variables:**
  - **Methods**
  - **Means**
  - **Opportunity**

Deductive Reasoning

- Must be tested for each potential configuration
- Security test results should be verified
- Tests should be updated after modifications are made
- May be used on delivered system to support:
  - Verification
  - Certification
- Level of transparency is important, Security Content Automation Protocol (SCAP) checklists and procedures can be used
  - Defined in NIST SP 800-53

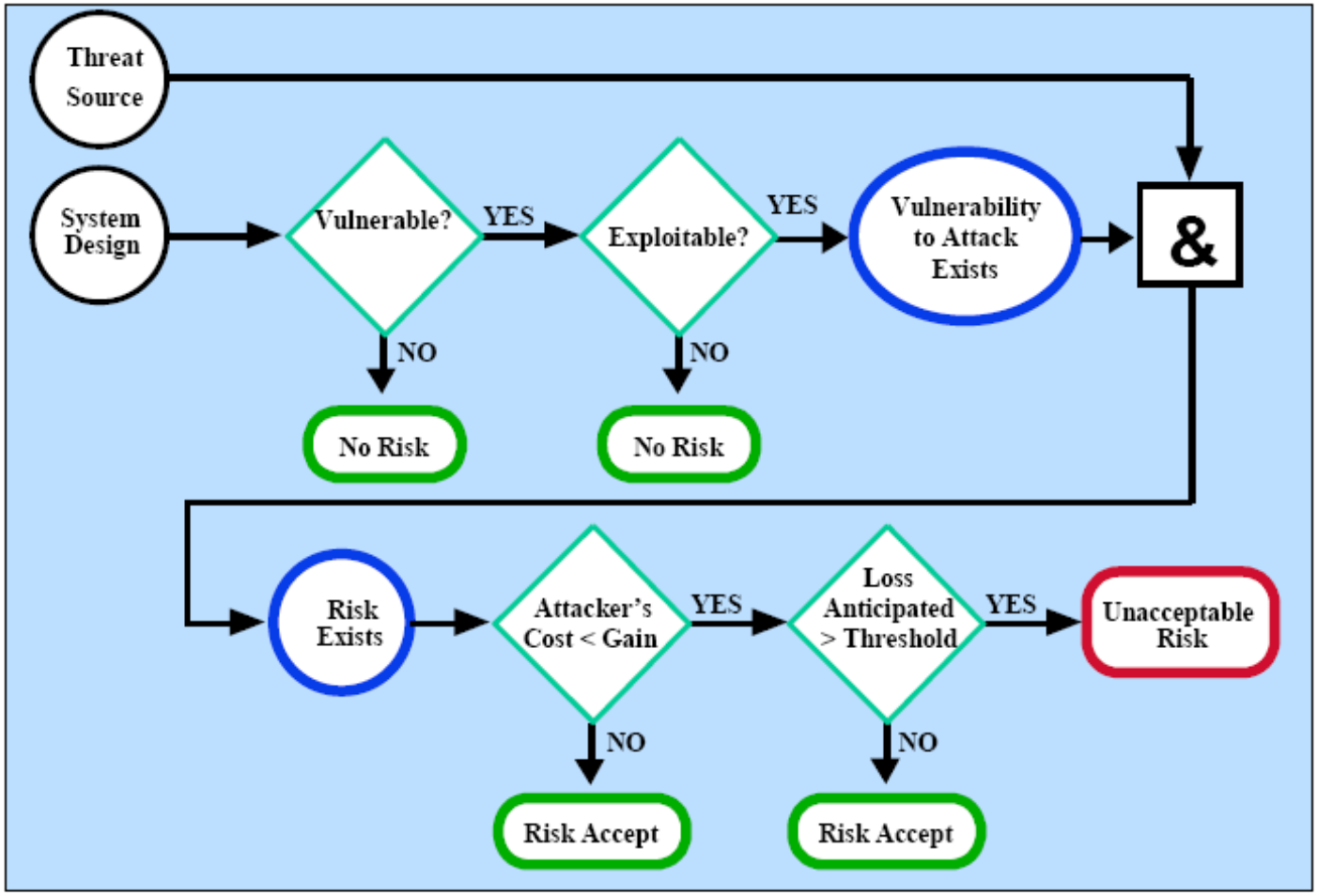
Detailed Residual Risk

- Systems may still be, and probably are, susceptible after countermeasures are applied
- Change is inevitable and aggressive, continuous monitoring is required
- An effective continuous monitoring program requires:
  - Configuration management and control processes for the information system;
  - Security impact analyses of changes to the information system;
  - Assessment of selected security controls in the information system
  - Security status reporting to appropriate agency officials
- Effectiveness can change due to changes in:
  - Hardware
  - Software
  - Firmware
  - Etc.

Effects of Countermeasures on Risk

- Sometimes risks must be taken
- If possibility is low, risk might be worth while, i.e.. While in combat using an unsecured radio
- Countermeasures should be used cost-effectively
  - Cost-benefit ratio is determined
  - Risk probability is calculated
  - Countermeasure is or is not implemented

Effects of Mitigation



Effects of Mitigation Continued

Risk mitigation options:

- **Risk Assumption.** To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level
- **Risk Avoidance.** To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)
- **Risk Limitation.** To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls)
- **Risk Planning.** To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls
- **Research and Acknowledgment.** To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability
- **Risk Transference.** To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

All Risk Variables

- **Loss of Integrity.** System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.
- **Loss of Availability.** If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.
- **Loss of Confidentiality.** System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

All Risk Variables

Original release date: 12/10/2007
Last revised: 12/10/2007
Source: US-CERT/NIST

Overview

Multiple unspecified vulnerabilities in IBM Hardware Management Console (HMC) 6 R1.3 allow attackers to gain privileges via "some HMC commands."

Impact

CVSS Severity (version 2.0):
CVSS v2 Base score: 10.0 (High) (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Impact Subscore: 10.0
Exploitability Subscore: 10.0

Access Vector: Network exploitable
Access Complexity: Low
****NOTE: Access Complexity scored Low due to insufficient information**
Authentication: Not required to exploit
Impact Type: Provides administrator access, Allows complete confidentiality, integrity, and availability violation , Allows unauthorized disclosure of information , Allows disruption of service

Source: nvd.nist.gov

Risk Assessment (Environment and Threat Description)

To determine what threats and vulnerabilities exist in a development effort, methodologies for identification early in the development process exist. Some of them are:

- **SecureUML – a modeling language that incorporates information pertinent to access control into applications modeled or defined using the Uniform Modeling Language (UML) [Lodderstedt et al. 2002]. It models security requirement for "well-behaved applications in predictable environment' [McGraw 2006].**
- **UMLsec [Jurjens 2001] – an extension of UML to encapsulate the modeling of security-related features, such as confidentiality and access control.**
- **Abuse Cases [Sindre and Opdahl] – an approach that extends use-cases to include misuse-cases, showing side-by-side what behavior should be supported and/or prevented.**
- **Microsoft's Threat Analysis and Modeling Tool (TAMT) generates risks based on the components, roles, data, external dependencies and the application's use-cases of a given development effort. [Microsoft 2006]**

Risk Management Methodology

- Organization type, location and operating environment will affect types of threats and vulnerabilities
- Evaluating types of threats
  - Natural Threats—Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events.
  - Human Threats—Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network based attacks, malicious software upload, unauthorized access to confidential information).
  - Environmental Threats—Long-term power failure, pollution, chemicals, liquid leakage.
- Evaluating vulnerabilities
  - Use vulnerability sources
  - System security testing
  - Security requirements checklist

Security Countermeasures

Threat	Countermeasure
Using tracert to detect network topology	Use firewalls to mask private services
Packet sniffers placed on network	Encrypt all network traffic
SYN flood attack (DOS)	Filter Internet Control Message Protocol (ICMP) requests
Using telnet to open ports for banner grabbing	Use generic banners

Technical Vulnerability

- **Hardware**
  - Physical access is not controlled
  - Machines are not properly physically hardened (i.e. cd-rom drive on machines without install privilages)
- **Firmware**
  - Old firmware being used
  - Newest firmware with known vulnerability
- **Communications**
  - Bluetooth capability on secured devices
- **Software**
  - Buffer overflows
  - Not applying latest security patches

Threat Analysis

Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Threat Description

- **Threat Methods:**
  - Network-based exploits
  - Application-based exploits
  - User-based exploits
    - Social Engineering
    - Trusted Insiders
- **Threat Means:**
  - Buffer Overflow
  - Password Cracking
  - Distributed Denial of Service (DDoS)
  - Trojans
    - BackOrfice
  - Viruses (Polymorphic, Metamorphic)
  - Key Logger
  - SQL Injection
  - DNS Spoofing
  - Covert Channels
  - Certificate Spoofing
  - Phishing (more specifically, Spear Phishing)

Threat/Risk Assessment

- **Determination of risk for a particular threat/vulnerability pair can be expressed as a function of:**
  - **The likelihood of attempting to exercise a given vulnerability**
  - **The magnitude of the impact**
  - **The adequacy of planned or existing security controls**
- **To measure risk, a risk scale and a risk-level matrix should be developed.**

Threat Likelihood	Impact		
	Low (10)	*Medium* (50)	*High* (100)
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

M ~ O ~ M

- Means
- Opportunity
- Motivation – for intentional actions

of your adversaries

Mission

- **Mission impact analysis - Prioritizes impact levels associated with compromise**
- **Asset criticality assessment – identifies and prioritizes critical information assets**

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.

Vulnerabilities

- **Any weakness that can be exploited to gain access to an asset**
  - **Physical security**
  - **Computer/technical security**
  - **Communications security**
  - **Personnel security**
  - **Administrative/Management security**
    - **Note: Unmet security requirements are vulnerabilities**

Vulnerabilities (2)

Initiation

- The primary sources of vulnerabilities are derived from information about the considered or proposed network components, their operating systems and applications

Development and Acquisition

- Vulnerability identification expands to include automated tools and databases of known vulnerabilities to identify appropriate system security configurations

Operation and Maintenance

- Vulnerability identification includes determining and analyzing implemented security features using:
  - Proactive methods
  - Documented vulnerability sources

Vulnerabilities (3)

- **Proactive methods**
  - Automated vulnerability scanning
  - Network mapping
  - Security testing and evaluation
  - Penetration testing
- **Documented vulnerability sources**
  - Previous risk assessments
  - CERT and CIAC bulletins
  - Vendor advisories
  - Vulnerability listings
  - System software security analyses
  - System information analyses
  - System development test procedures
  - System test results
  - System anomaly reports

Vulnerability Analysis

- Requires more specialized tools
  - Scanning tools
  - Source code reviews
  - Statistical analysis of source code
- Analysis should include:
  - Previous risk assessment documentation of the IT system assessed
  - The IT system's audit reports, system anomaly reports, security review reports, and system test and evaluation reports
  - Vulnerability lists, such ashe NIST I-CAT vulnerability database (http://icat.nist.gov) SP 800-30 Page 17
  - Security advisories, such as FedCIRC and the Department of Energy's Computer Incident Advisory Capability bulletins
  - Vendor advisories
  - Commercial computer incident/emergency response teams and post lists (e.g., SecurityFocus.com forum mailings)
  - Information Assurance Vulnerability Alerts and bulletins for military systems
  - System software security analyses.

Recommended Readings

- NIST SP 800-30
- NIST SP 800-37
- NIST SP 800-53
- NIST SP 800-100
- FIPS 199
- FIPS 200

Documentation Outline

- Policies
- Access Control Principles
- Formal Methods of Security Design
- Generally Accepted Systems Security Principles
- Information Security Policy
- Laws, Regulations, and Other Public Policy
- Life Cycle System Security Planning
- Personnel Security Policies and Guidance
- Technical Knowledge of Information System
- Mission

Policies

- **Sources**
  - **International (ISO 9000)**
  - **Federal (e.g. FISMA)**
  - **Organization**
  - **Group / Departmental**

Access Control Policies

- DoD Password Management Guideline, 12 Apr 85
- Password Vulnerabilities
  - a password must be initially assigned to a user when enrolled on the ADP system;
  - a user's password must be changed periodically;
  - the ADP system must maintain a "password database";
  - users must remember their passwords; and
  - users must enter their passwords into the ADP system at authentication time.

Access Control Policies

- **Green Book Guidelines**
  - **Users should be able to change their own passwords.**
  - **Passwords should be machine-generated rather than user-created.**
  - **Certain audit reports (e.g., date and time of last login) should be provided by the system directly to the user.**

Formal Methods of Security Design

- **Programming Languages**
  - **SPARK (Ada subset)**
  - **Standard ML**
  - **Haskell**
- **Source Code Checkers**
  - **Coverity (C,C++, Java)**
  - **Klockwork (C, C++, Java)**

Generally Accepted Systems Security Principles

- **OECD's Guidelines for the Security of Information Systems**
  - **Accountability - The responsibilities and accountability of owners,providers and users of information systems and other parties...should be explicit.**
  - **Awareness - Owners, providers, users and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures...for the security of information systems.**

Generally Accepted Systems Security Principles

- Ethics - The Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interest of others are respected.
- Multidisciplinary - Measures, practices and procedures for the security of information systems should take account of and address all relevant considerations and viewpoints....
- Proportionality - Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm....

Generally Accepted Systems Security Principles

- **Integration - Measures, practices and procedures for the security of information systems should be coordinated and integrated with each other and other measures, practices and procedures of the organization so as to create a coherent system of security.**
- **Timeliness - Public and private parties, at both national and international levels, should act in a timely coordinated manner to prevent and to respond to breaches of security of information systems.**
- **Reassessment - The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.**
- **Democracy - The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.**

Generally Accepted Systems Security Principles

- **NIST 800-14**
  - **Computer Security Supports the Mission of the Organization**
  - **Computer Security is an Integral Element of Sound Management**
  - **Systems Owners Have Security Responsibilities Outside Their Own Organizations**
  - **Computer Security Responsibilities and Accountability Should Be Made Explicit**
  - **Computer Security Requires a Comprehensive and Integrated Approach**
  - **Computer Security Should Be Periodically Reassessed**
  - **Computer Security is Constrained by Societal Factors**

Information Security Policy

- **In some cases, security policies allow actions that may have an adverse affect on a system**
  - **Example: Linux Users are often assigned "sudo" access instead of "root", yet "sudo" can have as many rights as a "root" user if not locked down properly**
  - **Example: Remote Administration to save maintenance costs may expose Enterprise to remote network attacks**

Laws, Regulations, and Other Public Policy

- Organizations must implement laws, regulations and public policies in their IT infrastructure
- Privacy Protection
  - Protect user data (such a Health Care information) with encryption to guarantee confidentiality
  - HIPPA protections

Life Cycle System Security Planning

- **Integrated Logistics Support of IA:**
  1. **Maintenance planning of security systems**
  2. **Supply support of hardware or software**
  3. **Support and Test Equipment/Equipment support**
  4. **Manpower and personnel**
  5. **Training and training support**
  6. **Technical data**
  7. **Computer Resources support**
  8. **Facilities**
  9. **Packaging, Handling, Storage, and Transportation**
  10. **Design interface**

Personnel Security Policies and Guidance

- **Some personnel security policies include:**
  - **Deactivate accounts within 30 days after an employee is released**
  - **Review level of account access every 6 months to ensure strict access control is maintained and users are associated with the correct roles**
  - **To prevent collusion, employees should be rotated into areas of different duties**
  - **Mandatory vacation time ensures access policies and chain of responsibility remains intact for continuity plans**

Threat / Risk Assessment

- **Risk Assessment**
  - **Determine Assessment's scope and methodology**
  - **Collecting and analyzing data**
    - **Asset Valuation**
    - **Consequence Assessment**
    - **Threat identification**
    - **Safeguard Analysis**
    - **Vulnerability analysis**
    - **Likelihood assessment**
  - **Interpreting risk analysis results**
    - **High, medium, low**
    - **Or 1-10**

Threat / Risk Assessment

Threats, Vulnerabilities, Safeguards, and Assets

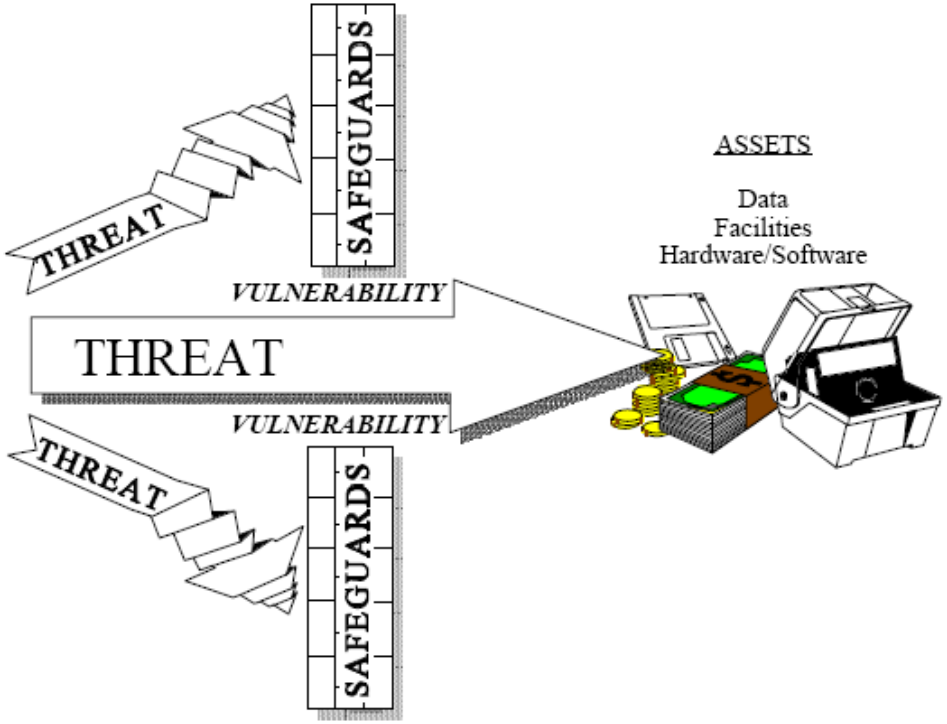


Figure 7.1 Safeguards prevent threats from harming assets. However, if an appropriate safeguard is not present, a vulnerability exists which can be exploited by a threat, thereby puttting assets at risk.

Mission

- **Current mission may affect adherence to security policy**
  - **Example: Not using secure communications channel when under fire**
  - **Not encrypting network traffic when not connected to an outside network**
- **Factors may include:**
  - **Personal safety**
  - **Criticality of timeline**
  - **Emergency situation**
  - **Reasonable expectation of information safety**

Effect of Countermeasure Outline

- Access Control Policies
- Agency Specific Policies and Procedures
- Cost / Benefit Analysis
- Countermeasures
- Life Cycle System Security Planning
- Network Firewalls
- Preventative Controls
- Security Domains
- Security Product Testing / Evaluation
- Technical Knowledge of Information System
- Technological Threats
- Threat / Risk Assessment
- Mission

Access Control Policies

- **Logical Access**
  - **Procedures for granting, modifying and revoking access,**
  - **Install detection mechanisms for unauthorized access attempts,**
  - **Timeout a session after 15 minutes of inactivity, and**
  - **Revoke access after an inactivity period of 60 days**

Access Control Policies

- **Physical Access**
  - **All telecommunication and computer related equipment are to be in a secured, locked environment**
  - **Access codes for secure environments must be changed at least every 60 days or in the event of a individual departing that previously had access**
  - **Account for all keys issued for those facilities using this method and replace locking mechanism when a key is missing,**
  - **When the system permits, log all accesses and retain records**
  - **Secure all peripherals such as air conditioning, generators, etc.**

Agency Specific Policies and Procedures

- **Steps to implement higher-level regulations**
  - **Identify applicable policies**
    - **International**
    - **Federal**
    - **State**
  - **Compare required policies against applicable policies**
  - **Develop agency policies**

Cost / Benefit Analysis

- Cost of Data Protection depends on
  - Sensitivity of the data
  - Lifetime data must be available
  - Most often cost of data protection is used as a business decision.
- Cost of Data Compromise
  - Legal prosecution by government or local individuals
  - Loss of trust
  - Cost to recover

Countermeasures

- **Methods that reduce vulnerabilities or threats**
  - **Network devices (e.g. Firewalls, IDS)**
  - **Automatic Software Updates**
  - **User Training**
    - **Social Engineering**
  - **Developer Training**
    - **Secure programming and design**

Life Cycle Security System Planning

- **Life Cycle of systems**
  - **Need:**
    - **Location of system components**
    - **Identify users**
    - **Determine type of data**
    - **Lifetime of the system**
  - **Design and Construction**
  - **Operation**
  - **Disposal**

Network Firewalls

- **Features:**
  - **Packet Filtering**
  - **User Authentication**
  - **Auditing and Logging**
  - **Stateful Packet Inspection**
  - **Application proxies**
  - **VPN**

Preventive Controls

- Audit system data for accuracy and reliability
- Determine the effectiveness of controls
- Validate the preventive controls implement appropriate policies

Security Domains

- **Defined as the people and systems that must adhere to a security policy.**
- **Knowledge of Security Domains and Physical Security helps to think about :**
  - **What is to be protected?**
  - **Who is allowed and when they to access it?**
  - **How the system data is accessed?**
  - **Design of the system and facilities?**

Security Product Testing / Evaluation

- **Security posture is there to provide an understanding of the weaknesses, vulnerabilities and likelihood of exploitation of a system or network infrastructure.**
- **Determining a security posture of a system requires**
  - **System installed in operational environment**
  - **Knowledge of hardware and software configuration.**
  - **Criteria against which the system will be compared.**

Technical Knowledge of Information System

- **Simply installing security equipment and applications within an organizations is not enough to ensure an infrastructure is adequately protected**
- **Each system also needs to have skilled operators knowledgeable about:**
  - **Hardware (e.g. network devices, workstations)**
  - **Software (e.g. firmware, operating systems)**

Technological Threats

- No useful system or application is constructed without flaws. Therefore there are flaws that can be exploited to cause harm to a system or data.
- Understanding the flaws in a system or application requires intimate knowledge of the system or application
- Organizations need to know what flaws exist so they can be removed or mitigate the possibility of a threat.

Threat / Risk Assessment

- **Life Cycle Analysis of security requirements and countermeasures**
  - **Identification of vulnerability**
  - **Determine the extent of the impact of an exploitation of the vulnerability**
  - **Determine the security requirements and countermeasures that mitigate a threat**
  - **Reevaluate security requirements and countermeasures after vendor fixes vulnerability.**

Mission

- **Risk assessment and certification process can impact the mission of a system**
  - **Reduced availability due to taking systems off-line for testing**
  - **Add additional items to the mission of a system**
  - **Add a delay to the responsiveness of a system during assessment period**

Operating System Scanning

- **Operating System Scanning**
  1. **Find out what systems are running (ping sweep)**
  2. **Port scan the hosts**
  3. **Correlate the services that are running**
  4. **Run a vulnerability scan**

Wrappers

- An additional layer of protection can be applied in Unix-like systems by using “wrappers”
- Information gathering
  - Browsing – a general technique used by technique used by intruders to obtain information they are not authorized to access
    - Perusing file listings on devices
    - Dumpster diving
    - Shoulder surfing

Sniffers

- A network sniffer is a tool that monitors traffic as it traverses a network
  - Also referred to as network analyzers or protocol analyzers
  - Runs with the NIC in promiscuous mode
- Secure versions of services and protocols should be used when possible in order to combat sniffers
  - Example: Secure RPC (S-RPC): uses Diffie-Hellman public key cryptography to determine the shared secret key
  - R-utilities (rlogin, rexec, rsh, rcp) in Unix all have several weaknesses and should be replaced by a service that requires stronger authentication such as secure shell

Session Hijacking

- **Session Hijacking**
  - **Can be countered with IPSec or Kerberos**
- **Loki attack**
  - **Uses ICMP protocol for covert channel communications**
  - **Writes data behind the ICMP header (which is designed for status and error messages)**
  - **Successful because ICMP is not typically scanned by firewalls**

Password Cracking

- **Password Cracking**
  - **Static passwords are the technique of choice, both for familiarity and cost reasons**
  - **Easily cracked, other options would be smart cards or biometrics (at a greater cost)**
  - **Password cracking tools (i.e.: John the Ripper, Crack, Ophcrack) attack encoded hashes**
  - **Dictionary or brute force attacks on stolen password files (rainbow tables not addressed)**
  - **Strong password policies: at least 8 characters, upper case, lower case, at least 2 special characters**

Backdoors

- A backdoor is a program that is installed by an attacker to enable them to come back into the computer at a later date without having to supply login credentials or go through any type of authorization process
  - Such behaviors can often be detected by host-based intrusion detection systems

Vulnerability Testing

- **Goals of a vulnerability testing assessment**
  - **Evaluate the true security posture of an environment (minimize false positives)**
  - **Identify as many vulnerabilities as possible with honest evaluations and prioritization of each**
  - **Test how systems react to certain circumstances and attacks, to learn not only what the known vulnerabilities are (given a specific operating environment), but also how the unique elements of the environment might be abused (such as SQL injection attacks, buffer overflows, and process design flaws that facilitate social engineering)**

Written Agreement

- **<u>Highlighted caution:</u> Before carrying out vulnerability testing, a written agreement from management is required! This protects the tester against prosecution for doing his job, and ensures there are no misunderstandings by providing in writing what the tester should – and should not – do.**

Personnel Testing

- **Personnel testing: includes reviewing employee tasks and thus identifying vulnerabilities in the standard practices and procedures that employees are instructed to follow, demonstrating social engineering attacks and the value of training users to detect and resist such attacks, and reviewing employee policies and procedures to ensure those security risks that cannot be reduced through physical and logical controls are met with the final control category (Administrative)**

Physical Testing

- **Physical testing: includes reviewing facility and perimeter protection mechanisms. For example do the doors automatically close and an alarm sound if the door is open too long? Are interior protection mechanisms of server rooms, wiring closets, sensitive systems, and assets appropriate? Is dumpster diving a threat? What of protection mechanisms for manmade, natural, or technical threats? Is there a fire suppression system? Are sensitive electronics kept above raised floors so they survive a minor flood?**

System and Network Testing

- **Systems and network testing: perhaps what most people think of when discussing information security vulnerability testing. For efficiency, an automated scanning product identifies known system vulnerabilities, and some may (if management has signed off on the performance impact and the risk of disruption) attempt to exploit vulnerabilities**

Penetration Testing

- **Penetration Testing: the process of simulating attacks on a network and its systems at the request of the owner or senior management**
  - **Measures an organization's level of resistance to an attack and uncovers weaknesses within their environment**
  - **Foundation is established by a vulnerability scan**

Get Out of Jail Free

- **Highlighted note: A "Get Out of Jail Free Card" is a document you can present to someone who thinks you are up to something malicious, when in fact you are carrying out an approved test.**
- **There have been many situations in which an individual (or a team) was carrying out a penetration test and was approached by a security guard or someone who thought this person was in the wrong place at the wrong time**

Pen Test Process

The process steps of a penetration test:

1. **Discovery: Footprinting and information gathering**
2. **Enumeration: Port scans and resource identification**
3. **Vulnerability mapping: Identifying vulnerabilities**
4. **Exploitation: Gaining unauthorized access**
5. **Reporting: Documentation and suggestions to management**

Types of Pen Tests

- **Types of tests**
  - **Zero knowledge v. partial knowledge (advance knowledge of the tester)**
  - **Blind, double-blind, or targeted (use of public knowledge or targeted knowledge, and whether the staff is aware)**

Vulnerability Targets

- **Vulnerability targets**
  - **Kernel flaws: fixed by patching**
  - **Buffer overflows: fixed by defensive programming and developer education**
  - **Symbolic links: fixed by requiring scripts to ensure use of fully qualified paths**
  - **File descriptor attacks: fixed by defensive programming and developer education**
  - **Race conditions: fixed by defensive programming and developer education**
  - **File and directory permissions: fixed by use of file integrity checkers**

Operations Security

Test Type	Frequency	Benefits
Network Scanning	Continuously to quarterly	- Enumerates the network structure and determines the set of active hosts and associated software - Identifies unauthorized hosts connected to a network - Identifies open ports - Identifies unauthorized services
Wardialing	Annually	- Detects unauthorized modems and prevents unauthorized access to a protected network
War Driving	Continuously to weekly	- Detects unauthorized wireless access points and prevents unauthorized access to a protected network
Virus Detectors	Weekly or as required	- Detects and deletes viruses before successful installation on the system
Log Reviews	Daily for critical systems	- Validates that the system is operating according to policy
Password Cracking	Continuously to same frequency as expiration policy	- Verifies the policy is effective in producing passwords that are more or less difficult to break - Verifies that users select passwords compliant with the organization's security policy
Vulnerability Scanning	Quarterly or bimonthly (more often for high risk systems), or whenever the vulnerability database is updated	- Enumerates the network structure and determines the set of active hosts and associated software - Identifies a target set of computers to focus vulnerability analysis - Identifies potential vulnerabilities on the target set - Validates operating systems and major applications are up-to-date with security patches and software versions
Penetration Testing	Annually	- Determines how vulnerable an organization's network is to penetration and the level of damage that can be incurred - Tests the IT staff's response to perceived security incidents and their knowledge and implementation of the organization's security policy and the system's security requirements
Integrity Checkers	Monthly and in case of a suspicious event	- Detects unauthorized file modifications

Table 12-3 Example Testing Schedules for Each Operations and Security Department

Summary

- Confidentiality, integrity and availability concepts
- Security governance
- Compliance
- Legal and Regulatory Issues
- Professional Ethics
- Security policies, standards and procedure