INFORMATION SECURITY

UNIT-2

Legal, Ethical, and Professional Issues In Information Security

Introduction

As a future information security professional, it is vital that you understand the scope of an organization's legal and ethical responsibilities.

To minimize liabilities and reduce risks from electronic, physical threats and reduce the losses from legal action, the information security practitioner must understand the current legal environment, stay current as new laws and regulations emerge, and watch for issues that need attention.

Law and Ethics in Information Security

As individuals we elect to trade some aspects of personal freedom for social order.

Laws are rules adopted for determining expected behavior in modern society and are drawn from Ethics, which define socially acceptable behaviors.

Ethics in turn are based on cultural mores: fixed moral attitudes or customs of a particular group.

Some ethics are recognized as universal among cultures.

Types of Law

- **Civil law** represents a wide variety of laws that are recorded in volumes of legal "code" available for review by the average citizen.
- **Criminal law** addresses violations harmful to society and is actively enforced through prosecution by the state.
- **Tort law** allows individuals to seek recourse against others in the event of personal, physical, or financial injury.
- **Private law** regulates the relationship between the individual and the organization, and encompasses family law, commercial law, and labor law.
- **Public law** regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments, providing careful checks and balances. Examples of public law include criminal, administrative, and constitutional law.

Relevant U.S. Laws

- **General Computer Crime Laws:**

The Computer Fraud and Abuse Act of 1986 is the cornerstone of many computer-related federal laws and enforcement efforts.

It was amended in October 1996 with the National Information Infrastructure Protection Act of 1996, which modified several sections of the CFA, and increased the penalties for selected crimes.

The USA Patriot Act of 2001 modified a wide range of existing laws to provide law enforcement agencies with broader latitude of actions to combat terrorism-related activities.

The Communication Act of 1934 was revised by the Telecommunications Deregulation and Competition Act of 1996, which attempts to modernize the archaic terminology of the older act.

These much-needed updates of terminology were included as part of the Communications Decency Act (CDA).

The CDA was immediately ensnared in a thorny legal debate over the attempt to define indecency, and ultimately rejected by the Supreme Court.

Another key law that is of critical importance for the information security professions is the Computer Security Act of 1987.

It was one of the first attempts to protect federal computer systems by establishing minimum acceptable security practices.

The National Bureau of Standards, in cooperation with the National Security Agency, became responsible for developing these security standards and guidelines.

- **Privacy**

The issue of privacy has become one of the hottest topics in information.

The ability to collect information on an individual, combine facts from separate sources, and merge it with other information has resulted in databases of information that were previously impossible to set up.

The aggregation of data from multiple sources permits unethical organizations to build databases of facts with frightening capabilities.

Privacy of Customer Information

The Privacy of Customer Information Section of Common Carrier regulation specifies that any proprietary information shall be used explicitly for providing services, and not for any marketing purposes.

It also stipulates that carriers cannot disclose this information except when necessary to provide its services.

The only other exception is when a customer requests the disclosure of information, and then the disclosure is restricted to that customer's information only.

The Federal Privacy Act of 1974 regulates the government in the protection of individual privacy and was created to insure that government agencies protect the privacy of individuals' and businesses' information and to hold those agencies responsible if any portion of this information is released without permission.

The Electronic Communications Privacy Act of 1986 regulates the interception of wire, electronic and oral communications. The ECPA works in conjunction with the Fourth Amendment of the US Constitution, which provides protections from unlawful search and seizure.

The Health Insurance Portability & Accountability Act Of 1996 (HIPAA) also known as the Kennedy-Kassebaum Act, impacts all healthcare organizations including small doctor practices, health clinics, life insurers and universities, as well as some organizations which have self-insured employee health programs.

The act requires organizations that retain healthcare information to use information security mechanisms to protect this information, as well as policies and procedures to maintain this security.

It also requires a comprehensive assessment of the organization's information security systems, policies, and procedures.

There is no specification of particular security technologies for each of the security requirements; only that security must be implemented to ensure the privacy of the healthcare information.

The Privacy standards of HIPAA severely restrict the dissemination and distribution of private health information without documented consent.

The standards provide patients the right to know who has access to their information and who has accessed it and also restrict the use of health information to the minimum required for the healthcare services required.

The Financial Services Modernization Act or Gramm-Leach-Bliley Act of 1999 requires all financial institutions to disclose their privacy policies on the sharing of non-public personal information.

It also requires due notice to customers, so that they can request that their information not be shared with third parties.

The act ensures that the privacy policies in effect in an organization are fully disclosed when a customer initiates a business relationship, as well as distributed at least annually for the duration of the professional association.

Export and Espionage Laws

In an attempt to protect American ingenuity, intellectual property, and competitive advantage, Congress passed the **Economic Espionage Act** (EEA) in 1996. This law attempts to prevent trade secrets from being illegally shared.

The **Security and Freedom through Encryption Act of 1997** (SAFE) was an attempt by Congress to provide guidance on the use of encryption, and provided measures of public protection from government intervention.

US Copyright Law

Intellectual property is recognized as a protected asset in the US. US copyright law extends this right to the published word, including electronic formats.

Fair use of copyrighted materials includes the use to support news reporting, teaching, scholarship, and a number of other related permissions, so long as the purpose of the use is for educational or library purposes, not for profit, and is not excessive

Freedom of Information Act of 1966 (FOIA)

The Freedom of Information Act provides any person with the right to request access to federal agency records or information, not determined to be of national security.

US Government agencies are required to disclose any requested information on receipt of a written request.

There are exceptions for information that is protected from disclosure, and the Act does not apply to state or local government agencies or to private businesses or individuals, although many states have their own version of the FOIA.

State & Local Regulations

In addition to the national and international restrictions placed on an organization in the use of computer technology, each state or locality may have a number of laws and regulations that impact operations.

It is the responsibility of the information security professional to understand state laws and regulations and insure the organization's security policies and procedures comply with those laws and regulations.

International Laws And Legal Bodies

Recently the Council of Europe drafted the European Council Cyber-Crime Convention, designed to create an international task force to oversee a range of security functions associated with Internet activities, and to standardize technology laws across international borders.

It also attempts to improve the effectiveness of international investigations into breaches of technology law.

This convention is well received by advocates of intellectual property rights with its emphasis on copyright infringement prosecution.

Digital Millennium Copyright Act (DMCA)

The Digital Millennium Copyright Act (DMCA) is the US version of an international effort to reduce the impact of copyright, trademark, and privacy infringement especially through the removal of technological copyright protection measures.

The European Union also put forward Directive 95/46/EC that increases protection of individuals with regard to the processing of personal data and on the free movement of such data.

The United Kingdom has already implemented a version of this directive called the Database Right.

United Nations Charter

To some degree the United Nations Charter provides provisions for information security during Information Warfare.

Information Warfare (IW) involves the use of information technology to conduct offensive operations as part of an organized and lawful military operation by a sovereign state. IW is a relatively new application of warfare, although the military has been conducting electronic warfare and counter-warfare operations for decades, jamming, intercepting, and spoofing enemy communications.

Policy Versus Law

Most organizations develop and formalize a body of expectations that describe acceptable and unacceptable behaviors of the employee within the workplace. This body of expectations is called policy.

Properly executed policies function in an organization like laws, complete with penalties, judicial practices, and sanctions to require compliance.

For a policy to become enforceable, it must be:

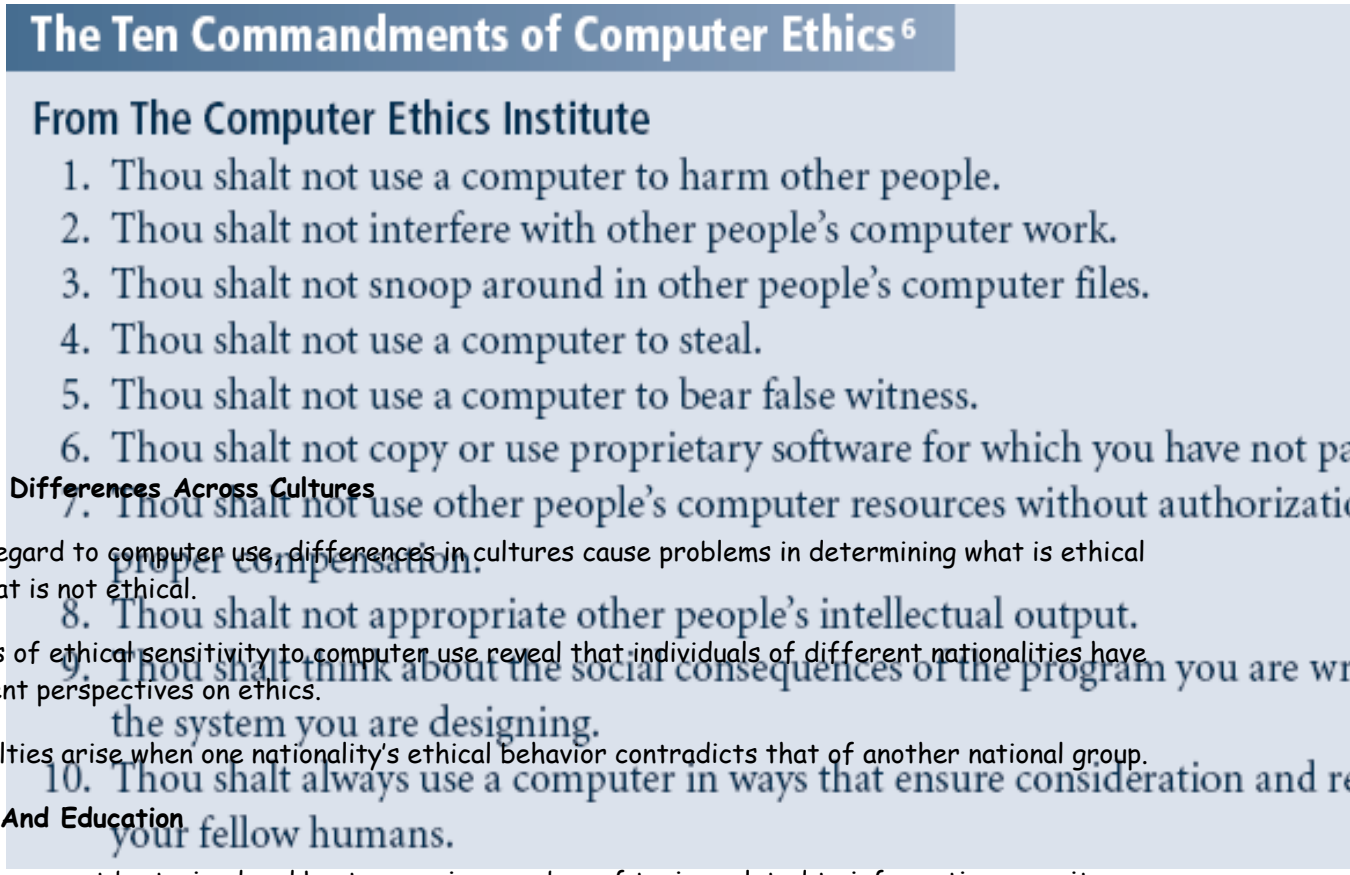
Distributed to all individuals who are expected to comply with it.

Readily available for employee reference.

Easily understood with multi-language translations and translations for visually impaired, or literacy-impaired employees.

Acknowledged by the employee, usually by means of a signed consent form.

Only when all of these conditions are met, does the organization have the reasonable expectation that should an employee violate policy, they may be appropriately penalized without fear of legal retribution.



The Ten Commandments of Computer Ethics [6]

From The Computer Ethics Institute

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 pa
7. Thou shalt not use other people's computer resources without authorizati
   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 wr
   the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and re
    your fellow humans.

Ethical Differences Across Cultures

With regard to computer use, differences in cultures cause problems in determining what is ethical and what is not ethical.

Studies of ethical sensitivity to computer use reveal that individuals of different nationalities have different perspectives on ethics.

Difficulties arise when one nationality's ethical behavior contradicts that of another national group.

Ethics And Education

Employees must be trained and kept aware in a number of topics related to information security, not the least of which is the expected behaviors of an ethical employee.

This is especially important in areas of information security, as many employees may not have the formal technical training to understand that their behavior is unethical or even illegal. Proper ethical and legal training is vital to creating an informed, well prepared, and low-risk system user.

Deterrence To Unethical And Illegal Behavior

Deterrence is the best method for preventing an illegal or unethical activity. Laws, policies, and technical controls are all examples of deterrents.

However, it is generally agreed that laws and policies and their associated penalties only deter if three conditions are present.

- Fear of penalty.
- Probability of being caught.
- Probability of penalty being administered.

Codes Of Ethics, Certifications And Professional Organizations

- A number of professional organizations have established codes of conduct and/or codes of ethics that members are expected to follow.
- Codes of ethics can have a positive effect on an individual's judgment regarding computer use.
- Unfortunately, having a code of ethics is not enough, because many employers do not encourage their employees to join these professional organizations.
- It is the responsibility of security professionals to act ethically and according to the policies and procedures of their employer, their professional organization, and the laws of society.

Association of Computing Machinery.

The ACM (www.acm.org) is a respected professional society, originally established in 1947, as "the world's first educational and scientific computing society".

The ACM's code of ethics requires members to perform their duties in a manner befitting an ethical computing professional.

The code contains specific references to protecting the confidentiality of information, causing no harm, protecting the privacy of others, and respecting the intellectual property and copyrights of others.

International Information Systems Security Certification Consortium

The $(ISC)^2$ (www.isc2.org) is a non-profit organization that focuses on the development and implementation of information security certifications and credentials.

The code of ethics put forth by $(ISC)^2$ is primarily designed for information security professionals who have earned a certification from $(ISC)^2$.

This code focuses on four mandatory canons:

Protect society, the commonwealth, and the infrastructure;

Act honorably, honestly, justly, responsibly, and legally;

Provide diligent and competent service to principals; and

Advance and protect the profession.

System Administration, Networking, and Security Institute

The System Administration, Networking, and Security Institute, or SANS (www.sans.org), is a professional organization with a large membership dedicated to the protection of information and systems.

SANS offers a set of certifications called the Global Information Assurance Certification or GIAC.

Information Systems Audit and Control Association

The Information Systems Audit and Control Association or ISACA (www.isaca.org) is a professional association with a focus on auditing, control, and security.

Although it does not focus exclusively on information security, the Certified Information Systems Auditor or CISA certification does contain many information security components.

The ISACA also has a code of ethics for its professionals. It requires many of the same high standards for ethical performance as the other organizations and certifications.

CSI - Computer Security Institute

The Computer Security Institute (www.gocsi.com) provides information and certification to support the computer, networking, and information security professional.

While CSI does not promote a single certification certificate like the CISSP or GISO, it does provide a range of technical training classes in the areas of Internet Security, Intrusion Management, Network Security, Forensics, as well as technical networking.

Information Systems Security Association (ISSA)

- Nonprofit society of information security (IS) professionals
- Primary mission to bring together qualified IS practitioners for information exchange and educational development
- Promotes code of ethics similar to $(ISC)^2$, ISACA and ACM

OTHER SECURITY ORGANIZATIONS

- The Information Systems Security Association (ISSA)® (www.issa.org) is a non-profit society of information security professionals.
- As a professional association, its primary mission is to bring together qualified practitioners of information security for information exchange and educational development.
- The Internet Society or ISOC (www.isoc.org) is a non-profit, non-governmental, international organization for professionals.

- It promotes the development and implementation of education, standards, policy, and education and training to promote the Internet.
- The Computer Security Division (CSD) of the National Institute for Standards and Technology (NIST), contains a resource center known as the Computer Security Resource Center (CSRC) which is a must know for any current or aspiring information security professional.
- This Web site (csrc.nist.gov) houses one of the most comprehensive sets of publicly available information on the entire suite of information security topics.
- The CERT® Coordination Center or CERT/CC (www.cert.org) is a center of Internet security expertise operated by Carnegie Mellon University.
- The CERT/CC studies security issues and provides publications and alerts to help educate the public to the threats facing information security. The center also provides training and expertise in the handling of computer incidents.
- The **Computer Professionals for Social Responsibility** (CPSR) is a public organization for technologists and anyone with a general concern for the impact of computer technology on society.
- CPSR promotes ethical and responsible development and use of computing, and seeks to inform public and private policy and lawmakers on this subject. It acts as an ethical watchdog for the development of ethical computing.

KEY U.S. FEDERAL AGENCIES

- The Federal Bureau of Investigation's National Infrastructure Protection Center (NIPC) (www.nipc.gov) was established in 1998 and serves as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against critical U.S. infrastructures.
- A key part of the NIPC's efforts to educate, train, inform and involve the business and public sector in information security is the National InfraGard Program.
- Established in January of 2001, the National InfraGard Program began as a cooperative effort between the FBI's Cleveland Field Office and local technology professionals.
- Another key federal agency is the National Security Agency (NSA). The NSA is "the Nation's cryptologic organization. It coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information"
- The NSA is responsible for signal intelligence and information system security.
- The U.S. Secret Service is a department within the Department of the Treasury.
- The Secret Service is also charged with the detection and arrest of any person committing a U.S. Federal offense relating to computer fraud and false identification crimes.

- This represents an extension of the original mission of protecting U.S. currency-related issues to areas of communications fraud and abuse.

RISK MANAGEMENT

Introduction

The Security Systems Development Life Cycle (or SecSDLC) is a process framework or methodology that can be used in a flexible fashion to assist organizations in deploying information security initiatives.

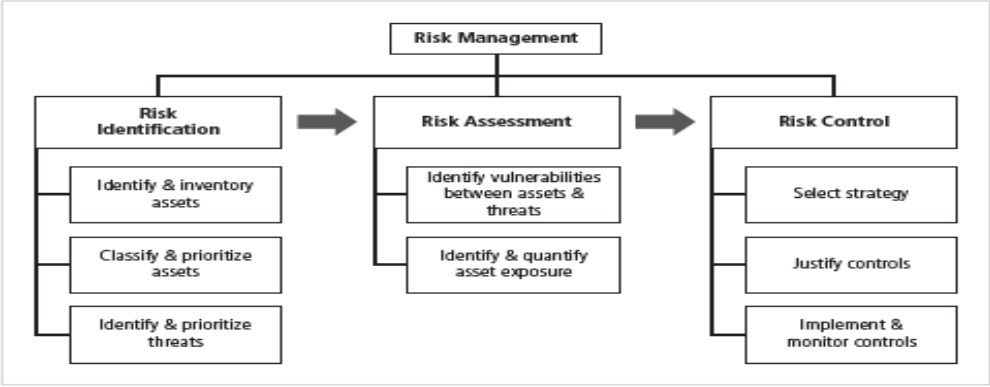
Risk identification is the formal process of examining and documenting the current information technology security situation.

Risk identification is conducted within the larger process of identifying and justifying risk controls, known as **risk management**.

An Overview of Risk Management

- **Know yourself**: identify, examine, and understand the information and systems currently in place
- **Know the enemy**: identify, examine, and understand threats facing the organization
- **Responsibility of each community of interest** within an organization to manage risks that are encountered

COMPONENTS OF RISK MANAGEMENT



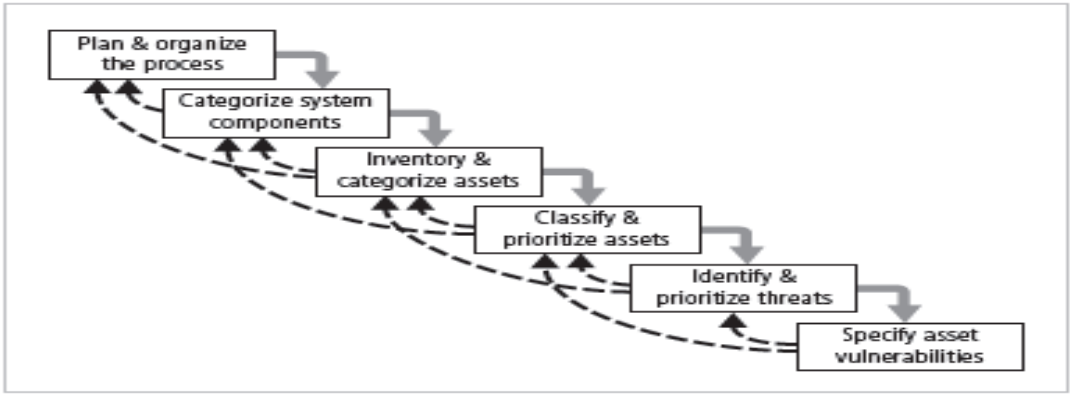
Roles of the Communities of Interest

- Information security, management and users, and information technology all must work together
- Communities of interest are responsible for:
  - Evaluating the risk controls
  - Determining which control options are cost effective for the organization
  - Acquiring or installing the needed controls
  - Ensuring that the controls remain effective

Risk Identification

- A risk management strategy calls on us to "know ourselves" by identifying, classifying, and prioritizing the organization's information assets.
- These assets are the targets of various threats and threat agents, and our goal is to protect them from these threats.
- Once we have gone through the process of self-examination, we then move into threat identification.
- We must assess the circumstances and setting of each information asset.
- To begin managing the risk from the vulnerabilities, we must identify those vulnerabilities and begin exploring the controls that might be used to manage the risks.
- We begin the process by identifying and assessing the value of our information assets.

Components of risk identification



Plan and Organize the Process

- First step in the Risk Identification process is to follow your project management principles
- Begin by organizing a team with representation across all affected groups

- The process must then be planned out
  - Periodic deliverables
  - Reviews
  - Presentations to management
- Tasks laid out, assignments made and timetables discussed

Asset Identification and Valuation

- This iterative process begins with the identification of assets, including all of the elements of an organization's system: people, procedures, data and information, software, hardware, and networking elements.
- Then, we classify and categorize the assets adding details as we dig deeper into the analysis.

Categorizing components of information systems

Traditional System Components	SesSDLC Components	Risk Management System Components
People	Employees	Trusted employees Other staff
	Nonemployees	People at trusted organizations Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive procedures
Data	Information	Transmission Processing Storage
Software	Software	Applications Operating systems Security components
Hardware	System devices and peripherals	Systems and peripherals Security devices
	Networking components	Intranet components Internet or DMZ components

People, Procedures, and Data Asset Identification

Unlike the tangible hardware and software elements already described, the human resources, documentation, and data information assets are not as readily discovered and documented.

These assets should be identified, described, and evaluated by people using knowledge, experience, and judgment.

As these elements are identified, they should also be recorded into some reliable data-handling process.

For People:

- Position name/number/ID – Try to stay away from names and stick to identifying positions, roles or functions
- Supervisor
- Security clearance level
- Special skills

Hardware, Software, and Network Asset Identification

- What information attributes to track depends on:
  - Needs of organization/risk management efforts
  - Preferences/needs of the security and information technology communities
- Asset attributes to be considered are: name; IP address; MAC address; element type; serial number; manufacturer name; model/part number; software version; physical or logical location; controlling entity
- Automated tools can identify system elements for hardware, software, and network components

Data Classification and Management

- A variety of classification schemes are used by corporate and military organizations.
- Information owners are responsible for classifying the information assets for which they are responsible.
- At least once a year, information owners must review information classifications to ensure the information is still classified correctly and the appropriate access controls are in place.
- The U.S. Military Classification Scheme has a more complex categorization system than required by most corporations. For most information, the military uses a five-level classification scheme: Unclassified, Sensitive But Unclassified (i.e., For Official Use Only), Confidential, Secret, and Top Secret.
- Most organizations do not need the detailed level of classification used by the military or federal agencies. A simple scheme will allow the organization to protect its sensitive information, such as: Public, For official use only, Sensitive, Classified.

- **Security Clearances:** The other side of the data classification scheme is the personnel security clearance structure. For each user of data in the organization, a single level of authorization must be assigned, indicating the level of classification he or she is authorized to view.
- Before individuals are allowed access to a specific set of data, they must meet the need-to-know requirement.
- This extra level of protection ensures that the confidentiality of information is properly maintained.
- **Management of Classified Data**: Requirements for the management of information include the storage, distribution, portability, and destruction of classified information.
- Information that has a classification designation other than unclassified or public must be clearly marked as such.
- When classified data is stored, it must be unavailable to unauthorized individuals.
- When an individual carries classified information, it should be inconspicuous, as in a locked briefcase or portfolio.
- The **clean desk policy** requires each employee to secure any and all information in its appropriate storage container at the end of each day.
- When classified information is no longer valuable or excessive copies exist, proper care should be taken to destroy any unneeded copies through shredding, burning, or transfer to an authorized document destruction service.
- There are those individuals who would not hesitate to engage in **dumpster diving** to retrieve information that could prove embarrassing or compromise the security of information in the organization.

Information Asset Classification

- Many organizations already have a classification scheme.
- Examples of these kinds of classifications are confidential data, internal data, and public data. Informal organizations may have to organize themselves to create a usable data classification model.

- The other side of the data classification scheme is the personnel security clearance structure, identifying the level of information each individual is authorized to view, based on his or her need-to-know.

Information Asset Valuation

- As each asset of the organization is assigned to its category, these questions will assist in developing the criteria to be used for asset valuation:

a) Which information asset is the most critical to the success of the organization?
b) Which information asset generates the most revenue?
c) Which information asset generates the most profitability?
d) Which information asset would be the most expensive to replace?
e) Which information asset would be the most expensive to protect?
f) Which information asset would be the most embarrassing or cause the greatest liability if revealed?

Sample inventory work sheet

System Name: SLS E-Commerce
Date Evaluated: February 2006
Evaluated By: D. Jones

Information assets	Data classification	Impact to profitability
Information Transmitted:		
EDI Document Set 1—Logistics BOL to outsourcer (outbound)	Confidential	High
EDI Document Set 2—Supplier orders (outbound)	Confidential	High
EDI Document Set 2—Supplier fulfillment advice (inbound)	Confidential	Medium
Customer order via SSL (inbound)	Confidential	Critical
Customer service Request via e-mail (inbound)	Private	Medium
DMZ Assets:		
Edge Router	Public	Critical
Web server #1—home page and core site	Public	Critical
Web server #2—Application server	Private	Critical

Notes: BOL: Bill of Lading:
DMZ: Demilitarized Zone
EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

- In order to finalize this step of the information asset identification process, each organization should create a weighting for each category based on the answers to the previous questions.
- Which factor is the most important to the organization?
- Once each question has been weighted, calculating the importance of each asset is straightforward. The final step is to list the assets in order of importance. This can be achieved by using a weighted factor analysis worksheet.

Information Asset	Criteria 1: Impact to Revenue	Criteria 2: Impact to Profitability	Criteria 3: Impact to Public Image	Weighted Score
Criterion Weight (1-100) Must total 100	30	40	30	
EDI Document Set 1—Logistics BOL to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2—Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2—Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1.0	1.0	1.0	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

The above table shows Example of a Weighted Factor Analysis Worksheet

EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

Threat Identification

Each of these threats identified has the potential to attack any of the assets protected.
If we assume every threat can and will attack every information asset, this will quickly become more complex and overwhelm the ability to plan.
To make this part of the process manageable, each step in the threat identification and vulnerability identification process is managed separately and then coordinated at the end of the process.

Various threats to information security is listed in the following table

Threat	Example
Compromises to intellectual property	Piracy, copyright infringement
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, flood, earthquake, lightning
Human error or failure	Accidents, employee mistakes, failure to follow policy
Information extortion	Blackmail of information disclosure
Missing, inadequate, or incomplete controls	Software controls, physical security
Missing, inadequate, or incomplete organizational policy or planning	Training issues, privacy, lack of effective policy
Quality of service deviations from service providers	Power and WAN quality of service issues
Sabotage or vandalism	Destruction of systems or information
Software attacks	Viruses, worms, macros, denial of service
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of property

Vulnerability Identification

- Specific avenues threat agents can exploit to attack an information asset are called vulnerabilities
- Examine how each threat could be perpetrated and list organization's assets and vulnerabilities
- Process works best when people with diverse backgrounds within organization work iteratively in a series of brainstorming sessions
- At end of risk identification process, list of assets and their vulnerabilities is achieved

Risk Assessment

- We can determine the relative risk for each of the vulnerabilities through a process called **risk assessment**.
- Risk assessment assigns a risk rating or score to each specific information asset, which is useful in gauging the relative risk introduced by each vulnerable information asset and making comparative ratings later in the risk control process.

Likelihood

- The probability that a specific vulnerability will be the object of a successful attack
- Assign numeric value: number between 0.1 (low) and 1.0 (high), or a number between 1 and 100
- Zero not used since vulnerabilities with zero likelihood are removed from asset/vulnerability list

- Use selected rating model consistently
- Use external references for values that have been reviewed/adjusted for your circumstances

Risk Determination

For the purpose of relative risk assessment:

risk = likelihood of vulnerability occurrence times
value (or impact)
minus
percentage risk already controlled
plus
an element of uncertainty

Identify Possible Controls

- For each threat and associated vulnerabilities that have residual risk, create preliminary list of control ideas
- Residual risk is risk that remains to information asset even after existing control has been applied
- There are three general categories of controls:
  - Policies
  - Programs
  - Technologies

Documenting Results of Risk Assessment

The goal of this process has been to identify the information assets of the organization that have specific vulnerabilities and create a list of them, ranked for focus on those most needing protection first.

In preparing this list, we have collected and preserved a wealth of factual information about the assets, the threats they face, and the vulnerabilities they experience.

We should also have collected some information about the controls that are already in place.

Ranked vulnerability risk worksheet

Asset	Asset Impact or Relative Value	Vulnerability	Vulnerability Likelihood	Risk-Rating Factor
Customer service request via e-mail (inbound)	55	E-mail disruption due to hardware failure	0.2	11
Customer order via SSL (inbound)	100	Lost orders due to web server hardware failure	0.1	10
Customer order via SSL (inbound)	100	Lost orders due to Web server or ISP service failure	0.1	10
Customer service request via e-mail (inbound)	55	E-mail disruption due to SMTP mail relay attack	0.1	5.5
Customer service request via e-mail (inbound)	55	E-mail disruption due to ISP service failure	0.1	5.5
Customer order via SSL (inbound)	100	Lost orders due to Web server denial-of-service attack	0.025	2.5
Customer order via SSL (inbound)	100	Lost orders due to Web server software failure	0.01	1

Risk identification and assessment deliverables

Table is shown below

Deliverable	Purpose
Information asset classification worksheet	Assembles information assets and their impac
Weighted criteria analysis worksheet	Assigns ranked value each information asset
Ranked vulnerability risk worksheet	Assigns ranked value each uncontrolled asse

Risk Control Strategies

When organizational management has determined that risks from information security threats are creating a competitive disadvantage, they empower the information technology and information security communities of interest to control the risks.
Once the project team for information security development has created the Ranked Vulnerability Worksheet, the team must choose one of four basic strategies to control the risks that result from these vulnerabilities.
The four risk strategies guide an organization to:
1. Apply safeguards that eliminate or reduce the remaining uncontrolled risks for the vulnerability (avoidance)
2. Transfer the risk to other areas or to outside entities (transference)
3. Reduce the impact should the vulnerability be exploited (mitigation)
4. Inform themselves of all of the consequences and accept the risk without control or mitigation (acceptance)

Defend

Defend is the risk control strategy that attempts to prevent the realization or exploitation of the vulnerability. This is the preferred approach, as it seeks to avoid risk in its entirety rather than deal with it after it has been realized.

Avoidance is accomplished through countering threats, removing vulnerabilities in assets, limiting access to assets, and/or adding protective safeguards.

The most common methods of avoidance involve three areas of controls, avoidance through application of policy, training and education, and technology.

Transfer

Transfer is the control approach that attempts to shift the risk to other assets, other processes, or other organizations.

If an organization does not already have quality security management and administration experience, it should hire individuals or firms that provide such expertise.

This allows the organization to transfer the risk associated with the management of these complex systems to another organization with established experience in dealing with those risks.

Mitigation

Mitigation is the control approach that attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation.

This approach includes three types of plans: disaster recovery planning (DRP), business continuity planning (BCP), and incident response planning (IRP).

Mitigation begins with the early detection that an attack is in progress.

The most common of the mitigation procedures is the disaster recovery plan.

The DRP includes the entire spectrum of activities to recover from an incident. The DRP can include strategies to limit losses before and during the disaster.

DRPs usually include all preparations for the recovery process, strategies to limit losses during the disaster, and detailed steps to follow when the disaster has ended.

The actions an organization can and perhaps should take while the incident is in progress should be defined in a document referred to as the incident response plan or IRP.

The IRP provides answers to questions victims might pose in the midst of a disaster.

It answers the questions:

What do I do NOW?!

What should the administrators do first?

Who should they contact?

What should they document?

DRP and IRP planning overlap to a degree. In many regards, the DRP is the subsection of the IRP that covers disastrous events.

While some DRP and IRP decisions and actions are the same, their urgency and results can differ dramatically.

The DRP focuses more on preparations completed before and actions taken after the incident, while the IRP focuses on intelligence gathering, information analysis, coordinated decision making, and urgent, concrete actions.

The third type of planning document under mitigation is the business continuity plan or BCP.

The BCP is the most strategic and long-term plan of the three plans. It encompasses the continuation of business activities if a catastrophic event occurs, such as the loss of an entire database, building, or operations center.

The BCP includes planning for the steps to insure the continuation of the organization when the scope or scale of a disaster exceeds the DRP's ability to restore operations.

Accept

With the acceptance control approach, an organization evaluates the risk of a vulnerability and allows the risky state to continue as is.

The only acceptance strategy that is recognized as valid occurs when the organization has:

- Determined the level of risk
- Assessed the probability of attack
- Estimated the potential damage that could occur from these attacks
- Performed a thorough cost benefit analysis
- Evaluated controls using each appropriate type of feasibility
- Decided that the particular function, service, information, or asset did not justify the cost of protection

Acceptance of risk is the choice to do nothing to protect a vulnerability and to accept the outcome of its exploitation.

This control, or rather lack of control, is based on the assumption that it may be a prudent business decision to examine the alternatives and determine that the cost of protecting an asset does not justify the security expenditure.

The term risk appetite is used to describe the degree to which an organization is willing to accept risk as a trade-off to the expense of applying controls.

Terminate

The terminate control strategy directs the organization to avoid those business activities that introduce uncontrollable risks.

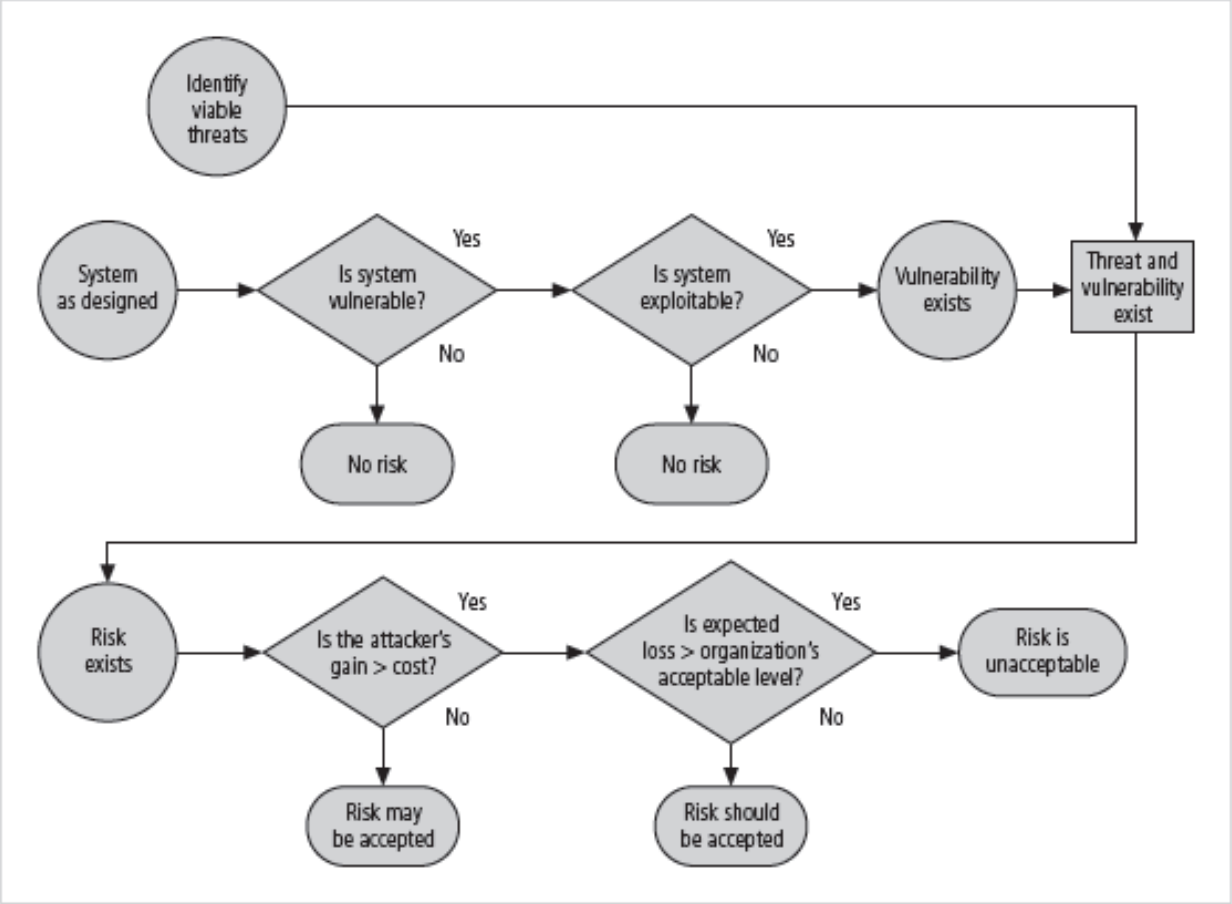
Mitigation Strategy Selection

The level of threat and value of the asset should play a major role in the selection of strategy.

The following rules of thumb can be applied in selecting the preferred strategy:

- When a vulnerability exists, implement assurance techniques to reduce the likelihood of a vulnerability being exercised.
- When a vulnerability can be exploited, apply layered protections, architectural designs, and administrative controls to minimize the risk or prevent this occurrence.
- When the attacker's cost is less than his or her potential gain, apply protections to increase the attacker's cost (e.g., use system controls to limit what a system user can access and do, thereby significantly reducing an attacker's gain).
- When potential loss is substantial, apply design principles, architectural designs, and technical and nontechnical protections to limit the extent of the attack, thereby reducing the potential for loss.

Risk handling decision points



Feasibility Studies and the Cost Benefit Analysis

Before deciding on the strategy for a specific vulnerability, all information about the economic and noneconomic consequences of the vulnerability facing the information asset must be explored.

Fundamentally we are asking, "What are the actual and perceived advantages of implementing a control contrasted with the actual and perceived disadvantages of implementing the control?"

Cost Benefit Analysis (CBA)

The approach most commonly considered for a project of information security controls and safeguards is the economic feasibility of implementation.

An organization begins by evaluating the worth of the information assets to be protected and the loss in value if those information assets are compromised by the specific vulnerability.

It is only common sense that an organization should not spend more to protect an asset than it is worth.

The formal process to document this is called a cost benefit analysis or an economic feasibility study.

CBA: Factors

Some of the items that impact the cost of a control or safeguard include:

- Cost of development or acquisition
- Training fees
- Cost of implementation
- Service costs
- Cost of maintenance

CBA: Loss Estimates

- Once an organization has estimated the worth of various assets, it can begin to examine the potential loss that could occur from the exploitation of vulnerability or a threat occurrence. This process results in the estimate of potential loss per risk.
- The questions that must be asked here include:
- What damage could occur, and what financial impact would it have?
- What would it cost to recover from the attack, in addition to the costs from the previous question?
- What is the single loss expectancy for each risk?

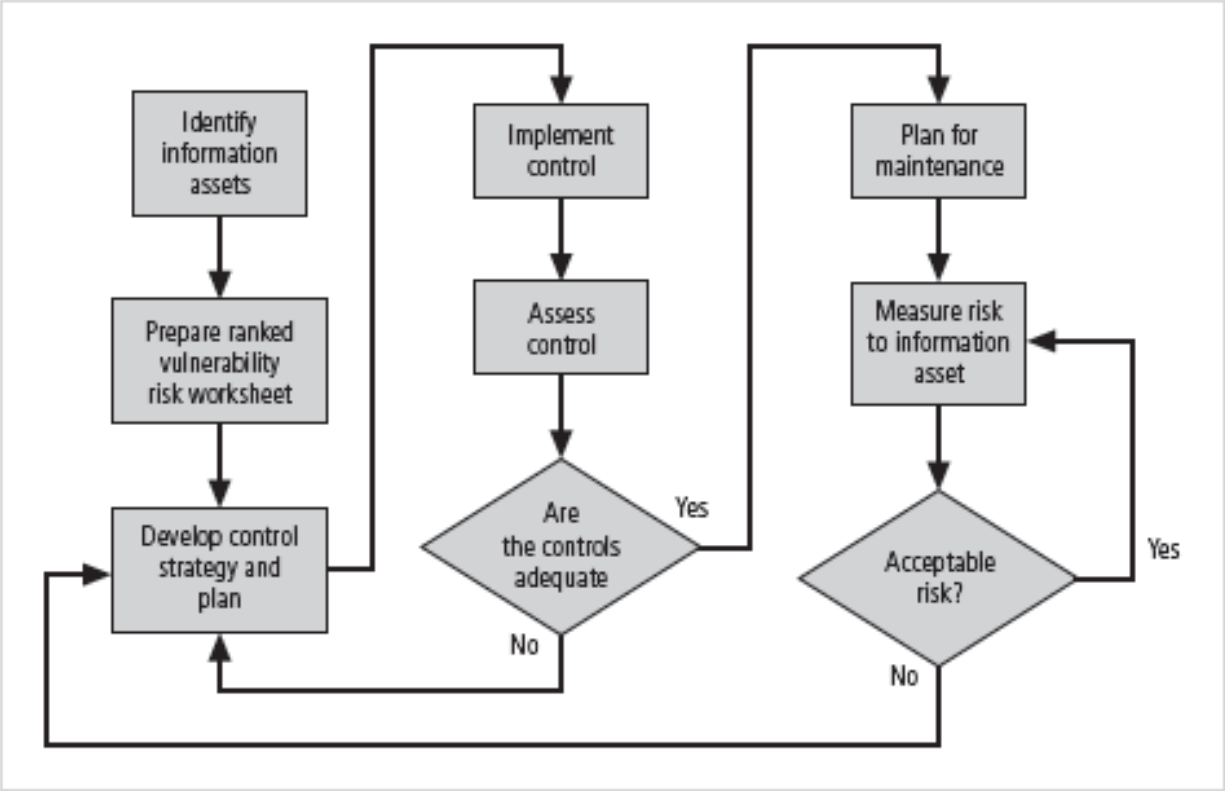
CBA: Formula

- In its simplest definition, CBA is whether or not the control alternative being evaluated is worth the associated cost incurred to control the specific vulnerability.
- While many CBA techniques exist, for our purposes, the CBA is most easily calculated using the ALE from earlier assessments.
- CBA = ALE(prior) – ALE(post) – ACS
- ALE prior is the Annualized Loss Expectancy of the risk before the implementation of the control.
- ALE post is the ALE examined after the control has been in place for a period of time.
- ACS is the Annual Cost of the Safeguard.

Evaluation, Assessment, and Maintenance of Risk Controls

- Selection and implementation of control strategy is not end of process
- Strategy and accompanying controls must be monitored/reevaluated on ongoing basis to determine effectiveness and to calculate more accurately the estimated residual risk
- Process continues as long as organization continues to function

Risk control cycle



Quantitative versus Qualitative Risk Control Practices

- Performing the previous steps using actual values or estimates is known as quantitative assessment
- Possible to complete steps using evaluation process based on characteristics using nonnumerical measures; called qualitative assessment
- Utilizing scales rather than specific estimates relieves organization from difficulty of determining exact values

Benchmarking

An alternative strategy to the cost benefit analysis and its attempt to place a hard dollar figure on each information asset is to approach risk management from a different angle.

Instead of determining the financial value of information and then implementing security as an acceptable percentage of that value, an organization could look at peer institutions to determine what others are doing to protect their information (benchmarking).

Benchmarking is the process of seeking out and studying the practices used in other organizations that produce the results you desire in your organization.

When benchmarking, an organization typically uses one of two measures to compare practices, to determine which practices it would prefer to implement.

These are metrics-based measures and process-based measures.

Metrics-based measures are comparisons based on numerical standards, such as:

- Numbers of successful attacks
- Staff-hours spent on systems protection
- Dollars spent on protection
- Numbers of security personnel
- Estimated losses in dollars of information due to successful attacks
- Loss in productivity hours associated with successful attacks

An organization uses this information by ranking competitive businesses within a similar size or market and determining how their measures compare to others.

Process-based measures are generally less number-focused and more strategic than metrics-based measures.

For each of the areas the organization is interested in benchmarking, process-based measures enable the companies to examine the activities an individual company performs in pursuit of its goal, rather than the specifics of how goals were attained.

The primary focus is the method the organization uses to accomplish a particular process, rather than the outcome.

In information security, two categories of benchmarks are used: standards of due care/due diligence and best practices.

Within best practices is a subcategory of practices referred to as the gold standard, those practices typically viewed as "the best of the best."

Due Care/Due Diligence

When organizations adopt levels of security for a legal defense, they may need to show that they have done what any prudent organization would do in similar circumstances. This is referred to as a standard of due care.

It is insufficient to just implement these standards and then ignore them. The application of controls at or above the prescribed levels and the maintenance of those standards of due care show that the organization has performed due diligence.

Due diligence is the demonstration that the organization is diligent in ensuring that the implemented standards continue to provide the required level of protection.

Failure to support a standard of due care or due diligence can open an organization to legal liability, provided it can be shown that the organization was negligent in its application or lack of application of information protection.

Best Business Practices

Security efforts that seek to provide a superior level of performance in the protection of information are referred to as best business practices or simply best practices or recommended practices.

Best security practices (BSPs) are those security efforts that are among the best in the industry, balancing the need to access with the need to provide adequate protection.

Best practices seek to provide as much security as possible for information and systems while maintaining a solid degree of fiscal responsibility.

When considering best practices for adoption in your organization, consider the following:

Does your organization resemble the identified target organization of the best practice?

Are the resources you can expend similar to those identified in the best practice? A best practice proposal that assumes unlimited funding and does not identify needed trade-offs will be of limited value if your approach has strict resource limits.

Are you in a similar threat environment as that proposed in the best practice? A proposal of best practice from months and even weeks ago may not be appropriate for the current threat environment.

Problems with Benchmarking and Best Practices

The biggest problem with benchmarking in information security is that organizations don't talk to each other.

Another problem with benchmarking is that no two organizations are identical.

A third problem is that best practices are a moving target. What worked well two years ago may be completely worthless against today's threats.

One last issue to consider is that simply knowing what was going on a few years ago, as in benchmarking, doesn't necessarily tell us what to do next.

Baselining

Baselining is the analysis of measures against established standards.

In information security, baselining is the comparison of security activities and events against the organization's future performance.

When baselining, it is useful to have a guide to the overall process.

Other Feasibility Studies

- **Organizational:** examines how well proposed IS alternatives will contribute to organization's efficiency, effectiveness, and overall operation
- **Operational:** examines user and management acceptance and support, and the overall requirements of the organization's stakeholders
- **Technical:** examines if organization has or can acquire the technology necessary to implement and support the control alternatives
- **Political:** defines what can/cannot occur based on consensus and relationships

Risk Management Discussion Points

Not every organization has the collective will to manage each vulnerability through the application of controls.

Depending on the willingness to assume risk, each organization must define its risk appetite.

Risk appetite defines the quantity and nature of risk that organizations are willing to accept as they evaluate the trade-offs between perfect security and unlimited accessibility.

Above diagram represents residual risk

Documenting Results

At minimum, each information asset-vulnerability pair should have a documented control strategy that clearly identifies any residual risk remaining after the proposed strategy has been executed.

Some organizations document the outcome of the control strategy for each information asset-vulnerability pair as an action plan.

This action plan includes concrete tasks, each with accountability assigned to an organizational unit or to an individual.

Recommended Practices in Controlling Risk

We must convince budget authorities to spend up to the value of the asset to protect a particular asset from an identified threat.

Each and every control or safeguard implemented will impact more than one threat-asset pair.

Between the impossible task associated with the valuation of information assets and the dynamic nature of the ALE calculations, it's no wonder organizations are looking for a more straightforward method of implementing controls that doesn't involve such imperfect calculations.