UNIT II

Law and Ethics in Information Security

As individuals, we elect to trade some aspects of personal freedom for social order. Laws are rules that mandate or prohibit certain behaviour in society. They are drawn from ethics, which define socially acceptable behaviours. Ethics are based on cultural mores and express the fixed moral attitudes or customs of a particular group. Some ethics are recognized as universal among cultures.

Organizational Liability and the Need for Counsel

Even if there is no breach of criminal law, there can still be liability. Liability is the legal obligation of an entity that extends beyond criminal or contract law; it includes the legal obligation to make restitution, or to compensate for wrongs committed by an organization or its employees. An organization increases its liability if it refuses to take measures known as due care. Due care has to be taken when an organization makes sure that every employee knows what is acceptable or unacceptable behaviour, and knows the consequences of illegal or unethical actions. Due diligence requires that an organization make a valid effort to protect others and continually maintain this level of effort. Under the U.S. legal system, any court can impose its authority over an individual or organization if it can establish jurisdiction—that is, the court's right to hear a case if the wrong was committed in its territory or involving its citizenry. Trying a case in the injured party's home area is usually favourable to the injured party.

Policy versus Law

Within an organization, information security professionals help maintain security via the establishment and enforcement of policies. These policies—a body of expectations that describe acceptable and unacceptable employee behaviours in the workplace—function as organizational laws, complete with penalties, judicial practices, and sanctions to require compliance. Policies function as laws and must be crafted with the same care to ensure that they are complete, appropriate, and fairly applied to everyone in the workplace. The difference between a policy and a law, which is that ignorance of a policy is an acceptable defense.

For a policy to be enforceable, it must meet the following five criteria and demonstrate that it has done so:

- Dissemination (distribution)
- Review (reading)
- Comprehension (understanding)
- Compliance (agreement)
- Uniform enforcement

When all of these conditions are met can an organization penalize employees who violate the policy, without fear of legal retribution.

Types of Law

- Civil law represents a wide variety of laws that govern a nation or state and deal with the relationships and conflicts between organizational entities and people.
- Criminal law addresses violations harmful to society and is actively enforced by the state.
- 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** (**CFA Act**) is the cornerstone of many computer-related federal laws and enforcement efforts. The **National Information Infrastructure Protection Act of 1996** amended the CFA Act in October 1996. It modified several sections of the CFA and increased the penalties for selected crimes. The severity of the penalty depends on the value of the information obtained and whether the offense is judged to have been committed:

- For purposes of commercial advantage
- For private financial gain
- In furtherance of a criminal act

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

Note that in 2006, this act was amended with the **USA PATRIOT Improvement and Reauthorization Act**, which made permanent 14 of the 16 expanded powers of the Department of Homeland Security and the FBI in investigating terrorist activity. The act also reset the date of expiration written into the law for certain wiretaps under the Foreign Intelligence Surveillance Act of 1978 (FISA) and revised many of the criminal penalties and procedures associated with criminal and terrorist activities. The **Computer Security Act of 1987** 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 security at the beginning of the 21st century. The ability to collect information, combine facts from separate sources, and merge it all with other information has resulted in databases of information that were previously impossible to set up. In response to pressure for privacy protection, the number of statutes addressing an individual's right to privacy has grown. It must be understood, however, that privacy in this context is not absolute freedom from observation, but rather is a more precise "state of being free from unsanctioned intrusion."

Privacy of Customer Information

The **Privacy of Customer Information Section** of the 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 their 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. Aggregate information is created by combining pieces of non-private data—often collected during software updates, and via cookies—that when combined may violate privacy. The **Federal Privacy Act of 1974** regulates government agencies and holds them

accountable if they release private information about individuals or businesses 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 U.S. Constitution**, which protects citizens from unlawful search and seizure.

The **Health Insurance Portability & Accountability Act Of 1996** (**HIPAA**), also known as the **Kennedy-Kassebaum Act**, protects the confidentiality and security of health-care data by establishing and enforcing standards and by standardizing electronic data interchange. This act impacts all health-care organizations. The act requires organizations that retain health-care information to use information security mechanisms to protect this information, as well as policies and procedures to maintain this security. The act 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 health-care 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. The standards also restrict the use of health information to the minimum necessary for the health-care services required.

1. HIPAA has five fundamental principles:
2. Consumer control of medical information
3. Boundaries on the use of medical information
4. Accountability for the privacy of private information
5. Balance of public responsibility for the use of medical information for the greater good measured against impact to the individual
6. Security of health information

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 nonpublic 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 both fully disclosed when a customer initiates a business relationship and distributed at least annually for the duration of the professional association.

Identity theft

The Federal Trade Commission defines identity theft as "occurring when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes". In May of 2006, President Bush signed an Executive Order creating the Identity Theft Task Force. The goals of this group are to create a strategic plan to improve efforts of the government and private organizations and individuals in combating identity theft. The group seeks better coordination among groups, more effective prosecution of criminals engaged in these activities, and methods to increase restitution made to victims. While numerous states have passed identity theft laws, at the federal level the primary legislation is the **Fraud And Related Activity In Connection With Identification Documents, Authentication Features, And Information** (Title 18, U.S.C. § 1028), which criminalizes creation, reproduction, transfer, possession, or use of unauthorized or false identification documents or document-making equipment. Penalties for such offenses range from one to 25 years in prison and fines as determined by the courts.

The Federal Trade Commission recommends the following four steps people can take when they suspect a theft of identity has occurred:

- Report to the three dominant consumer reporting companies that your identity is threatened so that they may place a fraud alert on your record. This informs current and potential creditors to follow certain procedures before taking credit-related actions.
- If you know which accounts have been compromised, close them. If new accounts are opened using your identity without your permission, the U.S. FTC has provided a document template online that may be used to dispute these new accounts
- Register your concern with the U.S. FTC.
- Report the incident to either your local police or police in the location where the identity theft occurred. Use your copy of the FTC ID Theft complaint form to make the report. Once your police report has been filed, be sure to get a copy of it or else acquire the police report number.

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 1999** (**SAFE**) provides guidance on the use of encryption and provides measures of protection from government intervention.

U.S. Copyright Law

Intellectual property is recognized as a protected asset in the United States. U.S. copyright laws extend this privilege to the published word, including electronic formats. The fair use of copyrighted materials includes their use to support news reporting, teaching, scholarship, and a number of other related activities, as long as the use is for educational or library purposes, not for profit, and is not excessive. As long as proper acknowledgment is provided to the original author of such works, including a proper citation, and the work is not represented as one's own, it is entirely permissible to include portions of someone else's work as reference.

Financial Reporting

Sarbanes-Oxley Act of 2002 is a critical piece of legislation that affects the executive management of publicly traded corporations and public accounting firms, seeks to improve the reliability and accuracy of financial reporting, as well as increase the accountability of corporate governance, in publicly traded companies. The executives working in firms covered by this law will seek assurance on the reliability and quality of information systems from senior information technology managers who, in turn, will likely ask information security managers to verify the confidentiality and integrity of those same information systems.

Freedom of Information Act of 1966 (FOIA)

The Freedom of Information Act allows any person to request access to federal agency records or information not determined to be a matter of national security. U.S. government agencies are required to disclose any requested information upon receipt of a written request. Some information is protected from disclosure, however, 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 and Local Regulations

In addition to the national and international restrictions placed on organizational use of computer technology, each state or locality may have a number of its own applicable laws and regulations. The information security professional must understand state laws and regulations and ensure that the organization's security policies and procedures comply with those laws and regulations.

International Laws and Legal Bodies

It is important for IT professionals and information security practitioners to realize that when their organizations do business on the Internet, they do business globally. As a result, these professionals must be sensitive to the laws and ethical values of many different cultures, societies, and countries. While there are currently few international laws relating to privacy and information security, the few that do exist are important but are limited in their enforceability.

European Council Cyber-Crime Convention

The Council of Europe adopted the **European Council Cyber-Crime Convention** in 2001.

- It provides for the creation of an international task force to oversee a range of security functions associated with Internet activities for standardized technology laws across international borders.
- It also attempts to improve the effectiveness of international investigations into breaches of technology law.

While 34 countries attended the signing in November 2001, only 18 nations, including the U.S., have ratified the Convention as of February 2007. While the U.S. is technically not a "member state of the council of Europe" but does participate in the convention. The Cyber-Crime Convention lacks any realistic provisions for enforcement. The overall goal of the convention is to simplify the acquisition of information for law enforcement agencies in certain types of international crimes. It also simplifies the extradition process.

Agreement on Trade-Related Aspects of Intellectual Property Rights

The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), created by the World Trade Organization (WTO), introduced intellectual property rules into the multilateral trade system. This agreement is the first significant international effort to protect the intellectual property rights of individuals and of sovereign nations. This agreement outlines requirements for governmental oversight and legislation of WTO member countries to provide minimum levels of protection for intellectual property.

The WTO TRIPS agreement covers five issues:

- How basic principles of the trading system and other international intellectual property agreements should be applied
- How to give adequate protection to intellectual property rights
- How countries should enforce those rights adequately in their own territories
- How to settle disputes on intellectual property between members of the WTO
- Special transitional arrangements during the period when the new system is being introduced

Digital Millennium Copyright Act (DMCA)

The **Digital Millennium Copyright Act** (**DMCA**) is the American contribution to an international effort to reduce the impact of copyright, trademark, and privacy infringement, especially through the removal of technological copyright protection measures. In 1995 the European Union had adopted **Directive 95/46/EC**, which added protection for individuals with regard to the processing of personal data and the use and movement of such data. The United Kingdom has also already implemented a version of this law called the **Database Right**, in order to comply with Directive 95/46/EC.

The DMCA provisions are

- Protections and countermeasures implemented by copyright owners to control access to protected content may not be circumvented.
- Devices may not be manufactured to circumvent protections and countermeasures to control access to protected content.

- Trafficking in devices manufactured to circumvent protections and countermeasures to control access to protected content is banned.
- Information attached or imbedded into copyrighted material may not be altered.
- Internet service providers are excluded from certain forms of contributory copyright infringement.

Ethics and Information Security

Many professional groups have explicit rules governing ethical behavior in the workplace. The information technology field and the information security field do not have a binding code of ethics. Instead, professional associations (such as the Association for Computing Machinery and the Information Systems Security Association) and accreditation agencies (such as ISC2) work to establish the profession's ethical codes of conduct.

The "Ten Commandments of Computer Ethics" 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 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.

Ethical Differences across Cultures

Cultural differences can make it difficult to determine what is and is not ethical, especially when it comes to the use of computers. Difficulties arise when one nationality's ethical behavior violates the ethics of another national group. Approximately 90 percent of all

software is created in the United States. A study published in 1999 examined computer use ethics of nine nations: Singapore, Hong Kong, the United States, England, Australia, Sweden, Wales, and the Netherlands.

- This study selected a number of computer-use vignettes and presented them to students in universities in these nine nations.
- The responses indicated a degree of ethical sensitivity or knowledge about the performance of the individuals in the short case studies.
- The scenarios were grouped into three categories of ethical computer use: software license infringement, illicit use, and misuse of corporate resources.

Software license infringement.

- Overall, most of the nations studied by Dr.Whitman had similar attitudes toward software piracy.
- Statistically speaking, only the United States and the Netherlands had attitudes that differed substantially from those of all other countries examined.
- The United States was significantly less tolerant of piracy, while the Netherlands was significantly more permissive.
- Although a number of studies have reported that the Pacific Rim countries of Singapore and Hong Kong are hotbeds of software piracy, this study found their tolerance for copyright infringement to be moderate.
- This could mean is that the individuals surveyed understood what software license infringement was but felt either that their use was not piracy, or that their society permitted this piracy in some way.
- Peer pressure, the lack of legal disincentives, the lack of punitive measures, or any one of a number of other reasons could also explain why these alleged piracy centers were not oblivious to intellectual property laws.

Illicit use

- The study respondents unilaterally condemned viruses, hacking, and other forms of system abuse.
- There were, however, different degrees of tolerance for such activities among the groups.

- The low overall degree of tolerance for illicit system use may be a function of the easy association between the common crimes of breaking and entering, trespassing, theft, and destruction of property to their computer-related counterparts.

Misuse of corporate resources.

- In general, individuals displayed a rather lenient view of personal use of company equipment.
- Only Singapore and Hong Kong view personal use of company equipment as unethical.
- With the exceptions of Singapore and Hong Kong, it is apparent that many individuals, regardless of cultural background, feel that if an organization does not specifically forbid personal use of its computing resources, such use is acceptable.
- Overall, the researchers found that there is a general agreement among nationalities as to what is acceptable or unacceptable computer use.
- There is, however, a range of views as to whether some actions are moderately or highly unacceptable.
- This study underscores the intercultural similarities that exist as much as it describes the differences between cultures.

Ethics and Education

Employees must be trained and kept aware of 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 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.

Deterring Unethical and Illegal Behavior

It is the responsibility of information security personnel to do everything in their power to deter illegal, immoral, or unethical behavior and to use policy, education and training, and technology to protect information and systems. Many security professionals understand the technology aspect of protection but underestimate the value of policy.

The three general causes of unethical and illegal behavior: ignorance, accident, and intent.

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

Many professional organizations have established codes of conduct 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, many employers do not encourage their employees to join these professional organizations. Security professionals must act ethically and according to the policies and procedures of their employers, their professional organizations, and the laws of society.

Major Professional Organizations for IT

Association of Computing Machinery (ACM).

- 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, Inc. (ISC) ^{2}

- The **(ISC)** ^{2} (www.isc2.org) is a nonprofit 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.
    - Advance and protect the profession.

System Administration, Networking, and Security Institute (SANS).

- **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 (ISACA).

- **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 (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.

Information Systems Security Association (ISSA).

- **ISSA** (www.issa.org) is a nonprofit 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.
- ISSA also promotes a code of ethics whose focus is "promoting management practices that will ensure the confidentiality, integrity, and availability of organizational information resources."

Key U.S. Federal Agencies

The key U.S. federal agencies charged with the protection of American information resources and the investigation of threats to, or attacks on, these resources. These agencies include the Department of Homeland Security (DHS), the Federal Bureau of Investigation's National Infrastructure Protection Center (NIPC), the National Security Administration, and the U.S. Secret Service. The Department of Homeland Security (DHS), which was created in 2003 through the Homeland Security Act of 2002, which was passed in response to the events of September 11, 2001. DHS is made up of five directorates, or divisions, through which it carries out its mission of protecting the people, as well as the physical and informational assets, of the United States.

The Directorate of Information & Infrastructure works to create and enhance capabilities used to discover and respond to attacks on national information systems and critical infrastructure. The Science and Technology Directorate is responsible for research and development activities in support of homeland defense. This effort is guided by a continuing examination of the vulnerabilities throughout the national infrastructure. It sponsors the emerging best practices developed to counter threats and weaknesses in the system.

The National InfraGard Program began as a cooperative effort between the FBI's Cleveland field office and local technology professionals, which was established in January of 2001. Every FBI field office has established an InfraGard chapter and collaborates with public and private organizations and the academic community to share information about attacks, vulnerabilities, and threats. The National InfraGard Program serves its members in four basic ways:

- Maintains an intrusion alert network using encrypted e-mail
- Maintains a secure Web site for communication about suspicious activity or intrusions
- Sponsors local chapter activities
- Operates a help desk for questions

The National Security Agency (NSA), which 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 NSA's Information Assurance

Directorate (IAD) provides information security "solutions including the technologies, specifications and criteria, products, product configurations, tools, standards, operational doctrine, and support activities needed to implement the project, detect and report, and respond elements of cyber defense." Prominent among the NSA's efforts and activities in the information security arena are the Information Security Outreach programs. The NSA recognizes universities that not only offer information security education, but ones that have also integrated information security philosophies and efforts into the internal operations of the schools. The NSA also has a program to certify curriculum in information security. The Information Assurance Courseware Evaluation process examines information security courses in an institution and, if accepted, provides a three-year accreditation. Graduates of these programs receive certificates that indicate this accreditation.

The U.S. Secret Service, which is a department within the Department of the Treasury. The Secret Service has been charged with the responsibility of detecting and arresting 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 to areas of communications fraud and abuse—a logical extension, given that the communications networks of the U.S. carry more funds than all of the armored cars in the world combined.

An Overview of Risk Management

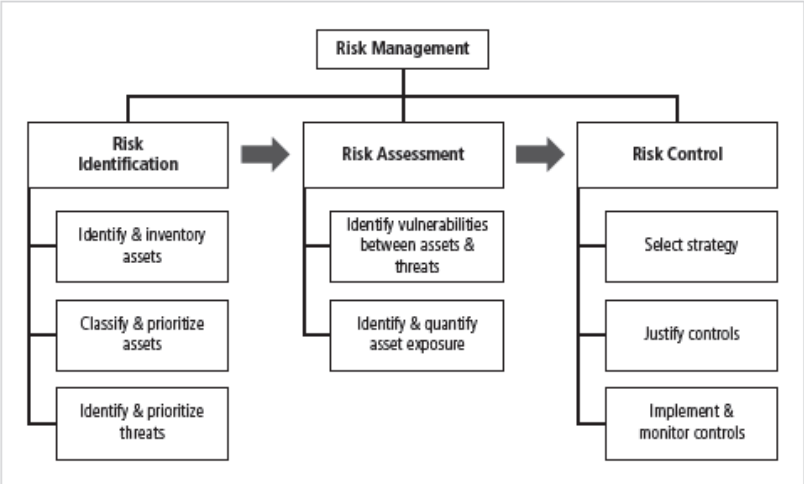

Figure: Components of Risk Management

Risk management is the process of identifying vulnerabilities in an organization's information systems and taking carefully reasoned steps to ensure the confidentiality, integrity,

and availability of all the components in the organization's information system. An organization needs to do when it depends on IT-based systems to remain viable, and information security and the discipline of risk management become an integral part of the economic basis for making business decisions. These decisions are based on trade-offs between the costs of applying information systems controls and the benefits realized from the operation of secured, available systems. Risk management requires two major undertakings: risk identification and risk control.

Risk identification, which is the process of examining and documenting the security posture of an organization's information technology and the risks it faces. Risk control, which is the process of applying controls to reduce the risks to an organization's data and information systems.

Know Yourself

We must first know ourselves by identifying, examining, and understanding the information and systems currently in place. In order to protect our assets, defined here as the systems that use, store, and transmit information, we have to understand everything about the information. These aspects have been examined, we can then look at what we are already doing to protect the information and systems from the threats.

Know the Enemy

For information security, knowing the enemy means identifying, examining, and understanding the threats that most directly affect our organization and the security of our organization's information assets. We can use our understanding of these aspects to create a list of threats prioritized by importance to the organization.

The Roles of the Communities of Interest

Each community of interest must manage the risks the organization encounters. Information security understands the threats and attacks that introduce risk into the organization. Management and users play a part in the early detection and response process; ensure that sufficient resources are allocated. Information technology assists in building secure systems and operating them safely. General management, IT management, and information

security management are collectively accountable for identifying and classifying all levels of risk. The three communities of interest that are also responsible for the following:

- 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 information security professionals to identify, classify, and prioritize their organizations' information assets. A threat assessment process is then undertaken to identify and quantify the risks facing each asset. This process is made up of steps to document the circumstances and settings of each information asset and to identify the vulnerabilities of those assets. When vulnerabilities are found, including identifying and assessing controls as to their capability to limit possible losses in the eventuality of attack.

Plan and Organize the Process

A risk management process requires applying the organization's project management principles to the risk management process. The process will need a proper project plan with periodic deliverables, including a task list and appropriate assignments.

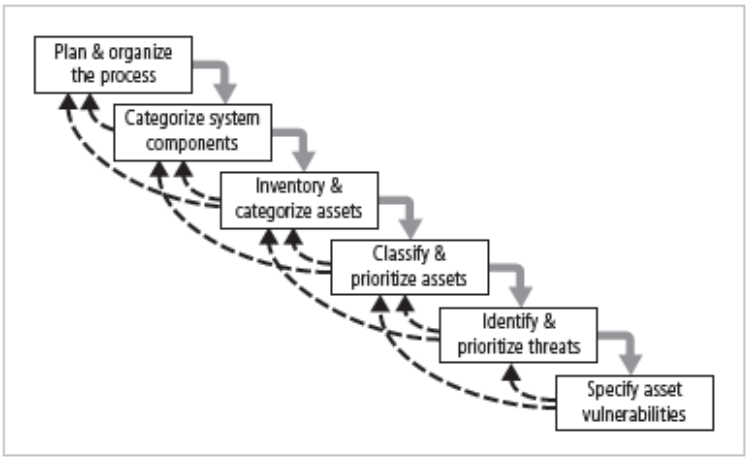

Figure: Components of Risk Identification

Asset Identification and Inventory

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

Identification of people, procedures, and data assets

Identifying human resources, documentation, and data information is more difficult than identifying hardware and software assets. As the people, procedures, and data assets are identified, they should be recorded using a reliable data-handling process. When deciding which information assets to track, consider the following asset attributes:

- People: Position name/number/ID (try to avoid names and stick to identifying positions, roles, or functions); supervisor; security clearance level; special skills
- Procedures: Description; intended purpose; relationship to software, hardware, and networking elements; storage location for reference; storage location for update
- Data: Classification; owner, creator, and manager; size of data structure; data structure used (sequential or relational); online or offline; location; backup procedures employed

As you develop the data-tracking process, consider carefully how much data should be tracked and for which specific assets. Most large organizations find that that they can only effectively track a few valuable facts about the most critical devices.

Identification of hardware, software, and network assets

Depending on the needs of the organization and its risk management efforts, as well as the preferences and needs of the management of the information security and information technology communities, when deciding which information assets to track, you may want to consider including these asset attributes:

- Name
- IP address
- MAC address
- Element type

- DeviceClass = S (server)
- DeviceOS = W2K (Windows 2000)
- DeviceCapacity = AS (advanced server)
- Hardware, software, and network asset identification
- Serial number
- Manufacturer's name
- Manufacturer's model number or part number
- Software version, update revision, or FCO number
- Physical location
- Logical location
- Controlling entity

Automated risk identification tools

- Automated tools can sometimes identify the system elements that make up the hardware, software, and network components.
- Once stored, typically in a database or in a form that can be exported to a database, the inventory list must be kept current by using a tool that periodically refreshes the data.
- In the later steps of risk management, which require involved calculations, the case is strong for the use of automated risk management tools for tracking information assets. At this point in the process, however, simple word-processing, spreadsheet, and database tools can provide adequate record keeping.

Data classification and management

- Corporate and military organizations use a variety of data classification schemes.
- Information owners are responsible for classifying the information assets for which they are responsible. Annually, they must review information classifications to ensure the information is still classified correctly and appropriate access controls are in place.
- The typical information classification scheme has three categories:
    - Confidential: Used for corporate information that must be tightly controlled, even within the company. Access to this information is strictly on a need-to-know basis or as required by the terms of a contract.

    - Internal: Used for internal information that does not meet the criteria for the confidential category. It is to be viewed only by corporate employees, authorized contractors, and other third parties.
    - External: This includes all information that has been approved by management for public release.

- 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 (SBU), Confidential, Secret, and Top Secret.
- The military also has some specialty classification ratings, such as Personnel Information and Evaluation Reports, to protect related areas of information. Federal agencies such as the FBI and CIA also use specialty classification schemes, like Need-to-Know and Named Projects.
- Most organizations do not need the detailed level of classification used by the military or federal agencies. A simple scheme, such as Public, For Official Use Only, Sensitive, and Classified, will allow the organization to protect its sensitive information.

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 that indicates the level of classification he or she is authorized to view.
- Before an individual is allowed access to a specific set of data, he or she 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

- Management of classified data includes its storage, distribution, portability, and destruction.
- Information that is not unclassified or public must be clearly marked as such.
- When classified data is stored, it must be available only to authorized individuals.
- When an individual carries classified information, it should be transported via inconspicuous means, such as in a locked briefcase or portfolio.

- The clean desk policy requires employees to secure all information in appropriate storage containers at the end of each day.
- When copies of classified information are no longer valuable or excessive copies exist, proper care should be taken to destroy them by means of shredding, burning, or transferring to an authorized document destruction service.
- It is important to enforce policies to ensure that no classified information is disposed of in trash or recycling areas since some individuals would not hesitate to engage in dumpster diving to retrieve information that could embarrass an organization or compromise information security.

Classifying and Prioritizing Information Assets

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 classification of components must be specific enough to allow determination of priority levels because the next step is to rank the components based on criteria established by the categorization. It is important that the categories be comprehensive and mutually exclusive. Comprehensive means that all information assets must fit in the list somewhere, and mutually exclusive means that an information asset should fit in only one category. The other side of the data classification scheme is the personnel security clearance structure, which identifies the level of information individuals are authorized to view based on what each person needs to know.

Information Asset Valuation

The questions that need posing as each asset of the organization is assigned to a category. These questions assist in developing the weighting criteria to be used for asset valuation. These questions include:

- Which information asset is the most critical to the success of the organization?
- Which information asset generates the most revenue?
- Which information asset generates the most profitability?
- Which information asset would be the most expensive to replace?
- Which information asset would be the most expensive to protect?

- Which information asset would be the most embarrassing or cause the greatest liability if revealed?

What is necessary to calculate, estimate or derive values for information assets, consideration might be given to the following:

- Value retained from the cost of creating the information asset
- Value retained from past maintenance of the information asset
- Value implied by the cost of replacing the information
- Value from providing the information
- Value incurred from the cost of protecting the information
- Value to owners
- Value of intellectual property
- Value to adversaries

How additional company-specific criteria may add value to the asset evaluation process and should be identified, documented, and added to the process. To finalize this step, the organization should assign a weight to each asset based on their given answers.

Information asset prioritization

- Once the process of inventorying and assessing value is complete, you can prioritize each asset using weighted factor analysis.
- In this process, each information asset is assigned a score for each critical factor. In addition, each critical factor is also assigned a weight (ranging from 1 to 100) to show that criteria's assigned importance for the organization.

Identify and Prioritize Threats

After identifying and performing the preliminary classification of an organization's information assets, the analysis phase examines the threats facing the organization. The realistic threats must be investigated further, while the unimportant threats are set aside. If you assume every threat can and will attack every information asset, the project scope quickly becomes so complex it overwhelms the ability to plan. Each threat must be examined to assess its potential impact on the organization. This is referred to as a threat assessment.

To frame the discussion of threat assessment, you must address each threat with a few questions:

- Which threats present a danger to the organization's assets in the given environment?
- Which threats represent the most danger to the organization's information?
- How much would it cost to recover from a successful attack?
- Which of these threats would require the greatest expenditure to prevent?

Answering these questions helps establish a framework for the discussion of threat assessment. This list may not cover everything that affects the information security threat assessment. An organization's guidelines and/or policies should influence this process and may require the posing of additional questions.

Vulnerability Identification

After identification of the organization's information assets and documentation of criteria for beginning to assess the threats it faces, review each information asset for each threat it faces and create a list of vulnerabilities. Vulnerabilities, which are specific avenues that threat agents can exploit to attack an information asset. Each of the threats that are possible or likely and how they could be perpetrated are examined. A list of the organization's assets and their vulnerabilities is created. This process works best when groups of people with diverse backgrounds within the organization work iteratively in a series of brainstorming sessions. The end deliverable of the risk identification process is a list of threats, assets, and their vulnerabilities. This list, along with any supporting documentation, is the starting point for the next step, risk assessment.

Risk Assessment

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

Introduction to Risk Assessment

Risk is the likelihood of the occurrence of a vulnerability multiplied by the value of the information asset minus the percentage of risk mitigated by current controls plus the uncertainty of current knowledge of the vulnerability. The goal at this point is to create a method for evaluating the relative risk of each of the listed vulnerabilities.

Likelihood

Likelihood is the probability that a specific vulnerability will be attacked. The National Institute of Standards and Technology recommends in Special Publication 800-30 assigning a number between 0.1 for low and 1.0 for high. Zero is not used because vulnerabilities with a zero likelihood have been removed from the asset/vulnerability list. Whatever rating system is utilized for assigning likelihood, use professionalism, experience, and judgment— and use the rating model you select consistently. Whenever possible, you should use external references for likelihood values that have been reviewed and adjusted for your specific circumstances.

Risk Determination

For the purpose of relative risk assessment, risk equals 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 its associated vulnerabilities that have residual risk, we need to create a preliminary list of control ideas. Residual risk is the risk that remains to the information asset even after the existing control has been applied. There are three general categories of controls: policies, programs, and technologies. Policies are documents that specify an organization's approach to security. There are four types of security policies: general security policy, program security policy, issue-specific policies, and systems-specific policies.

The general security policy is an executive-level document that outlines the organization's approach and attitude towards information security and relates the strategic value of information security within the organization. The program security policy is a planning

document that outlines the process of implementing security in the organization. This policy is the blueprint for the analysis, design, and implementation of security. Issue-specific policies address the specific implementations or applications of which users should be aware. These policies are typically developed to provide detailed instructions and restrictions associated with security issues. Systems-specific policies address the particular use of certain systems. Programs are activities performed within the organization to improve security. These include security education, training, and awareness programs.

Security technologies are the technical implementations of the policies defined by the organization. Access control, which is a fundamental process of information security, is often considered a simple function of the information system that uses it.

Documenting the Results of Risk Assessment

The goal of this process has been to identify the organization's information assets that have specific vulnerabilities and list them, ranked according to those that most need protection. 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 expose, as well as some information about the controls that are already in place. The final summarized document is the ranked vulnerability risk worksheet and contains the following data:

- Asset: Each vulnerable asset
- Asset Impact: Shows the results for this asset from the weighted factor analysis worksheet
- Vulnerability: Each uncontrolled vulnerability
- Vulnerability Likelihood: The likelihood of the realization of the vulnerability by a threat agent, as noted in the vulnerability analysis step
- Risk-Rating Factor: The figure calculated from the asset impact multiplied by likelihood

The process you develop for risk identification should include defining what function the reports will serve, who is responsible for preparing the reports, and who is responsible for reviewing them. The ranked vulnerability risk worksheet, which is the working document for the next step in the risk management process: assessing and controlling risk.

Risk Control Strategies

When members of management have determined that risks from information security threats are creating a competitive disadvantage, they empower the information technology and information security communities to control the risks. Once the project team for information security development has created the ranked vulnerability risk worksheet. Once it is complete, the team must choose one of four basic strategies to control the risks that result from these vulnerabilities.

The four strategies:

- Apply safeguards that eliminate or reduce the remaining uncontrolled risks for the vulnerability (avoidance).
- Transfer the risk to other areas or to outside entities (transference).
- Reduce the impact should the vulnerability be exploited (mitigation).
- Understand the consequences and accept the risk without control or mitigation (acceptance).

Defend

The defend strategy is the preferred approach by preventing exploitation of the vulnerability. The three common methods of defense are the application of policy, education and training, and the application of technology. The policy decision made by McDonald's in 2002 to improve relations with animal rights activists. A defense strategy is a security control that deflects attacks and minimizes the probability that an attack will succeed.

Transfer

Transference is the control approach that attempts to shift the risk to other assets, other processes, or other organizations. One characteristic of excellent organizations is that they focus energy and resources on what they do best, while relying on consultants or contractors for other types of expertise. In other words, they "stick to their knitting...". 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. Outsourcing is not without risks. It is up to

the owner of the information asset, IT management, and the information security team to ensure that the disaster recovery requirements of the outsourcing contract are sufficient and have been met before they are needed for recovery efforts.

Mitigate

Mitigation is the control approach that attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation. The three types of plans in this approach: the incident response plan (IRP), the disaster recovery plan (DRP), and the business continuity plan (BCP). Mitigation begins with early detection of an attack in progress and relies on the ability of the organization to respond quickly, efficiently, and effectively.

Incident response plan

- The actions that an organization should take while the incident is in progress are defined in a document called the incident response plan or IRP.
- The IRP provides answers to questions that victims might pose in the midst of a disaster. It answers questions such as the following:

    - What do I do NOW?
    - What should the administrators do first?
    - Whom should they contact?
    - What should they document?

Disaster recovery plan.

- The most common mitigation procedure is the disaster recovery plan.
- The DRP includes the entire spectrum of activities used to recover from an incident. The DRP can include strategies to limit losses before and during the disaster.
- A DRP usually includes all preparations for the recovery process, strategies to limit losses during the disaster, and detailed steps to follow when the disaster has ended.
- DRP and IRP planning overlap to a degree. In many ways, 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.

Business continuity plan.

- The third type of planning document within the mitigation strategy is the business continuity plan or BCP.
- The BCP is the most strategic and long term 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 the steps necessary to ensure the continuation of the organization when the scope or scale of a disaster exceeds the ability of the DRP to restore operations.

Accept

The acceptance of risk is the choice to do nothing to protect a vulnerability and to accept the outcome of its exploitation. This may or may not be a conscious business decision.

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

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 then possibly determine that the cost of protecting an asset does not justify the security expenditure. If every vulnerability identified in the organization is handled by means of acceptance, it may reflect an inability to conduct proactive security activities and an apathetic approach to security in general. Acceptance as a

strategy is often mistakenly chosen based on the school of fish justification—that sharks will not come after a small fish in a school of other small fish. But this reasoning can be very risky.

Terminate

The final risk control strategy is for the business to terminate the activities that introduce the risk.

Selecting a Risk Control Strategy

The level of threat and value of the asset should play a major role in the selection of a risk control strategy. The following rules of thumb that can be applied in selecting the preferred strategy:

- When a vulnerability exists, implement security controls 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 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.

Feasibility Studies

Before deciding on the strategy for a specific vulnerability, all the economic and noneconomic consequences of the vulnerability facing the information asset must be explored. We need to ask, "What are the actual and perceived advantages of implementing a control as opposed to the actual and perceived disadvantages of implementing the control?"

Cost avoidance is the process of avoiding the financial impact of an incident by implementing a control.

Cost Benefit Analysis (CBA)

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 the asset is worth. The formal decision-making process, which is used to consider the economic feasibility of implementing information security controls and safeguards is called a cost benefit analysis or an economic feasibility study. As it is difficult to determine the value of information, it is also difficult to determine the costs of safeguards. 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

Benefit is the value that the organization realizes by using controls to prevent losses associated with a specific vulnerability. This is usually determined by valuing the information asset or assets exposed by the vulnerability and then determining how much of that value is at risk and how much risk there is for the asset.

Asset valuation is the process of assigning financial value or worth to each information asset. Some will argue that it is virtually impossible to accurately determine the true value of information and information-bearing assets. The valuation of assets involves the estimation of real and perceived costs associated with the design, development, installation, maintenance, protection, recovery, and defense against market loss, and litigation for every set of information-bearing systems or information assets. Some information assets acquire value over time that is beyond the intrinsic value of the asset itself. This value gained over time is referred to as acquired value.

Some of the components of asset valuation as follows:

- Value retained from the cost of creating or acquiring the information asset
- Value retained from past maintenance of the information asset

- Value implied by the cost of replacing the information
- Value from providing the information
- Value incurred from the cost of protecting the information
- Value to owners
- Value of intellectual property
- Value to adversaries
- Loss of productivity while the information assets are unavailable
- Loss of revenue while information assets are unavailable

The organization must be able to place a dollar value on each collection of information and the information assets it comprises. This value is based on the answers to these questions:

- How much did it cost to create or acquire this information?
- How much would it cost to recreate or recover this information?
- How much does it cost to maintain this information?
- How much is this information worth to the organization?
- How much is this information worth to the competition?

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 a vulnerability or a threat occurrence. This process results in the estimate of potential loss per risk.

The questions that must be asked here:

- What damage could occur, and what financial impact would it have?
- What would it cost to recover from the attack, in addition to the financial impact of damage?
- What is the single loss expectancy for each risk?

A single loss expectancy (SLE) is the calculation of the value associated with the most likely loss from an attack. It is a calculation based on the value of the asset and the exposure factor (EF), which is the expected percentage of loss that would occur from a particular attack, as follows:

SLE = asset value × exposure factor (EF)

Where EF equals the percentage loss that would occur from a given vulnerability being exploited.

As difficult as it is to estimate the value of information, and that the estimation of the probability of a threat occurrence or attack is even more difficult. In most cases, an organization can rely only on its internal information to calculate the security of its information assets. Even if the data has been actively and accurately tracked, the organization's information is sketchy at best. As a result, this information is usually estimated.

The annualized rate of occurrence (ARO), which is simply how often you expect a specific type of attack to occur. To standardize calculations, you convert the rate to a yearly (annualized) value. This is expressed as the probability of a threat occurrence.

The expected value of a loss can be stated in the following equation:

Annualized Loss Expectancy = **Single Loss Expectancy ×**

Annualized Rate of Occurrence

or

ALE = **SLE × ARO**

Cost benefit analysis formula.

- In its simplest definition, the CBA determines whether or not a particular control is worth its cost. The CBA is 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.
- Once controls are implemented, it is crucial to continue to examine their benefits to determine when they must be upgraded, supplemented, or replaced.

Evaluation, Assessment, and Maintenance of Risk Controls

The selection and implementation of a control strategy is not the end of a process. The strategy and its accompanying controls must be monitored and reevaluated on an ongoing basis to determine their effectiveness and to calculate more accurately the estimated residual risk.

Quantitative Versus Qualitative Risk Control Practices

The process performed using actual values or estimates is known as a quantitative assessment. An organization could determine that it cannot put specific numbers on these values. Fortunately, it is possible to repeat these steps using an evaluation process, called qualitative assessment, which is based on characteristics that do not use numerical measures.

Benchmarking and Best Practices

Instead of determining the financial value of information and then implementing security as an acceptable percentage of that value, an organization could take a different approach and look to peer institutions for benchmarks. 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: metrics-based measures or process-based measures.

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

- Number of successful attacks
- Staff hours spent on systems protection
- Dollars spent on protection
- Number of security personnel
- Estimated value in dollars of the information lost in successful attacks
- Loss in productivity hours associated with successful attacks

An organization uses this information to rank competitive businesses with a similar size or market to determine how it measures up to competitors. The difference between an organization’s measures and those of others is often referred to as a **performance gap**.

Process-based measures are generally less focused on numbers and more strategic than metrics-based measures. For each of the areas the organization is interested in benchmarking, process-based measures enable the organization to examine the activities an individual company performs in pursuit of its goal, rather than the specifics of how goals are attained. The primary focus is the method the organization uses to accomplish a particular process, rather than the outcome.

The two categories of benchmarks that are used in information technology: standards of due care and due diligence, and best practices. 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**. Organizations cannot 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. Organizations should remember the adage, "Good security now is better than perfect security never." 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. Within best practices, the **gold standard** is a subcategory of practices that are typically viewed as "the best of the best."

The application of best practices.

- When considering to adopt best practices in your organization, consider the following:

- Does your organization resemble the identified target organization with the best practice under consideration?
- Are the resources your organization can expend similar to those identified with the best practice?
- Is your organization in a similar threat environment as that proposed in the best practice?

Problems with the application of 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

- A baseline is a "value or profile of a performance metric against which changes in the performance metric can be usefully compared."
- 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

Other qualitative approaches can be used to determine an organization's readiness for any proposed set of controls are operational, technical, and political feasibility analyses.

Organizational feasibility:

- Organizational feasibility examines how well the proposed information security alternatives will contribute to the efficiency, effectiveness, and overall operation of an organization.

- Above and beyond the impact on the bottom line, the organization must determine how the proposed alternatives contribute to the business objectives of the organization.

Operational feasibility:

- Operational feasibility analysis examines user acceptance and support, management acceptance and support, and the overall requirements of the organizations' stakeholders. Operational feasibility is sometimes known as behavioral feasibility, because it measures the behavior of users.
- One of the fundamental principles of systems development is obtaining user buy-in on a project. A common method for obtaining user acceptance and support is through user involvement. User involvement can be obtained via three simple steps: communicate, educate, and involve.
- Organizations should communicate with system users throughout the development of the security program, letting them know that changes are coming. Organizations should make efforts to design training to educate employees about how to work under the new constraints and avoid any negative impact on performance. Those making changes must also involve users by asking them what they want from the new systems and what they will tolerate from the new systems, and by including selected representatives from the various constituencies in the development process.
- These three basic undertakings—communication, education, and involvement—can reduce resistance to change and build resilience for change. Resilience is that ethereal quality that allows workers not only to tolerate constant change, but also to accept it as a necessary part of their jobs.

Technical feasibility:

- In addition to the economic costs and benefits of proposed controls, the project team must also consider the technical feasibilities of their design, implementation, and management.
- Technical feasibility analysis examines whether or not the organization has or can acquire the technology necessary to implement and support the proposed control.
- Technical feasibility also examines whether the organization has the technological expertise to manage the new technology.

Political feasibility:

- For some organizations, the most significant feasibility evaluated may be political. Within organizations, political feasibility defines what can and cannot occur based on the consensus and relationships between the communities of interest.
- The limits placed on an organization's actions or behaviors by the information security controls must fit within the realm of the possible before they can be effectively implemented, and that realm includes the availability of staff resources.

Risk Management Discussion Points

Not every organization has the collective will or budget to manage each vulnerability by applying controls; therefore, each organization must define the level of risk it is willing to live with.

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. The key for an organization is to find the balance in its decision-making processes and in its feasibility analyses, therefore assuring that an organization's risk appetite is based on experience and facts and not on ignorance or wishful thinking.

Residual Risk

Even when vulnerabilities have been controlled as much as possible, there is often still some risk that has not been completely removed, shifted, or planned for. This remainder is called residual risk. "residual risk is a combined function of (1) a threat less the effect of some threat reducing safeguards; (2) a vulnerability less the effect of some vulnerability reducing safeguards; and (3) an asset less the effect of some asset value reducing safeguards."

The significance of residual risk, which must be judged within the context of the organization. The goal of information security is not to bring residual risk to zero; it is to bring residual risk into line with an organization's comfort zone or risk appetite.

Documenting Results

The results of risk assessment activities can be delivered. There are a number of ways: a report on a systematic approach to risk control, a project-based risk assessment, or a topic-specific risk assessment. When the organization is pursuing an overall risk management program, it requires a systematic report that enumerates the opportunities for controlling risk. This report documents a series of proposed controls, each of which has been justified by one or more feasibility or rationalization approaches. At a 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. Another option is to document the outcome of the control strategy for each information asset-threat pair in an action plan. This action plan includes concrete tasks, each with accountability assigned to an organizational unit or to an individual.

Sometimes a risk assessment is prepared for a specific IT project at the request of the project manager, either because it is required by organizational policy or because it is good project management practice. The project risk assessment should identify the sources of risk in the finished IT system, with suggestions for remedial controls, as well as those risks that might impede the completion of the project.

When management requires details about a specific risk to the organization, risk assessment may be documented in a topic-specific report. These are usually demand reports that are prepared at the direction of senior management and are focused on a narrow area of information systems operational risk.

Recommended Risk Control Practices

Planned expenditures to implement a control strategy must be justified, and budget authorities must be convinced to spend the necessary amount to protect a particular asset from an identified threat. Unfortunately, most budget authorities focus on trying to cut a percentage of the total figure to save the organization money. This underlines the importance of developing strong justifications for specific action plans and providing concrete estimates in those plans. Another factor to consider is that each control or safeguard affects more than one asset- threat pair. Information security professionals manage a dynamic matrix covering a broad range of threats, information assets, controls, and identified vulnerabilities.

If a new safeguard is implemented, there is a risk decrease associated with all subsequent control evaluations. To make matters even more complex, the action of implementing a control may change the values assigned or calculated in a prior estimate. There is an ongoing search for ways to design security architectures that go beyond the direct application of specific controls in which each is justified for a specific information asset vulnerability, to safeguards that can be applied to several vulnerabilities at once.