UNIT 2

LEGAL, ETHICAL AND PROFESSIONAL ISSUES

2.1 LEGAL, ETHICAL AND PROFESSIONAL ISSUES

The information security professional plays an important role in an organization's approach to managing liability for privacy and security risks. In the modern litigious societies of the world, sometimes laws are enforced in civil courts, where large damages can be awarded to plaintiffs who bring suits against organizations.

Sometimes these damages are punitive—assessed as a deterrent. To minimize liability and reduce risks from electronic and physical threats, and to reduce all losses from legal action, information security practitioners must thoroughly understand the current legal environment, stay current with laws and regulations, and watch for new and emerging issues. By educating the management and employees of an organization on their legal and ethical obligations and the proper use of information technology and information security, security professionals can help keep an organization focused on its primary objectives.

2.1.1 Law and Ethics in Information Security

In general, people elect to trade some aspects of personal freedom for social order. As Jean Jacques Rousseau explains in The Social Contract, or Principles of Political Right, the rules the members of a society create to balance the individual rights to self-determination against the needs of the society as a whole are called laws.

Laws are rules that mandate or prohibit certain behavior; they are drawn from ethics, which define socially acceptable behaviors. The key difference between laws and ethics is that laws carry the authority of a governing body, and ethics do not. Ethics in turn are based on cultural mores: the fixed moral attitudes or customs of a particular group. Some ethical standards are universal. For example, murder, theft, assault, and arson are actions that deviate from ethical and legal codes throughout the world.

Organizational Liability and the Need for Counsel

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. The bottom line is that if an employee, acting with or without the authorization

of the employer, performs an illegal or unethical act that causes some degree of harm, the employer can be held financially liable for that action. An organization increases its liability if it refuses to take measures known as due care.

Due care standards are met when an organization makes sure that every employee knows what is acceptable or unacceptable behavior, and knows the consequences of illegal or unethical actions. Due diligence requires that an organization make a valid effort to protect others and continually maintains this level of effort. Given the Internet's global reach, those who could be injured or wronged by an organization's employees could be anywhere in the world.

Under the U.S. legal system, any court can assert its authority over an individual or organization if it can establish jurisdiction—that is, the court's right to hear a case if a wrong is committed in its territory or involves its citizenry. This is sometimes referred to as long arm jurisdiction—the long arm of the law extending across the country or around the world to draw an accused individual into its court systems. Trying a case in the injured party's home area is usually favorable 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—guidelines that describe acceptable and unacceptable employee behaviors in the workplace—function as organizational laws, complete with penalties, judicial practices, and sanctions to require compliance. Because these policies function as laws, they must be crafted and implemented 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, however, is that ignorance of a policy is an acceptable defense. Thus, for a policy to become enforceable, it must meet the following five criteria:

1. **Dissemination (distribution)**: The organization must be able to demonstrate that the relevant policy has been made readily available for review by the employee. Common dissemination techniques include hard copy and electronic distribution.
2. **Review (reading):** The organization must be able to demonstrate that it disseminated the document in an intelligible form, including versions for illiterate, non-English reading, and reading-impaired employees. Common techniques include recordings of the policy in English and alternate languages.
3. **Comprehension (understanding):** The organization must be able to demonstrate that the employee understood the requirements and content of the policy. Common techniques include quizzes and other assessments.
4. **Compliance (agreement):** The organization must be able to demonstrate that the employee agreed to comply with the policy through act or affirmation. Common

techniques include logon banners, which require a specific action (mouse click or keystroke) to acknowledge agreement, or a signed document clearly indicating the employee has read, understood, and agreed to comply with the policy.

5. **Uniform enforcement:**The organization must be able to demonstrate that the policy has been uniformly enforced, regardless of employee status or assignment.

Only 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 comprises 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 activities and conduct harmful to society, and is actively enforced by the state. Law can also be categorized as private or public. Private law encompasses family law, commercial law, and labor law, and regulates the relationship between individuals and organizations. Public law regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments. Public law includes criminal, administrative, and constitutional law.

2.1.2 Relevant U.S Laws

Historically, the United States has been a leader in the development and implementation of information security legislation to prevent misuse and exploitation of information and information technology. The implementation of information security legislation contributes to a more reliable business environment, which in turn, enables a stable economy. In its global leadership capacity, the United States has demonstrated a clear understanding of the importance of securing information and has specified penalties for people and organizations that breach U.S. civil statutes.

Most important U.S. laws that apply to information security

The sections that follow present the most important U.S. laws that apply to information security.

1. **General Computer Crime Laws :** There are several key laws relevant to the field of information security and of particular interest to those who live or work in the United States. The Computer Fraud and Abuse Act of 1986 (CFA Act) is the cornerstone of many computer-related federal laws and enforcement efforts. It was amended in October 1996 by the National Information Infrastructure Protection Act of 1996, which modified several sections of the previous act and increased the penalties for selected crimes. The punishment for offenses prosecuted under this statute varies from fines

to imprisonment up to 20 years, or both. The severity of the penalty depends on the value of the information obtained and whether the offense is judged to have been committed:

1. For purposes of commercial advantage
2. For private financial gain
3. In furtherance of a criminal act

The previous law, along with many others, was further modified by the USA PATRIOT Act of 2001, which provides law enforcement agencies with broader latitude in order to combat terrorism-related activities. In 2006, this act was amended by the USA PATRIOT Improvement and Reauthorization Act, which made permanent fourteen of the sixteen 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 as a so-called sunset clause 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.

Another key law 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, is responsible for developing these security standards and guidelines.

2. **Privacy :** Privacy has become one of the hottest topics in information security at the beginning of the 21st century. Many organizations are collecting, swapping, and selling personal information as a commodity, and many people are looking to governments for protection of their privacy.

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. One technology that was proposed in the past was intended to monitor or track private communications.

In response to the 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."

3. **Export and Espionage Laws :** To meet national security needs and to protect trade secrets and other state and private assets, several laws restrict which information and information management and security resources may be exported from the United States. These laws attempt to stem the theft of information by establishing strong penalties for these crimes. To protect American ingenuity, intellectual property, and competitive advantage, Congress passed the Economic Espionage Act in 1996. This

law attempts to prevent trade secrets from being illegally shared. The Security and Freedom through Encryption Act of 1999 provides guidance on the use of encryption and provides protection from government intervention. The acts include provisions that:

1. Reinforce an individual's right to use or sell encryption algorithms, without concern for regulations requiring some form of key registration. Key registration is the storage of a cryptographic key (or its text equivalent) with another party to be used to break the encryption of data. This is often called "key escrow."
2. Prohibit the federal government from requiring the use of encryption for contracts, grants, and other official documents and correspondence.
3. State that the use of encryption is not probable cause to suspect criminal activity.
4. Relax export restrictions by amending the Export Administration Act of 1979.
5. Provide additional penalties for the use of encryption in the commission of a criminal act.

4. **U.S. Copyright Law :** Intellectual property is a protected asset in the United States. The U.S. copyright laws extend this privilege to the published word, including electronic formats. Fair use allows copyrighted materials to be used to support news reporting, teaching, scholarship, and a number of similar activities, as long as the use is for educational or library purposes, is not for profit, and is not excessive. As long as proper acknowledgement is provided to the original author of such works, including a proper description of the location of source materials (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. For more detailed information on copyright regulations, visit the U.S. Copyright Office Web site at www.copyright.gov.

5. **Financial Reporting :** The Sarbanes-Oxley Act of 2002 is a critical piece of legislation that affects the executive management of publicly traded corporations and public accounting firms. This law seeks to improve the reliability and accuracy of financial reporting, as well as increase the accountability of corporate governance, in publicly traded companies. Penalties for non-compliance range from fines to jail terms. Executives working in firms covered by this law seek assurance on the reliability and quality of information systems from senior information technology managers. In turn, IT managers are likely to ask information security managers to verify the confidentiality and integrity of those information systems in a process known in the industry as sub-certification.

6. **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. Agencies of the federal government are required to disclose any requested information on receipt of a written request. This requirement

is enforceable in court. Some information is, however, 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.

7. **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. Information security professionals must therefore understand state laws and regulations and ensure that the organization's security policies and procedures comply with those laws and regulations. For example, in 1991 the state of Georgia passed the Georgia Computer Systems Protection Act, which seeks to protect information, and which establishes penalties for the use of information technology to attack or exploit information systems.

2.1.3 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 it may be impossible to please all of the people all of the time, dealing with the laws of other states and nations is one area where it is certainly not easier to ask for forgiveness than for permission.

A number of different security bodies and laws are described in this section. Because of the political complexities of the relationships among nations and the differences in culture, there are currently few international laws relating to privacy and information security. The laws discussed below are important, but are limited in their enforceability. The American Society of International Law is one example of an American institution that deals in international law (see www.asil.org).

1. **Council of Europe Convention on Cybercrime** : The Council of Europe adopted the Convention on Cybercrime in 2001. It created 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. This convention has been well received by advocates of intellectual property rights because it emphasizes prosecution for copyright infringement. However, many supporters of individual rights oppose the convention because they think it unduly infringes on freedom of speech and threatens the civil liberties of U.S. residents.

   While thirty-four countries attended the signing in November 2001, only twenty-nine nations, including the United States, have ratified the Convention as of April 2010. The United States is technically not a "member state of the council of Europe" but does participate in the Convention.

As is true with much complex international legislation, the Convention on Cybercrime 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. The convention has more than its share of skeptics, who see it as an overly simplistic attempt to control a complex problem.

2. **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) and negotiated over the years 1986–1994, introduced intellectual property rules into the multilateral trade system. It is the first significant international effort to protect intellectual property rights. It 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 ?

3. **Digital Millennium Copyright Act (DMCA) :** The Digital Millennium Copyright Act (DMCA) is the American contribution to an international effort by the World Intellectual Properties Organization (WIPO) to reduce the impact of copyright, trademark, and privacy infringement, especially when accomplished via the removal of technological copyright protection measures. This law was created in response to the 1995 adoption of Directive 95/46/EC by the European Union, 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 implemented a version of this law called the Database Right, in order to comply with Directive 95/46/EC.

   The DMCA includes the following provisions:

   1. Prohibits the circumvention protections and countermeasures implemented by copyright owners to control access to protected content.
   2. Prohibits the manufacture of devices to circumvent protections and countermeasures that control access to protected content.
   3. Bans trafficking in devices manufactured to circumvent protections and countermeasures that control access to protected content.

4. Prohibits the altering of information attached or imbedded into copyrighted material.
5. Excludes Internet service providers from certain forms of contributory copyright infringement.

2.1.4 Ethics and Information Security

Many Professional groups have explicit rules governing ethical behavior in the workplace. For example, doctors and lawyers who commit egregious violations of their professions' canons of conduct can be removed from practice. Unlike the medical and legal fields, however, the information technology field in general, and the information security field in particular, do not have a binding code of ethics. Instead, professional associations—such as the Association for Computing Machinery (ACM) and the Information Systems Security Association—and certification agencies—such as the International Information Systems Security Certification Consortium, Inc., or (ISC) —work to establish the profession's ethical codes of conduct. While these professional organizations can prescribe ethical conduct, they do not always have the authority to banish violators from practicing their trade. To begin exploring some of the ethical issues particular to information security, take a look at the Ten Commandments of Computer Ethics in the nearby Offline.

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. Studies on ethics and computer use reveal that people of different nationalities have different perspectives; difficulties arise when one nationality's ethical behavior violates the ethics of another national group. For example, to Western cultures, many of the ways in which Asian cultures use computer technology is software piracy. This ethical conflict arises out of Asian traditions of collective ownership, which clash with the protection of intellectual property. Approximately 90 percent of all software is created in the United States. Some countries are more relaxed with intellectual property copy restrictions than others.

A study published in 1999 examined computer use ethics of eight nations: Singapore, Hong Kong, the United States, England, Australia, Sweden, Wales, and the Netherlands. This study selected a number of computer-use vignettes (see the Offline titled The Use of Scenarios in Computer Ethics Studies) and presented them to students in universities in these eight nations. This study did not categorize or classify the responses as ethical or unethical. Instead, the responses only 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.

1. **Software License Infringement** : The topic of software license infringement, or piracy, is routinely covered by the popular press. Among study participants, attitudes toward piracy were generally similar; however, participants from the United States and the Netherlands showed statistically significant differences in attitudes from the overall group. Participants from the United States were significantly less tolerant of piracy, while those from the Netherlands were significantly more permissive. Although other studies have reported that the Pacific Rim countries of Singapore and Hong Kong are hotbeds of software piracy, this study found tolerance for copyright infringement in those countries to be moderate, as were attitudes in England, Wales, Australia, and Sweden. This could mean 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, and number of other reasons could a explain why users in these alleged piracy centers disregarded intellectual property laws despite their professed attitudes toward them. Even though participants from the Netherlands displayed a more permissive attitude toward piracy, that country only ranked third in piracy rates of the nations surveyed in this study.

2. **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. Students from Singapore and Hong Kong proved to be significantly more tolerant than those from the United States, Wales, England, and Australia. Students from Sweden and the Netherlands were also significantly more tolerant than those from Wales and Australia, but significantly less tolerant than those from Hong Kong. The low overall degree of tolerance for illicit system use may be a function of the easy correspondence between the common crimes of breaking and entering, trespassing, theft, and destruction of property and their computer-related counterparts.

3. **Misuse of Corporate Resources :** The scenarios used to examine the levels of tolerance for misuse of corporate resources each presented a different degree of non company use of corporate assets without specifying the company's policy on personal use of company resources. In general, individuals displayed a rather lenient view of personal use of company equipment. Only students from Singapore and Hong Kong view personal use of company equipment as unethical.

   There were several substantial differences in this category, with students from the Netherlands revealing the most lenient views. With the exceptions of those from Singapore and Hong Kong, it is apparent that many people, regardless of cultural background, believe that unless an organization explicitly forbids personal use of its computing resources, such use is acceptable. It is interesting to note that only

participants among the two Asian samples, Singapore and Hong Kong, reported generally intolerant attitudes toward personal use of organizational computing resources.

Ethics and Education

Attitudes toward the ethics of computer use are affected by many factors other than nationality. Differences are found among individuals within the same country, within the same social class, and within the same company. Key studies reveal that the overriding factor in leveling the ethical perceptions within a small population is education.

Employees must be trained and kept aware of a number of topics related to information security, not the least of which are 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

There are three general causes of unethical and illegal behavior:

1. **Ignorance:** Ignorance of the law is no excuse; however, ignorance of policy and procedures is. The first method of deterrence is education. This is accomplished by means of designing, publishing, and disseminating organization policies and relevant laws, and also obtaining agreement to comply with these policies and laws from all members of the organization. Reminders, training, and awareness programs keep the policy information in front of the individual and thus better support retention and compliance.
2. **Accident:** Individuals with authorization and privileges to manage information within the organization are most likely to cause harm or damage by accident. Careful planning and control helps prevent accidental modification to systems and data.
3. **Intent:** Criminal or unethical intent goes to the state of mind of the person performing the act; it is often necessary to establish criminal intent to successfully prosecute offenders. Protecting a system against those with intent to cause harm or damage is best accomplished by means of technical controls, and vigorous litigation or prosecution if these controls fail.

Whatever the cause of illegal, immoral, or unethical behavior, one thing is certain: it is the responsibility of information security personnel to do everything in their power to deter these acts 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. However, laws and policies and their associated penalties only deter if three conditions are present:

1. Fear of penalty—Potential offenders must fear the penalty. Threats of informal reprimand or verbal warnings may not have the same impact as the threat of imprisonment or forfeiture of pay.
2. Probability of being caught Potential offenders must believe there is a strong possibility of being caught. Penalties will not deter illegal or unethical behavior unless there is reasonable fear of being caught.
3. Probability of penalty being administered Potential offenders must believe that the penalty will in fact be administered.

2.2 RISK MANAGEMENT

Introduction

Information security risk management, or ISRM, is the process of managing risks associated with the use of information technology. It involves identifying, assessing, and treating risks to the confidentiality, integrity, and availability of an organization's assets. The end goal of this process is to treat risks in accordance with an organization's overall risk tolerance. Businesses shouldn't expect to eliminate all risks; rather, they should seek to identify and achieve an acceptable risk level for their organization.

Types of Risk Management

There are three types of risk management which are as follows :

1. **Project risks** : Project risks concern multiple forms of budgetary, schedule, personnel, resource, and user-associated problems. A basic project risk is schedule slippage. Because the software is intangible, it is complex to monitor and control a software project. It is complex to control something which cannot be recognized. For some manufacturing program, including the manufacturing of cars, the plan executive can identify the product taking shape.
2. **Technical risks** : Technical risks concern potential issues, implementation, interfacing, testing, and maintenance problems. It also includes an ambiguous specification, incomplete specification, changing specification, technical uncertainty, and technical obsolescence. Some technical risks appear because of the development team's insufficient knowledge about the project.
3. **Business risks** : In business risks, it involves risks of building an excellent product that no one required, losing budgetary or personnel commitments, etc.

2.2.1 Overview of Risk Management

Risk management is the process of identifying risk, as represented by vulnerabilities, to an organization's information assets and infrastructure, and taking steps to reduce this

risk to an acceptable level. When an organization depends on IT-based systems to remain viable, information security and the discipline of risk management must 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 involves three major undertakings:

1. Risk identification
2. Risk assessment
3. Risk control

Risk identification is the examination and documentation of the security posture of an organization's information technology and the risks it faces. Risk assessment is the determination of the extent to which the organization's information assets are exposed or at risk. Risk control is the application of controls to reduce the risks to an organization's data and information systems.

Components of Risk Management

The various components of risk management and their relationship to each other are shown in figure.

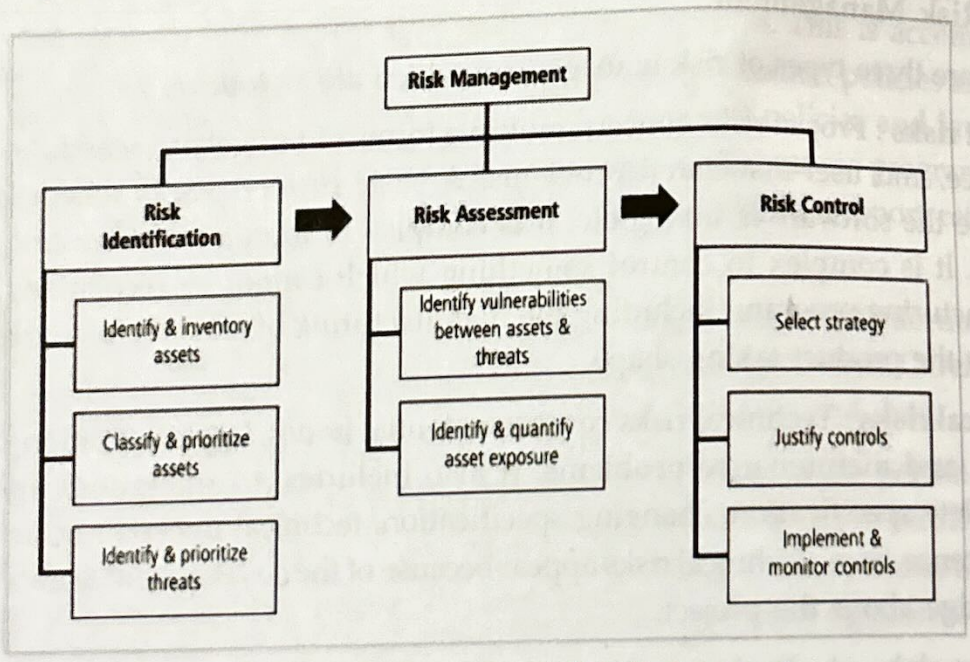

Figure : Components of Risk Management

Know Yourself

First, you must identify, examine, and understand the information and systems currently in place within your organization. This is self-evident. To protect assets, which are defined here as information and the systems that use, store, and transmit information, you must know what they are, how they add value to the organization, and to which

vulnerabilities they are susceptible. Once you know what you have, you can identify what you are already doing to protect it. Just because a control is in place does not necessarily mean that the asset is protected. Frequently, organizations implement control mechanisms but then neglect the necessary periodic review, revision, and maintenance. The policies, education and training programs, and technologies that protect information must be carefully maintained and administered to ensure that they remain effective.

Know the Enemy

Having identified your organization's assets and weaknesses, you move on to Sun Tzu's second step: Know the enemy. This means identifying, examining, and understanding the threats facing the organization. You must determine which threat aspects most directly affect the security of the organization and its information assets, and then use this information to create a list of threats, each one ranked according to the importance of the information assets that it threatens.

The Roles of the Communities of Interest

Each community of interest has a role to play in managing the risks that an organization encounters. Because the members of the information security community best understand the threats and attacks that introduce risk into the organization, they often take a leadership role in addressing risk.

Management and users, when properly trained and kept aware of the threats the organization faces, play a part in the early detection and response process. Management must also ensure that sufficient resources (money and personnel) are allocated to the information security and information technology groups to meet the security needs of the organization. Users work with the systems and the data and are therefore well positioned to understand the value these information assets offer the organization and which assets among the many in use are the most valuable. The information technology community of interest must build secure systems and operate them safely.

For example, IT operations ensure good backups to control the risk from hard drive failures. The IT community can provide both valuation and threat perspectives to management during the risk management process. All of the communities of interest must work together to address all levels of risk, which range from disasters that can devastate the whole organization to the smallest employee mistakes.

The three communities of interest are also responsible for the following:

1. Evaluating the risk controls
2. Determining which control options are cost effective for the organization
3. Acquiring or installing the needed controls
4. Ensuring that the controls remain effective

It is essential that all three communities of interest conduct periodic management reviews. The first focus of management review is asset inventory. On a regular basis, management must verify the completeness and accuracy of the asset inventory. In addition, organizations must review and verify the threats to and vulnerabilities in the asset inventory, as well as the current controls and mitigation strategies. They must also review the cost effectiveness of each control and revisit the decisions on deployment of controls. Furthermore, managers at all levels must regularly verify the ongoing effectiveness of every control deployed.

2.2.2 Risk Identification

A risk management strategy requires that information security professionals know their organizations' information assets—that is, identify, classify, and prioritize them. Once the organizational assets have been identified, a threat assessment process identifies and quantifies the risks facing each asset. The components of risk identification are shown in figure.

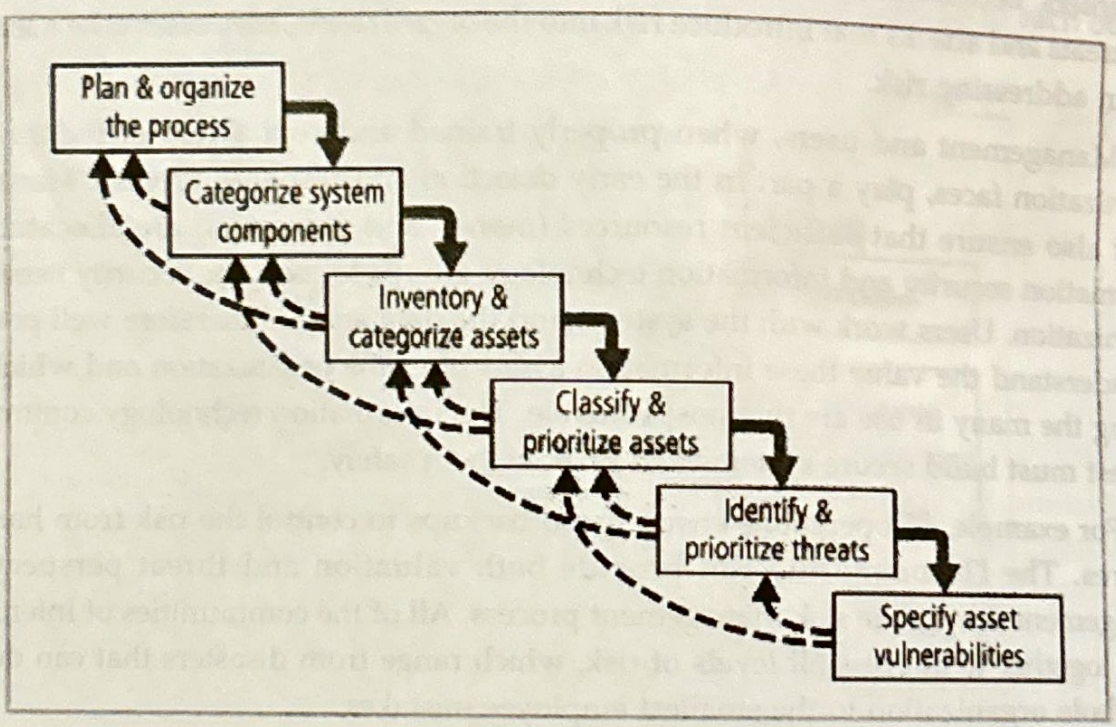

Fig. : Components of Risk Identification

1. **Plan and Organize the Process :** Just as with any major information security undertaking, the first step in the Risk Identification process is to follow your project management principles. You begin by organizing a team, typically consisting of representatives of all affected groups. With risk identification, since risk can exist

everywhere in the organization, representatives will come from every department from users, to managers, to IT and InfoSec groups.

The process must then be planned out, with periodic deliverables, reviews, and presentations to management. Once the project is ready to begin, a meeting like the one Charlie is conducting in the opening case begins. Tasks are laid out, assignments made, and timetables discussed. Only then is the organization ready to actually begin the next step—identifying and categorizing assets.

2. **Asset Identification and Inventory :** This iterative process begins with the enumeration of assets, including all of the elements of an organization's system, such as people, procedures, data and information, software, hardware, and networking elements. Then, you classify and categorize the assets, adding details as you dig deeper into the analysis. The objective of this process is to establish the relative priority of the assets to the success of the organization.

3. **Classifying and Prioritizing Information Assets :** Some organizations further subdivide the categories listed. For example, the category "Internet components" can be subdivided into servers, networking devices (routers, hubs, switches), protection devices (firewalls, proxies), and cabling. Each of the other categories can be similarly subdivided as needed by the organization.

   You should also include a dimension to represent the sensitivity and security priority of the data and the devices that store, transmit, and process the data—that is, a data classification scheme. Examples of data classification categories are confidential, internal, and public. A data classification scheme generally requires a corresponding personnel security clearance structure, which determines the level of information individuals are authorized to view, based on what they need to know.

4. **Information Asset Valuation :** To assign value to information assets for risk assessment purposes, you can pose a number of questions and collect your answers on a worksheetfor later analysis. Before beginning the inventory process, the organization should determine which criteria can best establish the value of the information assets.

5. **Identifying and Prioritizing Threats** : After identifying and performing the preliminary classification of an organization's information assets, the analysis phase moves on to an examination of the threats facing the organization., A wide variety of threats face an organization and its information and information systems. 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.

6. **Vulnerability Identification :** Once you have identified the organization's information assets and documented some criteria for beginning to assess the threats it faces, you then review each information asset for each threat it faces and create a list of vulnerabilities. What are vulnerabilities? They are specific avenues that threat agents can exploit to attack an information asset. They are chinks in the armor—a flaw or weakness in an information asset, security procedure, design, or control that could be exploited accidentally or on purpose to breach security.

2.2.3 Risk Assessment

Now that you have identified the organization's information assets and the threats and vulnerabilities, you can evaluate the relative risk for each of the vulnerabilities. This process is called risk assessment. Risk assessment assigns a risk rating or score to each information asset. While this number does not mean anything in absolute terms, it is useful in gauging the relative risk to each vulnerable information asset and facilitates the development of comparative ratings later in the risk control process. The major stages of risk assessment are shown in figure

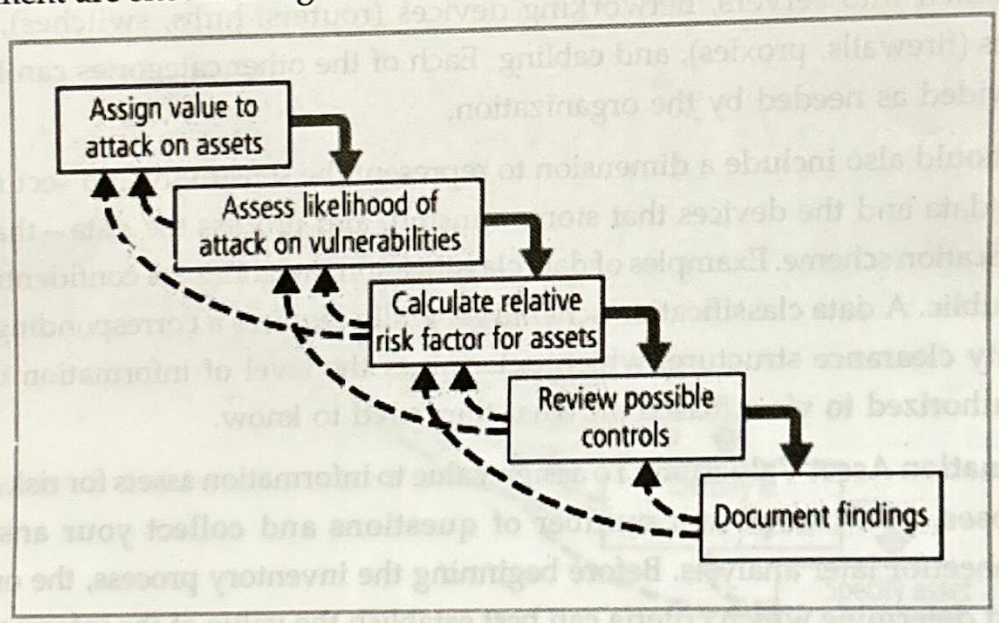

Fig.: Major Stages of Risk Assessment

The following sections itemize the factors that are used to calculate the relative risk for each vulnerability.

1. **Likelihood : Likelihood** is the probability that a specific vulnerability will be the object of a successful attack. In risk assessment, you assign a numeric value to likelihood. The National Institute of Standards and Technology recommends in Special Publication 800-30 assigning a number between 0.1 (low) and 1.0 (high). For example, the likelihood

of an asset being struck by a meteorite while indoors would be rated 0.1. At the other extreme, receiving at least one e-mail containing a virus or worm in the next year would be rated 1.0. You could also choose to use a number between 1 and 100 (zero is not used, since vulnerabilities with a zero likelihood have been removed from the asset/vulnerability list). Whichever rating system you choose, use professionalism, experience, and judgment—and use the rating model you select consistently. Whenever possible, use external references for likelihood values that have been reviewed and adjusted for your specific circumstances. Many asset/vulnerability combinations have sources for likelihood, for example:

The likelihood of a fire has been estimated actuarially for each type of structure. The likelihood that any given e-mail contains a virus or worm has been researched. The number of network attacks can be forecast based on how many assigned network addresses the organization.

2. **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, as illustrated in Figure.

For example: Information asset A has a value score of 50 and has one vulnerability. Vulnerability 1has a likelihood of 1.0 with no current controls. You estimate that assumptions and data are 90 percent accurate.

Information asset B has a value score of 100 and has two vulnerabilities: Vulnerability 2 has a likelihood of 0.5 with a current control that addresses 50 percent of its risk; vulnerability 3 has a likelihood of 0.1 with no current controls. You estimate that assumptions and data are 80 percent accurate.

The resulting ranked list of risk ratings for the three vulnerabilities is:

- **Asset A: Vulnerability 1 rated as $55 = (50 \times 1.0) - 0\% + 10\%$ where**
  $55 = (50 \times 1.0) - ((50 \times 1.0) \times 0.0) + ((50 \times 0.0) \times 0.1)$
  $55 = 50 - 0 + 5$
- **Asset B: Vulnerability 2 rated as $35 = (100 \times 0.5) - 50\% + 20\%$ where**
  $35 = (100 \times 0.5) - ((100 \times 0.5) \times 0.5) + ((100 \times 0.5) \times 0.2)$
  $35 = 50 - 25 + 10$
- **Asset B: Vulnerability 3 rated as $12 = (100 \times 0.1) - 0\% + 20\%$ where**
  $12 = (100 \times 0.1) - ((100 \times 0.1) \times 0.0) + ((100 \times 0.1) \times 0.2)$
  $12 = 10 - 0 + 2$

3. **Identify Possible Controls :** For each threat and its associated vulnerabilities that have residual risk, you must create a preliminary list of potential controls. Residual risk is the risk to the information asset that remains even after the application of controls.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 policies, program security policies, issue-specific policies, and systems-specific policies. The general security policy is an executive-level document that outlines the organization's approach and attitude toward information security and relates the strategic value of information security within the organization. This document, typically created by the CIO in conjunction with the CEO and CISO, sets the tone for all subsequent security activities.

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. Examples include policies for Internet use, e-mail, and access to the building. Finally, systems-specific policies address the particular use of certain systems. This could include firewall configuration policies, systems access policies, and other technical configuration areas. Programs are activities performed within the organization to improve security.

Security technologies are the technical implementations of the policies defined by the organization. One particular approach to control is fundamental to the processes of information security.

Access control is often considered a simple function of the information system that uses it. In fact the principles of access control apply to physical control and other kinds of systems unrelated to IT.

4. **Documenting the Results of Risk Assessment** : By the end of the risk assessment process, you probably have in hand long lists of information assets with data about each of them. The goal so far has been to identify the information assets that have specific vulnerabilities and list them, ranked according to those most needing protection. In preparing this list, you collected and preserved a wealth of factual information about the assets, the threats they face, and the vulnerabilities they expose. You should also have collected some information about the controls that are already in place.

2.2.4 Risk Control Strategies

When organizational management determines 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 five basic strategies to control each of the risks that result from these vulnerabilities.

Five Risk Control Strategies

The five Risk Control Strategies are as follows :

1. **Defend :** The defend control strategy attempts to prevent the exploitation of the vulnerability. This is the preferred approach and is accomplished by means of countering threats, removing, vulnerabilities from assets, limiting access to assets, and adding protective safeguards. There are three common methods used to defend: Application of policy Education and training Application of technology

2. **Transfer** : The transfer control strategy attempts to shift risk to other assets, other processes, or other organizations. This can be accomplished by rethinking how services are offered, revising deployment models, outsourcing to other organizations, purchasing insurance, or implementing service contracts with providers.

3. **Mitigate** : The mitigate control strategy attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation. This approach requires the creation of three types of plans:

   A. Incident Response Plan

   B. Disaster Recovery Plan

   C. Business Continuity Plan

   Each of these plans depends on the ability to detect and respond to an attack as quickly as possible and relies on the quality of the other plans. Mitigation begins with the early detection that an attack is in progress and a quick, efficient, and effective response.

   A. **Incident Response Plan :** The actions an organization can and perhaps should take while an incident is in progress should be specified in a document called the incident response (IR) plan.

   B. **Disaster Recovery Plan** : The most common of the mitigation procedures is the disaster recovery (DR) plan. Although media backup strategies are an integral part of the DR plan, the overall program includes the entire spectrum of activities used to recover from an incident. The DR plan can include strategies to limit losses before and during the disaster. These strategies are fully deployed once the disaster has stopped.

C. **Business Continuity Plan :** The business continuity (BC) plan 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 BC plan 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 DR plan to restore operations.

4. **Accept :** The accept control strategy 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 industry-recognized valid use of this strategy occurs when the organization has done the following:

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

   This strategy is based on the conclusion that the cost of protecting an asset does not justify the security expenditure

5. **Terminate** : The terminate control strategy directs the organization to avoid those business activities that introduce uncontrollable risks. If an organization studies the risks from implementing business-to-consumer e-commerce operations and determines that the risks are not sufficiently offset by the potential benefits, the organization may seek an alternate mechanism to meet customer needs—perhaps developing new channels for product distribution or new partnership opportunities. By terminating the questionable activity, the organization reduces the risk exposure.

2.2.5 Selecting a Risk Control Strategy

Risk control involves selecting one of the five risk control strategies for each vulnerability. The flowchart in figure guides you through the process of deciding how to proceed with one of the five strategies. As shown in the diagram, after the information system is designed, you query as to whether the protected system has vulnerabilities that can be exploited.

If the answer is yes and a viable threat exists, you begin to examine what the attacker would gain from a successful attack. To determine if the risk is acceptable or not, you estimate the expected loss the organization will incur if the risk is exploited.

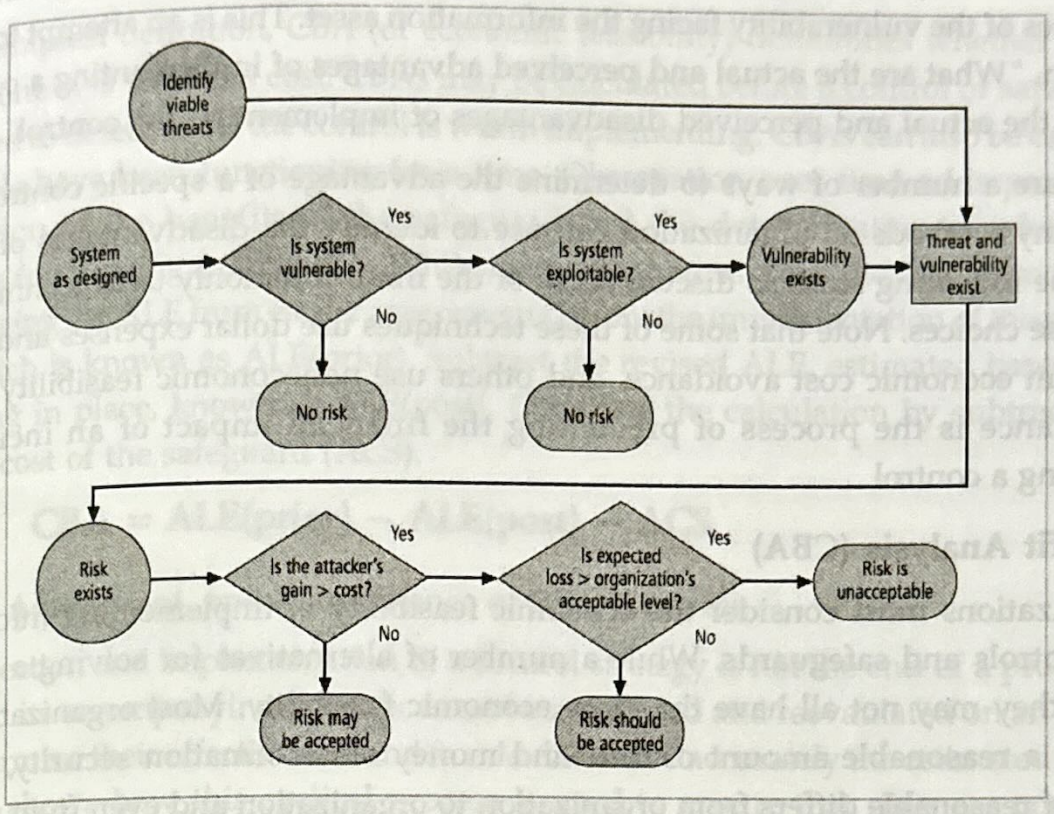

Fig: Risk Handling Decision Points

Rules for Selecting a Risk Control Strategy

Some rules of thumb on strategy selection are presented below. When weighing the benefits of the different strategies, keep in mind that the level of threat and value of the asset should play a major role in strategy selection.

1. When a vulnerability (flaw or weakness) exists: Implement security controls to reduce the likelihood of a vulnerability being exercised.
2. When a vulnerability can be exploited: Apply layered protections, architectural designs, and administrative controls to minimize the risk or prevent occurrence.
3. 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).
4. 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 (defend, transfer, mitigate, accept, or terminate) for a specific vulnerability, the organization must explore all the economic and noneconomic consequences of the vulnerability facing the information asset. This is an attempt to answer the question, "What are the actual and perceived advantages of implementing a control as opposed to the actual and perceived disadvantages of implementing the control.

There are a number of ways to determine the advantage of a specific control. There are also many methods an organization can use to identify the disadvantages of specific controls. The following sections discuss some of the more commonly used techniques for making these choices. Note that some of these techniques use dollar expenses and savings implied from economic cost avoidance, and others use noneconomic feasibility criteria. Cost avoidance is the process of preventing the financial impact of an incident by implementing a control.

Cost Benefit Analysis (CBA)

Organizations must consider the economic feasibility of implementing information security controls and safeguards. While a number of alternatives for solving a problem may exist, they may not all have the same economic feasibility. Most organizations can spend only a reasonable amount of time and money on information security, and the definition of reasonable differs from organization to organization and even from manager to manager.

Organizations are urged to begin the cost benefit analysis by evaluating the worth of the information assets to be protected and the loss in value if those information assets were compromised by the exploitation of a 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 is called a cost benefit analysis or an economic feasibility study.

Just as it is difficult to determine the value of information, it is also difficult to determine the cost of safeguards. Some of the items that affect the cost of a control or safeguard include the following:

1. Cost of development or acquisition (purchase cost) of hardware, software, and services
2. Training fees (cost to train personnel)
3. Cost of implementation (cost to install, configure, and test hardware, software, and services)
4. Service costs (vendor fees for maintenance and upgrades)

5. Cost of maintenance (labor expense to verify and continually test, maintain, and update)

The Cost Benefit Analysis (CBA) Formula

In its simplest definition, CBA (or economic feasibility) determines whether or not a particular control is worth its cost. CBAs may be calculated before a control or safeguard is implemented to determine if the control is worth implementing. CBAs can also be calculated after controls have been functioning for a time. Observation over time adds precision to the evaluation of the benefits of the safeguard and the determination of whether the safeguard is functioning as intended. While many techniques exist, the CBA is most easily calculated using the ALE from earlier assessments before the implementation of the proposed control, which is known as ALE(prior). Subtract the revised ALE, estimated based on the control being in place, known as ALE(post). Complete the calculation by subtracting the annualized cost of the safeguard (ACS).

$$\mathbf{CBA = ALE(prior) - ALE(post) - ACS}$$

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 reevaulated on an ongoing basis to determine their effectiveness and to calculate more accurately the estimated residual risk. Figure shows how this cyclical process is used to ensure that risks are controlled. Note that there is no exit from this cycle; it is a process that continues for as long as the organization continues to function.

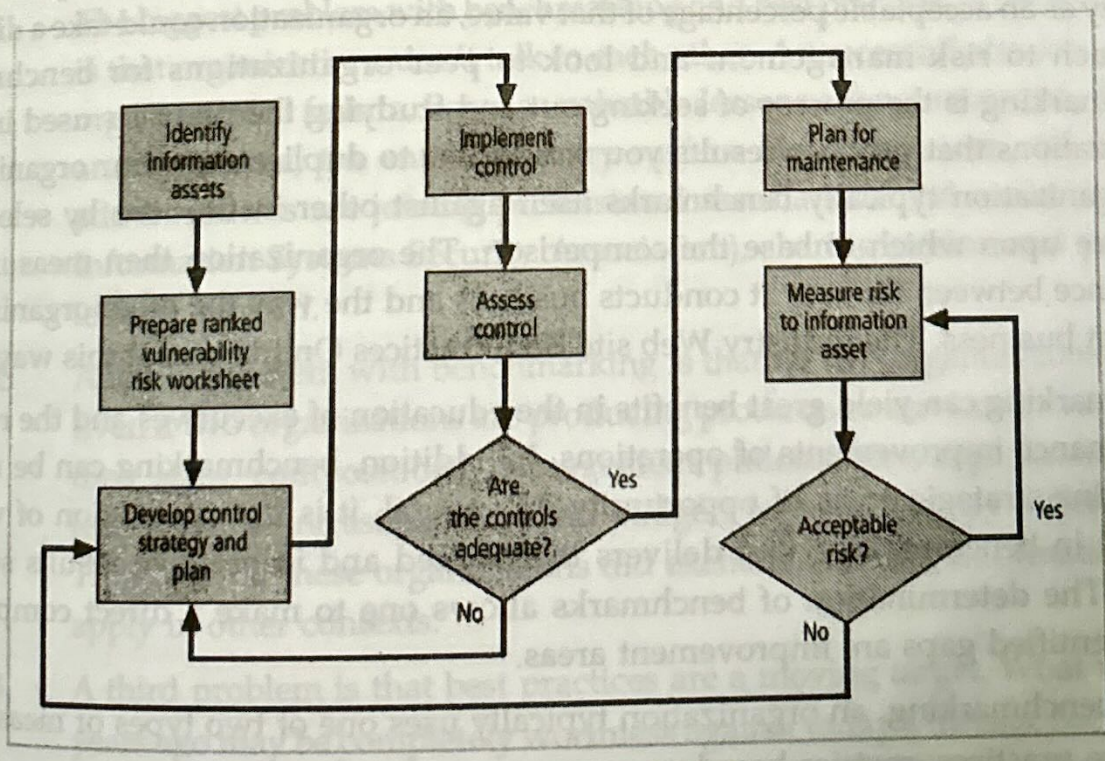

Fig. : Risk Control Cycle

2.2.6 Quantities versus Qualitative Risk Control Practices

The many steps described previously were performed using actual values or estimates. This is known as a quantitative assessment. However, an organization could decide that it cannot put specific numbers on these values. Fortunately, it is possible to repeat these steps using an evaluation process, called qualitative assessment that does not use numerical measures.

For example, instead of placing a value of once every 10 years for the ARO, the organization could list all possible attacks on a particular set of information and rate each by the probability of occurrence. This could be accomplished using scales rather than specific estimates. A sample scale could include none, representing no chance of occurrence, then low, medium, high, up to very high, representing almost certain occurrence. Organizations may, of course, prefer other scales: A–Z, 0–10, 1–5, or 0–20. Using scales also relieves the organization from the difficulty of determining exact values. Many of these same scales can be used in any situation requiring a value, even in asset valuation.

For example, instead of estimating that a particular piece of information is worth $1 million, you can value information on a scale of 1–20, with 1 indicating relatively worthless information, and indicating extremely critical information, such as a certain soda manufacturer's secret recipe or those eleven herbs and spices of a popular fried chicken vendor.

1. **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 to risk management and look to peer organizations for benchmarks. Benchmarking is the process of seeking out and studying the practices used in other organizations that produce results you would like to duplicate in your organization. An organization typically benchmarks itself against other institutions by selecting a measure upon which to base the comparison. The organization then measures the difference between the way it conducts business and the way the other organizations conduct business. The industry Web site Best Practices Online puts it this way:

   Benchmarking can yield great benefits in the education of executives and the realized performance improvements of operations. In addition, benchmarking can be used to determine strategic areas of opportunity. In general, it is the application of what is learned in benchmarking that delivers the marked and impressive results so often noted. The determination of benchmarks allows one to make a direct comparison. Any identified gaps are improvement areas.

   When benchmarking, an organization typically uses one of two types of measures to compare practices: metrics-based measures or process-based measures.

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

1. Numbers of successful attacks
2. Staff-hours spent on systems protection
3. Dollars spent on protection
4. Numbers of security personnel
5. Estimated value in dollars of the information lost in successful attacks
6. Loss in productivity hours associated with successful attacks

An organization uses numerical standards like these to rank competing organizations with a similar size or market to its own and then determines how it measures up to the competitors. The difference between an organization's measures and those of others is often referred to as a **performance gap**. Performance gaps provide insight into the areas that an organization should work on to improve its security postures and defenses.

Applying Best Practices

The preceding sections have presented a number of sources you can consider when applying standards to your organization. You can study the documented best practice processes or procedures that have been shown to be effective and are thus recommended by a person or organization and evaluate how they apply to your organization.

Problems with the Application of Benchmarking and Best Practices

1. The biggest problem with benchmarking and best practices in information security is that organizations don't talk to each other. A successful attack is viewed as an organizational failure. Because valuable lessons are not recorded, disseminated, and evaluated, the entire industry suffers. However, more and more security administrators are joining professional associations and societies (such as the Information Systems Security Association), sharing stories, and publishing the lessons learned.
2. Another problem with benchmarking is that no two organizations are identical. Even if two organizations are producing products or services in the same market, their sizes, compositions, management philosophies, organizational cultures, technological infrastructures, and budgets for security may differ dramatically. Thus, even if these organizations did exchange specific information, it may not apply in other contexts.
3. A third problem is that best practices are a moving target. What worked well 2 years ago may be completely worthless against today's threats. Security practices must keep abreast of new threats in addition to the methods, techniques, policies,

guidelines, educational and training approaches, and technologies used to combat the threats.

4. The last issue to consider is that simply researching information security benchmarks don't necessarily prepare a practitioner for what to do next. It is said that those who cannot remember the past are condemned to repeat it. In security, those who do not prepare for the attacks of the past see them occur again and again. However, preparing for past threats does not safeguard against new challenges to come.

2. Other Feasibility Studies

Other qualitative approaches that can be used to determine an organization's readiness for any proposed set of controls are operational, technical, and political feasibility analyses. The methods for these feasibility evaluations are discussed in the following sections.

1. Organizational Feasibility

Organizational feasibility analysis examines how well the proposed information security alternatives will contribute to the efficiency, effectiveness, and overall operation of an organization. In other words, the proposed control must contribute to the organization's strategic objectives. Above and beyond their impact on the bottom line, the organization must determine how the proposed alternatives contribute to the business objectives of the organization.

2. Operational Feasibility

Operational feasibility analysis addresses several key areas not covered in the other feasibility measures. Operational feasibility analysis examines user acceptance and support, management acceptance and support, and the overall requirements of the organization's stakeholders. Operational feasibility is also known as behavioral feasibility, because it measures the behavior of users.

One of the fundamental requirements of systems development is user buy-in. If the users do not accept a new technology, policy, or program, it will fail. Users may not openly oppose a change, but if they do not support a control, they will find ways of disabling or circumventing it, thereby creating yet vulnerability. One of the most common methods for obtaining user acceptance and support is through user involvement. User involvement can be obtained via three simple steps: communicate, educate, and involve.

3. 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. Some safeguards, especially technology-based safeguards, are extremely difficult to implement, configure, and manage. 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.

4. **Political Feasibility**

For some organizations, the most important feasibility evaluated may be political. Politics has been defined as the art of the possible. Within organizations, political feasibility determines what can and cannot occur based on the consensus and relationships among 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. In some cases, resources are provided directly to the information security community under a budget apportionment model. The management and professionals involved in information security then allocate the resources to activities and projects using processes of their own design.

In other organizations, resources are first allocated to the IT community of interest, and the information security team must compete for these resources. In some cases, cost benefit analysis and other forms of justification discussed previously in this chapter are used in an allocation process to make rational decisions about the relative merit of various activities and projects. Unfortunately in some settings, these decisions are politically charged and are not made according to the pursuit of the greater organizational goals.

Another methodology for budget allocation requires the information security team to propose and justify use of the resources for activities and projects in the context of the entire organization. This requires that arguments for information security spending articulate the benefit of the expense for the whole organization, so that members of the organizational communities of interest can understand its value.

2.2.7 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

1. **Risk Appetite**

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

For instance, a financial services company, regulated by government and conservative by nature, may seek to apply every reasonable control and even some invasive controls to protect its information assets. Other, non-regulated organizations may also be conservative by nature, seeking to avoid the negative publicity associated with the perceived loss of integrity from the exploitation of a vulnerability. Thus, a firewall vendor may install a set of firewall rules that are far stricter than normal because the negative consequence of being hacked would be catastrophic in the eyes of its customers.

Other organizations may take on dangerous risks through ignorance. The reasoned approach to risk is one that balances the expense (in terms of finance and the usability of information assets) of controlling vulnerabilities against the losses possible if these vulnerabilities were exploited.

2. 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. To express it another way, "residual risk is a combined function of (1) a threat less the effect of threat-reducing safeguards, (2) a vulnerability less the effect of vulnerability-reducing safeguards, and (3) an asset less the effect of asset value-reducing safeguards."

Figure illustrates how residual risk remains after safeguards are implemented.

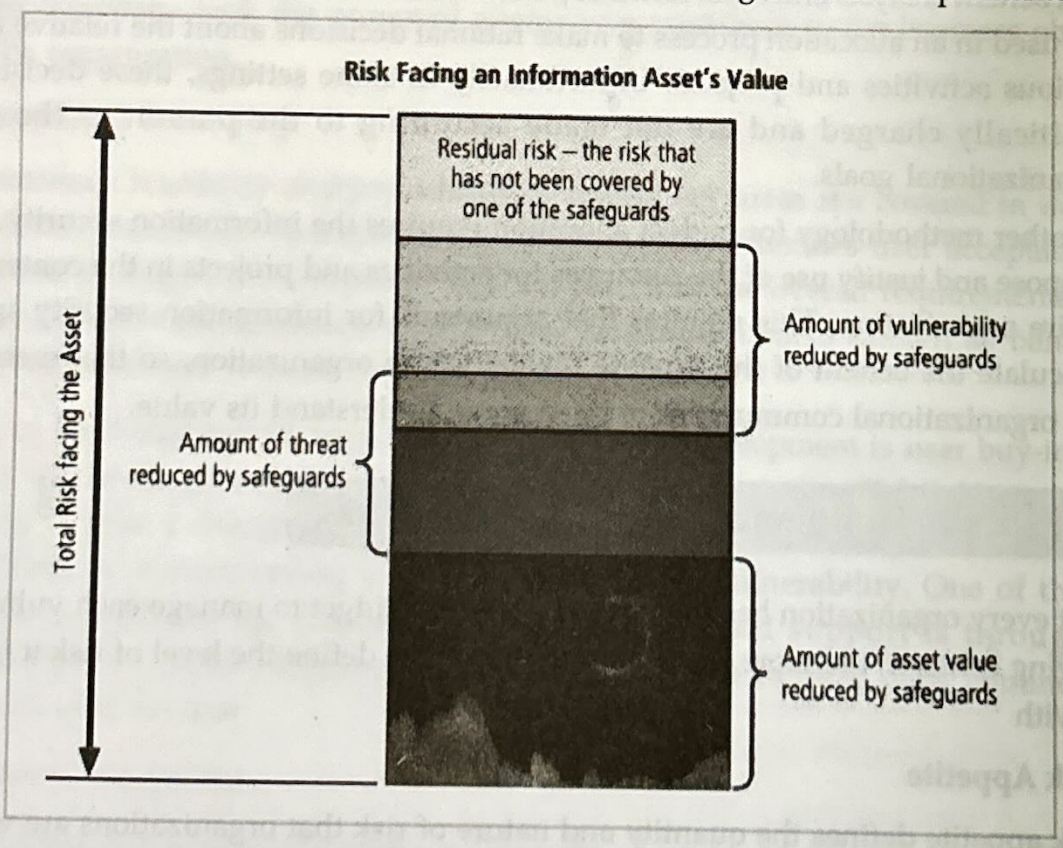

Fig : Residual Risk

The significance of residual risk must be judged within the context of the organization. Although it is counterintuitive, 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. If decision makers have been informed of uncontrolled risks and the proper authority groups within the communities of interest have decided to leave residual risk in place, the information security program has accomplished its primary goal.

3. Documenting Results

The results of risk assessment activities can be delivered in 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-threat pair should have a documented control strategy that clearly identifies any residual risk remaining after the proposed strategy has been executed. Furthermore, each control strategy should articulate which of the four fundamental risk-reducing approaches will be used or how they might be combined, and how that should justify the findings by referencing the feasibility studies. Additional preparatory work for project management should be included where available.

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. It may also include hardware and software requirements, budget estimates, and detailed timelines to activate the project management activities needed to implement the control.

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. On some occasions, the project risk assessment may be requested by auditors or senior management if they perceive that an IT project has sidestepped the organization's information security objectives. 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. For example, a new application usually requires a project risk assessment at system design time and then periodically as the project evolves toward completion.

Lastly, 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.

2.2.8 Recommended Risk Control Practices

If an organization seeks to implement a control strategy that requires a budget of $50,000, the planned expenditures must be justified and budget authorities must be convinced to spend up to $50,000 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. If a new $50,000 firewall is installed to protect the Internet connection infrastructure from the threat posed by hackers launching port-scanning attacks, the same firewall may protect this Internet connection infrastructure from other threats and attacks. In addition, the firewall may protect other information assets from other threats and attacks. The chosen controls may in the end be a balanced mixture that provides the greatest value to as many asset-threat pairs as possible.

This reveals another facet of the risk management problem: information security professionals manage a dynamic matrix covering a broad range of threats, information assets, controls, and identified vulnerabilities. Each time a control is added to the matrix, it undoubtedly changes the ALE for the information asset vulnerability for which it has been designed, and it also may alter the ALE for other information asset vulnerabilities. To put it more simply, if you put in one safeguard, you decrease the risk 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.

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 way to implement controls that doesn't involve such complex, inexact, and dynamic calculations. 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.

IMPORTANT QUESTIONS

1. Explain about Law and ethics in information security.
2. Discuss briefly about Relevant U.S laws , international laws and legal bodies.
3. Explain about Ethics and information security.
4. What is Risk Management? Explain the Overview of Risk Management.
5. Discuss briefly about Risk identification Risk assessment.
6. Discuss briefly about Risk control strategies and selecting a risk control strategy.
7. Explain about Quantities versus qualitative risk control practices.
8. Discuss briefly about Risk management discussion points and recommended risk control practices.