

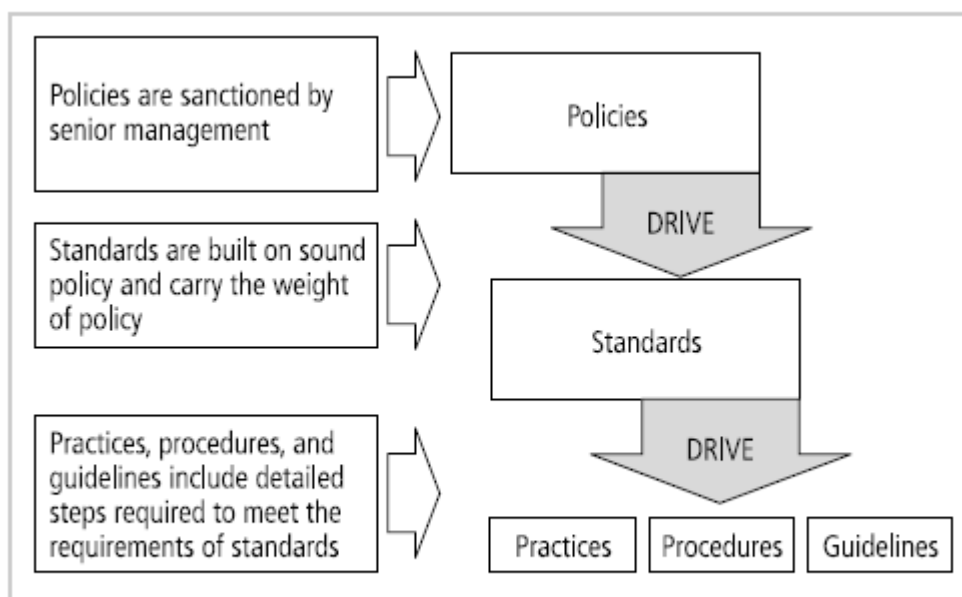
LOGICAL DESIGN

LOGICAL DESIGN: Blueprint for Security - Information Security Policy - Standards and Practices - ISO 17799/BS 7799 - NIST Models - VISA International Security Model - Design of Security Architecture - Planning for Continuity.

4.1 INFORMATION SECURITY POLICY, STANDARDS, AND PRACTICES

Definitions

- A **policy** is a plan or course of action that conveys instructions from an organization's senior management to those who make decisions, take actions, and perform other duties.
- Policies are organizational laws in that they dictate acceptable and unacceptable behaviour within the organization.
- **Standards** are more detailed statements of what must be done to comply with policy. They have the same requirements for compliance as policies.
- Standards may be informal or part of an organizational culture, as in de facto standards. Or standards may be published, scrutinized, and ratified by a group, as in formal or de jure standards.
- Finally, **practices, procedures**, and guidelines effectively explain how to comply with policy.
- The below figure shows policies as the force that drives standards, which in turn drive practices, procedures, and guidelines.



Policies, Standards, and Practices

- Management must define three types of security policy, according to the National Institute of Standards and Technology's Special Publication 800-14
 1. Enterprise information security policies (EISP)
 2. Issue-specific security policies (ISSP)
 3. Systems-specific security policies (SysSP)

4.1.1 Enterprise Information Security Policy (EISP)

- An enterprise information security policy (EISP) is also known as a general security policy, organizational security policy, IT security policy, or information security policy.
- The EISP is based on and directly supports the mission, vision, and direction of the organization and sets the strategic direction, scope, and tone for all security efforts.
- The EISP is an executive level document, usually drafted by or in cooperation with the chief information officer of the organization. This policy is usually two to ten pages long and shapes the philosophy of security in the IT environment.
- The EISP guides the development, implementation, and management of the security program.
- According to the National Institute of Standards and Technology (NIST), the EISP typically addresses compliance in the following two areas:
 - General compliance to ensure meeting the requirements to establish a program and the responsibilities assigned therein to various organizational components.
 - The use of specified penalties and disciplinary action.

4.1.2 Issue-Specific Security Policy (ISSP)

- As an organization executes various technologies and processes to support routine operations, it must instruct employees on the proper use of these technologies and processes.
- In general, the issue-specific security policy, or ISSP,
 - Addresses specific areas of technology
 - Requires frequent updates, and
 - Contains a statement on the organization's position on a specific issue.
- An ISSP may cover the following topics, among others:
 - E-mail
 - Use of the Internet
 - Specific minimum configurations of computers to defend against worms and viruses.

Approaches to creating and managing ISSPs

- There are a number of approaches to creating and managing ISSPs within an organization.
- Three of the most common are:
 1. Independent ISSP documents, each tailored to a specific issue.
 2. A single comprehensive ISSP document covering all issues.
 3. A modular ISSP document that unifies policy creation and administration, while maintaining each specific issue's requirements.
- The independent ISSP document typically has a scattershot effect. Each department responsible for a particular application of technology creates a policy governing its use, management, and control.
- The single comprehensive ISSP is centrally managed and controlled. With formal procedures for the management of ISSPs in place, the comprehensive policy approach establishes guidelines for overall coverage of necessary issues and clearly identifies processes for the dissemination, enforcement, and review of these guidelines.

Components of ISSP

- Statement of Policy
 - Scope and Applicability
 - Definition of Technology Addressed
 - Responsibilities
- Authorized Access and Usage of Equipment
 - User Access
 - Fair and Responsible Use
 - Protection of Privacy
- Prohibited Usage of Equipment
 - Disruptive Use or Misuse
 - Criminal Use
 - Offensive or Harassing Materials
 - Copyrighted, Licensed or other Intellectual Property
 - Other Restrictions
- Systems Management
 - Management of Stored Materials
 - Employer Monitoring

- Virus Protection
- Physical Security
- Encryption
- Violations of Policy
 - Procedures for Reporting Violations
 - Penalties for Violations
- Policy Review and Modification
 - Scheduled Review of Policy and Procedures for Modification
- Limitations of Liability
 - Statements of Liability or Disclaimers

4.1.3 Systems-Specific Policy (SysSP)

- While issue-specific policies are formalized as written documents readily identifiable as policy, system-specific security policies (SysSPs) sometimes have a different look.
- SysSPs often function as standards or procedures to be used when configuring or maintaining systems. Foreexample, a SysSP might describe the configuration and operation of a network firewall.
- SysSPs can be separated into two general groups, managerial guidance and technical specifications, or they can be combined into a single policy document.
- **Managerial guidance SysSP** document is created by management to guide the implementation and configuration of technology as well as to address the behavior of people in the organization in ways that support the security of information.
- **Technical Specifications SysSPs** - While a manager can work with a systems administrator to create managerial policy as described in the preceding section, the system administrator may in turn need to create a policy to implement the managerial policy.
- There are two general methods of implementing such technical controls:
 - **Access control lists (ACLs)** consist of the access control lists, matrices, and capability tables governing the rights and privileges of a particular user to a particular system
 - **Configuration rules** comprise the specific configuration codes entered into security systems to guide the execution of the system.

Access Control Lists

- Access control lists (ACLs) consist of the user access lists, matrices, and capability tables that govern the rights and privileges of users. ACLs can control access to file storage systems, software components, or network communications devices.
- Both Microsoft Windows NT/2000 and Novell Netware 5.x/6.x families of systems translate ACLs into sets of configurations that administrators use to control access to their respective systems
- ACLs allow a configuration to restrict access from anyone and anywhere
- In general, ACLs regulate the following:
 - Who can use the system?
 - What authorized users can access
 - When authorized users can access the system
 - Where authorized users can access the system from

Policy Management

- Policies are living documents that must be managed. It is unacceptable to create such an important set of documents and then shelve it. These documents must be properly disseminated (distributed, read, understood, agreed to, and uniformly applied) and managed.
- Good management practices for policy development and maintenance make for a more resilient organization. For example, all policies, including security policies, undergo tremendous stress when corporate mergers and divestitures occur; in such situations, employees are faced with uncertainty and many distractions.

4.2 THE INFORMATION SECURITY BLUEPRINT

- It is the basis for the design, selection, and implementation of all security policies, education and training programs, and technological controls.
- More detailed version of *security framework*, which is an outline of overall information security strategy for organization and a road map for planned changes to the information security environment of the organization.
- Should specify tasks to be accomplished and the order in which they are to be realized.
- Should also serve as a scalable, upgradeable, and comprehensive plan for the information security needs for coming years.

4.2.1 ISO 17799/BS 7799

- One of the most widely referenced security models is the Information Technology—Code of Practice for Information Security Management, which was originally published as British Standard BS7799.
- In 2000, this code of practice was adopted as an international standard framework for information security by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as ISO/IEC 17799.

Drawbacks of ISO 17799/BS 7799

- Several countries have not adopted 17799 claiming there are fundamental problems:
 - The global information security community has not defined any justification for a code of practice as identified in the ISO/IEC 17799.
 - 17799 lacks “the necessary measurement precision of a technical standard”.
 - There is no reason to believe that 17799 is more useful than any other approach currently available.
 - 17799 is not as complete as other frameworks available.
 - 17799 is perceived to have been hurriedly prepared given the tremendous impact its adoption could have on industry information security controls.

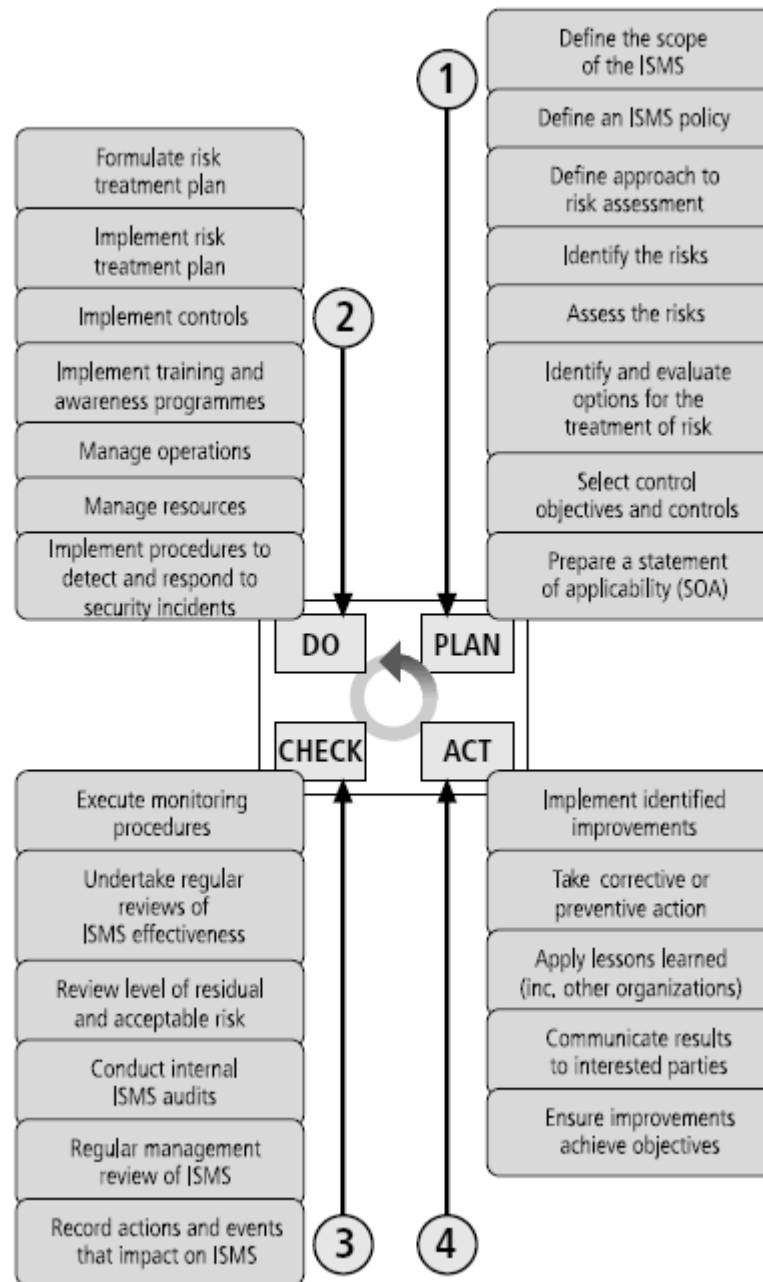
ISO/IEC sections

- While the details of ISO/IEC 27002 are available to those who purchase the standard, its structure and general organization are well known.

1.	Risk Assessment and Treatment
2.	Security Policy
3.	Organization of Information Security
4.	Asset Management
5.	Human Resource Security
6.	Physical and Environmental Security
7.	Communications and Operations
8.	Access Control
9.	Information Systems Acquisition, Development and Maintenance
10.	Information Security Incident Management
11.	Business Continuity Management
12.	Compliance

The Sections of the ISO/IEC 27002¹⁴

The overall methodology for this process and its major steps are presented in Figure.



BS7799:2 Major Process Steps

- Although ISO/IEC 27001 provides some implementation information, it simply specified what must be done—not how to do it.
- ISO/IEC 27001’s primary purpose is to enable organizations that adopt it to obtain certification, and thus it serves better as an assessment tool than as an implementation framework.

4.2.2 NIST SECURITY MODELS

- This refers to “The National Security Telecommunications and Information systems Security Committee” document. This document presents a comprehensive model for information security. The model consists of three dimensions.
- Approaches are described in the many documents available from the Computer Security Resource Center of the National Institute for Standards and Technology.
- The following NIST documents can assist in the design of a security framework:
 - SP 800-12: *An Introduction to Computer Security: The NIST Handbook*
 - SP 800-14: Generally Accepted Security Principles and Practices for Securing Information Technology Systems
 - SP 800-18 Rev. 1: Guide for Developing Security Plans for Federal Information Systems
 - SP 800-26: Security Self-Assessment Guide for Information Technology Systems (removed from active list but still available in archives)
 - SP 800-30: Risk Management Guide for Information Technology Systems.

NIST Special Publication SP 800-12

- SP 800-12 is an excellent reference and guide for the security manager or administrator in the routine management of information security.
- It provides little guidance, however, on design and implementation of new security systems, and therefore should be used only as a valuable precursor to understanding an information security blueprint.

NIST Special Publication SP 800-14

- Generally accepted Principles and practices for Security Information Technology Systems.
- Provides best practices and security principles that can direct the security team in the development of Security Blue Print.
- The scope of NIST SP 800-14 is broad. It is important to consider each of the security principles it presents, and therefore the following sections examine some of the more significant points in more detail:
 1. Security Supports the Mission of the Organization
 2. Security is an Integral Element of Sound Management
 3. Security Should Be Cost-Effective

4. Systems Owners Have Security Responsibilities Outside Their Own Organizations
5. Security Responsibilities and Accountability Should Be Made Explicit
6. Security Requires a Comprehensive and Integrated Approach
7. Security Should Be Periodically Reassessed
8. Security is Constrained by Societal Factors

NIST Special Publication 800-18 Rev. 1

- The Guide for Developing Security plans for Information Technology Systems can be used as the foundation for a comprehensive security blueprint and framework.
- It provides detailed methods for assessing, and implementing controls and plans for applications of varying size.
- It can serve as a useful guide to the activities and as an aid in the planning process.
- It also includes templates for major application security plans.
- The table of contents for Publication 800-18 is presented in the following.

NIST SP 800-26 Table of contents

- Management Controls
 - Risk Management
 - Review of Security Controls
 - Life Cycle Maintenance
 - Authorization of Processing (Certification and Accreditation)
 - System Security Plan
- Operational Controls
 - Personnel Security
 - Physical Security
 - Production, Input/Output Controls
 - Contingency Planning
 - Hardware and Systems Software
 - Data Integrity
 - Documentation
 - Security Awareness, Training, and Education
 - Incident Response Capability
- Technical Controls



- Identification and Authentication
- Logical Access Controls
- Audit Trails
- **Management controls**
 - Management controls address the design and implementation of the security planning process and security program management.
 - They also address risk management and security control reviews. They further describe the necessity and scope of legal compliance and the maintenance of the entire security life cycle.
- **Operational controls**
 - Operational controls deal with the operational functionality of security in the organization. They include management functions and lower level planning, such as disaster recovery and incident response planning.
 - They also address personnel security, physical security, and the protection of production inputs and outputs. They guide the development of education, training and awareness programs for users, administrators, and management.
 - Finally, they address hardware and software systems maintenance and the integrity of data.
- **Technical controls**
 - Technical controls address the tactical and technical issues related to designing and implementing security in the organization, as well as issues related to examining and selecting the technologies appropriate to protecting information.
 - They address the specifics of technology selection and the acquisition of certain technical components. They also include logical access controls, such as identification, authentication, authorization, and accountability. They cover cryptography to protect information in storage and transit.
 - Finally, they include the classification of assets and users, to facilitate the authorization levels needed.
- Using the three sets of controls, the organization should be able to specify controls to cover the entire spectrum of safeguards, from strategic to tactical, and from managerial to technical.

4.3 VISA INTERNATIONAL SECURITY MODEL

- It promotes strong security measures in its business associates and has established guidelines for the security of its information systems.
- It has developed two important documents
 1. Security Assessment Process
 2. Agreed Upon Procedures.
- Both documents provide specific instructions on the use of the VISA Cardholder Information Security Program.
- The *Security Assessment Process* document is a series of recommendations for the detailed examination of an organization's systems with the eventual goal of integration into the VISA systems.
- The *Agreed upon Procedures* document outlines the policies and technologies required for security systems that carry the sensitive card holder information to and from VISA systems.
- Using the two documents, a security team can develop a sound strategy for the design of good security architecture.
- The only downside to this approach is the specific focus on systems that can or do integrate with VISA's systems with the explicit purpose of carrying the aforementioned cardholder information.

Baselining & Best Business Practices

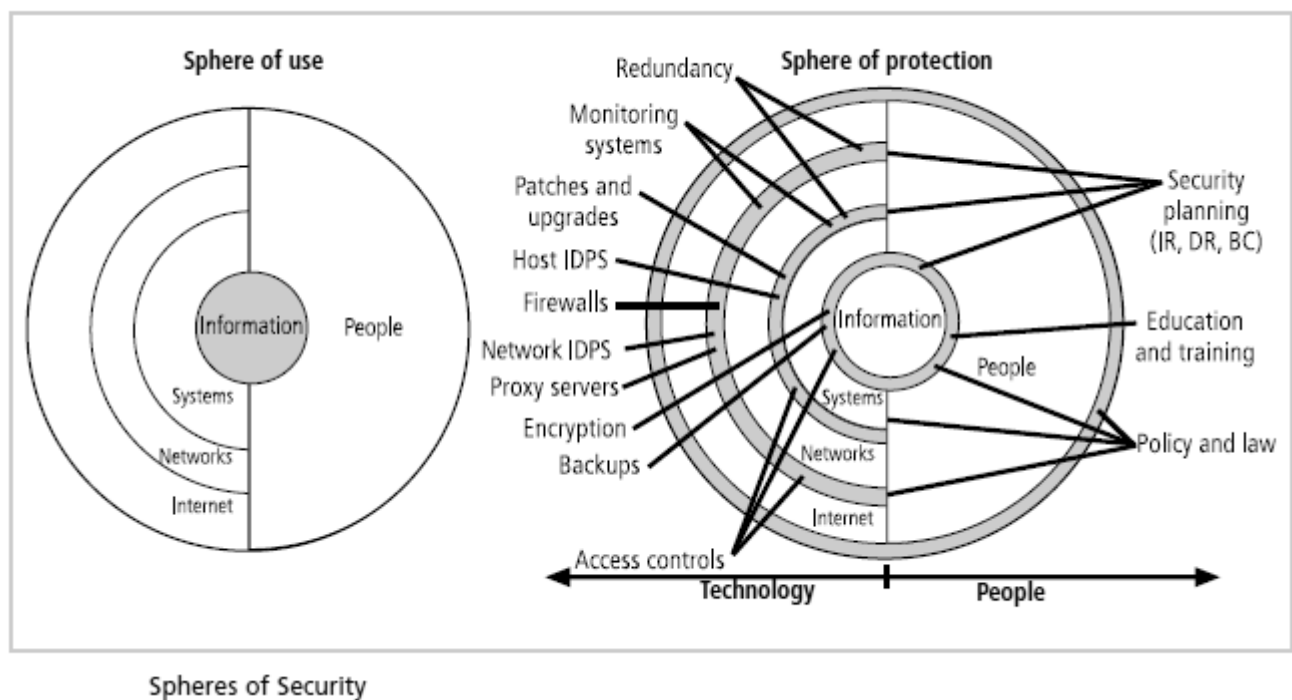
- Baselining and best practices are solid methods for collecting security practices, but provide less detail than a complete methodology
- Possible to gain information by baselining and using best practices and thus work backwards to an effective design
- The Federal Agency Security Practices (FASP) site (fasp.nist.gov) designed to provide best practices for public agencies and adapted easily to private institutions.
- The documents found in this site include specific examples of key policies and planning documents, implementation strategies for key technologies, and position descriptions for key security personnel.
- Of particular value is the section on program management, which includes the following:
 - A summary guide: public law, executive orders, and policy documents

- Position description for computer system security officer.
- Position description for information security officer
- Position description for computer specialist.
- Sample of an information technology(IT) security staffing plan for a large service application(LSA)
- Sample of an information technology(IT) security program policy
- Security handbook and standard operating procedures.
- Telecommuting and mobile computer security policy.

4.4 DESIGN OF SECURITY ARCHITECTURE

4.4.1 Spheres of Security

- The spheres of security, shown in Figure are the foundation of the security framework. Generally speaking, the spheres of security illustrate how information is under attack from a variety of sources.
- The sphere of use, on the left-hand side of Figure, illustrates the ways in which people access information.
- The sphere of protection, on the right-hand side of Figure, illustrates that between each layer of the sphere of use there must exist a layer of protection, represented in the figure by the shaded bands.



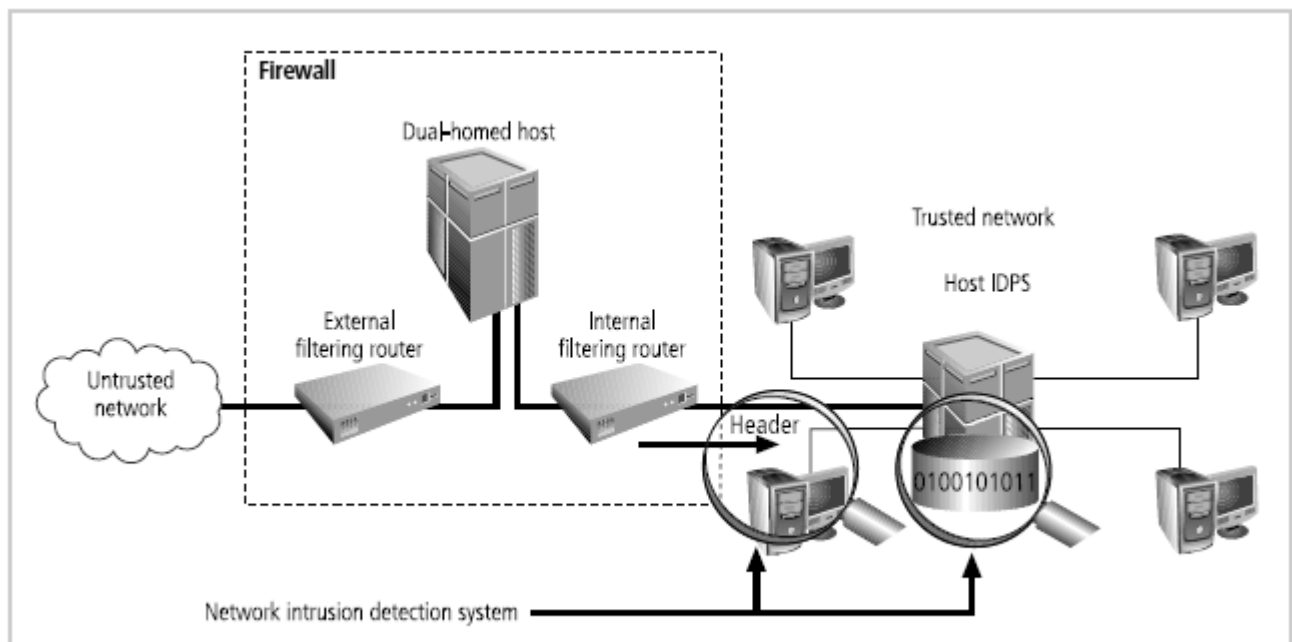
- “Education and training” are placed between people and the information. Controls are also implemented between systems and the information, between networks and the computer systems, and between the Internet and internal networks.
- Information security is designed and implemented in three layers:
 1. Policies
 2. People (education, training, and awareness programs), and
 3. Technology
- Commonly referred to as PPT.
- Each of the layers contains controls and safeguards that protect the information and information system assets that the organization values.

Levels of Controls

- Information security safeguards provide three levels of control:
 1. Managerial
 2. Operational and
 3. Technical
- **Management controls**
 - It covers security processes that are designed by strategic planners and performed by the security administration of the organization.
 - Management controls address the design and implementation of the security planning process and security program management.
- **Operational controls**
 - It deal with the operational functionality of security in the organization.
 - They include management functions and lower-level planning, such as disaster recovery and incident response planning.
 - Operational controls also address personnel security, physical security, and the protection of production inputs and outputs.
- **Technical controls**
 - Address those tactical and technical issues related to designing and implementing security in the organization.
 - Technical controls include logical access controls, such as identification, authentication, authorization, and accountability.

4.4.2 Defense in Depth

- One of the basic tenets of security architectures is the layered implementation of security.
- Defense in depth requires that the organization establish sufficient security controls and safeguards, so that an intruder faces multiple layers of controls.
- These layers of control can be organized into policy, training and education and technology as per the NSTISSC model.
- While policy itself may not prevent attacks, they coupled with other layers and deter attacks.
- Training and Education are similar.
- Technology is also implemented in layers, with detection equipment, all operating behind access control mechanisms.
- Implementing multiple types of technology and thereby preventing the failure of one system from compromising the security of the information is referred to as redundancy.
- Redundancy can be implemented at a number of points throughout the security architecture, such as firewalls, proxy servers, and access controls.

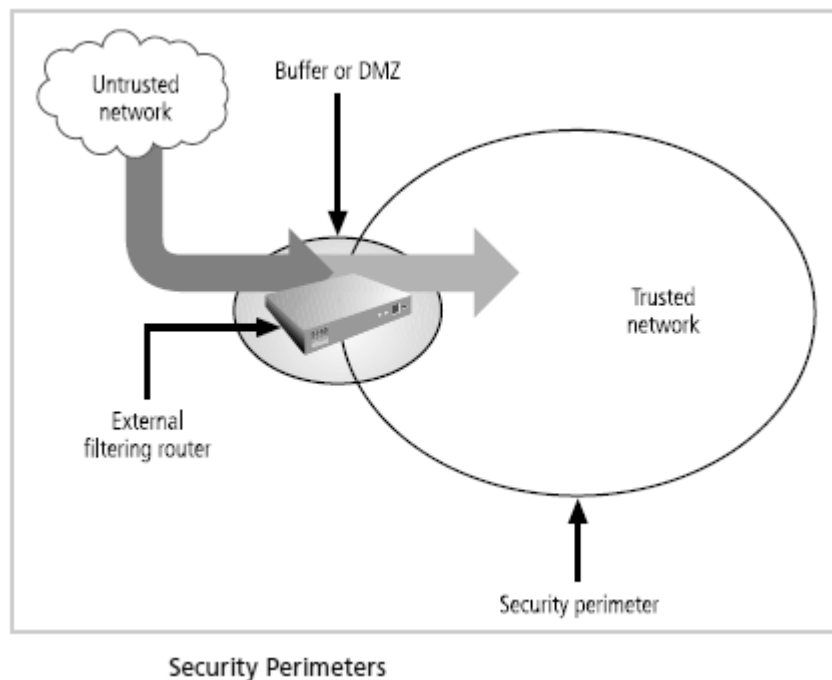


Defense in Depth

- Illustrates the concept of building controls in multiple, sometimes redundant layers. The figure shows the use of firewalls and prevention IDPS that use both packet-level rules (shown as the header in the diagram) and content analysis (shown as 0100101011 in the diagram)

4.4.3 Security Perimeter

- A perimeter is boundary of an area. A security perimeter defines the boundary between the outer limit of an organization's security and the beginning of the outside world.
- A Security Perimeter is the level of security that protects all internal systems from outside threats.
- Unfortunately, the perimeter does not protect against internal attacks from employee threats, or on-site physical threats.
- Security perimeters can effectively be implemented as multiple technologies that segregate the protected information from those who would attack it.
- Within security perimeters the organization can establish security domains, or areas of trust within which users can freely communicate.
- The presence and nature of the security perimeter is an essential element of the overall security framework, and the details of implementing the perimeter make up a great deal of the particulars of the completed security blueprint.
- The key components used for planning the perimeter are presented in the following sections on firewalls, DMZs, proxy servers, and intrusion detection systems.



Key components of the security perimeter

- Firewalls
- DMZs
- Proxy servers and
- IDPSs

Firewalls

- A firewall is a device that selectively discriminates against information flowing into or out of the organization.
- Firewall is usually a computing device or a specially configured computer that allows or prevents access to a defined area based on a set of rules.
- Firewalls are usually placed on the security perimeter, just behind or as part of a gateway router. While the gateway router's primary purpose is to connect the organization's systems to the outside world, it too can be used as the front-line defense against attacks, as it can be configured to allow only set types of protocols to enter.
- There are a number of types of firewalls— packet filtering, stateful packet filtering, proxy, and application level—and they are usually classified by the level of information they can filter.
- A firewall can be a single device or a firewall subnet, which consists of multiple firewalls creating a buffer between the outside and inside networks.

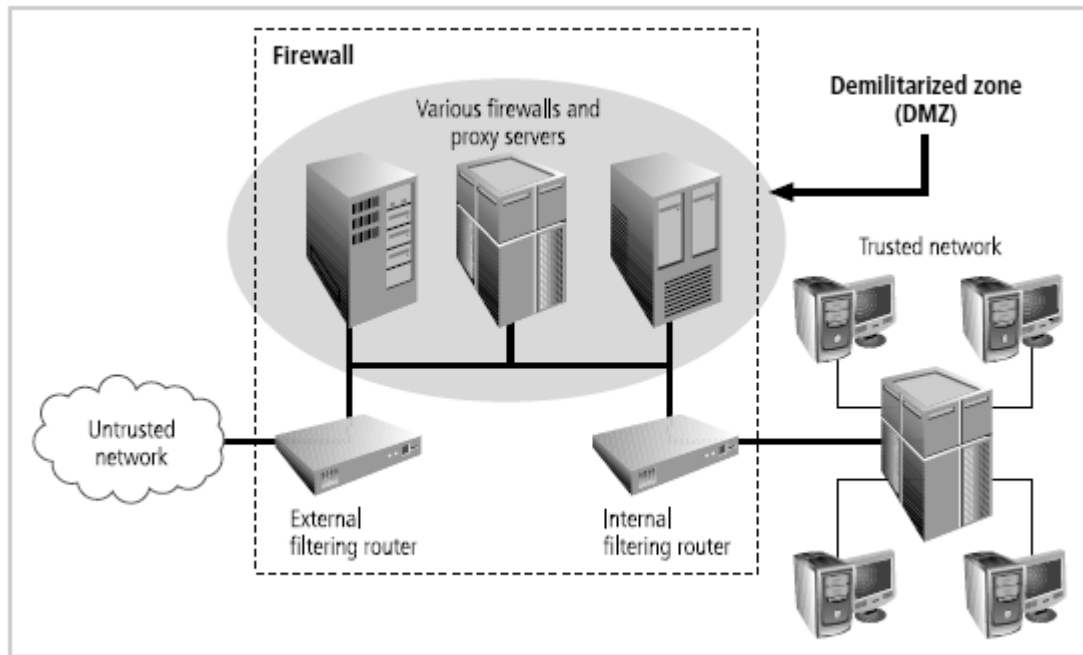
DMZs

- A buffer against outside attacks is frequently referred to as a demilitarized zone (DMZ). The DMZ is a no-man's-land between the inside and outside networks; it is also where some organizations place Web servers.
- These servers provide access to organizational Web pages, without allowing Web requests to enter the interior networks.

Proxy server

- An alternative approach to the strategies of using a firewall subnet or a DMZ is to use a proxy server, or proxy firewall.
- When an outside client requests a particular Web page, the proxy server receives the request as if it were the subject of the request, then asks for the same information from the true Web server(acting as a proxy for the requestor), and then responds to the request as a proxy for the true Web server.

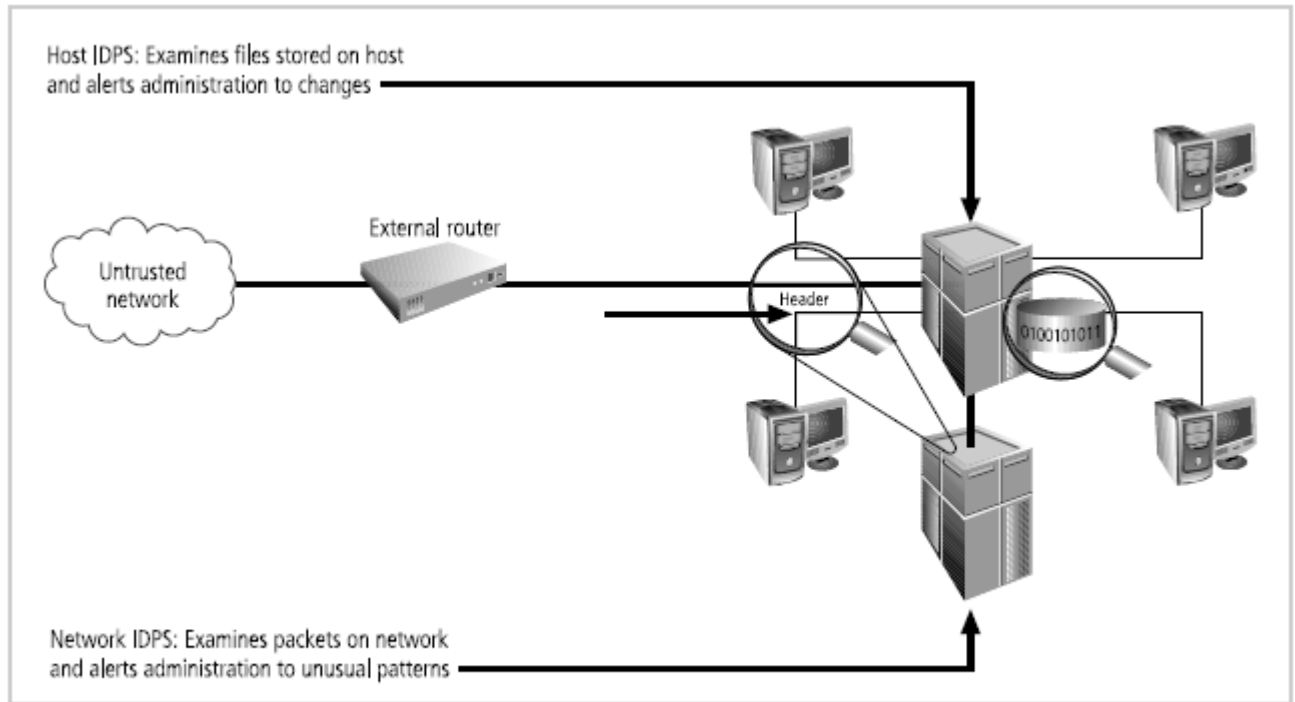
- For more frequently accessed Web pages, proxy servers can cache or temporarily store the page, and thus are sometimes called cache servers.



Firewalls, Proxy Servers, and DMZs

Intrusion Detection and Prevention Systems (IDPSs)

- In an effort to detect unauthorized activity within the inner network, or on individual machines, an organization may wish to implement Intrusion Detection Systems or IDS.
- IDs come in two versions. Host-based & Network-based IDSs.
- Host-based IDSs are usually installed on the machines they protect to monitor the status of various files stored on those machines.
- Network-based IDSs look at patterns of network traffic and attempt to detect unusual activity based on previous baselines.
- This could include packets coming into the organization's networks with addresses from machines already within the organization (IP spoofing).
- It could also include high volumes of traffic going to outside addresses (as in cases of data theft) or coming into the network (as in a denial of service attack).
- Both host-and network based IDSs require a database of previous activity.



Intrusion Detection and Prevention Systems

4.5 SECURITY TRAINING AND AWARENESS PROGRAM

Security Education, Training, and Awareness Program

- As soon as general security policy exists, policies to implement security education, training and awareness (SETA) program should follow.
- SETA is a control measure designed to reduce accidental security breaches by employees.
- Security education and training builds on the general knowledge the employees must possess to do their jobs, familiarizing them with the way to do their jobs securely
- The SETA program consists of three elements: security education; security training; and security awareness
- The purpose of SETA is to enhance security by:
 - Improving awareness of the need to protect system resources.
 - Developing skills and knowledge so computer users can perform their jobs more securely.
 - Building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.

Security Education

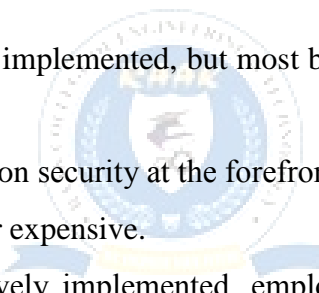
- Everyone in an organization needs to be trained and aware of information security, but not every member of the organization needs a formal degree or certificate in information security.
- A number of universities have formal coursework in information security.
- For those interested in researching formal information security programs, there are resources available, such as the NSA-identified Centers of Excellence in Information Assurance Education.

Security Training

- It involves providing members of the organization with detailed information and hands-on instruction to prepare them to perform their duties securely.
- Management of information security can develop customized in-house training or outsource the training program.

Security Awareness

- One of the least frequently implemented, but most beneficial programs is the security awareness program.
- Designed to keep information security at the forefront of users' minds
- Need not be complicated or expensive.
- If the program is not actively implemented, employees may begin to “tune out” and risk of employee accidents and failures increases.

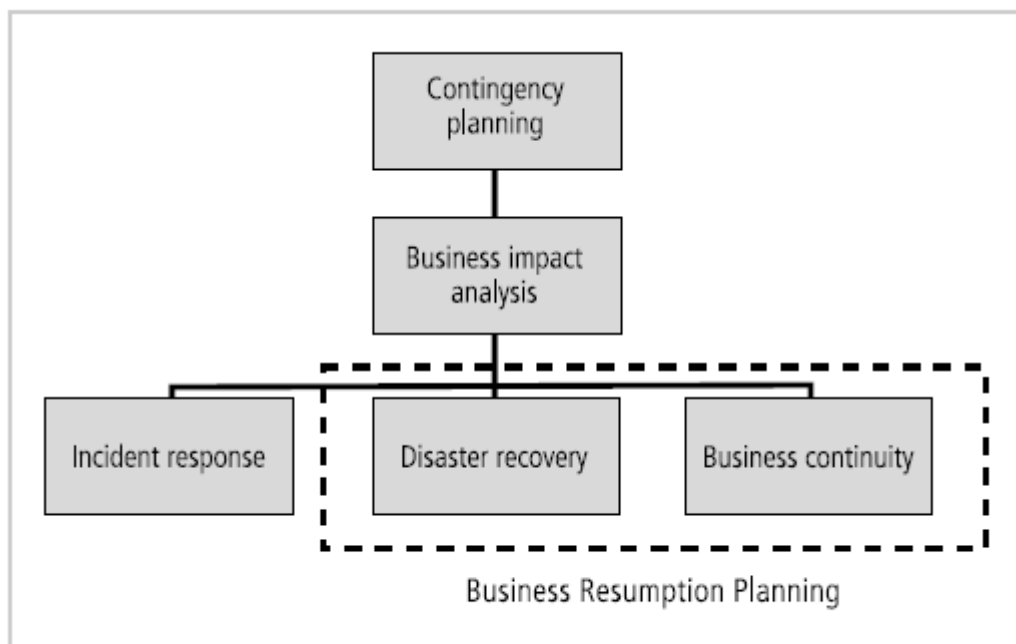


	Education	Training	Awareness
Attribute	Why	How	What
Level	Insight	Knowledge	Information
Objective	Understanding	Skill	Exposure
Teaching	Theoretical instruction	Practical instruction	Media
method	<ul style="list-style-type: none"> • Discussion seminar • Background reading • Hands-on practice 	<ul style="list-style-type: none"> • Lecture • Case study workshop • Posters 	<ul style="list-style-type: none"> • Videos • Newsletters
Test measure	Essay (interpret learning)	Problem solving (apply learning)	<ul style="list-style-type: none"> • True or false • Multiple choice (identify learning)
Impact timeframe	Long term	Intermediate	Short term

Comparative Framework of SETA (from NIST SP800-12²²)

4.6 PLANNING FOR CONTINUITY / CONTINUITY STRATEGIES

- A key role for all managers is *contingency planning*. Managers in the IT and information security communities are usually called on to provide strategic planning to assure the continuous availability of information systems.
- Contingency Planning (CP) comprises a set of plans designed to ensure the effective reaction and recovery from an attack and the subsequent restoration to normal modes of business operations.
- There are various types of contingency plans for events of this type:
 1. Incident response plans
 2. Disaster recovery plans and
 3. Business continuity plans
- Incident response, disaster recovery, and business continuity planning are components of contingency planning.
- A contingency plan is prepared by the organization to anticipate, react to, and recover from events that threaten the security of information and information assets in the organization and, subsequently, to restore the organization to normal modes of business operations.

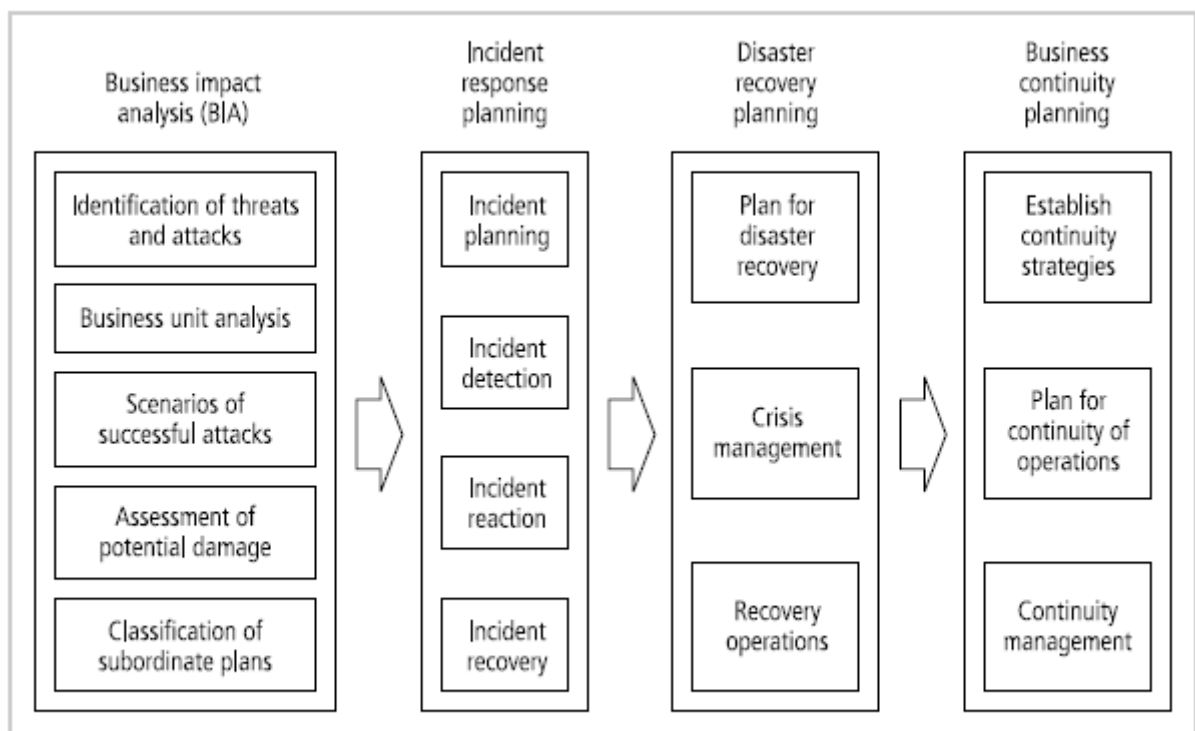


Components of Contingency Planning

- An incident is any clearly identified attack on the organization's information assets that would threaten the assets' confidentiality, integrity, or availability.

- An **incident response (IR)** plan addresses the identification, classification, response, and recovery from an incident.
- The IR plan focuses on immediate response, but if the attack escalates or is disastrous (e.g., fire, flood, earthquake, or total blackout) the process moves on to disaster recovery and the BC plan.
- A **disaster recovery (DR)** plan addresses the preparation for and recovery from a disaster, whether natural or man-made. The DR plan typically focuses on restoring systems at the original site after disasters occur, and as such is closely associated with the BC plan.
- A **business continuity (BC)** plan ensures that critical business functions continue if a catastrophic incident or disaster occurs.
- The BC plan occurs concurrently with the DR plan when the damage is major or ongoing, requiring more than simple restoration of information and information resources. The BC plan establishes critical business functions at an alternate site.

Major Steps in Contingency Planning



Major Steps in Contingency Planning

Business Impact Analysis

- The first phase in the development of the contingency planning process is the business impact analysis (BIA). A BIA is an investigation and assessment of the impact that various attacks can have on the organization.
- BIA takes up where the risk assessment process leaves off. It begins with the prioritized list of threats and vulnerabilities identified in the risk management process and adds information about the criticality of the systems involved and a detailed assessment of the threats and vulnerabilities to which they are subjects.
- The BIA is a crucial component of the initial planning stages, as it provides detailed scenarios of the potential impact each attack could have on the organization.
- The contingency planning team conducts the BIA in the following stages
 1. Threat attack identification and prioritization
 2. Business unit analysis
 3. Attack success scenario development
 4. Potential damage assessment
 5. Subordinate plan classification

Incident response plan (IRP)

- It is the set of activities taken to plan for, detect, and correct the impact of an incident on information assets.
- IRP consists of the following 4 phases:
 - Incident Planning
 - Incident Detection
 - Incident Reaction
 - Incident Recovery

Incident Planning

- Planning for an incident is the first step in the overall process of incident response planning.
- The planners should develop a set of documents that guide the actions of each involved individual who reacts to and recovers from the incident.
- These plans must be properly organized and stored to be available when and where needed, and in a useful format.

Incident Detection

- Incident Detection relies on either a human or automated system, which is often the help desk staff, to identify an unusual occurrence and to classify it properly as an incident.
- The mechanisms that could potentially detect an incident include intrusion detection systems (both host-based and network based), virus detection software, systems administrators, and even end users.
- Once an attack is properly identified, the organization can effectively execute the corresponding procedures from the IR plan. Thus, **incident classification** is the process of examining a potential incident, or **incident candidate**, and determining whether or not the candidate constitutes an actual incident.
- **Incident Indicators**- There is a number of occurrences that could signal the presence of an incident candidate.
- Donald Pipkin, an IT security expert, identifies three categories of incident indicators: Possible, Probable, and Definite Indicators.

Possible Indicators- There are 4 types of possible indicators of events, they are,

1. Presence of unfamiliar files.
2. Presence or execution of unknown programs or processes.
3. Unusual consumption of computing resources
4. Unusual system crashes

Probable Indicators- The four types of probable indicators of incidents are

1. Activities at unexpected times.
2. Presence of new accounts
3. Reported attacks
4. Notification from IDS

Definite Indicators- The five types of definite indicators of incidents are

1. Use of Dormant accounts
2. Changes to logs
3. Presence of hacker tools
4. Notifications by partner or peer
5. Notification by hacker

Incident Reaction

- It consists of actions outlined in the IRP that guide the organization in attempting to stop the incident, mitigate the impact of the incident, and provide information for recovery from the incident.
- These actions take place as soon as the incident itself is over.
- In reacting to the incident there are a number of actions that must occur quickly, including notification of key personnel and documentation of the incident.
- These must have been prioritized and documented in the IRP for quick use in the heat of the moment.

Incident Recovery

- The recovery process involves much more than the simple restoration of stolen, damaged, or destroyed data files.
- It involves the following steps.
 1. Identify the Vulnerabilities
 2. Address the safeguards.
 3. Evaluate monitoring capabilities
 4. Restore the data from backups.
 5. Restore the services and processes in use.
 6. Continuously monitor the system
 7. Restore the confidence of the members of the organization's communities of interest.

Disaster Recovery Plan (DRP)

- DRP provides detailed guidance in the event of a disaster and also provides details on the roles and responsibilities of the various individuals involved in the disaster recovery effort, and identifies the personnel and agencies that must be notified.
- At a minimum, the DRP must be reviewed during a walk-through or talk-through on a periodic basis.

Many of the same precepts of incident response apply to disaster recovery:

1. There must be a clear establishment of priorities
2. There must be a clear delegation of roles and responsibilities
3. Someone must initiate the alert roster and notify key personnel.

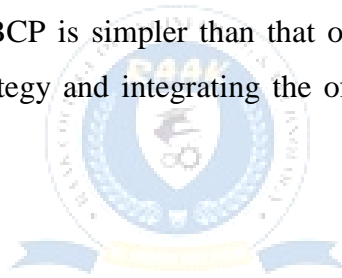
4. Someone must be tasked with the documentation of the disaster.
5. If and only if it is possible, attempts must be made to mitigate the impact of the disaster on the operations of the organization.

Business Continuity Plan (BCP)

- It prepares an organization to reestablish critical business operations during a disaster that affects operations at the primary site.
- If a disaster has rendered the current location unusable for continued operations, there must be a plan to allow the business to continue to function.

Developing Continuity Programs

- Once the incident response plans and disaster recovery plans are in place, the organization needs to consider finding temporary facilities to support the continued viability of the business in the event of a disaster.
- The development of the BCP is simpler than that of the IRP and DRP, in that it consists of selecting a continuity strategy and integrating the off-site data storage and recovery functions into this strategy.



Continuity Strategies

- There are a number of strategies from which an organization can choose when planning for business continuity.
- The determining factor in selection between these options is usually cost.
- In general there are three exclusive options: Hot sites, Warm Sites, and Cold sites; and three shared functions: Time-share, Service bureaus, and Mutual Agreements.
 - **Hot sites:** A hot site is a fully configured facility, with all services, communications links, and physical plant operations including heating and air conditioning. It is the pinnacle of contingency planning, a duplicate facility that needs only the latest data backups and the personnel to function as a fully operational twin of the original. Disadvantages include the need to provide maintenance for all the systems and equipment in the hot site, as well as physical and information security.
 - **Warm sites:** A warm site includes computing equipment and peripherals with servers but not client work stations. It has many of the advantages of a hot site, but at a lower cost.

- **Cold Sites:** A cold site provides only rudimentary services and facilities, No computer hardware or peripherals are provided. Basically a cold site is an empty room with heating, air conditioning, and electricity. The main advantage of cold site is in the area of cost.
- **Time-shares:** It allows the organization to maintain a disaster recovery and business continuity option, but at a reduced overall cost. The advantages are identical to the type of site selected (hot, warm, or cold). The disadvantages are the possibility that more than one organization involved in the time share may need the facility simultaneously and the need to stock the facility with the equipment and data from all organizations involved, the negotiations for arranging the time-share, and associated arrangements, should one or more parties decide to cancel the agreement or to sublease its options.
- **Service bureaus:** A service bureau is an agency that provides a service for a fee. In the case of disaster recovery and continuity planning, the service is the agreement to provide physical facilities in the event of a disaster. These types of agencies also provide off-site data storage for a fee. The disadvantage is that it is a service, and must be renegotiated periodically. Also, using a service bureau can be quite expensive.
- **Mutual Agreements:** A mutual agreement is a contract between two or more organizations that specifies how each will assist the other in the event of a disaster.

