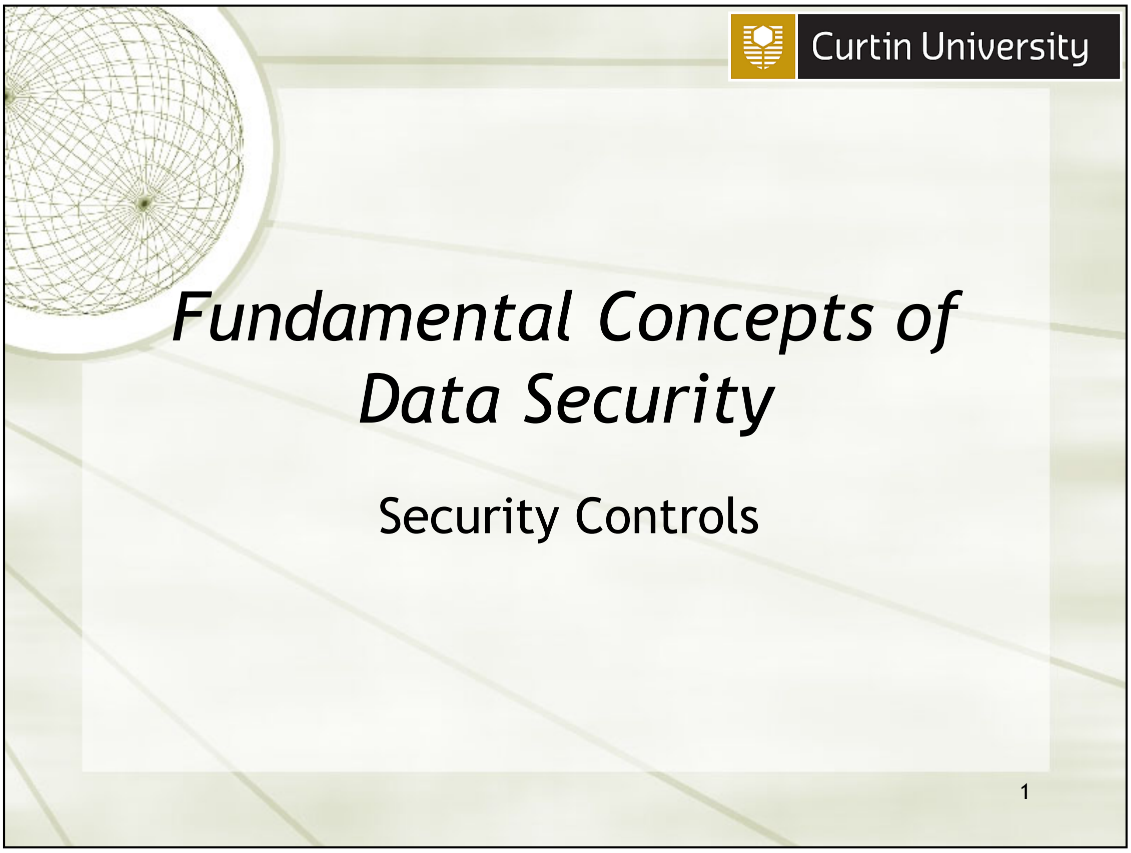
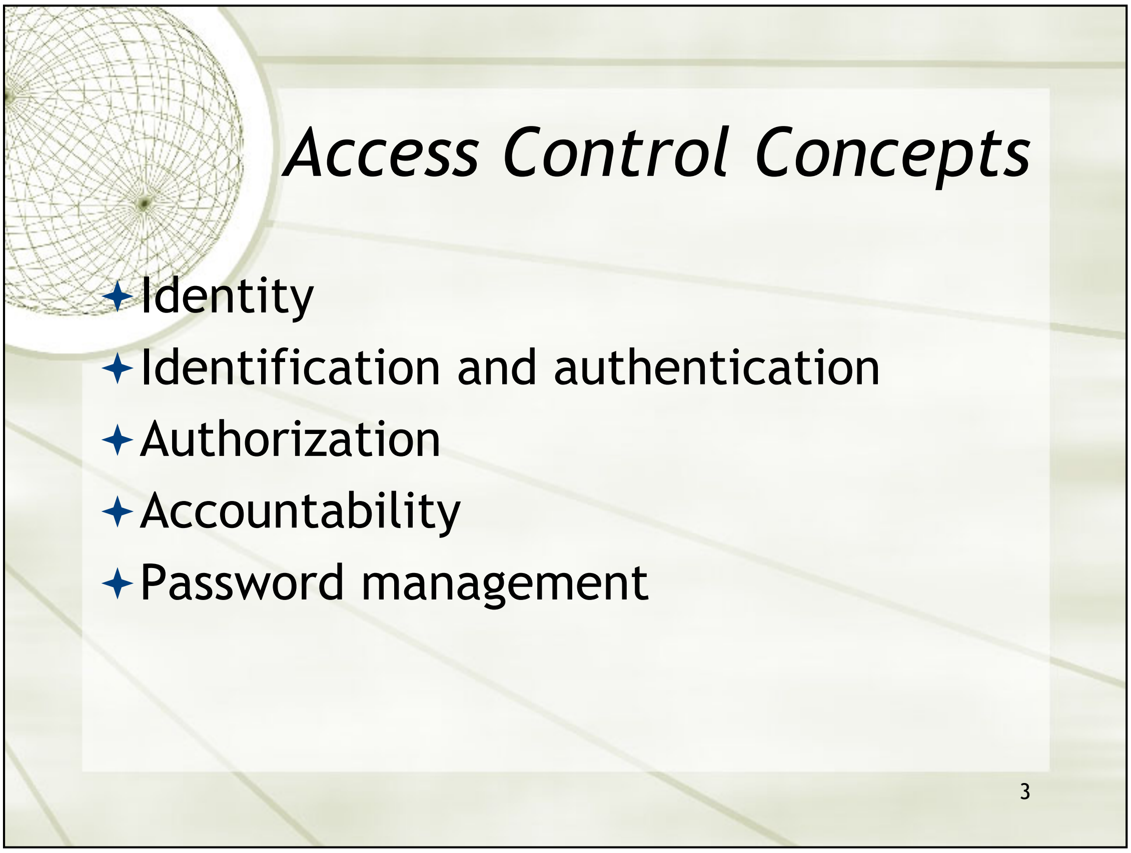


Fundamental Concepts of Data Security

Security Controls



Access Control Concepts

- Identity
- Identification and authentication
- Authorization
- Accountability
- Password management

Access controls are security features that control how users and systems communicate and interact with other systems and resources. They protect the systems and resources from unauthorized access and can be components that participate in determining the level of authorization after an authentication procedure has successfully completed. Access control is a broad term that covers several different types of mechanisms that enforce access control features on computer systems, networks, and information. Access control is extremely important because it is one of the first lines of defense in battling unauthorized access to systems and network resources.

Access Control Review

The following is a review of the basic concepts in access control:

- Identification
- Subjects supplying identification information
- Username, user ID, account number
- Authentication
- Verifying the identification information
- Passphrase, PIN value, biometric, one-time password, password
- Authorization
- Using criteria to make a determination of operations that subjects can

carry out on objects

- “I know who you are, now what am I going to allow you to do?”
- Accountability
- Audit logs and monitoring to track subject activities with objects

Identity

Identity is a complicated concept with many varied nuances, ranging from the philosophical to the practical. A person can have multiple digital identities. Creating or issuing secure identities should include three key aspects: uniqueness, nondescriptive, and issuance. The first, uniqueness, refers to the identifiers that are specific to an individual, meaning every user must have a unique ID for accountability. Things like fingerprints and retina scans can be considered unique elements in determining identity. Nondescriptive means that neither piece of the credential set should indicate the purpose of that account. For example, a user ID should not be “administrator,” “backup_operator,” or “CEO.” The third key aspect in determining identity is issuance. These elements are the ones that have been provided by another authority as a means of proving identity. ID cards are a kind of security element that would be considered an issuance form of identification.

Identification Component Requirements: When issuing identification values to users, the following should be in place:

- Each value should be unique, for user accountability.
- A standard naming scheme should be followed.
- The value should be non-descriptive of the user’s position or tasks.
- The value should not be shared between users.

Identification and Authentication

Identification describes a method of ensuring that a subject (user, program, or process) is the entity it claims to be. Identification can be provided with the use of a username or account number. Once a person has been identified through the user ID or a similar value, she must be ***authenticated***, which means she must prove she is who she says she is. Three general factors can be used for authentication: ***something a person knows, something a person has,*** and ***something a person is***. They are also commonly called authentication by knowledge, authentication by ownership, and authentication by characteristic. ***Strong authentication*** contains two out of these three methods: something a person knows, has, or is. Strong authentication is also sometimes referred to as ***multi-authentication***, which just means that more than one authentication method is used. ***Three-factor authentication*** is possible, which includes all authentication approaches.

Authorization

Once the subject provides its credentials and is properly identified, the system it is trying to access needs to determine if this subject has been given the necessary rights and privileges to carry out the requested actions. The system will look at some type of access control matrix or compare security labels to verify that this subject may indeed access the requested resource and perform the actions it is attempting. If the system determines that the subject may access the resource, it ***authorizes*** the subject.

Identity Management

Identity management is a broad and loaded term that encompasses the use of different products to identify, authenticate, and authorize users through automated means. The following are many of the common questions enterprises deal with today in controlling access to assets:

- What should each user have access to?
- Who approves and allows access?
- How do the access decisions map to policies?
- Do former employees still have access?
- How do we keep up with our dynamic and ever-changing environment?
- What is the process of revoking access?
- How is access controlled and monitored centrally?
- Why do employees have eight passwords to remember?

Accountability

Auditing capabilities ensure users are accountable for their actions, verify that the security policies are enforced, and can be used as investigation tools. There are several reasons why network administrators and security professionals want to make sure accountability mechanisms are in place and configured properly: to be able to track bad deeds back to individuals, detect intrusions, reconstruct events and system conditions, provide legal recourse material, and produce problem reports. Audit documentation and log files hold a mountain of information—the trick is usually deciphering it and presenting it in a useful and understandable format.

Accountability is tracked by recording user, system, and application activities. This recording is done through auditing functions and mechanisms within an operating system or application. Audit trails contain information about operating system activities, application events, and user actions. Audit trails can be used to verify the health of a system by checking performance information or certain types of errors and conditions. After a system crashes, a network administrator often will review audit logs to try and piece together the status of the system and attempt to understand what events could be attributed to the disruption.

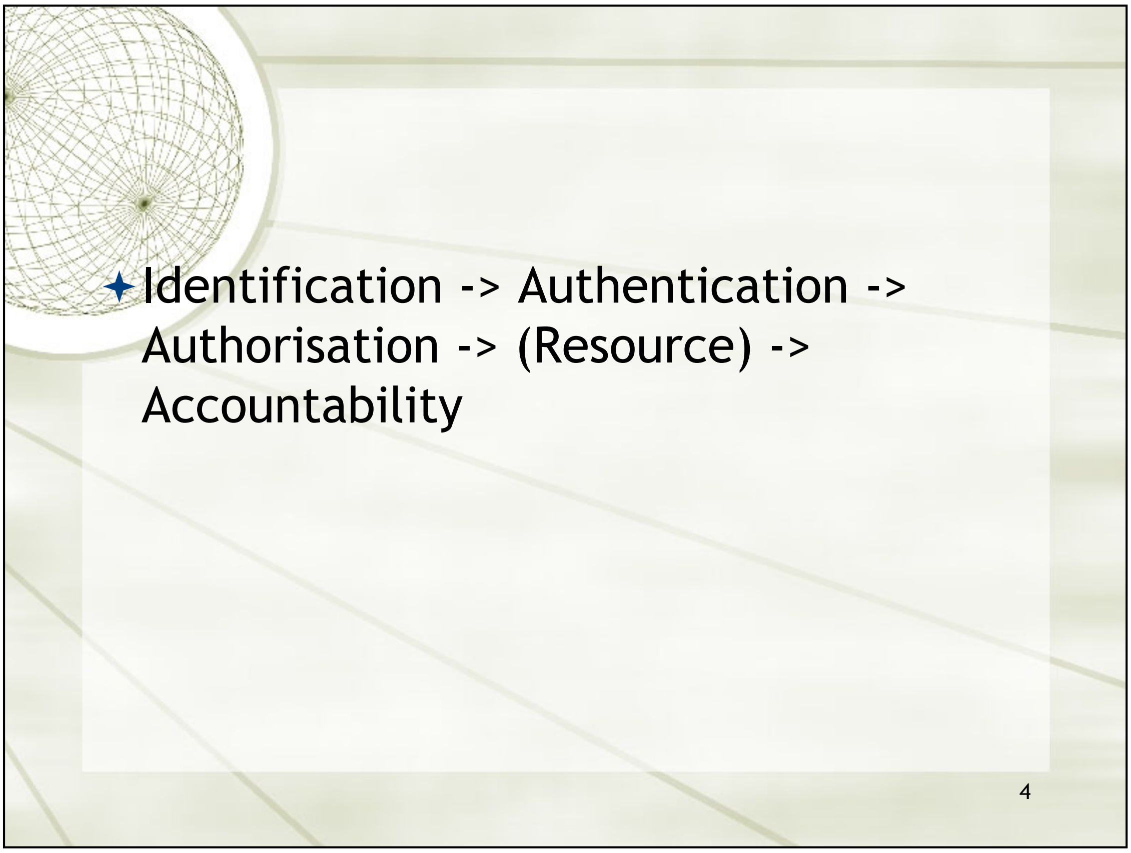
It is a good idea to keep the following in mind when dealing with auditing:

- Store the audits securely.
- The right audit tools will keep the size of the logs under control.
- The logs must be protected from any unauthorized changes in order to safeguard data.
- Train the right people to review the data in the right manner.
- Make sure the ability to delete logs is only available to administrators.
- Logs should contain activities of all high-privileged accounts (root, administrator).

Password Management

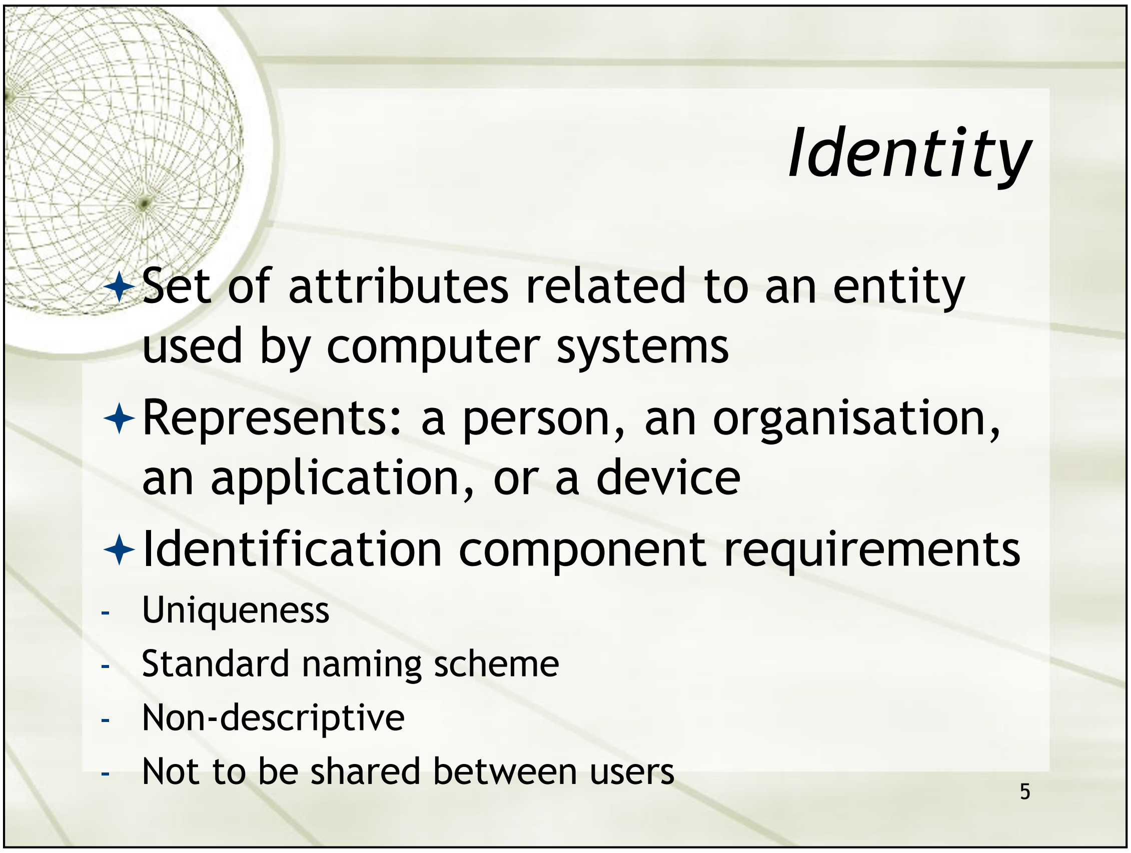
Different types of password management technologies have been developed to get these pesky users off the backs of IT and the help desk by providing a more secure and automated password management system. The most common password management approaches are listed next:

- **Password Synchronization** Reduces the complexity of keeping up with different passwords for different systems.
- **Self-Service Password Reset** Reduces help-desk call volumes by allowing users to reset their own passwords.
- **Assisted Password Reset** Reduces the resolution process for password issues for the help desk. This may include authentication with other types of authentication mechanisms (biometrics, tokens).



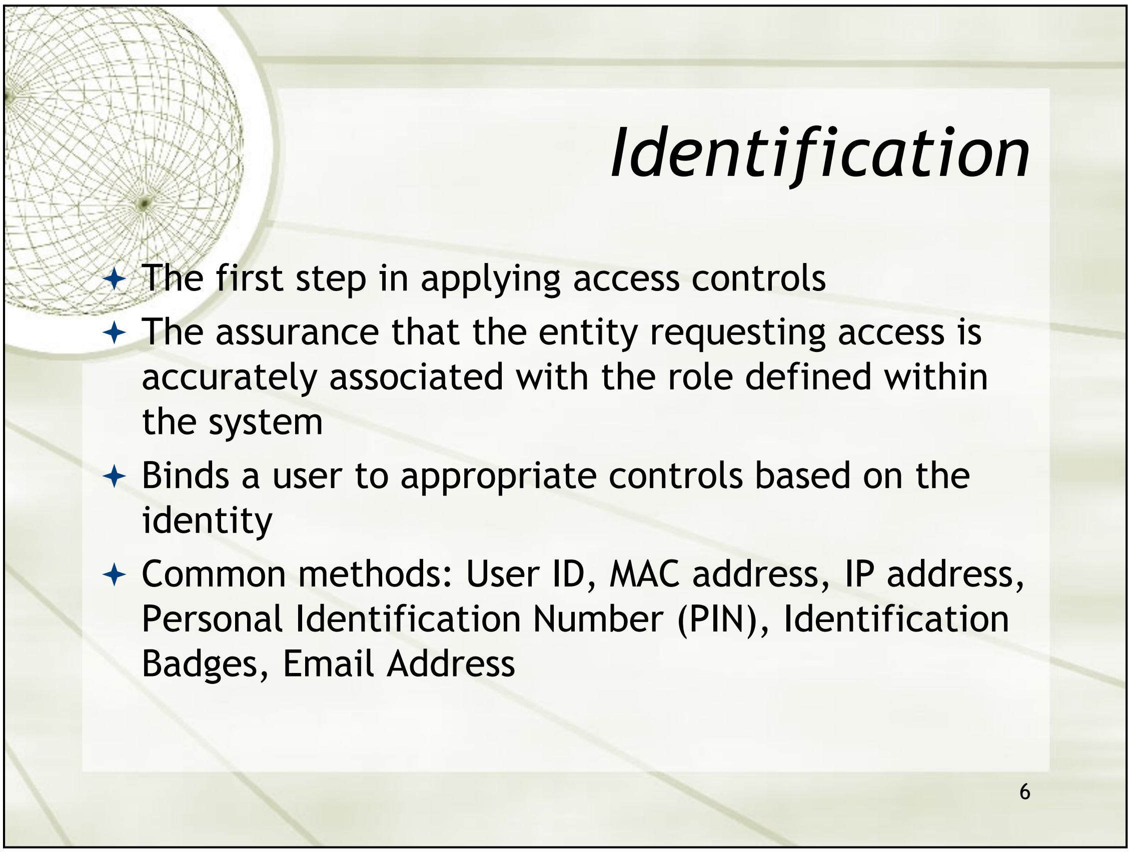
- Identification -> Authentication -> Authorisation -> (Resource) -> Accountability

4



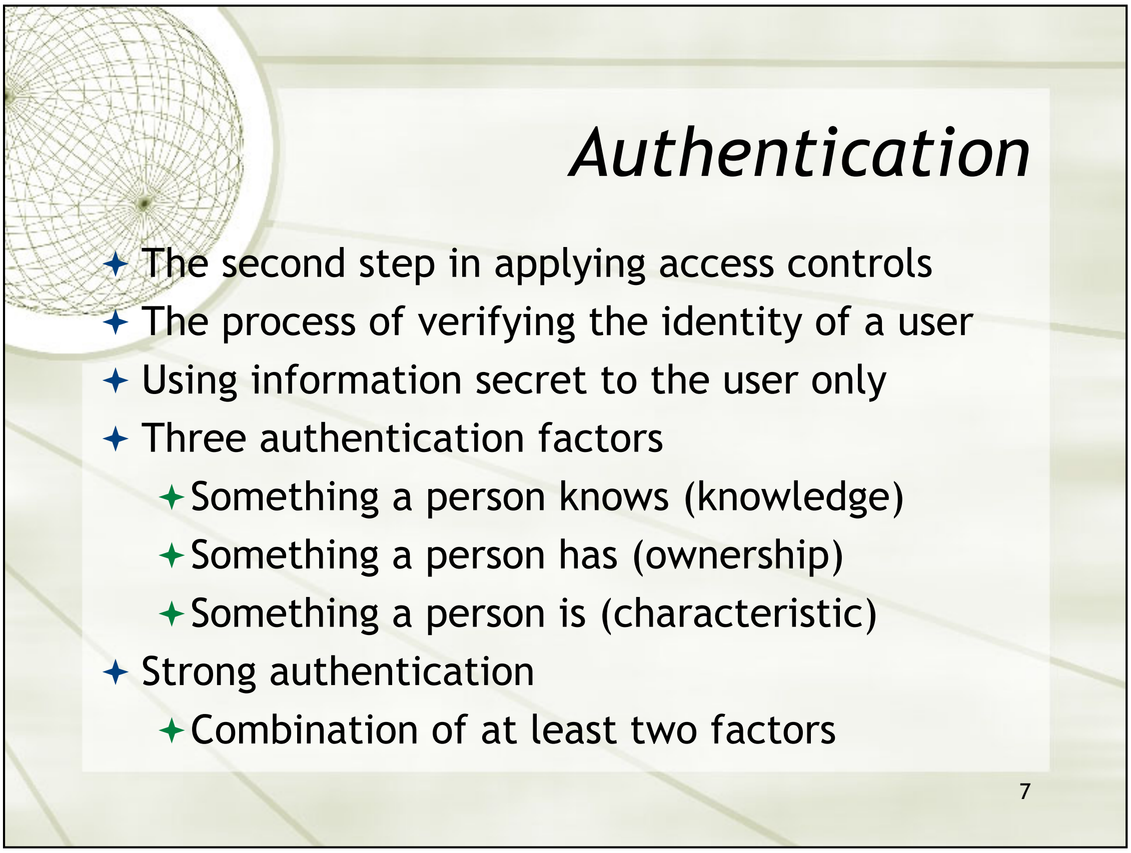
Identity

- Set of attributes related to an entity used by computer systems
- Represents: a person, an organisation, an application, or a device
- Identification component requirements
  - Uniqueness
  - Standard naming scheme
  - Non-descriptive
  - Not to be shared between users



Identification

- The first step in applying access controls
- The assurance that the entity requesting access is accurately associated with the role defined within the system
- Binds a user to appropriate controls based on the identity
- Common methods: User ID, MAC address, IP address, Personal Identification Number (PIN), Identification Badges, Email Address



Authentication

- The second step in applying access controls
- The process of verifying the identity of a user
- Using information secret to the user only
- Three authentication factors
  - Something a person knows (knowledge)
  - Something a person has (ownership)
  - Something a person is (characteristic)
- Strong authentication
  - Combination of at least two factors

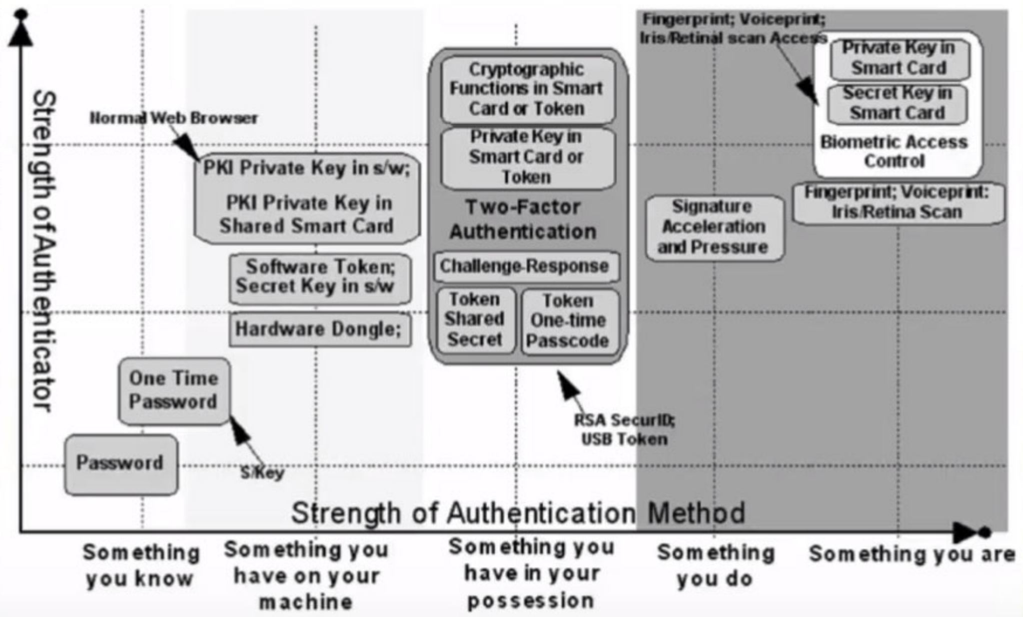
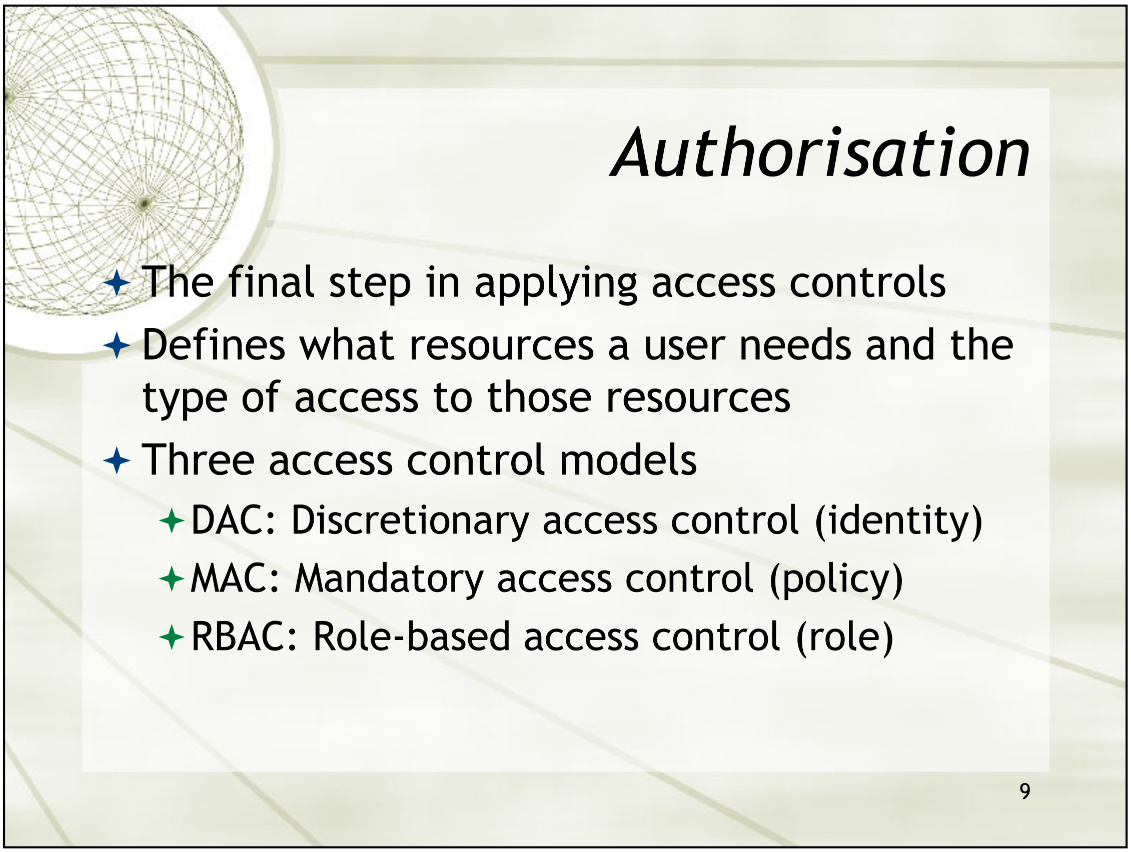
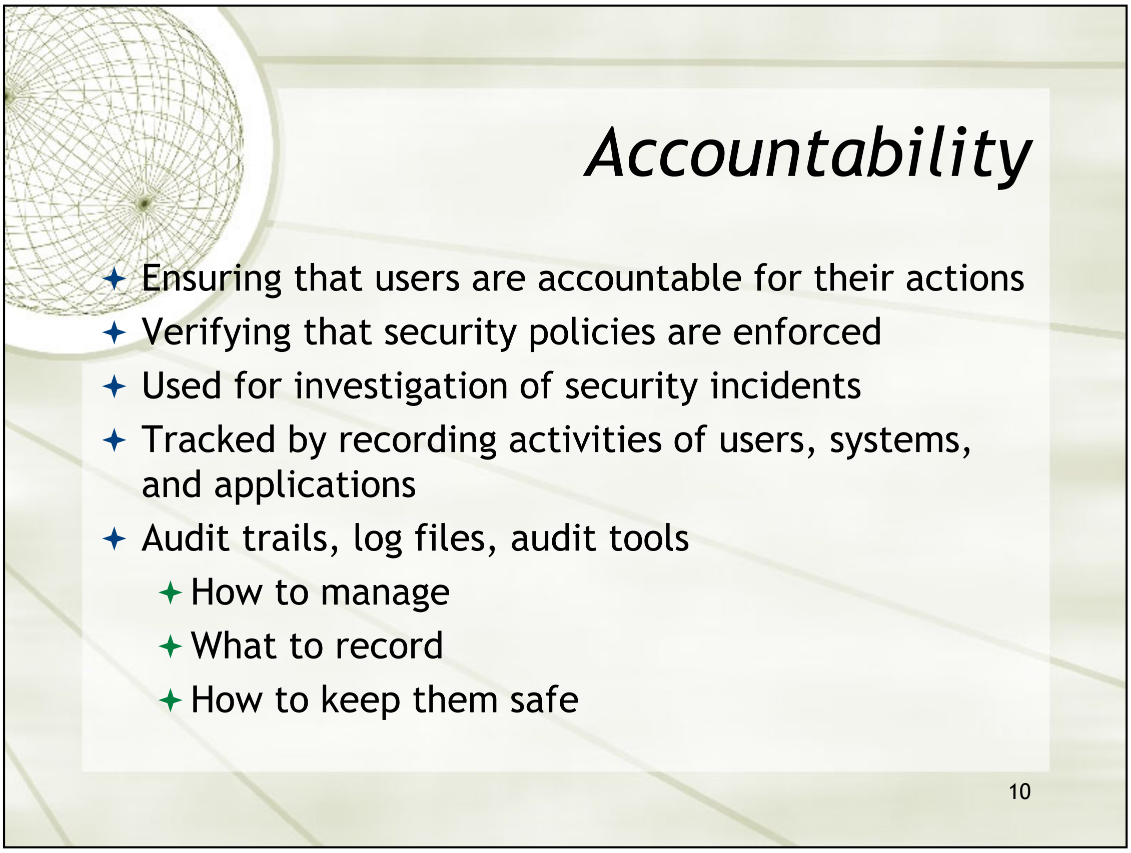

Strength of Authenticator
Normal Web Browser
PKI Private Key in s/w;
PKI Private Key in Shared Smart Card
Software Token; Secret Key in s/w
Hardware Dongle;
One Time Password
Password
S/Key
Cryptographic Functions in Smart Card or Token
Private Key in Smart Card or Token
Two-Factor Authentication
Challenge-Response
Token Shared Secret
Token One-time Passcode
RSA SecurID; USB Token
Fingerprint; Voiceprint; Iris/Retinal scan Access
Private Key in Smart Card
Secret Key in Smart Card
Biometric Access Control
Fingerprint; Voiceprint: Iris/Retina Scan
Signature Acceleration and Pressure
Strength of Authentication Method
Something you know
Something you have on your machine
Something you have in your possession
Something you do
Something you are

Figure 2.7. Authentication method comparison.



Authorisation

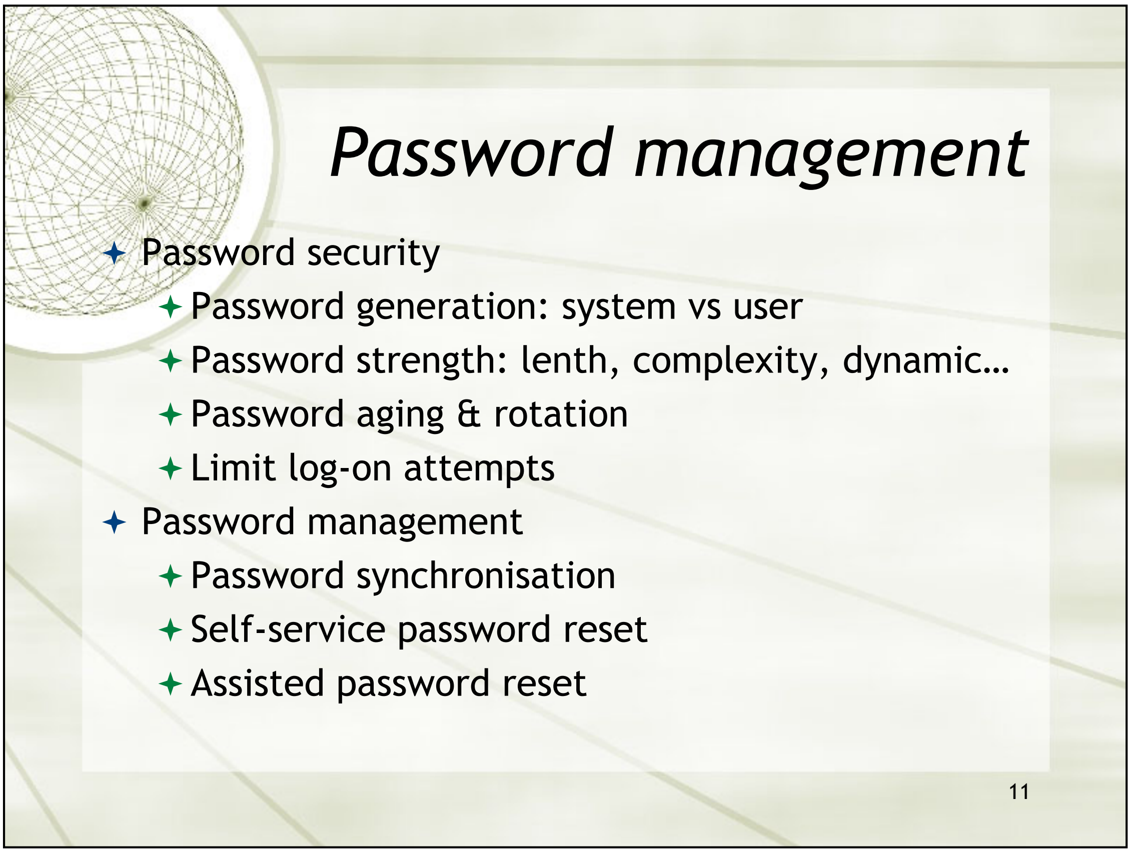
- The final step in applying access controls
- Defines what resources a user needs and the type of access to those resources
- Three access control models
  - DAC: Discretionary access control (identity)
  - MAC: Mandatory access control (policy)
  - RBAC: Role-based access control (role)



Accountability

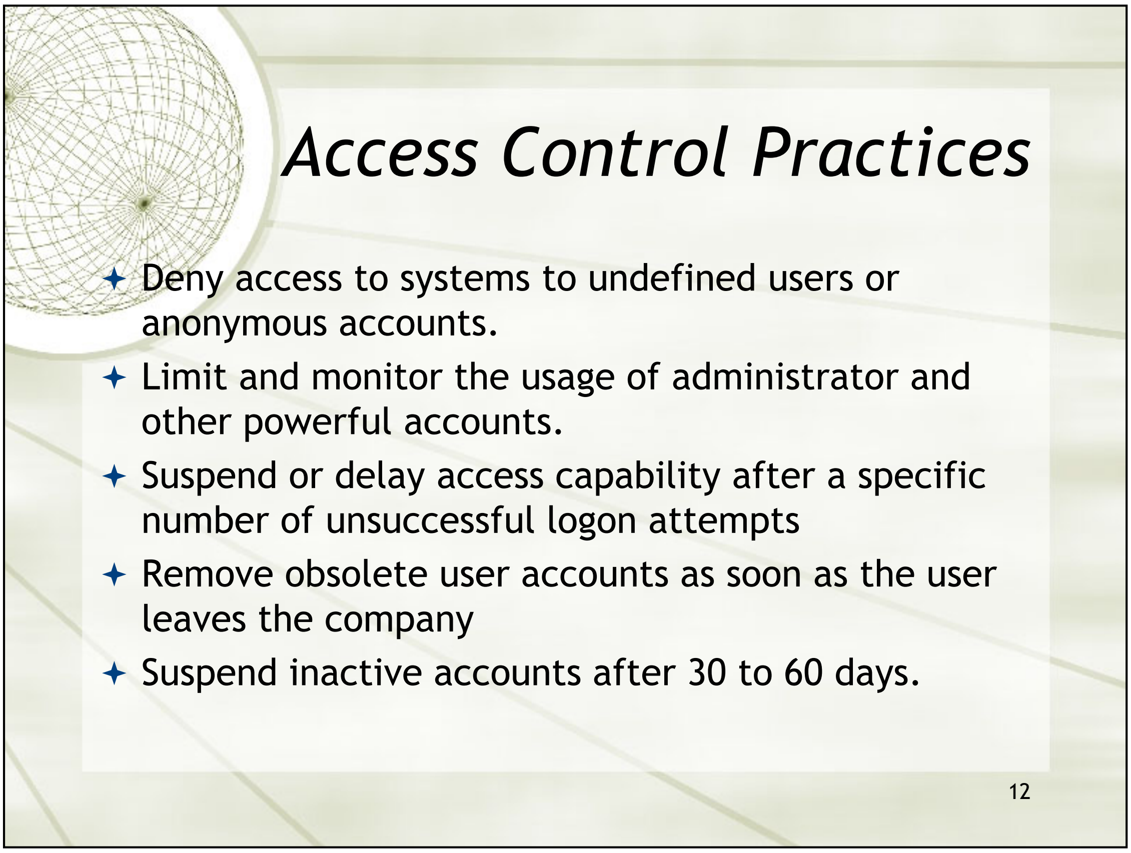
- Ensuring that users are accountable for their actions
- Verifying that security policies are enforced
- Used for investigation of security incidents
- Tracked by recording activities of users, systems, and applications
- Audit trails, log files, audit tools
  - How to manage
  - What to record
  - How to keep them safe

10



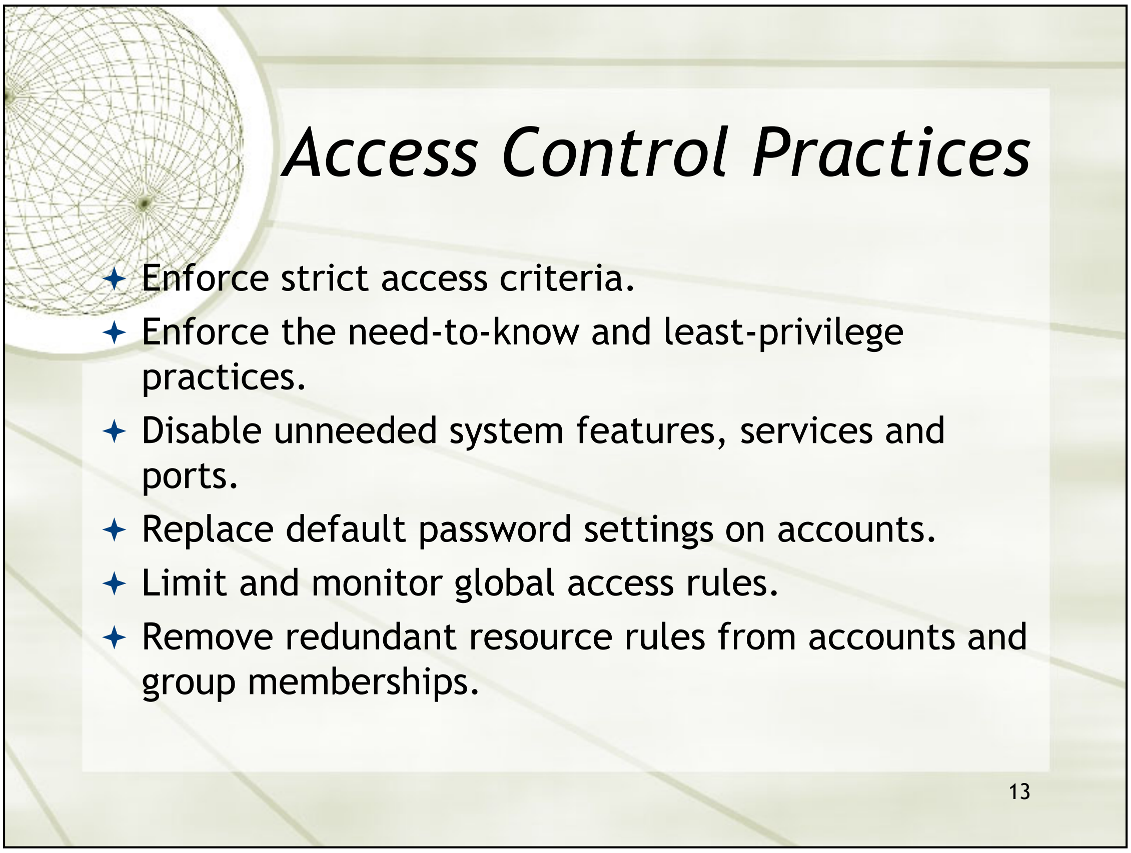
Password management

- Password security
  - Password generation: system vs user
  - Password strength: lenth, complexity, dynamic…
  - Password aging & rotation
  - Limit log-on attempts
- Password management
  - Password synchronisation
  - Self-service password reset
  - Assisted password reset



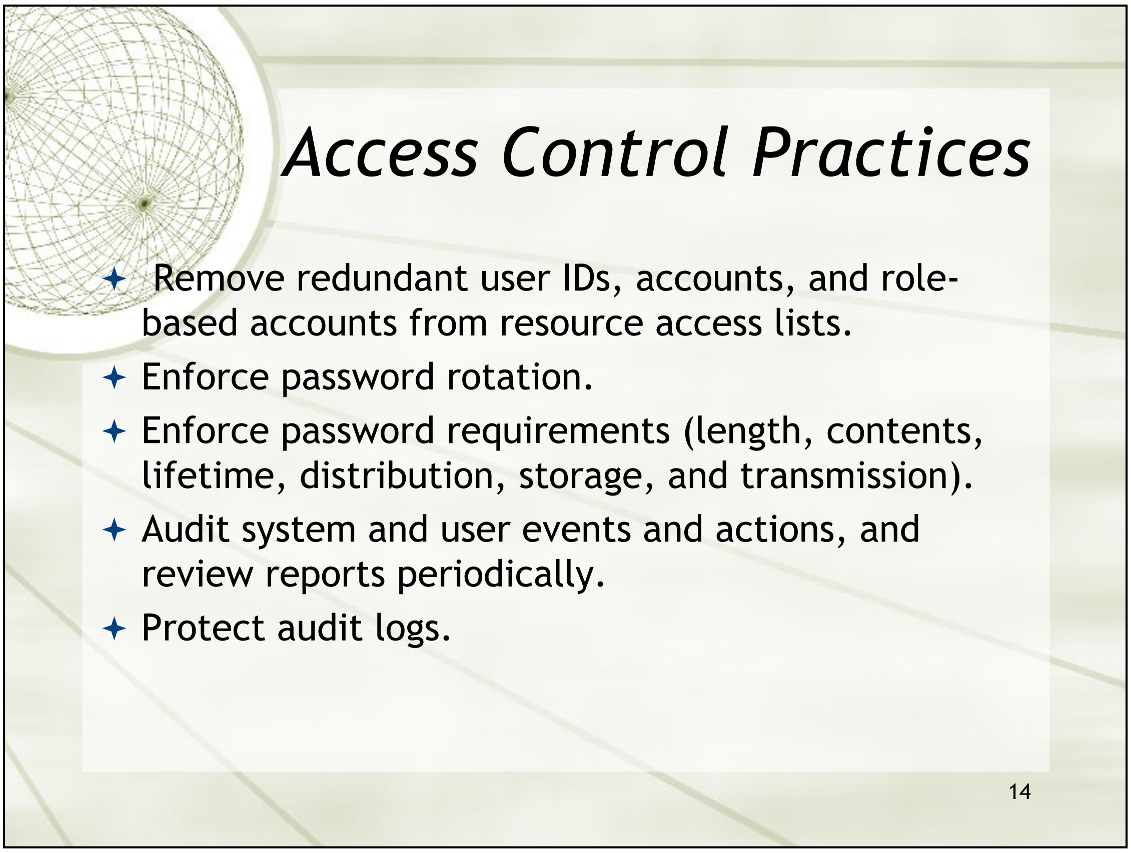
Access Control Practices

- Deny access to systems to undefined users or anonymous accounts.
- Limit and monitor the usage of administrator and other powerful accounts.
- Suspend or delay access capability after a specific number of unsuccessful logon attempts
- Remove obsolete user accounts as soon as the user leaves the company
- Suspend inactive accounts after 30 to 60 days.



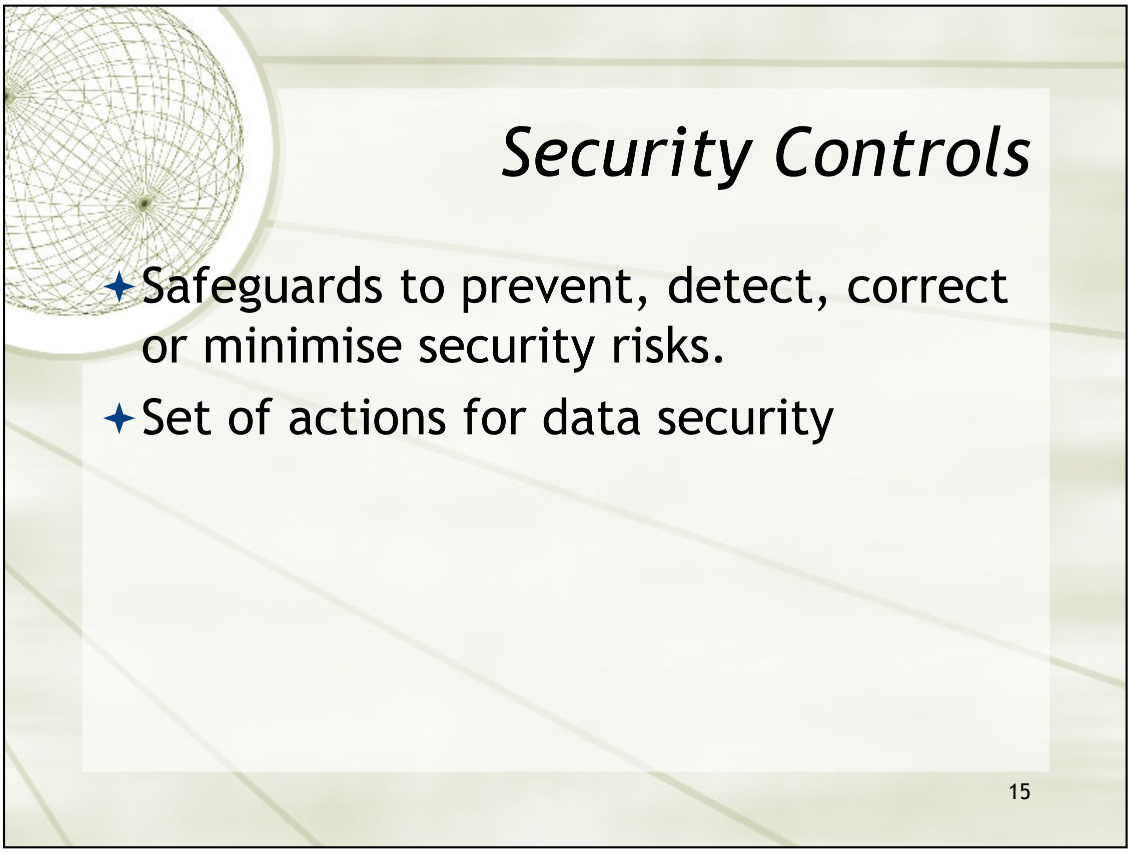
Access Control Practices

- Enforce strict access criteria.
- Enforce the need-to-know and least-privilege practices.
- Disable unneeded system features, services and ports.
- Replace default password settings on accounts.
- Limit and monitor global access rules.
- Remove redundant resource rules from accounts and group memberships.



Access Control Practices

- Remove redundant user IDs, accounts, and role-based accounts from resource access lists.
- Enforce password rotation.
- Enforce password requirements (length, contents, lifetime, distribution, storage, and transmission).
- Audit system and user events and actions, and review reports periodically.
- Protect audit logs.



Security Controls

- Safeguards to prevent, detect, correct or minimise security risks.
- Set of actions for data security

15

Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. A principle benefit of the Controls is that they prioritize and focus a smaller number of actions with high pay-off results. The Controls are effective because they are derived from the most common attack patterns highlighted in the leading threat reports and vetted across a very broad community of government and industry practitioners. They were created by the people who know how attacks work - NSA Red and Blue teams, the US Department of Energy nuclear energy labs, law enforcement organizations and some of the nation's top forensics and incident response organizations - to answer the question, "what do we need to do to stop known attacks." That group of experts reached consensus and today we have the most current Controls. The key to the continued value is that the Controls are updated based on new attacks that are identified and analyzed by groups from Verizon to Symantec so the Controls can stop or mitigate those attacks.

https://www.sans.org/critical-security-controls

Inventory of Authorized and Unauthorized Devices

Inventory of Authorized and Unauthorized Software

Secure Configurations for Hardware and Software on Mobile Device

Laptops, Workstations, and Servers

Continuous Vulnerability Assessment and Remediation

Controlled Use of Administrative Privileges

Maintenance, Monitoring, and Analysis of Audit Logs

Email and Web Browser Protections

Malware Defenses

Limitation and Control of Network Ports, Protocols, and Services

Data Recovery Capability

Secure Configurations for Network Devices such as Firewall Routers, and Switches

Boundary Defense

Data Protection

Controlled Access Based on the Need to Know

Wireless Access Control

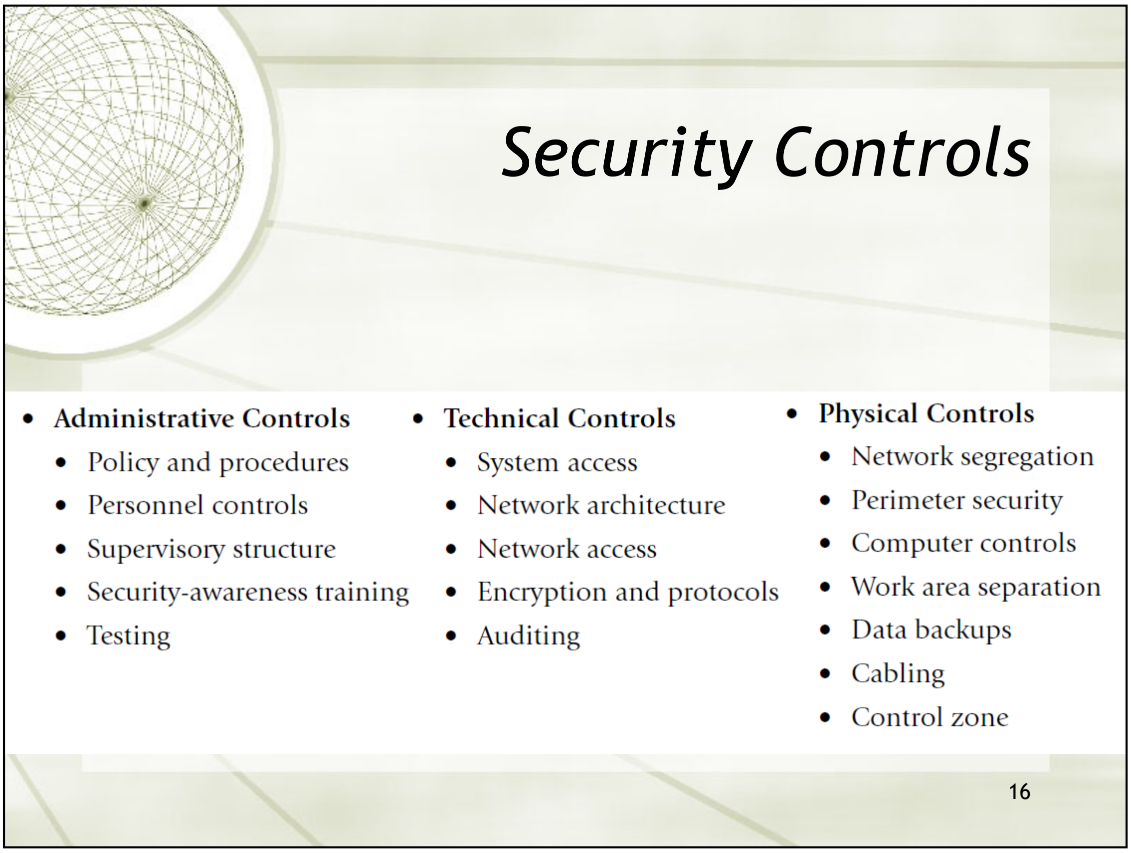
Account Monitoring and Control

Security Skills Assessment and Appropriate Training to Fill Gaps

Application Software Security

Incident Response and Management

Penetration Tests and Red Team Exercises



Security Controls

- **Administrative Controls**
  - Policy and procedures
  - Personnel controls
  - Supervisory structure
  - Security-awareness training
  - Testing
- **Technical Controls**
  - System access
  - Network architecture
  - Network access
  - Encryption and protocols
  - Auditing
- **Physical Controls**
  - Network segregation
  - Perimeter security
  - Computer controls
  - Work area separation
  - Data backups
  - Cabling
  - Control zone

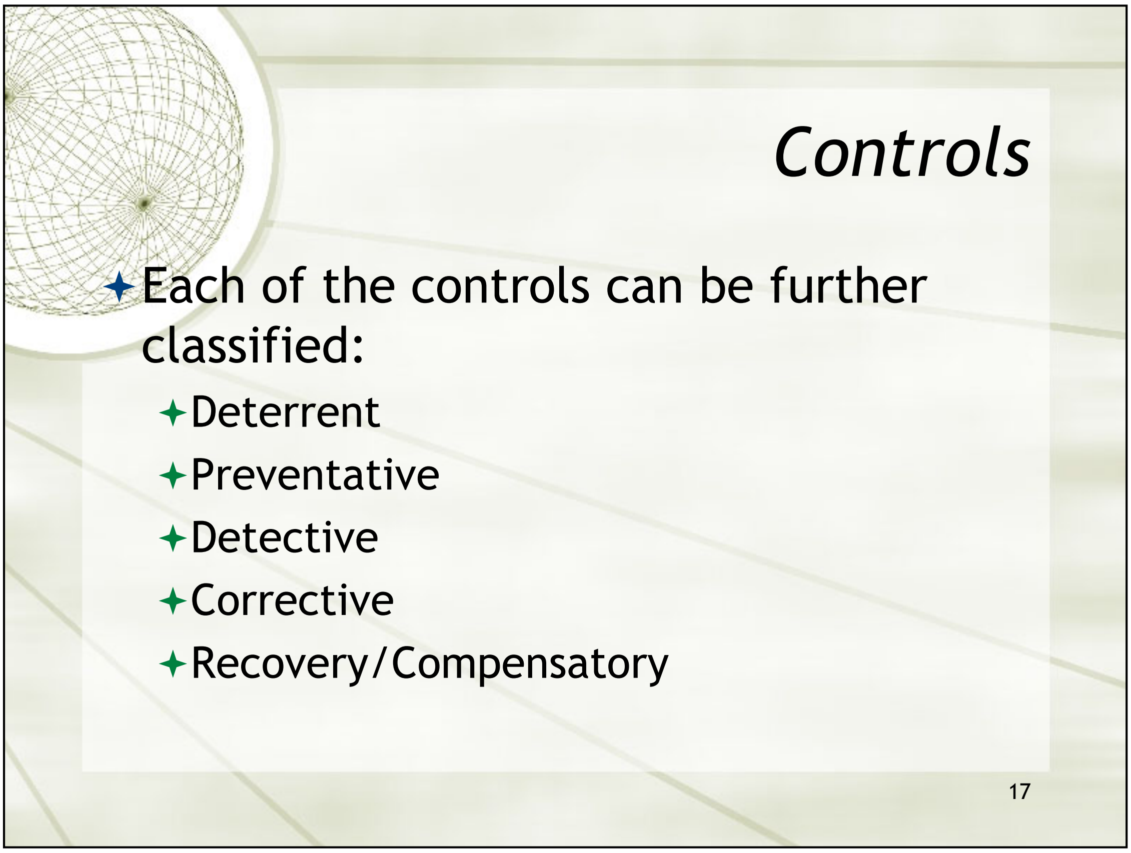
16

The following controls should be utilized to achieve management's security directives:

Administrative controls: These include the developing and publishing of policies, standards, procedures, and guidelines; risk management; the screening of personnel; conducting security-awareness training; and implementing change control procedures.

Technical controls (also called logical controls): These consist of implementing and maintaining access control mechanisms, password and resource management, identification and authentication methods, security devices, and the configuration of the infrastructure.

Physical controls: These entail controlling individual access into the facility and different departments, locking systems and removing unnecessary floppy or CD-ROM drives, protecting the perimeter of the facility, monitoring for intrusion, and environmental controls.



Controls

- Each of the controls can be further classified:
  - Deterrent
  - Preventative
  - Detective
  - Corrective
  - Recovery/Compensatory

17

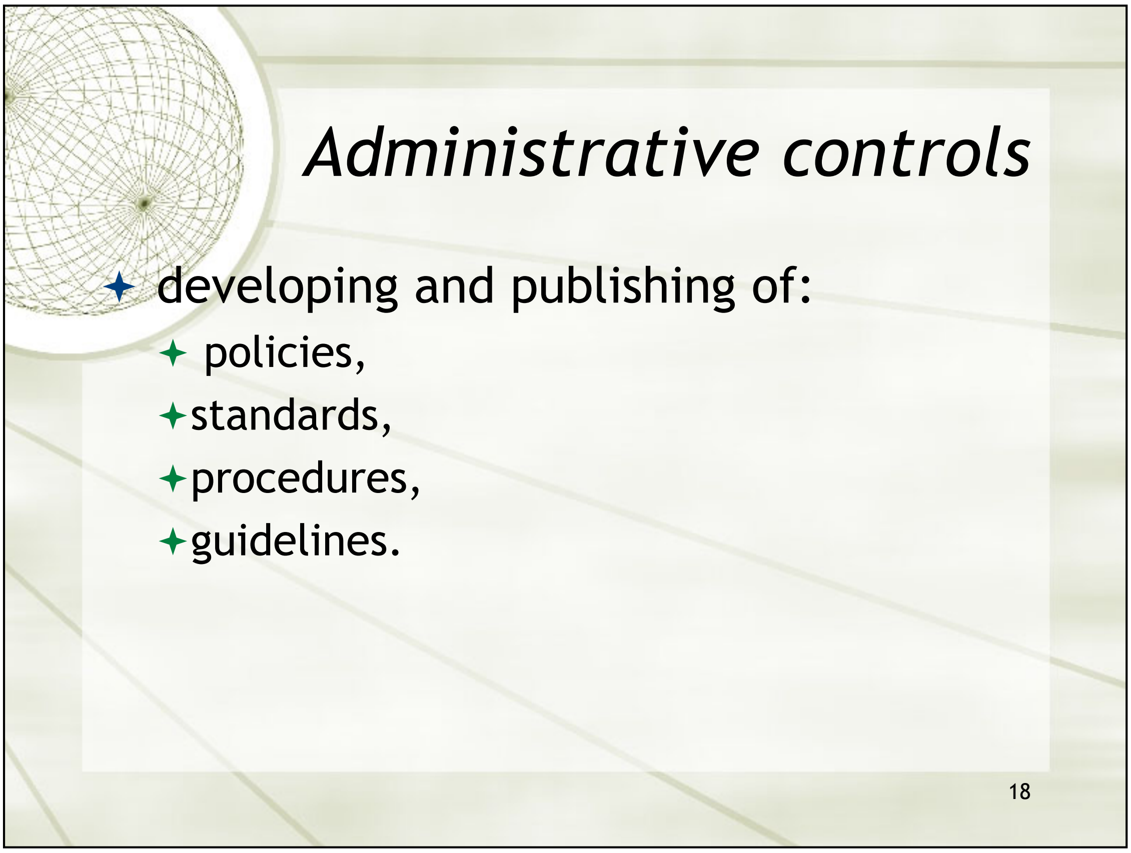
Deterrent: controls to discourage attacks at the first place, deter people from breaching security, e.g warning, banner, logon message, fake CCTV cameras to warn people, security measures on websites to tell people that they are protected

Preventive: controls that make it hard for attacks to succeed, e.g. firewall (stops unwelcomed traffic), encryption, locked doors

Detective: controls that detect if an attack has occurred, e.g. checksum, intrusion detection system, rotation of duties, security audits, monitors and sensors, motion sensors installed in the buildings to detect intruders, CCTV cameras, sometimes firewall that tells when an attack has been made on the system, intrusion detection systems that monitor the activity on the hosts and computers over the network

Corrective: corrective aspects of security, controls that reverse the damage, e.g. version control, incident handling procedures, fire extinguishers, undo, recycle bin, DOS attack (ban the IP addresses to stop from jamming the servers), Fire extinguishers (putting out fires when it has happened), Incident handling procedures (tells employees what to do when an incident happens)

Recovery: controls that bring the system back after a major disaster like earthquakes or tsunamis , e.g. disaster recovery plan, hot/cold/warm sites, backup power, eg. Speeding(have fines and punishment, and preventive controls like speed bumps, detection – security cameras)



Administrative controls

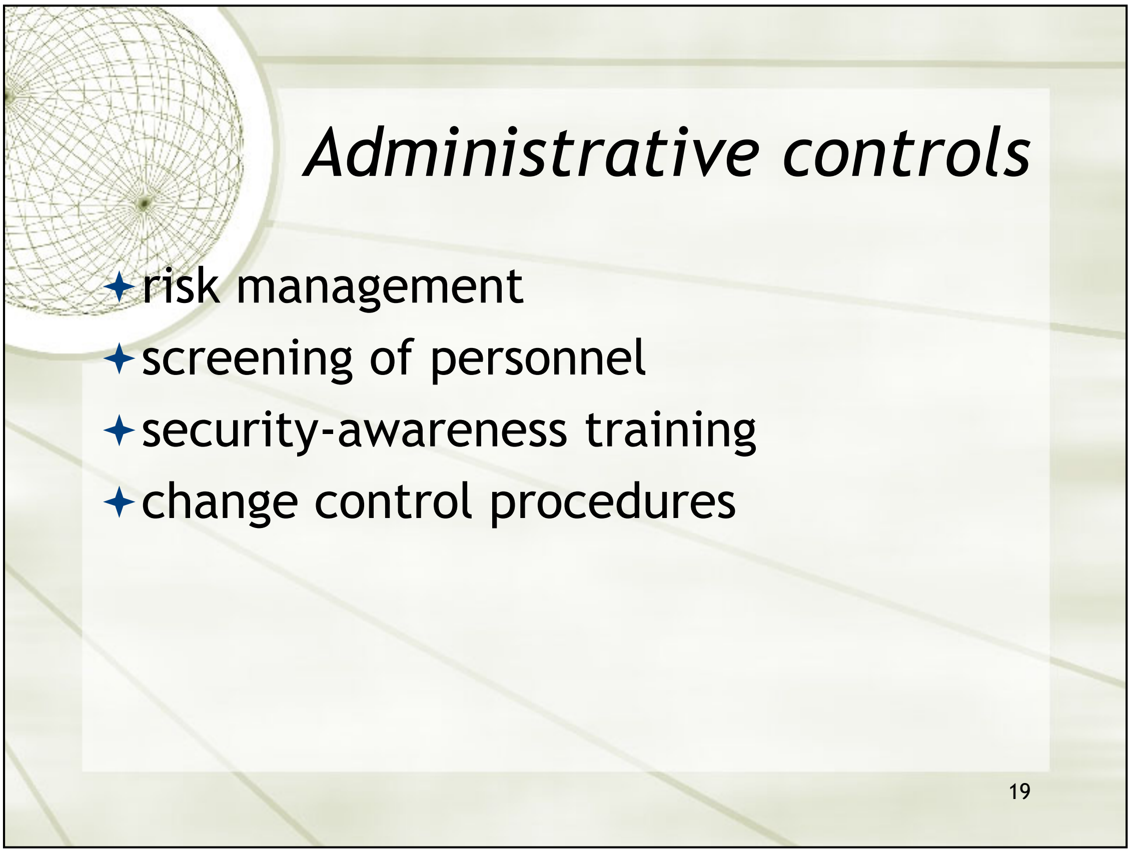
- developing and publishing of:
  - policies,
  - standards,
  - procedures,
  - guidelines.

18

According to the Government Accountability Office (GAO), "The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, and competence of the entity's people; management's philosophy and operating style; and the way management assigns authority and organizes and develops its people.“

From this we can derive that some controls are the actions that people take, we call these administrative controls. Administrative controls are the process of developing and ensuring compliance with policy and procedures. They tend to be things that employees may do, or must always do, or cannot do.

http://www.sans.edu/research/security-laboratory/article/security-controls



Administrative controls

- risk management
- screening of personnel
- security-awareness training
- change control procedures

Risk management

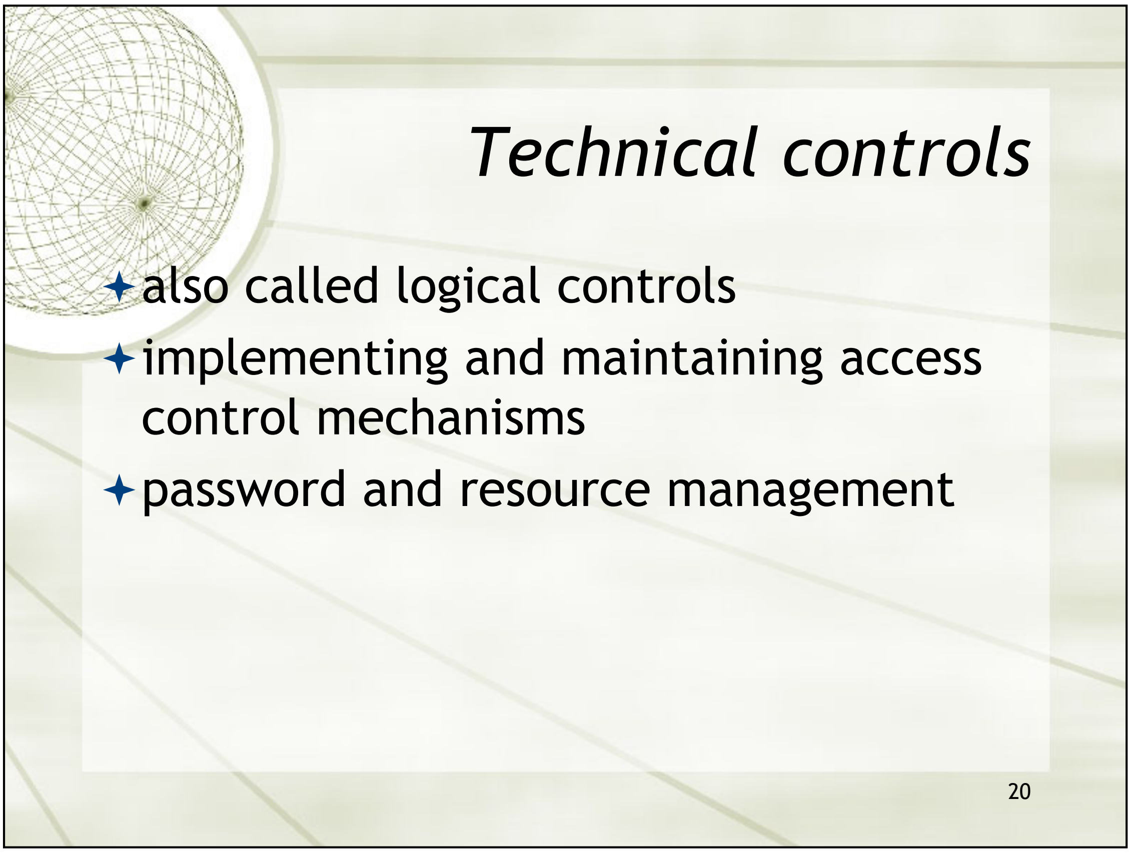
Evaluate the risks and try to address them

Screening of personnel

Do background checks on people before hiring them

Security-awareness training

Change control procedures



Technical controls

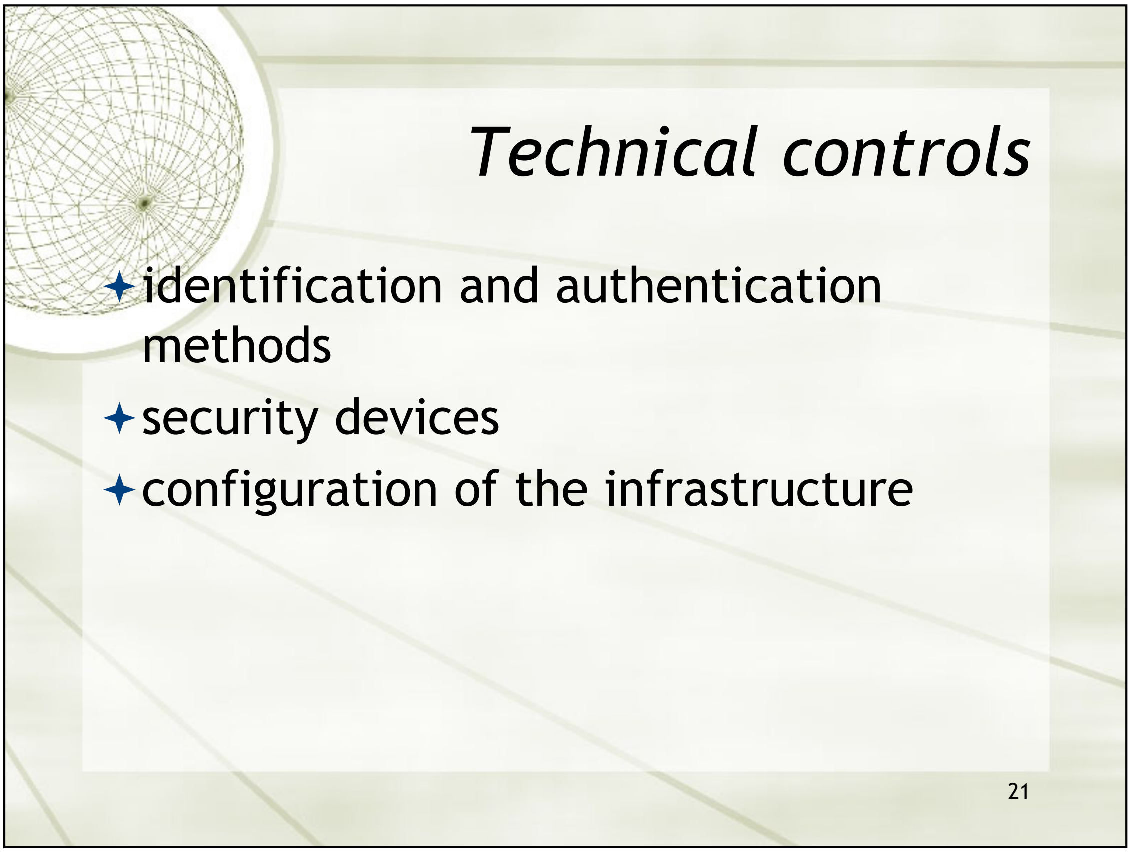
- also called logical controls
- implementing and maintaining access control mechanisms
- password and resource management

20

Another class of controls in security that are carried out or managed by computer systems, these are technical controls.

http://www.sans.edu/research/security-laboratory/article/security-controls

- also called logical controls
- implementing and maintaining access control mechanisms
- password and resource management



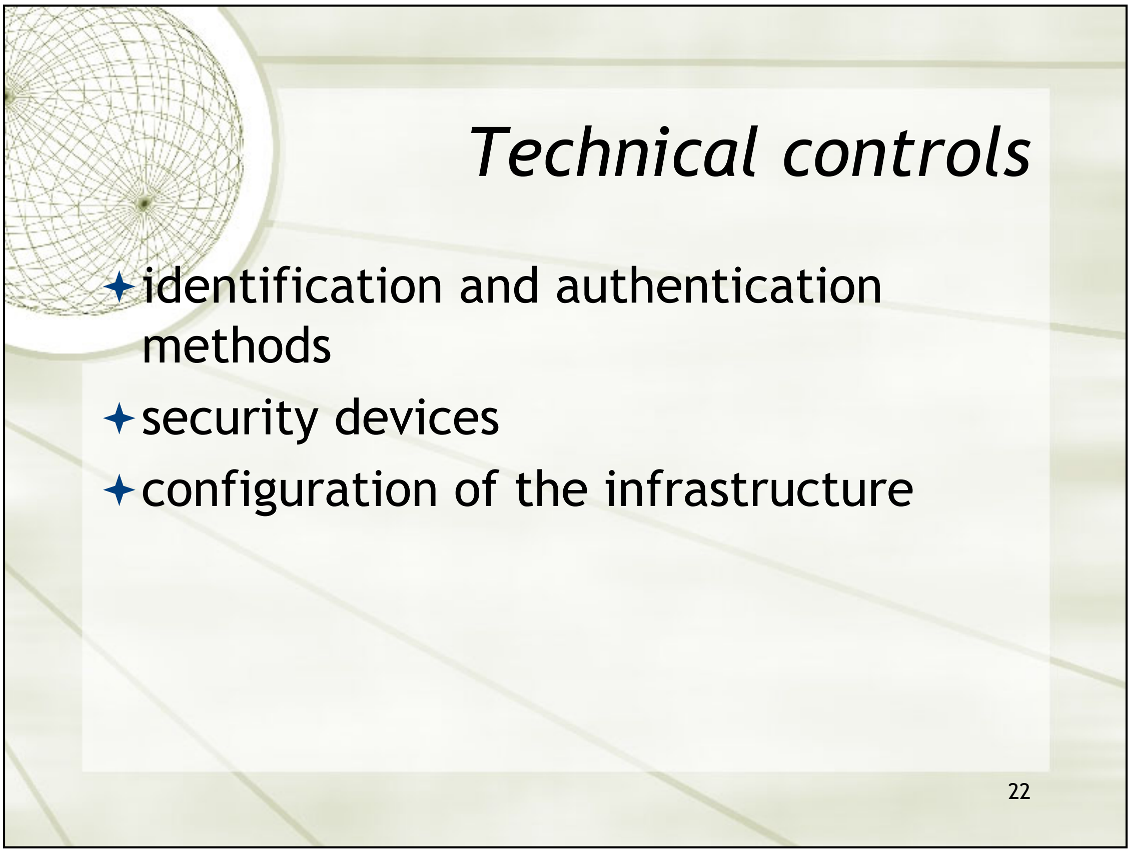
Technical controls

- identification and authentication methods
- security devices
- configuration of the infrastructure

- identification and authentication methods
- security devices

Firewalls, Anti-virus softwares

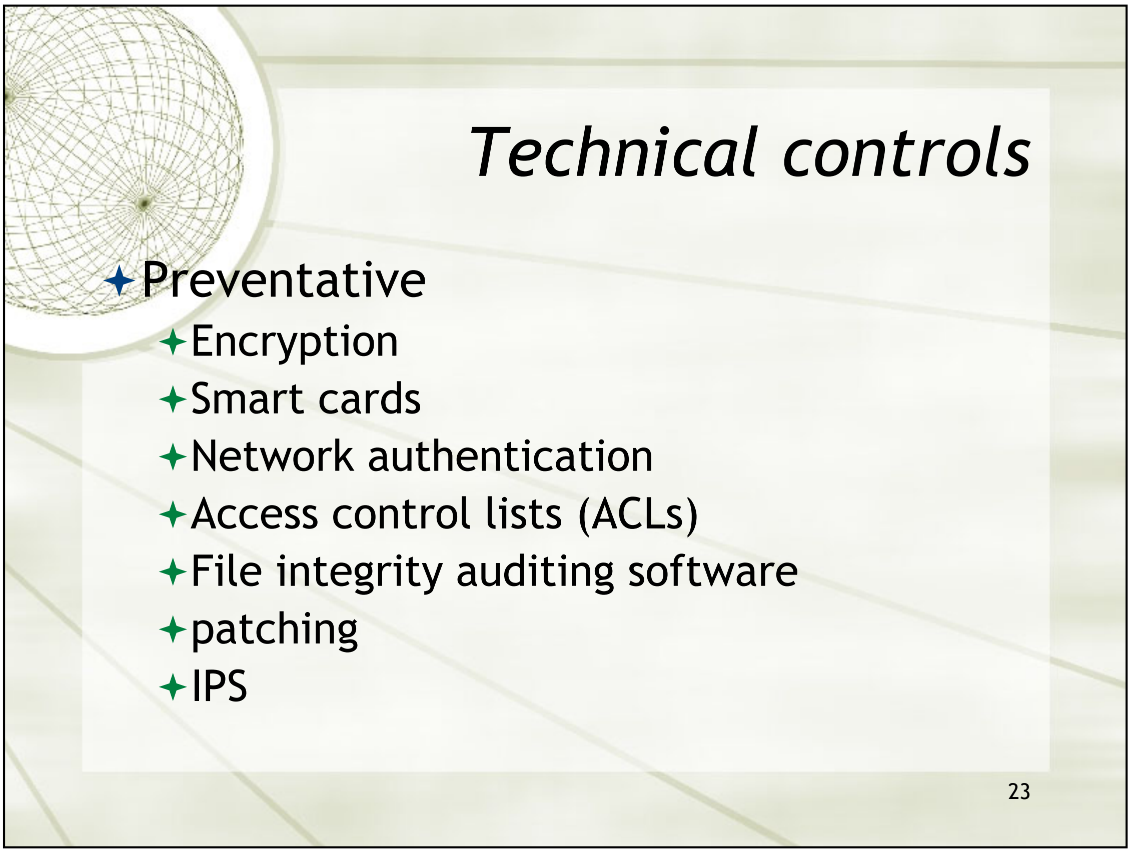
- configuration of the infrastructure in a security aware way



Technical controls

- identification and authentication methods
- security devices
- configuration of the infrastructure

22



Technical controls

- Preventative
  - Encryption
  - Smart cards
  - Network authentication
  - Access control lists (ACLs)
  - File integrity auditing software
  - patching
  - IPS

Encryption

- Authentication measures

Smart cards

Network authentication

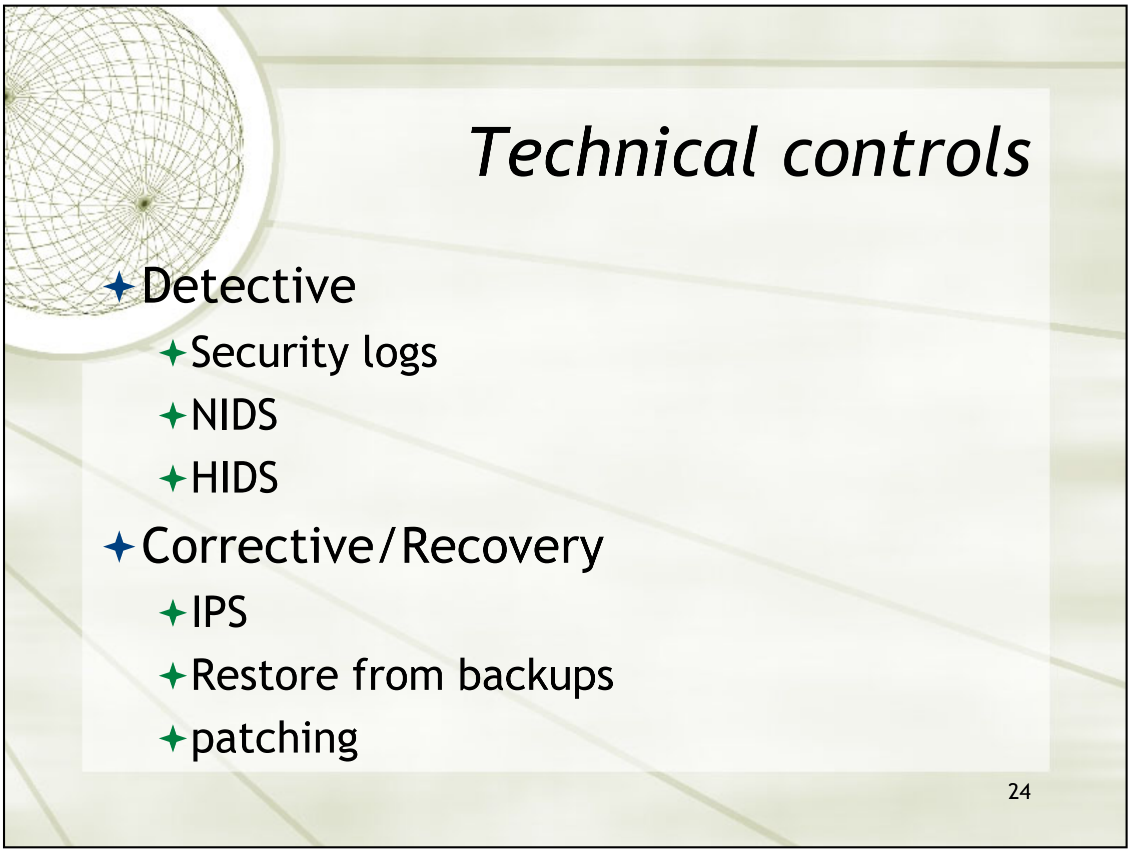
- Make sure to patch software on time
- Have intrusion detection and prevention systems

Access control lists (ACLs)

File integrity auditing software

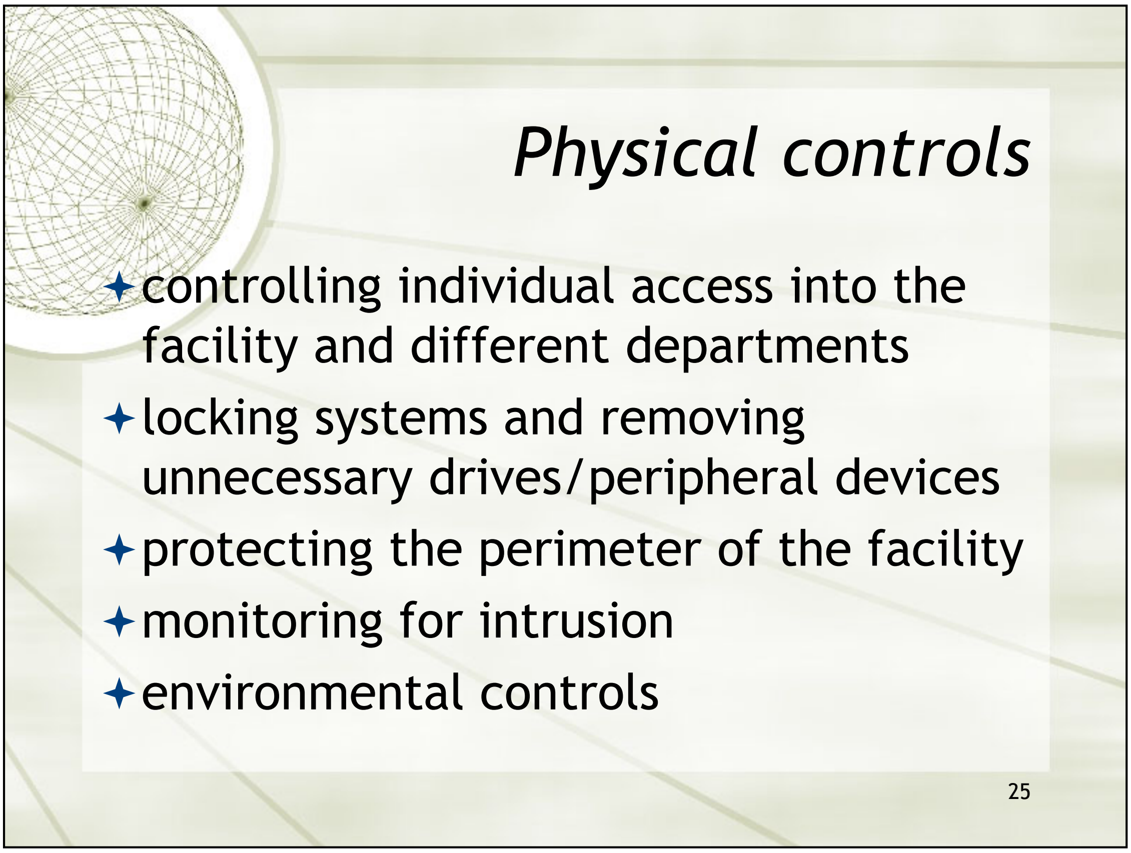
Patching

IPS



Technical controls

- Detective
  - Security logs
  - NIDS
  - HIDS
- Corrective/Recovery
  - IPS
  - Restore from backups
  - patching

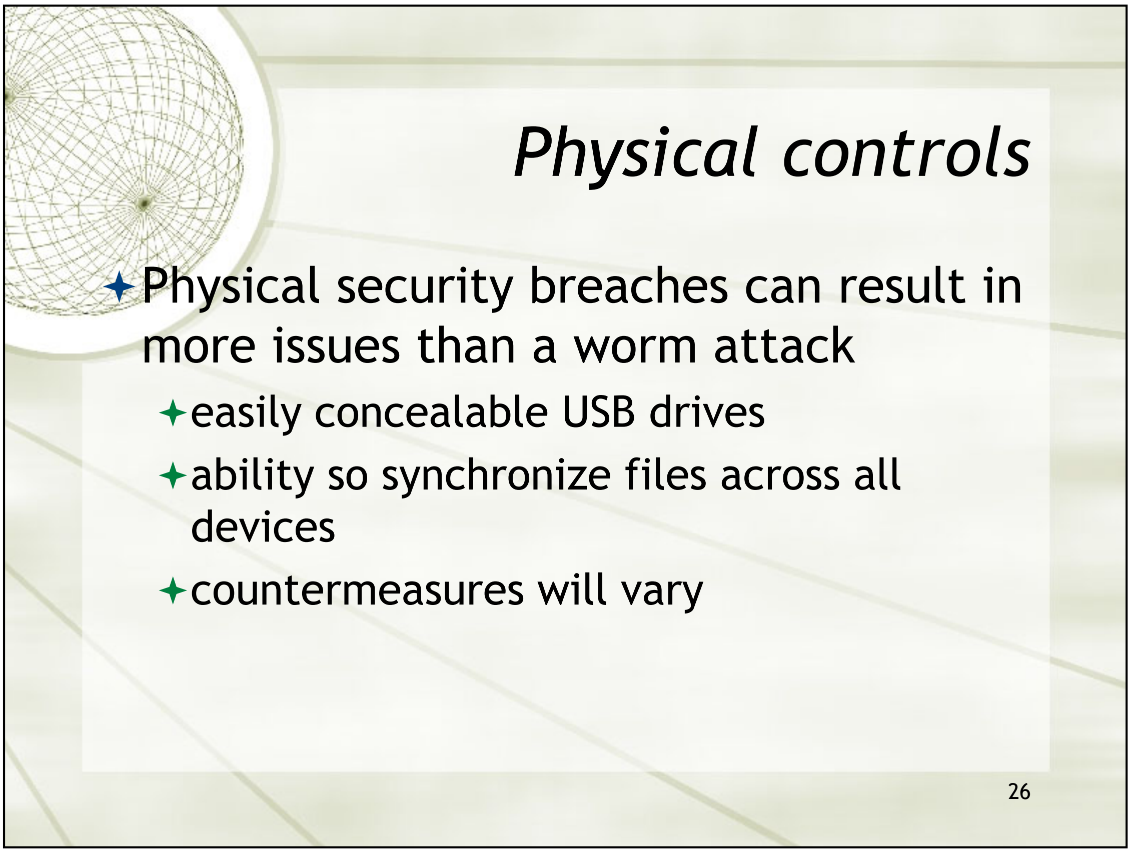


Physical controls

- controlling individual access into the facility and different departments
- locking systems and removing unnecessary drives/peripheral devices
- protecting the perimeter of the facility
- monitoring for intrusion
- environmental controls

25

Controlling the environment eg. Access to different buildings, removings hazards from our normal environment like fire or security hazards



Physical controls

- Physical security breaches can result in more issues than a worm attack
  - easily concealable USB drives
  - ability so synchronize files across all devices
  - countermeasures will vary

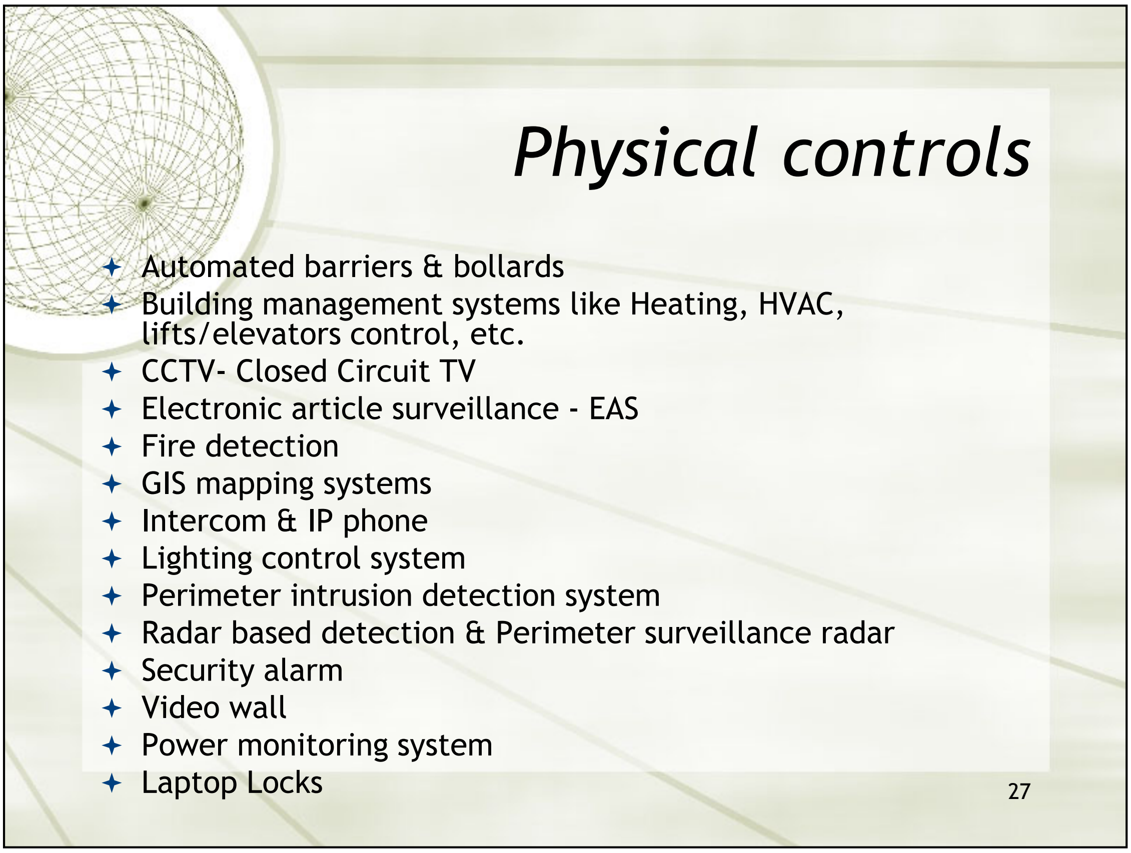
26

Physical security breaches can result in more issues for an organization than a worm attack. Loss of data, temporary loss of availability by shutting systems down, or longer term loss of availability by bomb or arson are all things to consider when implementing physical security. This is a survey article, for more in-depth information please consult the references, they are in the order they are used.

With the advent of easily concealable USB drives, or iPods for that matter, the issue of physical security is becoming more important than it was in the past. "Pod Slurping" is a significant threat to data. If you query a search engine for "steal data USB" you will find a number of approaches.

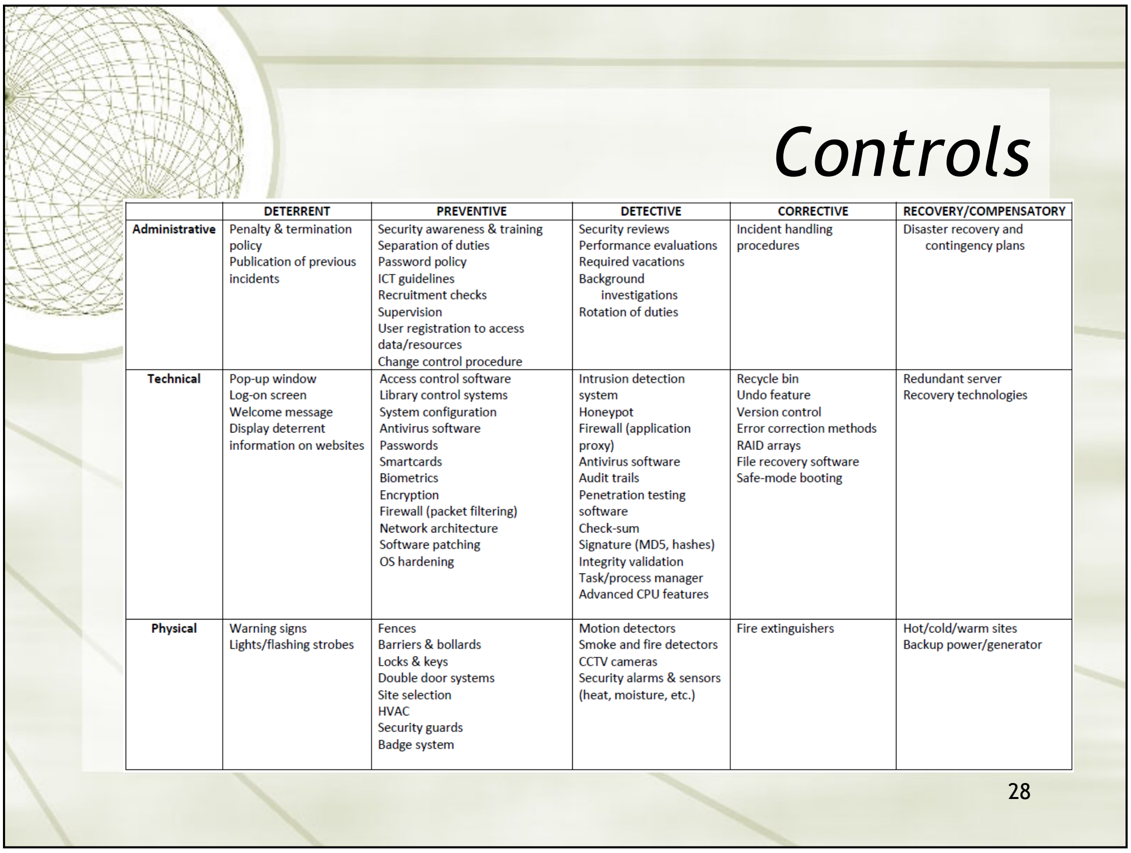
The protection of laptops and desktops is often overlooked; laptops in particular. According to Statistica, laptop usage compared to desktop has been increasing since 2010 and their 2019 projection is 121 million desktops compared to 170.4 million laptops. They also project tablet use to continue to decrease after the tablets will replace PCs hysteria of 2013 when more tablets were sold than laptops. Not only are these mobile devices subject to theft, but Android, Windows and Mac also have the ability so synchronize files across all devices: PC, laptop, tablet, smartphone. If one of them is lost, it is a potential portal into all of them.

Depending on the organization physical security countermeasures will vary. A government agency such as the Department of Defense may have armed guards at the door of the building. Many organizations are not in the position of breaching national security so armed guards are not a necessity. In many cases a receptionist greets any new visitors and makes the appropriate arrangements for an on-site visit. Let's review some physical security countermeasures for the server room, as well as laptops and desktops.



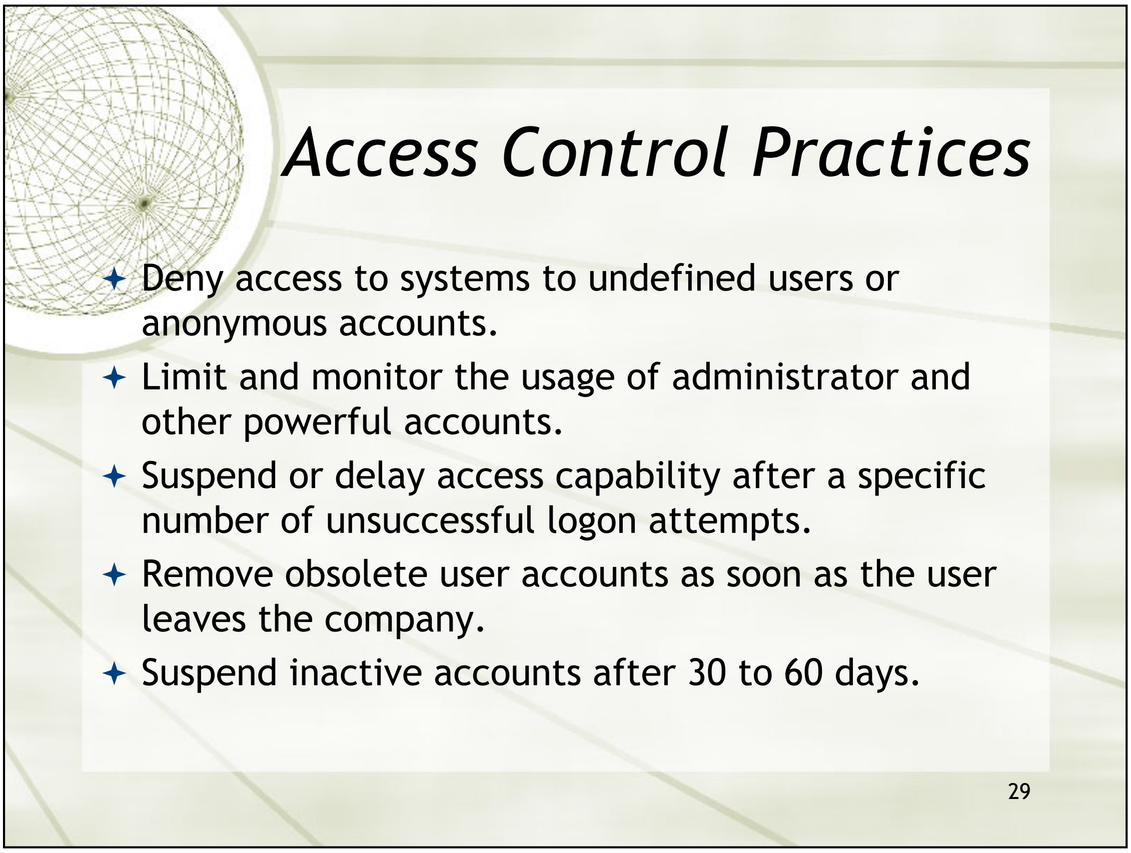
Physical controls

- Automated barriers & bollards
- Building management systems like Heating, HVAC, lifts/elevators control, etc.
- CCTV- Closed Circuit TV
- Electronic article surveillance - EAS
- Fire detection
- GIS mapping systems
- Intercom & IP phone
- Lighting control system
- Perimeter intrusion detection system
- Radar based detection & Perimeter surveillance radar
- Security alarm
- Video wall
- Power monitoring system
- Laptop Locks



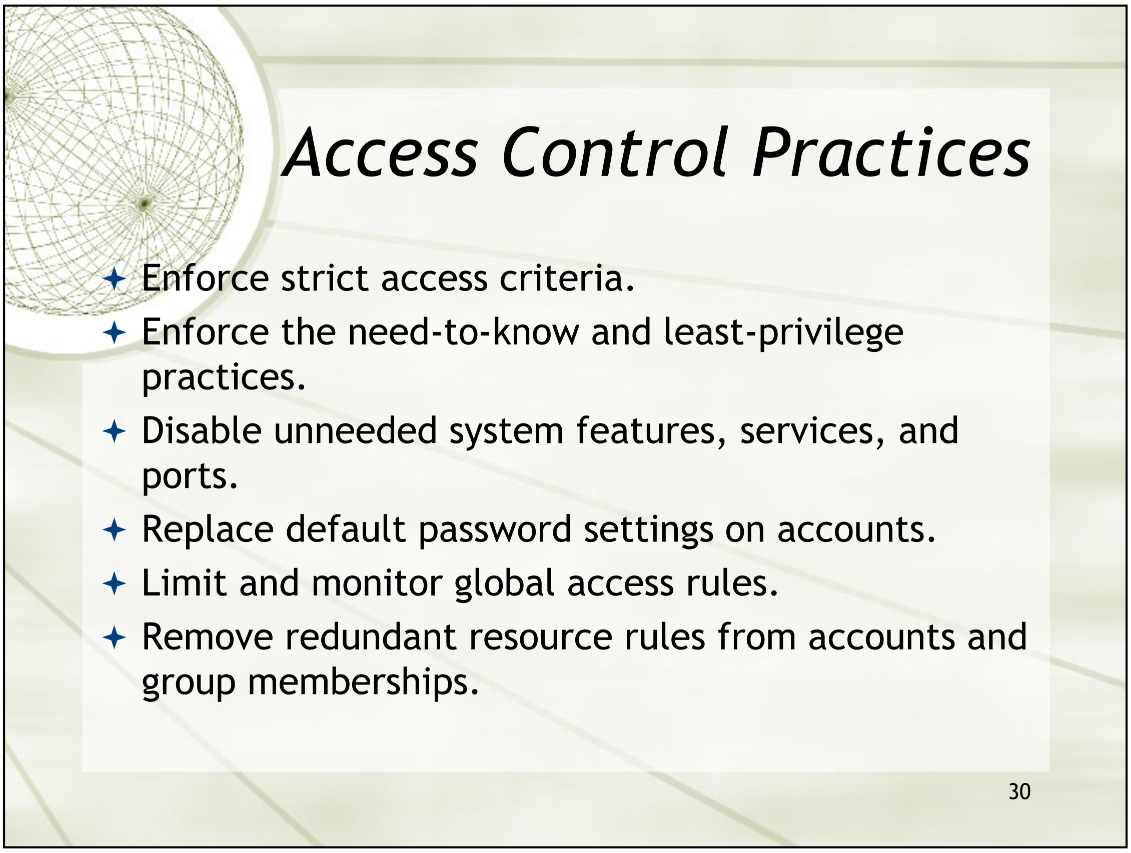
Controls

	DETERRENT	PREVENTIVE	DETECTIVE	CORRECTIVE	RECOVERY/COMPENSATORY
Administrative	Penalty & termination policy Publication of previous incidents	Security awareness & training Separation of duties Password policy ICT guidelines Recruitment checks Supervision User registration to access data/resources Change control procedure	Security reviews Performance evaluations Required vacations Background investigations Rotation of duties	Incident handling procedures	Disaster recovery and contingency plans
Technical	Pop-up window Log-on screen Welcome message Display deterrent information on websites	Access control software Library control systems System configuration Antivirus software Passwords Smartcards Biometrics Encryption Firewall (packet filtering) Network architecture Software patching OS hardening	Intrusion detection system Honeypot Firewall (application proxy) Antivirus software Audit trails Penetration testing software Check-sum Signature (MD5, hashes) Integrity validation Task/process manager Advanced CPU features	Recycle bin Undo feature Version control Error correction methods RAID arrays File recovery software Safe-mode booting	Redundant server Recovery technologies
Physical	Warning signs Lights/flashing strobes	Fences Barriers & bollards Locks & keys Double door systems Site selection HVAC Security guards Badge system	Motion detectors Smoke and fire detectors CCTV cameras Security alarms & sensors (heat, moisture, etc.)	Fire extinguishers	Hot/cold/warm sites Backup power/generator



Access Control Practices

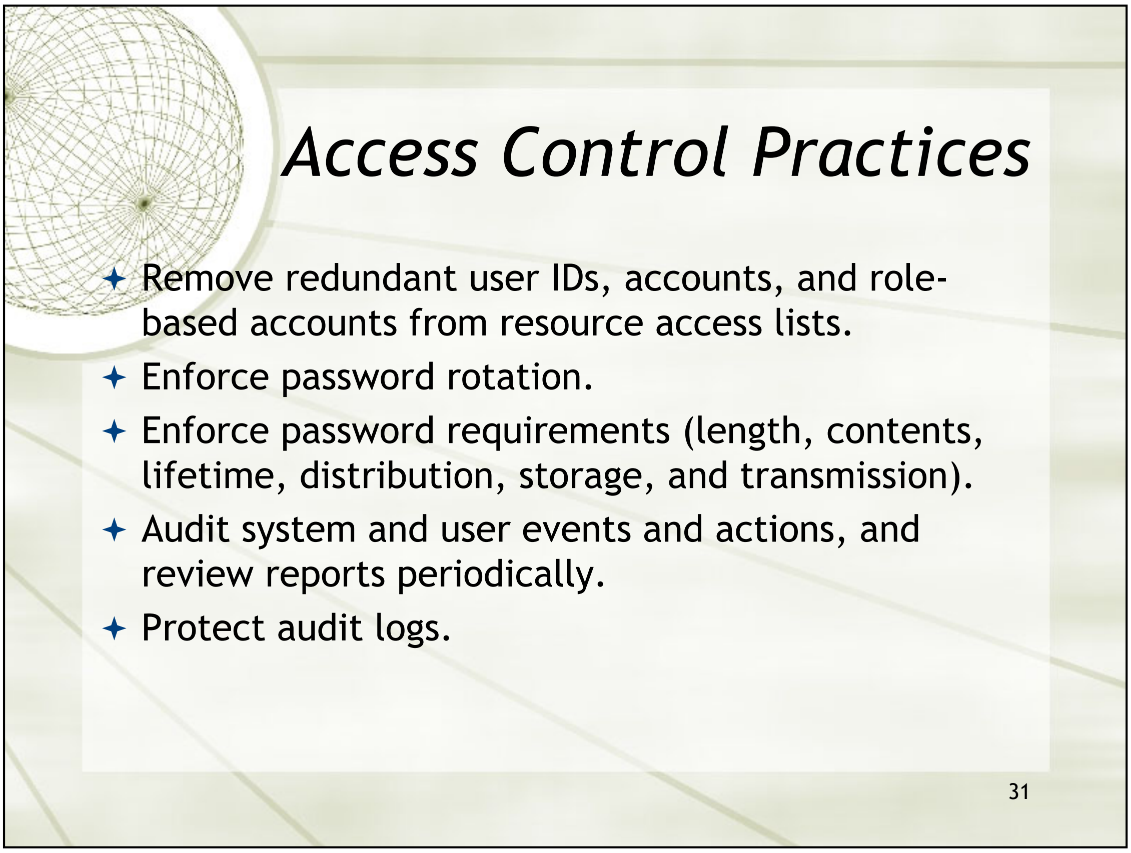
- Deny access to systems to undefined users or anonymous accounts.
- Limit and monitor the usage of administrator and other powerful accounts.
- Suspend or delay access capability after a specific number of unsuccessful logon attempts.
- Remove obsolete user accounts as soon as the user leaves the company.
- Suspend inactive accounts after 30 to 60 days.



Access Control Practices

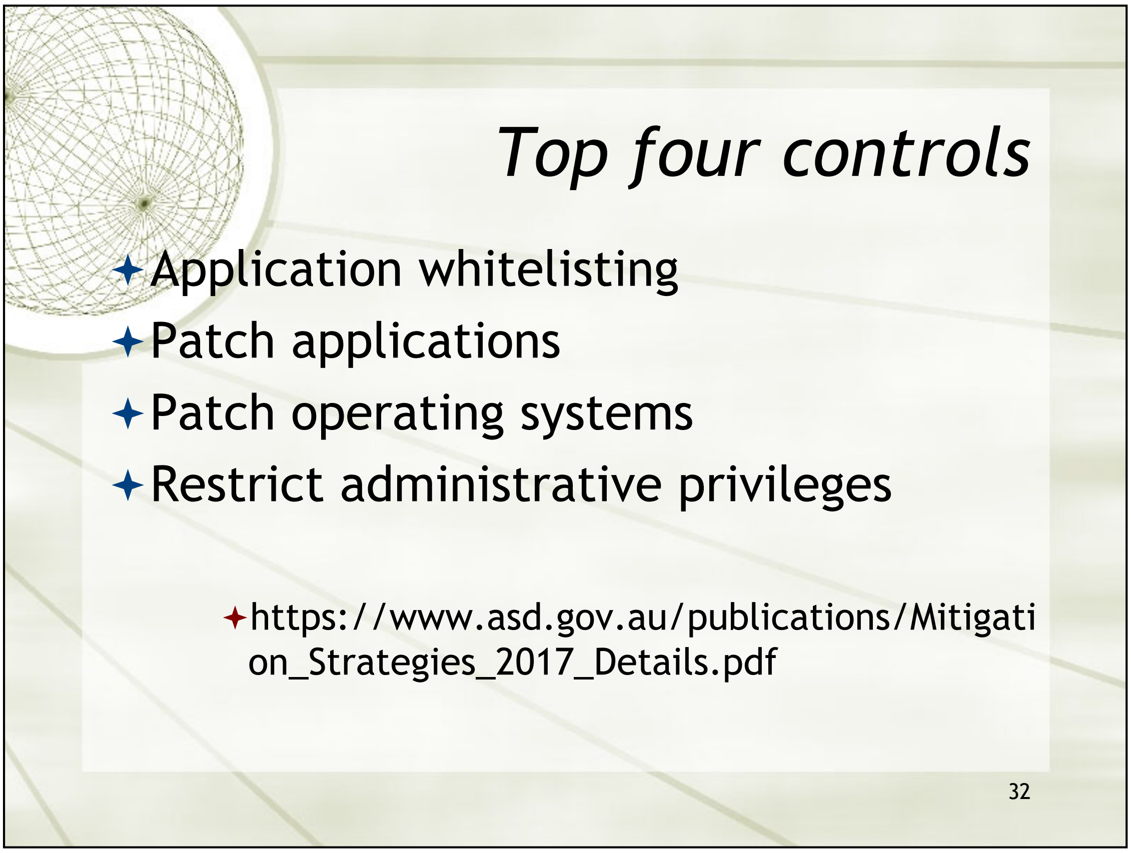
- Enforce strict access criteria.
- Enforce the need-to-know and least-privilege practices.
- Disable unneeded system features, services, and ports.
- Replace default password settings on accounts.
- Limit and monitor global access rules.
- Remove redundant resource rules from accounts and group memberships.

30



Access Control Practices

- Remove redundant user IDs, accounts, and role-based accounts from resource access lists.
- Enforce password rotation.
- Enforce password requirements (length, contents, lifetime, distribution, storage, and transmission).
- Audit system and user events and actions, and review reports periodically.
- Protect audit logs.



Top four controls

- Application whitelisting
- Patch applications
- Patch operating systems
- Restrict administrative privileges
  - https://www.asd.gov.au/publications/Mitigation_Strategies_2017_Details.pdf

32

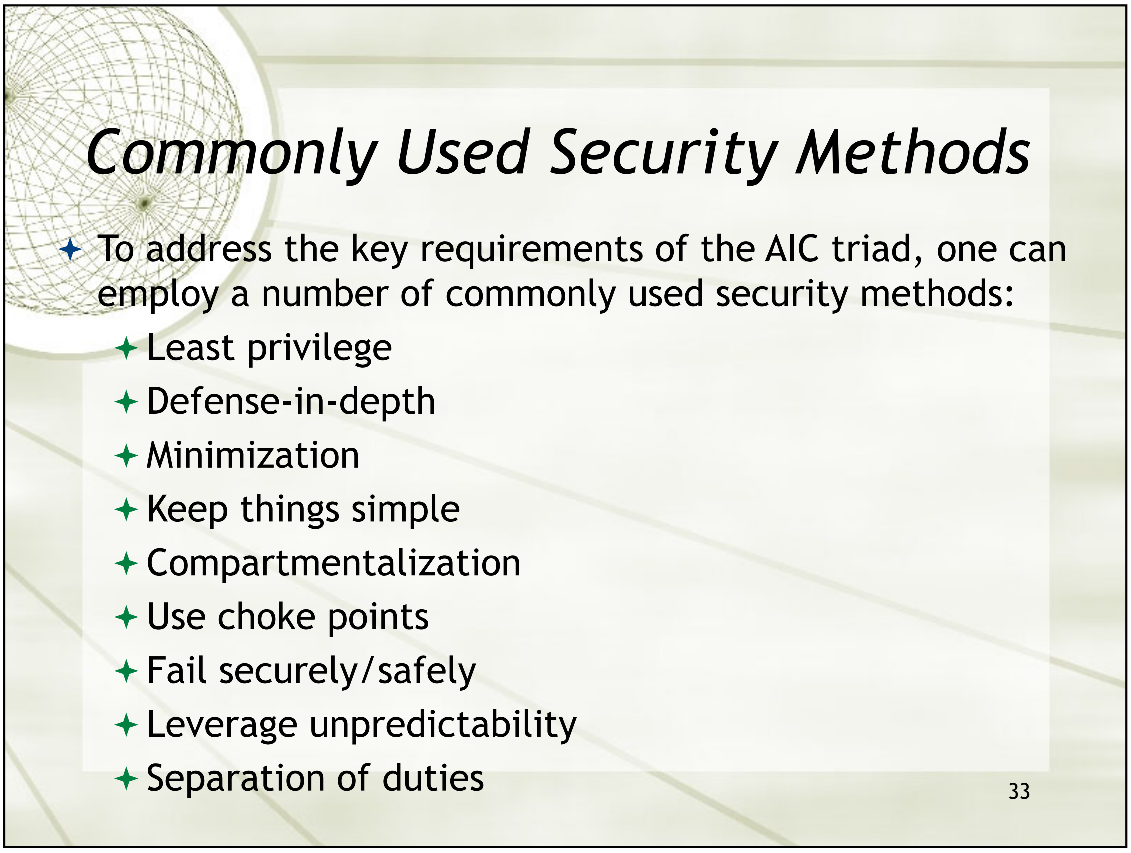
Application whitelisting of permitted/trusted programs, to prevent execution of malicious or unapproved programs including .DLL files, scripts and installers. (more work compared to blacklisting)

Patch applications e.g. Java, PDF viewer, Flash, web browsers and Microsoft Office. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest version of applications.

Patch operating system vulnerabilities. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest suitable operating system version. Avoid Microsoft Windows XP.

Essential

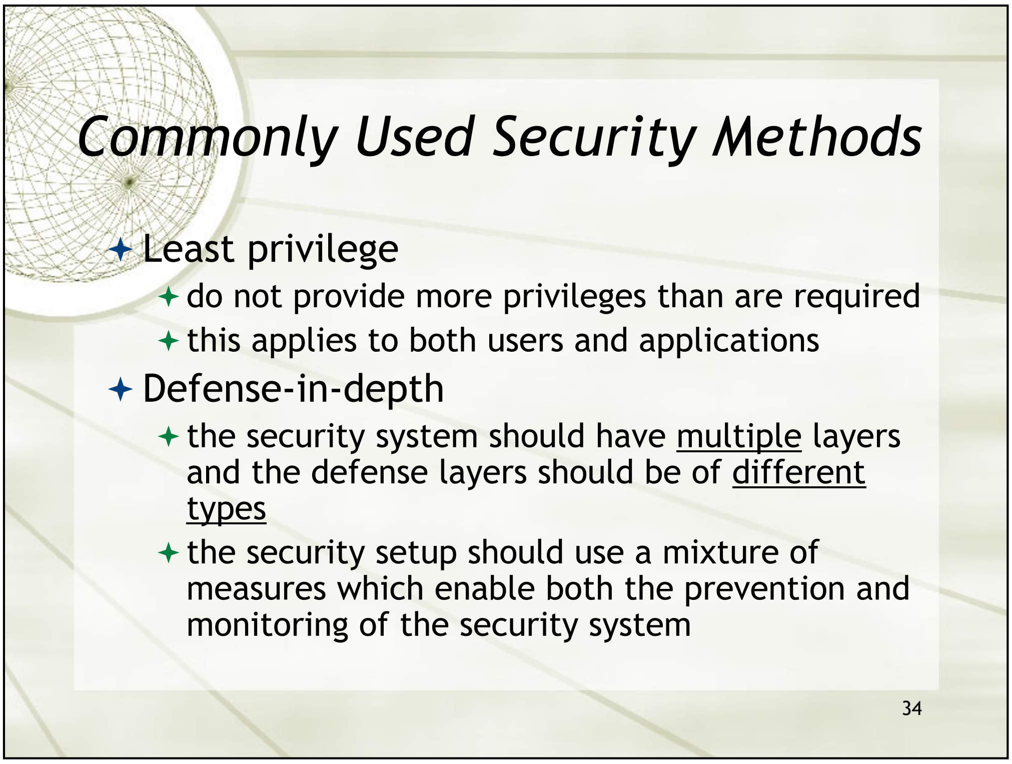
Restrict administrative privileges to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing.



Commonly Used Security Methods

- To address the key requirements of the AIC triad, one can employ a number of commonly used security methods:
  - Least privilege
  - Defense-in-depth
  - Minimization
  - Keep things simple
  - Compartmentalization
  - Use choke points
  - Fail securely/safely
  - Leverage unpredictability
  - Separation of duties

Now that we have covered the fundamental concepts of information security, let’s consider some of the universal security principles/methods, such as principles of least privilege, minimization, and compartmentalization. They are known as control methodologies – different ways to apply controls.



Commonly Used Security Methods

- Least privilege
  - do not provide more privileges than are required
  - this applies to both users and applications
- Defense-in-depth
  - the security system should have multiple layers and the defense layers should be of different types
  - the security setup should use a mixture of measures which enable both the prevention and monitoring of the security system

Least Privilege

The principle of least privilege stipulates, “Do not give any more privileges than absolutely necessary to do the required job.” (No administrative rigts to guests accounts, unidentified applications should not be able to have the power to change the system file etc.) This principle applies not only to privileges of users and applications on a computer system, but also to other noninformation systems privileges of an organization’s staff. The principle of least privilege is a preventive control, because it reduces the number of privileges that may be potentially abused and therefore limits the potential damage. Like most good principles, the principle of least privilege is applicable in all information systems environments. Some examples of application of this principle include the following:

■ Giving users only read access to shared files if that’s what they need, and making sure write access is disabled

■ Not allowing help desk staff to create or delete user accounts if all that they may have to do is to reset a password

■ Not allowing software developers to move software from development servers to production servers

Privilege : The ability to access data to run processes and applications

Product: keep system more stable by giving less privilege to untrustworthy users

Defense in Depth (multiple types of security controls in different layers)

The principle of defense in depth is about having more than one layer or type of defense. The reasoning behind this principle is that any one layer or type of defense may be breached, no matter how strong and reliable you think it is, but two or more layers are much more difficult to breach. Defense in depth works best when you combine two or more different types of defense mechanisms—such as using a firewall between the Internet and your LAN, plus the IP Security Architecture (IPSEC) to encrypt all sensitive traffic on the LAN. In this scenario, even if your firewall is compromised, the attackers still have to break IP Security to get to your data flowing across the LAN.

Eg.

1st layer – Deterrent control (easy to implement, use it to warn hackers to not attack, breaching policies may not be legal)

2nd layer – Preventive control (Firewall installed on server that monitors all the traffic gg btw the internet and internal network and intercept any suspicious activities)

3rd layer – Detective layer (Network monitoring tools like intrusion detection systems that will alert ppl on any attacks being made on the system)

4th layer – Corrective layer (software installed like antivirus that could get rid of virus that the computer has been infected)

5th layer – Recovery layer (Data backup, another image of the system software for recovery in the event that the system breaks)

Generally, different types of controls should be used together: first, preventive controls should be in place to try and prevent security incidents from happening at all; second, detective controls are necessary so that you can know whether preventive controls are working or have failed; and third, corrective controls are needed to help you respond effectively to security incidents and contain damage. However, the defense in depth principle does not mean that you should indiscriminately apply all the controls and security measures you can get your hands on: balance has to be found between security provided by the defense in depth approach and the financial, human, and organizational resources you are willing to expend following it. This balance is addressed by the cost-benefit analysis.

How is file access protection provided in a layered approach?

If an administrator puts all users in specific groups and dictates what those groups can and cannot do with the company's files, this is only one layer in the approach.

To properly protect file access, the administrator must do the following:

1) Configure application, file, and Registry access control lists (ACLs) to provide more granularity to users and groups's file permissions.

2) Configure the system default user rights (in a Windows environment) to give certain types of users certain types of rights.

3) Consider the physical security of the environment and the computers, and apply restraints where required.

4) Place users into groups that have implicit permissions necessary to perform their duties and no more.

5) Draft and enforce a strict logon credential policy so that not all users are logging on as the same user.

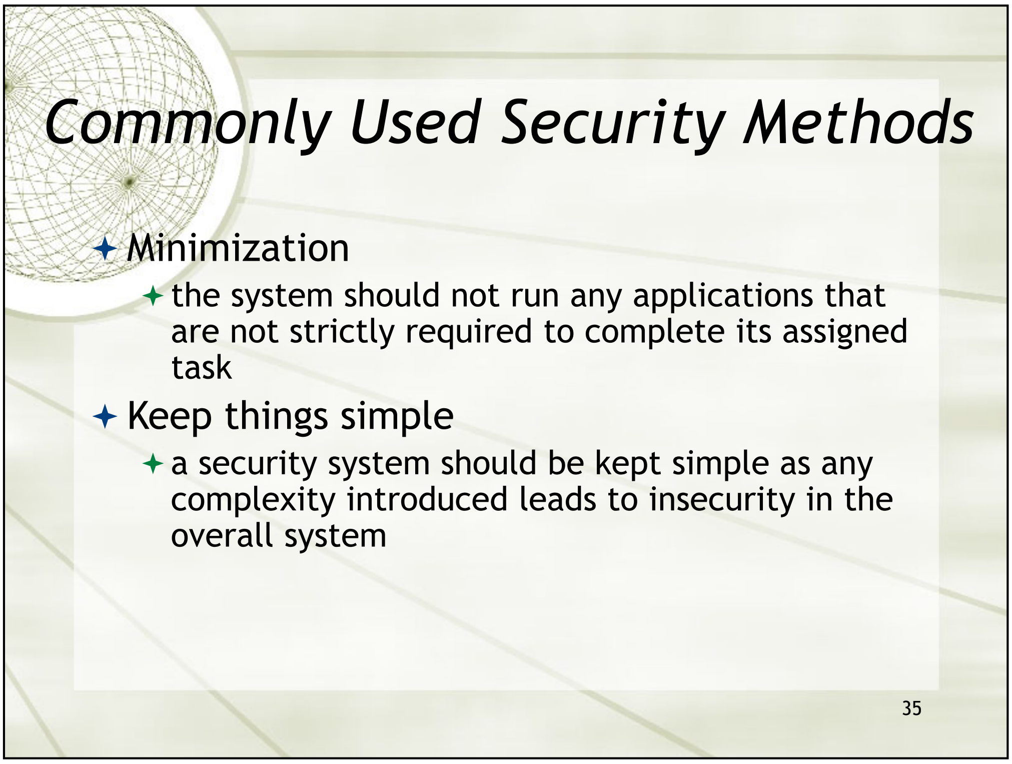
6) Implement monitoring and auditing of file access and actions to identify any suspicious activity.

Sound like overkill? It really isn't. If an administrator makes all users log in using different accounts, applies file and Registry ACLs, configures groups, and monitors audit logs but

does not consider physical security, a user could use a USB drive with a simple program to get around all other security barriers. All of these components must work in a synergistic manner to provide a blanket of security that individual security mechanisms could not fulfill on their own.

A network that has a firewall with packet filtering, a proxy server with content filtering, its public and private DNS records clearly separated, SSL for Internet users, IPSec for VPN connections, and public key infrastructure (PKI), as well as restricted service and port configuration, may seem like a fortified environment, and a network administrator most likely implemented these mechanisms with the best intentions. However, one problem is that it is fortified only for a moment in time.

Without a scanning device that probes the environment on a scheduled basis or an IDS that looks out for suspicious activity, the environment could be vulnerable even after the company has spent thousands of dollars to protect it. Technology and business drivers continually change, and so do networks and environments. When you configure a new application, apply a patch, or install a device, the change to the environment could have unpredictable con- sequences (not to mention the new ways hackers have found to circumvent the original security mechanisms).



Commonly Used Security Methods

- Minimization
  - the system should not run any applications that are not strictly required to complete its assigned task
- Keep things simple
  - a security system should be kept simple as any complexity introduced leads to insecurity in the overall system

35

Minimization

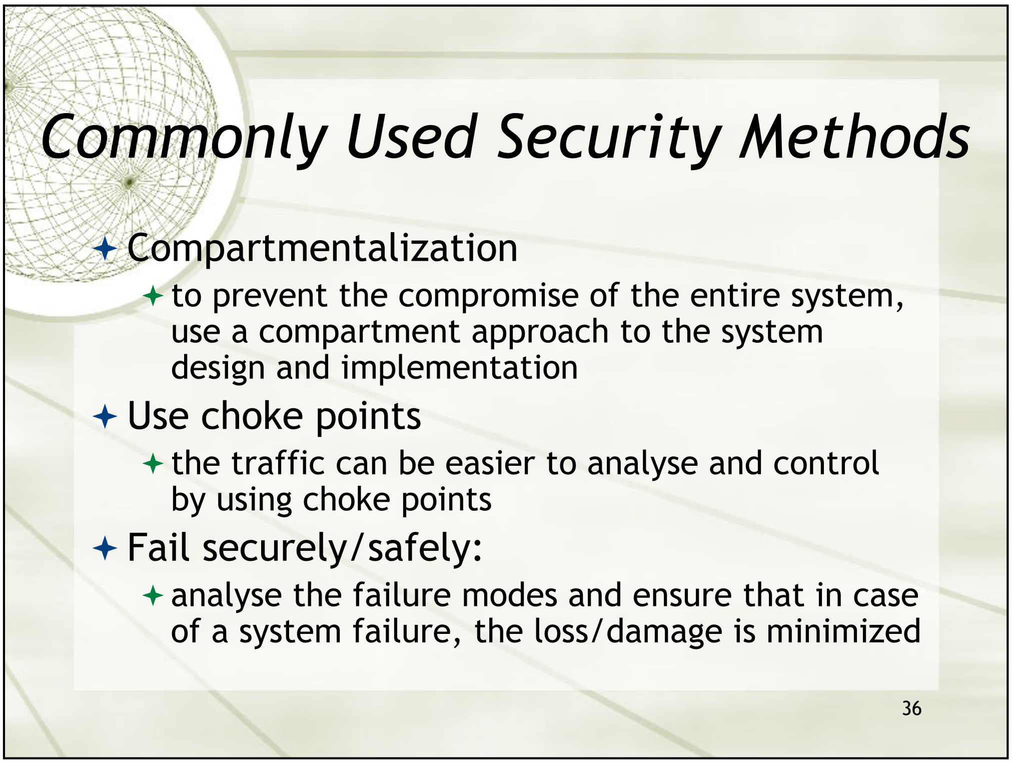
The minimization principle is the cousin of the least privilege principle and mostly applies to system configuration. The minimization principle says “do not run any software, applications, or services that are not strictly required to do the entrusted job.” To illustrate, a computer whose only function is to serve as an e-mail server should have only e-mail server software installed and enabled. All other services and protocols should either be disabled or not installed at all to eliminate any possibility of compromise or misuse. Adherence to the minimization principle not only increases security but usually also improves performance, saves storage space, and is a good system administration practice in general.

Cost-Benefit Analysis

Although not strictly a principle, the cost-benefit analysis is a must when considering implementation of any security measure. It says that the overall benefits received from a particular security control or mechanism should clearly exceed its total costs; otherwise, implementing it would make no sense. Cost-benefit analysis directly affects return on investment (ROI). This may sound like simple common sense, and it probably is; nevertheless, this is an important and often overlooked concern. When doing cost-benefit analysis, one should consider all costs and all benefits over a period of time, for example from one to five years, to have a complete picture.

Keep Things Simple

Complexity is the worst enemy of security. Complex systems are inherently more insecure because they are difficult to design, implement, test, and secure. The more complex a system, the less assurance we may have that it will function as expected. Although complexity of information systems and processes is bound to increase with our increasing expectations of functionality, we should be very careful to draw a line between avoidable and unavoidable complexity and not sacrifice security for bells and whistles, only to regret it later. When you have to choose between a complex system that does much and a simple system that does a bit less but enough, choose the simple one.



Commonly Used Security Methods

- Compartmentalization
  - to prevent the compromise of the entire system, use a compartment approach to the system design and implementation
- Use choke points
  - the traffic can be easier to analyse and control by using choke points
- Fail securely/safely:
  - analyse the failure modes and ensure that in case of a system failure, the loss/damage is minimized

36

Compartmentalization

Compartmentalization, or the use of compartments (also known as zones, jails, sandboxes, and virtual areas), is a principle that limits the damage and protects other compartments when software in one compartment is malfunctioning or compromised. It can be best compared to compartments on ships and submarines, where a disaster in one compartment does not necessarily mean that the entire ship or submarine is lost. Compartmentalization in the information security context means that applications run in different compartments are isolated from each other. In such a setup, the compromise of web server software, for example, does not take down or affect e-mail server software running on the same system but in a separate compartment. Zones in Solaris 10 implement the compartmentalization principle and are powerful security mechanisms.

Use Choke Points

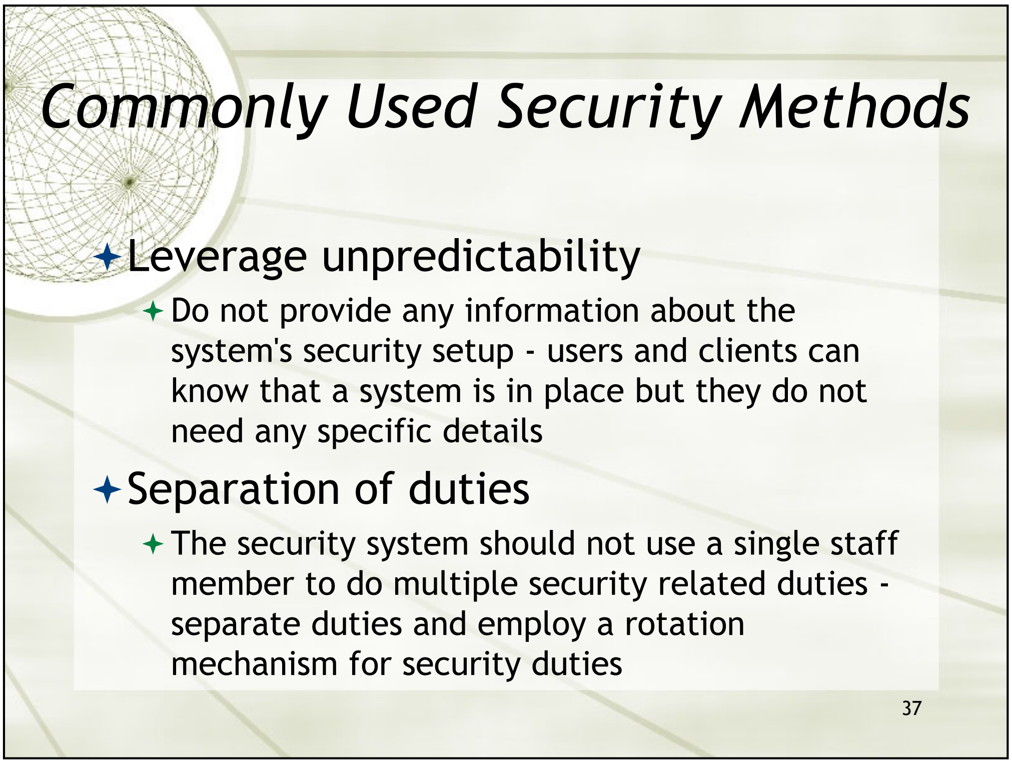
Security is very much about control, and control is so much more effective and efficient when you know all ways in and out of your systems or networks. Choke points are logical “narrow channels” that can be easily monitored and controlled. An example of a choke point is a firewall—unless traffic can travel only via the firewall, the firewall's utility is reduced to zero. Consider the example of controlled entrances to buildings or facilities of high importance, such as perimeter fencing and guard posts.

Fail Securely

Although fail securely may sound like an oxymoron, it isn't. Failing securely means that if a security measure or control has failed for whatever reason, the system is not rendered to an insecure state. For example, when a firewall fails, it should default to a "deny all" rule, not a "permit all." However, fail securely does not mean "close everything" in all cases; if we are talking about a computer-controlled building access control system, for example, in case of a fire the system should default to "open doors" if humans are trapped in the building. In this case, human life takes priority over the risk of unauthorized access, which may be dealt with using some other form of control that does not endanger the lives of people during emergency situations.

Secure the Weakest Link

To people new to information security, many information security principles and approaches may sound like little more than common sense. Although that may well be the case, it doesn't help us much, because very often we still fail to act with common sense. The principle of securing the weakest link is one such case: look around and you will likely see a situation in which instead of securing the weakest link, whatever it may be, resources are spent on reinforcing already adequate defenses. For example, there are technological solutions already employed to protect the system but no training on how to handle attachments in email messages.



Commonly Used Security Methods

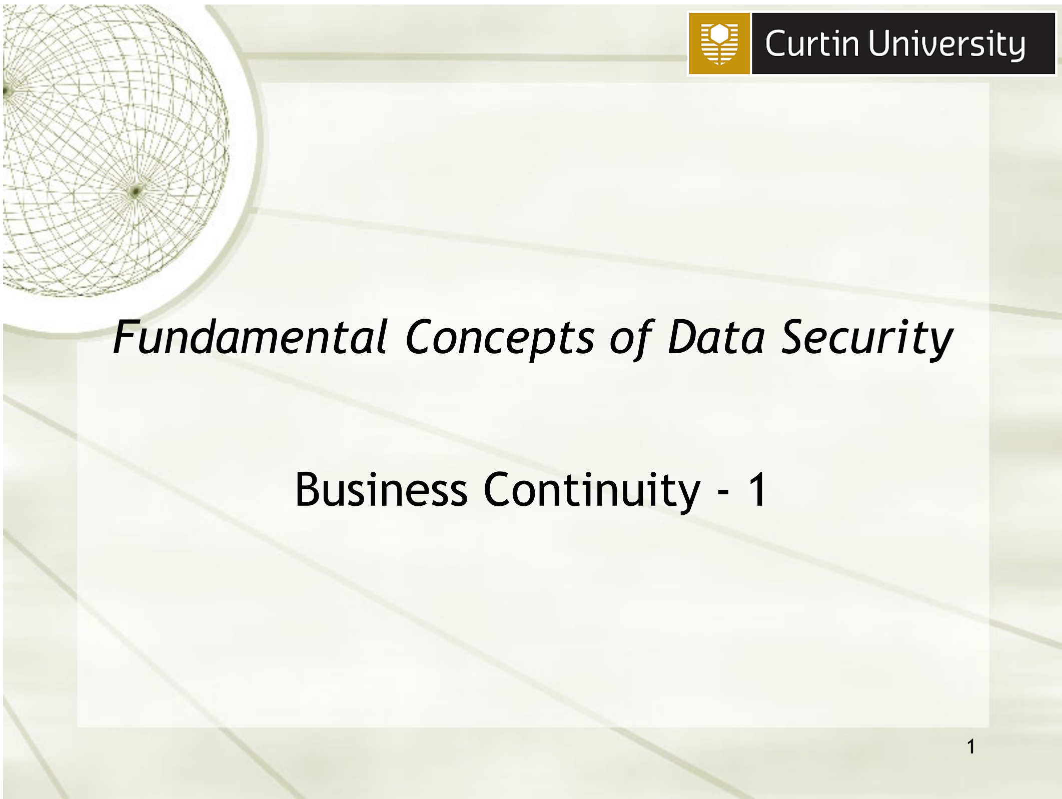
- Leverage unpredictability
  - Do not provide any information about the system's security setup - users and clients can know that a system is in place but they do not need any specific details
- Separation of duties
  - The security system should not use a single staff member to do multiple security related duties - separate duties and employ a rotation mechanism for security duties

Leverage Unpredictability

Remain unpredictablie.Just as states don't publicize the specifics of their armaments, exact locations, or numbers of armed forces, you should not publicize the details of your security measures and defenses. This principle should not be seen as contradicting deterrent security controls—controls that basically notify everyone that security mechanisms are in place and that violations will be resisted, detected, and acted upon. The important difference here is that deterrent controls don't provide details of the defenses but merely announce their existence so as to deter potential attackers without giving them detailed information that later may be used against the defenders. In practical terms, this means you can, for example, announce that you are using a firewall that, in particular, logs all traffic to and from your network, and these logs are reviewed by the organization—there is no need to disclose the type, vendor, or version number of the firewall; where it is located; how often logs are reviewed; and whether any backup firewalls or network intrusion detection systems are in place.

Segregation of Duties

The purpose of the segregation (or separation) of duties is to avoid the possibility of a single person being responsible for different functions within an organization, which when combined may result in a security violation that may go undetected. Segregation of duties can prevent or discourage security violations and should be practiced when possible. Although the actual job titles and organizational hierarchies may differ greatly, the idea behind the principle of separation of duties stays the same: no single person should be able to violate security and get away with it. Rotation of duties is a similar control that is intended to detect abuse of privileges or fraud and is a practice to help your organization avoid becoming overly dependent on a single member of the staff. By rotating staff, the organization has more chances of discovering violations or fraud.



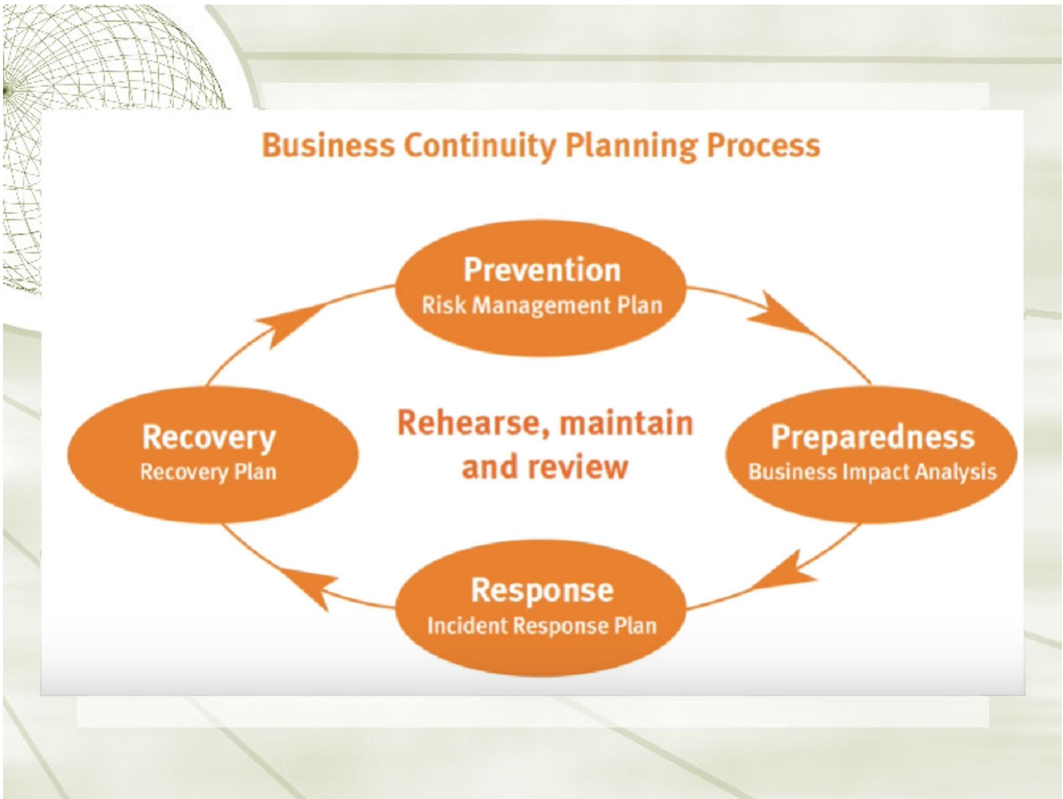
Curtin University

Fundamental Concepts of Data Security

Business Continuity - 1

Comprehensive approach to business continuity plan

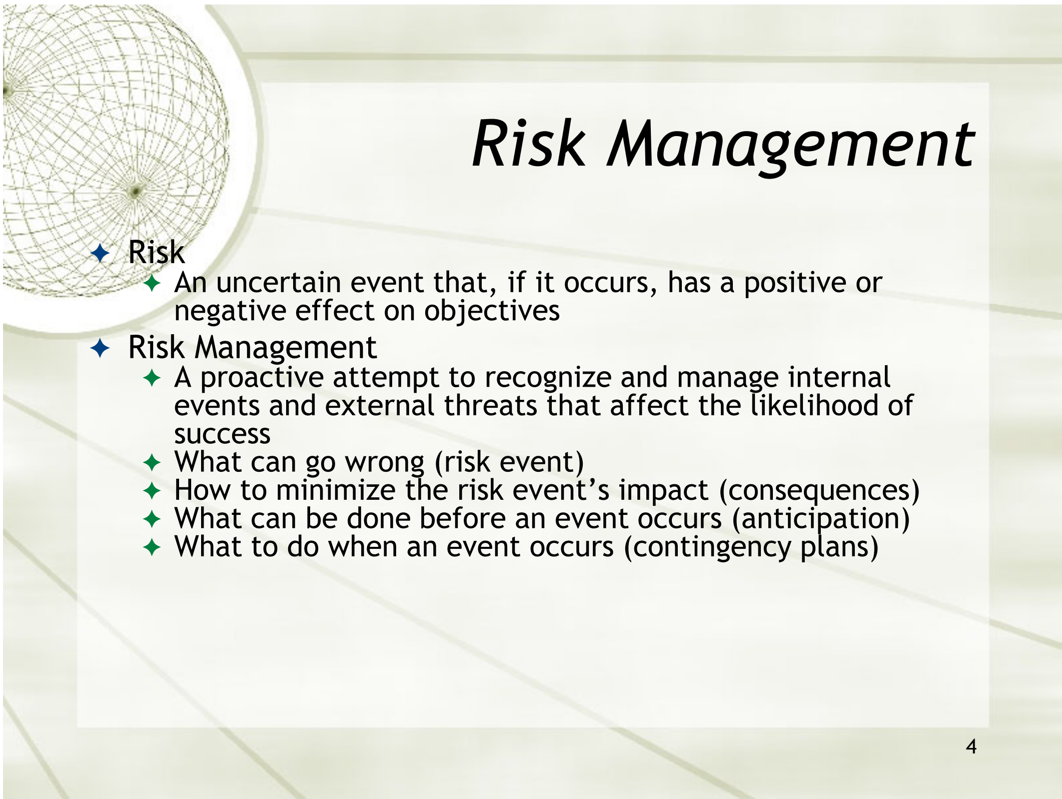
- Prevention: risk management plan (this lecture) – what to do to prevent incidents
- Preparedness: business impact analysis – if incidents do happen, what would be the impact
- Response: incident response plan – what to do when incidents happen
- Recovery: recovery plan – how to recover after an incident/disaster



Business Continuity Planning Process

Comprehensive approach to business continuity plan

- Prevention: risk management plan (this lecture) – what to do to prevent incidents
- Preparedness: business impact analysis – if incidents do happen, what would be the impact
- Response: incident response plan – what to do when incidents happen
- Recovery: recovery plan – how to recover after an incident/disaster



Risk Management

- Risk
  - An uncertain event that, if it occurs, has a positive or negative effect on objectives
- Risk Management
  - A proactive attempt to recognize and manage internal events and external threats that affect the likelihood of success
  - What can go wrong (risk event)
  - How to minimize the risk event's impact (consequences)
  - What can be done before an event occurs (anticipation)
  - What to do when an event occurs (contingency plans)

4

Risk management plan consists of three stages

I.Plan

I. Identify team
II. Identify scope
III. Identify method
IV. Identify tools
V. Understand acceptable risk level

II.Collect information/perform risk analysis

I. Identify assets
II. Assign value to assets
III. Identify vulnerabilities and threats
IV. Calculate risks
V. Cost/benefit analysis
VI. Uncertainty analysis

III.Define recommendations

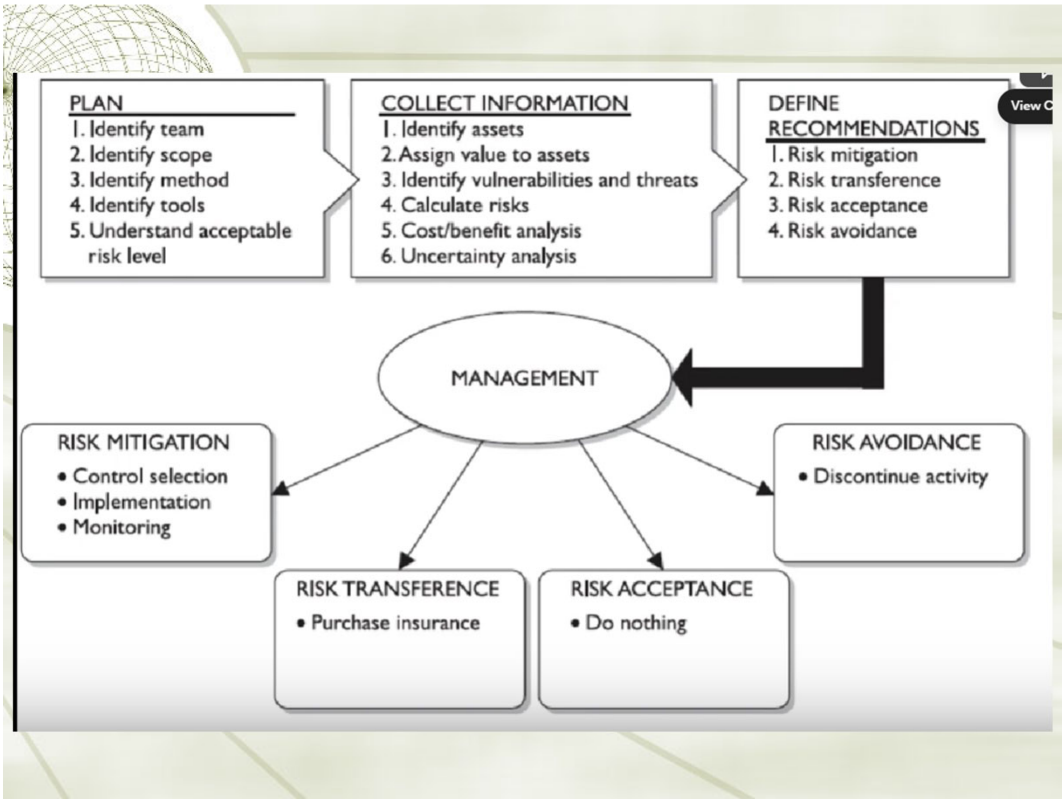
I. Defend the risk: lock the door, install IDS, block specific ports associated with specific attacks

II. Mitigate the risk: incident response, disaster recovery, and business continuity plans

III. Transfer the risk: outsource

IV. Avoid/terminate the risk: disable USB port

V. Accept the risk: do nothing



PLAN

1. Identify team
2. Identify scope
3. Identify method
4. Identify tools
5. Understand acceptable risk level

COLLECT INFORMATION

1. Identify assets
2. Assign value to assets
3. Identify vulnerabilities and threats
4. Calculate risks
5. Cost/benefit analysis
6. Uncertainty analysis

DEFINE RECOMMENDATIONS

1. Risk mitigation
2. Risk transference
3. Risk acceptance
4. Risk avoidance

MANAGEMENT

RISK MITIGATION

- Control selection
- Implementation
- Monitoring

RISK TRANSFERENCE

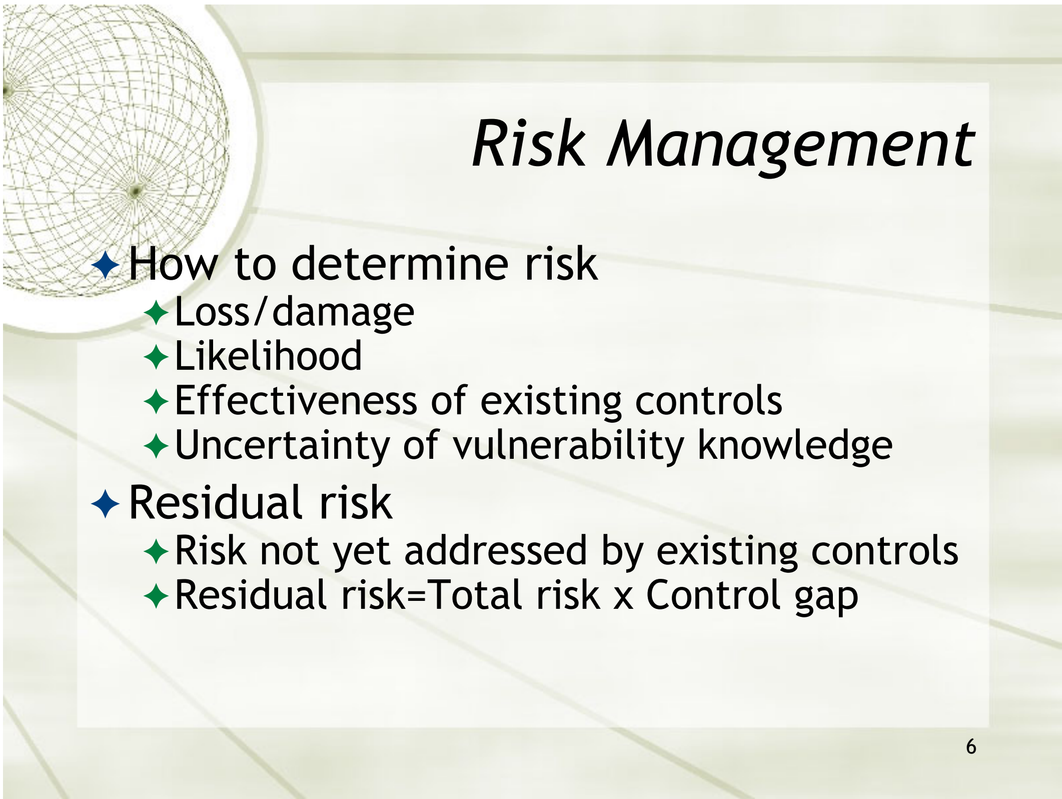
- Purchase insurance

RISK ACCEPTANCE

- Do nothing

RISK AVOIDANCE

- Discontinue activity



Risk Management

- How to determine risk
  - Loss/damage
  - Likelihood
  - Effectiveness of existing controls
  - Uncertainty of vulnerability knowledge
- Residual risk
  - Risk not yet addressed by existing controls
  - Residual risk=Total risk x Control gap

6

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.

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:

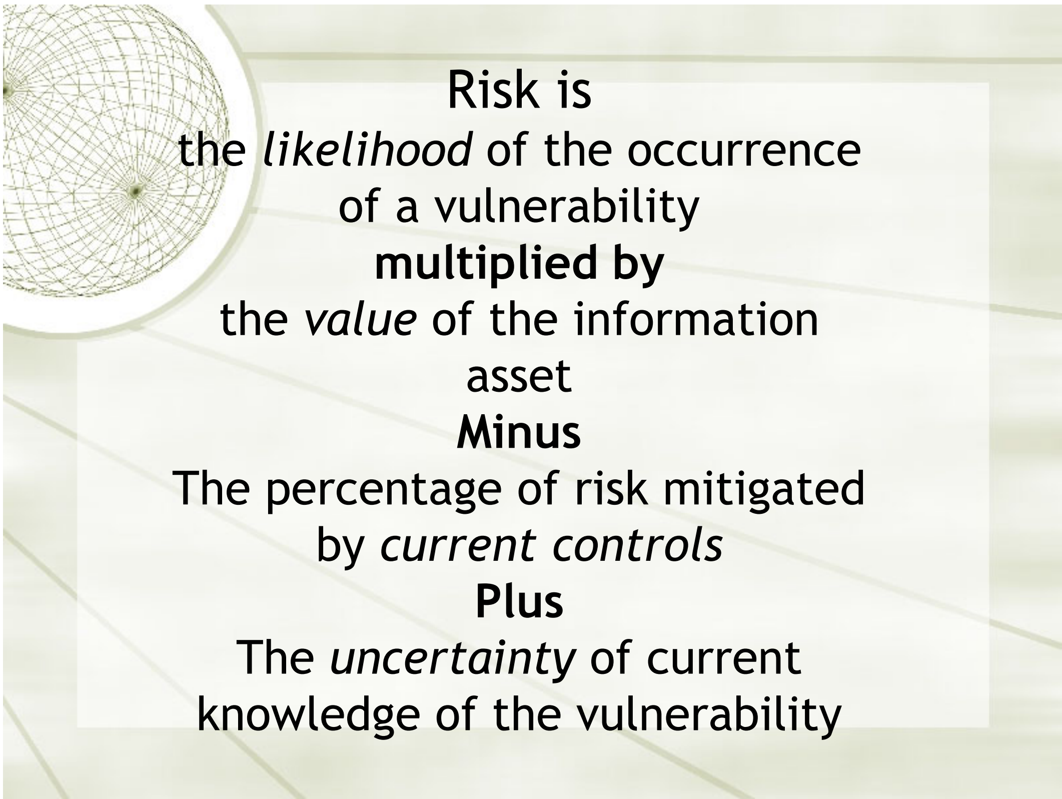
The likelihood of a fire has been estimated actuarially for each type of structure.

The likelihood that any given e-mail contains a virus or worm has been researched.

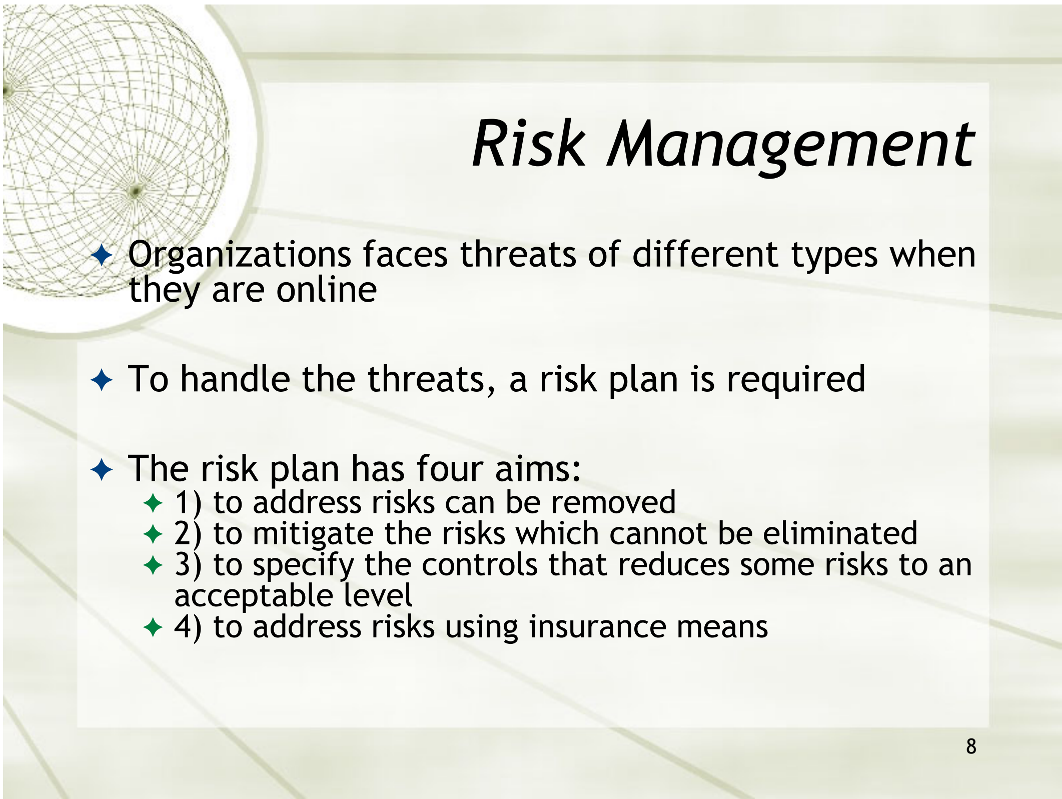
The number of network attacks can be forecast based on how many assigned network addresses the organization has.

If a company addresses 20% of the risk, then the control gap will be 80%

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.



Risk is
the *likelihood* of the occurrence
of a vulnerability
multiplied by
the *value* of the information
asset
Minus
The percentage of risk mitigated
by *current controls*
Plus
The *uncertainty* of current
knowledge of the vulnerability



Risk Management

- Organizations faces threats of different types when they are online
- To handle the threats, a risk plan is required
- The risk plan has four aims:
  - 1) to address risks can be removed
  - 2) to mitigate the risks which cannot be eliminated
  - 3) to specify the controls that reduces some risks to an acceptable level
  - 4) to address risks using insurance means

All organizations face risks of one sort or another on a daily basis. Risk management is a discipline that exists to deal with non-speculative risks those risks from which only a loss can occur. In other words, speculative risks, those from which either a profit or a loss can occur, are the subject of the organization's business strategy whereas non-speculative risks, which can reduce the value of the assets with which the organization undertakes its speculative activity, are (usually) the subject of a risk management plan (in the standard, a 'risk treatment plan'). These are sometimes called permanent and 'pure' risks, in order to differentiate them from the crisis and speculative types. Risk management plans usually have four, linked, objectives. These are:

1. to eliminate risks;

2. to reduce to 'acceptable' levels those that cannot be eliminated; and then either

3. to live with them, exercising carefully the controls that keep them 'acceptable'; or

4. to transfer them, by means of insurance, to some other organization.

Pure, permanent risks are usually identifiable in economic terms; they have a financially measurable potential impact upon the assets of the organization. Risk management strategies are usually therefore based on an assessment of the economic benefits that the organization can derive from an investment in a particular control; in other words, for every control that the organization might implement, the calculation would be

that the cost of implementation would be outweighed, preferably significantly, by the economic benefits that derive from, or economic losses that are avoided as a result of, its implementation. The organization should define its criteria for accepting risks (for example, it might say that it will accept any risk whose economic impact is less than the cost of controlling it) and for controlling risks (for example, it might say that any risk that has both a high likelihood and a high impact must be controlled to an identified level, or threshold)

Risk Management

- Major undertakings:
  - Identify risks: examine and document security posture of IT and the risks it faces
  - Assess risks: determine the extent to which assets are exposed or at risk
  - Address risks: recommend/apply security controls

9

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. Each of the three elements in the C.I.A. triad, is an essential part of every IT organization’s ability to sustain long-term competitiveness.

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**: *risk identification, risk assessment, and risk control*.

- Risk identification is the examination and documentation of the security posture of an organization’s information technology and the risks it faces. (Examining assets, going through the security policies

- 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

Risk Management

- Risk management: formal process
  - Planning
  - Documentation
  - Assurance
- Who/How
  - Periodic review
  - Appropriately qualified and experienced person

10

The risk assessment must be a **formal** process. In other words, the process must be *planned, and the input data, their analysis and the results should all be recorded*. ‘Formal’ does not mean that risk assessment tools must be used, although in many situations they are likely to turn a potentially difficult and time-consuming task into one that can be completed in a meaningful timescale and to add significant value. Risk assessments must also produce ‘comparable and reproducible results’; this requirement (clause 4.2.1.c) tends to support the use of a purpose-developed tool and a well-defined methodology. The complexity of the risk assessment will depend on the complexity of the organization and of the risks under review. The techniques employed to carry it out should be consistent with this complexity and the level of assurance required by the board.

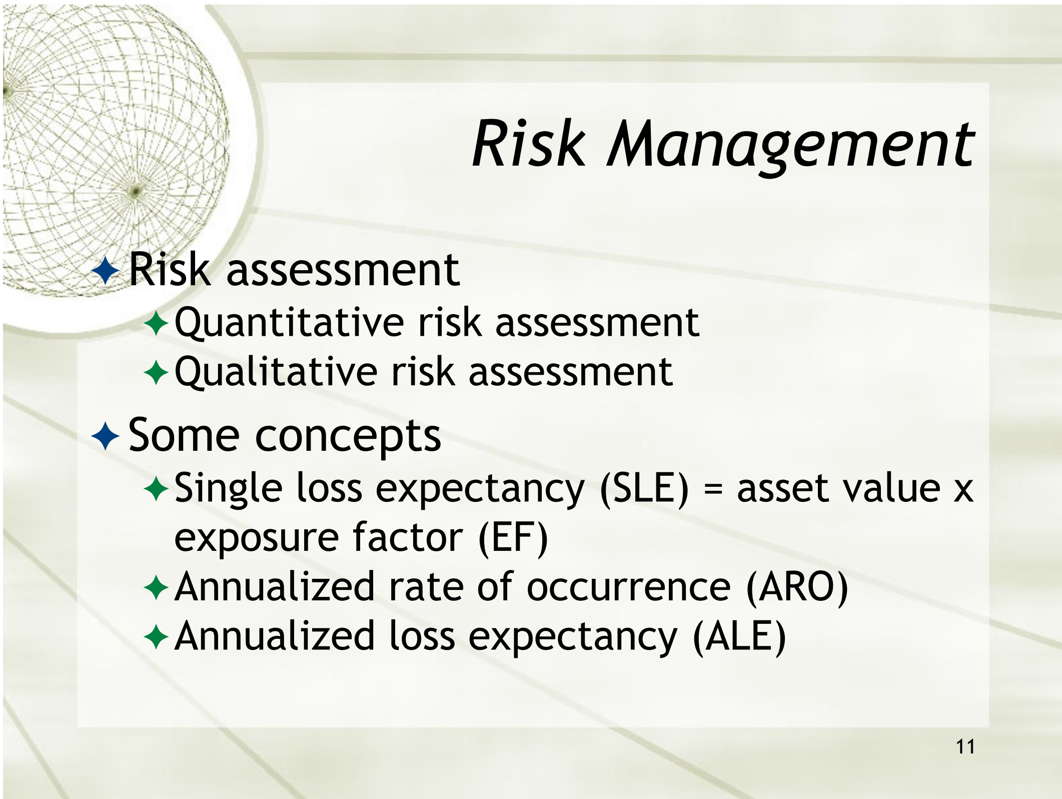
Organisations are constantly at risk. Need to set a timeline for periodically reviewing the risk again in the new environment and identifying the risk.

It is entirely up to the individual organization to choose **who is to undertake this risk assessment, and how**. There are two issues to consider before deciding who.

-

The first is that the standard expects that **periodic reviews** of security risks and related controls will be carried out –taking account of new threats and vulnerabilities, assessing the impact of changes in the business, its goals or processes, technology and/or its external environment (such as legislation, regulation or society) and simply to confirm that controls remain effective and appropriate. Periodic review is a fundamental requirement of any risk assessment or risk management strategy.

-The second is that it is an assumption of the standard 'that the execution of its provisions is entrusted to appropriately qualified and experienced people'. It is essential that risk assessment – the core competency of information security management – is conducted by **an appropriately qualified and experienced person**. This is logical; the key step on which the entire ISMS will be built needs, itself, to be solid. The ISO27001 auditor will therefore want to see documentary evidence of the formal qualifications and experience of this person.



Risk Management

- Risk assessment
  - Quantitative risk assessment
  - Qualitative risk assessment
- Some concepts
  - Single loss expectancy (SLE) = asset value x exposure factor (EF)
  - Annualized rate of occurrence (ARO)
  - Annualized loss expectancy (ALE)

Quantitative risk analysis attempts to assign real and meaningful numbers to all elements of the risk analysis process. (Not necessarily monetary values all the time)

These elements may include safeguard costs, asset value, business impact, threat frequency, safeguard effectiveness, exploit probabilities, and so on. When all of these are quantified, the process is said to be quantitative. Quantitative risk analysis also provides concrete probability percentages when determining the likelihood of threats. Each element within the analysis (asset value, threat frequency, severity of vulnerability, impact damage, safeguard costs, safeguard effectiveness, uncertainty, and probability items) is quantified and entered into equations to determine total and residual risks. Purely quantitative risk analysis is not possible because the method attempts to quantify qualitative items, and there are always uncertainties in quantitative values. How do you know how often a vulnerability will be exploited? How do you know the exact monetary business impact that would arise?

In short, this approach looks at two issues: the probability of an event occurring and the likely loss should it occur. A single figure is produced from these two elements, by simply multiplying the potential loss (measured in monetary terms) by its probability (measured as a percentage). This is sometimes called the ‘annual loss expectancy’ (ALE) or the ‘estimated annual cost’ (EAC). Clearly, the higher the number that an event or risk has, the more serious it is for the organization. It is then possible to rank events in order of risk (ALE) and to make decisions based upon this.

The problems with this type of risk analysis are usually associated with the unreliability and inaccuracy of the data. Probability is usually assessed subjectively and is rarely precise. In some cases, this approach can promote or reflect complacency about the real significance of particular risks.

The monetary value of the potential loss is also often assessed subjectively, and when the two components are multiplied together, the answer is equally subjective.

In addition, controls and countermeasures often have to tackle a number of potential events, and the events themselves are frequently interrelated. A detailed ranking in order of ALE can make it difficult to identify these interrelationships and lead to poor decisions about controls, and this approach is not, therefore, recommended.

Another method of risk analysis is qualitative, which does not assign numbers and monetary values to components and losses. Instead, qualitative methods walk through different scenarios of risk possibilities and rank the seriousness of the threats and the validity of the different possible countermeasures based on opinions. (A wide sweeping analysis can include hundreds of scenarios.) Qualitative analysis techniques include judgment, best practices, intuition, and experience. Examples of qualitative techniques to gather data are Delphi, brainstorming, storyboarding, focus groups, surveys, questionnaires, checklists, one-on-one meetings, and interviews. The risk analysis team will determine the best technique for the threats that need to be assessed, as well as the culture of the company and individuals involved with the analysis. The team that is performing the risk analysis gathers personnel who have experience and education on the threats being evaluated. When this group is presented with a scenario that describes threats and loss potential, each member responds with their gut feeling and experience on the likelihood of the threat and the extent of damage that may result.

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

SLE = asset value x exposure factor (EF)

where EF equals the percentage loss that would occur from a given vulnerability being exploited. For example, if a Web site has an estimated value of $1,000,000 (value determined by asset valuation), and a deliberate act of sabotage or vandalism (hacker defacement) scenario indicates that 10 percent of the Web site would be damaged or destroyed after such an attack, then the SLE for this Web site would be $1,000,000 0.10 $100,000.

Annualized rate of occurrence (ARO). This calculates how often an organisation expects an event. It is simply how often you expect a specific type of attack to occur **per year**. For example, a successful deliberate act of sabotage

or vandalism might occur about once every two years, in which case the ARO would be 50 percent (0.50), whereas some kinds of network attacks can occur multiple times per second. To standardize calculations, you convert the rate to a yearly (annualized) value. This is expressed as the probability of a threat occurrence.

Once each asset's worth is known, the next step is to ascertain *how much loss is expected from a single expected attack, and how often these attacks occur.* Once those values are established, the equation can be completed to determine the overall lost potential per risk. This is usually determined through an **annualized loss expectancy (ALE)**, which is calculated from the ARO and SLE, as shown here:

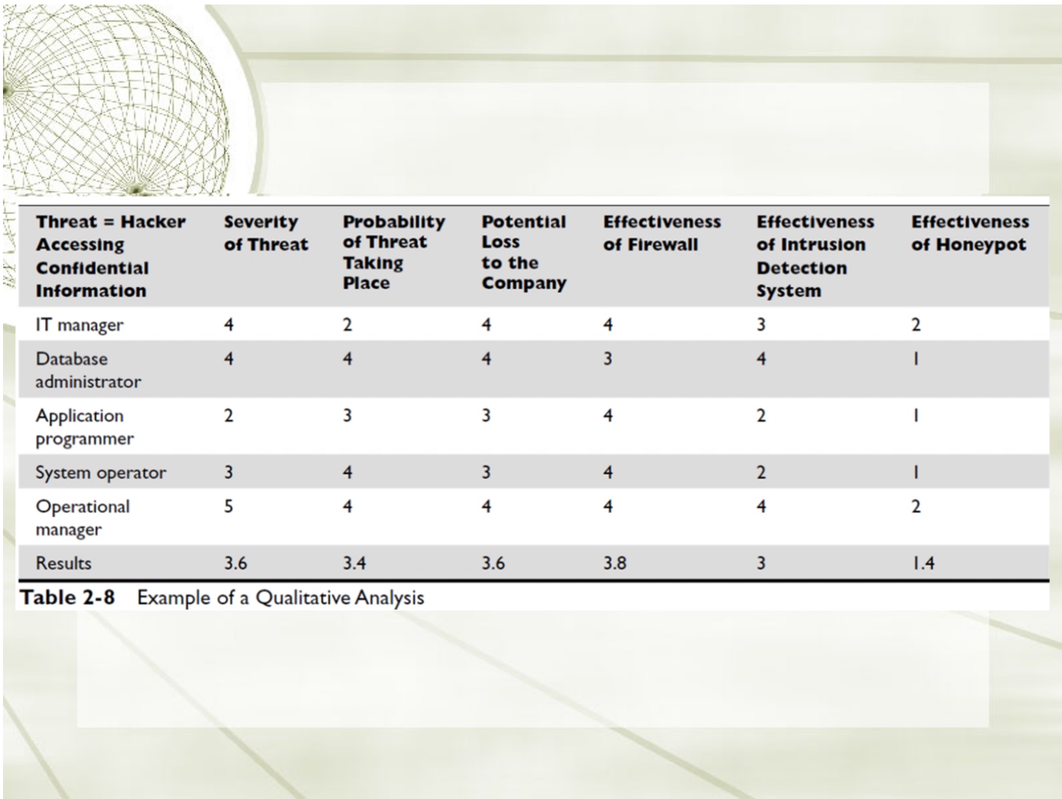
ALE = SLE x ARO

Using the example of the Web site that might suffer a deliberate act of sabotage or vandalism and thus has an SLE of $100,000 and an ARO of 0.50, the ALE would be calculated as follows:

ALE = $100,000 x 0.50 = $50,000

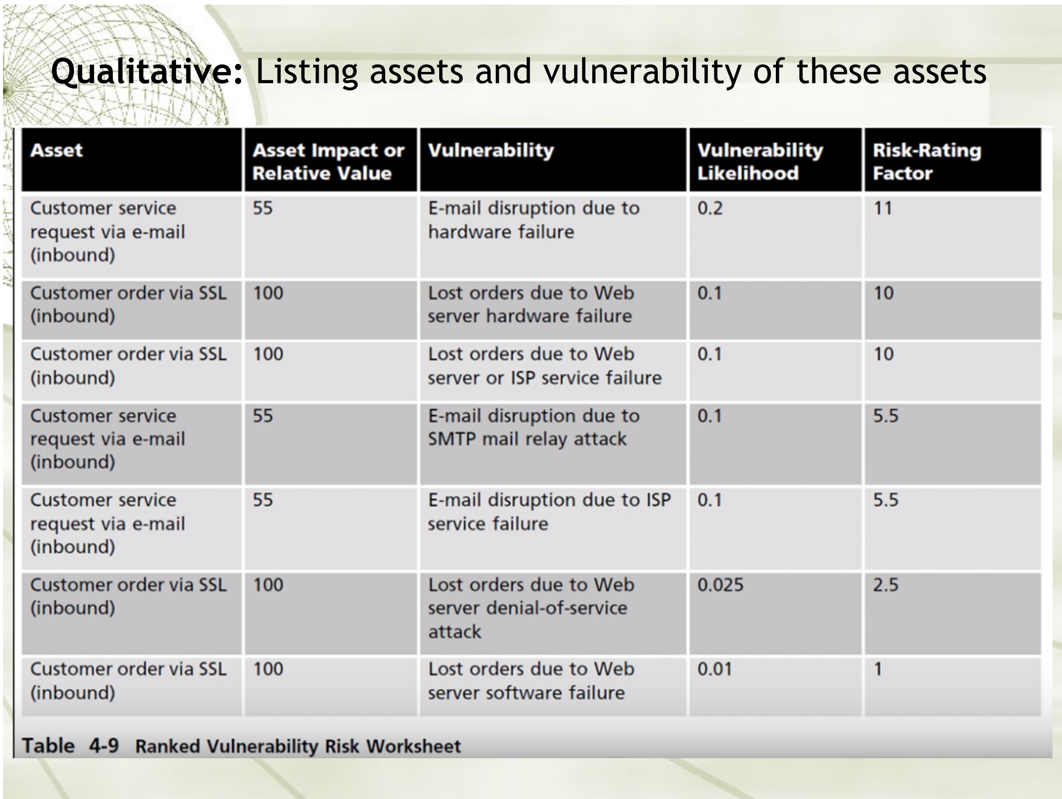
The Cost Benefit Analysis (CBA) Formula: Subtract the revised ALE, estimated based on the control being in place, known as ALE(post). Complete the calculation by subtracting the **annualized cost of the safeguard (ACS)**.

CBA = ALE(prior) - ALE(post) - ACS



Threat = Hacker Accessing Confidential Information	Severity of Threat	Probability of Threat Taking Place	Potential Loss to the Company	Effectiveness of Firewall	Effectiveness of Intrusion Detection System	Effectiveness of Honeypot
IT manager	4	2	4	4	3	2
Database administrator	4	4	4	3	4	1
Application programmer	2	3	3	4	2	1
System operator	3	4	3	4	2	1
Operational manager	5	4	4	4	4	2
Results	3.6	3.4	3.6	3.8	3	1.4

Table 2-8 Example of a Qualitative Analysis

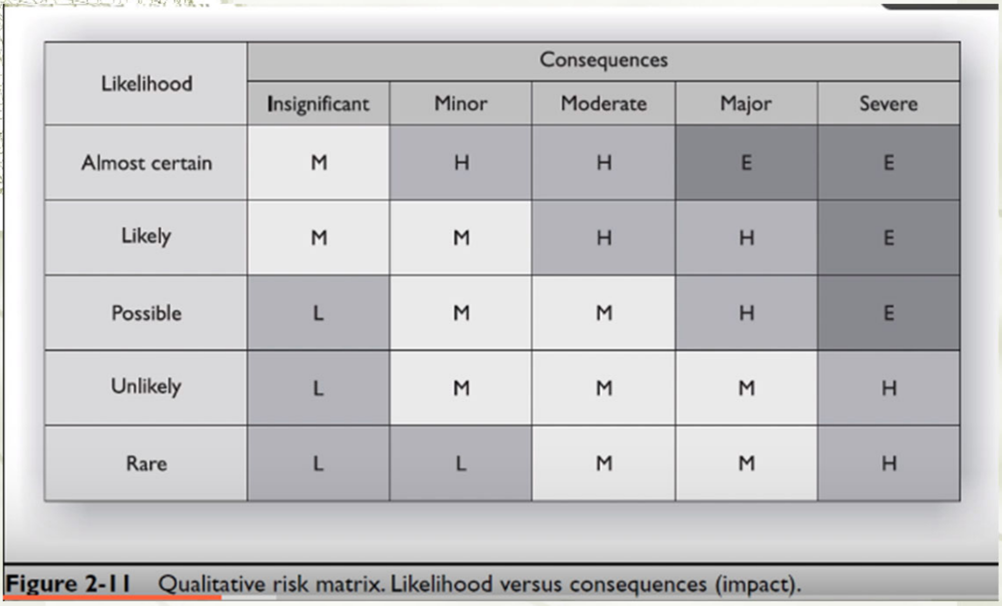


Qualitative: Listing assets and vulnerability of these assets

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

Table 4-9 Ranked Vulnerability Risk Worksheet

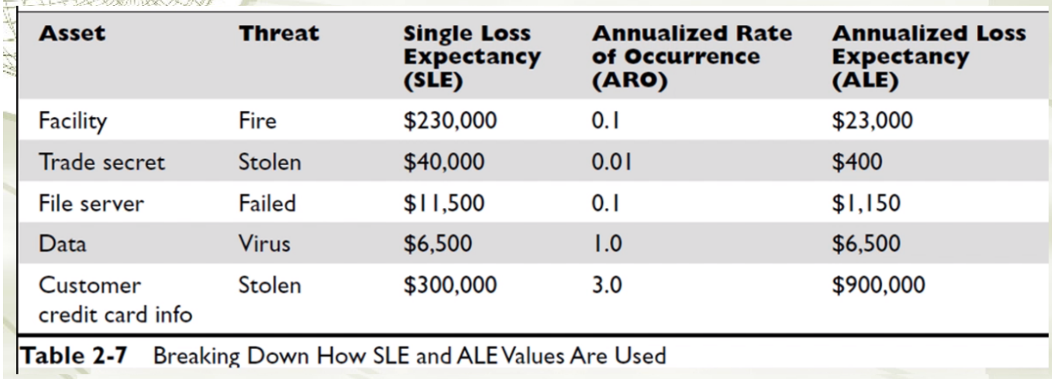
Qualitative Risk Matrix



Likelihood	Consequences				
	Insignificant	Minor	Moderate	Major	Severe
Almost certain	M	H	H	E	E
Likely	M	M	H	H	E
Possible	L	M	M	H	E
Unlikely	L	M	M	M	H
Rare	L	L	M	M	H

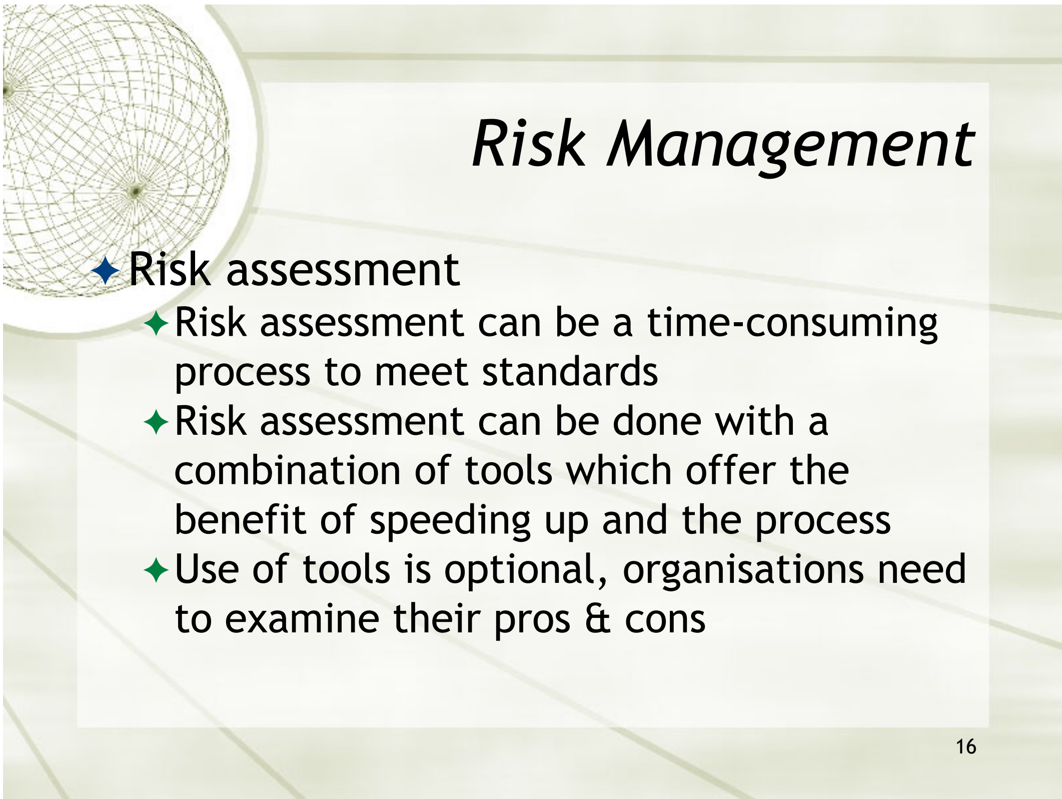
Figure 2-11 Qualitative risk matrix. Likelihood versus consequences (impact).

Quantitative Risk Assessment example



Asset	Threat	Single Loss Expectancy (SLE)	Annualized Rate of Occurrence (ARO)	Annualized Loss Expectancy (ALE)
Facility	Fire	$230,000	0.1	$23,000
Trade secret	Stolen	$40,000	0.01	$400
File server	Failed	$11,500	0.1	$1,150
Data	Virus	$6,500	1.0	$6,500
Customer credit card info	Stolen	$300,000	3.0	$900,000

Table 2-7 Breaking Down How SLE and ALE Values Are Used



Risk Management

- Risk assessment
  - Risk assessment can be a time-consuming process to meet standards
  - Risk assessment can be done with a combination of tools which offer the benefit of speeding up and the process
  - Use of tools is optional, organisations need to examine their pros & cons

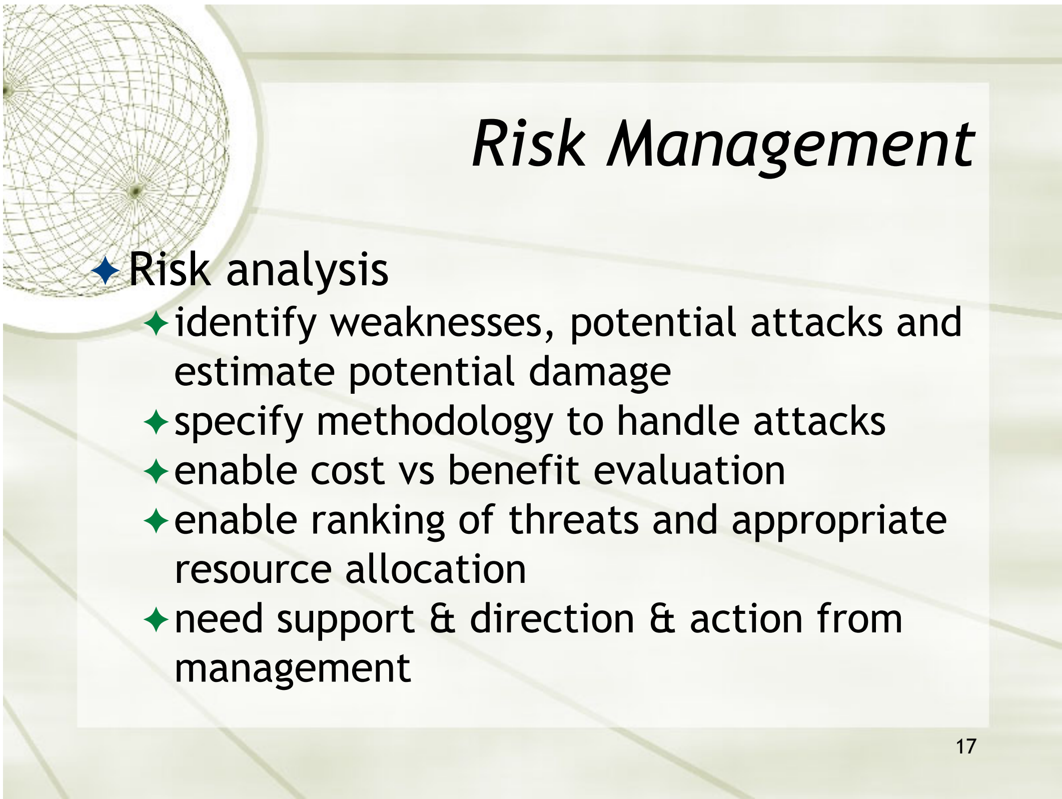
Tools to asses and handle threats

There are an increasing number of software tools available that can, to a varying extent, automate the risk assessment process and generate the statement of applicability. In theory, such a tool ought to encourage the user to perform a thorough and comprehensive security audit on the organization's information systems, and ought not to produce too much paperwork as a result. The organization will need to compare tools before making a selection and should concentrate, in the comparison process, on the extent to which the tool really does easily and effectively automate the risk assessment and statement of applicability development process; the amount of additional paperwork it generates; the flexibility it offers for dealing with changing circumstances and frequent, smaller-scale risk assessments; and the meaningfulness of the results it generates. Of course, normal due diligence should also be done into the status of the supplier and manufacturer of the product to ensure that it is properly supported and likely to continue to be. References might also be sought from happy customers. (Tools could generate and plot graphs or templates for risk assessment from surveys)

Cons:

- Organisation would be too dependent on these risk assessment tools
- Everytime an organisation hires new people they would have to train the new people on how to use these softwares

Risk assessments can, with difficulty, be done without using such tools. A thorough risk assessment of any significant business will be very time-consuming, and even more so if a software tool is not used. ‘Time-consuming’ means up to three months, or even longer for larger organizations. The use of a software tool will depend on the culture of the organization and the preferences of the information security adviser and manager. Practically speaking, once the organization has decided to purchase such a tool, it becomes dependent on that tool and on the staff members who are trained to use it. In considering the appropriate route forward, consideration should be given to the speed with which incoming staff can become familiar with the chosen risk assessment tool; practicality and ease of use are likely to be key attributes



Risk Management

- Risk analysis
  - identify weaknesses, potential attacks and estimate potential damage
  - specify methodology to handle attacks
  - enable cost vs benefit evaluation
  - enable ranking of threats and appropriate resource allocation
  - need support & direction & action from management

17

- Controls usually should not cost more than the amount of damage that is being reduced. Thus an organisation should compare the cost of the control and the benefit that you reap from the control in terms of reducing the quantitative risk. Implement the control if the benefit outweighs the cost. If the cost is too high then the control is not worth it, an organisation can then choose to accept the risk. Through risk analysis, an organisation could compare and rank the risk based on which is important and address the important threat first.

Risk analysis, which is really a tool for risk management, is a method of identifying vulnerabilities and threats and assessing the possible impacts to determine where to implement security safeguards. Risk analysis is used to ensure that security is cost-effective, relevant, timely, and responsive to threats. Security can be quite complex, even for well- versed security professionals, and it is easy to apply too much security, not enough security, or the wrong security components, and to spend too much money in the process without attaining the necessary objectives. Risk analysis helps companies prioritize their risks and shows management the amount of money that should be applied to protecting against those risks in a sensible manner.

A risk analysis **has four main goals**:

- Identify assets and their value to the organization.
- Identify vulnerabilities and threats.
- Quantify the probability and business impact of these potential threats.
- Provide an economic balance between the impact of the threat and the cost of the countermeasure.

Risk analysis provides a cost/benefit comparison, which compares the annualized cost of safeguards to the potential cost of loss. A safeguard, in most cases, should not be implemented unless the annualized cost of loss exceeds the annualized cost of the safe- guard itself. This means that if a facility is worth $100,000, it does not make sense to spend $150,000 trying to protect it. It is important to figure out what you are supposed to be doing before you dig right in and start working. Anyone who has worked on a project without a properly defined scope can attest to the truth of this statement. Before an assessment and analysis is started, the team must carry out project sizing to understand what assets and threats should be evaluated. Most assessments are focused on physical security, technology security, or personnel security. Trying to assess all of them at the same time can be quite an undertaking.

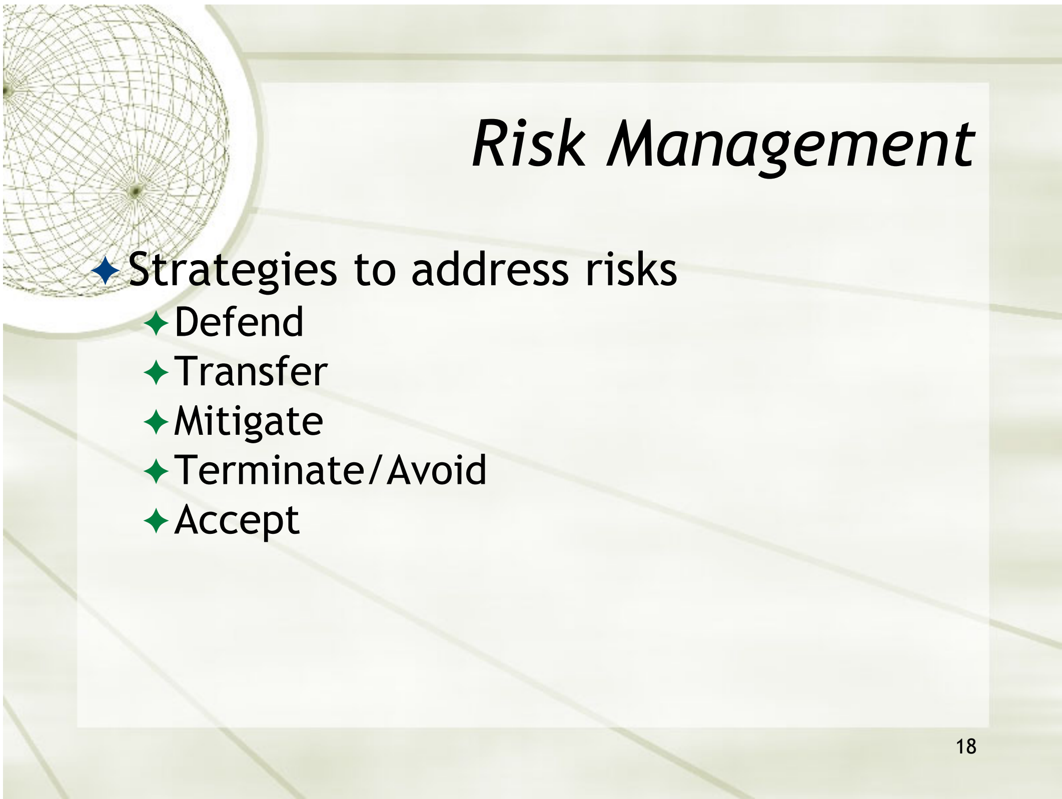
One of the team's tasks is to create a report that details the asset valuations. Senior management should review and accept the lists, and make them the scope of the IRM project. If management determines at this early stage that some assets are not important, the risk assessment team should not spend additional time or resources evaluating those assets. During discussions with management, everyone involved must have a firm understanding of the value of the security AIC triad (availability, integrity, and confidentiality) and how it directly relates to business needs.

Management should outline the scope, which most likely will be dictated by organizational governance, risk management, and compliance as well as budgetary constraints. Many projects have run out of funds, and consequently stopped, because proper project sizing was not conducted at the onset of the project. Don't let this happen to you. A risk analysis helps integrate the security program objectives with the company's business objectives and requirements. The more the business and security objectives are in alignment, the more successful the two will be. The analysis also helps the company draft a proper budget for a security program and its constituent security components. Once a company knows how much its assets are worth and the possible threats they are exposed to, it can make intelligent decisions about how much money to spend protecting

those assets.

A risk analysis must be supported and directed by senior management if it is to be successful. Management must define the purpose and scope of the analysis, appoint a team to carry out the assessment, and allocate the necessary time and funds to conduct the analysis***. It is essential for senior management to review the outcome of the risk assessment and analysis and to act on its findings***. After all, what good is it to go through all

the trouble of a risk assessment and not react to its findings? Unfortunately, this does happen all too often.



Risk Management

- Strategies to address risks
  - Defend
  - Transfer
  - Mitigate
  - Terminate/Avoid
  - Accept

18

Defend

To reduce the likelihood of the risk coming through.

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.

Organizations can mitigate risk to an asset by countering the threats it faces or by **eliminating its exposure**. It is difficult, but possible, to eliminate a threat. For example, in 2002 McDonalds Corporation, which had been subject to attacks by animal rights cyberactivists, sought to reduce risks by imposing stricter conditions on egg suppliers regarding the health and welfare of chickens. This strategy was consistent with other changes made by McDonalds to meet demands from animal rights activists and improve relationships with these groups.

Another **defend** strategy is the implementation of security controls and safeguards to deflect attacks on systems and therefore minimize the probability that an attack will be successful. An organization with dial-in access vulnerability, for example, may choose to implement a control or safeguard for that service. An authentication procedure based on a cryptographic technology, such as RADIUS (Remote Authentication Dial-In User Service), or another protocol or product, would provide sufficient control. On the other hand, the organization may choose to eliminate the dial-in system and service to avoid the potential risk

Transfer

The **transfer** control strategy attempts to shift risk to other assets, other processes, or other organizations. Contact the other party if the risk comes through. 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*.

In the popular book In Search of Excellence, management consultants Tom Peters and Robert Waterman present a series of case studies of high-performing corporations. One of the eight characteristics of excellent organizations is that they stick to their knitting... They stay reasonably close to the business they know. This means that Kodak, a manufacturer of photographic equipment and chemicals, focuses on photographic equipment and chemicals, while General Motors focuses on the design and construction of cars and trucks. Neither company spends strategic energies on the technology of Web site development or this expertise, they rely on consultants or contractors. This principle should be considered whenever an organization begins to expand its operations, including information and systems management and even information security. If an organization does not already have quality security management and administration experience, it should hire individuals or firms that provide such expertise. For example, many organizations want Web services, including Web presences, domain name registration, and domain and Web hosting. Rather than implementing their own servers and hiring their own Webmasters, Web systems administrators, and specialized security experts, savvy organizations hire an ISP or a consulting organization to provide these products and services for them. This allows the organization to transfer the risks associated with the management of these complex systems to another organization that has experience in dealing with those risks. A side benefit of specific contract arrangements is that the provider is responsible for disaster recovery, and through service level agreements is responsible for guaranteeing server and Web site availability.

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: the incident response plan, the disaster recovery plan, and the business continuity plan.

Terminate

The **terminate** control strategy directs the organization to avoid those business activities that introduce uncontrollable risks. (Terminate what you are doing that causes the risk) 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 partner- ship opportunities. By terminating the questionable activity, the organization reduces the risk exposure.

Accept

(Especially if the risk is relatively low)

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:

•Determined the level of risk

•Assessed the probability of attack

•Estimated the potential damage that could occur from attacks

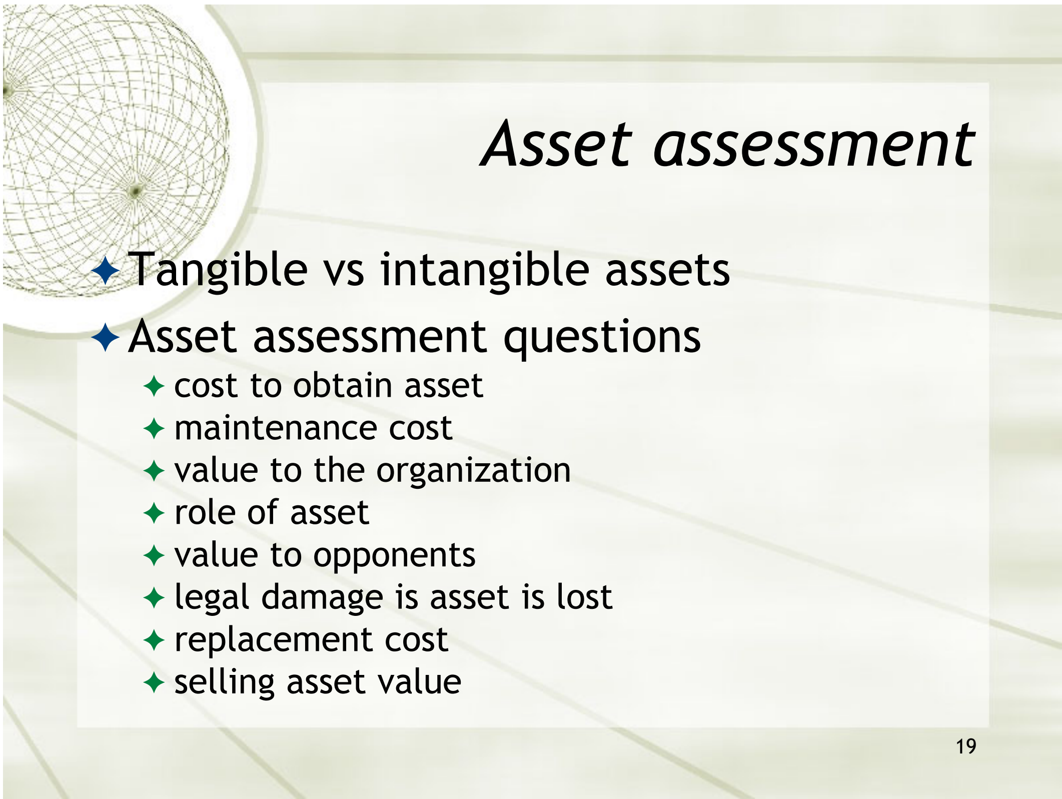
•Performed a thorough cost benefit analysis

•Evaluated controls using each appropriate type of feasibility

•Decided that the particular function, service, information, or asset did not justify the cost of protection

This strategy is based on the conclusion that the cost of protecting an asset does not justify the security expenditure. For example, suppose it would cost an organization $100,000 per year to protect a server. The security assessment determined that for $10,000 the organization could replace the information contained in the server, replace the server itself, and cover associated recovery costs. In this case, management may be satisfied with taking its chances and saving the money that would normally be spent on protecting this asset. If every vulnerability in the organization is handled by means of acceptance, it may reflect an inability to conduct proactive security activities and an apathetic approach to security in general. It is not acceptable for an organization to adopt a policy that ignorance is bliss and hope to avoid litigation by pleading ignorance of its obligation to protect employee and customer information. It is also unacceptable for management to hope that if they do not try to protect information, the opposition will assume that there is little to be gained by an attack. The risks far outweigh the benefits of this approach.

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



Asset assessment

- Tangible vs intangible assets
- Asset assessment questions
  - cost to obtain asset
  - maintenance cost
  - value to the organization
  - role of asset
  - value to opponents
  - legal damage is asset is lost
  - replacement cost
  - selling asset value

19

Tangible : Physical form, assets that can be sell in the market for fixed value

Intangible: Non-physical form

Assets may be **tangible** (computers, facilities, supplies) or **intangible** (reputation, data, intellectual property). It is usually harder to quantify the values of intangible assets, which may change over time. How do you put a monetary value on a company's reputation? This is not always an easy question to answer, but it is important to be able to do so.

An asset can have both quantitative and qualitative measurements assigned to it, but these measurements need to be derived. The actual value of an asset is determined by the cost it takes to acquire, develop, and maintain it. The value is determined by the importance it has to the owners, authorized users, and unauthorized users. Some information is important enough to a company to go through the steps of making it a trade secret.

The value of an asset should reflect all identifiable costs that would arise if the asset were actually impaired. If a server cost $4,000 to purchase, this value should not be input as the value of the asset in a risk assessment. Rather, the cost of replacing or re- pairing it, the loss of productivity, and the value of any data that may be corrupted or lost must be accounted for to properly capture the amount the company would lose if the server were to fail for one reason or another.

The following issues should be considered when assigning values to assets:

- Cost to acquire or develop the asset
- Cost to maintain and protect the asset
- Value of the asset to owners and users
- Value of the asset to adversaries
- Value of intellectual property that went into developing the information
- Price others are willing to pay for the asset
- Cost to replace the asset if lost
- Operational and production activities affected if the asset is unavailable
- Liability issues if the asset is compromised
- Usefulness and role of the asset in the organization

Understanding the value of an asset is the first step to understanding what security mechanisms should be put in place and what funds should go toward protecting it. A very important question is how much it could cost the company to not protect the asset.

Asset assessment

- role of asset
- value to opponents
- legal damage is asset is lost
- replacement cost
- selling asset value

Benefits of asset assessment:

•Determining the value of assets may be useful to a company for a variety of reasons, including the following:

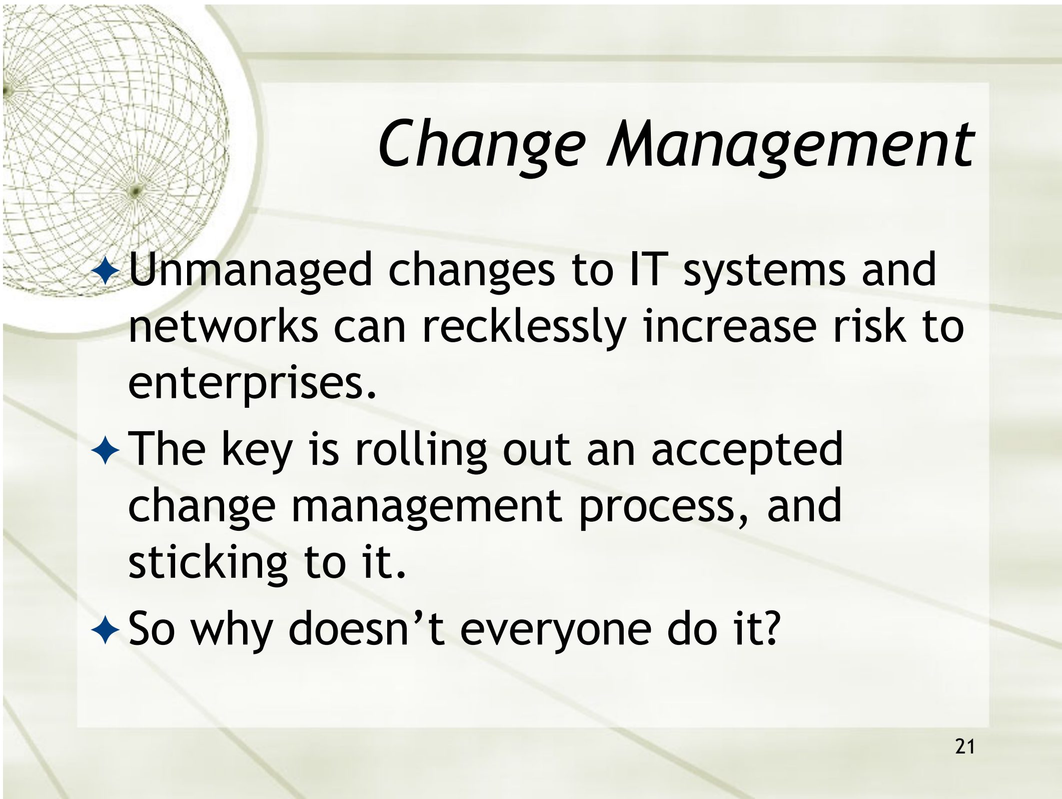
•To perform effective cost/benefit analyses

•To select specific countermeasures and safeguards

•To determine the level of insurance coverage to purchase

•To understand what exactly is at risk

•To conform to due care and to comply with legal and regulatory requirements



Change Management

- ✦ Unmanaged changes to IT systems and networks can recklessly increase risk to enterprises.
- ✦ The key is rolling out an accepted change management process, and sticking to it.
- ✦ So why doesn’t everyone do it?

21

Change management- process of implementing changes in a controlled manner for e.g. maintaining information integrity. Changes often happen on a very frequent basis e.g. I few are writing a piece of program, we are writing it incrementally, everytime a change ais made we have to push for those changes. That’s why we need standard procedures for pushing changes. There are different kinds of changes.

- Standard changes: low risk, follow standard procedure
- Approved by top-management : should follow the process of **change management**

Changes can be in the hardware or software of the system, patches or updates, new technology like facial recognition. Updates in the policy or when businesses are acquired by other businesses. All these changes need to go through change management. For minor changes such as adding a user or changing some non-critical user configurations, may not need to follow change management procedures.

Unmanaged changes to IT systems and networks can recklessly increase risk to enterprises. The key is rolling out an accepted change management process, and sticking to it.

So change management is good, right? Why doesn't everyone do it? Because sometimes following the rules seems like a real waste of time.

Trying to get things done at work can feel frustrating. Take for example a team of developers that has just written a much better looking and easier to use version of the organization's website. The only problem is that it can't be tested by the remote QA team because the firewall is blocking access. Waiting for change management approval could take weeks, so as the firewall admin, it may be very tempting to want to help out the development team by temporarily opening a port on the fiAn orewall. Sadly, we've all seen some variation of how that story ends: a worm or Trojan is introduced onto the internal network, a sniffer is planted on a server and credentials are stolen, or a previously protected database is exposed to attackers.

Many of the exposures associated with lack of change management are more complex and subtle than in the example. This is due to the complex nature of today's network environments. Networks are complicated ecosystems and dependencies are not always clear, especially to someone who only sees part of the whole system at a time. A database administrator changing an IP address could lead to a critical service outage. A router administrator that configures a new static route may inadvertently redirect or block traffic from hundreds of remote offices.

The purpose of change management is to prevent unintended consequences, such as the ones described, and ensure that changes or alterations to systems are implemented according to an approved framework or model. That's not something many employees would argue with. The problem occurs when an employee, such as the firewall admin in our example above, thinks that circumventing the system will allow things to work more efficiently--or feels that following the processes somehow detracts from getting "real work" done. So the challenge is not simply putting change management in place, but also gaining buy-in from all users of the system so that they're incented to follow the change management process rather than circumvent it.

LAYING THE GROUNDWORK FOR EFFECTIVE CHANGE MANAGEMENT

Whether your organization is just starting to build a change management program or is in the processing of improving and fine-tuning an existing one, it's important to focus the program around business improvement and maximum awareness. In the strictest IT sense of the word "change" refers to actual changes to a system or application such as a new sub-domain, firewall rule, or addition to a CMDB (configuration management database). As an integrative component in risk management, change extends to include all ramifications resulting from a particular change. Lindstrom explains, "The important point here is to forego the 'ready, aim, fire' mentality without implementing a monolithic process that is unmanageable and easily circumvented."

For example, how much downtime will be incurred? What is the cost associated with the change and any resulting downtime? Will the change impact other services? What is the schedule for the change and will it conflict with any other changes? The ability to answer these questions depends on a number of factors including the assessors' knowledge of the systems and operations in place as well as the tools and processes the organization has put in place to help manage change. For example, while a ticketing system such as Remedy can help provide information about what changes are in the queue, a shared calendar helps prevent scheduling conflicts.

The team responsible for the Unified Compliance Framework and "The Change Management Toolkit" sums this concept up nicely: "the objective of change management is to enable beneficial changes to be made with minimum disruption to services. . . Therefore, what you want to ensure through change management is that all changes are known." Ferguson recommends reading, "The Visible Ops Handbook: Implementing ITIL in 4 Practical and Auditable Steps," for specifics on building an effective change management program. Says Ferguson, "Of all the things you want to do with ITIL, the first thing to really look at is your change management," he says. "Organizations that invest in change management see a lot of benefit in reduced downtime and fewer outages."

Users report that as their change management programs mature, the scope of the program often expands. But this doesn't always translate to having complete control over every piece of equipment in an environment. Rather than trying to put all devices under the auspices of the IT department's change management program, try to understand what benefits can be offered to the device or service owner to encourage more active participation. For devices that can't be included in the change management program, maintain protection from other parts of the network with approved security controls such as zoning, intrusion protection and antimalware.

As repeatable standards and measures are put into place, change and risk related questions can be answered in a more efficient and normalized manner. At Northwest Hospital there is a workflow process known as pre-approved changes; routine changes that happen over and over. "We perform change management on these routine changes, but we simplify the approval process each time," Ferguson says. Some changes may, eventually, be considered routine and well known enough that they can be accepted outside of the formal approval process.

David Sherry, CISO for Brown University in Rhode Island notes that centralizing servers and services in a managed data center increases the number of known changes that can be performed without formal approval, which, in turn, serves as a motivation for departments and users to opt-in to the centrally managed data center offerings. "Moving to the data center has so many benefits that most departments want to do it voluntarily," says Sherry.

CHANGE MANAGEMENT BUY-IN AND ENFORCEMENT

Getting buy-in for the change management process is a much more successful strategy than using an audit or compliance "stick" to force participation. Not every vertical has a big compliance stick to yield, but even change management gurus in the heavily regulated financial services industry report that "carrots" are most effective. And the tastiest carrot is wrapped in a tangible business gain. As Ferguson explains, "Sometimes marketing change management to staff is difficult. It has to be marketed as beneficial."

As most security professionals know, selling "better security" isn't always the most motivating benefit for many users. Sherry cites a few positive ways his team has promoted buy-in.

"Change management can be a great communications vehicle, encouraging groups from different departments to work together," he says. Open communication can lead to smoother functionality too--he recalls one meeting where a team had seen a new firewall installation scheduled on the shared calendar and they came to the next change management review meeting with a comprehensive list of tests that would need to be performed "to ensure everything was running smoothly, and there was no loss of business continuity." Echoing the business continuity benefit, Ferguson points out similar benefits, "Without knowing what's causing a suspicious event, we have to treat them all as critical."

Another way to encourage participation is to make it easy for people to engage with the process. Make sure that the procedures are documented clearly and easy to find on an accessible website. If your organization is large and distributed, create a central landing page for the baseline change management procedures and branch as needed to sub-procedures that apply to business units and subsidiaries, different geographic locations, or departments.

Regular change management meetings were recommended by all interviewees. Both Northwest Hospital and Brown University have change management review committees that meet every week to review requests. This allows employees to plan change requests and reduce "last minute/just this once" workarounds. Of course, there are always going to be special requests for expedited approval. Make sure your system is flexible enough to allow for these exceptions. At Brown, there is a special line of ticketing that routes the request to key approval personnel who can approve the change and process it quickly, says Sherry. When looking at ways to reduce the approval timeline, Lindstrom says, "Change is continuous in any organization and your goals should be to make changes as quickly as you can within the realm of practical controls."

A final recommendation--automate wherever possible. Allow users to enter in their own change requests at a self-service site that feeds directly into the main ticketing and change management system. Configure the site on a wizard-type model that makes it easy for users to enter the most common requests, like new user provisioning and Web application updates.

CONTINUOUSLY ASSESS AND IMPROVE CHANGE MANAGEMENT

Over time, organizations will find it helpful to fine-tune their change management programs. As the change management administrator, Ferguson is responsible "for looking for improvement opportunities." Sometimes these opportunities are identified investigating failure points and determining whether they were caused by a lack of change management.

Auditing or performing assessments on your change management program is a useful way to measure coverage and effectiveness. Review the approval process and determine helpful metrics such as: Number of exceptions over time, are they increasing or decreasing? Or number of failures, how many unapproved/unplanned changes resulted in downtime over a given timeframe? Approval time may be streamlined by tuning the accountability flow and ensuring key approvers have time built into their day to review requests and coordinate responses. Another area for improvement is increased automation via integration with systems such as security information and event managers for better visibility into event root analysis and reduction in false positives during scheduled downtimes.

For additional guidance on change management assessment, ISACA has a useful publication entitled "Beyond Checklists: A Socratic Approach to Building a Sustainable Change Auditing Practice" that lays out a methodology for testing change management effectiveness on the basis of the 3 C's (culture, controls, and credibility.) And the Unified Compliance Framework recommends auditing change management in these seven areas:

- Acceptance
- Awareness
- Policies and Procedures
- Tools and Automation
- Skills and Expertise
- Responsibility and Accountability
- Measurement

As David Sherry says, change management is "absolutely necessary. It promotes standards, process improvement, reduces complexity and risk and provides sanity in complex environments." A small investment in change management can reap a great reward in disaster prevention. To benefit from the control and insight change management brings, organizations don't need to implement fully mature systems or spend a lot of money on expensive vendor solutions. But they do need to get a process in place and to make sure it's user-friendly enough that employees will opt-in rather than work-a-round.

The important thing is to, as Jim Ferguson advises, "Do something. Something is better than nothing. You don't need a huge, big investment. The real benefit is in defining a process and following that process."

Change Management

- ✦ Operational change management brings discipline and quality control to IS
- ✦ Management has recognised the importance of change management

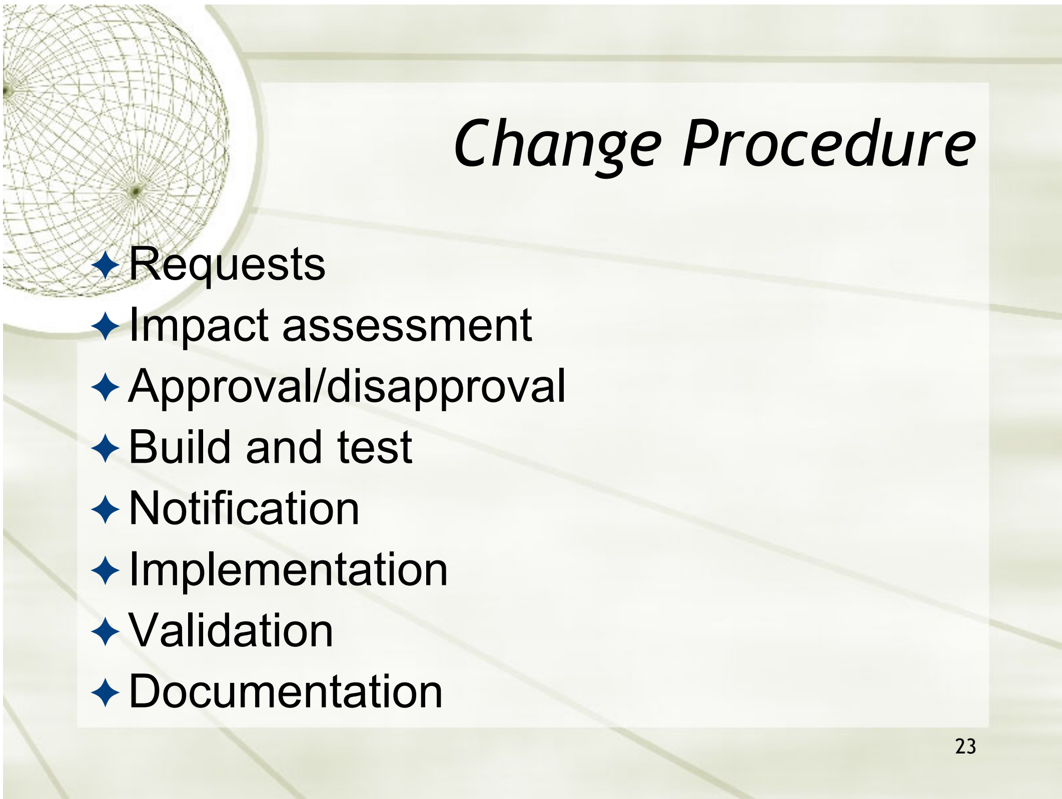
Ref: ISO27k Forum at www.ISO27001security.com

22

Operational change management brings discipline and quality control to IS. Attention to governance and formal policies and procedures will ensure its success. Adopting formalised governance and policies for operational change management delivers a more disciplined and efficient infrastructure. This formalisation requires communication; the documentation of important process workflows and personnel roles; and the alignment of automation tools, where appropriate. Where change management is non-existent, it is incumbent on IS's senior management to provide the leadership and vision to jump-start the process. By defining processes and policies, IS organisations can demonstrate increased agility in responding predictably and reliably to new business demands.

<Organisation> (hereafter called 'the company') management has recognised the importance of change management and control and the associated risks with ineffective change management and control and have therefore formulated this Change Management and Control Policy in order to address the opportunities and associated risks.

This policy applies to all parties operating within the company's network environment or utilising Information Resources. It covers the data networks, LAN servers and personal computers (stand-alone or network-enabled), located at company offices and company production related locations, where these systems are under the jurisdiction and/or ownership of the company or subsidiaries, and any personal computers, laptops, mobile device and or servers authorised to access the company's data networks. No employee is exempt from this policy.



Change Procedure

- Requests
- Impact assessment
- Approval/disapproval
- Build and test
- Notification
- Implementation
- Validation
- Documentation

23

The change management structure should be codified as an organization policy. Procedures for the operational aspects of the change management process should also be created. Change management policies and

procedures are forms of directive controls. The following subsections outline a recommended structure for a change management process.

○**Requests:** Proposed changes should be formally presented to the committee in writing. The request should include a detailed justification in the form of a business case argument for the change, focusing on the benefits of implementation and costs of not implementing. Can assign priority to these changes.

○**Impact Assessment:** Members of the committee should determine the impacts to operations regarding the decision to implement or reject the change.

○**Approval/Disapproval:** Requests should be answered officially regarding their acceptance or rejection.

○**Build and Test:** Once the proposal has been approved, the software would have to be put in an isolated environment but one that iss similar to the production system to test whether if everything works. Subsequent approvals are provided to operations support for test and integration development. A fallback plan should be in place such that the organisation would be able to recover from those unsuccessful changes. Go back to the previous working stage. The fallback has to be put in place before the testings are carried out.

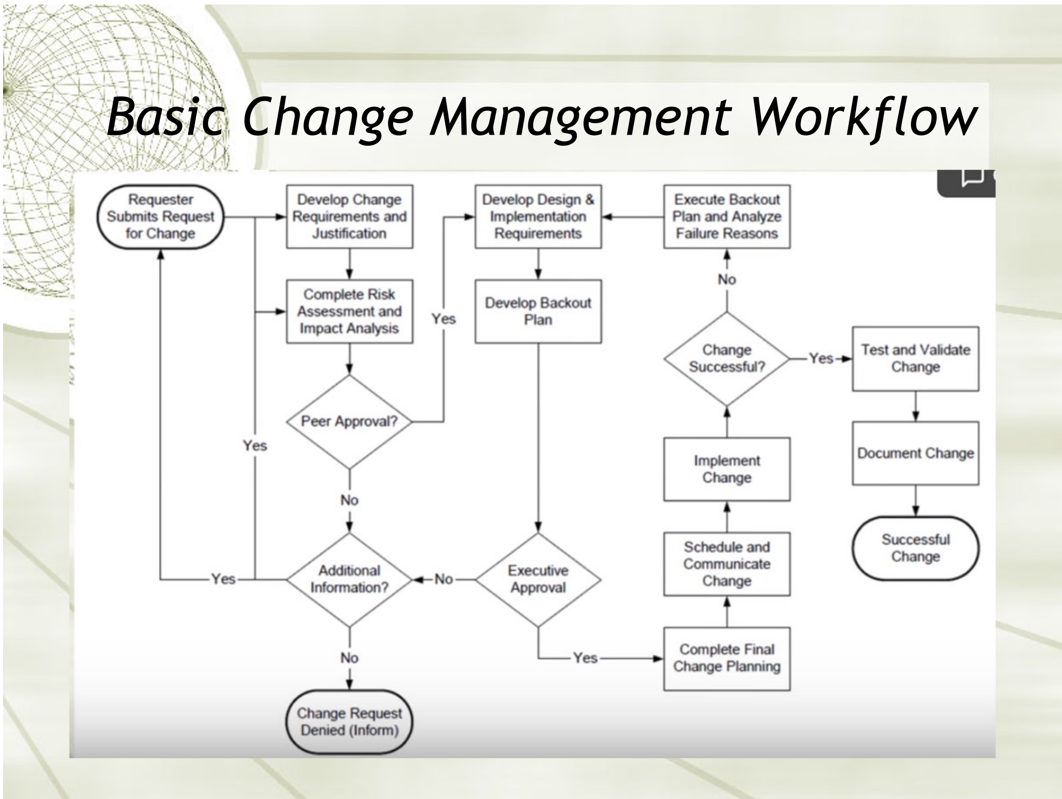
The necessary software and hardware should be tested in a nonproduction environment. All configuration changes associated with a deployment must be fully tested and documented. The security team should be invited to perform a final review of the proposed change within the test environment to ensure that no vulnerabilities are introduced into the production system. Change requests involving the removal of a software or a system component require a similar approach. The item should be removed from the test environment and have a determination made regarding any negative impacts.

○**Notification:** System users and stakeholders are notified of the proposed change and the schedule of deployment.

○**Implementation:** The change is deployed incrementally, when possible, and monitored for issues during the process.

○**Validation:** The change is validated by the operations staff to ensure that the intended machines received the deployment package. The security staff performs a security scan or review of the affected machines to ensure that new vulnerabilities are not introduced. Changes should be included in the problem tracking system until operations has ensured that no problems have been introduced.

○**Documentation:** The outcome of the system change, to include system modifications and lessons learned, should be recorded in the appropriate records. This is the way that change management typically interfaces with configuration management.



Basic Change Management Workflow

Requester Submits Request for Change

Develop Change Requirements and Justification

Complete Risk Assessment and Impact Analysis

Peer Approval?

Additional Information?

Change Request Denied (Inform)

Develop Design & Implementation Requirements

Develop Backout Plan

Executive Approval

Complete Final Change Planning

Schedule and Communicate Change

Implement Change

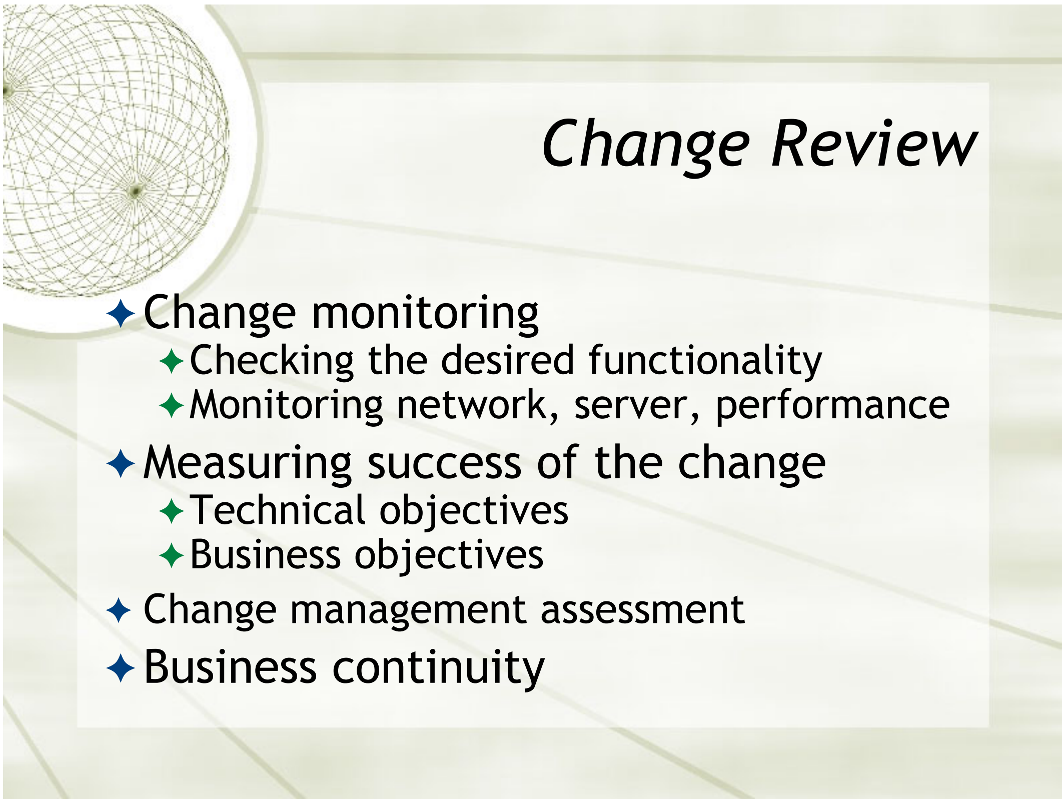
Change Successful?

Execute Backout Plan and Analyze Failure Reasons

Test and Validate Change

Document Change

Successful Change



Change Review

- Change monitoring
  - Checking the desired functionality
  - Monitoring network, server, performance
- Measuring success of the change
  - Technical objectives
  - Business objectives
- Change management assessment
- Business continuity

Importance of change monitoring: After a period of time, if a bug suddenly comes up, the organisation would still have to document the issue and escalate it.

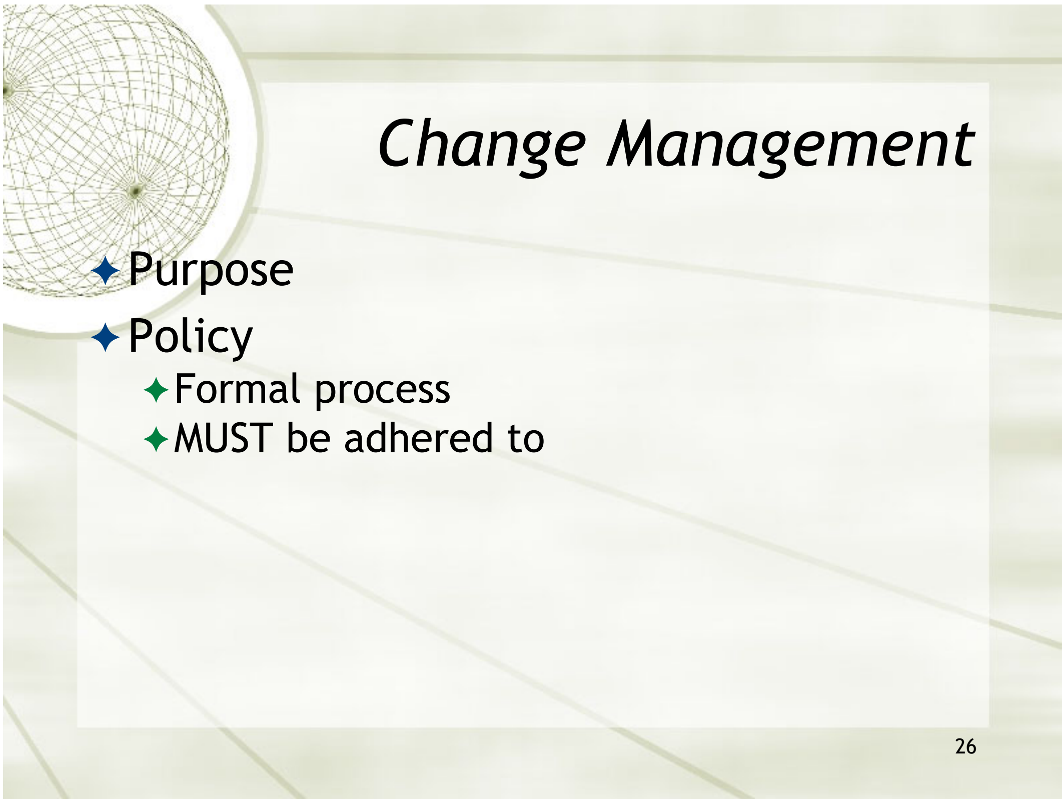
Different tools could be used to monitor these changes.

Technical objectives: whether the changes accomplishes everything that it is set to accomplish, and that there are no technical issues.

Business objectives: ensure that the changes that are made meet business objectives e.g. if it is set to increase productivity, ensure that is being met. Or if it is set to have solve certain issues, whether that goal is being met.

Assessing change management as a culture, whether it has been properly adhered to or whether the employees are not aware of it or accept the change management procedures. The organisation can run audits on the change management process to see if it is working.

If any changes are made, business continuity plans should be maintained accordingly.



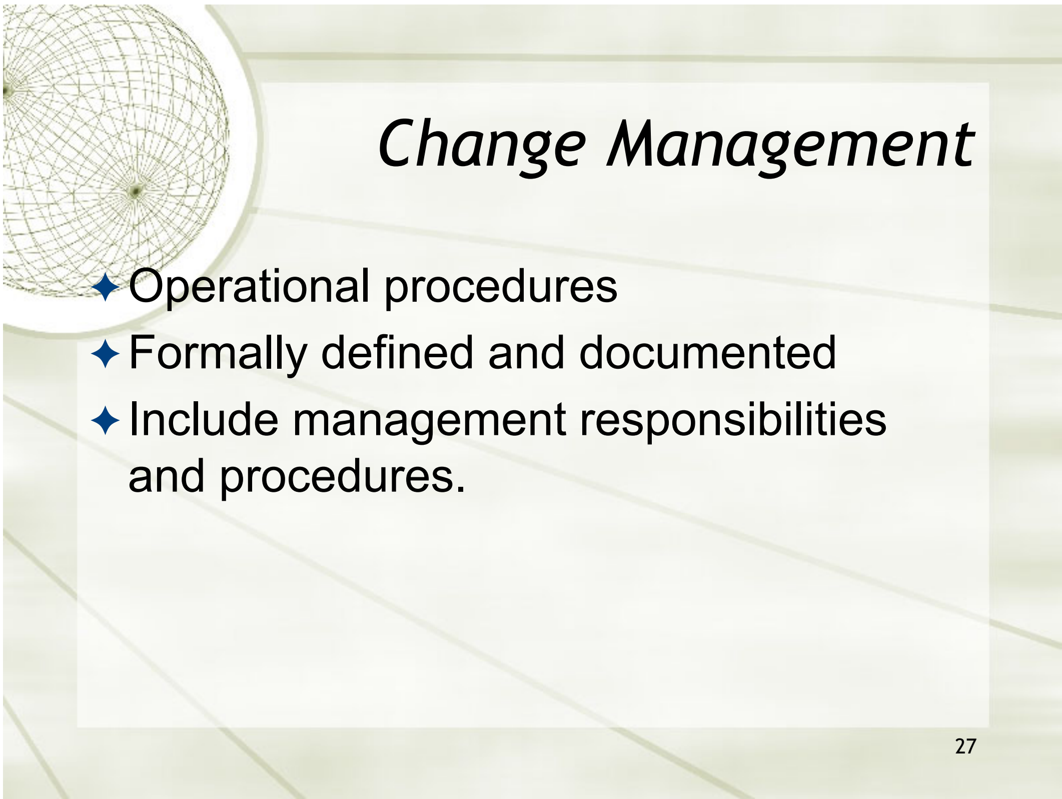
Change Management

- Purpose
- Policy
  - Formal process
  - MUST be adhered to

This policy applies to all parties operating within the company’s network environment or utilising Information Resources. It covers the data networks, LAN servers and personal computers (stand-alone or network-enabled), located at company offices and company production related locations, where these systems are under the jurisdiction and/or ownership of the company or subsidiaries, and any personal computers, laptops, mobile device and or servers authorised to access the company’s data networks. No employee is exempt from this policy.

Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorised, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.

In order to fulfil this policy, the following statements shall be adhered to:



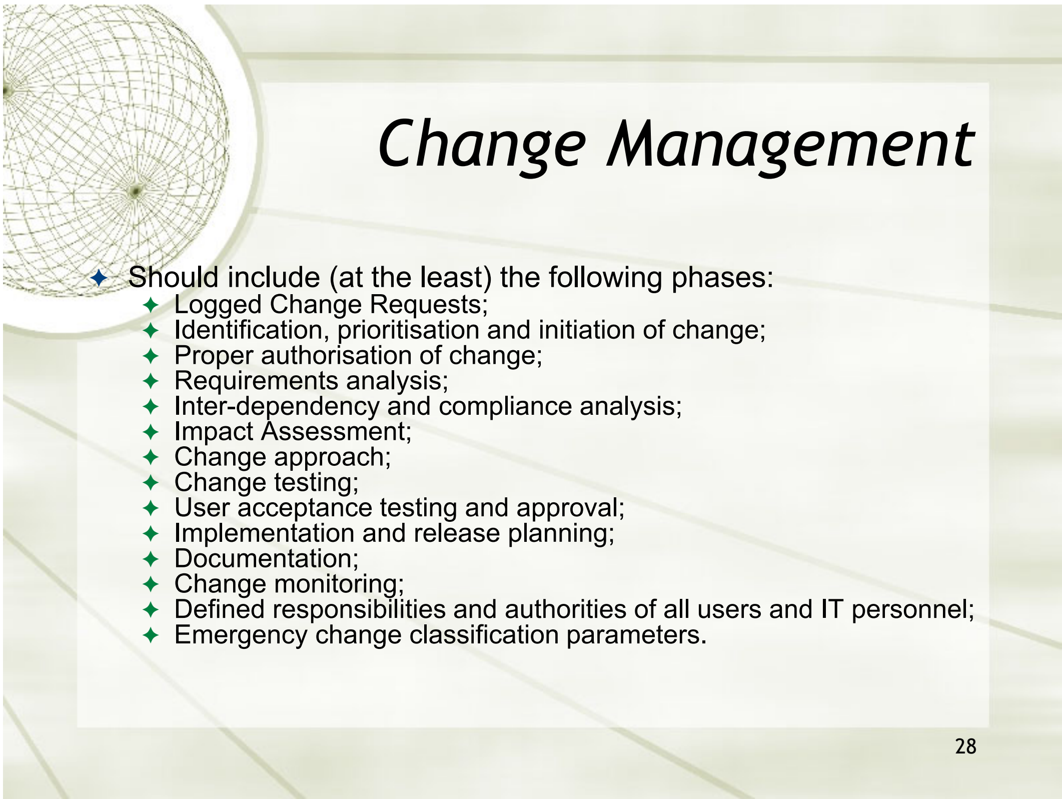
Change Management

- Operational procedures
- Formally defined and documented
- Include management responsibilities and procedures.

27

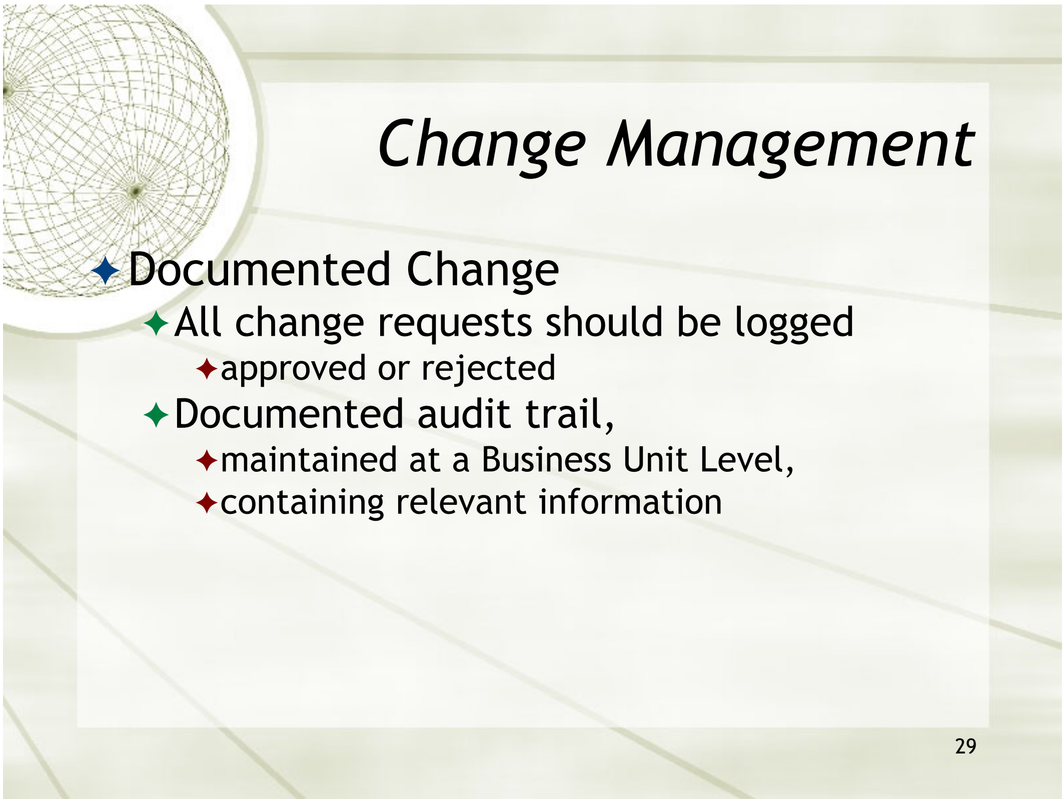
Operational Procedures

The change control process shall be formally defined and documented. A change control process shall be in place to control changes to all critical company information resources (such as hardware, software, system documentation and operating procedures). This documented process shall include management responsibilities and procedures. Wherever practicable, operational and application change control procedures should be integrated.



Change Management

- Should include (at the least) the following phases:
  - Logged Change Requests;
  - Identification, prioritisation and initiation of change;
  - Proper authorisation of change;
  - Requirements analysis;
  - Inter-dependency and compliance analysis;
  - Impact Assessment;
  - Change approach;
  - Change testing;
  - User acceptance testing and approval;
  - Implementation and release planning;
  - Documentation;
  - Change monitoring;
  - Defined responsibilities and authorities of all users and IT personnel;
  - Emergency change classification parameters.



Change Management

- Documented Change
  - All change requests should be logged
    - approved or rejected
  - Documented audit trail,
    - maintained at a Business Unit Level,
    - containing relevant information

Documented Change

All change requests shall be logged whether approved or rejected on a standardised and central system. The approval of all change requests and the results thereof shall be documented.

A documented audit trail, maintained at a Business Unit Level, containing relevant information shall be maintained at all times. This should include change request documentation, change authorisation and the outcome of the change. No single person should be able to effect changes to production information systems without the approval of other authorised personnel.

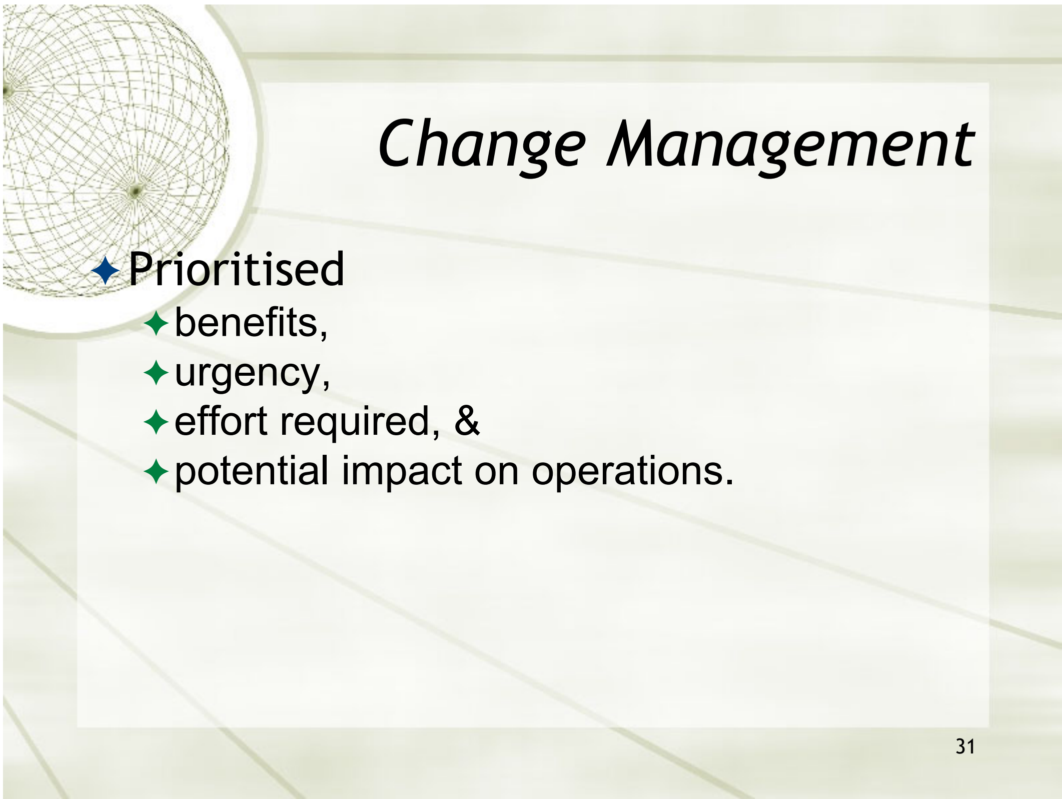
Change Management

- Risk Management
  - A risk assessment should be performed
  - Impact assessment should be performed.
  - The impact assessment should include
    - the potential effect on other information resources
    - potential cost implications.
    - consider compliance with legislative requirements and standards.

Risk Management

A risk assessment shall be performed for all changes and dependant on the outcome, an impact assessment should be performed.

The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable consider compliance with legislative requirements and standards.

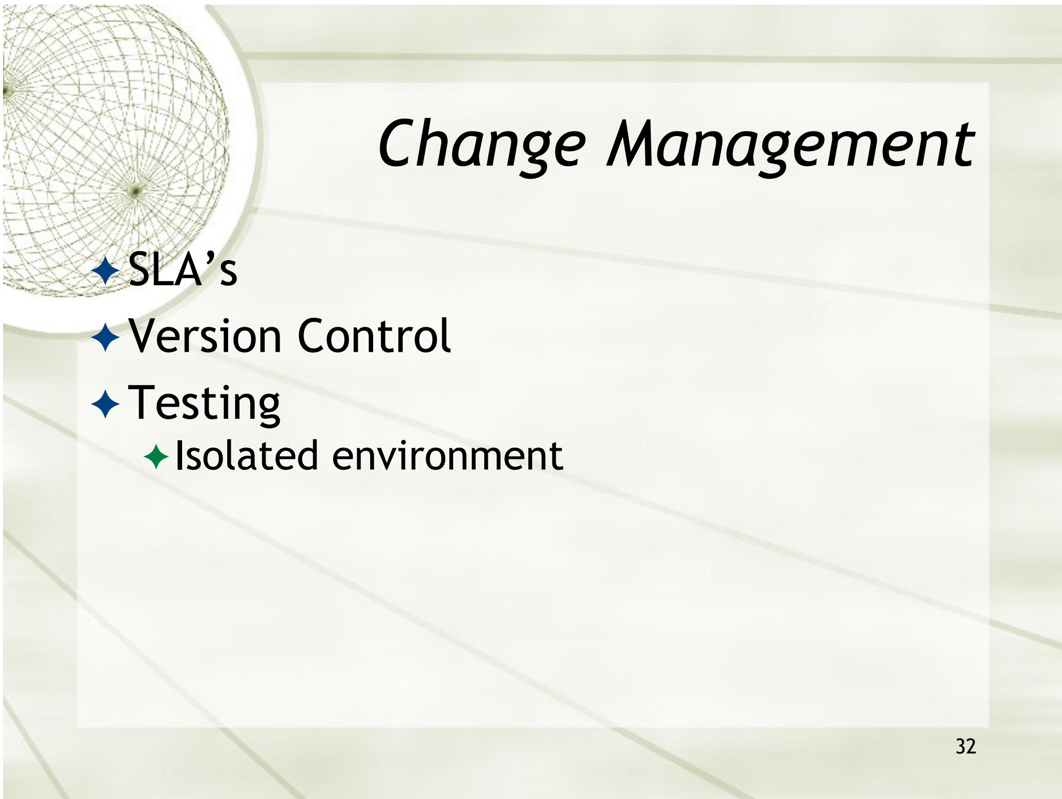


Change Management

- Prioritised
  - benefits,
  - urgency,
  - effort required, &
  - potential impact on operations.

Change Classification

All change requests shall be prioritised in terms of benefits, urgency, effort required and potential impact on operations.



Change Management

- SLA’s
- Version Control
- Testing
  - Isolated environment

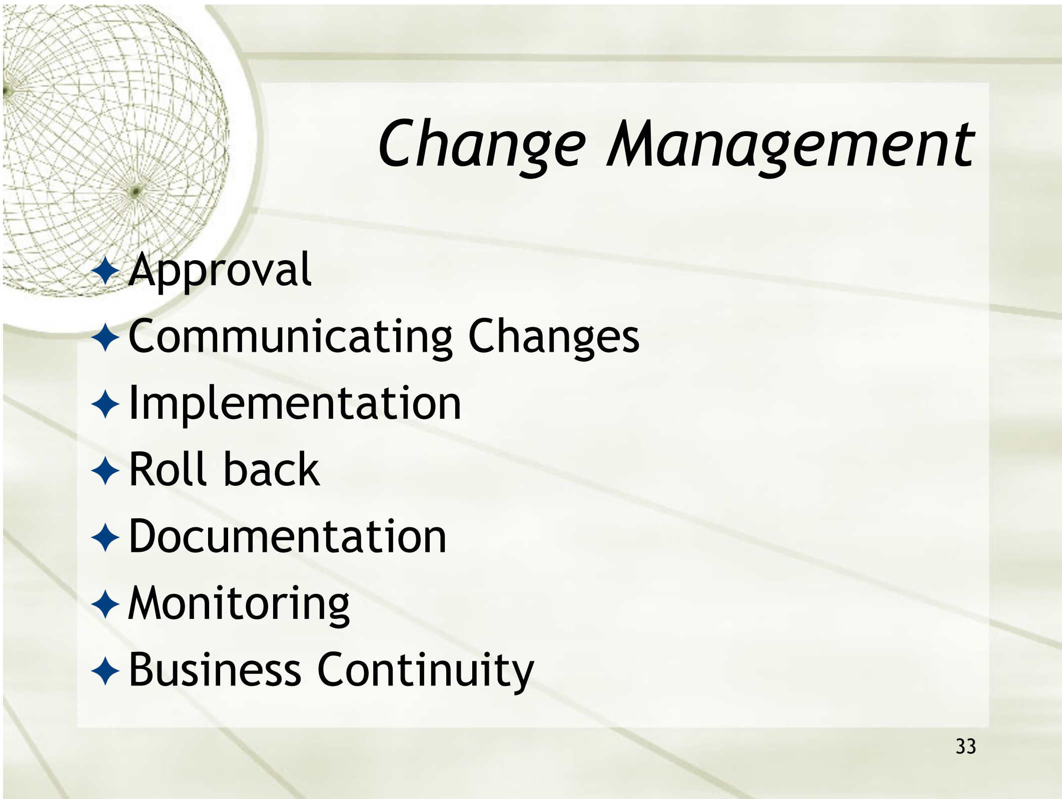
Changes affecting SLA‘s

The impact of change on existing SLA’s shall be considered. Where applicable, changes to the SLA shall be controlled through a formal change process which includes contractual amendments.

Version control

Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies.Testing

Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimise the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.



Change Management

- ✦ Approval
- ✦ Communicating Changes
- ✦ Implementation
- ✦ Roll back
- ✦ Documentation
- ✦ Monitoring
- ✦ Business Continuity

Approval

All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorised user, the impact assessment was performed and proposed changes were tested.

Communicating changes (and involve the users!)

All users, significantly affected by a change, shall be notified of the change. The user representative shall sign-off on the change. Users shall be required to make submissions and comment prior to the acceptance of the change.

Implementation

Implementation will only be undertaken after appropriate testing and approval by stakeholders. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to effort required to develop and implement said changes.

Fall back

Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures will be in place to ensure systems can revert back to what they were prior to implementation of changes.

Documentation

Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per the documentation and data retention policies.

Information resources documentation is used for reference purposes in various scenarios i.e. further development of existing information resources as well as ensuring adequate knowledge transfer in the event of the original developer and/or development house being unavailable. It is therefore imperative that information resources documentation is complete, accurate and kept up to date with the latest changes. Policies and procedures, affected by software changes, shall be updated on completion of each change.

Business Continuity Plans (BCP)

Business continuity plans shall be updated with relevant changes, managed through the change control process. Business continuity plans rely on the completeness, accuracy and availability of BCP documentation. BCP documentation is the road map used to minimise disruption to critical business processes where possible, and to facilitate their rapid recovery in the event of disasters.

Emergency Changes

Specific procedures to ensure the proper control, authorisation, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as Emergency changes.

Change Monitoring

All changes will be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

Change Management

- Roles and Responsibilities
  - Members of the Board (Change advisory board (CAB))
  - Information Security Manager
  - Operations Manager
  - IT Manager
  - Data Owner
- IT governance
- Policy Access

Members of the Board

•Members of the Board shall ensure that the necessary information security controls are implemented and complied with as per this policy.

Information Security Manager

•Establish and revise the information security strategy, policy and standards for change management and control with input from interest groups and subsidiaries;

•Facilitate and co-ordinate the necessary counter measures to change management and control initiatives and evaluate such policies and standards;

•Establish the security requirements for change management and control directives and approval of the change management and control standards and change control/ version control products;

•Co-ordinate the overall communication and awareness strategy for change management;

•Acts as the management champion for change management and control;

•Provide technical input to the service requirements and co-ordinate affected changes to SLA’s where applicable.

•Establish and co-ordinate appropriate interest group forums to represent, feedback, implement and monitor change management and control initiatives; and

•Co-ordinate the implementation of new or additional security controls for change management.

Operations Manager

•Implement, maintain and update the change management and control strategy, baselines, standards, policies and procedures with input from all stakeholders;

•Approve and authorise change management and control measures on behalf of the <Organisation>;

•Ensure that all application owners are aware of the applicable policies, standards, procedures and guidelines for change management and control;

•Ensure that policy, standards and procedural changes are communicated to applicable owners and management forums;

•Appoint the necessary representation to the interest groups and other forums created by each company for Information Security Management relating to change management and control;

•Establish and revise the information security strategy, policy and standards for change management and control;

•Facilitate and co-ordinate the necessary change management and control initiatives within each company;

•Report and evaluate changes to change management and control policies and standards;

•Co-ordinate the overall communication and awareness strategy for change management and control;

•Co-ordinate the implementation of new or additional security controls for change management and control

•Review the effectiveness of change management and control strategy and implement remedial controls where deficits are identified;

•Provide regular updates on change management and control initiatives and the suitable application;

•Evaluate and recommend changes to change management/ version control solutions; and

•Co-ordinate awareness strategies and rollouts to effectively communicate change management and control mitigation solutions in each company.

•Establish and implement the necessary standards and procedures that conform to the Information Security policy;

•Responsible for approving, authorising, monitoring and enforcing change management initiatives and related security controls within all <ORGANISATION> companies and divisions;

•Ensure that all solution owners are aware of policies, standards, procedures and guidelines for change management and control.

•Ensure the compliance of this policy and report deviations to the Information Manager.

IT Service Provider

•Shall comply with all change management and control statements of this policy.

Solution Owners

•Shall comply with all information security policies, standards and procedures for change management and control; and

•Report all deviations.

IT Governance Value statement

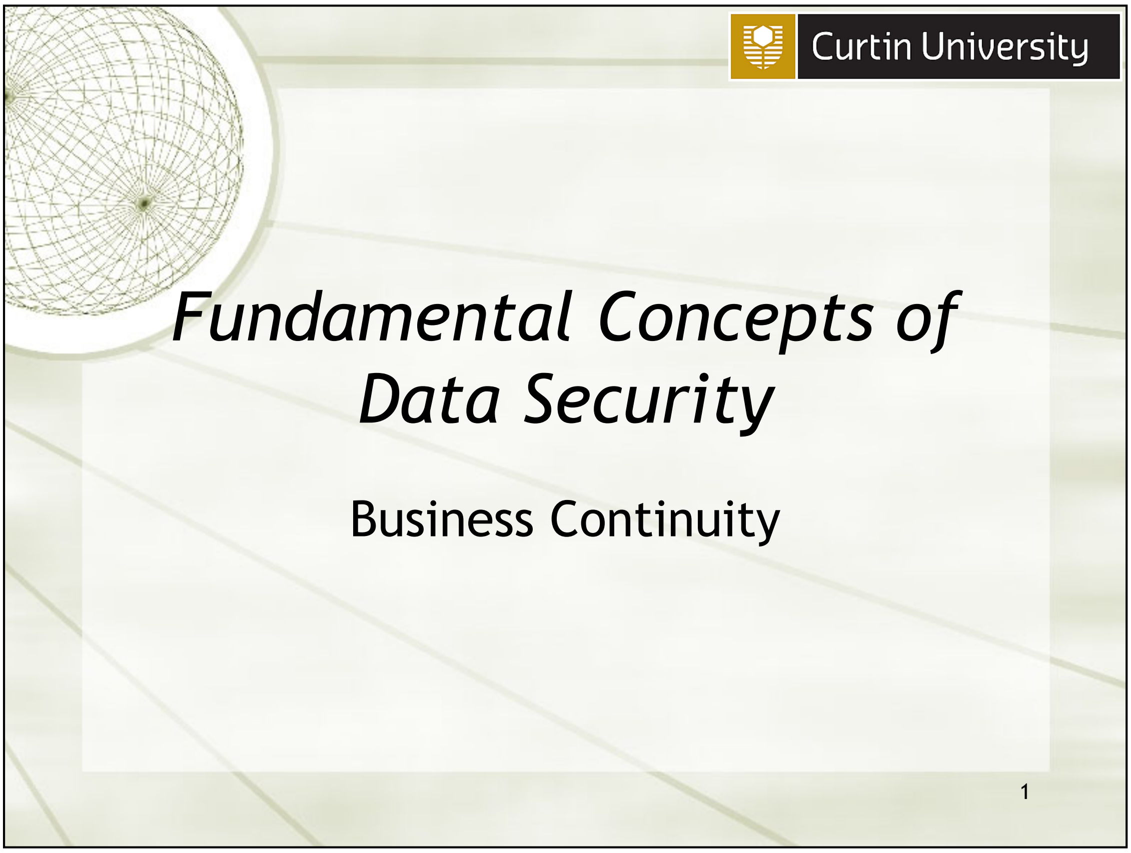
•Changes that materially affect the financial process must be evaluated and reported at some interval. Financial system upgrades or replacements will require new certification. The implication is that Sarbanes-Oxley compliance is reliant on the changes you make to the operational systems and procedures.

Policy Access Considerations

•All IT personnel

•Business Unit Management teams

•Executive Directors



Curtin University

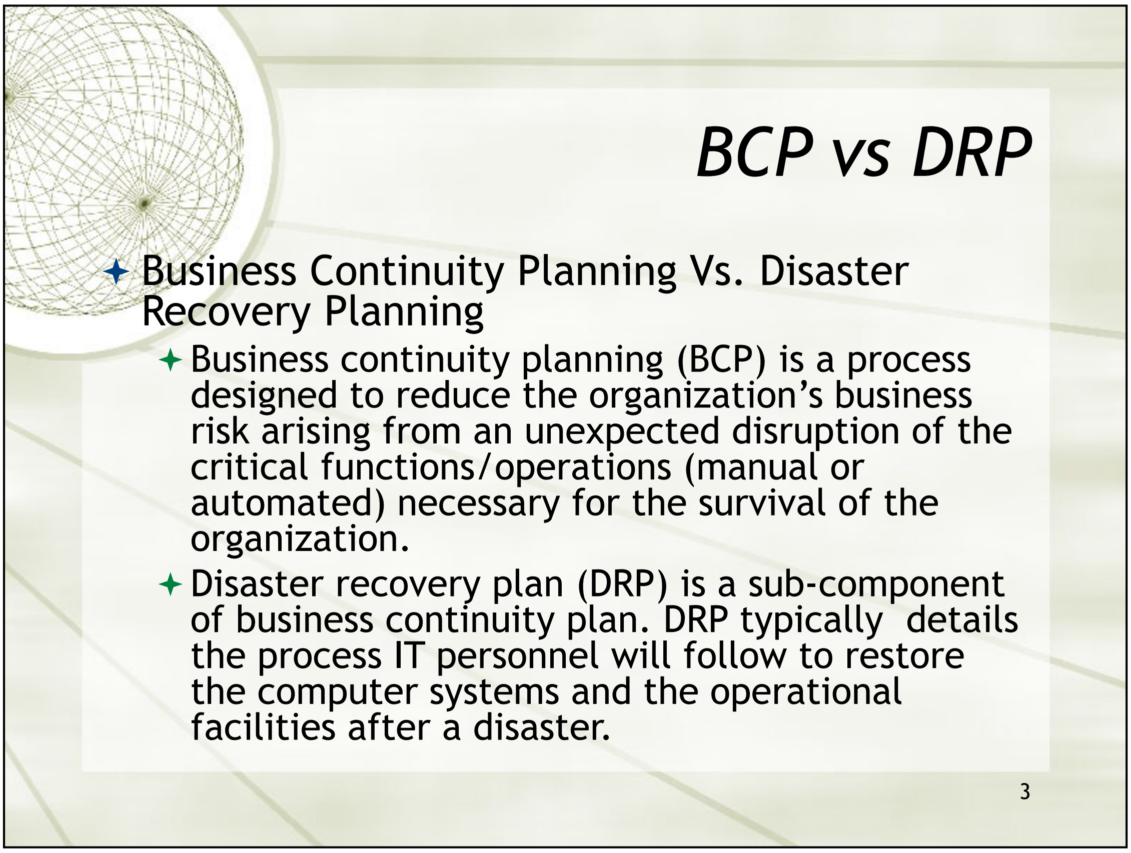
Fundamental Concepts of Data Security

Business Continuity

1

Comprehensive approach to business continuity plan

- Prevention: risk management plan (this lecture) – what to do to prevent incidents
- Preparedness: business impact analysis – if incidents do happen, what would be the impact
- Response: incident response plan – what to do when incidents happen
- Recovery: recovery plan – how to recover after an incident/disaster



BCP vs DRP

- Business Continuity Planning Vs. Disaster Recovery Planning
  - Business continuity planning (BCP) is a process designed to reduce the organization's business risk arising from an unexpected disruption of the critical functions/operations (manual or automated) necessary for the survival of the organization.
  - Disaster recovery plan (DRP) is a sub-component of business continuity plan. DRP typically details the process IT personnel will follow to restore the computer systems and the operational facilities after a disaster.

BCP purposes:

- Reduce business risks
- Make sure that any disruptions and losses due to the incidents or disasters are minimised

DRP purposes: (part of RBCP) aka Contingency Plans

- Coordinating recovery after a disaster
- Often referred to as restoring information system and operational facilities after a disaster.

Preparing for an emergency typically involves:

- Planning
- Practicing
- Rehearsing
- Evaluating
- Adjusting

There should be well documented procedures, strategies etc. This requires setting up an Emergency Response Team and inclusion of that information in BCP. Team should have general and local responsibilities. They should for example facilitate evacuation and shut down, protect companies properties and potentially cooperate with local authorities such as fire department. Depending on the type of disasters, there could be different plans.

An emergency is a potentially life-threatening situation, usually occurring suddenly and unexpectedly. Emergencies may be the result of natural and/or human causes.

Preparing for emergencies involves planning, practicing, evaluating, and adjusting.

An immediate response is critical in emergencies.

The Emergency Planning and Community Right-to-Know Act has the following four main components: emergency planning, emergency notification, information requirements, and toxic chemical release reporting.

For proper coordination of the internal emergency response, it is important that one person be in charge and that everyone involved knows who that person is.

Since there is no way to predict when first aid might be needed, part of preparing for emergencies should include training employees to administer first aid. In certain cases, OSHA requires that companies have at least one employee on-site who has been trained in first aid.

In addition to providing first aid training, it is important to have well-stocked first aid kits readily available, have personal protective devices available, post emergency telephone numbers, and keep all employees informed.

The OSHA standard for evacuation planning is 29 CFR 1910.38. This standard requires a written plan for evaluating the facility in the event of an emergency. Critical elements of the plan are as follows: marking of exit routes, communications, outside assembly, and training.

A company's emergency action plan should be a collection of small plans for each anticipated emergency. These plans should have the following components: procedures, coordination, assignments/responsibilities, accident prevention strategies, and schedules.

EAPs should be customized so that they are location-specific by including a map, an organization chart, local coordination information, and local training schedules.

An emergency response team is a special team to handle general and localized emergencies to facilitate evacuation and shutdown, protect and salvage company property, and work with civil authorities.

An emergency response network is a network of emergency response teams that covers a designated geographical area.

Computers can help simplify some of the complications brought by advances in technology. Expert systems mimic human thought processes in making decisions on an if-then basis regarding emergency responses.

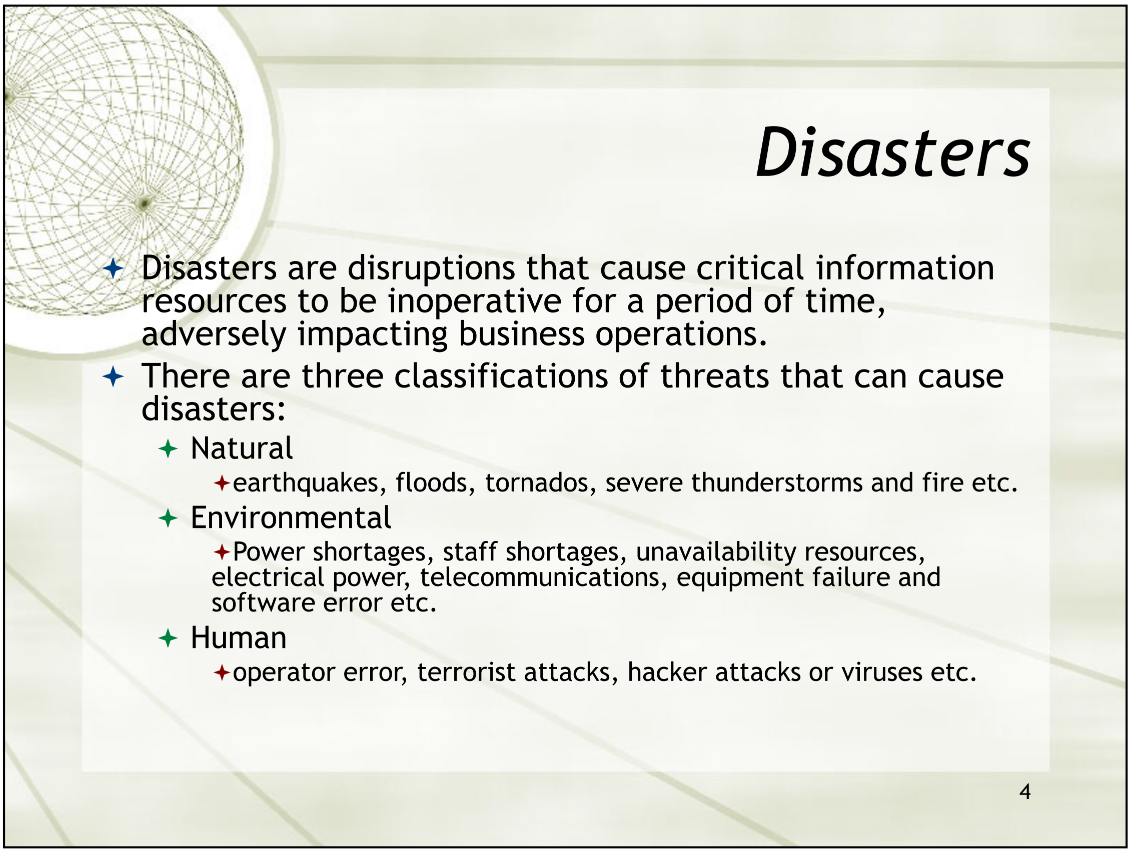
Trauma is psychological stress. It typically results from exposure to a disaster or emergency so shocking that it impairs a person's sense of security or well being. Trauma left untreated can manifest itself as post-traumatic stress disorder. This disorder is characterized by intrusive thoughts, flashbacks, paranoia, concentration difficulties, rapid heartbeat, and irritability.

A disaster recovery plan should have at least the following components: recovery coordinator, recovery team, recovery analysis and planning, damage assessment and salvage operations, recovery communications, and employee support and assistance.

Employers can help decrease the likelihood of a terrorist attack on their facilities by taking the following actions: run a safe and caring operation, listen to employees, train employees, communicate, know your personnel, empower personnel, harden the site against external threats and restrict access, remove any barriers to clear visibility around the facility, have and enforce parking and delivery regulations, make sure that visitors can be screened from a distance, keep all unstaffed entrance doors locked from the outside and alarmed, make air intakes and other utilities inaccessible to all but designated personnel, ensure contractors and visitors wear badges, have an emergency response plan and practice it on a regular basis, be cautious of what information is placed on your company’s website, keep up to date with the latest safety and security strategies, protect the integrity of your facility’s key system.

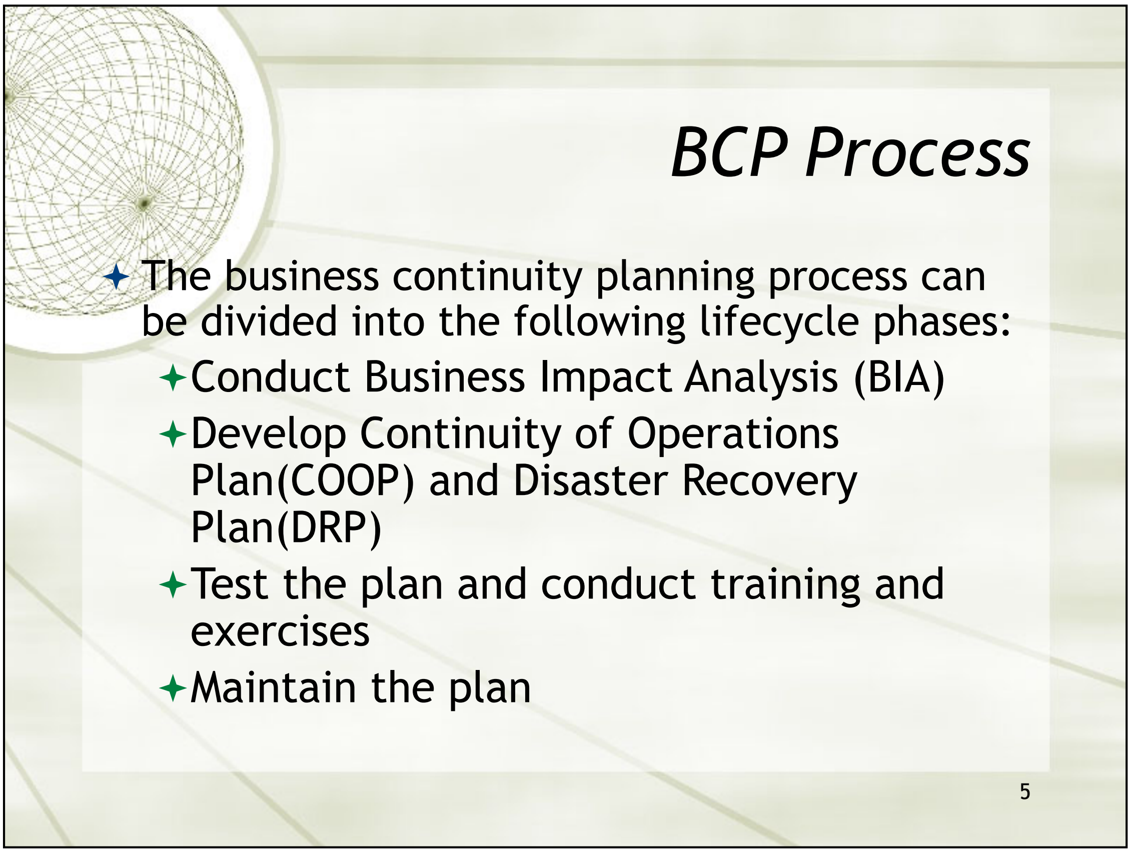
Secure hazardous materials so that terrorists cannot gain access to them for use in making bombs and other weapons of mass destruction. A hazmat security plan should have two components: personnel security and physical security.

All systems, conditions, and potential hazards should be checked and corrected as appropriate before resuming business after a disaster.



Disasters

- Disasters are disruptions that cause critical information resources to be inoperative for a period of time, adversely impacting business operations.
- There are three classifications of threats that can cause disasters:
  - Natural
    - earthquakes, floods, tornados, severe thunderstorms and fire etc.
  - Environmental
    - Power shortages, staff shortages, unavailability resources, electrical power, telecommunications, equipment failure and software error etc.
  - Human
    - operator error, terrorist attacks, hacker attacks or viruses etc.



BCP Process

- The business continuity planning process can be divided into the following lifecycle phases:
  - Conduct Business Impact Analysis (BIA)
  - Develop Continuity of Operations Plan(COOP) and Disaster Recovery Plan(DRP)
  - Test the plan and conduct training and exercises
  - Maintain the plan

5

Although no specific scientific equation must be followed to create continuity plans, certain best practices have proven themselves over time. The National Institute of Standards and Technology (NIST) is responsible for developing best practices and standards as they pertain to U.S. government and military environments. NIST outlines the following steps in its Special Publication 800-34, Continuity Planning Guide for Information Technology Systems:

1. *Develop the continuity planning policy statement.* Write a policy that provides the guidance necessary to develop a BCP, and that assigns authority to the necessary roles to carry out these tasks.

2. *Conduct the business impact analysis (BIA).* Identify critical functions and systems and allow the organization to prioritize them based on necessity. Identify vulnerabilities and threats, and calculate risks.

3. *Identify preventive controls.* Once threats are recognized, identify and implement controls and countermeasures to reduce the organization’s risk level in an economical manner.

4. *Develop recovery strategies.* Formulate methods to ensure systems and critical functions can be brought online quickly.

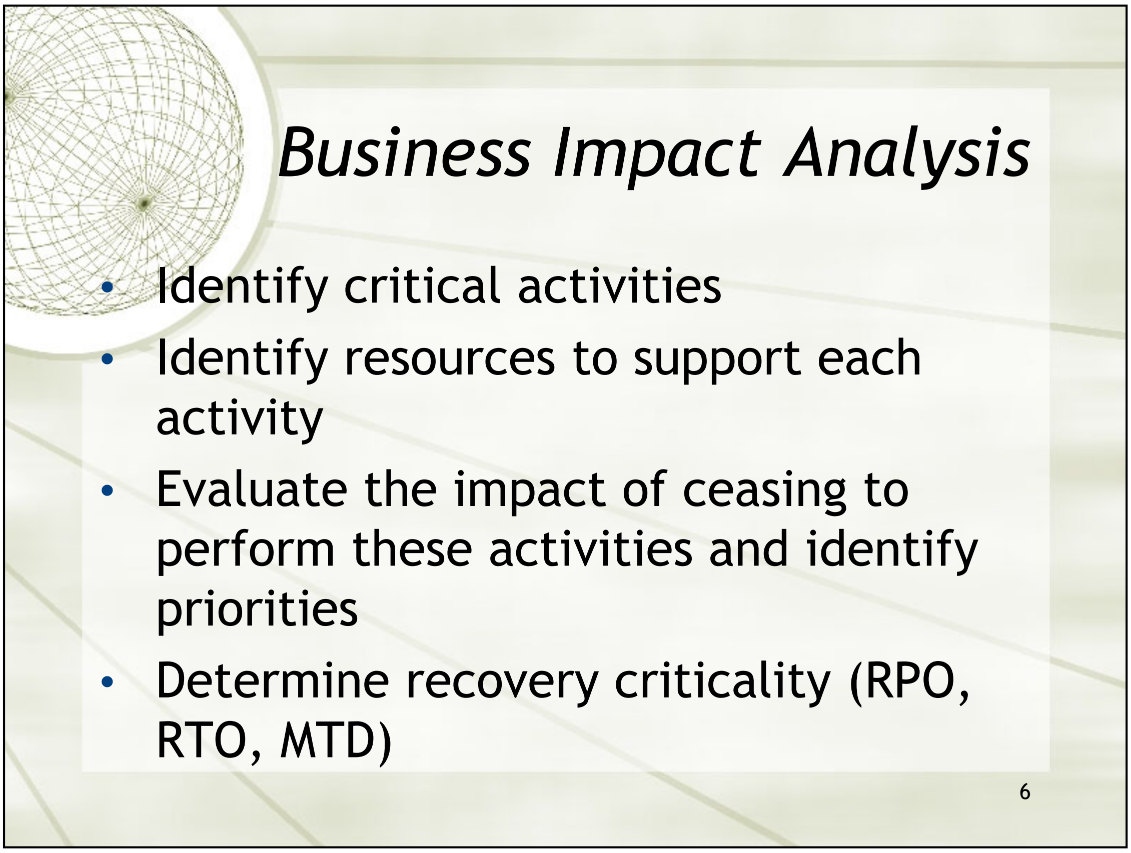
5. *Develop the contingency plan.* Write procedures and guidelines for how the organization can still stay functional in a crippled state.

6. *Test the plan and conduct training and exercises.* Test the plan to identify deficiencies in the BCP, and conduct training to properly prepare individuals on their expected tasks.

7. *Maintain the plan.* Put in place steps to ensure the BCP is a living document that is updated regularly.

The BCP effort has to result in a sustainable, long-term program that serves its purpose—assisting the organization in the event of a disaster. The effort must be well thought out and methodically executed. It must not be perceived as a mere “public relations” effort to make it simply appear that the organization is concerned about disaster response. The initiation process for BCP might include the following:

- Setting up a budget and staff for the program before the BCP process begins. Dedicated personnel and dedicated hours are essential for executing something as labor-intensive as a BCP.
- Setting up the program would include assigning duties and responsibilities to the BCP coordinator and to representatives from all of the functional units of the organization.
- Senior management should kick off the BCP with a formal announcement or, better still, an organization-wide meeting to demonstrate high-level support.
- Awareness-raising activities to let employees know about the BCP program and to build internal support for it.
- Establishment of skills training for the support of the BCP effort.
- The start of data collection from throughout the organization to aid in crafting various continuity options.
- Putting into effect “quick wins” and gathering of “low-hanging fruit” to show tangible evidence of improvement in the organization’s readiness, as well as improving readiness.



Business Impact Analysis

- Identify critical activities
- Identify resources to support each activity
- Evaluate the impact of ceasing to perform these activities and identify priorities
- Determine recovery criticality (RPO, RTO, MTD)

6

Business Impact Analysis is assisting the design of our contingency which is assuming that bad things will happen. BIA is in the Preparedness stage.

Risk Management includes controls that help the organisation prevent bad things from happening. Risk Management is in the Prevention stage.

Three steps are typically involved in accomplishing the BIA:

1. Determine mission/business processes and recovery criticality. Mission/Business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum time that an organization can tolerate while still maintaining the mission.

2. Identify resource requirements. Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.

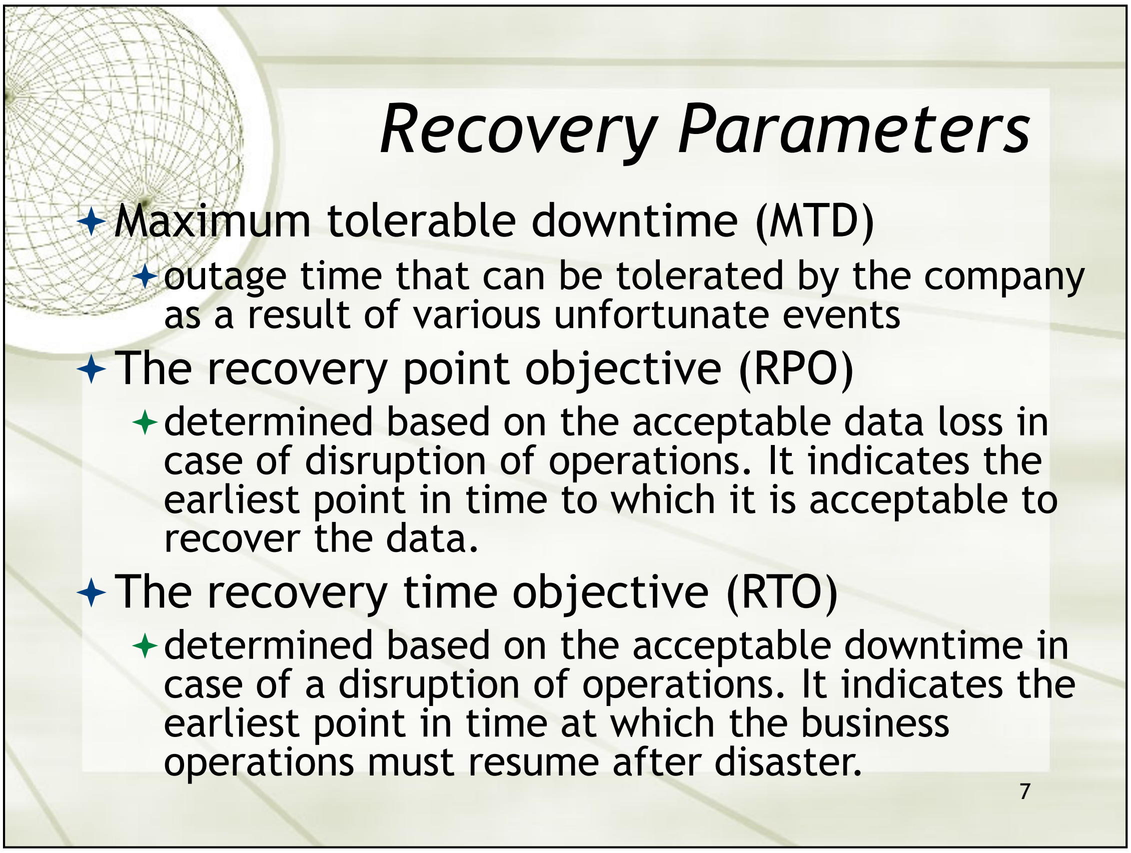
3. Identify recovery priorities for system resources. Based upon the results from the previous activities, system resources can be linked more clearly to critical mission/business processes and functions. Priority levels can be established for sequencing recovery activities and resources. **Evaluate the impact of ceasing to perform these activities and identify priorities/ assign priorities**

4. Identify an acceptable level of loss may pertain to recovery criticality (recovery parameters)

The ISCP Coordinator should next analyze the supported mission/business processes and with the process owners, leadership and business managers determine the acceptable downtime if a given process or specific system data were disrupted or otherwise unavailable. Downtime can be identified in several ways.

- **Maximum Tolerable Downtime (MTD)**. The MTD represents the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave contingency planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content.
- **Recovery Time Objective (RTO)**. RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD. When it is not feasible to immediately meet the RTO and the MTD is inflexible, a Plan of Action and Milestone should be initiated to document the situation and plan for its mitigation.
- **Recovery Point Objective (RPO)**. The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. Unlike RTO, RPO is not considered as part of MTD. Rather, it is a factor of how much data loss the mission/business process can tolerate during the recovery process.

Because the RTO must ensure that the MTD is not exceeded, the RTO must normally be shorter than the MTD. For example, a system outage may prevent a particular process from being completed, and because it takes time to reprocess the data, that additional processing time must be added to the RTO to stay within the time limit established by the MTD.



Recovery Parameters

- Maximum tolerable downtime (MTD)
  - outage time that can be tolerated by the company as a result of various unfortunate events
- The recovery point objective (RPO)
  - determined based on the acceptable data loss in case of disruption of operations. It indicates the earliest point in time to which it is acceptable to recover the data.
- The recovery time objective (RTO)
  - determined based on the acceptable downtime in case of a disruption of operations. It indicates the earliest point in time at which the business operations must resume after disaster.

7

The BIA identifies which of the company's critical systems are needed for survival and estimates the outage time that can be tolerated by the company as a result of various unfortunate events. The outage time that can be endured by a company is referred to as the ***maximum tolerable downtime (MTD)*** or ***maximum period time of disruption (MPTD)***

The following are some MTD estimates that an organization may use. Note that these are sample estimates that will vary from organization to organization and from business unit to business unit:

- **Nonessential** 30 days
- **Normal** 7 days
- **Important** 72 hours
- **Urgent** 24 hours
- **Critical** Minutes to hours

Each business function and asset should be placed in one of these categories, depending upon how long the company can survive without it. These estimates will help the company determine what backup solutions are necessary to ensure the availability of these resources. The shorter the MTD, the higher priority of recovery for the function in question. Thus, the items classified as Urgent should be addressed before those classified as Normal.

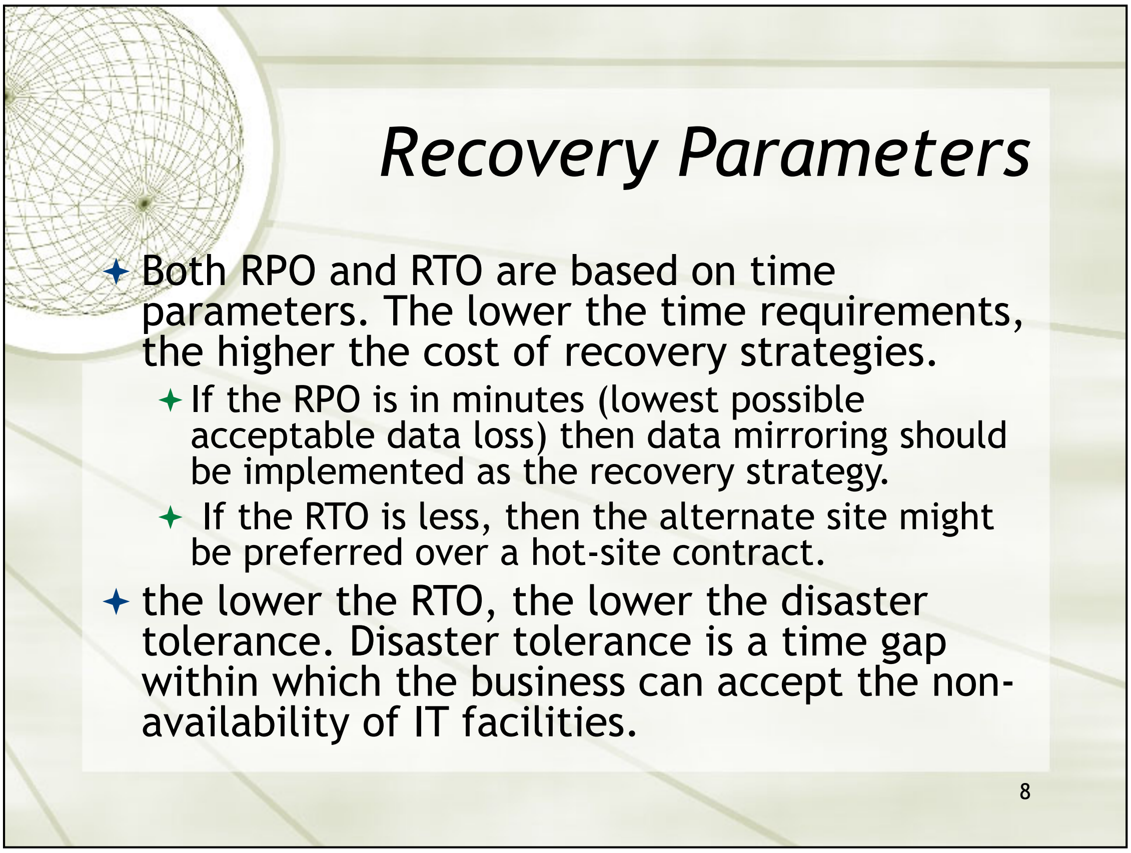
For example, if being without a T1 communication line for three hours would cost the company $130,000, the T1 line could be considered Critical and thus the company should put in a backup T1 line from a different carrier. If a server going down and being unavailable for ten days will only cost the company $250 in revenue, this would fall into the Normal category, and thus the company may not need to have a fully redundant server waiting to be swapped out. Instead, the company may choose to count on its vendor's service level agreement (SLA), which may promise to have it back online in eight days.

Sometimes the MTD will depend in large measure on the type of business in question. For instance, a call center—a vital link to current and prospective clients—will have a short MTD, perhaps measured in minutes instead of weeks. A common solution is to split up the calls through multiple call centers placed in differing locales. If one call center is knocked out of service, the other one can temporarily pick up the load. Manufacturing can be handled in various ways. Examples include subcontracting the making of products to an outside vendor, manufacturing at multiple sites, and warehousing an extra supply of products to fill gaps in supply in case of disruptions to normal manufacturing.

The ***Recovery Time Objective (RTO)*** is the earliest time period and a service level within which a business process must be restored after a disaster to avoid unacceptable consequences associated with a break in business continuity. The RTO value is smaller than the MTD value, because the MTD value represents the time after which an inability to recover significant operations will mean severe and perhaps irreparable damage to the organization's reputation or bottom line. The RTO assumes that there is a period of acceptable downtime. This means that a company can be out of production for a certain period of time (RTO) and still get back on its feet. But if the company cannot get production up and running within the MTD window, the company is sinking too fast to properly recover.

The ***Work Recovery Time (WRT)*** is the remainder of the overall MTD value. RTO usually deals with getting the infrastructure and systems back up and running, and WRT deals with restoring data, testing processes, and then making everything "live" for production purposes.

The ***Recovery Point Objective (RPO)*** is the acceptable amount of data loss measured in time. This value represents the earliest point in time at which data must be recovered. The higher the value of data, the more funds or other resources that can be put into place to ensure a smaller amount of data is lost in the event of a disaster.



Recovery Parameters

- Both RPO and RTO are based on time parameters. The lower the time requirements, the higher the cost of recovery strategies.
  - If the RPO is in minutes (lowest possible acceptable data loss) then data mirroring should be implemented as the recovery strategy.
  - If the RTO is less, then the alternate site might be preferred over a hot-site contract.
- the lower the RTO, the lower the disaster tolerance. Disaster tolerance is a time gap within which the business can accept the non-availability of IT facilities.

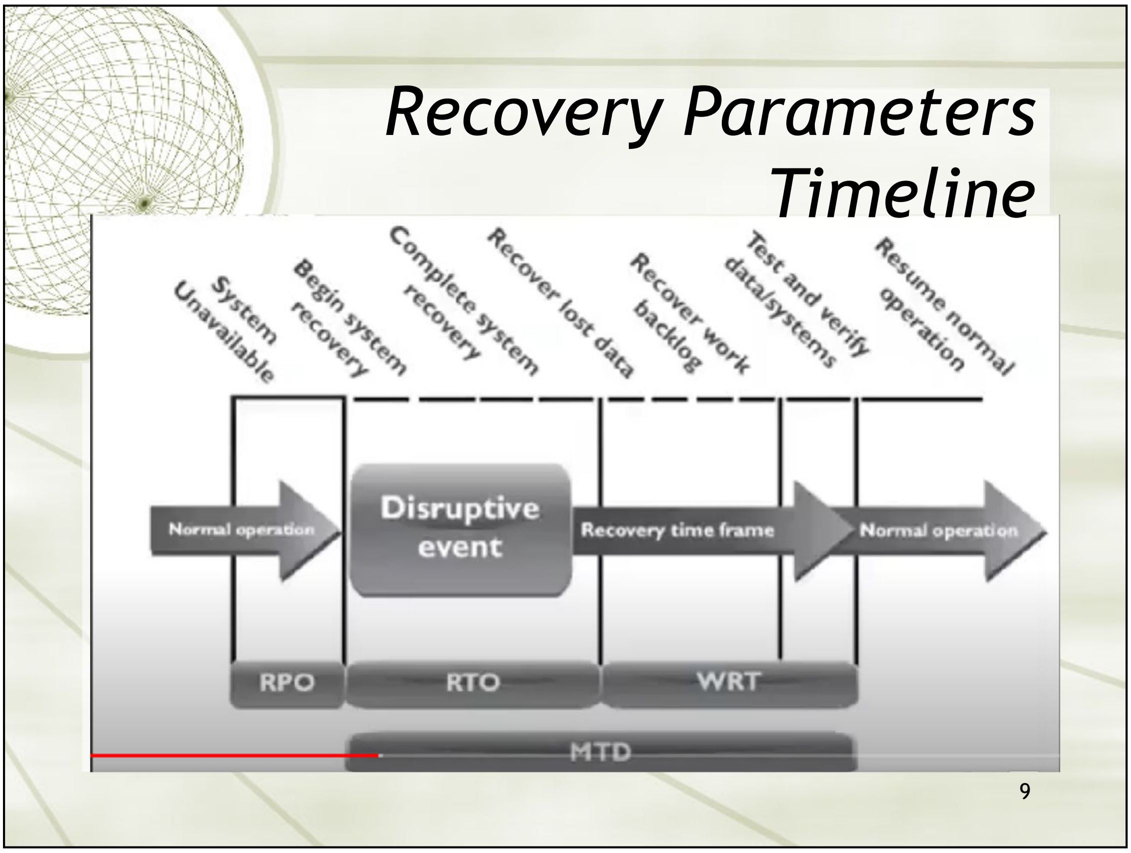
8

The RTO, RPO, and WRT values are critical to understand because they will be the basic foundational metrics used when determining the type of recovery solutions a company must put into place, so let's dig a bit deeper into them. RTO is the duration of time and a service level that a business process must be restored to in order to ensure that unacceptable consequences associated with a disaster are not endured. Let's say a company has determined that if it is unable to process product order requests for 12 hours, the financial hit will be too large for it to survive. So the company develops methods to ensure that orders can be processed manually if their automated technological solutions become unavailable. But if it takes the company 24 hours to actually stand up the manual processes, the company could be in a place operationally and financially where it can never fully recover. So RTO deals with "how long do we have to get everything up and working again?"

Now let's say that the same company experienced a disaster and got its manual processes up and running within two hours, so it met the RTO requirement. But just because business processes are back in place, we still might have a critical problem. The company has to restore the data it lost during the disaster. It does no good to restore data that is a week old. The employees need to have access to the data that was being processed right before the disaster hit. If the company can only restore data that is a week old, then all the orders that were in some stage of being fulfilled over the last seven days could be lost. If the company makes an average of

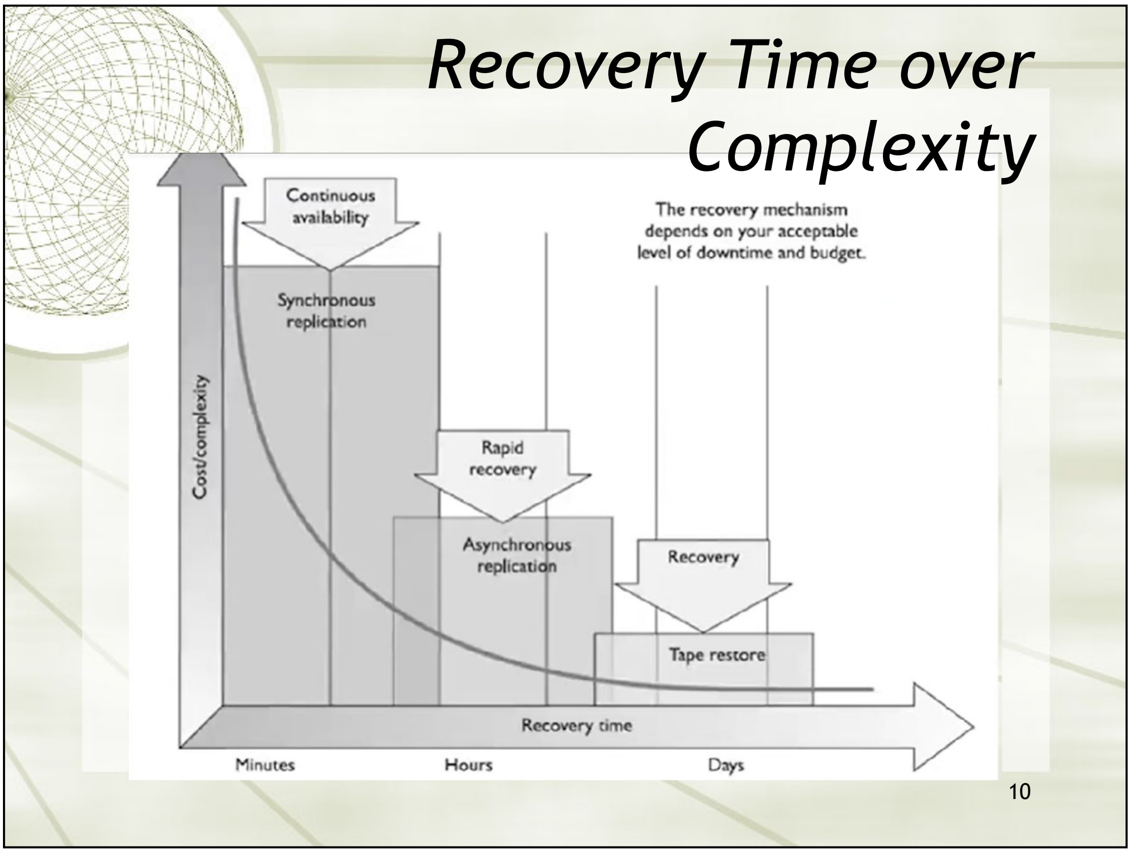
$25,000 per day in orders and all the order data was lost for the last seven days, this can result in a loss of $175,000 and a lot of unhappy customers. So just getting things up and running (RTO) is part of the picture. Getting the necessary data in place so that business processes are up to date and relevant (RPO) is just as critical.

The actual MTD, RTO, and RPO values are derived during the BIA. The impact analysis is carried out to be able to apply criticality values to specific business functions, resources, and data types. The company must have data restoration capabilities in place to ensure that mission-critical data is never older than one minute. The company cannot rely on something as slow as backup tape restoration, but must have a high-availability data replication solution in place. The RTO value for mission-critical data processing is two minutes or less. This means that the technology that carries out the processing functionality for this type of data cannot be down for more than two minutes. The company may choose to have a cluster technology in place that will shift the load once it notices that a server goes offline.



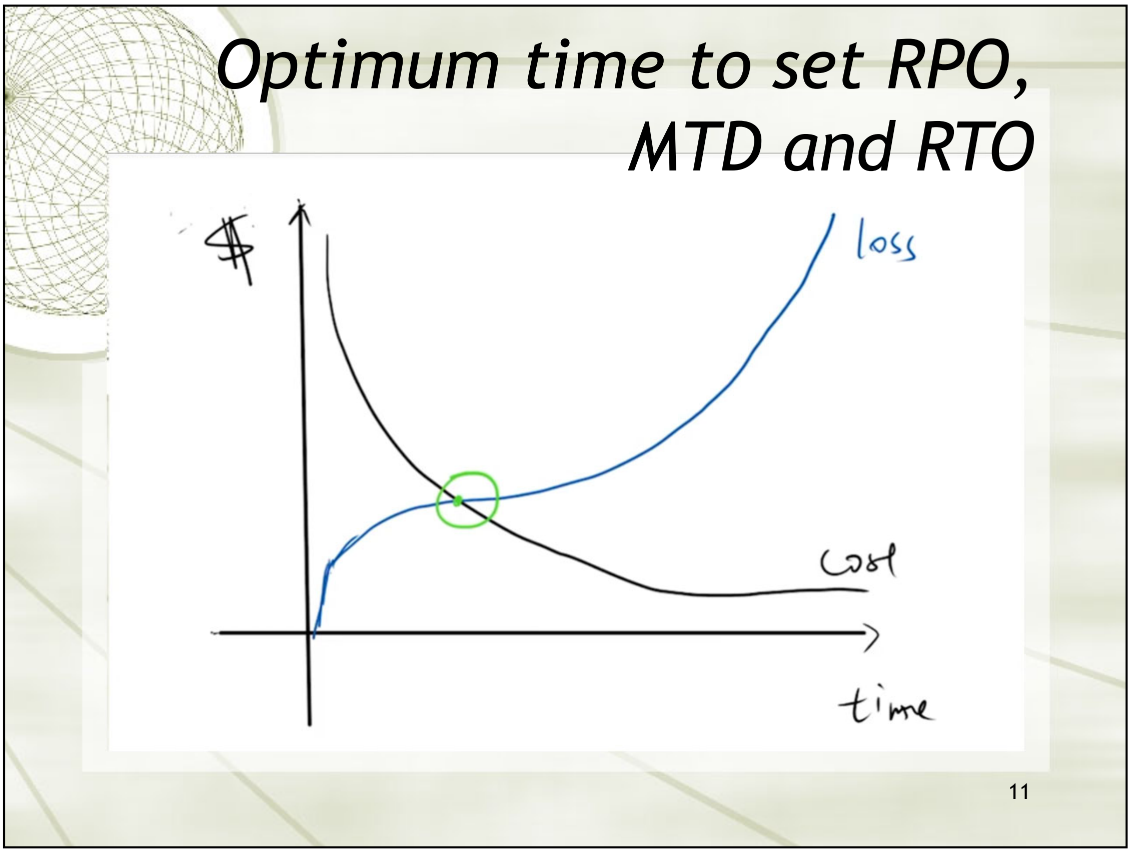
Recovery Parameters Timeline

WRT refers to Work Recovery Time – non-critical recovery such as loss data and backup recovery, system testing and verification etc.



Recovery Time over Complexity

The recovery mechanism depends on your acceptable level of downtime and budget.

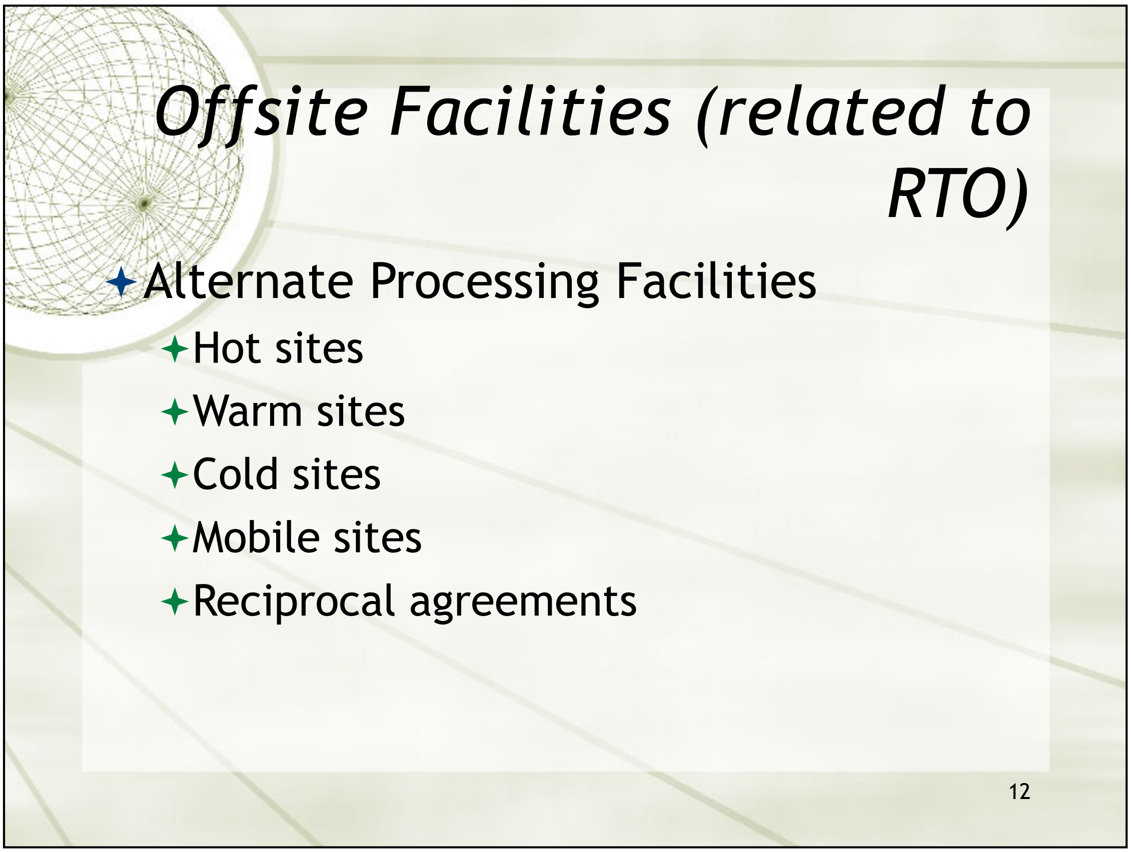


Optimum time to set RPO, MTD and RTO

11

Cost of recovering is more than the cost of loss with every unit of time that passes before the Optimum time. The method may not be worth its price.

Cost of loss is more than the cost of recovery with every unit of time that passes after the Optimum time. Loss due to damage is too high.



Offsite Facilities (related to RTO)

- Alternate Processing Facilities
  - Hot sites
  - Warm sites
  - Cold sites
  - Mobile sites
  - Reciprocal agreements

For larger disasters that affect the primary facility, an offsite backup facility must be accessible. Generally, contracts are established with third-party vendors to provide such services. The client pays a monthly fee to retain the right to use the facility in a time of need, and then incurs an activation fee when the facility actually has to be used. In addition, there would be a daily or hourly fee imposed for the duration of the stay. This is why subscription services for backup facilities should be considered a short-term solution, not a long-term solution.

It is important to note that most recovery site contracts do not promise to house the company in need at a specific location, but rather promise to provide what has been contracted for somewhere within the company's locale. On, and subsequent to, September 11, 2001, many organizations with Manhattan offices were surprised when they were redirected by their backup site vendor not to sites located in New Jersey (which were already full), but rather to sites located in Boston, Chicago, or Atlanta. This adds yet another level of complexity to the recovery process, specifically the logistics of transporting people and equipment to unplanned locations.

Companies can choose from three main types of leased or rented offsite facilities:

- ***Hot site*** A facility that is leased or rented and is fully configured and ready to operate within a few hours. The only missing resources from a hot site are usually the data, which will be retrieved from a backup site, and the people who will be processing the data. The equipment and system software must absolutely be compatible with the data being restored from the main site and must not cause any negative interoperability issues. Some facilities, for a fee, store data backups close to the hot site. These sites are a good choice for a company that needs to ensure a site will be available for it as soon as possible. Most hot-site facilities support annual tests that can be done by the company to ensure the site is functioning in the necessary state of readiness. This is the most expensive of the three types of offsite facilities. It can pose problems if a company requires proprietary or unusual hardware or software.

- ***Warm site*** A leased or rented facility that is usually partially configured with some equipment, such as HVAC, and foundational infrastructure components, but not the actual computers. In other words, a warm site is usually a hot site without the expensive equipment such as communication equipment and servers. Staging a facility with duplicate hardware and computers configured for immediate operation is extremely expensive, so a warm site provides an alternate facility with some peripheral devices. This is the most widely used model. It is less expensive than a hot site, and can be up and running within a reasonably acceptable time period. It may be a better choice for companies that depend upon proprietary and unusual hardware and software, because they will bring their own hardware and software with them to the site after the disaster hits. Drawbacks, however, are that much of the equipment has to be procured, delivered to, and configured at the warm site after the fact, and the annual testing available with hot-site contracts is not usually available with warm-site contracts. Thus, a company cannot be certain that it will in fact be able to return to an operating state within hours.

- ***Cold site*** A leased or rented facility that supplies the basic environment, electrical wiring, air conditioning, plumbing, and flooring, but none of the equipment or additional services. A cold site is essentially an empty data center. It may take weeks to get the site activated and ready for work. The cold site could have equipment racks and dark fiber (fiber that does not have the circuit engaged) and maybe even desks. However, it would require the receipt of equipment from the client, since it does not provide any. The cold site is the least expensive option, but takes the most time and effort to actually get up and functioning right after a disaster, as the systems and software must be delivered, tweaked, and configured. Cold sites are often used as backups for call centers, manufacturing plants, and other services that can be moved lock, stock, and barrel in one shot.

Most companies use *warm sites,* which have some devices such as disk drives, tape drives, and controllers, but very little else. These companies usually cannot afford a hot site, and the extra downtime would not be considered detrimental. A warm site can provide a longer-term solution than a hot site. Companies that decide to go with a *cold site* must be able to be out of operation for a week or two. The cold site usually includes power, raised flooring, climate control, and wiring.

The following provides a quick overview of the differences between offsite facilities:

Hot Site Advantages

- Ready within hours for operation
- Highly available
- Usually used for short-term solutions, but available for longer stays
- Annual testing available

Hot Site Disadvantages

- Very expensive
- Limited on hardware and software choices

Warm and Cold Site Advantages

- Less expensive
- Available for longer timeframes because of the reduced costs
- Practical for proprietary hardware or software use

Warm and Cold Site Disadvantages

- Operational testing not usually available
- Resources for operations not immediately available

Tertiary Sites

During the BIA phase, the team may recognize the danger of the primary backup facility not being available when needed, which could require a tertiary site. This is a secondary backup site, just in case the primary backup site is unavailable. The secondary backup site is sometimes referred to as a “backup to the backup.” This is basically plan B if plan A does not work out.

Reciprocal Agreements

Another approach to alternate offsite facilities is to establish a ***reciprocal agreement*** with another company, usually one in a similar field or that that has similar technological infrastructure. This means that company A agrees to allow company B to use its facilities if company B is hit by a disaster, and vice versa. This is a cheaper way to go than the other offsite choices, but it is not always the best choice. Most environments are maxed out pertaining to the use of facility space, resources, and computing capability. To allow another company to come in and work out of the same shop could prove to be detrimental to both companies. Whether it can assist the other company while tending effectively to its own business is an open question. The stress of two companies working in the same environment could cause tremendous levels of tension. If it did work out, it would only provide a short-term solution. Configuration management could be a nightmare. Does the other company upgrade to new technology and retire old systems and software? If not, one company's systems may become incompatible with that of the other company?

Important issues need to be addressed before a disaster hits if a company decides to participate in a reciprocal agreement with another company:

- How long will the facility be available to the company in need?
- How much assistance will the staff supply in integrating the two environments and ongoing support?
- How quickly can the company in need move into the facility?
- What are the issues pertaining to interoperability?
- How many of the resources will be available to the company in need?
- How will differences and conflicts be addressed?
- How does change control and configuration management take place?
- How often can drills and testing take place?
- How can critical assets of both companies be properly protected?

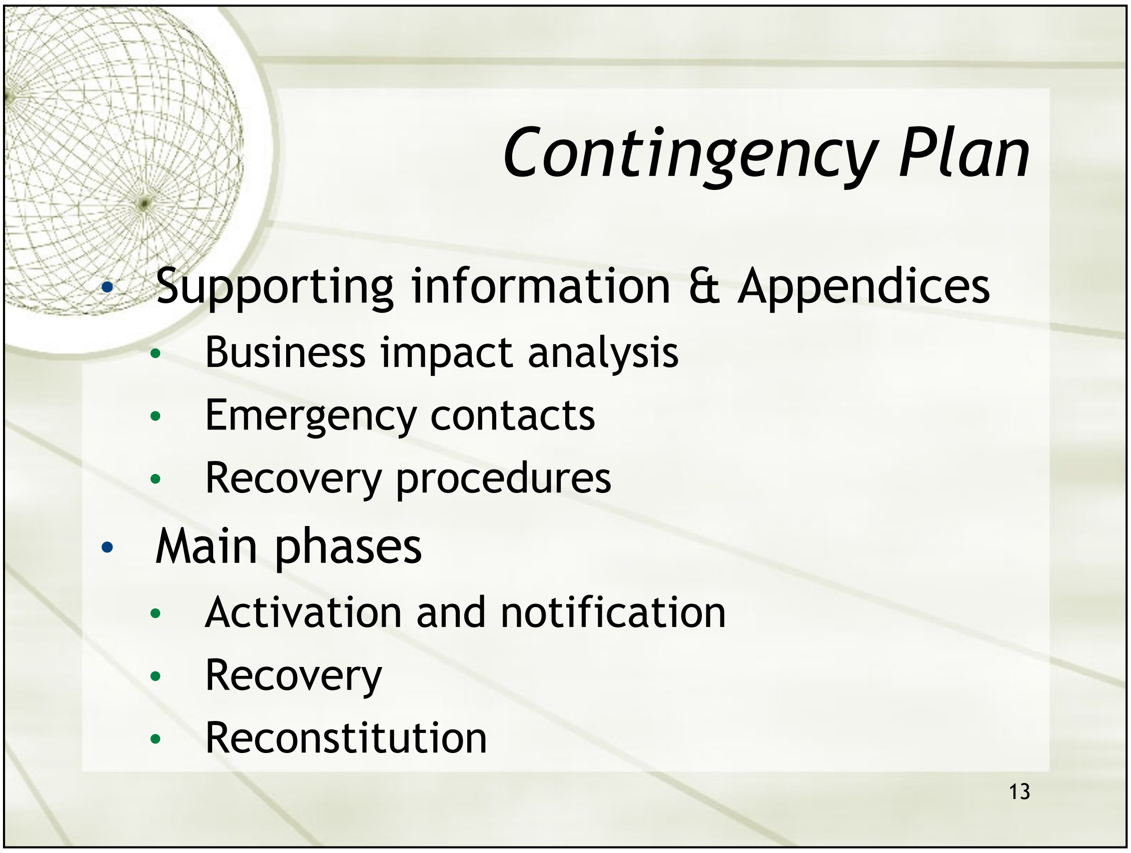
Offsite Location

When choosing a backup facility, it should be far enough away from the original site so that one disaster does not take out both locations. In other words, it is not logical to have the backup site only a few miles away if the company is concerned about tornado damage, because the backup site could also be affected or destroyed. There is a rule of thumb that suggests that alternate facilities should be, at a bare minimum, at least 5 miles away from the primary site, while 15 miles is recommended for most low-to-medium critical environments, and 50 to 200 miles is recommended for critical operations to give maximum protection in cases of regional disasters.

Redundant Sites

Some companies choose to have ***redundant sites***, or mirrored sites, meaning one site is equipped and configured exactly like the primary site, which serves as a redundant environment. The business-processing capabilities between the two sites can be completely synchronized. These sites are owned by the company and are mirrors of the original production environment. A redundant site has clear advantages: it has full availability, is ready to go at a moment's notice, and is under the organization's complete control. This is, however, one of the most expensive backup facility options, because a full environment must be maintained even though it usually is not used for regular production activities until after a disaster takes place that triggers the relocation of services to the redundant site.

But expensive is relative here. If the company would lose a million dollars if it were out of business for just a few hours, the loss potential would override the cost of this option. Many organizations are subjected to regulations that dictate they must have redundant sites in place, so expense is not an issue in these situations.



Contingency Plan

- Supporting information & Appendices
  - Business impact analysis
  - Emergency contacts
  - Recovery procedures
- Main phases
  - Activation and notification
  - Recovery
  - Reconstitution

13

According to NIST SP800-34r1:

There are five main components of the information system contingency plan (ISCP). The supporting information and plan appendices provide essential information to ensure a comprehensive plan. The Activation and Notification, Recovery, and Reconstitution Phases address specific actions that the organization should take following a system disruption or emergency.

Supporting information and Appendices

The supporting information component includes an introduction and concept of operations section providing essential background or contextual information that makes the contingency plan easier to understand, implement, and maintain. These details aid in understanding the applicability of the guidance, in making decisions on how to use the plan, and in providing information on where associated plans and information outside the scope of the plan may be found.

This section may contain the roles and responsibilities section presents the overall structure of contingency teams, including the hierarchy and coordination mechanisms and requirements among the teams. The section also provides an overview of team member roles and responsibilities in a contingency situation. Teams and team members should be designated for specific response and recovery roles during contingency plan activation.

Activation and Notification Phase

The Activation and Notification Phase defines initial actions taken once a system disruption or outage has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the plan. At the completion of the Activation and Notification Phase, ISCP staff will be prepared to perform recovery measures to restore system functions.

Activation criteria: The ISCP should be activated if one or more of the activation criteria for that system are met. If an activation criterion is met, the designated authority should activate the plan

Notification procedures: An outage or disruption may occur with or without prior notice. For example, advance notice is often given that a hurricane is predicted to affect an area or that a computer virus is expected on a certain date. However, there may be no notice of equipment failure or a criminal act. Notification procedures should be documented in the plan for both types of situation. The procedures should describe the methods used to notify recovery personnel during business and non business hours. Prompt notification is important for reducing the effects of a disruption on the system; in some cases, it may provide enough time to allow system personnel to shut down the system gracefully to avoid a hard crash. Following the outage or disruption, notification should be sent to the Outage Assessment Team so that it may determine the status of the situation and appropriate next steps. When outage assessment is complete, the appropriate recovery and system support personnel should be notified.

Outage assessment: To determine how the ISCP will be implemented following a system disruption or outage, it is essential to assess the nature and extent of the disruption. The outage assessment should be completed as quickly as the given conditions permit, with personnel safety remaining the highest priority. When possible, the Outage Assessment Team is the first team notified of the disruption. Once impact to the system has been determined, the appropriate teams should be notified of updated information and the planned response to the situation

Recovery Phase

Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or new alternate location. At the completion of the Recovery Phase, the information system will be functional and capable of performing the functions identified in the plan. Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation at an alternate system, or relocation and recovery at an alternate site. It is feasible that only system resources identified as high priority in the BIA will be recovered at this stage.

Sequence of Recovery Activities: The sequence of activities should reflect the system's MTD to avoid significant impacts to related systems. Procedures should be written in a stepwise, sequential format so system components may be restored in a logical manner. If conditions require the system to be recovered at an alternate site, certain materials will need to be transferred or procured. These items may include shipment of data backup media from offsite storage, hardware, copies of the recovery plan, and software programs. Procedures should designate the appropriate team or team members to coordinate shipment of equipment, data, and vital records. References to applicable appendices, such as equipment lists or vendor contact information, should be made in the plan where necessary. Procedures should clearly describe requirements to package, transport, and purchase materials required to recover the system.

Recovery Procedures: To facilitate Recovery Phase operations, the ISCP should provide detailed procedures to restore the information system or components to a known state. Procedures should be assigned to the appropriate recovery team and typically address the following actions:

- Obtaining authorization to access damaged facilities and/or geographic area;
- Notifying internal and external business partners associated with the system;
- Obtaining necessary office supplies and work space;
- Obtaining and installing necessary hardware components;
- Obtaining and loading backup media;
- Restoring critical operating system and application software;
- Restoring system data to a known state;
- Testing system functionality including security controls;
- Connecting system to network or other external systems; and
- Operating alternate equipment successfully.

Recovery procedures should be written in a straightforward, step-by-step style. To prevent difficulty or confusion in an emergency, no procedural steps should be assumed or omitted. A checklist format is useful for documenting the sequential recovery procedures and for troubleshooting problems if the system cannot be recovered properly.

Recovery Escalation and Notification: Effective escalation and notification procedures should define and describe the events, thresholds, or other types of triggers that are necessary for additional action. Actions would include additional notifications for more recovery staff, messages and status updates to leadership, and notices for additional resources. Procedures should be included to establish a clear set of events, actions and results, and should be documented for teams or individuals as appropriate.

Reconstitution Phase

The Reconstitution Phase is the third and final phase of ISCP implementation and defines the actions taken to test and validate system capability and functionality. During Reconstitution, recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. This phase consists of two major activities: validating successful recovery and deactivation of the plan.

<u>Validation</u> of recovery typically includes these steps:

-*Concurrent Processing*. Concurrent processing is the process of running a system at two separate locations concurrently until there is a level of assurance that the recovered system is operating correctly and securely.

-*Validation Data Testing*. Data testing is the process of testing and validating recovered data to ensure that data files or databases have been recovered completely and are current to the last available backup.

-*Validation Functionality Testing*. Functionality testing is a process for verifying that all system functionality has been tested, and the system is ready to return to normal operations.

At the successful completion of the validation testing, ISCP personnel will be prepared to declare that reconstitution efforts are complete and that the system is operating normally. The ISCP Coordinator must determine if the system has undergone significant change and will require reassessment and reauthorization.

<u>Deactivation</u> of the plan is the process of returning the system to normal operations and finalizing reconstitution activities to prepare the system against another outage or disruption. These activities include:

- *Notifications*. Upon return to normal operations, users should be notified by the ISCP Coordinator (or designee) using predefined notification procedures.
- *Cleanup.* Cleanup is the process of cleaning up work space or dismantling any temporary recovery locations, restocking supplies, returning manuals or other documentation to their original locations, and readying the system for another contingency event.
- *Offsite Data Storage*. If offsite data storage is used, procedures should be documented for returning retrieved backup or installation media to its offsite data storage location.
- *Data Backup*. As soon as reasonable following reconstitution, the system should be fully backed up and a new copy of the current operational system stored for

future recovery efforts. This full backup should be stored with other system backups and comply with applicable security controls.

- *Event Documentation*. All recovery and reconstitution events should be well documented, including actions taken and problems encountered during the recovery and reconstitution efforts.

An after-action report with lessons learned should be documented and included for updating the ISCP. Once all activities and steps have been completed and documentation has been updated, the ISCP can be formally deactivated. An announcement with the declaration should be sent to all business and technical contacts.