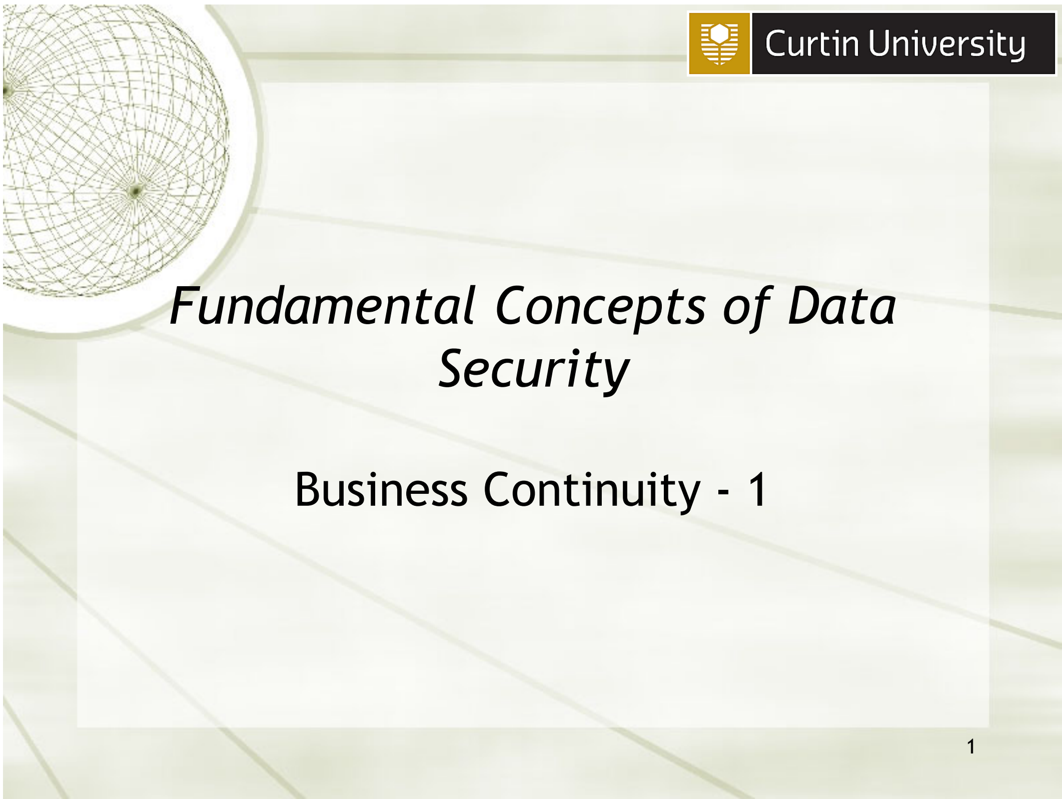
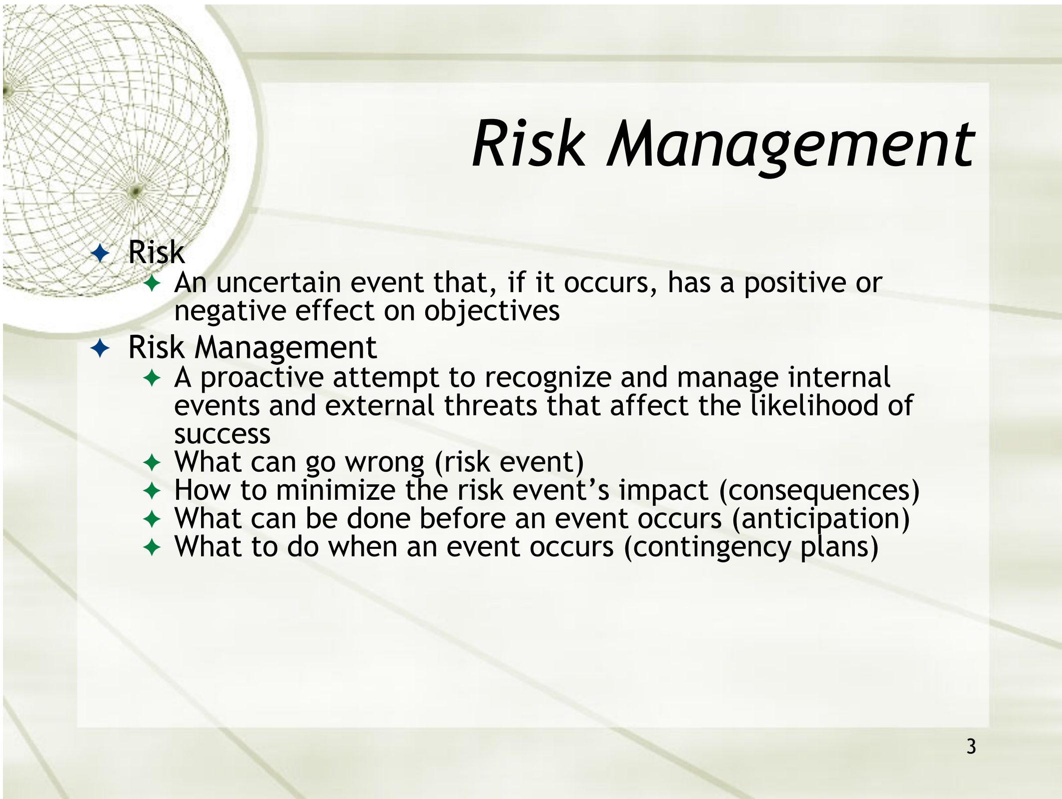


Fundamental Concepts of Data Security

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



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)

3

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

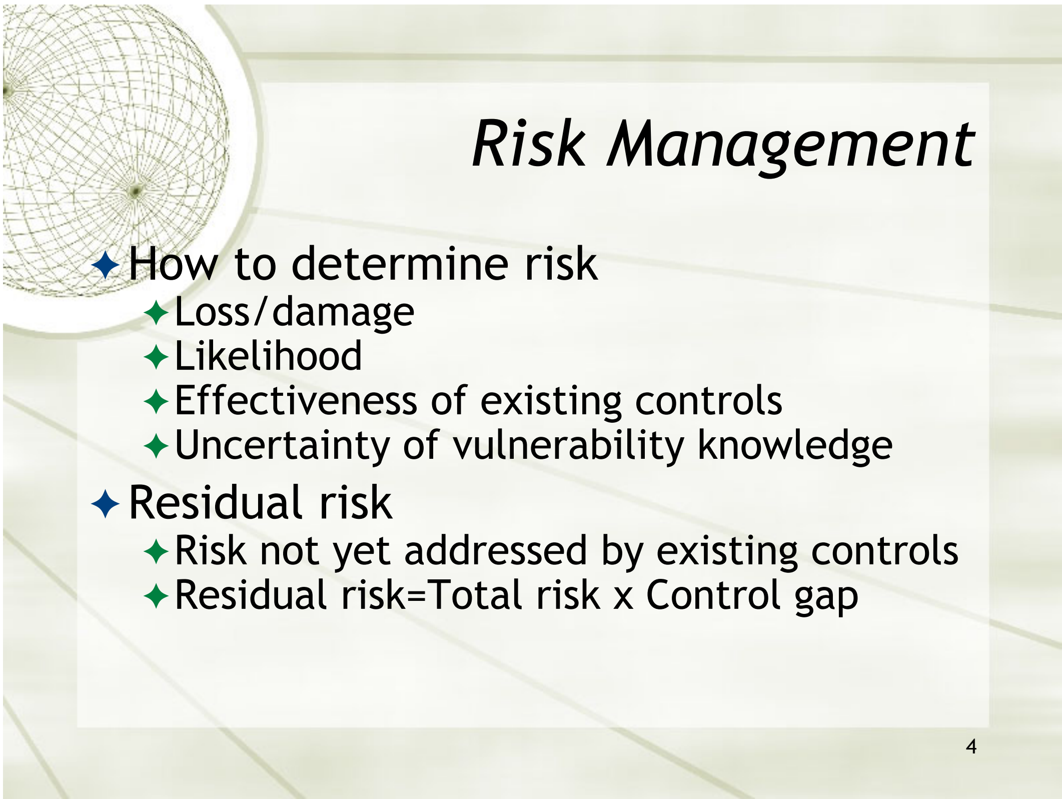
I. Defend the risk: lock the door, install IDS, block specific ports associated with specific attacks

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



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

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:

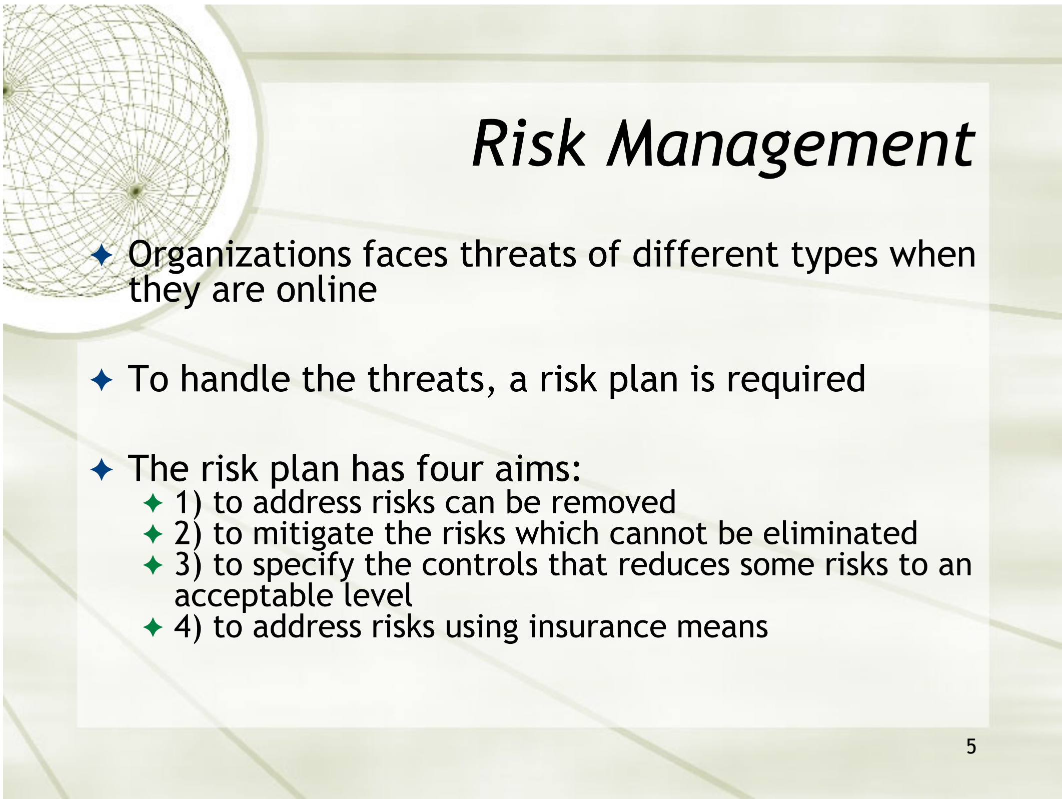
> The likelihood of a fire has been estimated actuarially for each

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.

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 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

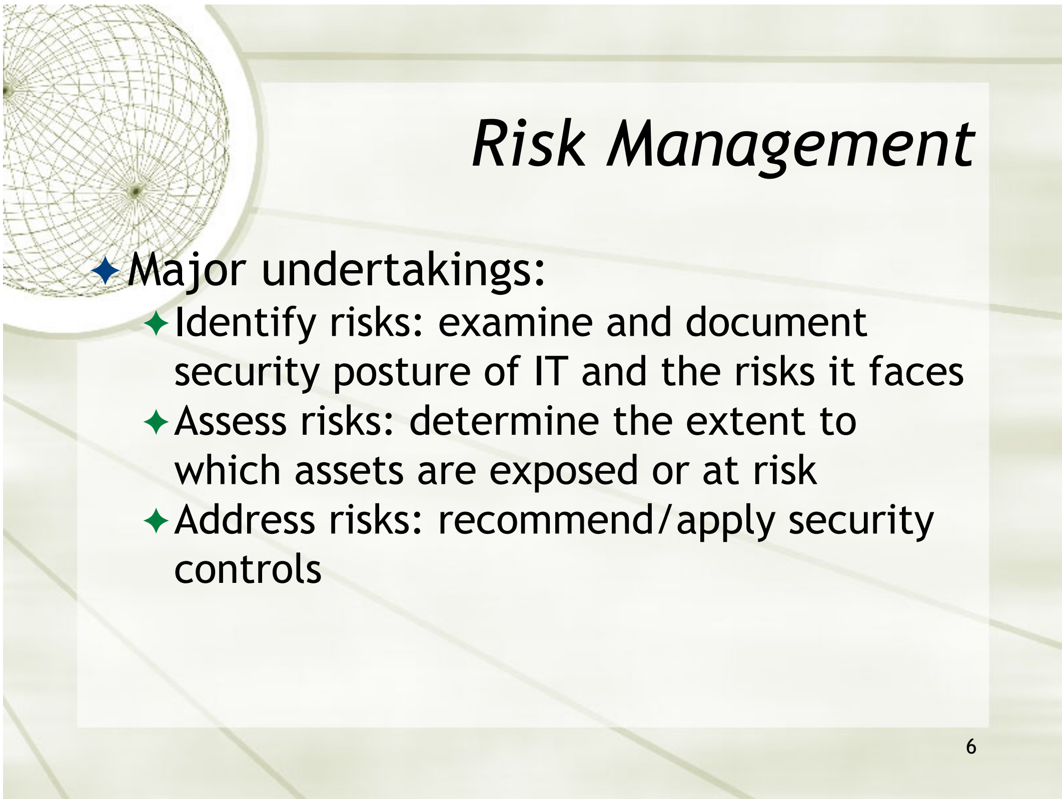
5

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

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.

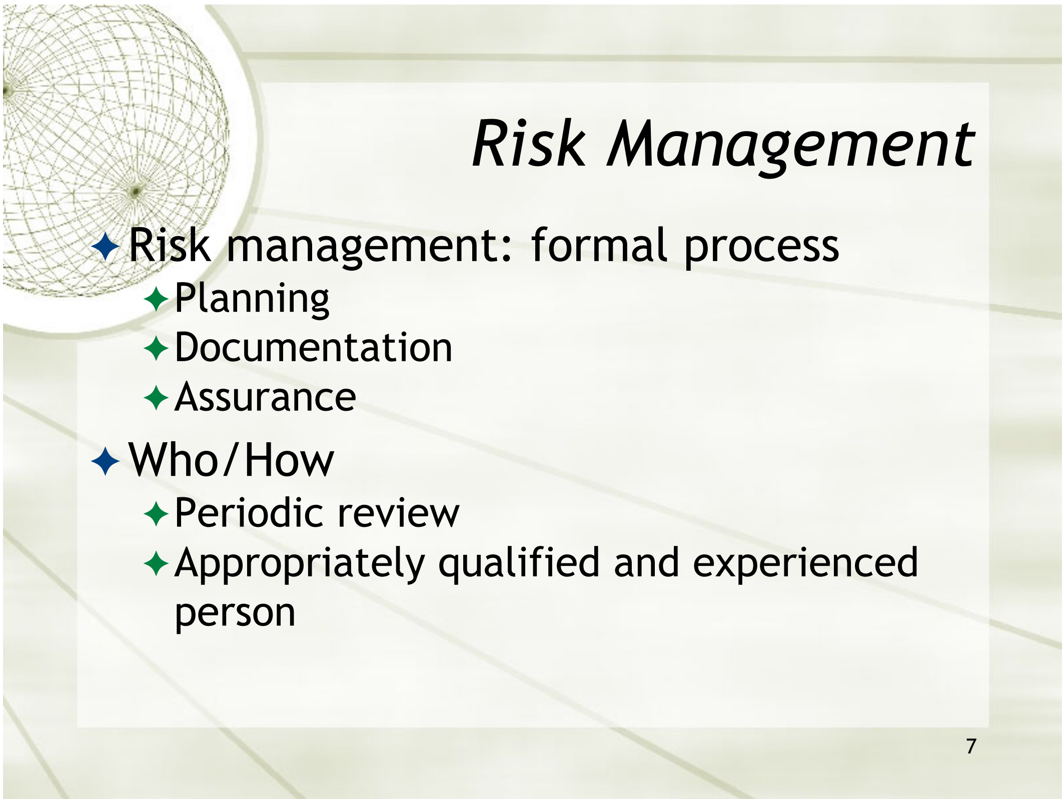
When an organization depends on IT-based systems to remain viable, information security and the discipline of risk management must become an integral part of the economic basis for making business decisions. These decisions are based on trade-offs between the costs of applying information systems controls 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.

- 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

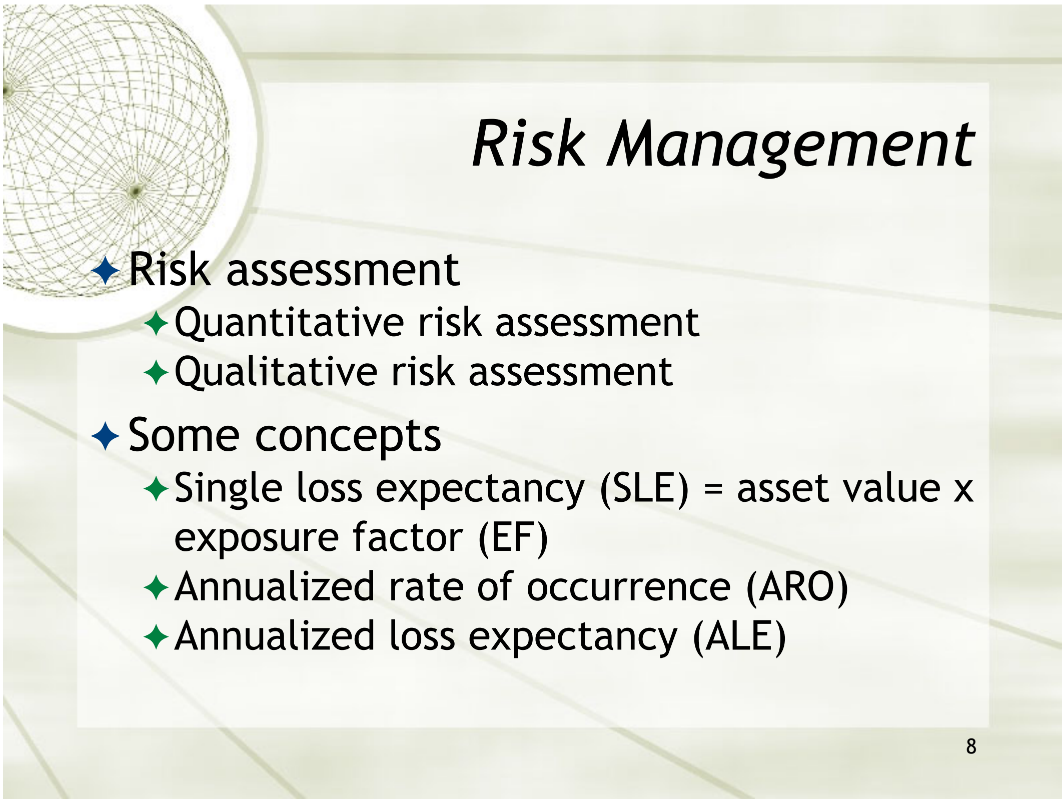
- Risk management: formal process
  - Planning
  - Documentation
  - Assurance
- Who/How
  - Periodic review
  - Appropriately qualified and experienced person

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.

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.

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). is simply how often you expect a specific type of attack to occur. 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:

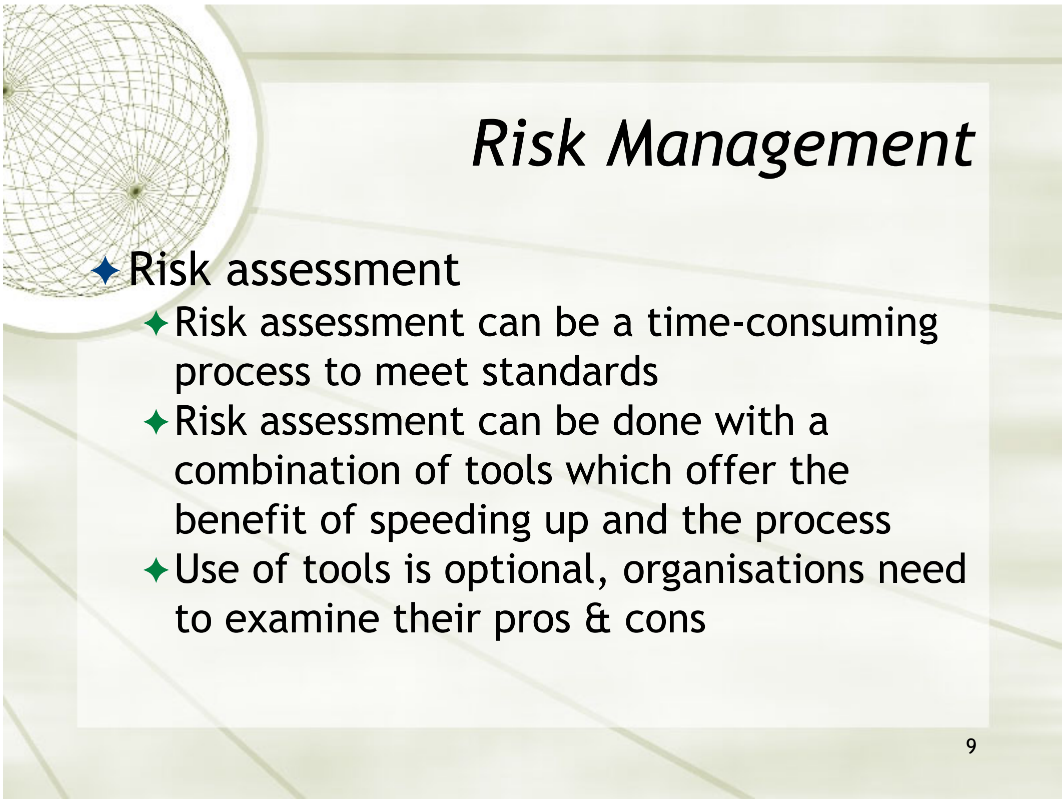
ALE = SLE x ARO

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



Risk Management

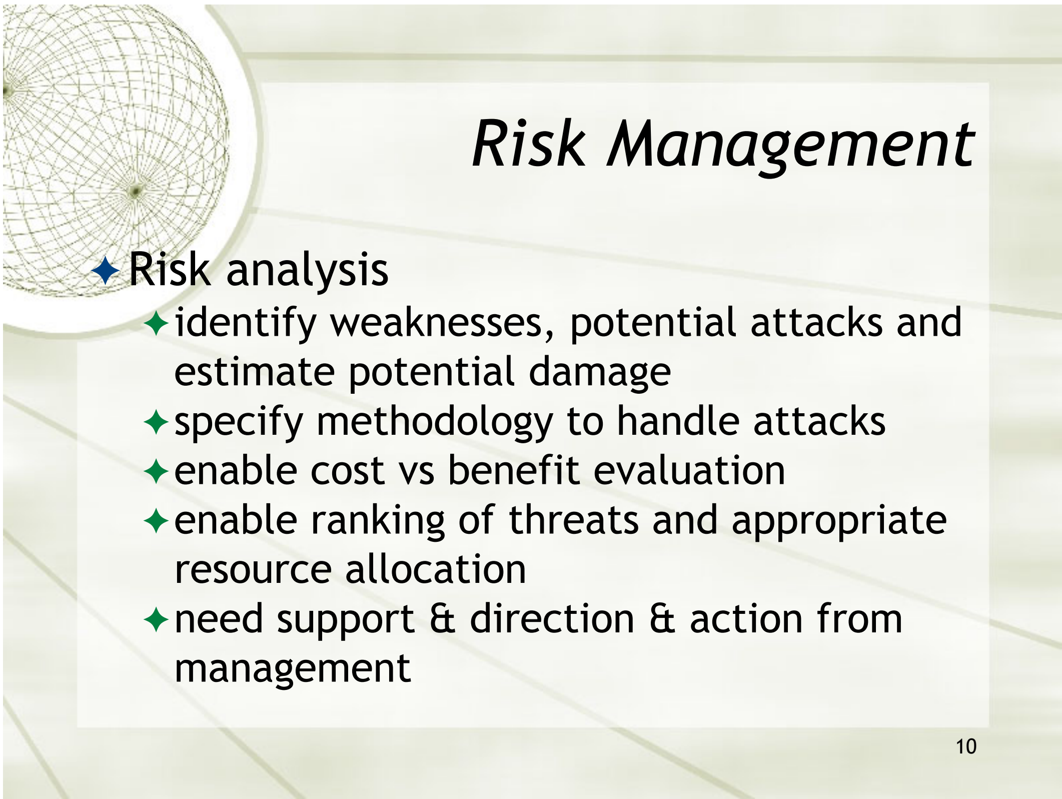
- Risk assessment
  - Risk assessment can be a time-consuming process to meet standards
  - Risk assessment can be done with a combination of tools which offer the benefit of speeding up and the process
  - Use of tools is optional, organisations need to examine their pros & cons

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.

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

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.

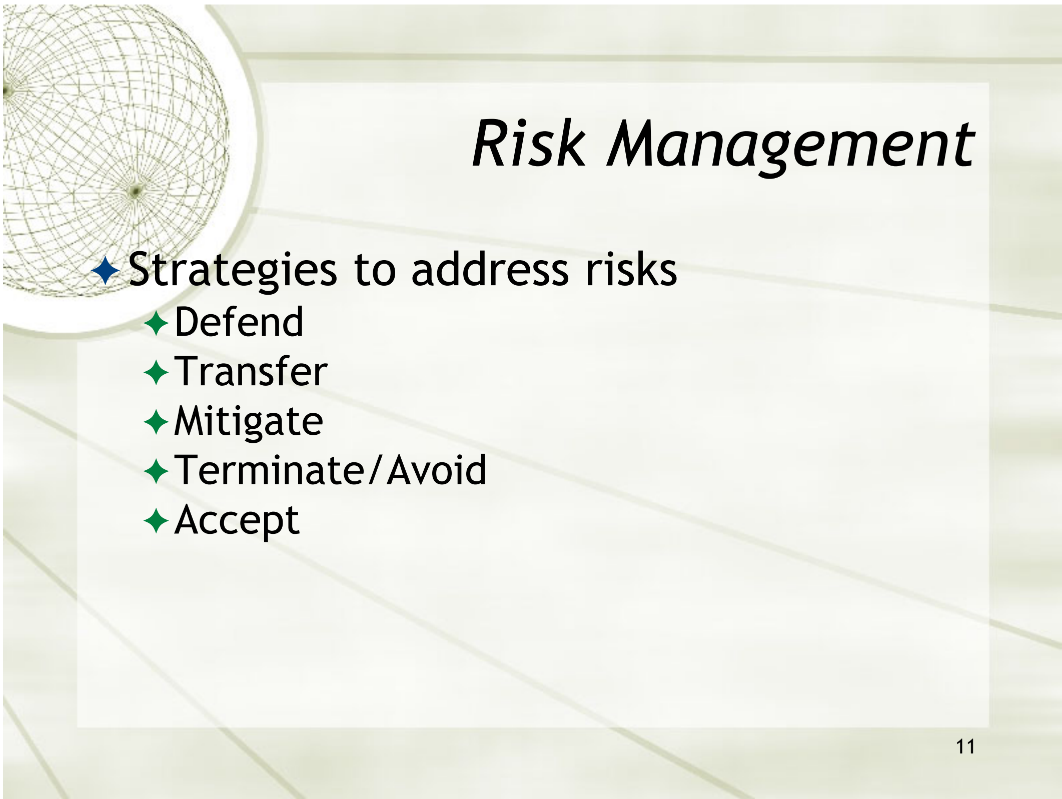
One of the team's tasks is to create a report that details the asset valuations. Senior management should review and accept the lists, and make them the scope of the IRM project. If management determines at this early stage that some assets are not important, the risk assessment team should not spend 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

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

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

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.

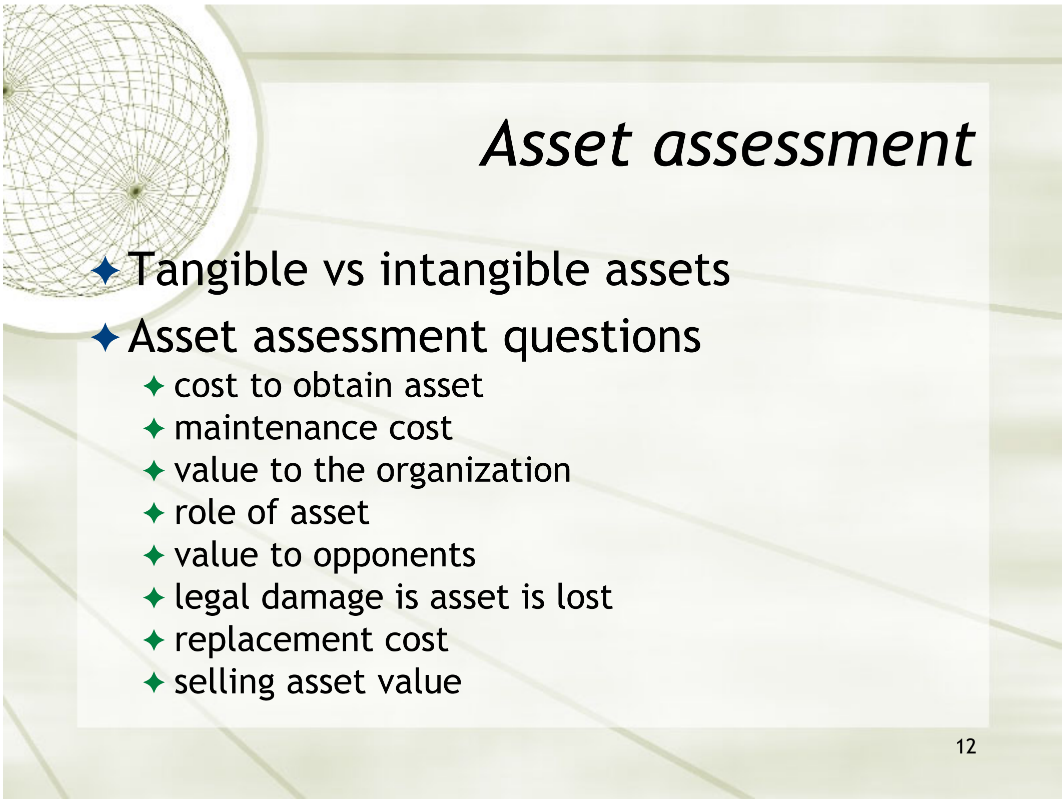
The **terminate** control strategy directs the organization to avoid those business activities that introduce uncontrollable risks. If an organization studies the risks from implementing business-to-consumer e-commerce operations and determines that the risks are not sufficiently offset by the potential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

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

12

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:

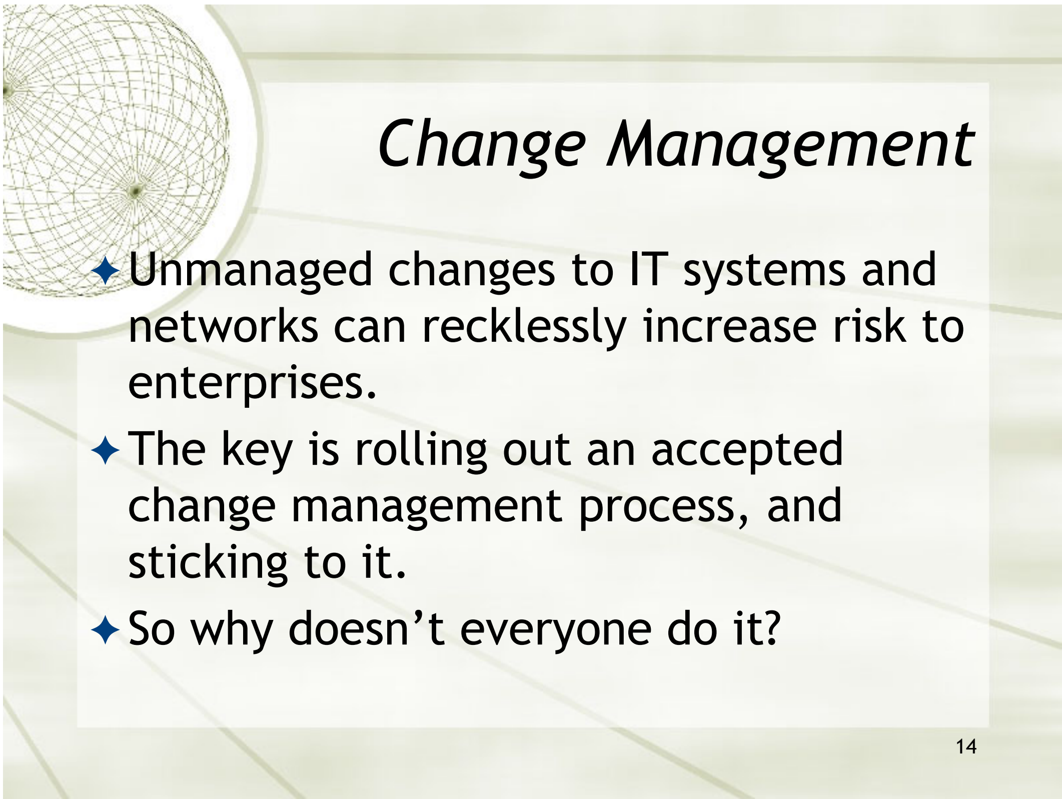
•To perform effective cost/benefit analyses

•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?

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.

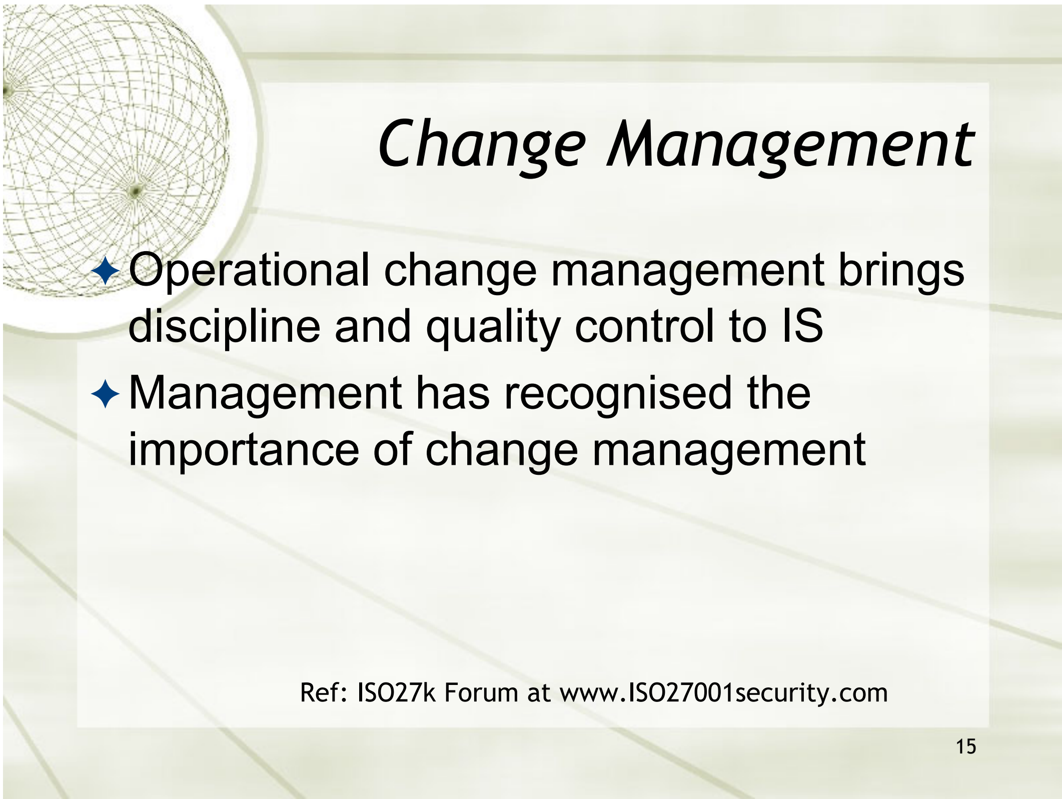
Auditing or performing assessments on your change management program is a useful way to measure coverage and effectiveness. Review the approval process and determine helpful metrics such as: Number of exceptions over time, are they increasing or decreasing? Or number of failures, how many unapproved/unplanned 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

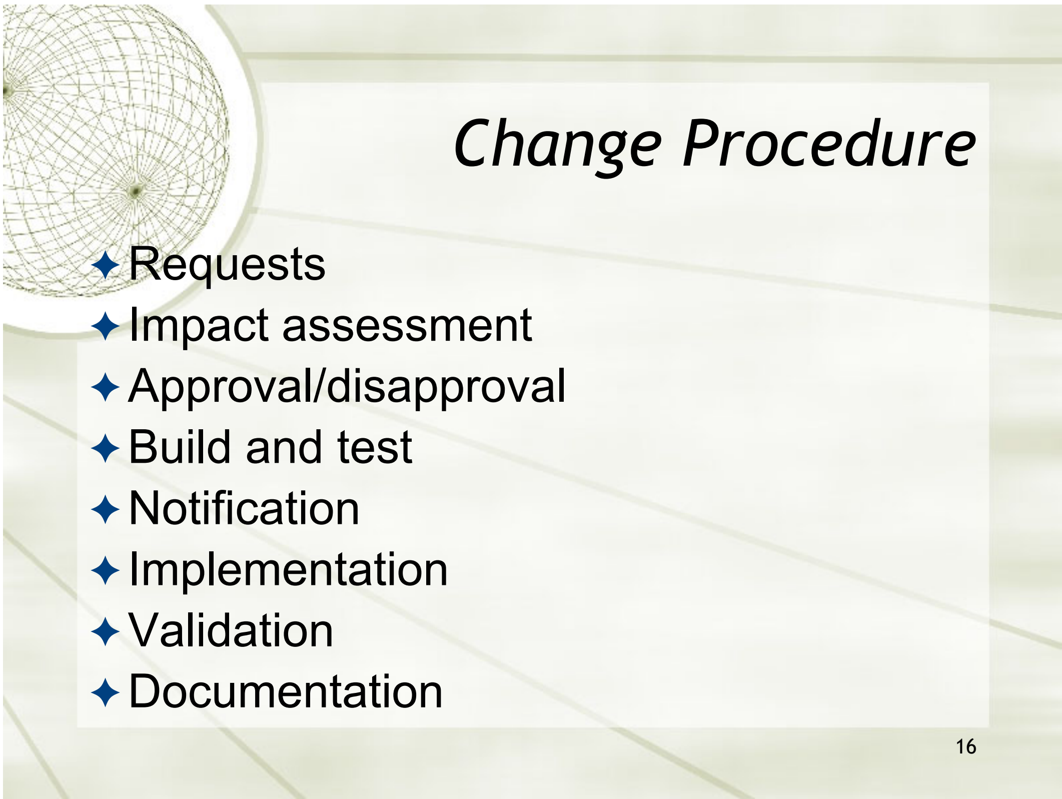
Ref: ISO27k Forum at www.ISO27001security.com

15

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

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.

○**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.

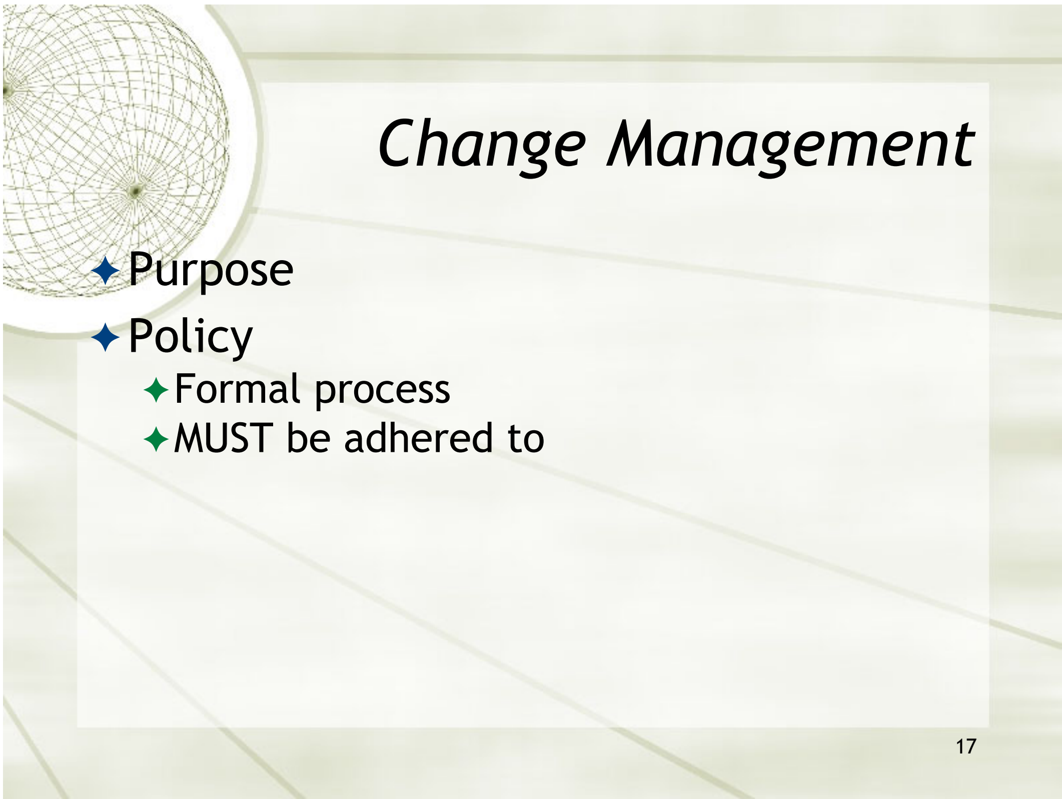
○**Build and Test:** Subsequent approvals are provided to operations support for test and integration development. The necessary software and hardware should be tested in a nonproduction environment. All configuration changes associated with a deployment must be fully tested and documented. The security 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 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.



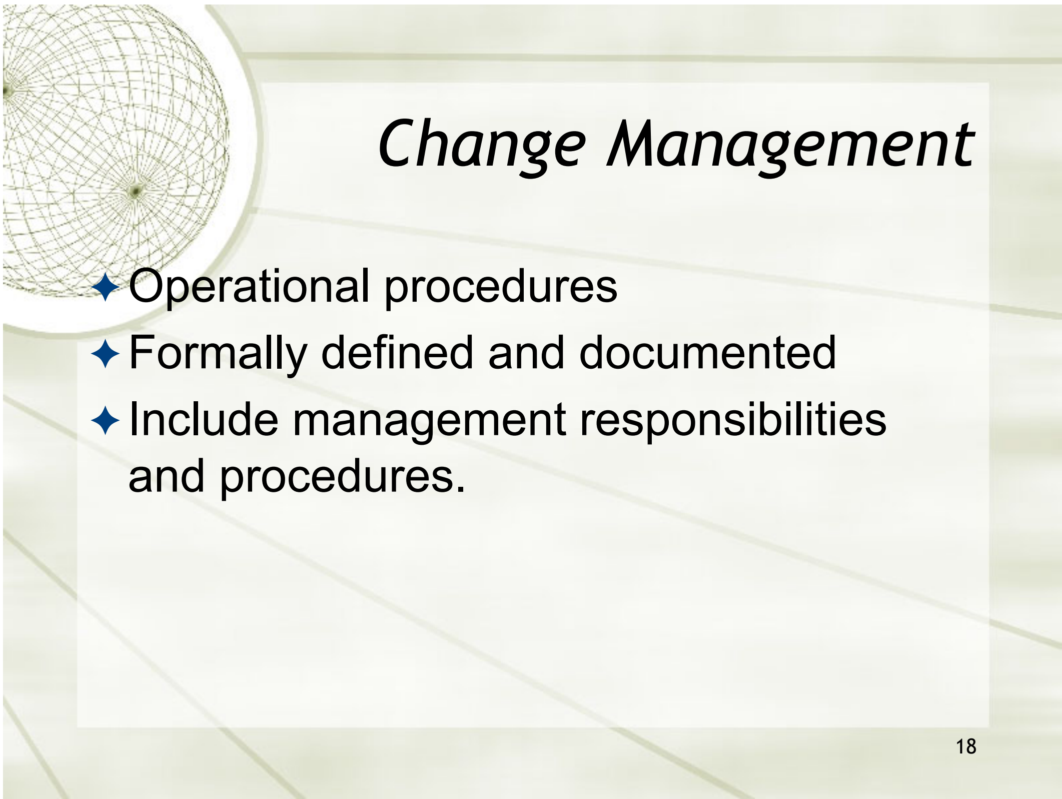
Change Management

- 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

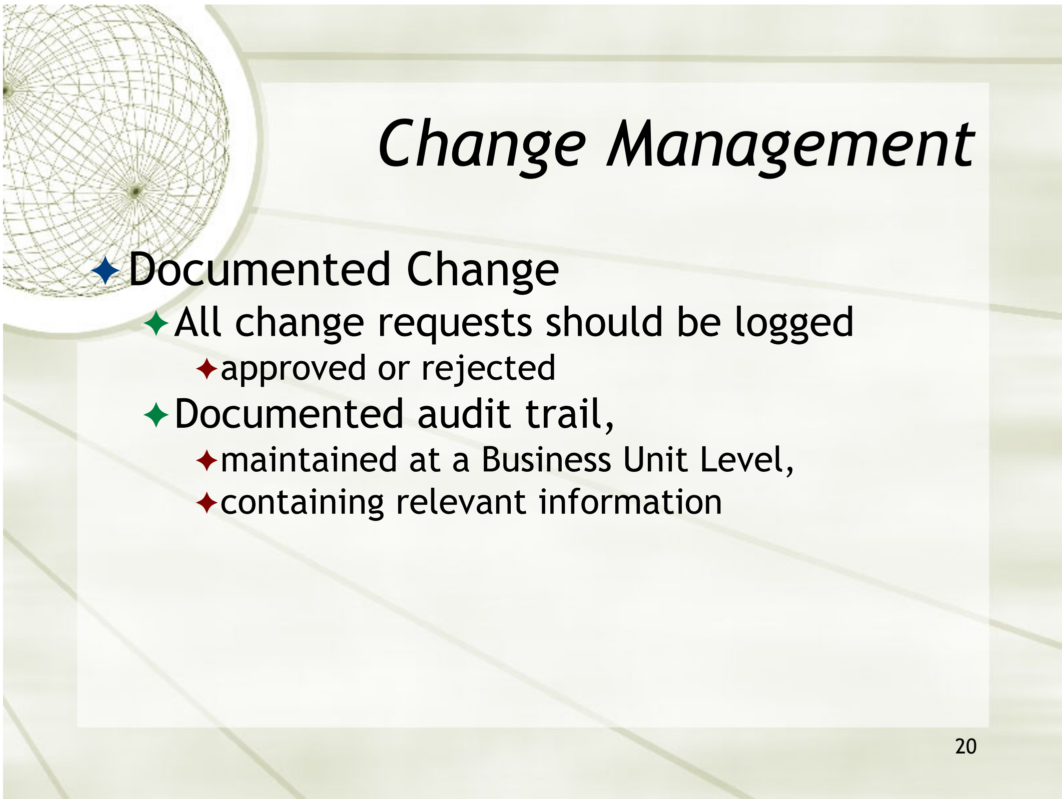
- Operational procedures
- Formally defined and documented
- Include management responsibilities and procedures.

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.



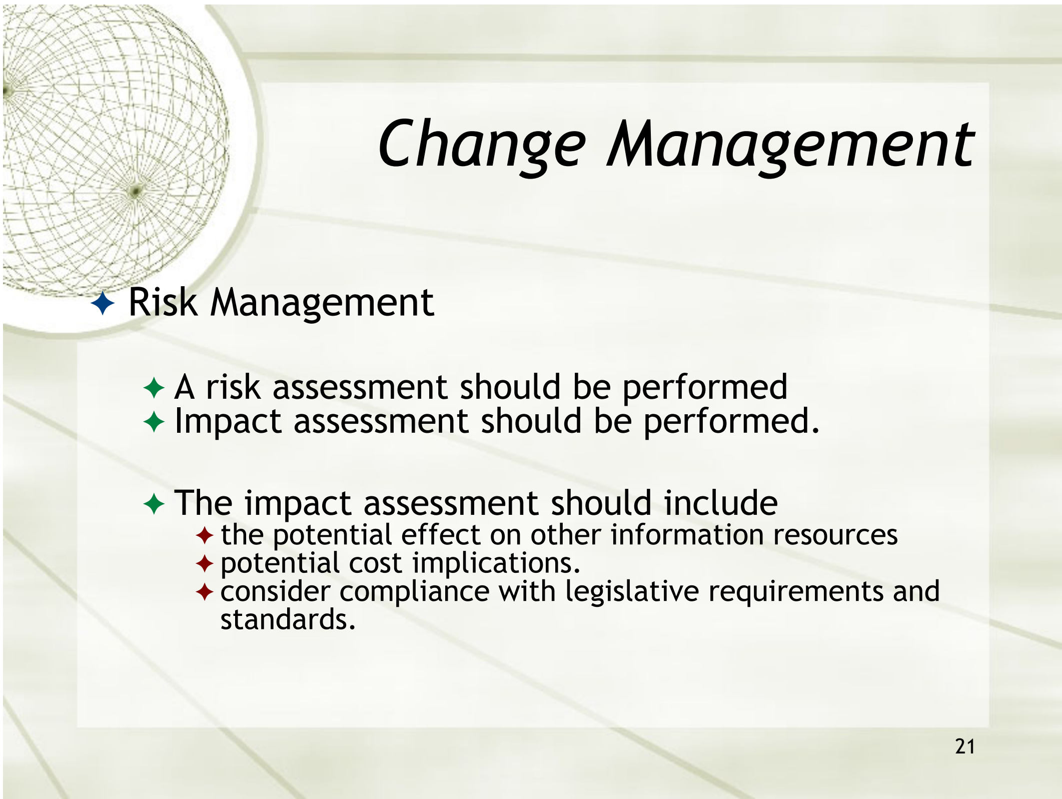
Change Management

- 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.



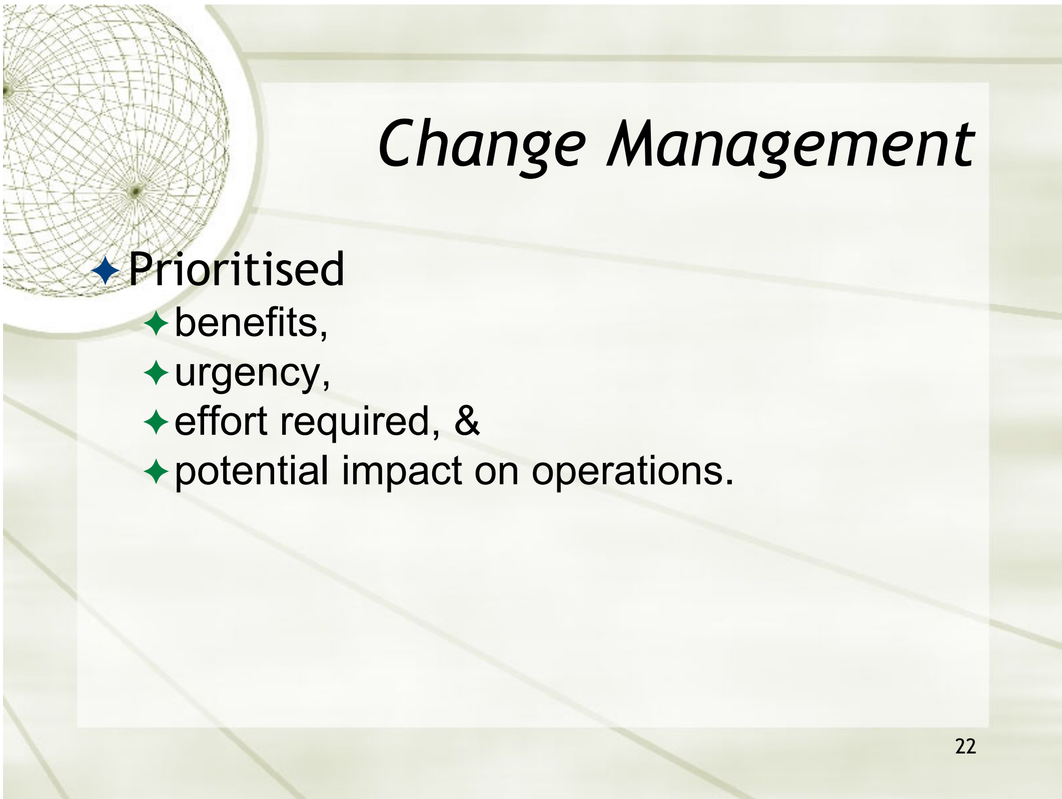
Change Management

- 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.



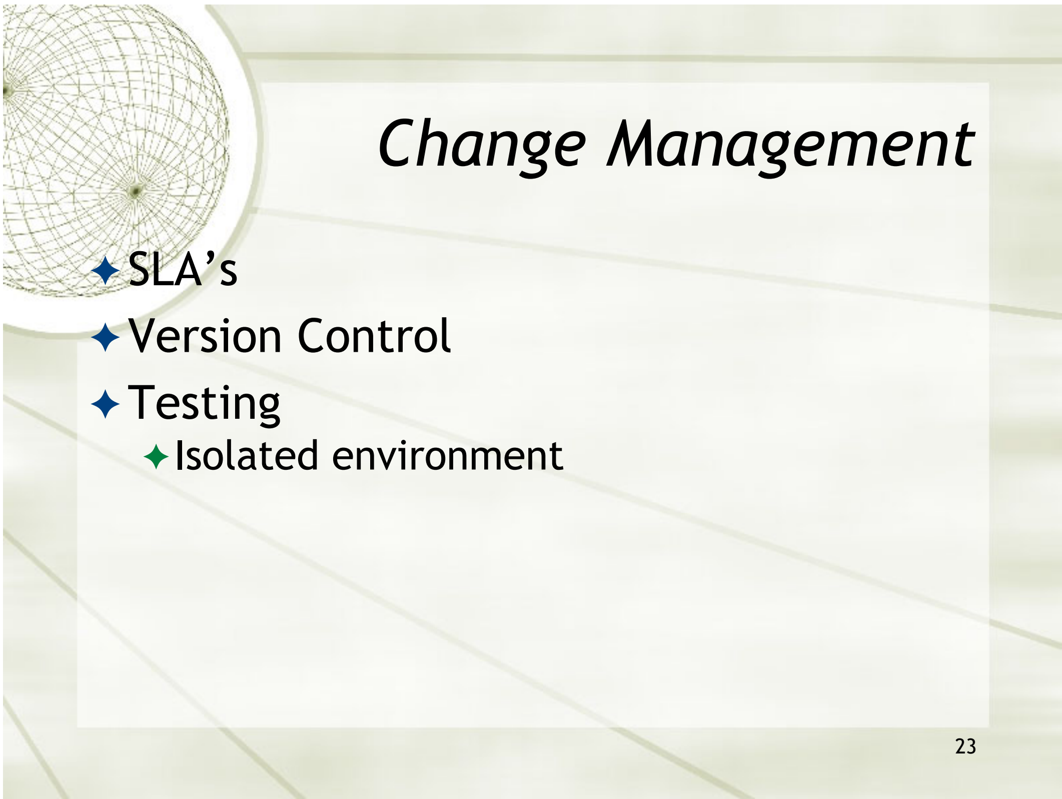
Change Management

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

22

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

23

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)

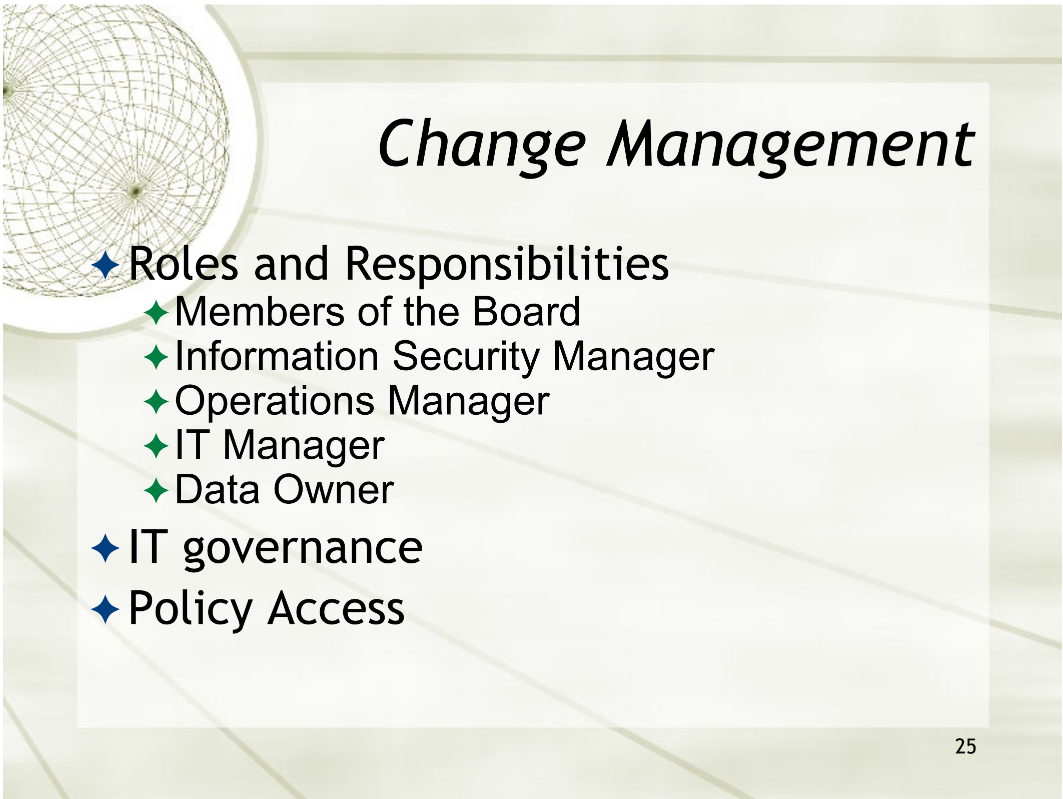
Business continuity plans shall be updated with relevant changes, managed through the change control process. Business continuity plans rely on the completeness, accuracy and availability of BCP documentation. BCP documentation is the road map used to minimise disruption to critical business processes 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
  - 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