Information Security Planning
INFO6027

Week 3

FANSHAWE

Housekeeping!

- Assignment 1 is 65% marked - will be completed tomorrow.

- Some news from https://www.securityweek.com/:

- **https://www.securityweek.com/zendesk-hacked-after-employees-fall-for-phishing-attack/**
- **https://www.securityweek.com/fbi-confirms-north-korean-hackers-behind-100-million-horizon-bridge-heist/**

- https://www.bloomberg.com/news/articles/2023-01-25/microsoft-networking-issues-take-down-outlook-and-teams

Drastic Rise in Cyber Security Issues

73% of black hat hackers said traditional firewall and antivirus security is irrelevant or obsolete.

209,000 payment card numbers and expiration dates were stolen from Equifax.

Cybercrime is more profitable than the global illegal drug trade – **$600 BILLION.** vs **$400 BILLION**

Marriot International – 500 million users' data stolen.

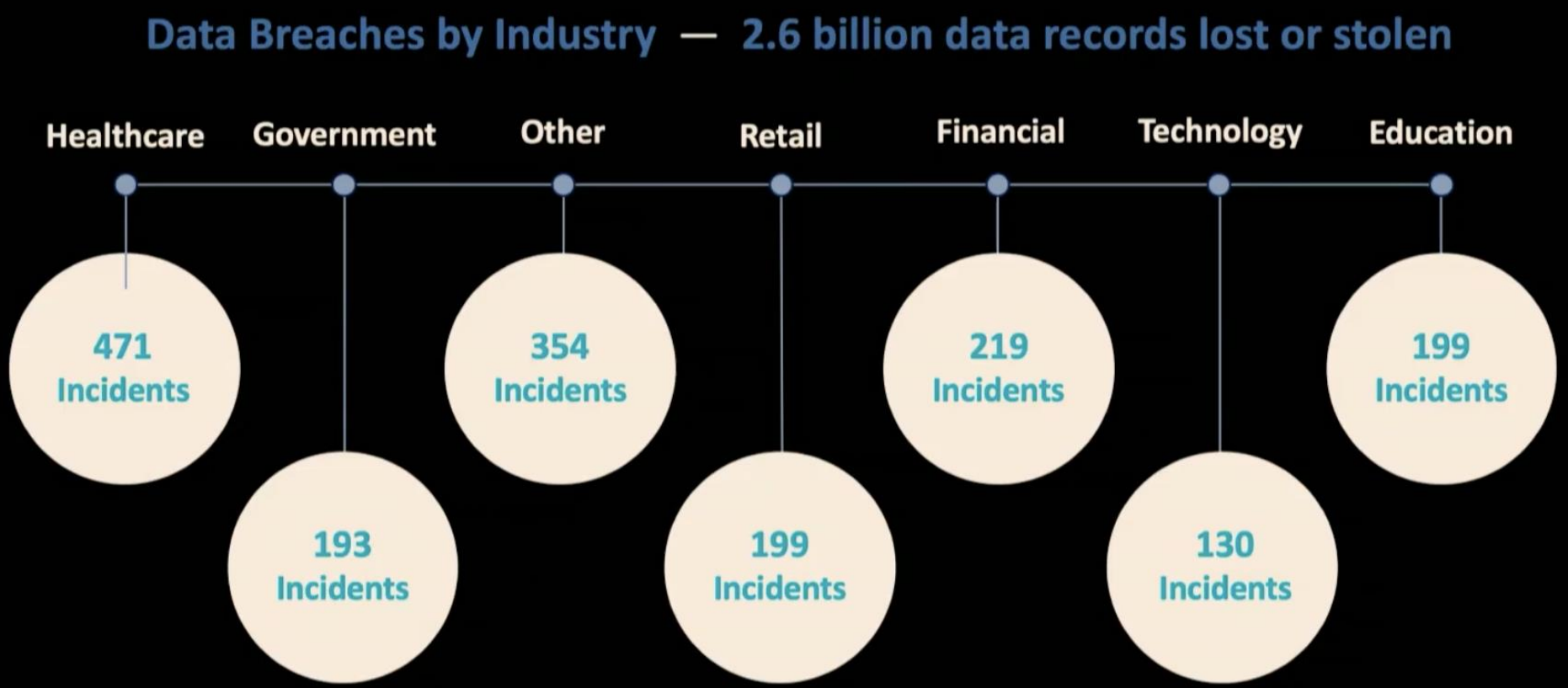
65% of companies have over 1,000 stale user accounts.

Russian hackers can infiltrate a computer network in **18 minutes**.

32% of black hat hackers admit privileged accounts are their number one way to hack systems.

Source: https://bit.ly/3d81H9U

Any Industry Can be Impacted



Breach Level Index: 2017 Annual Report

Lesson 3 Overview

- **Get the book**. The figures in this presentation all come from the course textbook. These slides are a ***reference*** to help you understand these concepts.

This week we will be discussing:

- Planning security management – ITSM
- ISO/IEC Security Standards – (*ISO: International Standards Organization*)
  – (IEC*: International Electrotechnical Commission*)
  - ➢ - Began working together in 1987
- Risk assessment
- IT Security Controls
- Plans, Policies, Procedures, and Processes

Guiding Questions for this Lesson

- What is ITSM and why do we need it?
- What are ISO standards and why do we need them?
- What is context and how does it impact security policy?

IT Security Management: Protecting Critical Assets (in a cost-effective manner)

ITSM is the formal process of answering these questions:

1. Consists of first determining a clear divide of an org's ITSec objectives and **general risk profile**
   - Who gets to make that call? Who determines your orgs risk profile/security context/risk stance? **Use Standards!!**
2. Next, an IT Security Risk Assessment is needed for each asset in the organization that requires protection. (which assets are the most valuable/critical?)
   - Provides information necessary to decide what management, operational, and technical controls are needed.
3. Selecting suitable **controls** and then writing **plans** and **procedures** to ensure these necessary controls are implemented effectively. **Policy helps management make decisions!**

ISO standards: Why create them?

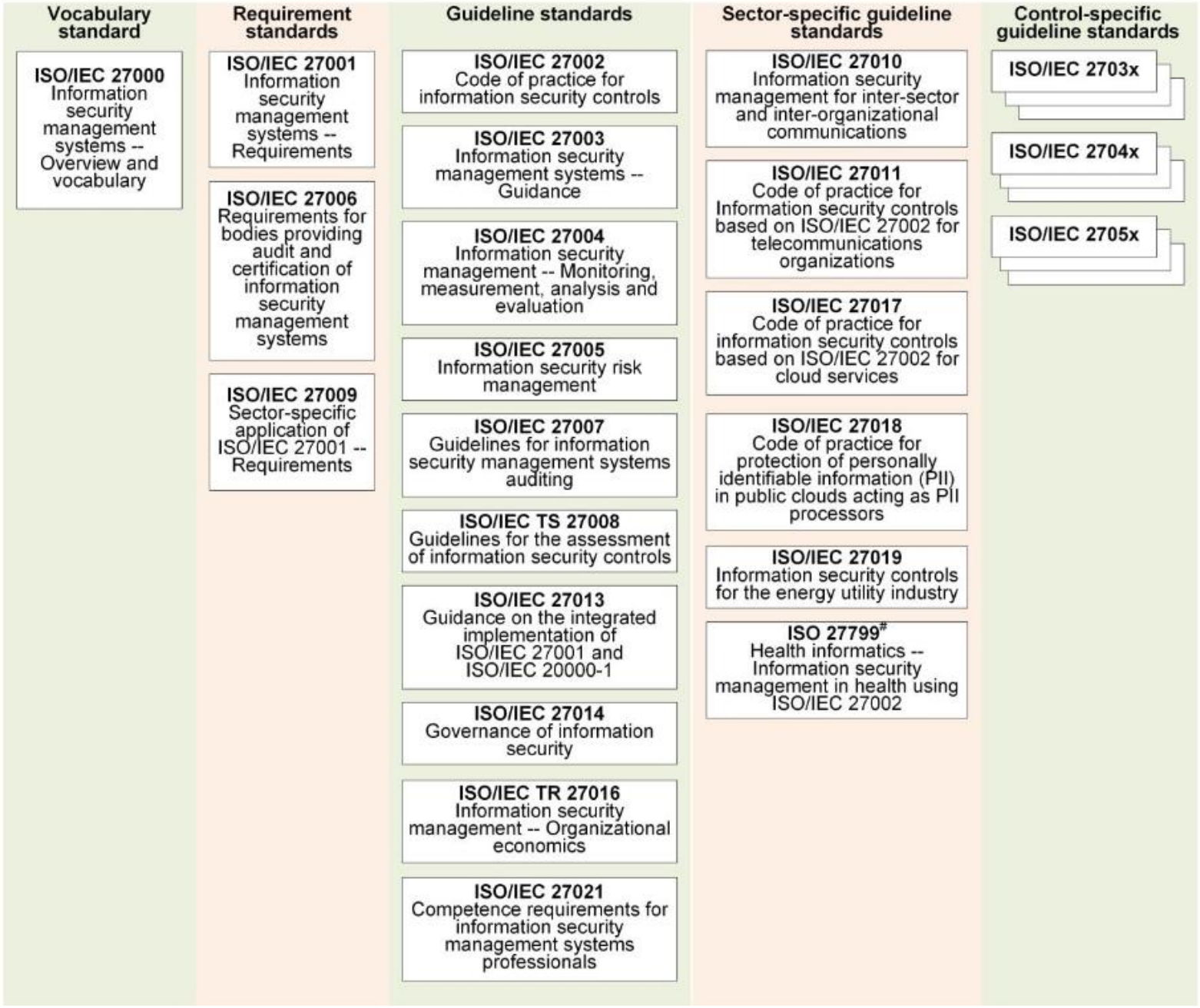
- **Assurance** when dealing with other businesses
  - Includes *compatibility* of products/services
- Competitive **Marketing** tool (to attract clients/customers)
- Assist with difficult ITSec and Planning **decisions** (including policy)
  - Benefit from the experience of other businesses
  - Cut costs through improved systems/processes
- **Accreditation** vs Certification?
- What is a "**standard**"?

ISO/IEC 27000 Series of Standards on IT Security Techniques

27000:2012	"Information security management systems - Overview and vocabulary" provides an overview of information security management systems, and defines the vocabulary and definitions used in the 27000 family of standards.
27001:2005	"Information security management systems – Requirements" specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System.
27002:2005	"Code of practice for information security management" provides guidelines for information security management in an organization and contains a list of best-practice security controls. It was formerly known as ISO17799.
27003:2010	"Information security management system implementation guidance" details the process from inception to the production of implementation plans of an Information Security Management System specification and design.
27004:2009	"Information security management – Measurement" provides guidance to help organizations measure and report on the effectiveness of their information security management system processes and controls.
27005:2011	"Information security risk management" provides guidelines on the information security risk management process. It supersedes ISO13335-3/4.
27006:2007	"Requirements for bodies providing audit and certification of information security management systems" specifies requirements and provides guidance for these bodies.

These represent a consensus of the best practices in the field. NIST has similar standards.

ISO/IEC 27000 Family of Standards Relationships



ISO 27001: Objectives of the "Code of Practice"

To provide:

- A **comprehensive set of controls** comprising best practices in information security
- **Single reference point** for identifying the range of controls
- Suitable basis for industry, commerce, public and private sectors
- Confidence in inter-organisational trading

Establishing a Management Framework to:

- Define an Information Security Policy (ISP)
- Define the scope and boundaries
- Undertake a Risk Assessment
- Manage the risk
- Select appropriate controls
- Prepare a Statement of Applicability
- Implement the selected control objectives
- Document the system and control it
- Maintain the system and records

ISO standards tell us the things that need to be done. Very useful tool.

Japan has the most ISO certified companies in the world (ISO is not as popular in the US).

ISO/IEC 27001:**2013**

"Information technology, Security techniques, Information security management systems, Requirements"

Revisions from previous version (from 2005). See? *Standards change too!*

- This standard emphasises measurement and evaluation of an organisation's *Information Security Management System* (ISMS).
- A section on **outsourcing** has been added, which reflects that many organizations rely on third parties to provide some aspects of IT.
- Other continuous improvement processes like Six Sigma's DMAIC method can be implemented **instead of Plan-Do-Check-Act cycle** if desired.
- More attention is paid to the organizational context of information security, and **risk assessment** has changed.
- Overall, 27001:2013 is designed **to fit better** alongside other management standards such as ISO 9000 and ISO/IEC 20000 (deals with ITIL), and it has more in common with them. (very business/process centric. Roots in industry and manufacturing)

ISO/IEC 27001:2013 Controls – more updates

- Our textbook contains American / Commonwealth content, but Stallings recognizes that ISO/IEC is very important.
- An organisation can respond to risks with a **risk treatment plan**; an important part of this is choosing appropriate **controls**.
- These controls, and control objectives, are listed in Annex A of the standard.
- There are now **114 controls in 14 groups**; the old standard had 133 controls in 11 groups….

1. **Information security policies** (2 controls)
2. **Organization of information security** (7 controls)
3. **Human resource security** (6 controls)
4. **Asset management** (10 controls)
5. **Access control** (14 controls)
6. **Cryptography** (2 controls)
7. **Physical and environmental security** (15 controls)
8. **Operations security** (14 controls)
9. **Communications security** (7 controls)
10. **System acquisition, development and maintenance** (13 controls)
11. **Supplier relationships** (5 controls)
12. **Information security incident management** (7 controls)
13. **Information security aspects of business continuity management** (4 controls)
14. **Compliance** (8 controls)

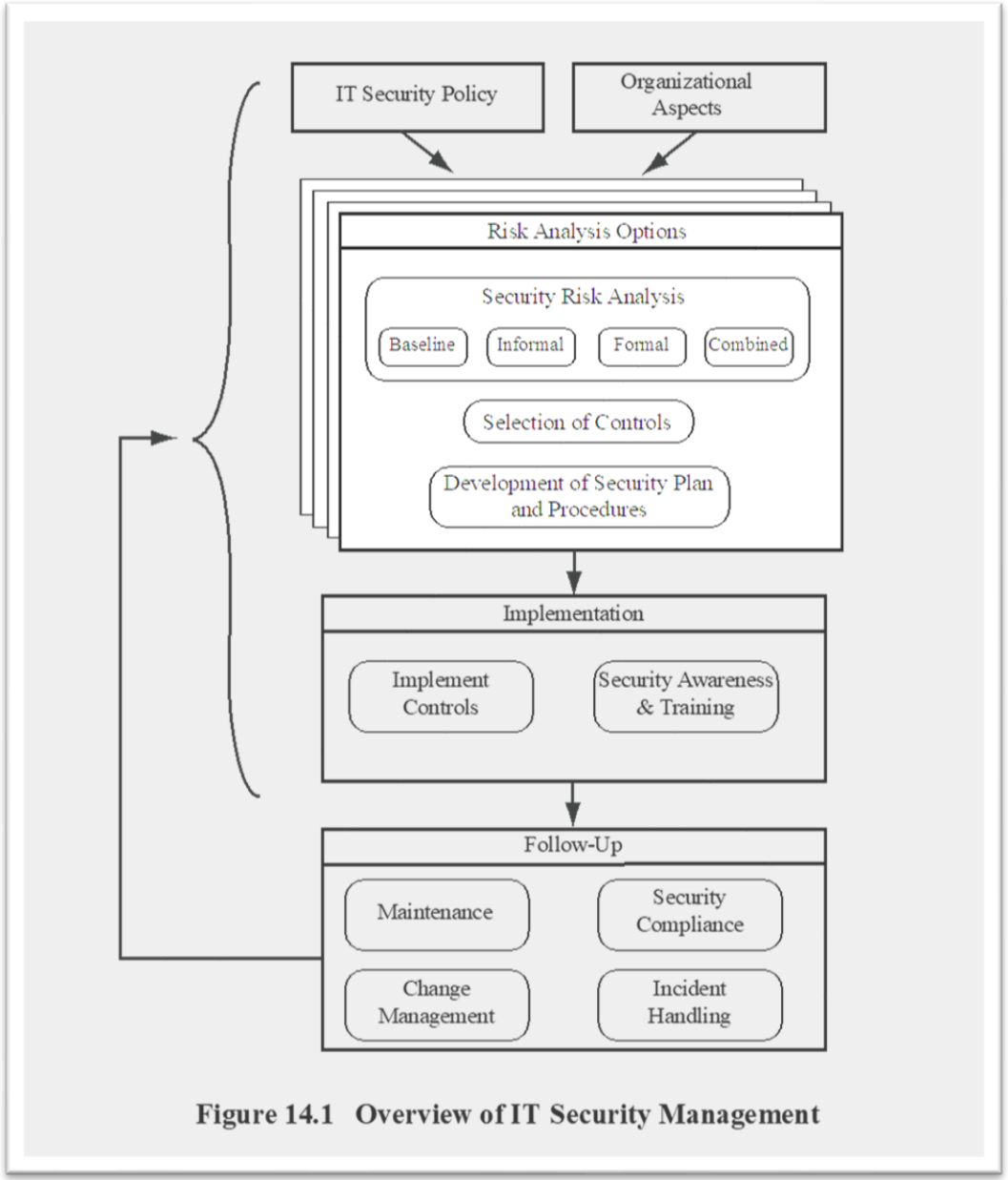


Figure 14.1 Overview of IT Security Management

IT management is not something undertaken just once. Rather it is a cyclic process that must be repeated constantly in order to keep pace with the rapid changes in both IT technology and the risk environment.

How fast does IT change? **Moore's Law?**
Doubles every 18-24 months?

Does/should this change how often you revise policy?

IT Security Management: [ISO13335] provides a conceptual framework for managing security. It defines **IT security management** as follows:

IT SECURITY MANAGEMENT: A process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity, and reliability. IT security management functions include:

Determining organizational IT security objectives, strategies, and policies	**Determining organizational IT security requirements**	**Identifying and analyzing security threats to IT assets within the organization**	**Identifying and analyzing risks**	**Specifying appropriate safeguards**	**Monitoring the implementation and operation of safeguards that are necessary in order to cost effectively protect the information and services within the organization**	**Developing and implementing a security awareness program**	**Detecting and reacting to incidents**

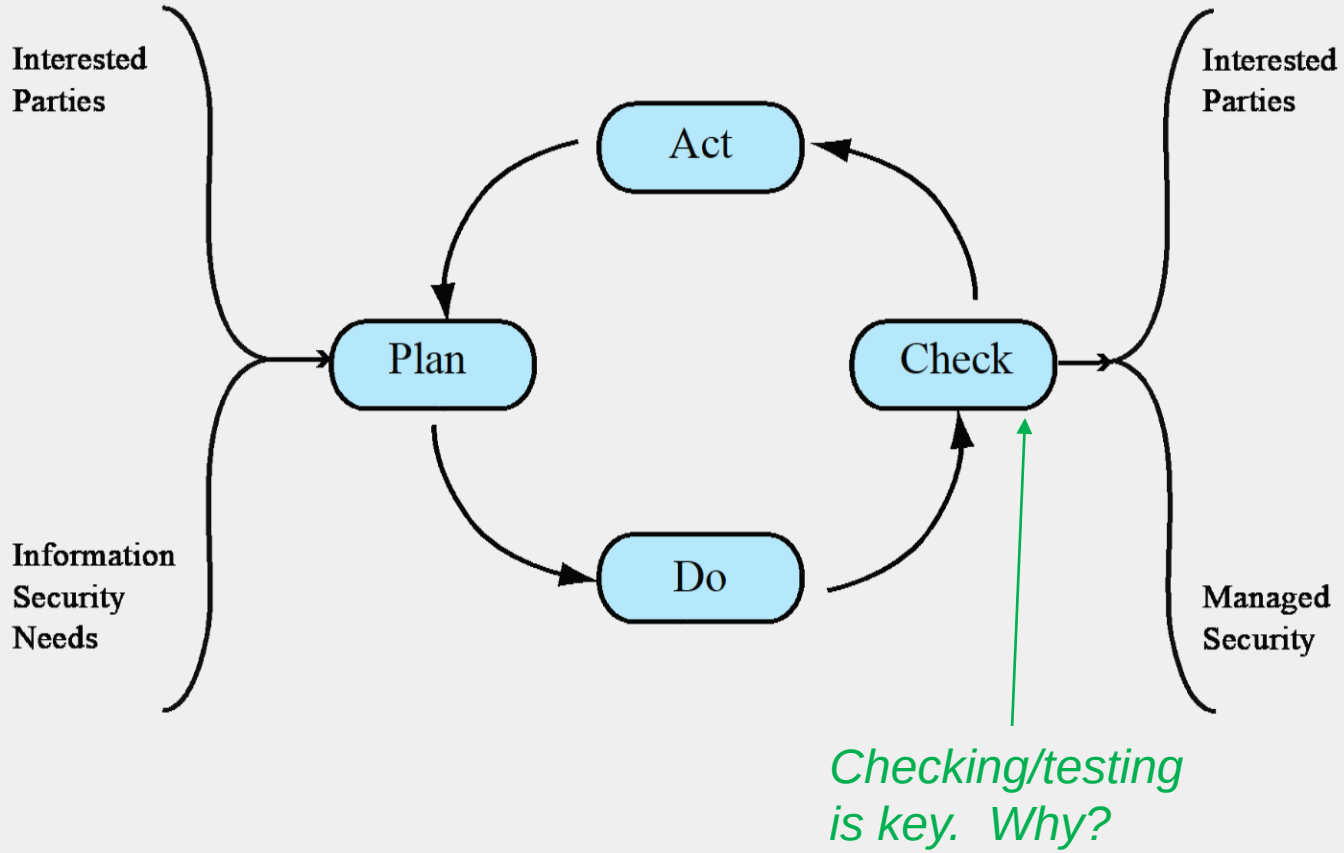


Figure 14.2 The Plan - Do - Check - Act Process Model

This is a model for managing information security that comprises the following steps:

PLAN: establish security policy, objectives, processes and procedures; perform risk assessment; develop risk treatment plan with appropriate selection of controls or acceptance of risk.

DO: Implement the risk treatment plan

CHECK: Monitor and Maintain the risk treatment plan

ACT: maintain and improve the information security risk management process in response to incidents, review, or identified changes

Policy

FANSHAWE

https://obayman9.wordpress.com/2014/09/26/excited-times-ahead/

Policy – what is it?

- A policy is a **statement** of intent, and is implemented as a procedure or protocol
- Policy guides **decisions** and achieves outcomes. May help determine **budget** priorities
- **Binding** to all employees
- No decisions can **contradict** policy, and policies cannot contradict each other or the law
- Can be an overarching **goal** (ex. We will beat any price by 10%)
- Have to be **enforceable** (include consequences for non-adherence or non-compliance)
- Often driven by organization's mission, relevant legislation, past experience, standards or Best Practices (BP).
- **Are you aware of any policies relevant to you at Fanshawe College?**
- **Do you have any personal policies? What prompted their creation?**

Organizational Context and Security Policy

Organizational Security:

- **Objectives** identify what IT security outcomes should be achieved
- **Strategies** identify how these objectives can be met
- **Policies** identify what needs to be done (strategy) to meet the objectives.
- These need to be maintained and **updated regularly** based on periodic security reviews
  - Reflect changing technical/risk environments

First examine organization's IT security:

Objectives - wanted IT security outcomes

Strategies - how to meet objectives

Policies - identify what needs to be done

Policies change (out of necessity)

Recommended review every 3 years.

Why 3 years?

- *Might take that long*
- *Distribute cost over that time*
- *Increases compliance*

InfoSec Policies

To help identify these organizational security objectives, the role and importance of the IT systems in the organization is examined. The value of IT systems in assisting the organization achieve its goals is reviewed, not just the direct costs of these systems.

Questions that help clarify these issues include the following:

- **What key aspects of the organization require IT support in order to function efficiently?**
- **What tasks can only be performed with IT support?**
- **Which essential decisions depend on the accuracy, currency, integrity, or availability of data managed by the IT systems?**
- **What data created, managed, processed, and stored by the IT systems need protection?**
- **What are the consequences to the organization of a security failure in their IT systems?**

Security Policy

If IT systems are important to the organization in achieving its goals, then clearly the risks to those systems should be assessed and appropriate action taken to address those risks. **A list of key organization security objectives should result** from this examination.

Once the objectives are listed, some broad strategy statements can be developed.

- outline in general terms how the identified objectives will be met in a consistent manner across the organization.
- The strategy statements should address the approaches the organization will use to manage the security of its IT systems.

Policy changes! you need a management plan that allows a **3 year cycle** to review all documentation and update as appropriate. You must have audited all your documents and controls to ensure they are still compliant.

Example: A policy must say you will review on a regular basis . A process kicks off that review (enacts it).

What can prompt a policy to change?

- ***new legislation, an incident, change in management, corporate direction, company growth***

Organizational Security Policies Must Address:

- Scope and purpose of policy; including relation of objectives to business, legal, regulatory requirements
- IT security requirements (CIA, accountability, authenticity, and reliability)
- Assignment of responsibilities – who manages IT Security?
- Risk management approach adopted/accepted by the organization/management (in writing!)
- Security awareness and training
- General personnel issues and any legal sanctions
- Integration of security into systems development
- Information classification scheme
- Contingency and business continuity planning - BIA
- Incident detection and handling processes
- How and when policy reviewed, and control if/how/when the policy changes

Management Support is **CRITICAL**

IT security policy/mandate must be supported/endorsed by senior management. This way, the policy is ***binding to all employees*** and empowers the IT security people with the authority to direct higher ranking employees

- Need IT security officer to
  - Provide consistent overall supervision
  - Liaison with senior management
  - Perform maintenance of IT security objectives, strategies, policies
  - Handle incidents
  - Manage the IT security ***awareness and training programs (SETA)*** ☺
  - Interact with IT project security officers

Larger Organizations…

- Large organizations need separate IT project security officers associated with major projects and systems. Their role is to:
  - Develop and manage security policies for their systems
  - Develop and implement security plans relating to these systems
  - Handle day-to-day monitoring of the implementation of these plans
  - Assist with the investigation of incidents involving their systems
- IOT – new facilities projects don't need to consider ITSec, do they?

RISK:

Assessment – Baseline, Informal, Detailed, Combined

Analysis

Management

FANSHAWE

Security Risk Assessment: the key risk management component of the IT security process

RA is a Critical component of any ITSM / ISMS process

Critical due to potential for improper or ineffective deployment of resources!

Is it possible to examine every risk to every asset?

Ideally examine every organizational asset

- Not feasible– too long, too expensive, many unknowns

Approaches to identifying and mitigating risks to an organization's IT infrastructure:

- Baseline Approach
- Informal Approach
- Detailed risk Analysis
- Combined Approach

Choice is determined by:
- resources
- initial risk analysis

Baseline Approach to Risk Analysis

- aims to implement a **basic, general level** of security controls on systems using baseline documents, codes of practice, and *industry* ***best practice***
- Provide protection against the **most common threats**
- Forms a good base for further security measures
- Uses “industry best practice” = **Standardization** or “one size fits all” or “turnkey”
  - Pro - Proven to be effective elsewhere
  - Pro - Easy and/or cheap to replicate
  - Con - Gives no special consideration to variations in risk exposure
  - Con - May give too much or too little security
- Generally recommended only for small organizations without the **resources** to implement more structured approaches
- ***Do we always need the best and most expensive? Or is something better than nothing?0***

Informal Approach to Risk Analysis

This is a **Qualitative** Approach

- involves conducting some form of informal, practical risk analysis for the organization's IT systems
- does not involve the use of a formal, structured process, but rather **exploits the knowledge and expertise** of the individuals performing this analysis.

Involves conducting an informal, pragmatic risk analysis on organization's IT systems

Exploits knowledge and expertise of analyst

Fairly quick and cheap

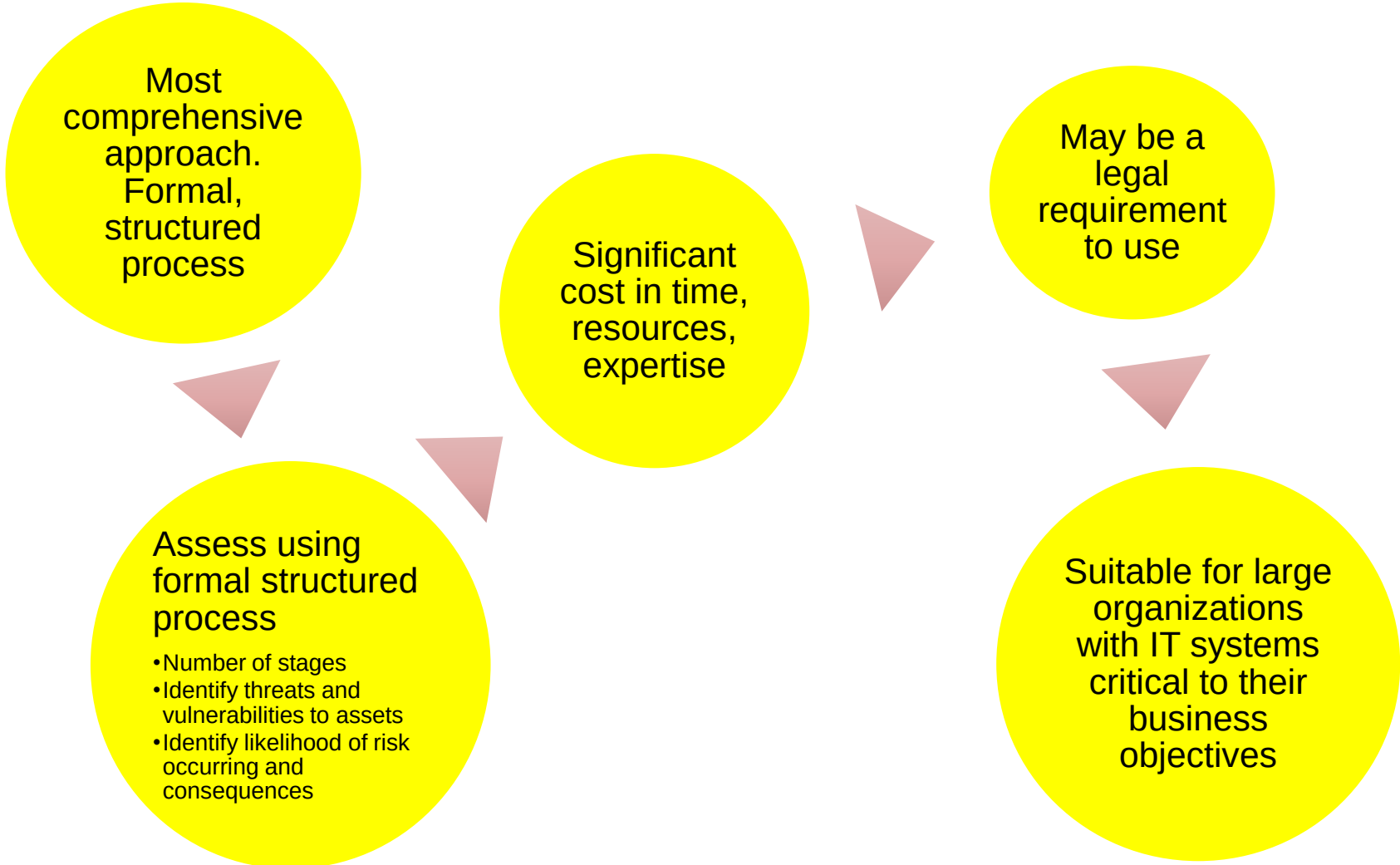
Judgments can be made about vulnerabilities and risks that baseline approach would not address

Some risks may be incorrectly assessed

Skewed by analyst's views, varies over time

Suitable for small to medium sized organizations where IT systems are not necessarily essential

Detailed Risk Analysis



Detailed Security Risk Analysis

Provides the most accurate evaluation of an organization's IT system's security risks

Highest cost

Initially focuses on addressing defense security concerns

Often mandated by government organizations and associated businesses

Why would gov't be required to complete this?

- ***Type of information***
  - ***Personal***
  - ***Secrets***
  - ***Required uptime***

What types of businesses need (or don't need) a detailed security risk analysis?

Combined/Hybrid Approach

1. Combines elements of other approaches
2. Initial baseline on all systems
3. Informal analysis to identify critical risks
4. Formal assessment on these systems

1. Results in the development of a strategic picture of the IT resources and where major risks are likely to occur
2. Ensures that a basic level of security protection is implemented early
3. For most organizations this approach is the most cost effective
4. Use is highly recommended

The decision on which approach to employ is OFTEN dictated by _____

FANSHAWE

This figure (reproduced from figure 3-1 in [NIST12]) illustrates a typical process used

This approach is often mandated by government organizations and associated businesses.

the expected **Formal/Detailed** risk analysis approach.

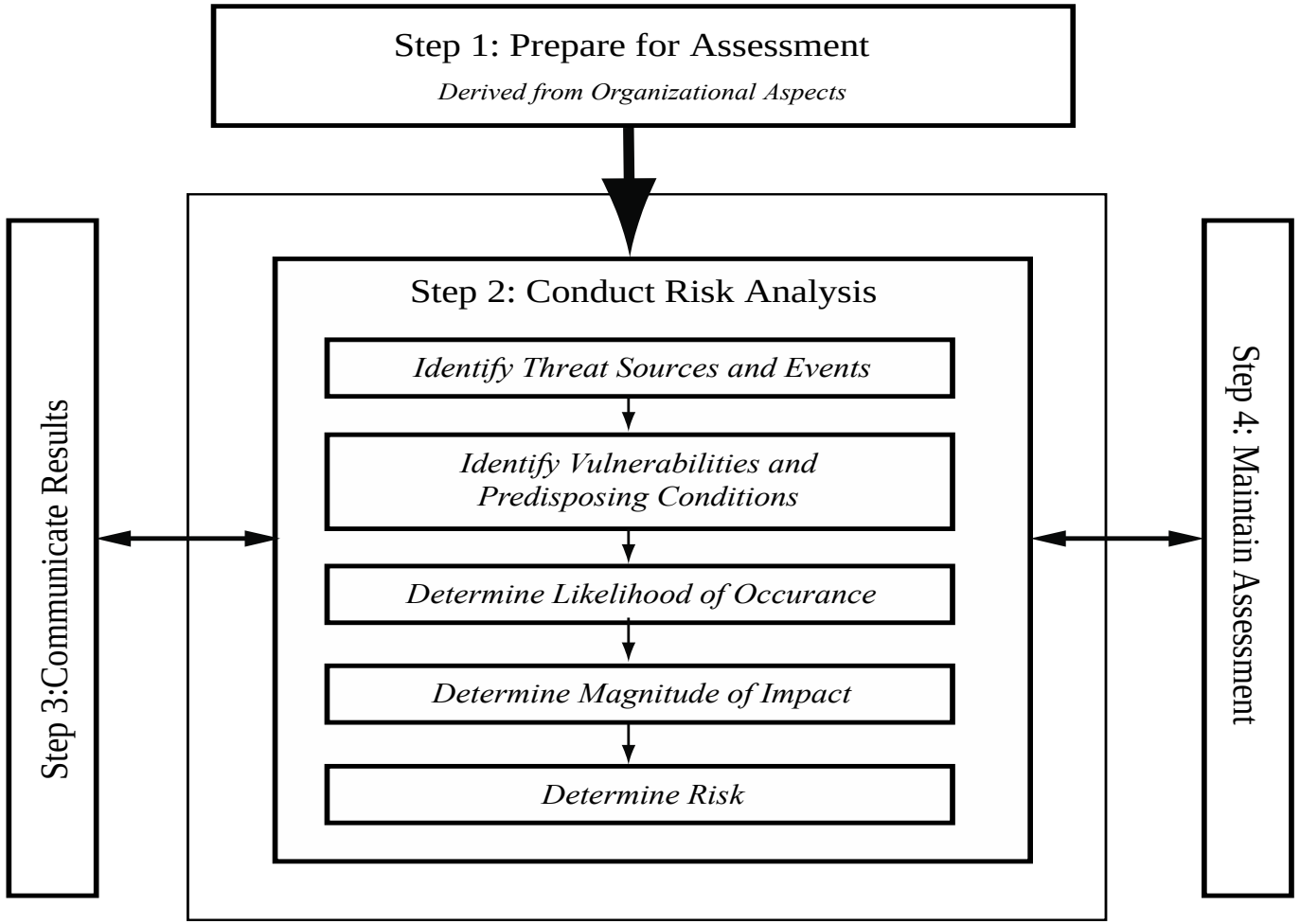


Figure 14.3 Risk Assessment Process

Establishing the Context aka "*System Characterization*"

Is the Initial step

- Purpose is to determine the basic parameters of the risk assessment, then to identify the assets to be examined (start small! Ex. **All** of Fanshawe College or just one department?)
  - **WHY?** Avoid "paralysis by analysis". Small scope = less costly mistakes. Crawl-walk-run.

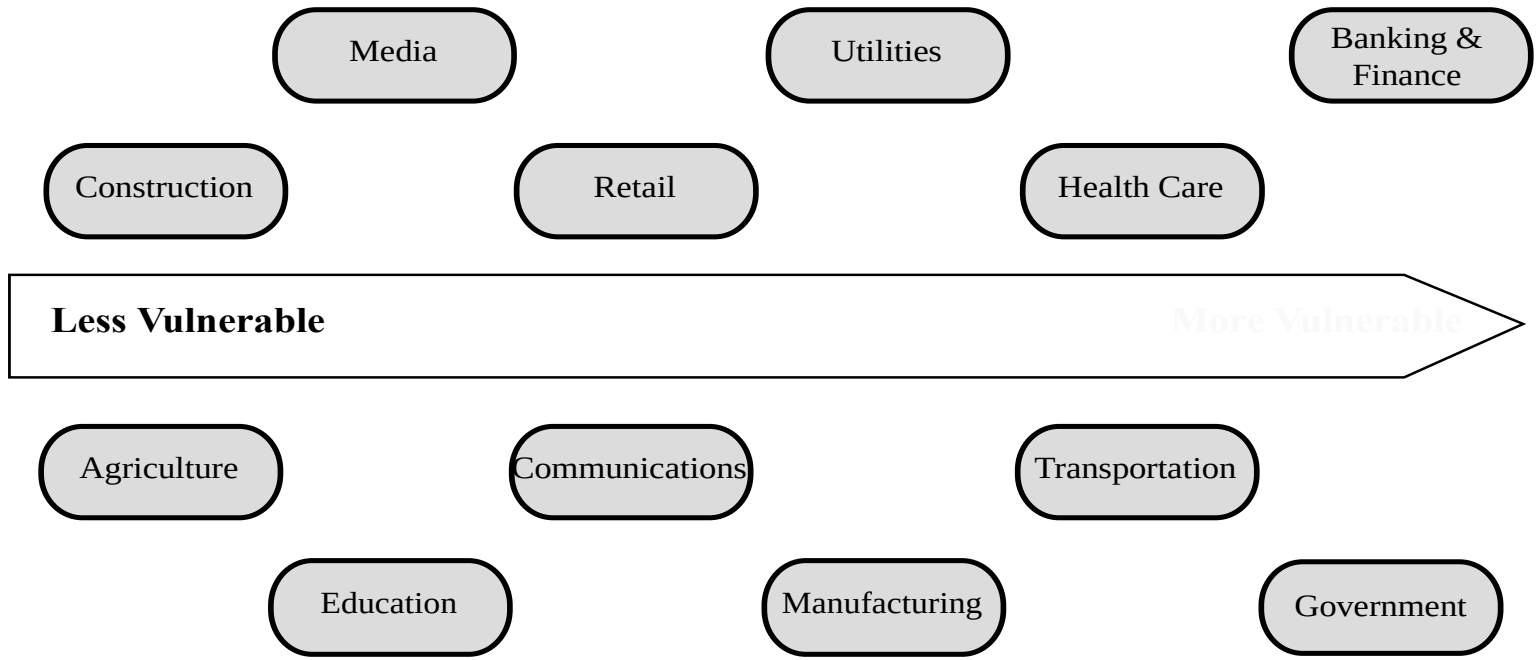
Explores **political and social environment** in which the organization operates

- Fanshawe choosing a Downtown campus vs East-end campus?
- Legal and regulatory constraints
- Provide baseline for organization's **risk exposure**. (aka: vulnerability) Will likely have to compromise somewhere. Deciding where is important!

Risk appetite

- The level of risk the organization views as **acceptable**

This figure (adapted from an IDC 2000 report) suggests a possible spectrum of organizational risk



When these industries collide, what happens?

Think critically!

Are construction and agriculture really less vulnerable?

Why or why not?

Think about the value of the assets of these industries…

Figure 14.4 Generic Organizational Risk Context

Brain Break!

(See you in 10 minutes!)

FANSHAWE

Asset Identification

- Last component is to identify assets to examine
- Draw on expertise of people in relevant areas of organization to identify key assets
  - Identify and interview such personnel

Asset

- "anything of **value** which needs to be **protected**"
- has value to organization to meet its objectives tangible or intangible whose compromise or loss would seriously impact the operation of the organization

Who are the best people to determine asset value?

Terminology Review

asset: anything that has value to the organization

threat: a potential cause of an unwanted incident which may result in harm to a system or organization

vulnerability: a weakness in an asset or group of assets which can be exploited by a threat

risk: the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets.

Threat Identification

- A threat is:

The pink bubbles are the key security services

Threat Sources

- Threats may be
  - Natural “acts of God”
  - Human or Man-made (intentional/deliberate or unintended - error)
  - Technical (ex. Equipment failure, power surge)

- Evaluation of human threat sources should consider
  - Motivation – why are you doing this?
  - Capability – are you able to do this?
  - Resources – do you have the resources required?
  - Probability of attack – what can make an attack more probable? Ex. Job loss? Stress?
  - Deterrence – **“inhibiting through fear of consequence”** (ex. target hardening, CPTED, transference, other controls)

- Any previous experience of attacks seen by the organization also needs to be considered (past history).

Vulnerability Identification

- Identify **exploitable flaws or weaknesses** in organization's IT systems or processes or the asset itself:
  - Determines applicability and significance of threat to organization
- **RISK**: it takes a combination of **threat + vulnerability** to create a risk to an asset.
- Outcome should be a list of threats and vulnerabilities with brief descriptions of how and why they might occur.
  - This goes into your BIA (Table 14.5 Risk Register)
    - Register examines & tracks, BIA adds valuation and treatmentDA / DR ratio.

Analyze Risks

- Specify **likelihood** of occurrence of each identified threat to asset given existing controls
- Specify **consequence/impact** should threat occur
- Derive overall risk rating for each threat
  - Risk = probability threat occurs x cost to organization
- Hard to determine accurate probabilities and realistic cost consequences
- Use qualitative ratings first. **Why?**
  - **Qualitative** defines the context of the assessment.
  - **Quantitative**: Challenges in assigning numerical value
  - Numbers are contextual and can be misleading
  - Focus on Priority / Rankings initially
    - COD / ROI will be examined in detail later.

Let’s talk about Controls

FANSHAWE

Analyze Existing **Controls**

- Controls are ways we mitigate/minimize risk
- **Existing controls** used to attempt to minimize threats need to be **identified**
- Security controls include:
  - **Management** processes and procedures
  - **Operational** processes and procedures
  - **Technical** processes and procedures
  - These controls are intended to reduce the exposure of the organization
- Use checklists of existing controls
  - e.g. Firewall in OS + hardware firewall = potential conflict. Others?
- Interview key organizational staff to solicit information that goes on that checklist.

Control Classes

Management controls

- Focus on policies, planning, guidelines, and standards
- Refer to issues that management needs to address
- Focuses on reducing the risk of loss and protecting the organization's mission
- Time and $$$

Operational controls

- Address correct implementation and use of security policies
- Correct identified operational deficiencies
- Relate to mechanisms and procedures that are **primarily implemented by people** rather than systems

Technical controls

- Involve the correct use of hardware and software security capabilities in systems
- Work together to secure critical and sensitive data, info, and IT systems functions.
- Avoid overlap and conflict.

NIST SP800-53 Security Controls

CLASS	CONTROL FAMILY
Management	Planning
Management	Program Management
Management	Risk Assessment
Management	Security Assessment and Authorization
Management	System and Services Acquisition
Operational	Awareness and Training
Operational	Configuration Management
Operational	Contingency Planning
Operational	Incident Response
Operational	Maintenance
Operational	Media Protection
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	System and Information Integrity
Technical	Access Control
Technical	Audit and Accountability
Technical	Identification and Authentication
Technical	System and Communications Protection

RISK

FANSHAWE

Risk Likelihood (also called Probability/Frequency)

Rating	Likelihood Description	Expanded Definition
1	**Rare**	May occur only in exceptional circumstances and may be deemed as “unlucky” or very unlikely.
2	**Unlikely**	Could occur at some time but not expected given current controls, circumstances, and recent events.
3	**Possible**	Might occur at some time, but just as likely as not. It may be difficult to control its occurrence due to external influences.
4	**Likely**	Will probably occur in some circumstance and one should not be surprised if it occurred.
5	**Almost Certain**	Is expected to occur in most circumstances and certainly sooner or later.

Rating	Consequence	Expanded Definition
1	**Insignificant**	Generally a result of a minor security breach in a single area. Impact is likely to last less than several days and requires only minor expenditure to rectify. Usually does not result in any tangible detriment to the organization.
2	**Minor**	Result of a security breach in one or two areas. Impact is likely to last less than a week but can be dealt with at the segment or project level without management intervention. Can generally be rectified within project or team resources. Again, does not result in any tangible detriment to the organization, but may, in hindsight, show previous lost opportunities or lack of efficiency.
3	**Moderate**	Limited systemic (and possibly ongoing) security breaches. Impact is likely to last up to 2 weeks and will generally require management intervention, though should still be able to be dealt with at the project or team level. Will require some ongoing compliance costs to overcome. Customers or the public may be indirectly aware or have limited information about this event.
4	**Major**	Ongoing systemic security breach. Impact will likely last 4-8 weeks and require significant management intervention and resources to overcome. Senior management will be required to sustain ongoing direct management for the duration of the incident and compliance costs are expected to be substantial. Customers or the public will be aware of the occurrence of such an event and will be in possession of a range of important facts. Loss of business or organizational outcomes is possible, but not expected, especially if this is a once off.
5	**Catastrophic**	Major systemic security breach. Impact will last for 3 months or more and senior management will be required to intervene for the duration of the event to overcome shortcomings. Compliance costs are expected to be very substantial. A loss of customer business or other significant harm to the organization is expected. Substantial public or political debate about, and loss of confidence in, the organization is likely. Possible criminal or disciplinary action against personnel involved is likely.
6	**Doomsday**	Multiple instances of major systemic security breaches. Impact duration cannot be determined and senior management will be required to place the company under voluntary administration or other form of major restructuring. Criminal proceedings against senior management is expected, and substantial loss of business and failure to meet organizational objectives is unavoidable. Compliance costs are likely to result in annual losses for some years, with liquidation of the organization likely.

Table can be found on pages 503-504 in textbook)

Risk Consequences

(also called impact/severity)

The organization's existing backup, disaster recovery, and contingency planning (or lack thereof) will influence the choice of rating

Risk Level Determination and Meaning

	Consequences					
Likelihood	**Doomsday**	**Catastrophic**	**Major**	**Moderate**	**Minor**	**Insignificant**
Almost Certain	E	E	E	E	H	H
Likely	E	E	E	H	H	M
Possible	E	E	E	H	M	L
Unlikely	E	E	H	M	L	L
Rare	E	H	H	M	L	L

Risk Level	Description
Extreme (E)	Will require detailed research and management planning at an executive/director level. Ongoing planning and monitoring will be required with regular reviews. Substantial adjustment of controls to manage the risk are expected, with costs possibly exceeding original forecasts.
High (H)	Requires management attention, but management and planning can be left to senior project or team leaders. Ongoing planning and monitoring with regular reviews are likely, though adjustment of controls are likely to be met from within existing resources.
Medium (M)	Can be managed by existing specific monitoring and response procedures. Management by employees is suitable with appropriate monitoring and reviews.
Low (L)	Can be managed through routine procedures.

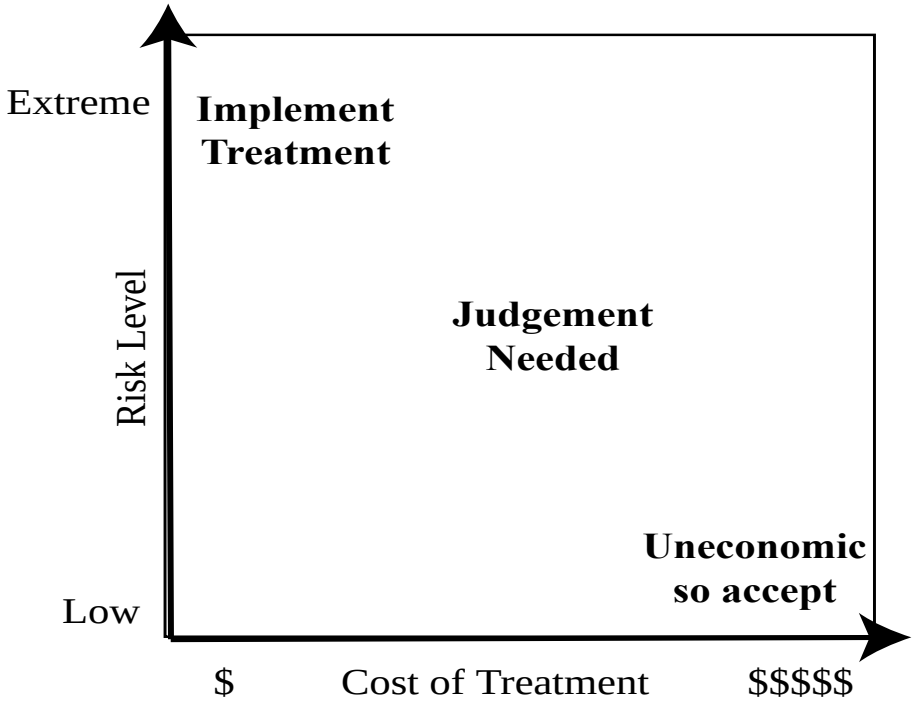
Risk Register

- The results of the risk analysis process should be documented in a **Risk Register**
- A **Risk Register** should include a summary table like this one.
- The risks are usually sorted in decreasing order of risk level/priority.
- Register examines & tracks, BIA adds valuation and treatment + DA / DR ratio
- *BIA uses Low, Medium, High* for Likelihood and Consequence for simplicity.

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Internet router	Outside hacker attack	Admin password only	Possible	Moderate	High	1
Destruction of data center	Accidental fire or flood	None (no disaster recovery plan)	Unlikely	Major	High	2

Risk Treatment

- Typically the risks with the higher ratings are those that need action most urgently
- it is likely that some risks will be easier, faster, and cheaper to address than others.

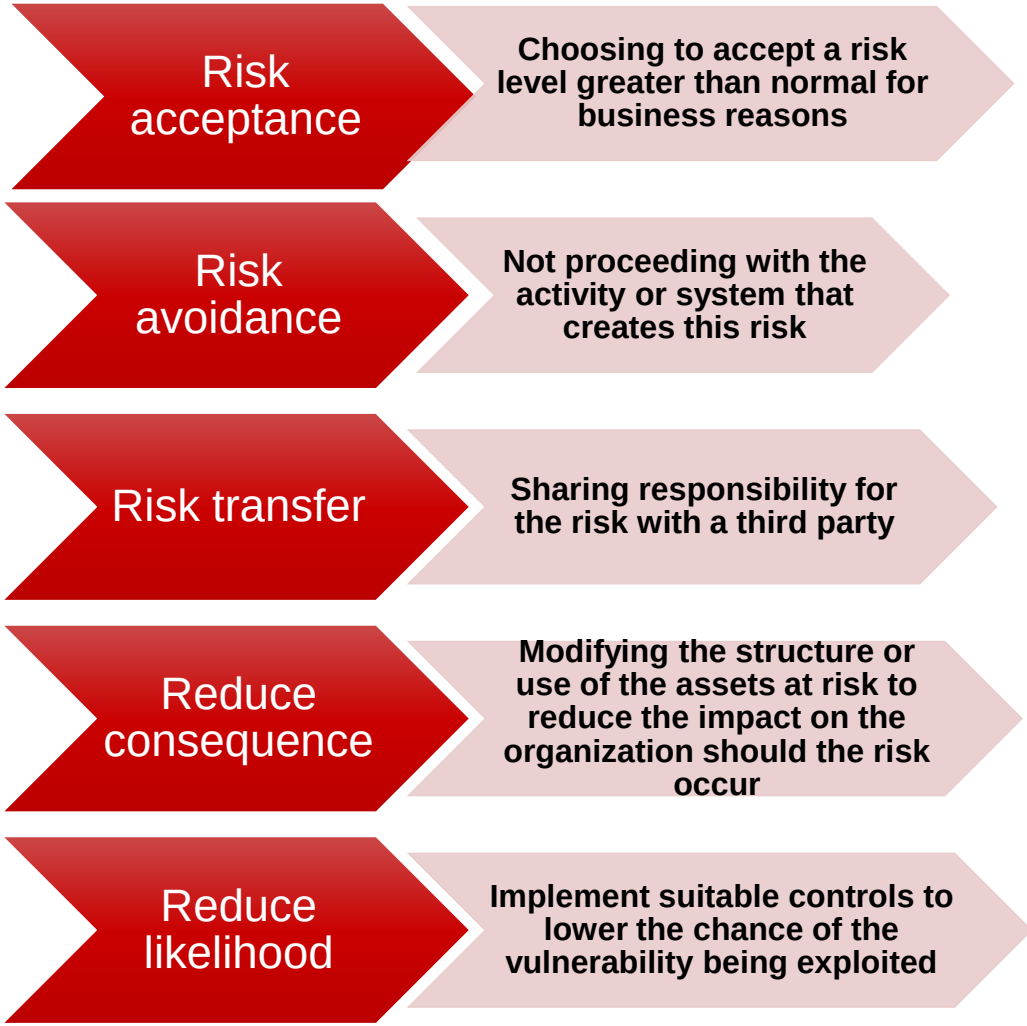


This figure indicates a range of possibilities for ***costs versus levels of risk***

Figure 14.5 Judgment About Risk Treatment

Risk Treatment Alternatives

These are five broad alternatives available to management for treating identified risk



Remember?

PLAN

DO

CHECK

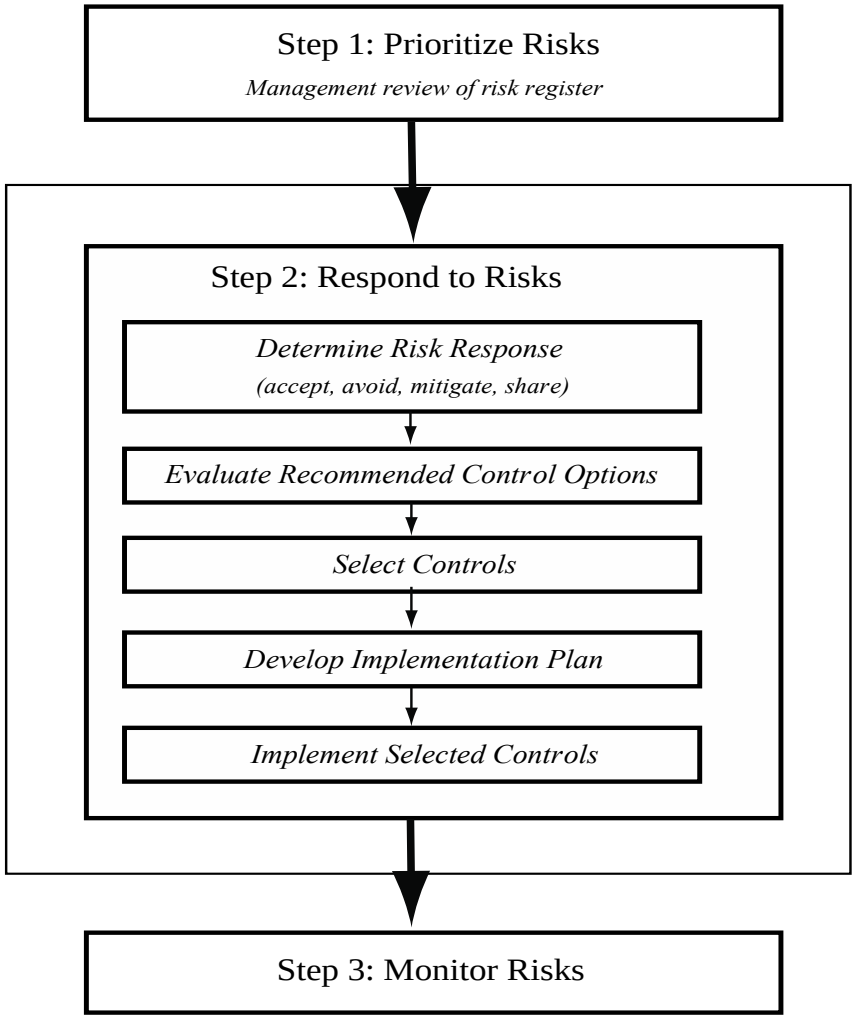


Figure 15.1 IT Security Management Controls and Implementation

Security Control

A Security Control (also called “safeguard” and/or “countermeasure”) is:

“A means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management, or legal nature” (2nd edition)

“An action, device, procedure, or other measure that **reduces risk** by **eliminating or preventing** a security violation, by **minimizing the harm** it can cause, or by discovering and reporting it to enable corrective action.” (3rd edition)

Notice that AVOIDANCE / MITIGATION is being emphasized more!!

Security Policies Ensure that information security policies support business requirements and comply with relevant laws and regulations.

Organization of Information Security Provide a management framework for controlling the implementation of security policies, and ensuring security of mobile devices.

Human Resource Security Ensure that employees and contractors understand and comply with security policies. Protect the organization's interests during the process of terminating or changing employment.

Asset Management Identify assets to be protected and define appropriate responsibilities for managing assets. prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

Access Control Define access privileges for access to information and information processing facilities. Ensure authorized user access and prevent unauthorized user access. Hold users accountable for safeguarding their authentication information.

Cryptography Ensure proper and effective use of cryptographic software and hardware so as to provide confidentiality, integrity, and authenticity services.

Physical and Environmental Security Define and implement policies to secure information processing facilities and to manage physical access to secure locations and secured facilities. Prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

Operations Security Ensure that the operation of information processing facilities conforms to security policies. Measures include ensuring that information and information processing facilities are protected against malware; protecting against loss of data; recording events and generate evidence; ensuring the integrity of operational systems to prevent exploitation of technical vulnerabilities.

Communications Security Implement security policies to protect network equipment and facilities, and to protect information transferred within an organization and with an external entity.

System acquisition, development and maintenance Ensure that security policies and procedures apply throughout a system's lifetime.

Supplier relationships Ensure that agreements with suppliers meet security policy requirements. Monitor and assess compliance with security agreements.

Information security incident management Implement an incident management capability that enables management of information security incidents, including reporting and documenting incidents and responses.

Information security continuity Ensure that security policies address requirements for incorporation into the organization's business continuity management systems.

Compliance Ensure that legal, statutory, regulatory or contractual obligations related to information security are met. Ensure that systems and personnel comply with the organization's security policies.

ISO/IEC 27002 Security Controls and Objectives

Do controls eliminate risk?

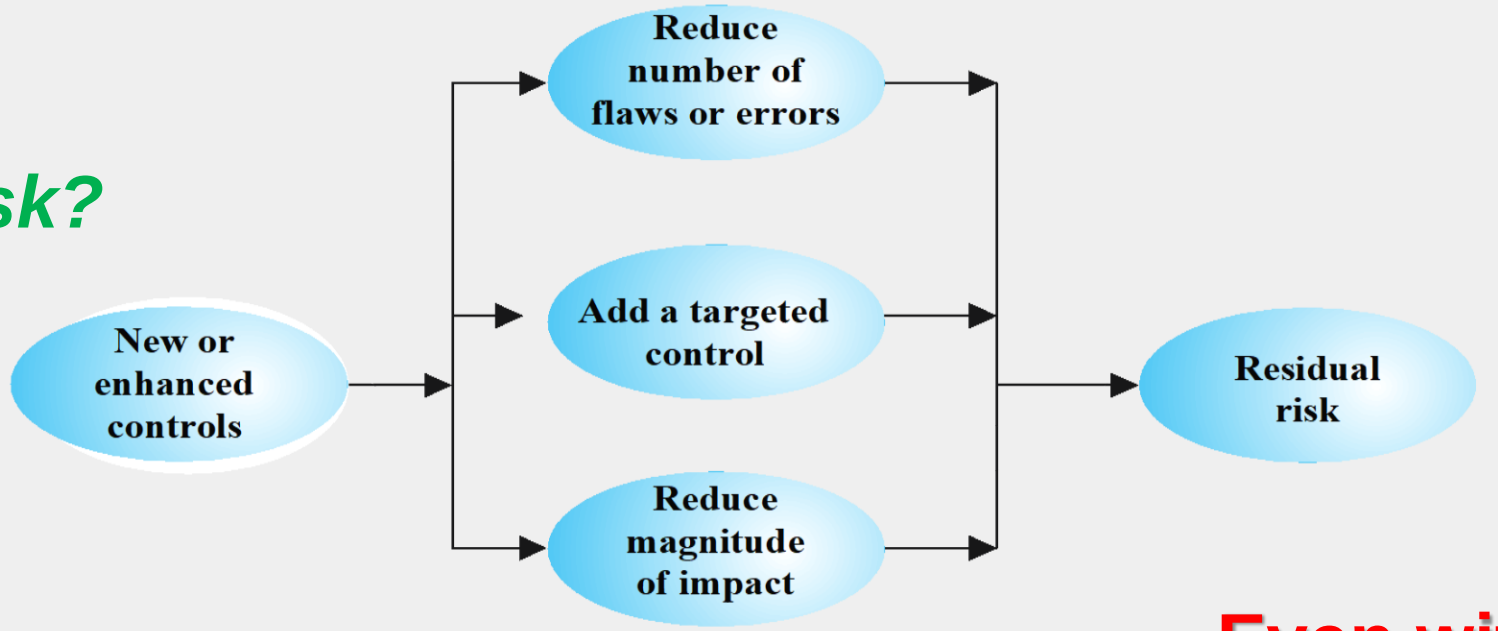


Figure 15.3 Residual Risk

Even with controls, there is still residual risk

Cost-Benefit Analysis

Should be conducted by management to identify controls that provide the greatest benefit to the organization given the available resources

May be qualitative or quantitative

Must show cost justified by reduction in risk

Should contrast the impact of implementing a control or not, and an estimation of cost

Management chooses selection of controls

Considers if it reduces risk too much or not enough, is too costly or appropriate

Fundamentally a business decision

IT Security Management Plan

- Provides details of:
  - What will be done
  - What resources are needed
  - **Who is responsible (ref: the policy!)**
- Goal is to detail the actions needed to improve the identified deficiencies in the risk profile

Should include

- Risks, recommended controls, action priority
- Selected controls, resources needed
- Responsible personnel, implementation dates
- Maintenance requirements

Implementation Plan Table – **An example**…

Risk (Asset/Threat)	Hacker attack on Internet router
Level of Risk	High
Recommended Controls	•Disable external telnet access •Use detailed auditing of privileged command use •Set policy for strong admin passwords •Set backup strategy for router configuration file •Set change control policy for the router configuration
Priority	High
Selected Controls	•Strengthen access authentication •Install intrusion detection software
Required Resources	•3 days IT net admin time to change & verify router configuration, write policies; •1 day of training for network administration staff
Responsible Persons	John Doe, Lead Network System Administrator, Corporate IT Support Team
Start – End Date	1-Feb-2011 to 4-Feb-2011
Other Comments	•Need periodic test and review of configuration and policy use

Why have an end date?

Security Plan Implementation

This process is usually monitored by an IT security officer.

- *Ensures that cost stay within bounds*
- *Desired risk level is achieved*
- *Controls are implemented when/as needed*.

IT security plan documents:

- What needs to be done for each selected control
- Personnel responsible
- Resources and time frame

Identified personnel:

- Implement new or enhanced controls
- May need system configuration changes, upgrades or new system installation
- May also involve development of new or extended procedures
- Need to be encouraged and monitored by management

When implementation is completed management needs to authorize the system for operational use

Maybe e a formal (ex. ISO accreditation) or informal process

Implementation Follow-Up *(the "Check" part)*

- Security management is **a cyclic process**
  - Constantly repeated to respond to changes in the IT systems and the risk environment
- Need to monitor implemented controls
- Evaluate changes for security implications
  - Otherwise increase chance of security breach

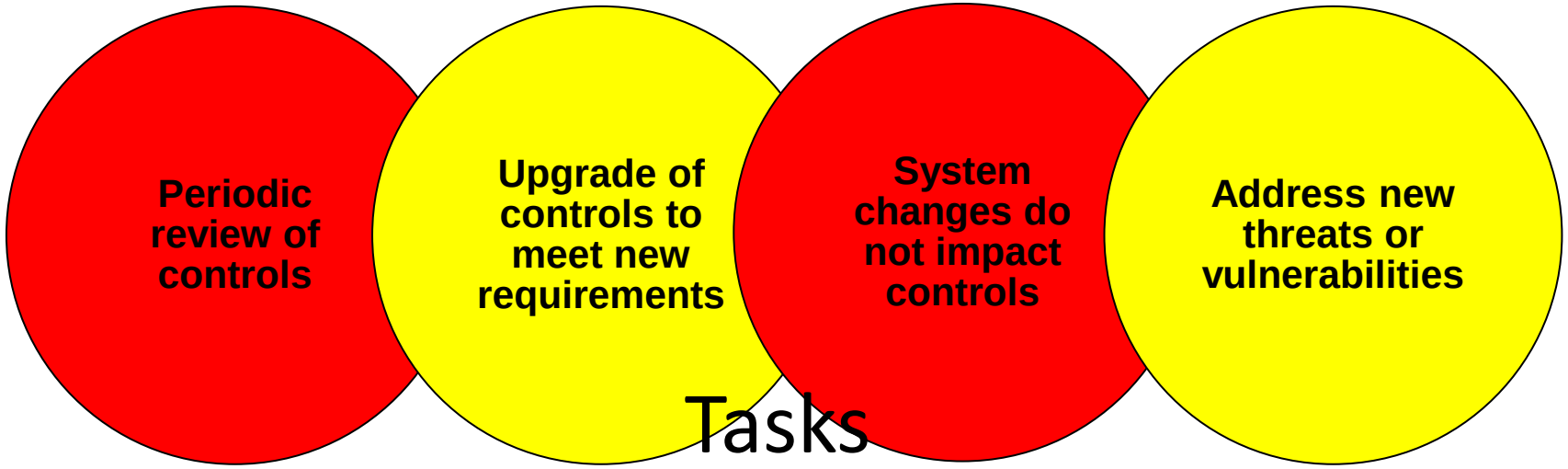
Implementation follow-up is often an afterthought (why?)*, but it is critical to the overall process*

Includes a number of aspects

- **Maintenance** (monitoring of implemented controls to ensure correct functioning)
- **Security compliance checking** (audit process)
- **Incident handling** (procedures used to respond to a security incident)
- **Change and configuration management** (review proposed changes)

Maintenance

- Need continued maintenance and monitoring of implemented controls to ensure continued correct functioning and appropriateness
- Goal is to ensure controls perform as intended



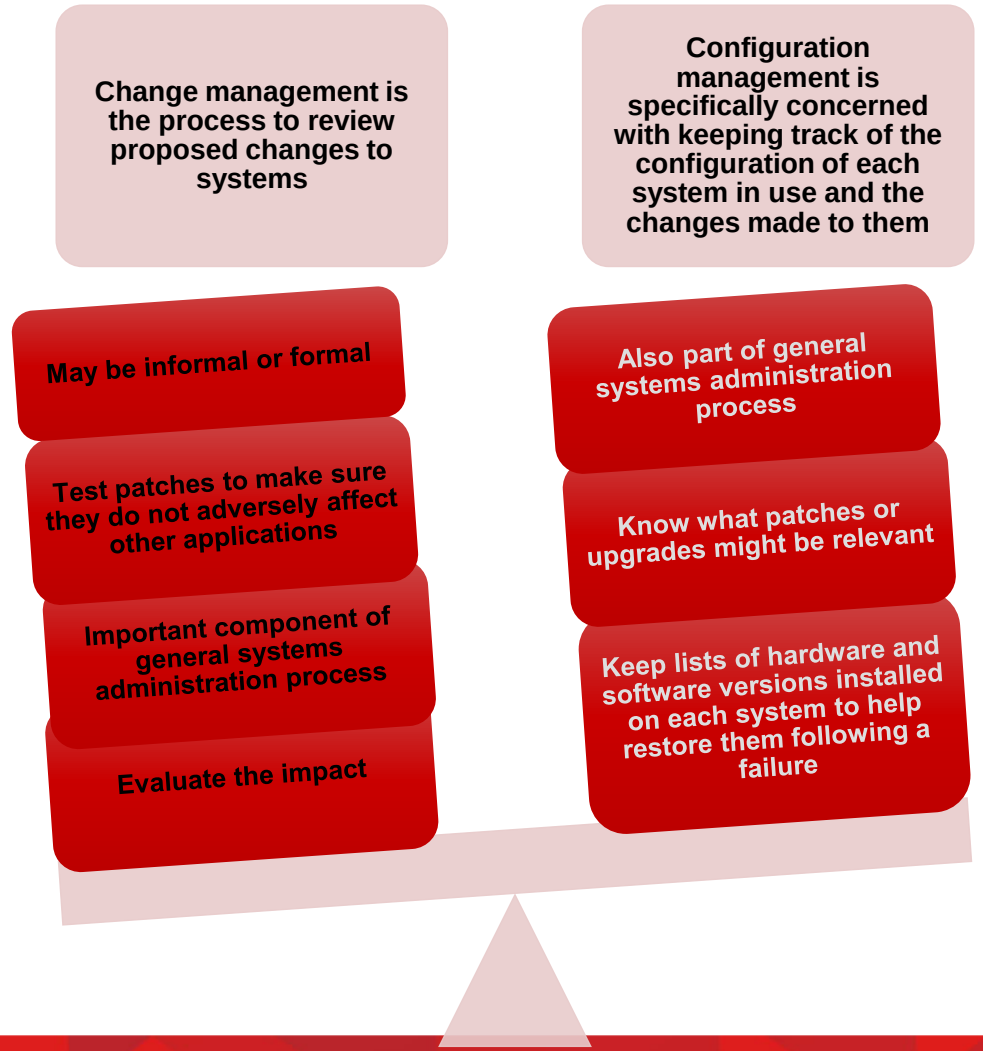
Security Compliance

- Audit process to review security processes
- Goal is to verify compliance with security plan
- Use internal or external personnel
- Usually based on use of checklists which verify:
  - Suitable policies and plans were created
  - Suitable selection of controls were chosen
  - That they are maintained and used correctly
- Often as part of wider general audit

Incident Handling

- Response
- Recovery
- Documentation!
- Statistical analysis
- Follow-up
  - Assignments, revisions, etc
- Policies/procedures
- Enforcement
- Communications

Change and Configuration Management



Summary

- IT security management
- Standards, Governance and Policy
- Security risk assessment
  - Baseline approach
  - Informal approach
  - Detailed risk analysis
  - Combined approach

Detailed security risk analysis

- Context and system characterization
- Identification of threats/risks/vulnerabilities
- Analyze risks
- Evaluate risks
- Risk treatment

- IT security management implementation
- Security controls or safeguards
- IT security plan
- Implementation of controls
  - Implementation of security plan
- Monitoring risks
  - Maintenance
  - Security compliance
  - Change and configure
  - Incident handling

FANSHAWE

Reminders

- Test week 6 Feb 08 on all material covered so far
- Next week we will be discussing:
  - Risk Management strategies
  - Corporate and security governance
  - Incident Management Systems
  - **We might also do some test review exercises ☺**