ACS-2821-001

Information Security in Business

Governance and Risk Management

ACS-2821-001 – Slides Used In The Course

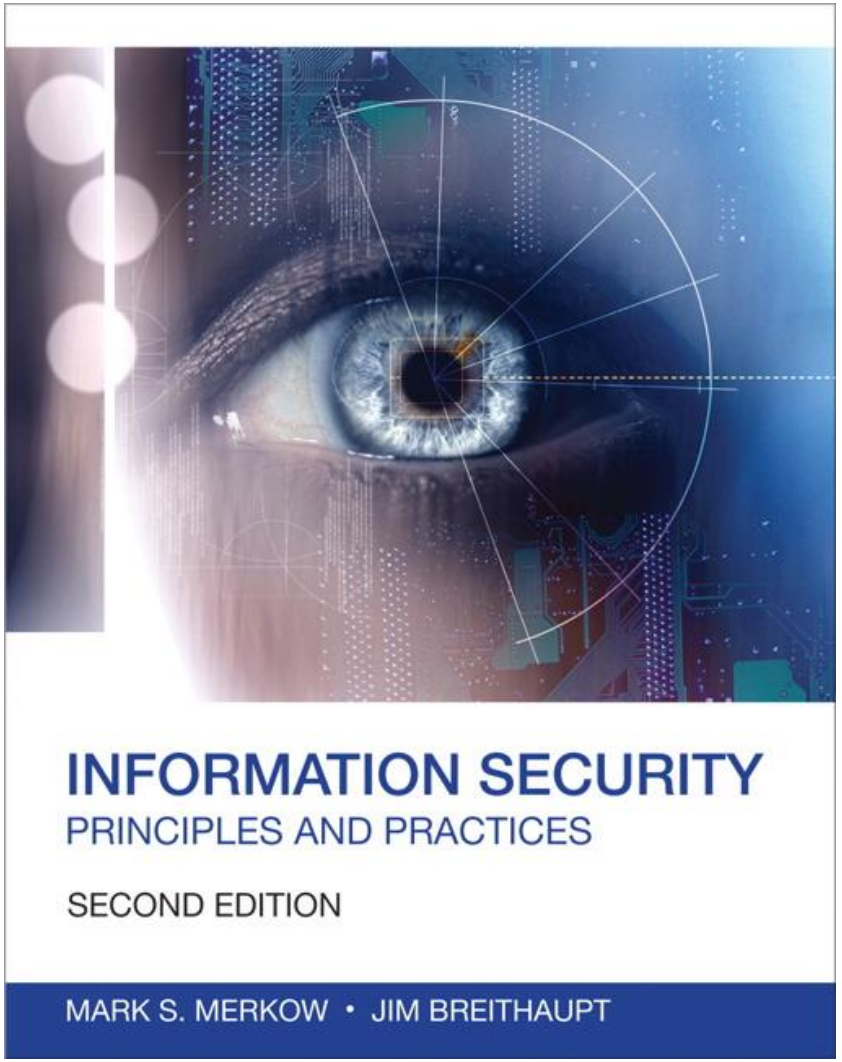
THE UNIVERSITY OF WINNIPEG

A note on the use of these slides:

These slides has been adopted and/or modified from the original for the use in this course. The author of the text have make these slides available to all (faculty, students, readers) and they obviously represent a *lot* of work on their part.

In return for use, please:

- If slides are being used (e.g., in a class) that the source be mentioned (after all, the author like people to use our book!)
- If any slides are being posted on a www site, note that they are adapted from (or perhaps identical to) the author original slides, and note their copyright of this material.



Objectives

- Governance vs Management
- Choose the appropriate type of policies
- Distinguish among the roles of standards, regulations, baselines, procedures, and guidelines
- Organize a typical standards and policies library
- Classify assets according to standard principles
- Incorporate the separation of duties principle
- Outline the minimum pre-employment hiring practices
- Analyze and manage risk
- IT Security Management
- Outline the elements of employee security education, awareness, and training
- List the eight types of people responsible for security

IT Security Governance vs IT Security Management

- IT Security Governance
  - Oversight and decision-making related to IT strategic direction
  - IT policies that outline the organization's IT purpose, values, and structure
  - Provide IT guidelines for management
- IT Security Management
  - Refers to the routine decisions and administrative work related to the daily IT operations of the organization
  - Management decisions support or implement goals and values defined by governing bodies (such as the Board of Directors) and documents (such as policies) with respect to IT security direction

Scope of Information Security in an Organization

- IT Security Governance, IT Risk Management and IT Security Management is a broad set of executive support and management activities that define an IT security programme
- IT security programme
  - Begins with statements of executive management's intent
  - Then translated into security policies
  - These then become the security standard, procedures and guidelines to follow

Security Policies Set the Stage for Success

- Policies are the most crucial element in a corporate information security infrastructure and must be considered before security technology is acquired and deployed
- Effective policies
  - Can rectify many of the weaknesses from failures to understand the business direction and security mission
  - Can help to prevent or eliminate many of the faults and errors caused by a lack of security guidance
  - Ultimately result in the development and implementation of better computer security and better protection of systems and information

Four Types of Policies

NIST defined the four type of policies as:

- Programme-level policy
- Programme-framework policy
- Issue-specific policy
- System-specific policy

Programme-level policy

- Establish a security programme
- Assign programme management responsibilities
- State an organization-wide computer security purpose and objectives
- Establish a basis for policy compliance
- Issued by senior management
- This high-level policy
  - Defines the purpose of the programme
  - Defines its scope within the organization
  - Assigns responsibilities for direct programme implementation as well as responsibilities to related offices
  - Addresses compliance issues

Programme-framework policy

- Provide an organization-wide direction for broad areas of programme implementation
- Define the organization's security programme elements that form the foundation for the computer security programme
- Reflect information technology management's decisions about priorities for protection, resource allocation, and assignment of responsibilities
- Examples of possible programme-framework policies
  - Business continuity planning (BCP) framework (Chapter 6)
  - Physical security requirements framework for data centers (Chapter 7)
  - Application development security framework (Chapter 13)

Issue-specific policy

- May come from the head of the organization, the top management official, the chief information officer (CIO), or the computer security programme manager (e.g., CISO)
- Examples
  - E-mail acceptable use
  - Internet acceptable use
  - Laptop security policy
  - Wireless security policy

Issue-specific policy cont.

- Basic components
  - Issue statement defines a security issue, along with any relevant terms, distinctions, and conditions
  - Statement of the organization's position clearly states an organization's position on the issue
  - Applicability clearly states where, how, when, to whom, and to what a particular policy applies
  - Roles and responsibilities assigns roles and responsibilities to the issue
  - ***Compliance gives descriptions of the infractions and states the corresponding penalties***
  - Points of contact and supplementary information lists the names of the appropriate individuals to contact for further information and lists any applicable standards or guidelines

System-specific policy

- State security objectives of a specific system
- Define how the system should be operated to achieve security objectives
- Specify how the protections and features of the technology used to support or enforce the security objectives
- Normally issued by the manager or owner of the system but may originate from a high-level executive or official
- Examples
  - Who is allowed to read or modify data in the system?
  - Under what conditions can data be read or modified?
  - Are users allowed to dial into the computer system from home or while on travel?

Development and Management of Security Policies

- Three-level model for system security policy
  - Security objectives
    - Consist of a series of statements to describe meaningful actions about specific resources
    - The three common questions in security management are:
      - What assets need to be protected
      - How are those assets threatened
      - What can be done to counter those threats
  - Operational security
    - List the rules for operating a system.
  - Policy implementation
    - The organization must determine the role technology plays in enforcing or supporting the policy

Policy Support Documents

- Provide levels of detail supporting the policy and explaining the system development, management, and operational requirements, including
  - **Regulations**: Laws passed by regulators and lawmakers
  - **Standards and baselines**: Topic-specific (standards) and system-specific (baselines) documents that describe overall requirements for security
  - **Guidelines**: Documentation that aids in compliance with standard considerations, hints, tips, and best practices in implementation
  - **Procedures**: Step-by-step instructions on how to perform a specific security activity

Suggested Standards Taxonomy

- Standards are formal written documents that describe several security concepts that are fundamental to all successful programmes
- The highest level includes
  - Asset and data classification
  - Separation of duties
  - Pre-employment hiring practices
  - Risk analysis and management
  - Education, awareness, and training

Suggested Standards Taxonomy cont.

- Asset and Data Classification
  - Asset and data classification is needed by businesses and agencies to help determine how much security is needed for appropriate protection
- Separation of Duties
  - Separating duties within a business or organization helps limit any individual's ability to cause harm or perpetrate theft
- Employment Hiring Practices
  - Policies, standards, and procedures issued by human resources should address internal information security processes and functions

Suggested Standards Taxonomy cont.

THE UNIVERSITY OF WINNIPEG

- Education, Training, and Awareness
  - Because people are the weakest link in any security-related process, it's crucial that a security programme address user education, awareness, and training on policies and procedures
  - Education must be driven top-down and must be comprehensive
  - Training must be ongoing (at least annually) and also take place whenever policies change
- Risk Analysis and Management
  - A risk analysis answers three fundamental questions:
    - What am I trying to protect?
    - What is threatening my system?
    - How much time, effort, and money am I willing to spend?

IT Security Risk Assessment Approach

There are four approaches to identifying and mitigating risks in an organization:

- Baseline
- Informal
- Detail Risk Analysis
- Combined

Baseline Approach

- Goal is to implement agreed controls to provide protection against the most common threats
- Forming a good base for further security measures
- Use industry recognize standards and best practice, e.g. ISO 27000, NIST SP-800 as guideline
- It is the easiest, most inexpensive, and can be replicated
- But this approach does not gives special consideration to variations in risk exposure
- May apply too much or too little security
- Is recommended only for a small organizations that do not have the resources to implement more structured approaches

Informal Approach

- Conducting an informal, pragmatic risk analysis on organization's IT systems
- Exploits knowledge and expertise of analyst
- It is fairly quick and inexpensive
- Would allow identifying vulnerabilities and risks that baseline approach would not have address
- Certain risks may still be incorrectly assessed
- Analyst's views may be skewed and varies over time
- Are suitable for small to medium sized organizations where IT systems are not necessarily essential

Detail Risk Analysis Approach

- Most comprehensive and accurate evaluation of an organization's IT system's security risks
- Significant cost in time, resources, expertise
- Focused on addressing defense security concerns
- Assess using formal structured process
- Number of stages and processes
- Identify threats and vulnerabilities to assets
- Identify likelihood of risk occurring and consequences
- May be a legal requirement to use
- Suitable for large organizations with IT systems critical to their business objectives

Combined Approach

- Combines elements of the baseline, informal, and detailed risk analysis approaches
- Provide reasonable levels of protection as quickly as possible and then examine and adjust the protection controls deployed on key systems over time
- Starts with the implementation of suitable baseline security recommendations on all systems
- Than systems that is exposed to high risk levels or critical to the organization's business objectives are identified in the high-level risk assessment
- A decision is made on these systems an immediate informal risk assessment aiming to quickly tailoring controls to more accurately reflect their requirements
- Lastly, an ordered process of performing detailed risk analyses of these systems can be instituted
- Over time, this approach can result in the most appropriate and cost-effective security controls being selected and implemented on these systems

Risk Assessment Process

A formal risk assessment approach are define into four steps:

- **Step 1: Prepare for Assessment**
  - Derived from organization aspect
- **Step 2: Conduct Risk Analysis**
  - Identify threat sources ad events
  - Identify vulnerability and predisposing conditions
  - Determine likelihood of occurrence
  - Determine magnitude of impact
  - Determine risk
- **Step 3: Communicate Result**
- **Step 4: Maintain Assessment**

Step 1: Preparing for Assessment

Need to established the context of the organization by:

- Determine the basic parameters and scope of the risk assessment
- Identify all the assets to be examined
- Determine political and social environment in which the organization operates
- Determine legal and regulatory constraints
- Provide baseline for organization's risk exposure
- Determine the organization risk appetite and the level of risk the organization views as acceptable
- Asset identification

Risk Management Terminology

- **Assets** – 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
- **Threat sources** – Can be either natural or human-made and may be accidental or deliberate
- **Vulnerability** – A weakness in an asset or group of assets that can be exploited by a threat
- **Risk** – the potential that a given threat will exploit vulnerabilities of an asset or a group of assets to cause loss or damage to the assets

Step 2: Conduct Risk Analysis

- Specify the likelihood of occurrence of each identified threat to asset and the given controls already in place
- Specify what consequence if the threat does occur
- Derive overall risk rating for each threat
  - Risk = (probability threat occurs) x (cost to organization)
- It maybe hard to determine accurate probabilities and realistic cost consequences therefore it maybe best using qualitative then quantitative ratings
- Two basic types of risk analysis
  - *Quantitative Risk Analysis*
  - *Qualitative Risk Analysis*

Quantitative Risk Analysis

- Attempts to establish and maintain an independent set of risk metrics and statistics
- Some of the calculations used for quantitative risk analysis
  - **Annualized loss expectancy (ALE)**: Single loss expectancy multiplied by annualized rate of occurrence
  - **Probability**: Chance or likelihood that an event will occur
  - **Threat**: An event, the occurrence of which could have an undesired impact
  - **Control**: Risk-reducing measure that acts to detect, prevent, or minimize loss associated with the occurrence of a specified threat
  - **Vulnerability**: The absence or weakness of a risk-reducing safeguard

Qualitative Risk Analysis

- The most widely used approach to risk analysis
- Makes use of a number of interrelated elements:
  - Threats: Things that can go wrong or that can “attack” the system
  - Vulnerabilities: Make a system more prone to attack or make an attack more likely to have some success or impact
  - Controls: The countermeasures for vulnerabilities

- A risk is real when there is a presence of threat, a vulnerability that the attacker can exploit, and a high likelihood that the attacker will carry out the threat

Step 2: Conduct Risk Analysis cont.

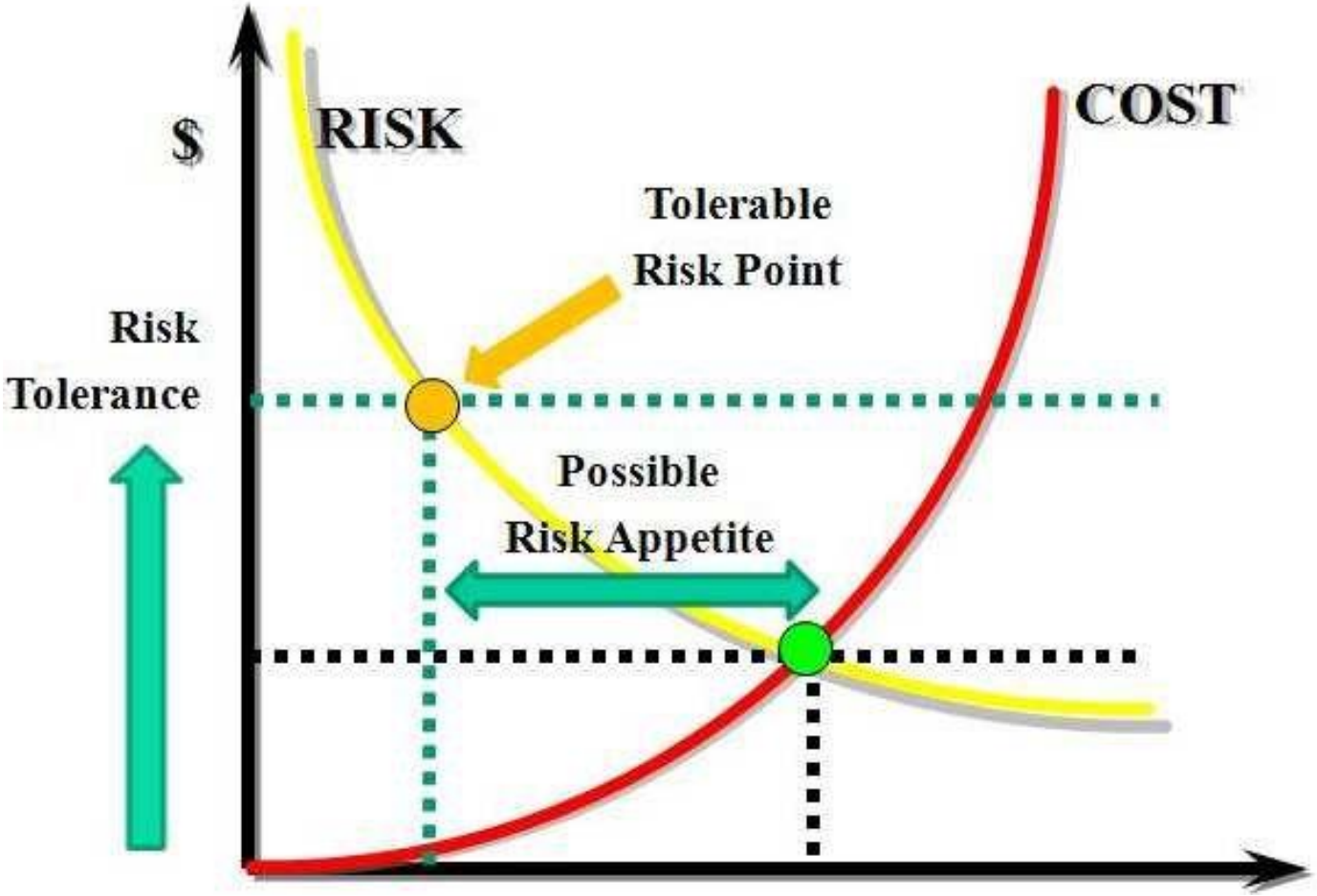
THE UNIVERSITY OF WINNIPEG

Analyze Existing Controls

- Existing controls used to attempt to minimize threats need to be identified
- Security controls include:
  - Management
  - Operational
  - Technical processes and procedures
- Use checklists of existing controls and interview key organizational staff to solicit information

Step 2: Conduct Risk Analysis cont.

Risk Treatment Vs Cost



Step 2: Conduct Risk Analysis cont.

THE UNIVERSITY OF WINNIPEG

Risk Treatment Alternatives

- **Risk acceptance**
  - Choosing to accept a risk level greater than normal for business reasons
- **Risk avoidance**
  - Not proceeding with the activity or system that creates this risk
- **Risk transfer**
  - Sharing responsibility for the risk with a third party
- **Reduce consequence**
  - Modifying the structure or use of the assets at risk to reduce the impact on the organization should the risk occur
- **Reduce likelihood**
  - Implement suitable controls to lower the chance of the vulnerability being exploited

Step 3: Communicate Result

- Risk Assessment Report and Risk Register
- Meet with management to discuss report finding
- Present management with different risk response, cost and benefit
- It will be up to the management to chose the right response and control

Risk Likelihood - Example

THE UNIVERSITY OF WINNIPEG

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.

Risk Consequences - Example

THE UNIVERSITY OF WINNIPEG

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.

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 - Example

THE UNIVERSITY OF WINNIPEG

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

Step 4: Maintain Assessment

- Maintained and updated regularly
  - Using periodic security reviews
  - Reflect changing technical/risk environments

IT Security Management

- Is a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity, and reliability

IT Security Management

IT security management are define into three steps:

Step 1: Prioritize Risks

- Management review of risk register

Step 2: Response to Risk

- Determine Risk Response (Accept, Avoid, Mitigate, Share)
- Evaluate Recommended Control Options
- Select Control
- Develop Implementation Plan
- Implement Selected Control

Step 3: Monitor Risks

What is a Security Control?

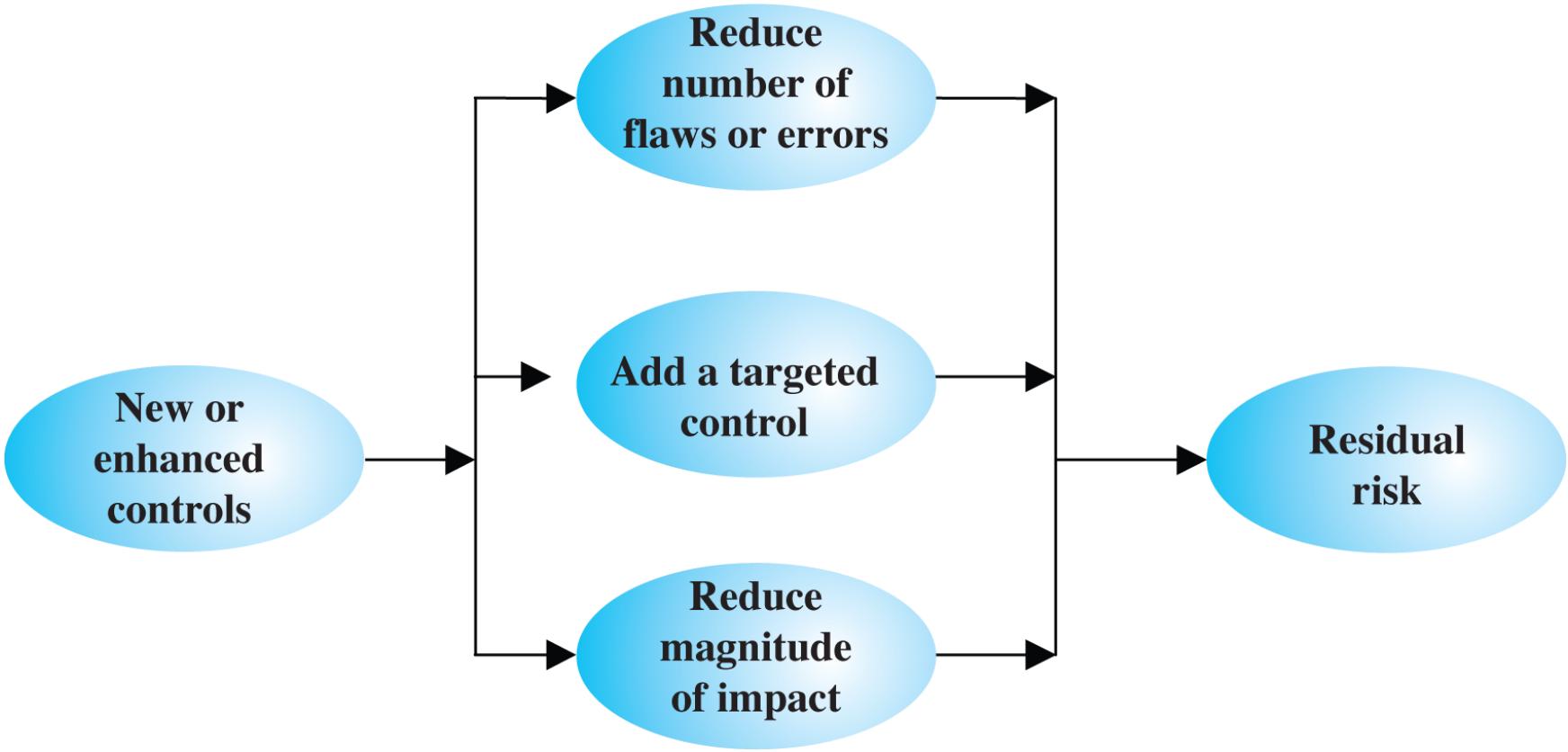
It can be an *action, device, procedure*, or *other measure* that reduces risk by eliminating or preventing a security violation, by minimizing the harm it can cause, or by discovering and reporting it to enable corrective action.

IT Security Management

Three Security Control Classes

- **Management controls**
  - Focus on security policies, planning, guidelines, and standards that influence the selection of operational and technical controls to reduce the risk of loss and to protect the organization's mission
  - These controls refer to issues that management needs to address
- **Operational controls**
  - Address the correct implementation and use of security policies and standards, ensuring consistency in security operations and correcting identified operational deficiencies
  - These controls relate to mechanisms and procedures that are primarily implemented by people rather than systems
  - They are used to improve the security of a system or group of systems
- **Technical controls**
  - Involve the correct use of hardware and software security capabilities in systems
  - These range from simple to complex measures that work together to secure critical and sensitive data, information, and IT systems functions

Residual Risk



IT Security Management

Security Plan Implementation

- **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 authorizes the system for operational use**

IT Security Management

Implementation Follow-Up

- Security management is a cyclic process
- Need to monitor implemented controls
- Evaluate changes for security implications

IT Security Management

Security Control Maintenance

- Maintenance of security controls to ensure
  - Periodic review of controls
  - Upgrade of controls to meet new requirements
  - System changes do not impact controls
  - Address new threats or vulnerabilities
- Security compliance checking
- Change and configuration management
- Incident handling

IT Security Management

Security Compliance

- Audit process to review security processes
- Goal is to verify compliance with security plan
- Can 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

IT Security Management

THE UNIVERSITY OF WINNIPEG

Change , Configuration and Patch Management

Change Management

- Is the process to review proposed changes to systems
- May be informal or formal
- Test patches to make sure they do not adversely affect other applications
- Important component of general systems administration process
- Evaluate the impact

Configuration Management

- Is specifically concerned with keeping track of the configuration of each system in use and the changes made to them
- Part of general systems administration process
- Keep lists of hardware and software versions installed on each system to help restore them following a failure
- Know what patches or upgrades might be relevant

Patch Management

- Security vulnerabilities are introduced by coding errors
- Once a necessary patch is identified, it should be tested to ensure it does not negatively impact operations. After the patch has been verified, it can be scheduled and installed where appropriate.

Who Is Responsible for Security

Everyone who uses information technology is responsible for maintaining the security and confidentiality of information resources and must comply with security policies and procedures

- Chief information security officer (CISO)
- Information resources manager
- Information resources security officer
- Owners of information resources
- Custodians of information resources
- Technical managers (network and system administrators)
- Internal auditors
- Users

Summary

- Security Management Practices domain is most concerned with the establishment and ongoing operation of the organization's security programme.
- This programme includes policies, standards, baselines, procedures, and guidance for compliance.

ACS-2821-001 – Questions?