

# IS4231

# Information Security Management

## Lecture 9

### Risk Management – Treating Risks

AY 2021/2022 Semester 2

**Lecturer:** Dr. YANG Lu

**Reading:** Chapter 7

# Learning Objectives

---

- ▶ Discuss the *strategy options* used to treat risk and be prepared to select from them when given background information
- ▶ Evaluate control alternatives under the defense risk treatment strategy and formulate a cost–benefit analysis (CBA) using existing conceptual frameworks
- ▶ Explain how to maintain and perpetuate controls
- ▶ Describe popular methodologies used in the industry to manage risk

# Topics

---

- ▶ Risk treatment strategies
- ▶ Feasibility and cost-benefit analysis
- ▶ Other methods of establishing feasibility
- ▶ Alternative risk management methodologies

## ► Risk Treatment Strategies

# Risk Treatment Strategies

---

- ▶ **An five basic risk control strategies:**
  - ▶ *Defense*—Applying safeguards that eliminate or reduce the remaining uncontrolled risk
  - ▶ *Transference*—Shifting risks to other areas or to outside entities
  - ▶ *Mitigation*—Reducing the impact to information assets should an attacker successfully exploit a vulnerability
  - ▶ *Acceptance*—Understanding the consequences of choosing to leave a risk uncontrolled and then properly acknowledging the risk that remains without an attempt at control
  - ▶ *Termination*—Removing or discontinuing the information asset from the organization's operating environment

# 1. Defense

---

- ▶ Attempts to **prevent** the exploitation of the vulnerability
- ▶ This is the preferred approach and is accomplished by means of countering threats, removing vulnerabilities in assets, limiting access to assets, and adding protective safeguards
- ▶ This approach is sometimes referred to as “avoidance”.
- ▶ Three common methods of risk defense are:
  - ▶ Application of policy
  - ▶ Application of training and education
  - ▶ Implementation of technology

## 2. Transference

---

- ▶ Attempts to shift risk to another entity
- ▶ Implement risk sharing by
  - ▶ Revising deployment models
  - ▶ Out-sourcing to other organizations
  - ▶ Implement service contracts with providers with more experience
  - ▶ Buying insurance
- ▶ **Transferral may create new risks, or modify existing risks (that have already been identified)**
  - ▶ May need additional risk treatment
  - ▶ Can share risk, but (usually) not possible to share liability of an impact

# Service Level Agreement

---

- ▶ The key to an effective transference risk control strategy is the implementation of an *effective service level agreement (SLA)*
- ▶ In some circumstances, an SLA is the only guarantee that an external organization will implement the level of security the client organization wants
- ▶ Recommended four steps to create a successful SLA
  - ▶ Determining objectives
  - ▶ Defining requirements
  - ▶ Setting measurements
  - ▶ Establishing accountability



## Example: Symantec Hosted Email Security SLA

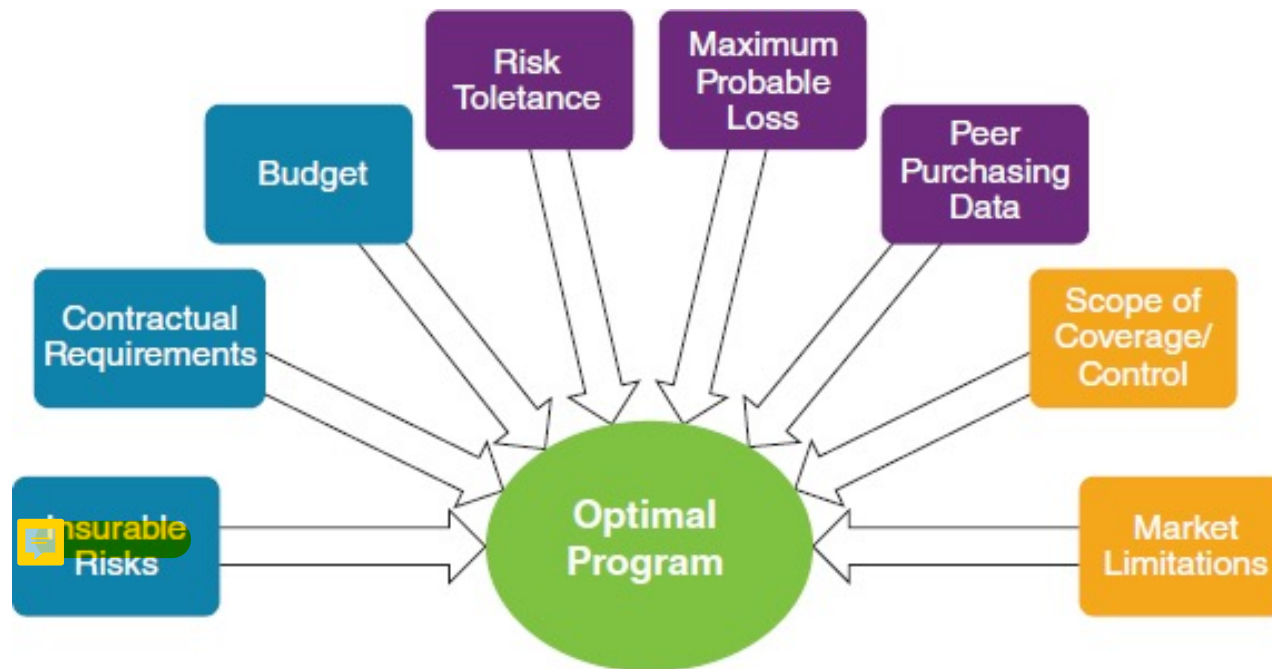
---

**“Our Service Level Agreement provides money back or other remedies if the following performance levels are not met:**

- ▶ Antivirus Effectiveness – 100% protection against known and unknown email viruses
- ▶ Antivirus Accuracy – no more than 0.0001% false positives
- ▶ Antispam Effectiveness – 99% spam capture (95% for email with Asian characters)
- ▶ Antispam Accuracy – no more than 0.0003% false positives
- ▶ Email Delivery – 100% email delivery
- ▶ Latency – average email scanning time within 60 seconds
- ▶ Availability – 100% service uptime”

# Buying insurance


- ▶ Typical components that make up an optimal cyber insurance program.



Source: Cybersecurity Handbook, 2017

### 3. Mitigation

---

- ▶ Attempt to reduce the impact of loss caused by an incident o disaster
  - ▶ Types of mitigation plans
    - ▶ Incident response (IR) plan
    - ▶ Disaster recovery (DR) plan
    - ▶ Business continuity (BC) plan
    - ▶ Crisis management (CM) plan
- 

## 4. Acceptance

---

- ▶ Knowingly and objectively accept the risk and do nothing beyond the current level of protection, because
  - ▶ The level of risk **meets the risk acceptance** criteria
- OR**
- ▶ The level of risk does *not* meet the risk acceptance criteria but the cost-benefit analysis shows that
  - ▶ The *costs* of controlling the risk are too high; or
  - ▶ The *benefits* accompanying the controls are extremely unattractive

this will usually be based on an economic/monetary perspective

# Risk Tolerance

## ► Risk tolerance table

► E.g.,

Risks companies might tolerate:

1. Power Outage - already have backup / chances are too low
2. Natural Disasters - too many resource limitation/too low chance
3. Tailgating problems - too difficult to control for low security areas

Risk Level	Risk Tolerance Description
<b>Very High</b>	This level of risk cannot be accepted and would create an impact so severe that the related activity would need to cease immediately. Alternatively, mitigation or transference strategies need to be taken immediately.
<b>High</b>	This level of risk cannot be accepted. Treatment strategies aimed at reducing the risk level should be developed and implemented in the next 1 month.
<b>Medium High</b>	This level of risk cannot be accepted. Treatment strategies aimed at reducing the risk level should be developed and implemented in the next 3-6 months.
<b>Medium</b>	This level of risk can be accepted if there are no treatment strategies that can be easily and economically implemented. The risk must be regularly monitored to ensure that any change in circumstance is detected and acted upon appropriately.
<b>Low</b>	This level of risk can be accepted if there are no treatment strategies that can be easily and economically implemented. The risk must be periodically monitored to ensure that any change in circumstances is detected and acted upon appropriately.

# 5. Termination

---

- ▶ Like acceptance, the termination risk management strategy is based on the organization's intentional choice not to protect an asset;
- ▶ Here, however, the organization does not wish the information asset to remain at risk and so removes it from the environment that represents risk
- ▶ Examples:
  - ▶ Equipment disposal
  - ▶ Discontinuing a provided service
  - ▶ Firing an employee

---

# Feasibility & Cost-Benefit Analysis



# Managing Risk

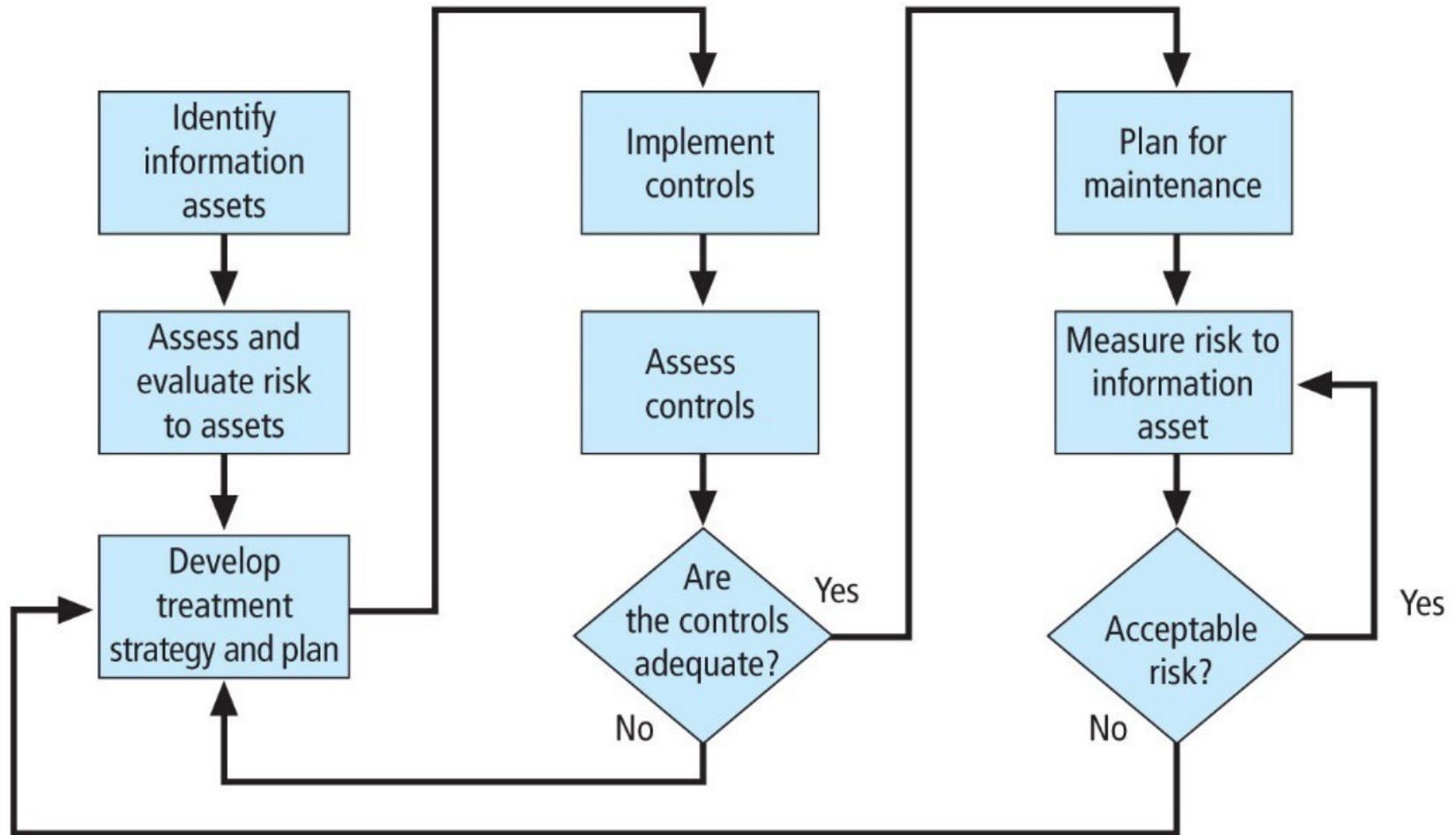
---

- ▶ **Residual risk**
  - ▶ The amount of risk that remains after the organization has implemented policy, education and training, and technical controls and safeguards
- ▶ The goal of information security is not to bring residual risk to zero; rather it is to bring it in line with an organization's risk appetite

Go to the assets management -> find the threats & vulnerability -> rank the risks -> control the risks



# Managing Risk



**Figure 7-4** Risk treatment cycle

# Feasibility Analysis

---

- ▶ Decision-making method that compares
  - ▶ *COST* of protecting an asset by implementing a risk control  
vs.
  - ▶ *ESTIMATED BENEFIT* that would accrue from implementation of the control
- ▶ Helps in selection and assessment of security controls
- ▶ The commonly used criterion when evaluating a strategy to implement InfoSec controls and safeguards is
  - ▶ Economic feasibility



# Cost

Total Cost Ownership - to take more perspectives to analyse the cost



- ▶ Life-cycle cost of implementing a control or safeguard includes things like:
  - ▶ Cost of developing or buying hardware, software, and services
  - ▶ Cost of getting personnel trained
  - ▶ Cost of implementation
    - ▶ Installing, configuring, and testing hardware & software
    - ▶ Professional services
  - ▶ Service costs
    - ▶ Vendor fees for maintenance and upgrades
  - ▶ Costs of maintenance
    - ▶ Labor expense to regularly verify test, maintain, train, and update
  - ▶ Potential cost from the loss of the asset

# Benefit

---

- ▶ The value to the organization of using controls to prevent **losses** associated with a specific vulnerability
- ▶ To calculate these we need to know
  - ▶ The dollar value of the information assets exposed by the vulnerability (i.e., **asset valuation**)
  - ▶ How much of that value is at risk
  - ▶ How much risk exists for the asset
- ▶ Expressed as the ***annualized loss expectancy*** (ALE)

# Asset Valuation

commercial entities will be easier to evaluate their branding  
- will be highly reflected by their consumer confidence in service/product  
- easily quantified/estimated from the financial market performances will be reflected very sensitively and immediately from the share performances

- ▶ The (complex) process of assigning financial value or worth to each **information asset**
- ▶ Different kinds of value, some easy to quantify while others more abstract
  - ▶ Real costs (concrete, easily quantifiable)
    - ▶ E.g., Direct replacement cost / maintenance cost
  - ▶ **Perceived or notional value**
    - ▶ E.g., Value of the **organization's reputation**
  - ▶ Acquired value ('real' value higher than intrinsic value)

how will NUS value their reputation



# Asset Valuation Approaches

---

- ▶ Some approaches of asset valuation include:
  - ▶ Value retained from the cost of creating the information asset
  - ▶ Value retained from past maintenance of the information asset
  - ▶ Value implied by the cost of replacing the information
  - ▶ Value from providing the information
  - ▶ Value acquired from the cost of protecting the information
  - ▶ Value to owners
  - ▶ Value of intellectual property
  - ▶ Value to adversaries
  - ▶ Loss of productivity while the information assets are unavailable
  - ▶ Loss of revenue while information assets are unavailable
  - ▶ Total cost of ownership

# Estimation of Potential Loss

- ▶ A traditional model of calculating quantitative cost–benefit analyses involves estimating the likelihood of an attack based on an annualized rate of occurrence and the impact of an attack based on loss expectancy
- ▶ The questions that must be asked: If a vulnerability is exploited
  - ▶ What loss or damage could happen, and what financial impact would it have?
  - ▶ What would it cost to recover from the attack, in addition to the financial impact of damage?
  - ▶ What is the single loss expectancy for each risk?

# Step 1: Calculate Single Loss Expectancy for the Vulnerability

---

- ▶ The most likely loss (in value) from a single exploitation of the vulnerability
- ▶ Inputs
  - ▶ AV = Asset Value
  - ▶ EF = Exposure Factor
    - ▶ Expected percentage loss that would occur from a given vulnerability being exploited

$$\text{SLE} = \text{AV} \times \text{EF}$$



## Step 2: Calculate Annualized Loss Expectancy for the Vulnerability

---

- ▶ Overall loss potential of the risk on an annual basis
  - ▶ Inputs
    - ▶ SLE (from Step 1)
    - ▶ ARO (Annualized Rate of Occurrence)
      - Indicates how often a *successful* attack (that exploits the vulnerability) is expected to occur in a year
    - ▶ Examples
      - If a successful attack occurs once every 2 years  $\Rightarrow ARO=0.5$
      - If an attack happens several times a second but succeeds once each month  $\Rightarrow ARO=12$ .
  - ▶ **ALE (Annualized Loss Expectancy)=SLE\*ARO**

# Example: Website


---

- ▶ Estimated value of website  $AV = \$1,000,000$ 
  - ▶ Sabotage/vandalism would damage or destroy 10% of website
  - ▶ Annualized rate of occurrence  $ARO=0.5$

So  $SLE=?$   $ALE=?$

$$SLE = 1000000 \times 0.1 = 100\ 000$$

$$ALE = 100\ 000 \times 0.5 = 50\ 000$$

 thus the selected control should cost less than 50k

# More Examples

---

Asset	Risk	AV	EF	SLE	ARO	ALE
Customer database	Hacked	\$432,000	0.74	\$320,000	0.25	\$80,000
Word documents and data files	Virus	\$9,450	0.17	\$1,650	0.9	\$1,485
Domain controller	Server failure	\$82,500	0.88	\$72,500	0.25	\$18,125
E-commerce website	DDoS	\$250,000	0.44	\$110,000	0.45	\$49,500

# What is the ALE good for?

---

- ▶ Indicates how much the organization could benefit from addressing a specific vulnerability
- ▶ A clear, easily understood value that can be used for budgetary purposes
- ▶ Can be used to test economic feasibility of every control alternative for a specific vulnerability
  - ▶ Using the **cost-benefit analysis formula**

# Feasibility Analysis (cont.)

---

- ▶ When is a feasibility analysis done?
  - ▶ *Before* a risk control is implemented, to decide if the control is worth implementing
  - ▶ *After* a risk control has been implemented and been functioning for some time, to assess if the control was worth implementing

**Organization should not spend more to protect an asset than the asset is worth!**

# Cost-Benefit Analysis (CBA) Formula

---

- ▶ **ALE(prior)**

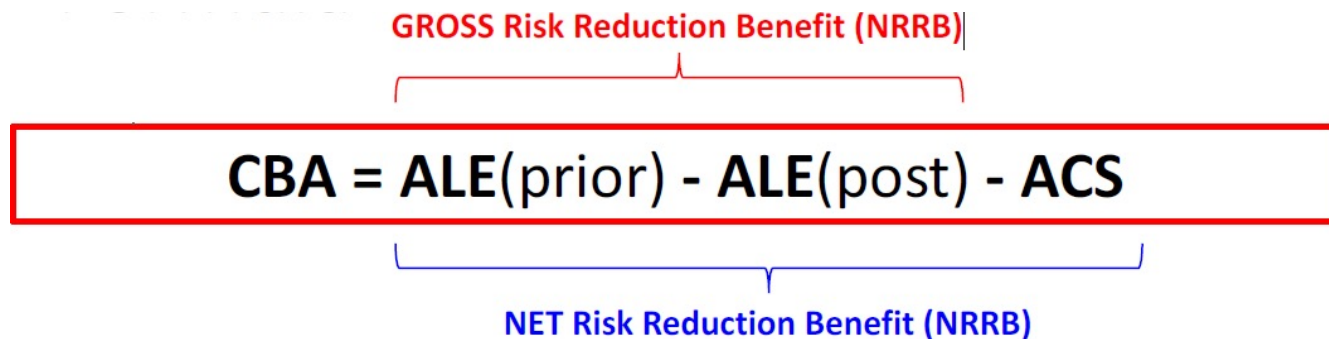
- ▶ Annualized loss expectancy *before* implementing the control

- ▶ **ALE(post)**

- ▶ Annualized loss expectancy *after* implementing the control

- ▶ **ACS**

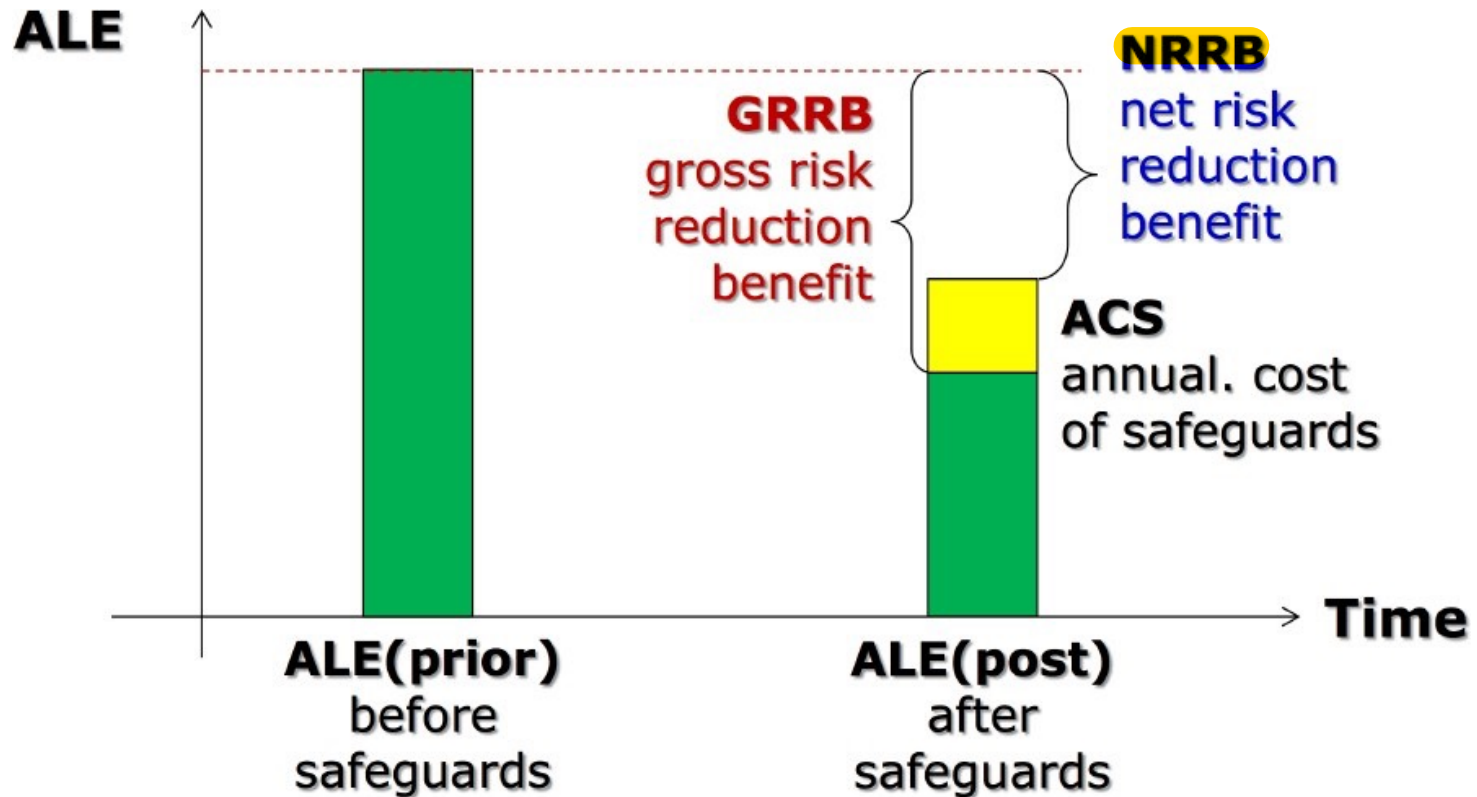
- ▶ Annual cost of **implementing the safeguard** (i.e., control)


$$\text{CBA} = \text{ALE}(\text{prior}) - \text{ALE}(\text{post}) - \text{ACS}$$

GROSS Risk Reduction Benefit (NRRB)

NET Risk Reduction Benefit (NRRB)

# Cost-Benefit Analysis (CBA) Formula (cont.)



Only  $NRRB > 0$  justifies the use of the control!

# Example: Determining NRRB

---

*Your organization has decide to centralize anti-virus support on a server which automatically updates virus signatures on user's PCs.*

*When calculating risk due to viruses, the annualized loss expected (ALE) is \$145,000.*

*The cost of this anti-virus countermeasure is estimated to \$24,000 per year, and it will lower the ALE to \$65,000.*

$$145 - 65 - 24 = 56k$$

*Is this a cost-effective control? Why or why not?*

*This control is cost-effective = Net Risk Reduction Benefit is 56k which is a positive number - plus it is around 50% of the original ALE (prior) thus it is very cost effective*



# Other Feasibility Measures

---

- ▶ Cost-benefit analysis determines whether a security control measure is economically feasible
- ▶ Other 'measures of feasibility' when evaluating a security control, include
  - ▶ Organizational feasibility
  - ▶ Operational (or behavioural feasibility)
  - ▶ Technical feasibility
  - ▶ Political feasibility

# Organizational Feasibility

---

- ▶ Examines how well a proposed information security control will contribute to organization's **strategic objectives**

to measure organisational feasibility - can just arrange a meeting with governance & senior manager team to check

# Operational Feasibility

---

- ▶ Known as behavioral feasibility
- ▶ Examines users' and management's **acceptance & support** of a proposed security control
  - ▶ e.g., A new policy / technology / programme will fail if users do not accept and support it
  - ▶ Most common methods for getting user acceptance
    - ▶ Communication
      - Affected parties must know the purpose and benefits of the proposed change
    - ▶ Education
      - Affected parties must be educated on how to work under the new constraints
    - ▶ Involvement
      - Affected parties must be given a chance to express what they want and what they will tolerate from the system



best way to detect/measure behavioral feasibility

= anonymous survey for pilot programmes

= focus group discussions

= workshops to interact with different employees

= adoption rate / usage time

# Technical Feasibility

---

- ▶ Determine whether organization has or can acquire the technology and/or tech expertise to implement and support the proposed controls
  - ▶ e.g., a firewall may require special software/hardware support/installation on all computers

# Political Feasibility

---

- ▶ Determines what can or cannot be done based on the consensus and relationships between the communities of interest
- ▶ e.g., IT and infosec departments may have to compete for same or limited resources      this might be because CISO is lower then CIO

or some privacy issue - since there are so many policy measures

- to monitor employee behaviour
- or to collect employee bio data or extra data

# Alternatives to Feasibility Analysis

---

- ▶ **Benchmarking**
- ▶ **Due care and due diligence**
- ▶ Best business practices
- ▶ Gold standard
  - ▶ Organizations aspire to set the standard for their industry.
- ▶ Government recommendations and best practices
- ▶ **Baseline**

# Documenting the Results of Risk Assessment

---

## ▶ What to document

### ▶ Risk Scenario

#### ▶ Threat event, vulnerability, asset, consequence

- E.g., Malware installed on POS terminals with no white-list application installation rule applied, makes credit card data stolen.

### ▶ Identification date

### ▶ Existing measures

### ▶ Current risk

### ▶ Treatment plan

### ▶ Progress status

### ▶ Residual risk

### ▶ Risk Owner

---

# Recommended Risk Control Practices





# Qualitative and Hybrid Measures

- ▶ Use if quantitative methods don't work or are too inaccurate
- ▶ Use *labels* for values
  - ▶ E.g., for ARO, list all the attacks possible on a particular information asset, then rate the attacks on low/medium/high probability of occurrence for annual risk of occurrence

	Definition
<b>Low</b>	0-25% chance of successful exercise of threat during a one-year period
<b>Moderate</b>	26-75% chance of successful exercise of threat during a one-year period
<b>High</b>	76-100% chance of successful exercise of threat during a one-year period

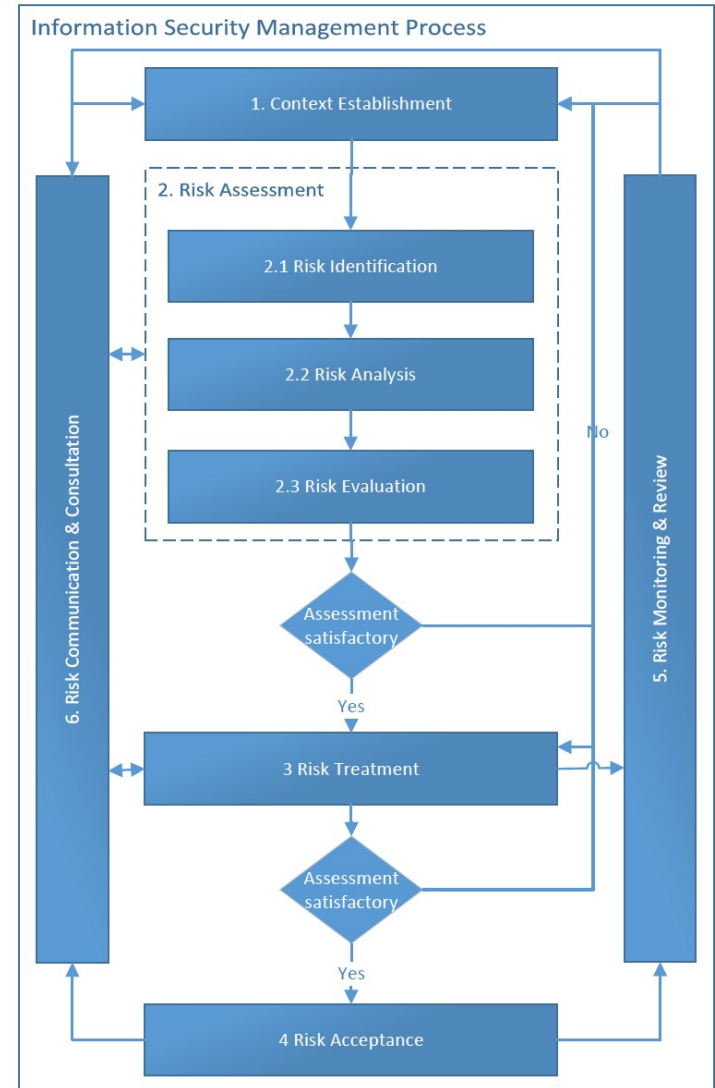
# Hybrid Assessment

---

- ▶ Try to improve on ambiguity of qualitative measures by using ranges of values instead of specific 'single number' values
- ▶ Examples
  - ▶ Chance of occurrence of a threat
    - ▶ Scale of 0 - 10, where
      - 0 = no chance of occurrence
      - 10 = almost certain occurrence
  - ▶ Value of information asset
    - ▶ Scale of 1 - 10, where
      - 1 = relatively worthless
      - 10 = extremely critical

# ISO27005 InfoSec Risk Management

- ▶ **ISO27005: Risk Management**
  - ▶ ISMS risk management process
    - ▶ 1. Context Establishment
    - ▶ 2. Risk Assessment
      - 2.1 risk identification
      - 2.2 risk analysis
      - 2.3 risk evaluation
    - ▶ 3. Risk Treatment
    - ▶ 4. Risk Acceptance
    - ▶ 5. Risk Monitoring & Review
    - ▶ 6. Risk Communication & Consultation

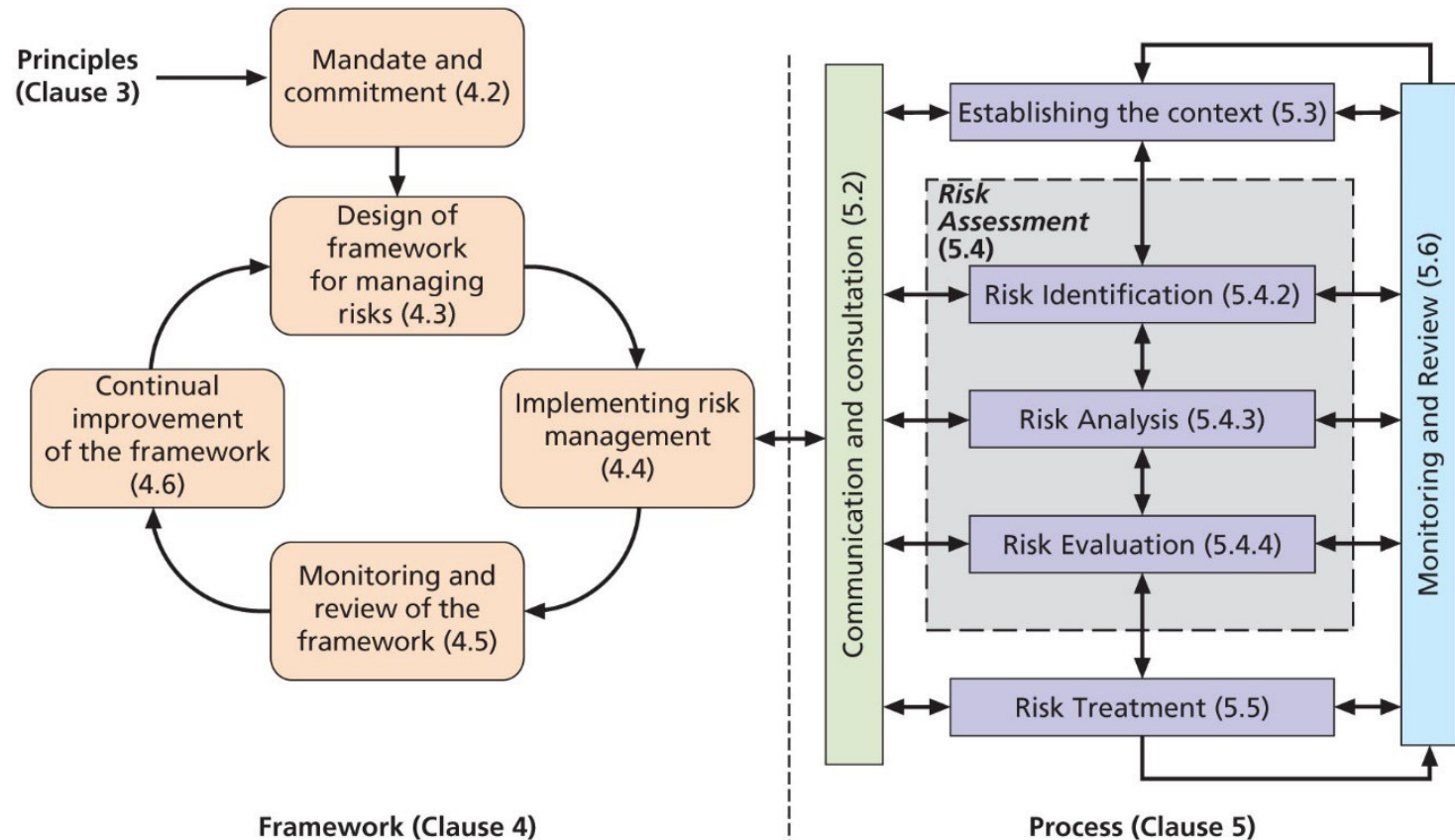


# ISO 31000 Risk Management

---

- ▶ ISO 31000 Risk Management
  - ▶ <https://www.iso.org/iso-31000-risk-management.html>
- ▶ It targeted towards any type of risk management
  - ▶ Enterprise risk management
  - ▶ Financial risk management
  - ▶ Environmental risk management
  - ▶ etc

# ISO 31000 Risk Management



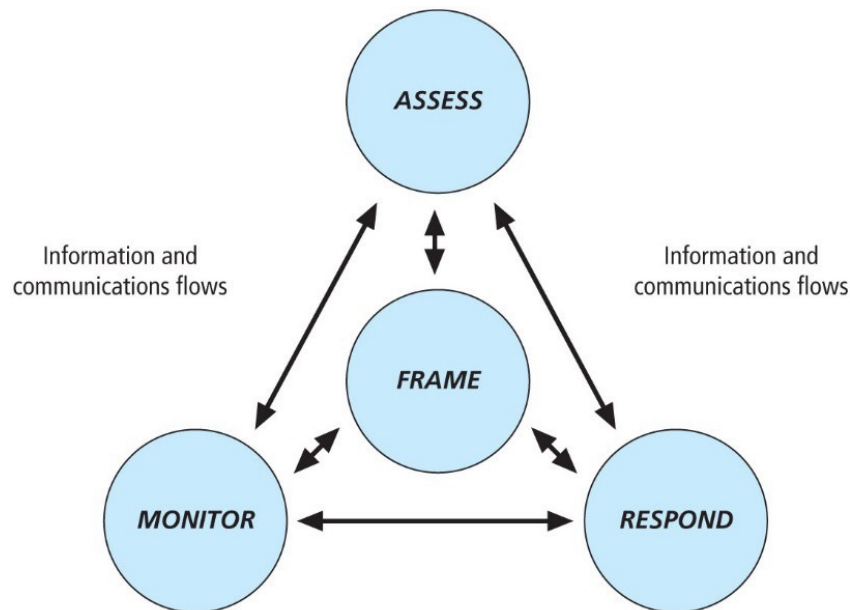
**Figure 7-11** ISO 31000 risk management framework and process

Source: ISO 31000: 2009.<sup>15</sup>

# NIST Risk Management Framework

---

- ▶ “Special Publication 800-39: Managing Information Security Risk: Organization, Mission, and Information System View”



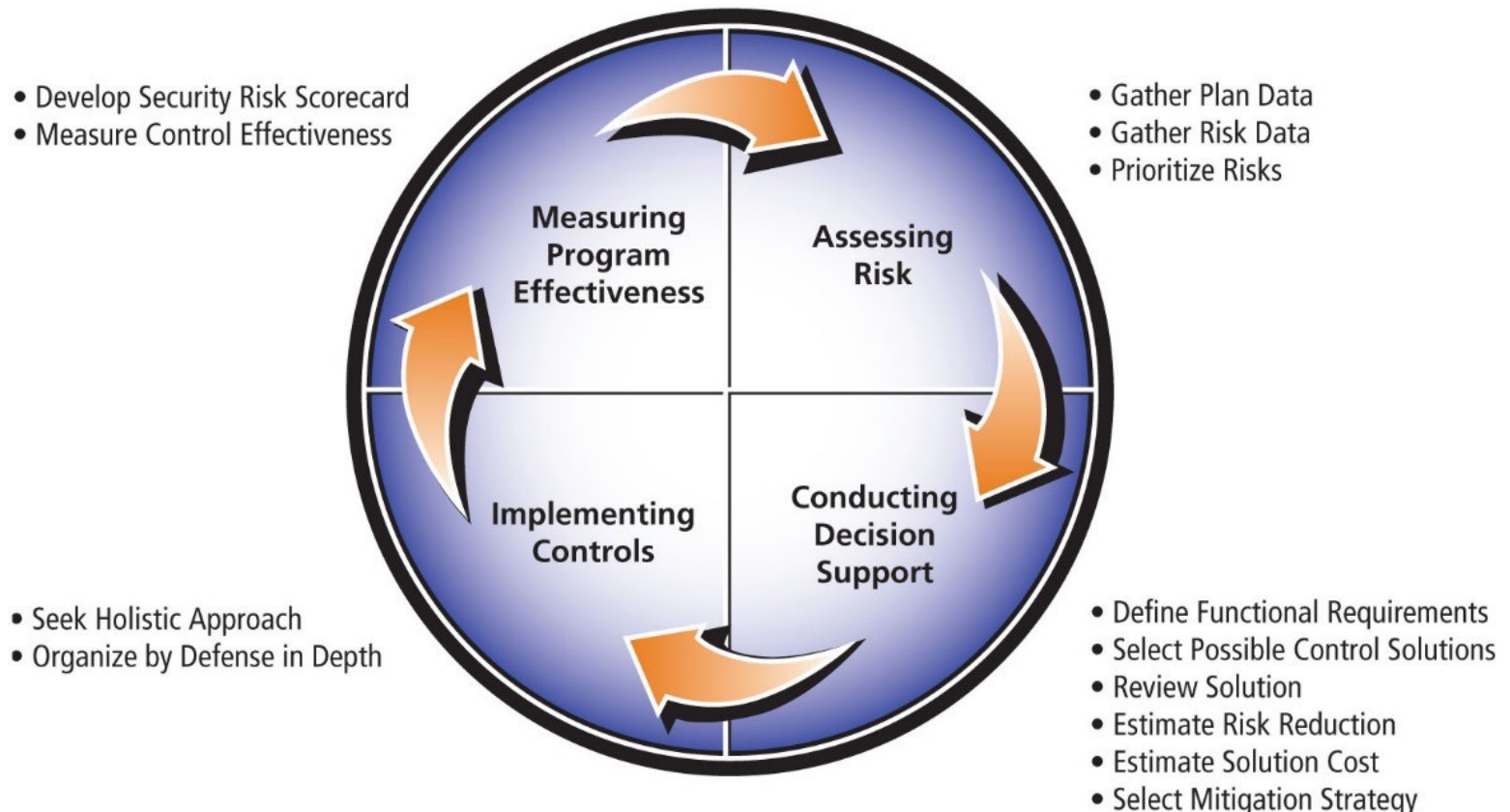
**Figure 7-12** NIST risk management framework overview

# Microsoft Risk Management Approach

---

- ▶ Four phases in the MS InfoSec risk management process:
  1. Assessing risk
  2. Conducting decision support
  3. Implementing controls
  4. Measuring program effectiveness

# Microsoft Risk Management Approach



**Figure 7-8** Microsoft's security risk management guide



# Next Week

---

- ▶ L10 Planning for Contingencies
  - ▶ Ch10