# INB255/INN255 Security

## Lecture 4:
## Managing Information Security

# Outline

- Why do we need to manage info. security?
- Who is responsible for info. sec. management?
- Information security and risk management
  - What is risk?
  - How do we manage risk?
  - Risk management and standards
    - AS/NZS 31000:2009 Risk Management
    - AS/NZS27005:2012 Information Security Risk Management
  - Information Security Management Standards
    - AS/NZS 27001:2006 Info Sec Management Systems
    - AS/NZS 27002:2006 Code of practice for IS management

# Why do we need to manage Info Sec?

- From a personal perspective:
  - You have valuable personal information assets you want to protect
- From a corporate perspective:
  - Organisations have valuable info assets to protect:
    - Some info is personal information
    - Also business materials relating to products, processes,
- From a national perspective:
  - Society relies on interactions across a range of sectors to function normally

# Why do we need to manage Info Sec?

- Information is a vital asset, so information security is a core business requirement:
  - To protect data assets (Think CIA)
    - During storage, transmission and use
  - To safeguards technological assets
    - Infrastructure: hardware, software, etc
  - To enable safe operation of applications
  - To protects the organisation's ability to function
    - In a changing business environment
- Want to avoid or minimize the effects of a security breach

# Why do we need to manage Info Sec?

- Questions to ask are:
  - What needs to be protected?
    - Which assets, and the value of asset?
  - Why does it need to be protected?
  - How can it be protected?
    - What does that cost?
    - How urgently is this required?
  - What happens if it is not protected?
    - What could that cost?
  - Need a systematic approach to ensure
    - all of the organisation's assets are considered, and
    - the approach taken is consistent.

# Why do we need to manage Info Sec?

- Information security is not addressed by technology alone
  - Decisions such as:
    - how important the information is (to the organisation, to replace)
    - the confidentiality, integrity and availability requirements associated with each asset
    - how information assets will be used, and by who
    - how much can be spent on controls
    - who is responsible for maintaining each of the assets

  involve management, not technology

# Why do we need to manage Info Sec?

- Information security is dynamic - needs change in response to changes in the environment:
  - Technological changes
    - May introduce new threats (e.g. wireless LAN, smartphone, BYOD)
    - Improved tools for attackers
    - Increased awareness of existing vulnerabilities
  - Business environment changes such as:
    - Size or structure of organisation
    - Business objectives and direction
    - Interactions with other entities: customers, trading partners, government agencies, etc.
  - Legal or regulatory environment
    - Liability, compliance with regulations

# Why do we need to manage Info Sec?

Comparison of security environments

- Q1: What is this information asset?
- Q2: What do we use now for this purpose?

# Why do we need to manage Info Sec?

## Comparison of security environments

| 1960s | 2000s |
|---|---|
| paper-based records | electronic storage |
| simple processing systems | distributed processing |
| physical controls | complex network systems |
| limited formal managerial responsibility | formal security requirements |

# Outline

- Why do we need to manage info. security?
- Who is responsible for info. sec. management?
- Information security and risk management
  - What is risk?
  - How do we manage risk?
  - Risk management and standards
    - AS/NZS 31000:2009 Risk Management
    - AS/NZS27005:2012 Information Security Risk Management
  - Information Security Management Standards
    - AS/NZS 27001:2006 Info Sec Management Systems
    - AS/NZS 27002:2006 Code of practice for IS management

# Who is responsible for ISM?

- In an organisation - consider these groups:
  - Management
    - CEO, CSO, CISO
  - General security staff
  - IT staff
  - Users
  - Third parties
    - Outsourced information security management
    - Customers, suppliers, business partners

# Who is responsible for ISM?

- Management:
  - Successful Information Security Management requires strong and consistent support from management
  - Demonstrate commitment to information security through:
    - allocation of resources and personnel
    - endorsement of information security policy
    - abiding by information security policy

# Who is responsible for ISM?

- General security staff:
  - Physical security impacts on information security
  - General security staff have procedures in place
    - monitoring access to buildings,
    - liason with police and/or emergency services
  - Include information security as a division of general security?
    - May require technical expertise

# Who is responsible for ISM?

- IT staff:
  - Staff have the skills required to:
    - manage technology
    - understand security issues and control measures
  - BUT information security is not just a technology issue
  - Dependence/independence of information security and IT:
    - Monitoring of IT department by IT department?
    - Conflict in relationships with other departments

# Who is responsible for ISM?

- Users:
  - Create, access and distribute information as part of their regular tasks
  - Training required so that users understand the security implications of simple actions
    - Like clicking links in email, or opening attachments
  - Security requirements may conflict with essential business activities the users carry out
    - tradeoff between efficiency and security?

# Who is responsible for ISM?

- Third parties:
  - Outsourced information security management
    - Experienced, expert
    - Separation of responsibilities: not aligned with staff
    - Which functions to outsource?
    - How do you evaluate the service provided?
  - Customers, suppliers, business partners
    - Investigate security implications of relationship
  - Contractors
    - What do they have access to?

# Who is responsible for ISM?

- Information security is a chain of protection:
  - Only as strong as the weakest link
    - An attacker only has to find one vulnerability to exploit
  - Need co-operation and collaboration at all levels, across an organisation
  - Individuals need to know:
    - what the security goals of the organisation are
    - why these goals are important
    - what their own duties and responsibilities are
    - how their actions impact on information security
    - what the consequences of a security breach are

# Outline

- Why do we need to manage info. security?
- Who is responsible for info. sec. management?
- Information security and risk management
  - What is risk?
  - How do we manage risk?
  - Risk management and standards
    - AS/NZS 31000:2009 Risk Management
    - AS/NZS27005:2012 Information Security Risk Management
  - Information Security Management Standards
    - AS/NZS 27001:2006 Info Sec Management Systems
    - AS/NZS 27002:2006 Code of practice for IS management

# Information security & risk management

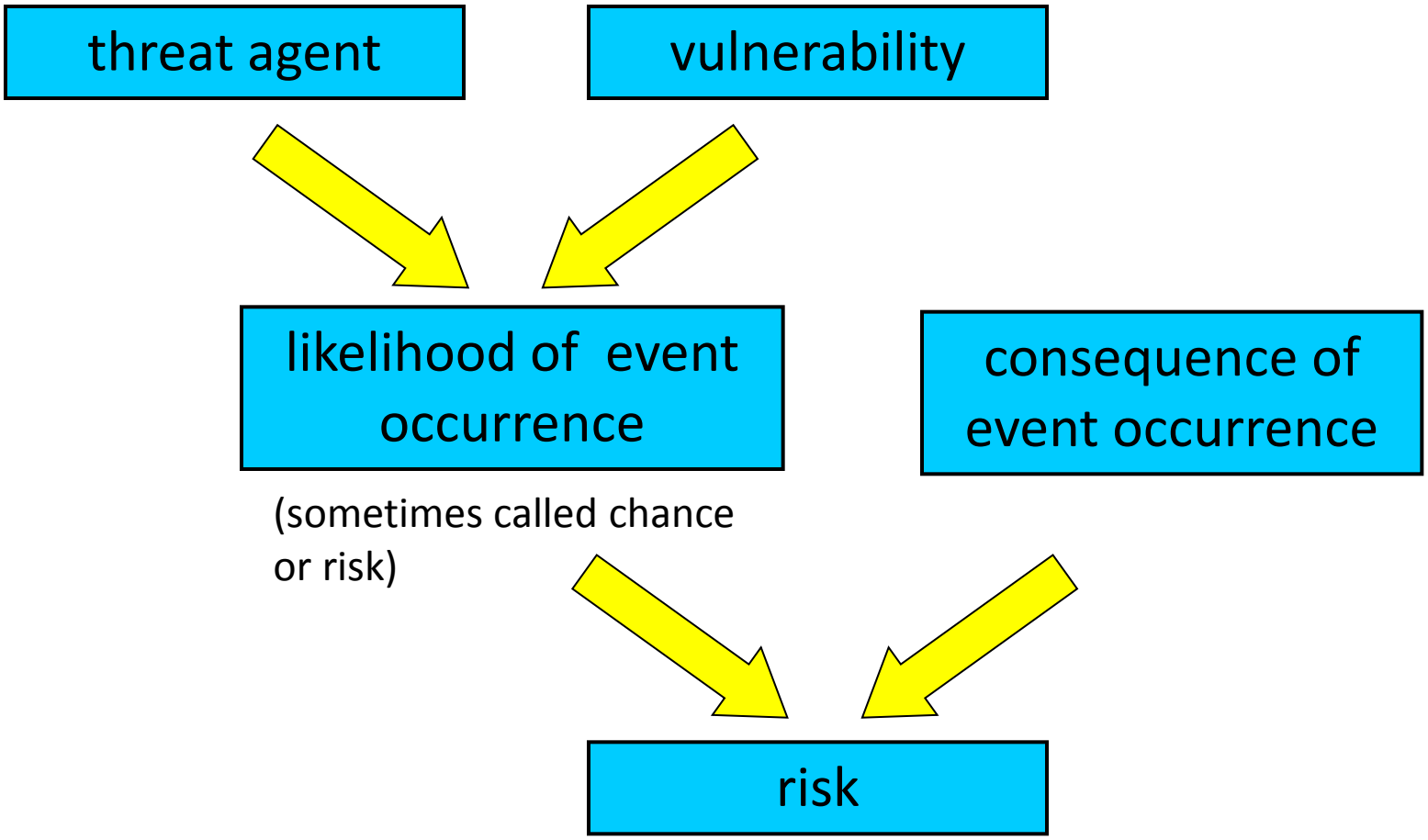
- Information security management involves asking questions like:
  - What needs to be protected?
  - Why does it need to be protected?
  - How can it be protected?
    - What does that cost?
    - How urgently is this required?
  - What happens if it is not protected?
- Organisations have limited resources (time, money, space) so making **tradeoffs** is necessary:
  - Can't afford to protect all assets against all possible threats
- Information security management involves risk management

# What is risk?

- Definition in AS/NZS 27005:2012 Information security risk management, on p 3 (Clause 3.9)
- Risk: 'effect of uncertainty on objectives.'
  - *Effect* includes positive and/or negative
  - Aspects of objectives to consider:
    - financial, health and safety, information security, environmental
  - May apply at different levels:
    - organizational, project, product, process
  - Information security risk expressed in terms of consequences and likelihood
    - Consequence: 'outcome of an event affecting objectives'
    - Likelihood: 'chance of something happening'

# What is risk?

Info sec risk considers potential for threats and vulnerabilities to coincide and harm assets



# How do we manage risk?

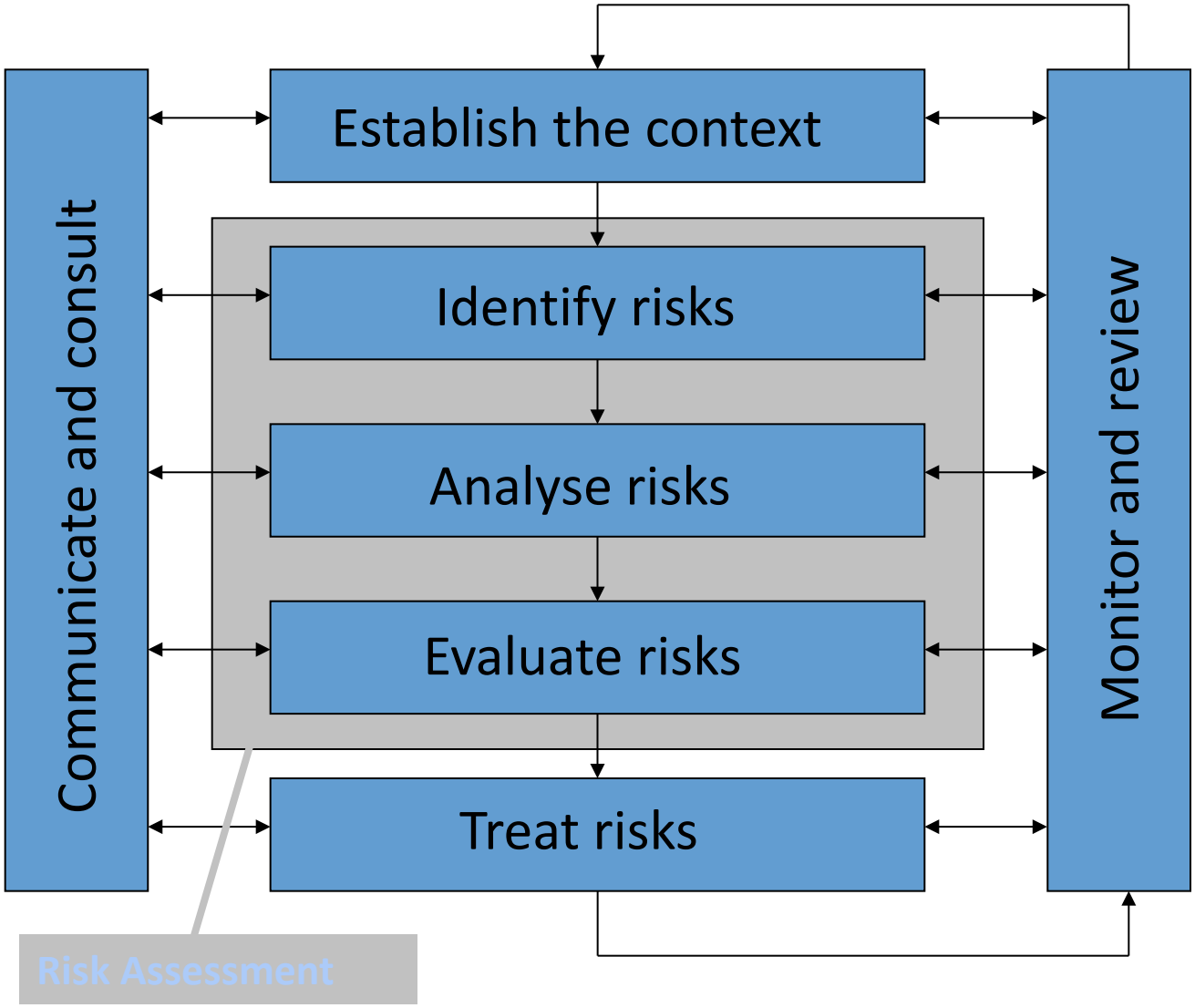
- Need a systematic approach:
  - Information security is dynamic, so process should be continual
- Australian Standards:
- *available from the SAI-Global Standards Online database (access this database through QUT Library)*
  - AS/NZS 31000:2009 *Risk management – Principles and guidelines*
    - Previous editions are: AS/NZS 4360:2004, AS/NZS 4360:1999 , AS/NZS 4360:1995
    - Generic: independent of specific industry or economic sectors
  - AS/NZ 27005:2012 *Information security risk management*
    - Provides guidelines for Information Security Risk Management

# Outline

- Why do we need to manage info. security?
- Who is responsible for info. sec. management?
- Information security and risk management
  - What is risk?
  - How do we manage risk?
  - Risk management and standards
    - AS/NZS 31000:2009 Risk Management
    - AS/NZS27005:2012 Information Security Risk Management
  - Information Security Management Standards
    - AS/NZS 27001:2006 Info Sec Management Systems
    - AS/NZS 27002:2006 Code of practice for IS management

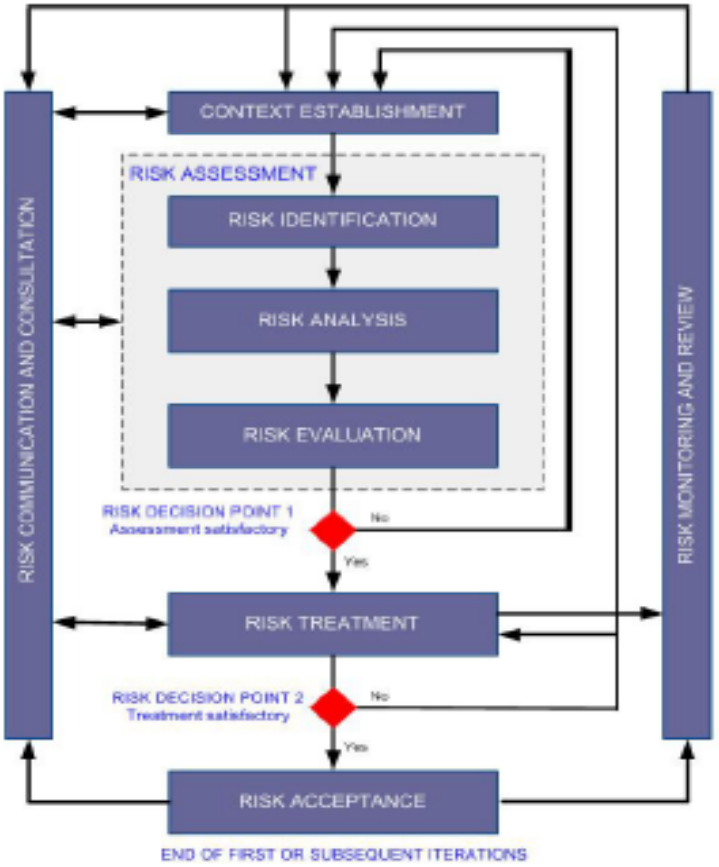
# How do we manage risk?

*Risk management process* (from AS/ISO 31000:2009)



# How do we manage risk?

*Info sec. risk management process* (from AS/NZS 27005:2012)



# Risk management process

*Establish the context*

- Establish the external context:
  - Relationship between organisation and external environment it operates in
- Establish the internal context:
  - Understand the organisation and its capabilities, goals and objectives
- Establish the risk management context:
  - Goals, objectives, strategies, scope and parameters of the area the risk management process is being applied to

# Risk management process

*Establish the context*

- Define risk criteria (Criteria against which risk is to be evaluated)
- For risk evaluation criteria consider:
  - Strategic value of the asset,
  - Criticality of the asset,
  - Legal, regulatory or contractual obligations,
  - Reputation
- For impact evaluation criteria consider:
  - Level of classification of asset, and type of breach (CIA)
  - Degree of impairment/disruption/loss of business
- For risk acceptance criteria consider:
  - What the timeframes will be
  - What level of risk is acceptable to organisation, etc

# Risk management process

*Risk Assessment: Identify risks*

- What can happen, where and when?
  - Identify assets and plausible threats, existing controls and existing vulnerabilities: combine these to identify events and potential consequences.
- Why and how it can happen?
  - Consider causes and scenarios
- Tools and techniques:
  - Identify risks using
    - Checklists (From other standards documents)
    - Judgements based on experience (own and others)
    - Systems analysis
- Include all risks, whether they are under the control of the organisation or not.

# Risk management process

*Risk Assessment: Analyse risks*

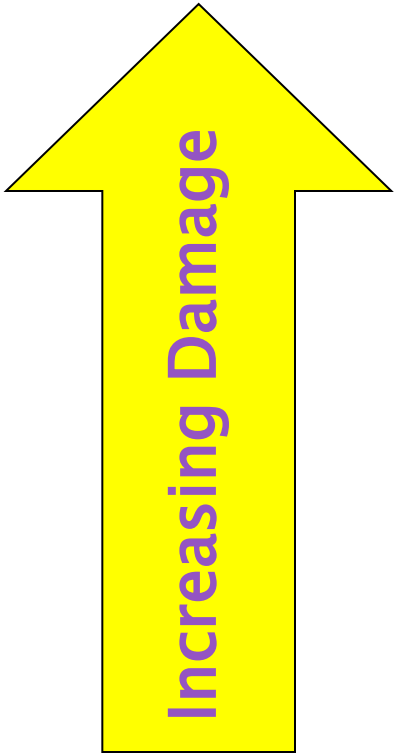
- **Determine the magnitude of identified risks**
- Types of analysis:
- **Qualitative**
  - Uses descriptive scales (in words). Example:
    - Consequence: Minor, moderate, major, catastrophic
    - Likelihood: Rare, unlikely, possible, likely, almost certain
- **Semi-quantitative**
  - Qualitative scales assigned numerical values
  - Can be used in formulae for prioritization (with caution!)
- **Quantitative**
  - Use numerical values for both consequence (e.g. $$$) and likelihood (e.g. probability value)

# Risk management process

*Qualitative Risk Analysis: Example*

**Qualitative Consequence scale** example:

From Information Risk Management Best Practice Guide p19



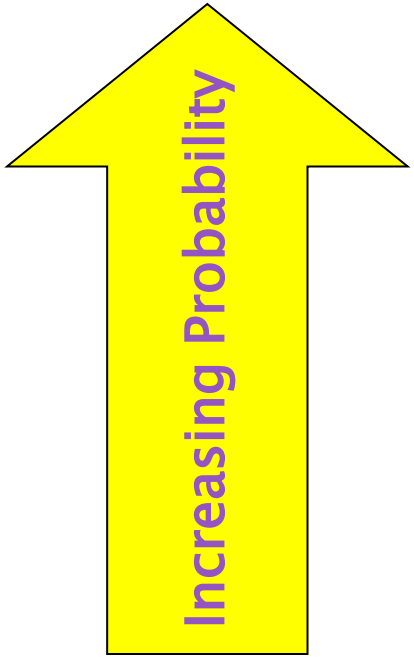

| Measure | Description |
|---|---|
| **Major** | **Major problems** would occur and threaten the provision of important processes **resulting in significant financial loss**. |
| **Moderate** | **Services would continue**, but would **need to be reviewed or changed.** |
| **Minor** | Effectiveness of services would be **threatened but dealt with**. |
| **Insignificant** | Dealt with as a part of **routine operations**. |

# Risk management process

*Qualitative Risk Analysis: Example*

**Qualitative Likelihood scale** example:

Information Risk Management Best Practice Guide p19




| Measure | Description |
|---|---|
| **High** | Is expected to occur in most conditions (1 or more times per year). |
| **Medium** | The event will probably happen in most conditions (about once every 2 years). |
| **Possible** | The event should happen at some time (once every 5 years). |
| **Unlikely** | The event could happen at some time (once every 10 years). |

# Risk management process

*Qualitative Risk Analysis: Example*

**Qualitative Level of Risk** example: Match consequences to likelihoods to determine levels of risk

**Consequence**

| Likelihood | Insignificant | Minor | Moderate | Major |
|---|---|---|---|---|
| High | M | H | E | E |
| Medium | M | M | H | E |
| Low | L | M | M | H |
| Unlikely | L | L | M | M |

Legend
**E: extreme risk**; immediate action required
**H: high risk**; senior management attention needed
**M: moderate risk**; management responsibility must be specified
**L: low risk**; manage by routine procedures

# Risk management process

*Quantitative Risk Analysis: Example*

- Quantitative parameters:
  - Sometimes possible to obtain numerical values for likelihood and consequence:
    - Based on prior knowledge, e.g. industry sector statistics
    - Where asset value is known (in $$)
    - Asset Value (AV): Estimated total value of asset
    - Exposure Factor (EF): % of asset loss caused by threat occurrence
    - Annualized Rate of Occurrence (ARO): Estimated frequency a threat will occur within a year
  - These can be used in numerical calculations:

# Risk management process

*Quantitative Risk Analysis: Example*

- Calculations:
  - Single Loss Expectancy (SLE)
    - SLE = AV × EF
    - Expected $value of loss if this event happens once
  - Annualised Loss Expectancy (ALE)
    - ALE = SLE × ARO
    - Expected $value of loss for this event in one year
- CAUTION: Results obtained from these calculations are worthless if the information is unreliable or imprecise.
  - Sometimes qualitative analysis is more appropriate

# Risk management process

*Quantitative Risk Analysis Example*

- *Example:*
  - Risk description
    - Asset: Public image (and trust)
    - Threat: Defacing web site through intrusion
    - Impact: Loss of image
  - Parameter estimates
    - AV(public image) = $1,000,000
    - EF(public image affected by defacing) = 0.05
    - SLE = AV × EF = $50,000
    - ARO(defacing) = 2
    - ALE = SLE × ARO = $100,000
  - How much would you be prepared to spend on controls to deal with this threat?

# Risk management process

*Risk Assessment: Evaluate risks*

- **Compare** the estimated risk found during risk analysis with the established risk criteria
  - NOTE: Consider analysis and criteria on same basis - qualitative or quantitative
- **Decide** which risks need treatment, and when
  - Output of this stage: Prioritized list of risks for further action
    - Risks in low or acceptable risk categories may be accepted without further treatment
    - High or extreme risks require immediate consideration of treatment possibilities

# Risk management process

*Treat risks*

- Select options for treating risks:
  - Risk modification: apply controls to
    - Change the likelihood of outcome
    - Change the consequences to increase the extent of the gains
  - Risk retention:
    - Decide to retain risk without further action
  - Risk Avoidance:
    - Avoid activity or condition that gives rise to the risk
  - Risk Sharing:
    - Share with another party that can effectively manage risk

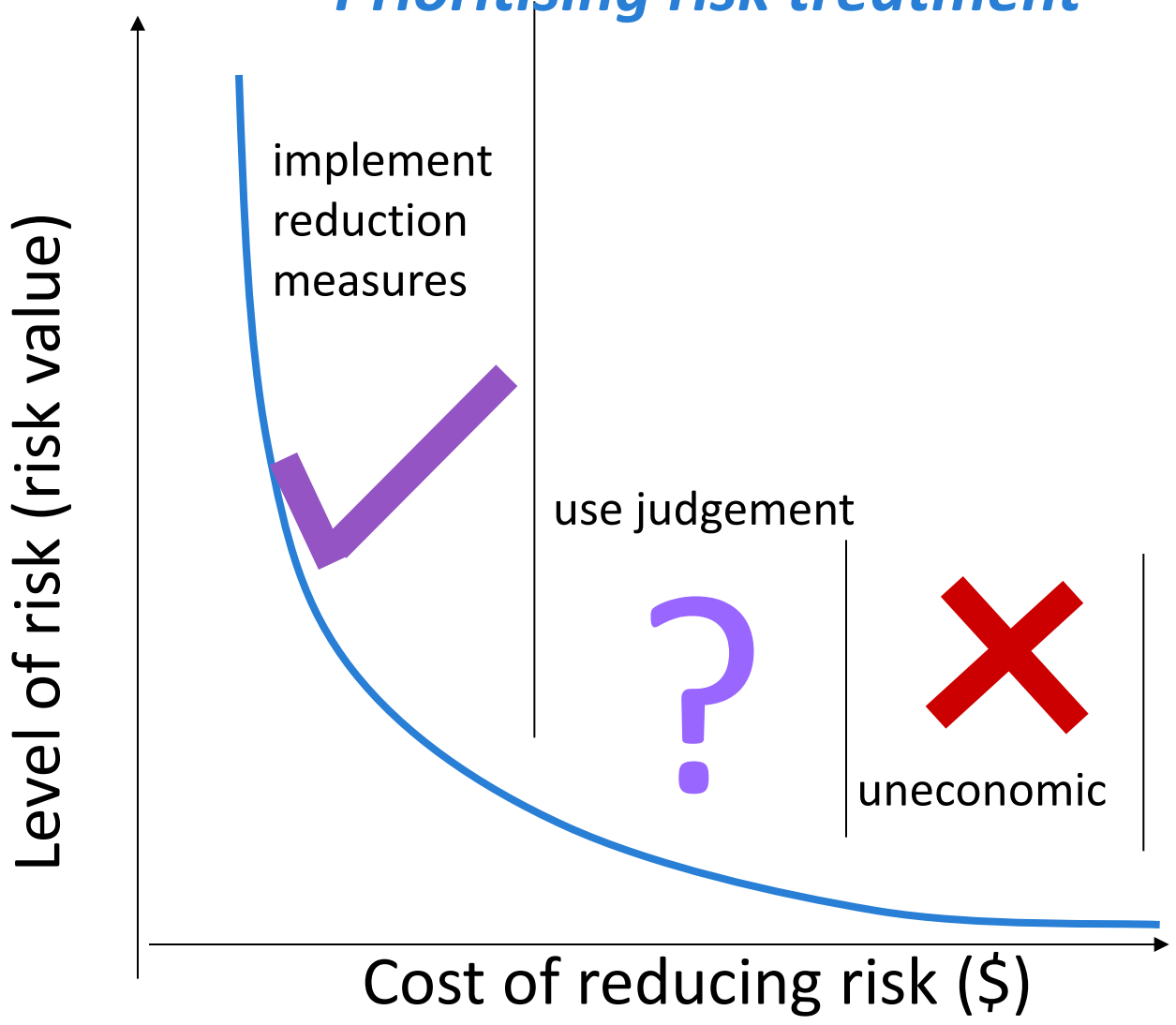
# Risk management process

*Treat risks*

- Assessing risk treatment options:
  - Assess based on
    - the extent of risk reduction, and
    - any additional benefits obtained
    - High risk levels may be acceptable if beneficial opportunities arise as a result of taking the risk
  - Balance
    - cost and effort of implementing treatment option against
    - benefits derived (proportionality principle)
  - Large risk reductions for low expenditure should be implemented
  - *Risk treatment itself can introduce secondary risks!*

# Risk management process

## *Prioritising risk treatment*



# Risk management process

*Treat risks*

- Prepare and implement treatment plans
- Document how the chosen options will be implemented:
  - Proposed actions
  - Resource requirements
  - Responsibilities
  - Timing
  - Performance measures
  - Reporting and monitoring requirements
- Determine the residual risk
  - Reiterate risk assessment including effects of proposed treatments
  - Does this meet organisation's risk criteria?

# Risk management process

*Communicate and consult phase*

- Communication and consultation:
  - should be considered at each step of risk managem't process
- Develop a communication plan for:
  - internal stakeholders
  - external stakeholders
- Two way dialogue: communication *and* consultation so all stakeholders understand:
  - the basis on which decisions are made
  - why particular actions are required

- *Stakeholders: those people and organizations who may affect, be affected by, or perceive themselves to be affected by, a decision or activity.*

# Risk management process

*Monitor and review*

- Ongoing review essential to ensure continuing relevance
- Need to monitor:
  - Risks (changes in likelihood or consequences)
  - Effectiveness of:
    - risk treatment plan
    - risk treatment strategies, and
    - management system controlling the implementation
- Few risks remain static
  - Identify emerging risks

# Risk management process

*Monitor and review*

- Need to monitor:
  - New assets included in risk management scope
  - Modified asset values
  - New threats
  - Existing vulnerabilities that might be exposed to new threats
  - New or increased vulnerabilities
  - Information security incidents

# Risk management process

*Record the process*

- Each stage of the risk management process should be recorded.

- Record:
  - assumptions, methods, data sources, analyses, results and reasons for decisions
- Record keeping decisions should consider:
  - Legal and business needs for records
  - Cost of creating and maintaining records
  - Benefits of reusing information

# Outline

- Why do we need to manage info. security?
- Who is responsible for info. sec. management?
- Info security and risk management
  - What is risk?
  - How do we manage risk?
  - Risk management and standards
    - AS/NZS 31000:2009 Risk Management
    - AS/NZS 27005:2012 Information Security Risk Management
  - Information Security Management Standards
    - AS/NZS 27001:2006 Info Sec Management Systems
    - AS/NZS 27002:2006 Code of practice for IS management

# Info security management standards

- What do we need to do to manage info security effectively?
- Australian and international standards provide guidance on information security best practice
- Applying IS Management Standards in your organisation provides:
  - evidence of management commitment to and responsibility for IS
  - assurance to other departments and organizations about your info sec practices (your security may impact on them)
  - assurance to staff that appropriate practices are in place
  - a checklist of important aspects of information security

# Info security management standards

- IS Management Standards: Australian
  - AS/NZS 27001:2006 Information Technology – Security Techniques - Information Security Management Systems. Requirements
  - AS/NZS 27002:2006 Information Technology - Security Techniques - Code of practice for information security management
  - AS/NZS 27005:2012 Information Technology - Security Techniques – Information security risk management

- Who uses these?
  - According to Aust. Cyber Crime & Security Survey Report 2012,
    - 64% of organisations apply IT security standards or guidelines
    - Of these, almost 50% followed ISO 27001

# Info security management standards

- Info Security Management Standards: International
- International (except USA):
  - ISO/IEC 27001:2005 Information Technology - Security techniques. Information security management systems. Requirements.
  - ISO/IEC 27002:2005 Information Technology – Security Techniques - Code of practice for information security management
  - ISO/IEC 27005:2011 Information Technology - Security Techniques – Information security risk management

- USA:
  - NIST (National Institute for Standards and Technology) Special Publications, including SP800-12, SP800-14, SP800-18, SP800-26 and SP800-30, SP800-64

# Info security management standards

- How do you know that organisations *are* managing security?
  - Do they have a certified Information Security Management System?
  - Can be certified against AS/ISO 27001
    - In Australia, this is the only information security standard that it is possible to obtain certification against
  - International register of organisations with ISMS certified against 27001 was kept at: http://www.iso27001certificates.com/
    - In 2013, number of certificates worldwide was 7940
    - Countries with most certified organisations include Japan, UK, India Taiwan, China, USA,
    - Australia in list at number 22, 30 organisations listed

# AS/NZS 27001:2006

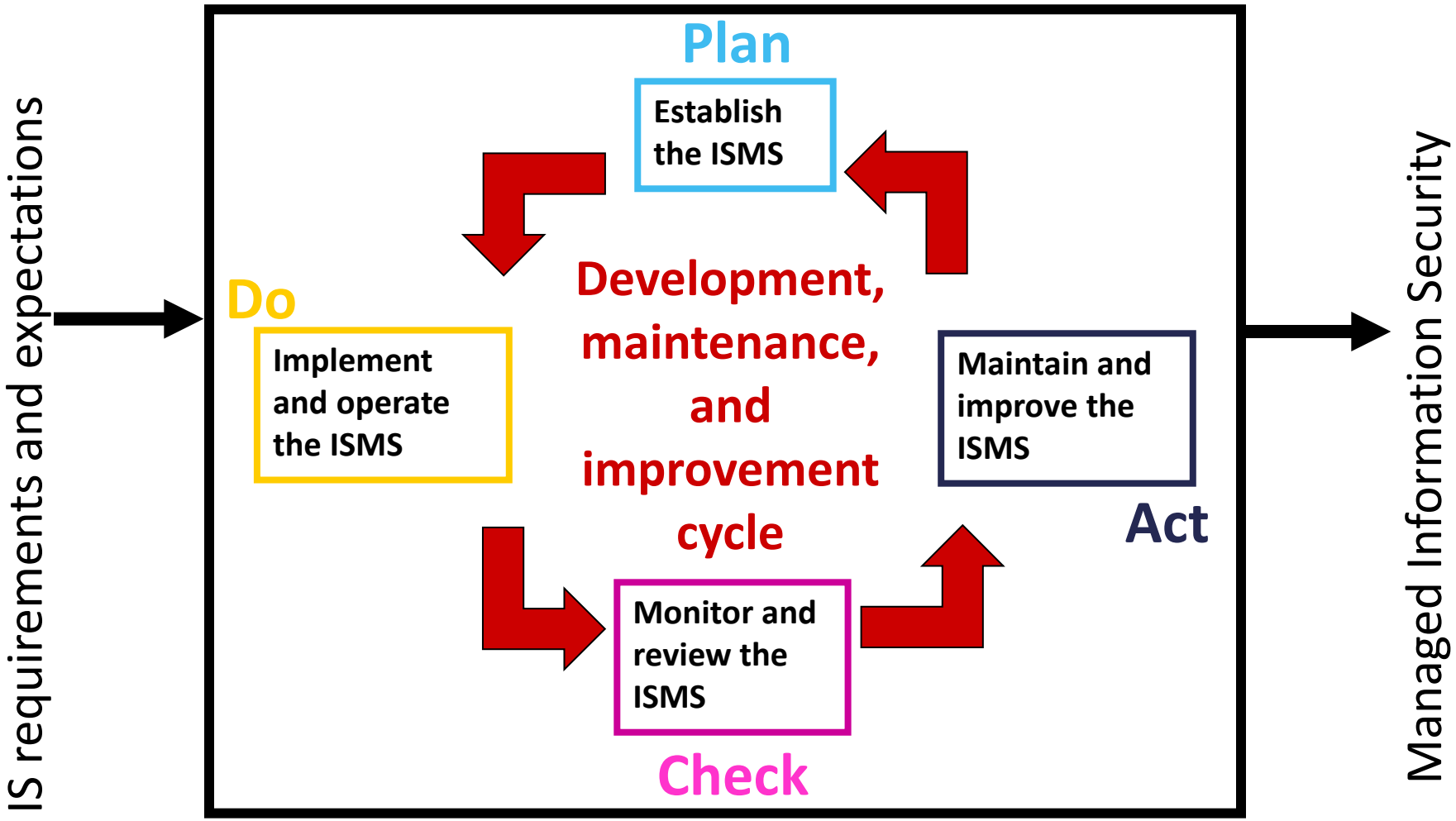
- **Background:**
- Original information security management documents were code of practice/guidelines
  - Such as AS4444, based on BS7799.
- Need for a certification scheme for information security management emerged in late 1990s
  - For certification purposes a general approach to security management was needed, not just a code of practice
  - BS 7799.2:1999 created to define a comprehensive Information Security Management System (ISMS) could certify against.
- Concept of an ISMS as important as original Code of Practice.

# AS/NZS 27001:2006

What is it?

- A comprehensive approach to information security management
- Objective of AS/NZS 27001:2006:
  - to specify requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS
- Use in conjunction with AS/NZS 27002:2006
  - AS 27001:2006 is about management
  - AS 27002:2006 is a code of practice, provides a set of information security goals and controls,
- Uses Plan-Do-Check-Act (PDCA) process model

# AS/NZS 27001:2006 - The PDCA Model



# AS/NZS 27001:2006

PDCA model

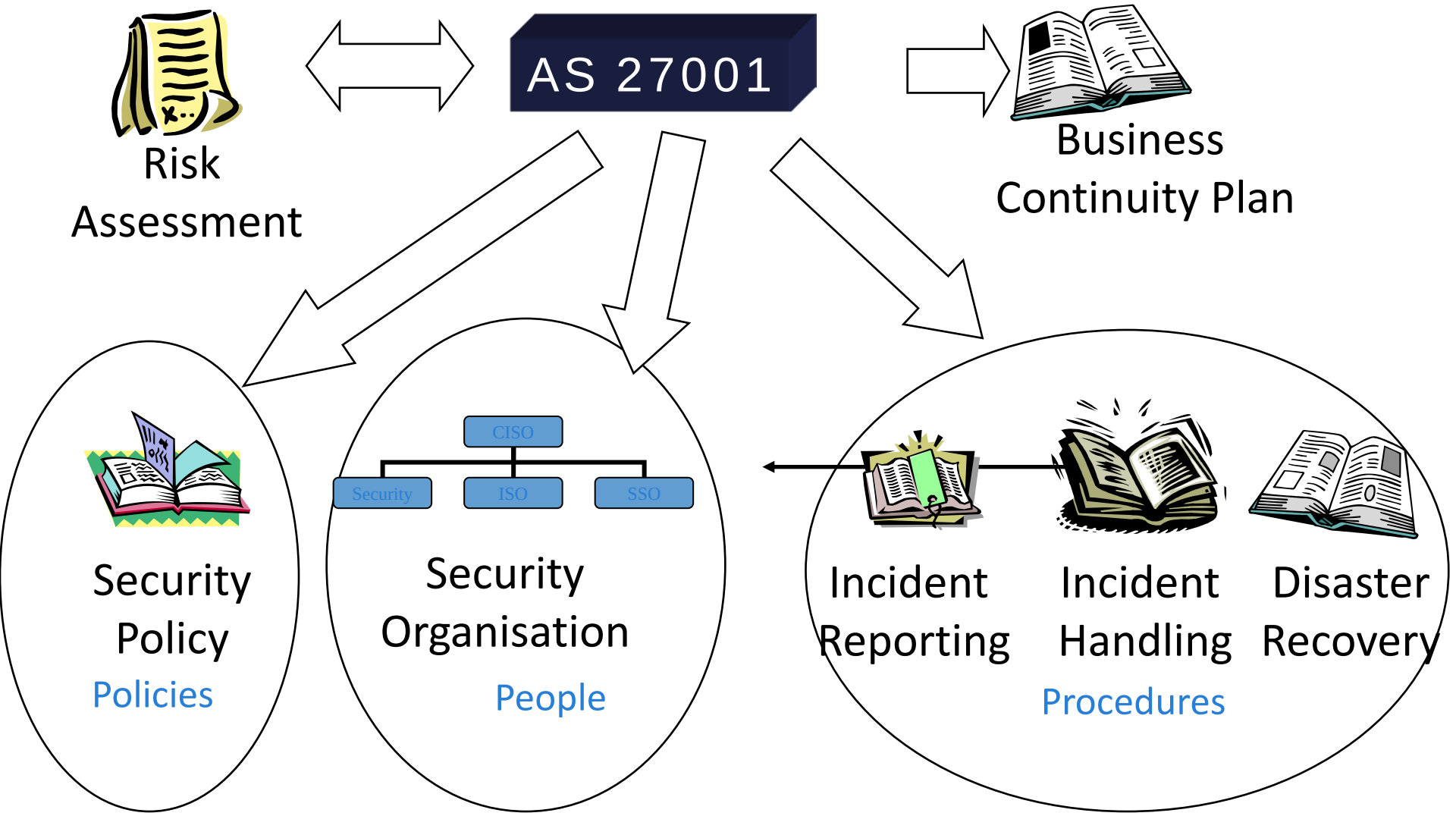
- **PLAN - Establish the ISMS**
  - Purpose: Establish policy, objectives, processes and procedures
- **DO - Implement and operate the ISMS**
  - Purpose: Implement selected controls, and promote actions to manage identified risks
- **CHECK - Monitor and review the ISMS**
  - Purpose: to ensure that controls are working effectively
- **ACT - Maintain and improve the ISMS**
  - Purpose: Take action as a result of the Check phase

# AS/NZS 27001:2006

## Relating the PDCA model and Info Sec Risk Manag't Process

| ISMS Process | InfoSec Risk Management Process |
|---|---|
| Plan | Establish the context<br>Risk assessment<br>Develop risk treatment plan<br>Risk acceptance |
| Do | Implementation of risk treatment plan |
| Check | Continual monitoring and review of risks |
| Act | Maintain and improve the Info Sec risk management process |

# AS/NZS 27001:2006 Output



# AS/NZS 27002:2006

- **Information Technology - Security Techniques - Code of practice for information security management.**
  - Same as international standard (ISO/IEC 27002:2005)
    - Basically an internationally recognised generic information security standard
  - Supersedes AS/NZS 17799:2001
  - Objective: "… to provide practical guidelines for developing organizational security, standards and effective security management practices and to help build confidence in inter-organizational activities."

# AS/NZS 27002:2006

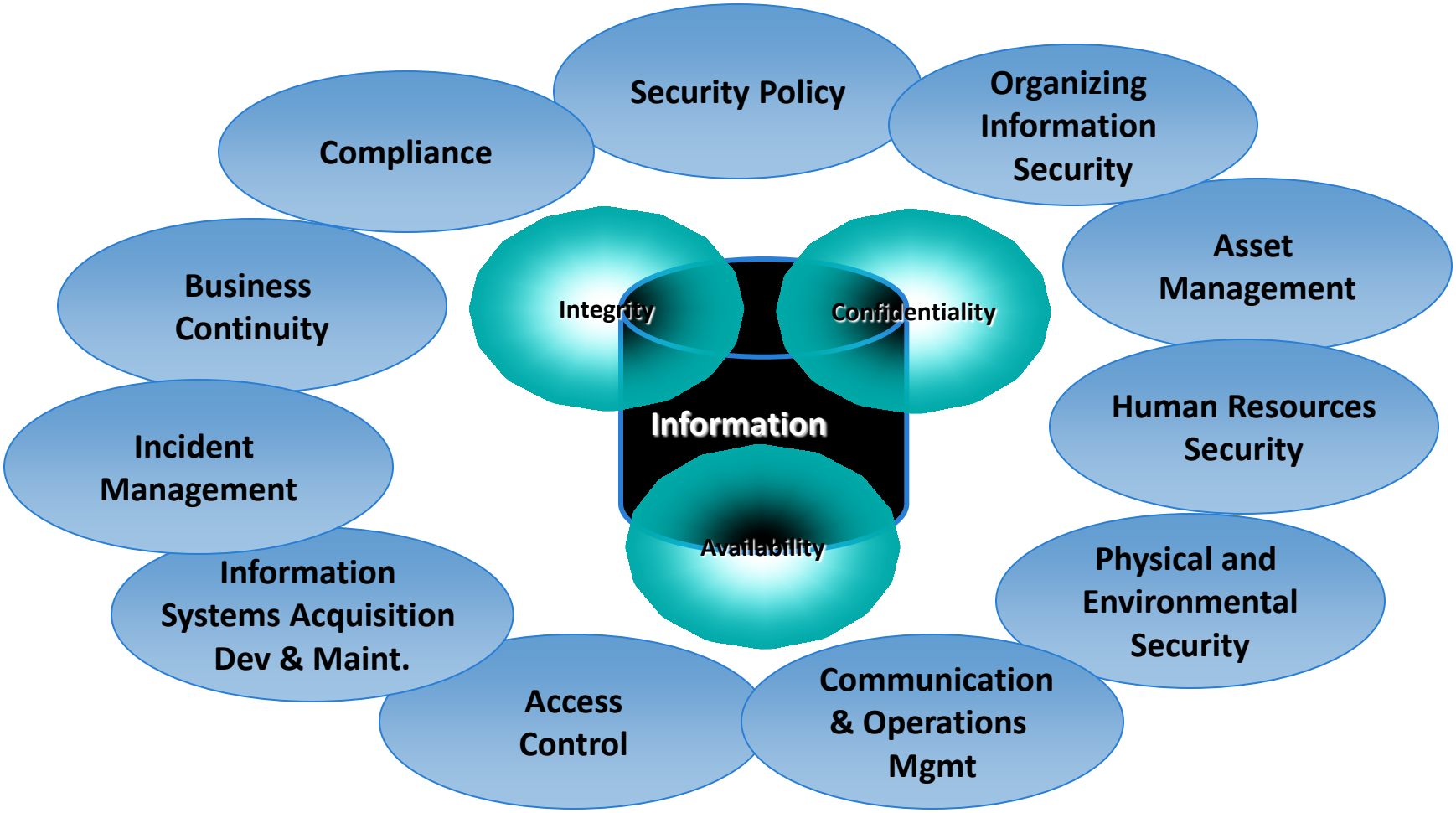
- **Background:**
- Early 1990's
  - Need for practical guide to info security management recognized
  - Group of leading companies in the UK combined to develop the *Code of Practice for Information Security Management*
- Feb 1995 - Published as BS7799 version 1
- 1996 - Adopted as AS/NZS 4444:1996
- 2001 - New version of BS 7799 adopted as AS/NZS 17799:2001
- 2006 - Updated to AS/NZS 27002:2006
- ISO/IEC 27002 - Updated in 2013, AS/NZS update 2014?

# Structure of AS/NZS 27002:2006

- AS/NZS 27002:2006 contains:
  - One clause on risk assessment and treatment
  - 11 security control clauses
    - Each clause contains a number of main security categories containing:
      - A control objective stating what is to be achieved, and
      - One or more controls that can be applied to achieve the objective.
  - "… each organization applying this standard should identify applicable clauses, how important these are and their application to individual business processes."

# AS/NZS 27002:2006

## The 11 Security Clauses



# AS/NZS 27002:2006

Clause 7: Asset Management

- **Clause 7.1 Responsibility for assets**

- Objective:To achieve and maintain appropriate protection of organizational assets.

- Subjects covered:
  - Inventory of assets
    - Including information, software assets, physical assets, services, people and intangibles such as reputation
  - Ownership of assets
  - Acceptable use of assets

# AS/NZS 27002:2006

Clause 7: Asset Management

- **Clause 7.2 Information classification**
- Objective: To ensure that information receives an appropriate level of protection.
- Subjects covered:
  - Classification guidelines
    - In terms of value legal requirements sensitivity and criticality to the organization
  - Information labelling and handling

# Asset management failure

- Example: Poor management of critical information asset:
- http://www.theregister.co.uk/2012/03/01/nasa_stolen_laptop_unencrypted/

Stolen NASA laptop had Space Station control codes

**And no encryption for supervillains to crack**

By **Brid-Aine Parnell** • **Get more from this author**

Posted in Enterprise Security, 1st March 2012 13:21 GMT

A NASA laptop stolen last year had not been encrypted, despite containing codes used to control and command the International Space Station, the agency's inspector general told a US House committee.

NASA IG Paul Martin said in written testimony (PDF) to the House Committee on Science, Space and Technology that a laptop was stolen in March 2011, which "resulted in the loss of the algorithms used to command and control the ISS".

# AS/NZS 27002:2006

Clause 8: Human Resources Security

- **Clause 8.1 Prior to employment**

- Objective: To ensure that employees, contractors and third party users understand their responsibilities and are suitable for their roles
  - To reduce the risk of theft, fraud or misuse of facilities

- Subjects covered:
  - Defining roles and responsibilities;
  - Screening;
  - Terms and conditions of employment.

# AS/NZS 27002:2006

Clause 8: Human Resources Security

- **Clause 8.2 During employment**
- Objective: To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities and … to reduce the risk of human error
- Subjects covered:
  - Management responsibilities
  - Information security awareness, education and training
  - Disciplinary process

# AS/NZS 27002:2006

Clause 8: Human Resources Security

- **Clause 8.3 Termination or change of employment**
- Objective: To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner
- Subjects covered:
  - Termination responsibilities
    - What are the ongoing security requirements and legal responsibilities?
  - Return of assets
    - Return all of the organization's assets, including hardware, software and information
  - Removal of access rights
    - Including physical and logical access mechanisms, ID cards, etc

# Example: Human resources security

- Vulnerability if access rights not removed:
  - '… access of former staff was not removed from the system that manages radiology images for the past three years, reportedly due to termination notices not being provided by the Human Resources section on a regular basis.'
  - '… there were 460 access cards with permission to enter the primary medical records area. This was considered to be excessive given that there were approximately 140 hospital information management staff.'
  - From Auditor-General Report to Parliament No 7 for 2010 *Information Systems - Governance and control,* p49.
  - Available at: https://www.qao.qld.gov.au/report-no-7-for-2010

# Example: Human resources security

- Example: employee access to email system after termination
- http://www.theregister.co.uk/2011/03/01/sacked_employee_sentenced/

Woman sentenced for breaching former employer's PCs

**Pants-ate-my-hard-drive defense fails**

By **Dan Goodin in San Francisco** • **Get more from this author**

Posted in Crime, 1st March 2011 05:00 GMT

A California woman has been sentenced to 60 days home detention and a year of probati for breaching the mail system of a former employer and posting confidential company documents to public websites.

Ming Shao, who was 44 years old according to court documents filed last week, pleaded guilty to one count of felony computer intrusion. In a plea agreement, she admitted that th value of stolen information, which included a "Weekly Ops Report" distributed to executive of PanTerra Networks was from $10,000 to 30,000 to the Sunnyvale, California company. She said she retaliated against the company after being fired August 2009.

Shao had access to two employee email accounts for months following her dismissal. On several occasions, she posted confidential information to websites such as

# AS/NZS 27002:2006

## Physical and Environmental Security

- **Clause 9 Physical and Environmental Security**
- Objectives:
  - To prevent unauthorized physical access, damage and interference to the organization's premises and information;
  - To prevent loss, damage, theft or compromise of assets and interruption to organizational activities.
- Subjects covered:
  - need to establish secure areas with defined perimeters and appropriate barriers and entry controls;
  - need to physically protect hardware equipment to prevent theft;
  - need to protect network cabling from tampering;
  - security of equipment taken off site or sent for disposal

# Summary

- Information is a vital organizational asset
  - Dynamic environment means ongoing process is required to manage information security
  - Everyone has a role to play in maintaining security
- Information security management involves risk management
  - Australian standard (similar to international standard)
  - AS/NZS 27005:2012 Information Security Risk Management
- Information security standards give guidance on managing information security in organisation
  - AS/NZS 27001:2006 Information Security Management Systems
  - AS/NZS 27002:2006 Code of practice for information security management