1

Summary, schedule and assessment

Slide 2

Week	Week Beginning	Weekly Teaching and Learning	Assessment and Learning activities
1	01 August	Introduction and Overview: IS risk and security	Class activity & reading (TBA)
2	08 August	Information Security & risks I	Class activity & reading (TBA); Submit CLA #1, Friday 12 August
3	15 August	Information Security & risks II	Class activity & reading (TBA)
4	22 August	Assessing security and establishing Internal Control	Class activity & reading (TBA); Submit CLA #2, Friday 26 August
5	29 August	Mitigation, treatment & control I	Class activity & reading (TBA)
6	05 September	Mitigation, treatment & control II	Class activity & reading (TBA); Submit Online Quiz #1, Friday 09 September
Mid Semester Break – 12 September to 18 September. ISRS Report Part A, due Friday 16 September.			
7	19 September	Information Security & Information Governance	Group Warm-up (TBA); Submit in class, Wednesday 21 September
8	26 September	Business Continuity Management	Class activity & reading (TBA);
9	03 October	Contingency Planning	Class activity & reading (TBA); Submit CLA #3, Friday 07 October
10	10 October	Cybersecurity and Business Continuity Management	Class activity & reading (TBA);
11	17 October	Fraud and forensic auditing: Fraud, cybercrime, forensic auditing and continuous monitoring	Class activity & reading (TBA); Submit Report Part B, Friday 21 October
12	24 October	Information Security ethics & compliance and pre-quiz revision	Class activity & reading (TBA); Submit Online Quiz #2, Friday 28 October

Classe

- 1 x 2hr F2F Workshops across the semester, Weds 8:30, 10:30
- Week 1, M001 completed, week 2 M002 available

Assessments

- CLA#1 , due Friday 12th August
- Individual & group (major) assignment expected release dates at end of week 2 and week 6
- 2 Class quizzes

News

- Guest presentations
  - Program to be confirmed
- ISACA student group
- *All parts of unit of study are relevant to you learning and assessment*

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

2

This week's learning plan

Slide 3

Develop an understanding of importance of *managing information risks*, with a focus on identifying and describing risks

Review: organisational data breach

1. Understanding risks, develop your understanding of related concepts in information security & risk management
   - What is a risk?
   - Assets, threats and vulnerabilities
   - Internal control *(wk 3 & 4)*
2. Risk management
   - Major categories of organisational risks including information risks)
3. Risk assessment (*next week*)

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

3

Preparing for coming week

Slide 4

Recommended introductory reading
Texts:

Whitman, Chapter 6 Assessing Risks

OR

Gibson, D - **Chapters 4-6 Planning for risk assessments**

Target data breach case materials in M002

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

4

Week 1 review

Slide 5

Data breach

A data breach is (a threat event)

- a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by a person/s unauthorised to do so.

  may involve financial information such as credit card or bank details, personal health information, other personally identifiable information (including the loss of privacy) trade secrets of corporations or intellectual property.

- A ***risk*** is ***likelihood*** that a ***threat*** will exploit a ***vulnerability*** of an ***asset*** or group of assets and thereby cause harm to the organisation.

  ISO/IEC 27000 family - Information security management systems

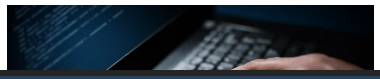
5

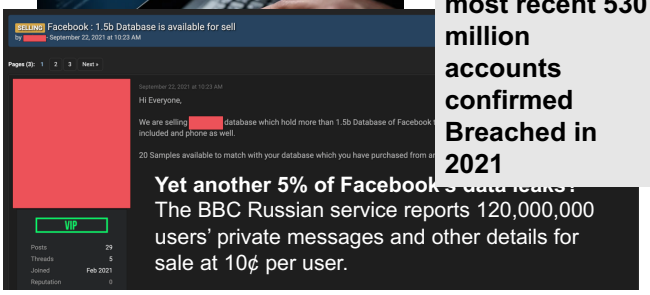
Data breaches affect everyone

Slide 6

Hacked Facebook, Gmail and Instagram accounts, banking information and even driver licences are being bought and sold on the dark web for as little as $21, with experts warning identity theft may have life-long consequences for victims.

Released last week, the US Privacy Affairs Dark Web Price Index shows the average price of a hacked Facebook account is $106, a hacked Instagram account is $80 and access to a Twitter account costs $70. Access to a hacked Gmail account is being sold for $220 on average, the report showed.





Yet another 5% of Facebook's data leaks?
The BBC Russian service reports 120,000,000 users' private messages and other details for sale at 10¢ per user.

Facebook , 18 known breaches since 2007 , with most recent 530 million accounts confirmed Breached in 2021

In 2022, LinkedIn more 5 million accounts, Twitter – July - $5.4 million accounts for $30K USD
Target data breach link

2021 & 2022

Data scrapers are selling sensitive personal data on between 530 million Facebook users. Data contains users': name, email, phone number, location, gender, and user ID. Data appears to be authentic. Personal data obtained through web scraping.

6

1. Understanding risk

Slide 7

Categories of threats

Table 6-3 Threats to InfoSec

Threat	Examples
Compromises to intellectual property	Software piracy or other copyright infringement
Deviations in quality of service from service providers	Fluctuations in power, data, and other services
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, flood, earthquake, lightning, etc.
Human error or failure	Accidents, employee mistakes, failure to follow policy
Information extortion	Blackmail threat of information disclosure
Sabotage or vandalism	Damage to or destruction of systems or information
Software attacks	Malware: viruses, worms, macros, denial-of-services, or script injections
Technical hardware failures or errors	Hardware equipment failure
Technical software failures or errors	Bugs, code problems, loopholes, back doors
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

Source: CACM.

7

Not a data breach! Not DDOS .. Just load

Slide 8

MyGov website crashes as thousands seek Centrelink help amid coronavirus pandemic, Government backflips on claims cyber attack to blame

Posted Mon 23 Mar 2020 at 10:55am, updated Tue 24 Mar 2020 at 1:02am

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

8

1. Understanding risk

Slide 9

Categories of threats

- Each organisation must prioritise the threats it faces based on their particular security situation
- Each threat presents a unique challenge to information security and must be handled with specific controls that designed to address that threat
- Threat assessment becomes a critical part of the overall assessment of information security risks

9

1. Understanding risk

Slide 10

What is risk?

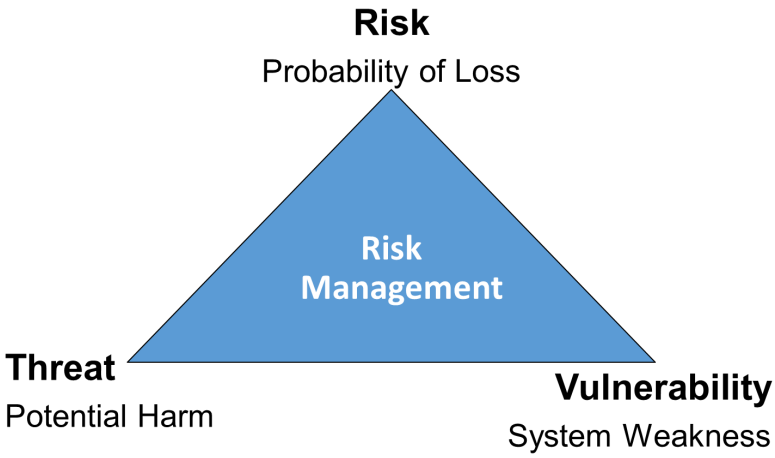
- ….risks are the price of doing business, they are the chances (***probability or likelihood***) of negative outcomes
- ***A risk is the potential to compromise the use or value of organisational asset***

  *The potential that a **threat** will exploit a **vulnerability** of an **asset** or group of assets and thereby cause harm to the organisation (*ISO/IEC 27000 = ISM suite)
- In this sense: Information security is an exercise in risk management, it involves the protection of information assets (whether in storage, processing, or transit) and systems from damage, misuse or attack; resulting in information being stable, reliable, and free of failure (thus considered confidentiality, integrity and availability)

10

Risk Management, is about dealing with the probability of a loss

Slide 11



11

1. Understanding risk

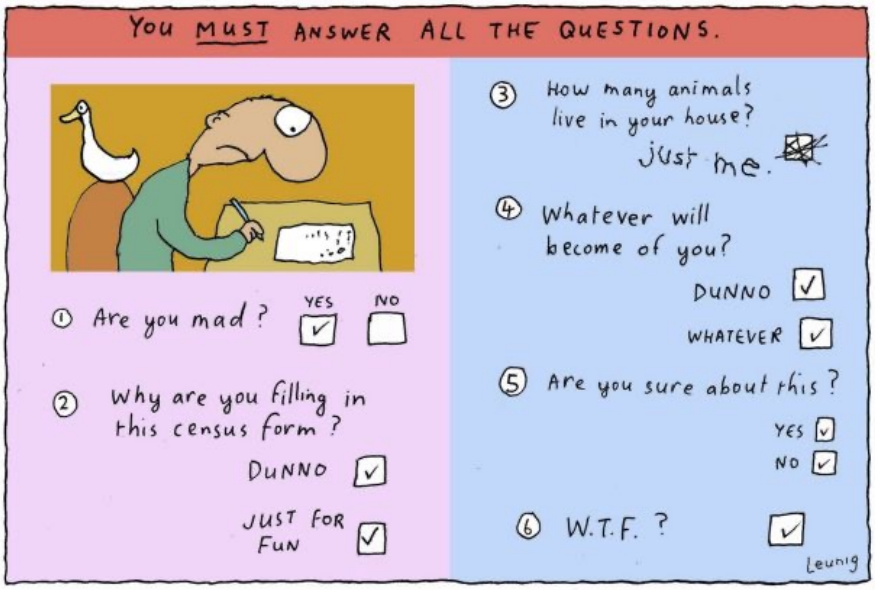
Slide 12

What is risk? AS/NZS IS0 31000:2018

- ***The chance of something happening that will have an <u>impact</u> on objectives. A risk is the effect of uncertainty on objectives***
- Note 1: Its often expressed in terms of an event or circumstance and the consequences that may flow from it. It is a deviation from the expected
- Note 2: Risk is measured in terms of a combination of the consequences of an event and their likelihood (more on this next week)

**AS/NZS IS0 31000:2018 is a recommended standard for your assignments*

12



Let's consider high risk, low risk VS. good risk, bad risk

Cartoon by © Michael Leunig, The Age 10 August, 2016

The ABS attack, August 2016

Not a data breach! ….NOT DDOS! … just load!

- ***The chance of something happening that will have an impact on objectives***
- Note 1: A risk is often expressed in terms of an event or circumstance and the consequences that may flow from it.
- 4th "attack" most damaging , via a 3rd party (suggest more than a simple and direct denial of service). ***Was it just citizen load?***
- A malicious external attack, perhaps international –will it be persistent?
- Preparation, load testing, possibly alternative live servers
- Implications/ Impacts
  - It will be seen as (*and is*) an IS security failing #censusfail
  - Angry citizenry
  - Vindicated privacy advocates
  - Cost of compromised trust
  - Cost of a prolonged and potentially inaccurate survey
  - Government enquiry
  - ABS blamed IBM blamed Nextgen, ABS claimed 30 million & settled out of court
- None of this is new for the ABS, 14 data beaches since 2013, Kammay & Hill sentenced in 2015

The ABS attack

Swinburne

Kammay &Hill

2015, 26 year old Lukas Kamay (7 yrs) and ex Australian Bureau of Statistics worker, Christopher Hill (3 yrs) , 25yrs old commit over $7million in illegal foreign exchange trades

2013, met at Fitzroy Pub and planned for Hill to send Kamay (confidential) sensitive unpublished stats on economic indicators that he obtained as a Commonwealth employee,

Shared info via mobile phones, Kamay would use that information to conduct trades on the foreign exchange (FX) derivatives market using the information that was not generally available to the wider public, which would have a material effect on the price or value of the foreign exchange derivative contracts.

The pairs plan was to to make around $200,000 profit from market sensitive information but Kammay made $7 million in profits through 45 trades over eight months with a starting trade of $1,000, he paid Hill $20,000

2007 -2011, Met at Monash University, Bachelor of Commerce and Bachelor of Economics

1. Understanding risk

SWIN BUR NE Slide 16

Risk management aims to accept risks that make sense to take and reduce unacceptable risks

Just a few examples

- Strategic – new business
- Operational – changed business process
- Project – outcomes outweighs risk

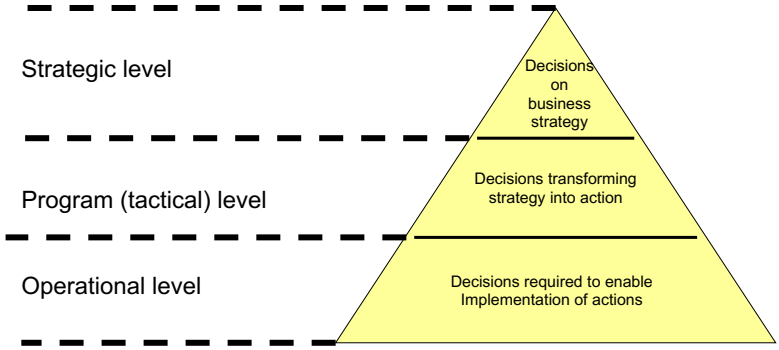
1. Risk management is about resolving obstacles , not about closing up shop!
2. Risk is the uncertainty that something of value could be damaged or lost

1. Understanding Risk – risk assessment

Slide 17

What is risk assessment

Risk assessment is the identification and analysis and priortisation of risks to support the achievement of business objectives. It is the process of applying risk management to the specific risks an organisation faces. It forms a basis for determining how risks should be managed.

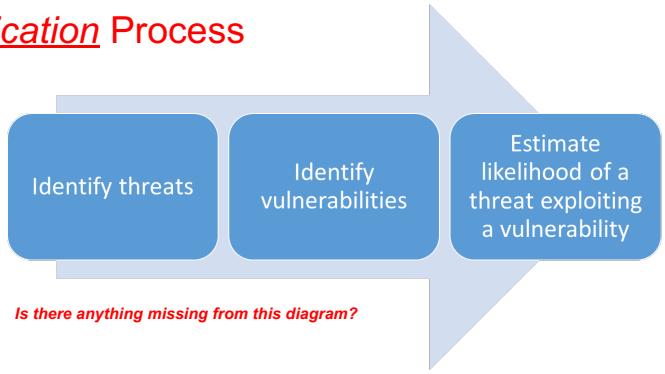


[Source: IT Governance Institute. 2005 Information risks: Whose business are they? Page 12]

1. Understanding Risk – risk assessment

Slide 18

Risk *Identification* Process



Is there anything missing from this diagram?

Risk assessment is the identification and analysis and priortisation of risks that might jeapordise our achievement of business objectives.

In this sense: Information security is an exercise in risk management, it involves the protection of information assets (whether in storage, processing, or transit) and systems from damage, misuse or attack;

1. Understanding Risk – risk assessment

Slide 19

Some definitions

- **Threat**: Any circumstance or event with the potential to adversely impact organisational operations, assets, individuals or the Nation (through an information system) via unauthorised access, destruction, disclosure, or modification information, and/or denial of service.
- **Vulnerability:** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

NIST SP800-30, (2012) Guide for conducting risk assessments

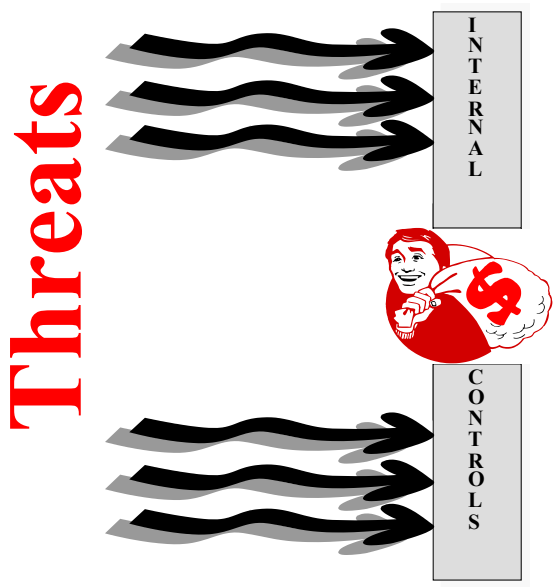
- **Asset:** any information resource valued by the organisation as such; e.g. data, device or component of the information environment; information and related resources – funds to support it, people, equipment, technology *–can be subject to intentional attacks, unintentional errors and mistakes*

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

19

1. Understanding Risk – risk assessment

Slide 20



SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

20

Information security threats

Slide 21

Internal Opportunistic / Accidental	Internal Malicious
External Opportunistic / Accidental	External Malicious

The opportunity presents itself in the work place

An insecure system offers the opportunity to 'look around' and ….

Disgruntled Staff; theft for personal gain

Pre-meditated; with ill intent; max damage hoped for ….e.g. virus and hacker attacks, planned cybercrime

How much of the above can be secured using technology tools alone?

(e.g. firewalls + anti-virus programs + IDS)

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

21

Information security threats

Slide 22

Internal Opportunistic / Accidental	Internal Malicious
External Opportunistic / Accidental	External Malicious

The opportunity presents itself in the work place

An insecure system offers the opportunity to 'look around' and ….

Disgruntled Staff; theft for personal gain

Pre-meditated; with ill intent; max damage hoped for ….e.g. virus and hacker attacks, planned cybercrime

Less than 15% of threats can be safeguarded using technology tools - what about the remaining 85% + ??

How much of the above can be secured using technology tools alone?

(e.g. firewalls + anti-virus programs + IDS)

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

22

Information security threats

Slide 23

- One of the biggest threats to organisations remains *us*; our use of information systems puts the information at risk (i.e. there is a chance of a loss or reduced value of an organisational asset)
- Any member of an organisation (e.g. an employee) who
  - Views, collects, modifies, processes, enhances, stores or deletes information; carries a USB stick, operates hard drive, answers emails, undertakes data entry, surfs the web,
  - The majority of incidents occur by accident and possibly without senior management's awareness due to a lack of knowledge …
  - Without policies in place, about how information *that may be at* risk should be managed; without procedures, processes or systematic approaches in place to guide policy implementation,
    i. incidents will continue to occur (sometimes without anyone being aware)
    ii. We will have little sense of which threats present the greatest risks

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

23

Responses to threats

Slide 24

- Need to remove or minimise the security Vs usability standoff
- Must not leave out the user!
- Account for all agents within user scenarios
  - The attacker
  - The IT team
  - The operator
  - The end user
    - The client / customer
    - The citizen / consumer
  - The Executive
- Design security with use of information assets (usability) in mind This requires a change in attitude from *Dr No to Dr Know*
- *It is a community response*

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

24

1. Understanding Risk – risk assessment

Slide 25

Identifying risks

- Unlimited number of threats that may be of concern to an organisation
- Elements of threats
  - The agent - the catalyst that performs the threat - human, machine or nature
  - The motive - cause an agent to act (accidental or intentional)
  - The results - outcome of the applied threat, eg. unauthorised access, destruction of the information asset

1. ***Focus on the organisations information assets and the user!***
2. ***The value creation activities and their protection***

[Source Peltier 2001]

2. Risk management

Slide 26

What is risk management?

- *Coordinated activities to direct and control an organisation with regard to the management of their risks* (enterprise or portfolio view)
- According to the ***COSO ERM framework***, every risk management decision either increases, decreases or erodes value :
  - Aligning risk appetite
  - Reducing operational surprises
  - Enhancing risk response
  - Identifying and managing multiple and cross-enterprise risks
  - Seizing opportunities
  - Improving deployment of capital

COSO Treadway Commission, 1985

Slide 27

Due to questionable corporate political campaign finance practices and foreign corrupt practices in the mid-1970s,

the U.S. Securities and Exchange Commission (SEC) and the U.S. Congress enacted campaign finance law reforms and the 1977 Foreign Corrupt Practices Act (FCPA) which criminalized transnational bribery and ***required companies to implement internal control programs***.

In response, the Treadway Commission, a private-sector initiative, was formed in 1985 to inspect, analyze, and make recommendations on fraudulent corporate financial reporting.

2. Risk management

Slide 28

Establishing the context

Enterprise Risk Management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across an enterprise, designed to identify potential events that may effect an entity, and manage risks to be within its risk appetite, to *provide reasonable assurance regarding achievement of entity objectives*

COSO, ERM framework 2004

- Governance of risk, identifying, assessment, acceptance, communication & treatment
- Control environment, risk assessment, control activities, information & communication and monitoring

Looking ahead

Slide 29

Controlling for risk?

- We can manage for risk by establishing **controls**
- Information *security* management is about establishing controls within and around organisations - for business (controls are approaches to managing for risk)
- The absence or weakness of a control is called an **exposure** to risk
- A weakness in the **internal controls** that an organisation puts in place can expose the business to:
  1. Destruction of assets (physical & information)
  2. Theft of assets (physical & information)
  3. Corruption of information or the information systems
  4. Disruption of information communication and the information system

29

Looking ahead

Slide 30

Internal controls (safeguards) are about context

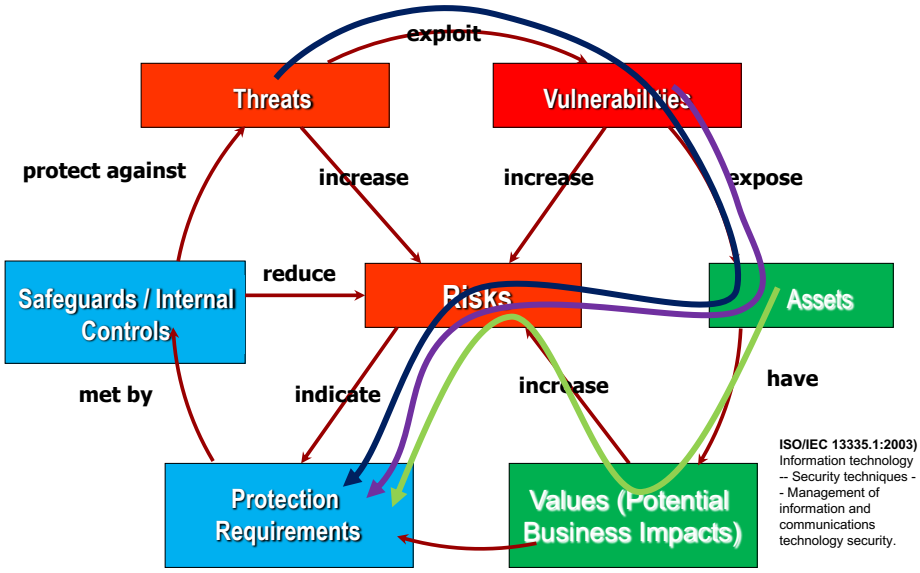
Comprises management's philosophy and operating style, ***and all the policies, practices and procedures*** employed by the organisation to achieve the organisation's objectives, broadly consisting of:

- Safeguarding assets of the firm (e.g. firewalls, IDS, zero tolerance ID)
- Ensuring the accuracy and reliability of records and information (e.g. procedures for validating invoices)
- Promoting efficiency in the firm's operations (e.g. automated secure procedures for real time processing of credit cards)
- Measuring compliance with prescribed policies, procedures, laws and regulations (e.g. Australian Privacy Principles)

30

Component relationships (ISO/IEC 13335)

Slide 31

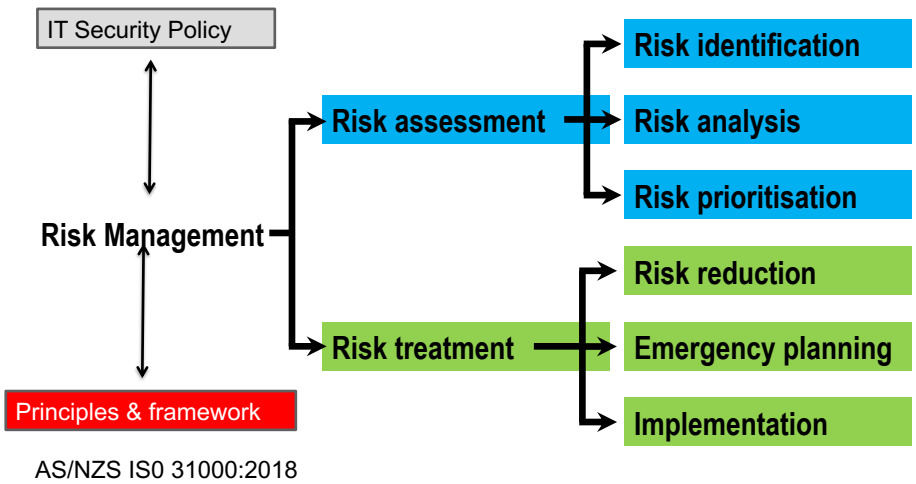


ISO/IEC 13335.1:2003) Information technology -- Security techniques -- Management of information and communications technology security.

31

2. Risk management

Slide 32

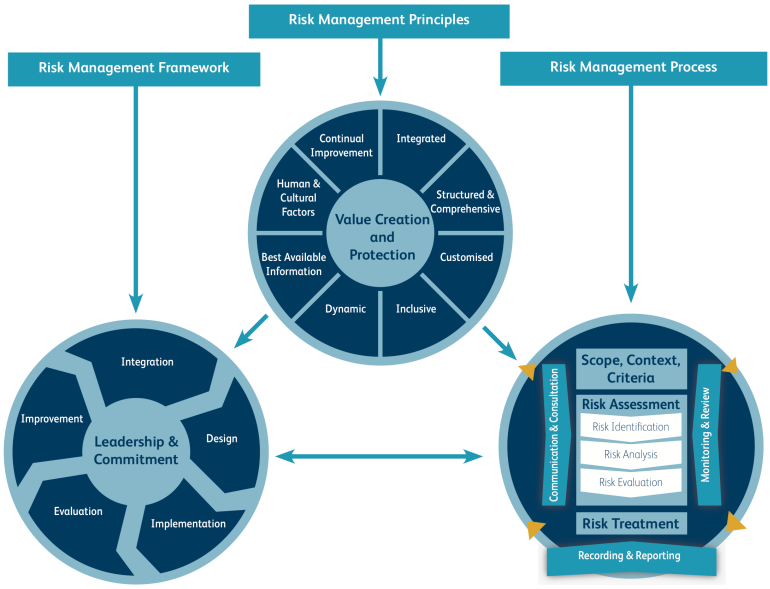


AS/NZS IS0 31000:2018

32

Principles, framework & practice 3100:2018

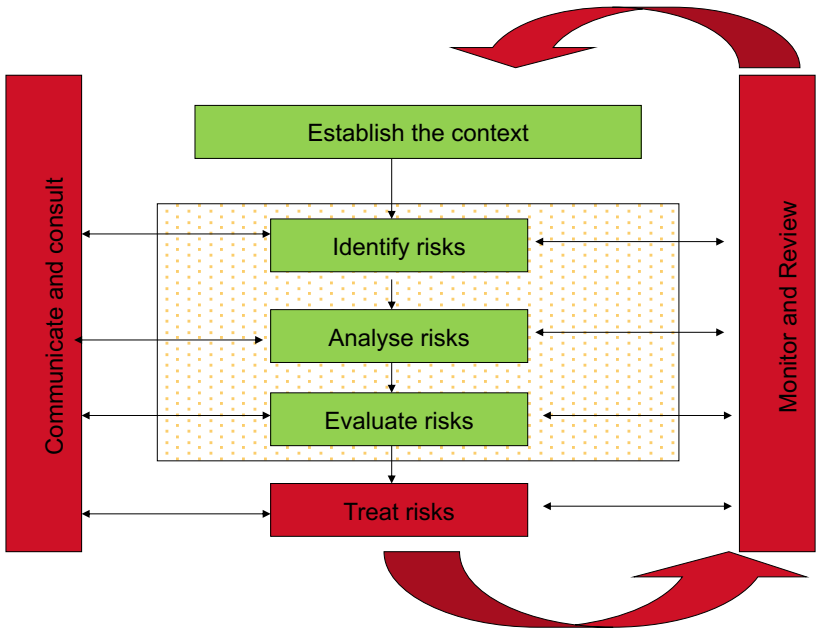
Slide 33



33

33

AS/NZS ISO 31000:2018



34

Thank you

Your questions

- Risk, Information risk
- Information Asset
- Asset, Threat & Vulnerability
- Risk Management

SWINBURNE UNIVERSITY OF TECHNOLOGY

Swinburne think forward

35