4. Security Management

Jin Hong

jin.hong@uwa.edu.au

Overview

- Security requirements asks **key security questions** of the system
  - What assets to be protected?
  - Which threats can compromise/damage the assets?
  - What are the means to mitigate those threats?

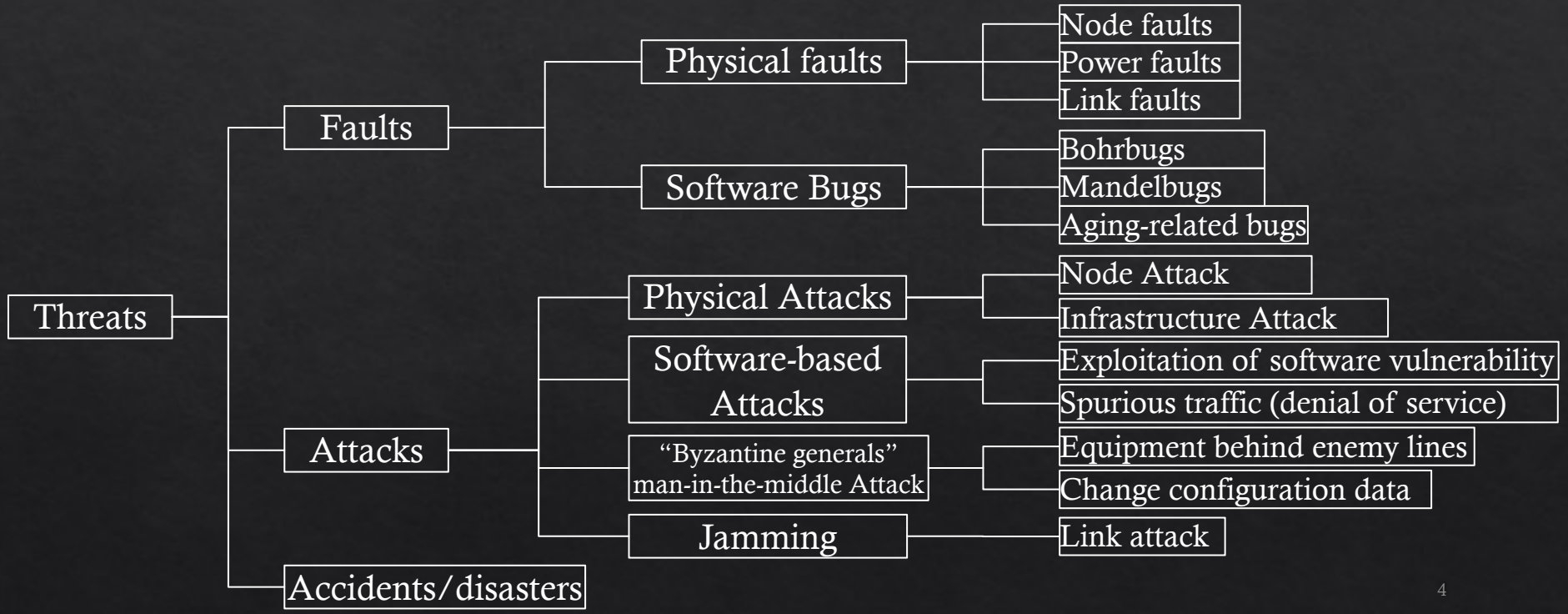
- Security management aims to **resolve those questions**
  - Define security objectives and potential threats
  - Carry out security risk assessment (w.r.t. assets)
  - Implement security solutions and monitoring

Terminology

Term	Meaning
Risk	The potential for an unwanted or adverse **outcome** resulting from an incident, event, or occurrence, as determined by the **likelihood (or the potential)** that a particular threat will exploit a particular vulnerability, with the associated consequences.
Vulnerability	A characteristic or specific **weakness** that renders an organization or asset (such as information or information system) open to exploitation by a given threat or susceptible to a given hazard.
Exploitation	A technique to breach the security of a network or information system in **violation** of security policy.
Threat	A circumstance or event (including accidental and non-human related) that has or indicates the **potential** to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.
Asset	A person, structure, facility, information, and records, information technology systems and resources, materials, process, relationships, or reputation allowing entities (e.g., individuals, businesses and governments) to achieve social, economic, and other objectives of **value**.

Threats in Security

also for Dependability and Survivability



K. S. Trivedi, D. S. Kim, A. Roy and D. Medhi, "Dependability and security models," *2009 7th International Workshop on Design of Reliable Communication Networks*, Washington, DC, 2009, pp. 11-20. doi: 10.1109/DRCN.2009.5340029

IT Security Management

- IT security management aims to achieve and maintain **appropriate levels** of confidentiality, integrity and availability of the system
- In addition, it also look at accountability, authenticity, reliability, and other security objectives

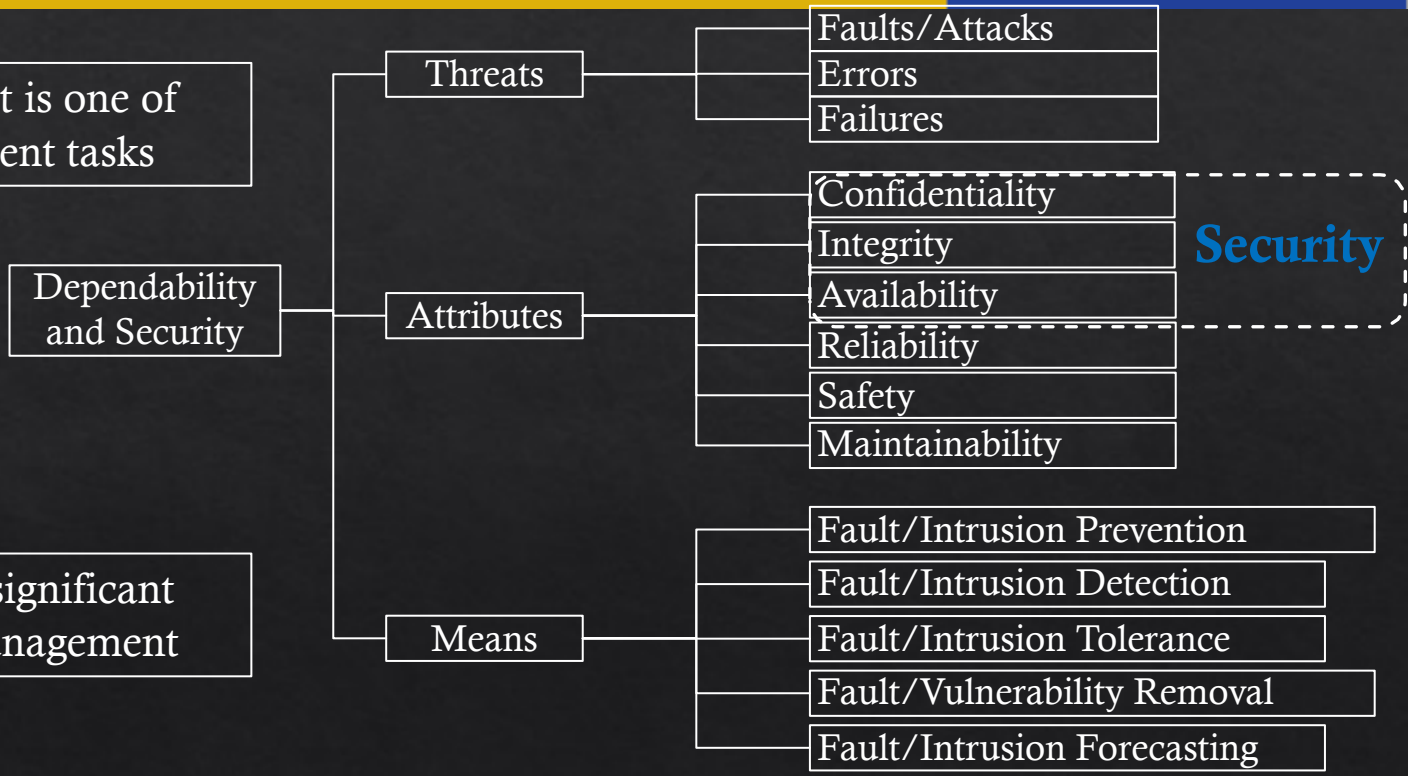
IT Security Management

- Related **tasks** for IT security management include
  - Specification of security objectives, strategies and policies
  - Determine organisational IT security requirements
  - Security threat assessments of IT assets and risks
  - Specification of appropriate security methods
  - Implementation and maintenance of security methods
  - Security awareness program and adoption
  - Detection and prevention of security incidents

IT Security Management

IT Security management is one of the IT system management tasks

Dependability is also a significant aspects of IT system management



K. S. Trivedi, D. S. Kim, A. Roy and D. Medhi, "Dependability and security models," *2009 7th International Workshop on Design of Reliable Communication Networks*, Washington, DC, 2009, pp. 11-20. doi: 10.1109/DRCN.2009.5340029

Security Standards

- Essential Eight (EE) Mitigation Strategies
  - Australian Standard publicly available
  - Not mandatory in Australia, but strongly encouraged (e.g., UWA implements Essential Eight)
- ISO 27000 Security Standards
  - About 36 standards[1]
  - Widely used, but not public
- NIST Security Framework
  - Publicly available
  - Broadly reviewed by government and industry professionals
  - E.g., SP800 series
    - E.g., SP800-12: Computer security handbook
    - E.g., SP800-14: Generally accepted security principles & practices etc.

[1]http://www.iso27001security.com/index.html

Security Standards

- IS management
  - ISO27001 – information security management systems – requirements
  - ISO27002 – Code of practice for information security management
  - ISO27003 – information security management system implementation guidance
  - ISO27007 – guidelines for information security management systems
  - SP800-14 – generally accepted principles and practices for securing IT systems
- Security measurement
  - ISO27004 – information security management – measurement
  - SP800-55 – performance measurement guide for information security

Security Standards

- Security risk management
  - ISO27005 – information security risk management
  - SP800-30 – guide for conducting risk assessments
  - SP800-37 – guide for applying the risk management framework to federal information systems: a security life cycle approach
- Incident management
  - ISO27035 – Security incident management
  - SP800-61 – computer security incident handling guide

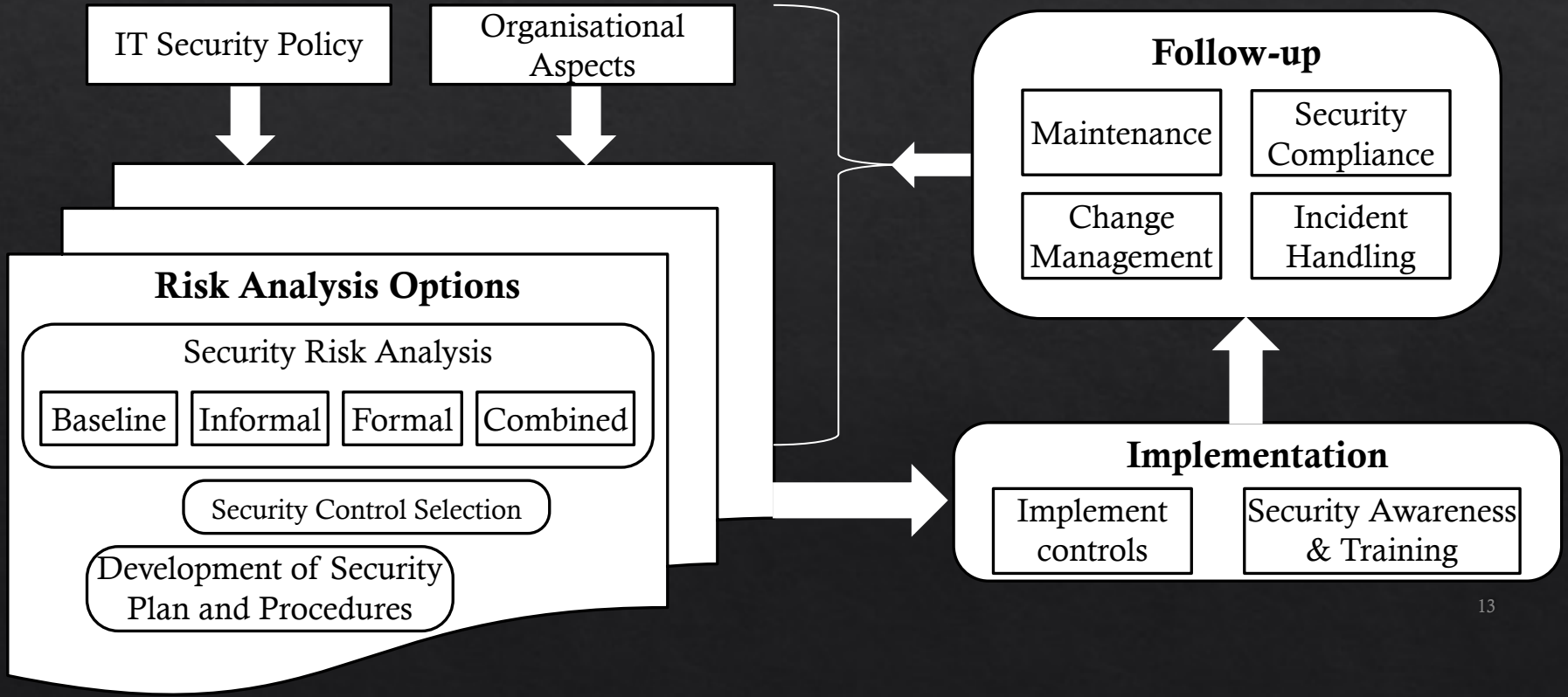
Security Standards

- Unlike ISO and NIST, the EE defines a set of tasks the organisation must do to mitigate attacks:
  1. Application Control
  2. Patching Applications
  3. Configuring Microsoft Office Macro Settings
  4. User Application Hardening
  5. Restrict Administrative Privileges
  6. Patching Operating Systems
  7. Multi-Factor Authentication
  8. Daily Backup

Security Standards

- How does EE differs to ISO or NIST?

Security Management Process



Security Risk Assessment

- Typical system includes many assets
  - Confidential data, user details, operational policies etc
- It is **infeasible** to examine the risk of all the assets due to *limited resources*
- To use the best security risk assessment approach given the organisation's resources
  - **Baseline**: use the "industry best practice"
    - Implementing standard security and safeguards against common threats
  - **Informal**: conduct informal, pragmatic/practical risk analysis
  - **Formal**: assess the security risk using formal structured process
  - **Combined**: combinations of other approaches

EE Maturity Level

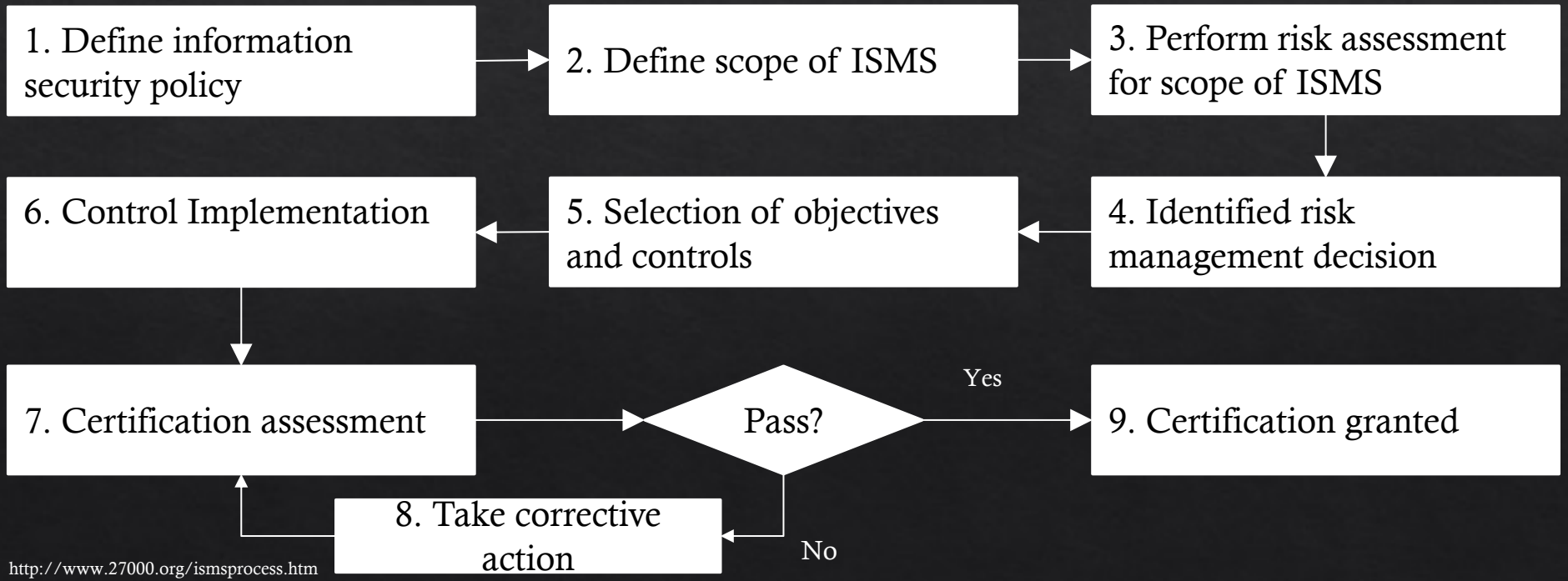
- EE is implemented using a risk-based approach.
- Maturity level is used to support the implementation of EE, defining different stages of security implementations.
- The levels are defined based on the tradecraft (i.e., capabilities of attackers/threats).
- Levels start from zero to three.
- Maturity Level 0 essentially confirms the organisation is susceptible to cyberattack to violate CIA.

EE Maturity Level

- Maturity Level 1
  - The attacker typically uses readily available tools and knowledge for exploits.
- Maturity Level 2
  - The attacker may invest time and resources to carry out attack, typically showing selective behaviour in target selection.
- Maturity Level 3
  - The attacker is more adaptive and less reliant on public tools and techniques, evading security monitoring tools and bypassing security solutions.

https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model

ISO27001


1. Define information security policy
2. Define scope of ISMS
3. Perform risk assessment for scope of ISMS
4. Identified risk management decision
5. Selection of objectives and controls
6. Control Implementation
7. Certification assessment
Pass?
Yes
9. Certification granted
No
8. Take corrective action
http://www.27000.org/ismsprocess.htm

ISO27001

Input

- -

1. Define information security policy

Output

- Delivers policy document

To specify a set of security policy to follow

ISO27001

Input

- -

2. Define scope of ISMS

Output

- Delivers ISMS scope document

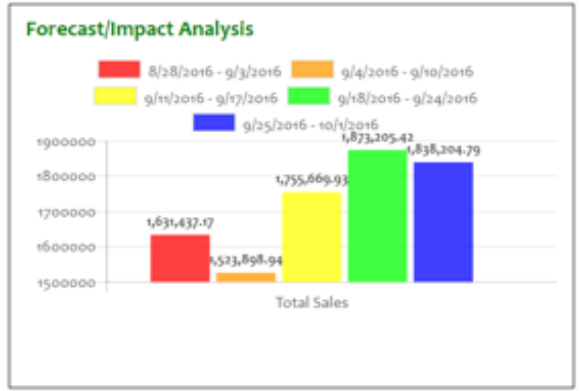
To define the scope of the information security management system e.g., Identify threats the ISMS will mitigate. Security objectives to satisfy

ISO27001

3. Perform risk assessment for scope of ISMS

Input

- Threats
- Risks
- Impacts
- Vulnerabilities



Output

- RA document

Carry out risk assessment given the scope of ISMS and the security policy.
This involves risk management and risk treatment.

ISO27001

Input

- Company decision makers

4. Identified risk management decision

Output

- Agreement document of accountabilities and responsibilities

Distribute tasks and identify responsibilities for managing the identified risks

ISO27001

5. Selection of objectives and controls

Input

- Controls and guidance from ISO17799
- Any other controls

Output

- Produce statement of applicability (SoA)

Produces SoA, which is a selection of controls to mitigate risks and the reason for selecting them. Also specifies their progress on implementation, and explanations on why certain controls are not implemented.

ISO27001

Input

- -

6. Control Implementation

Output

- -

Carry out implementation of controls specified in SoA.

ISO27001

Input

- -

7. Certification assessment

Output

- -

Review that all process steps are complete and identified risks are mitigated.

ISO27001

Input

- -

8. Take corrective action

Output

- -

Revisit incomplete process steps and complete them as necessary.

ISO27001

Input

- -

9. Certification granted

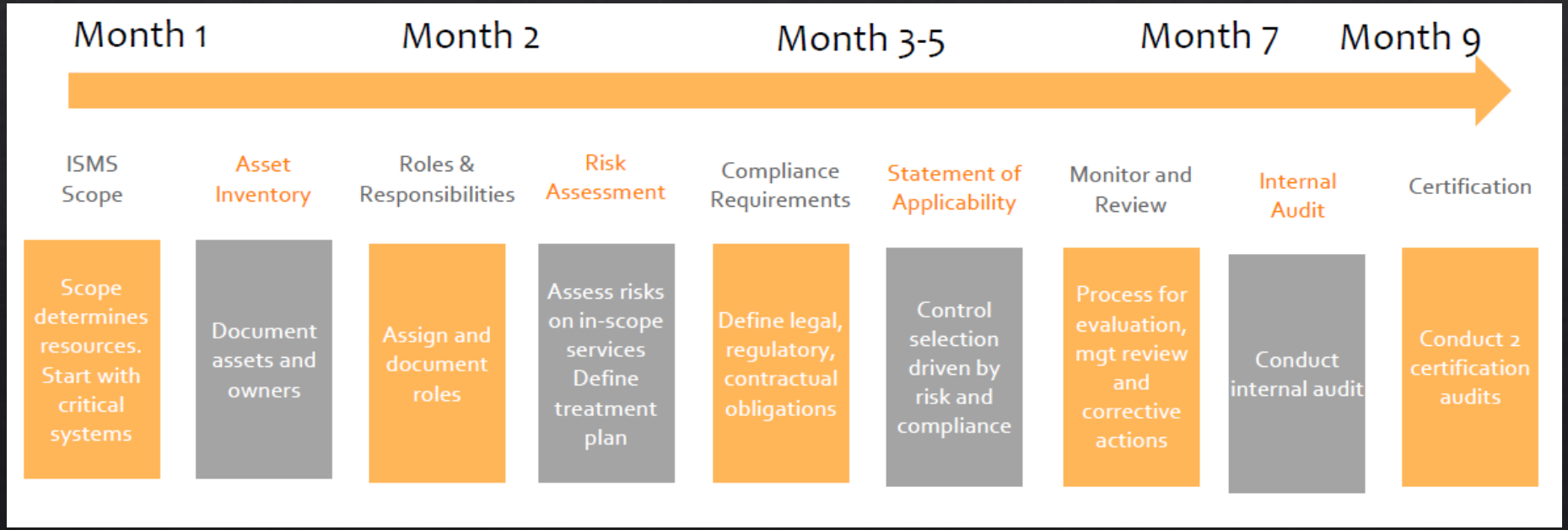
Output

- -

The company is now ISO27001 certified.

ISO27001 Timeframe

- Rough estimate



NIST SP800-30

- NIST SP800-30 outlines 9 risk assessment activities

Also ISO27005, but not covered.

NIST SP800-30

1. System characterisation

Input

- Hardware
- Software
- System interfaces
- Data and information
- People
- System mission

Output

- System boundary
- System functions
- System and data criticality
- System and data sensitivity

Process to profile the system
e.g., find the system configuration, dependencies, operations, usage etc.

NIST SP800-30

2. Threat identification

Input

- History of system attack
- Data from intelligence agencies, NIPC, OIG, FedCIRC, mass media, etc

Output

- Threat statement

Identify and understand possibilities of attacks to the system
e.g., latest attack methods and approaches that can violate the security requirements of the system

NIST SP800-30

3. Vulnerability identification

Input

- Reports from prior risk assessments
- Any audit comments
- Security requirements
- Security test results

Output

- List of potential vulnerabilities

Locate vulnerabilities in the system
e.g., using vulnerability scanners and IDS reports

NIST SP800-30

Input

- Current controls
- Planned controls

4. Control analysis

Output

- List of current and planned controls

Identify and evaluate the effects of current and planned security controls

e.g., authentication will protect the system from external users

NIST SP800-30

5. Likelihood determination

Input

- Threat-source motivation
- Threat capacity
- Nature of vulnerability
- Current controls

Output

- Likelihood rating

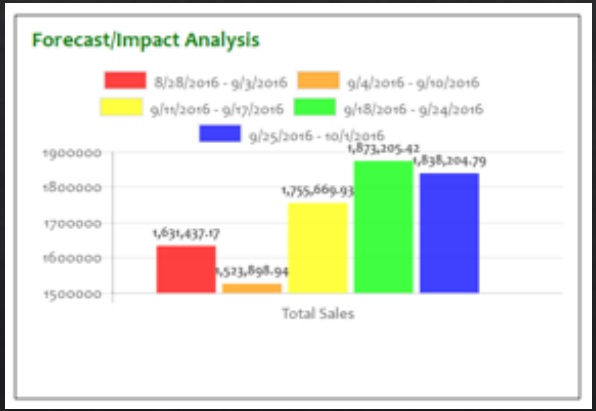
Consider the inputs to evaluate the likelihood (will someone exploit this?)
e.g., found a BoF vulnerability on a machine which is disconnected from the network

NIST SP800-30

6. Impact analysis

Input

- Mission impact analysis
- Asset criticality assessment
- Data criticality
- Data sensitivity



Output

- Impact rating

To determine the significance of an attack to the system and the organisation

e.g., compromised user profile database will disable users logging into the system to carry out their tasks

NIST SP800-30

Input

- Likelihood of threat exploitation
- Magnitude of impact
- Adequacy of planned or current controls

7. Risk determination

Output

- Risks and associated risk levels

Take consideration of the risk assessment results and determine the level of the system security risk
e.g., to prioritise security control selection (next activity)

NIST SP800-30

8. Control recommendation

Input

- -

Output

- Recommended controls

Based on the risk assessment results, select the security control to implement
e.g., update firewall rules, adopt new security policy, deploy IDS etc.

NIST SP800-30

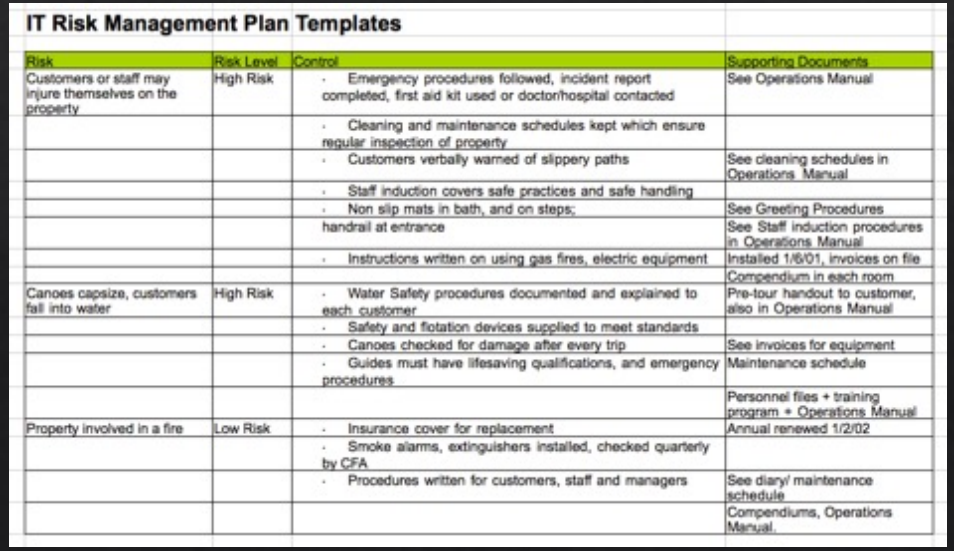
9. Results documentation

Input

- -

Output

- Risk assessment report



IT Risk Management Plan Templates

Risk	Risk Level	Control	Supporting Documents
Customers or staff may injure themselves on the property	High Risk	· Emergency procedures followed, incident report completed, first aid kit used or doctor/hospital contacted	See Operations Manual
		· Cleaning and maintenance schedules kept which ensure regular inspection of property	
		· Customers verbally warned of slippery paths	See cleaning schedules in Operations Manual
		· Staff induction covers safe practices and safe handling	
		· Non slip mats in bath, and on steps;	See Greeting Procedures
		handrail at entrance	See Staff induction procedures in Operations Manual
		· Instructions written on using gas fires, electric equipment	Installed 1/6/01, invoices on file
			Compendium in each room
Canoes capsize, customers fall into water	High Risk	· Water Safety procedures documented and explained to each customer	Pre-tour handout to customer, also in Operations Manual
		· Safety and flotation devices supplied to meet standards	
		· Canoes checked for damage after every trip	See invoices for equipment
		· Guides must have lifesaving qualifications, and emergency procedures	Maintenance schedule
			Personnel files + training program + Operations Manual
Property involved in a fire	Low Risk	· Insurance cover for replacement	Annual renewed 1/2/02
		· Smoke alarms, extinguishers installed, checked quarterly by CFA	
		· Procedures written for customers, staff and managers	See diary/ maintenance schedule
			Compendiums, Operations Manual.

Risk Treatment

- Different actions can be taken for identified risks
  - **Risk acceptance**
    - Understand the risk but will not act on it
  - **Risk avoidance**
    - Take actions to prevent this risk from happening
  - **Risk transfer**
    - Shift the risk to other assets, processes or organisations
    - E.g., outsourcing to other organisations, get insurance etc
  - **Reduce consequence**
    - Implement security controls
    - E.g., off-site backup, disaster recovery plan, replications etc
  - **Reduce likelihood**
    - Implement security controls
    - E.g., firewall, password complexity management /policy etc.

IT Security Management

- Related tasks for IT security management include
  - Specification of security objectives, strategies and policies
  - Determine organisational IT security requirements
  - Security threat assessments of IT assets and risks
  - Specification of appropriate security methods
  - Implementation and maintenance of security methods
  - Security awareness program and adoption
  - Detection and prevention of security incidents

Digital Forensics

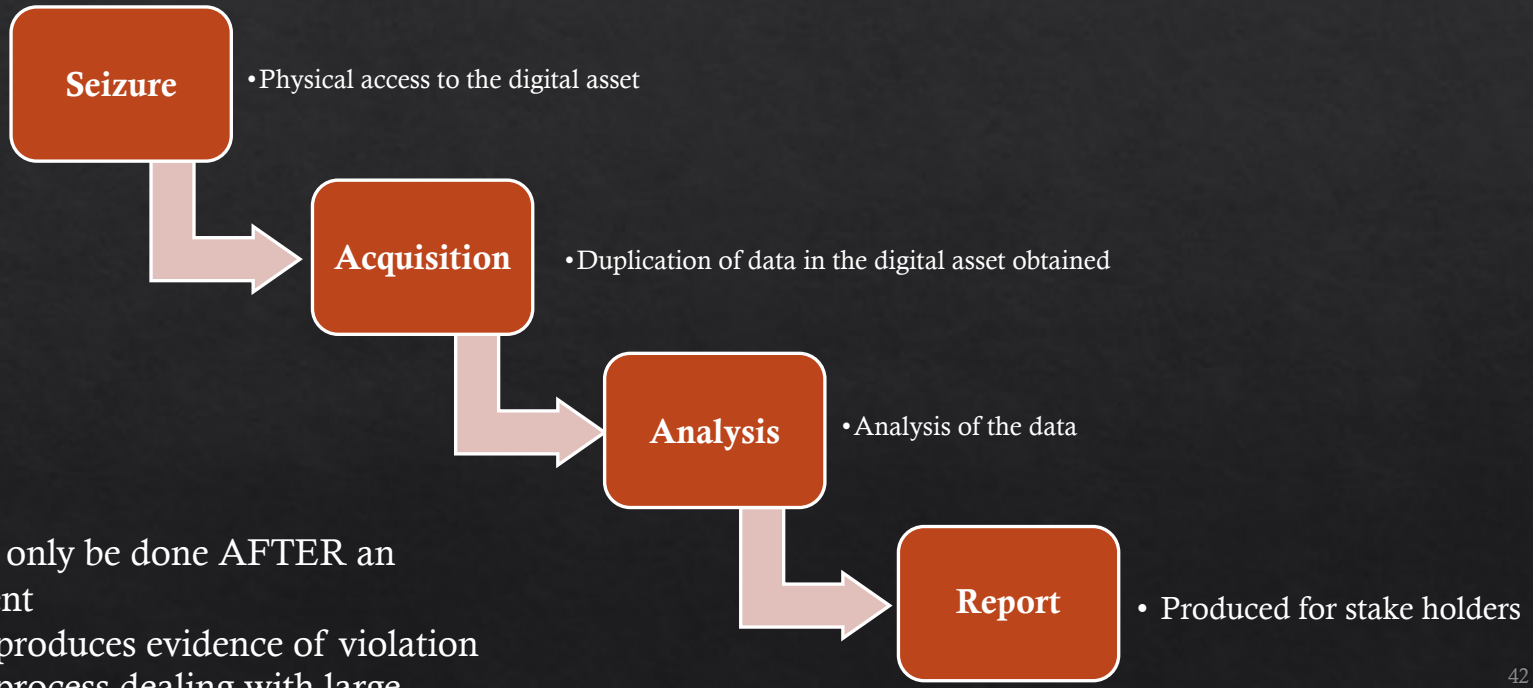
- Digital Forensic Science

> *"The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations." (Palmer, 2001: 16)*

Digital Forensics

- Digital evidence can be used for various reasons.
- People who could be interested in digital evidence are:
  - Law people
    - E.g. Criminal justice agencies, Prosecutor's Office/DA, Attorneys, and Judges
  - Business people
    - E.g. Corporate Councils, Company Legal resources, Human Resources
  - Security people
    - E.g. Auditors, Crackers/Hackers

Digital Forensics



But:

- It can only be done AFTER an incident
- Only produces evidence of violation
- Slow process dealing with large quantity of data

Digital Forensics

- How do we carry out DF?
  - Very good resource available from: https://www.jaiminton.com/cheatsheet/DFIR/#
    - ~30 mins read

Summary

- There are **various** security standards and frameworks internationally accepted as a common practice
  - E.g,. ISO and NIST security standards and frameworks
- They provide detailed **procedures** for organisations to follow, in order to assess the security posture of their systems
- Many steps are involved, so security administrators should ensure that each step is done **carefully and complete**
- Use of **automated tools** can speed up the process, as well as avoiding any human errors

Additional Items

- Security standards and framework
  - ISO: http://standards.iso.org/ittf/PubliclyAvailableStandards/
  - ISO: http://www.iso27001security.com/index.html
  - NIST: https://www.nist.gov/cyberframework
  - ASD: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight