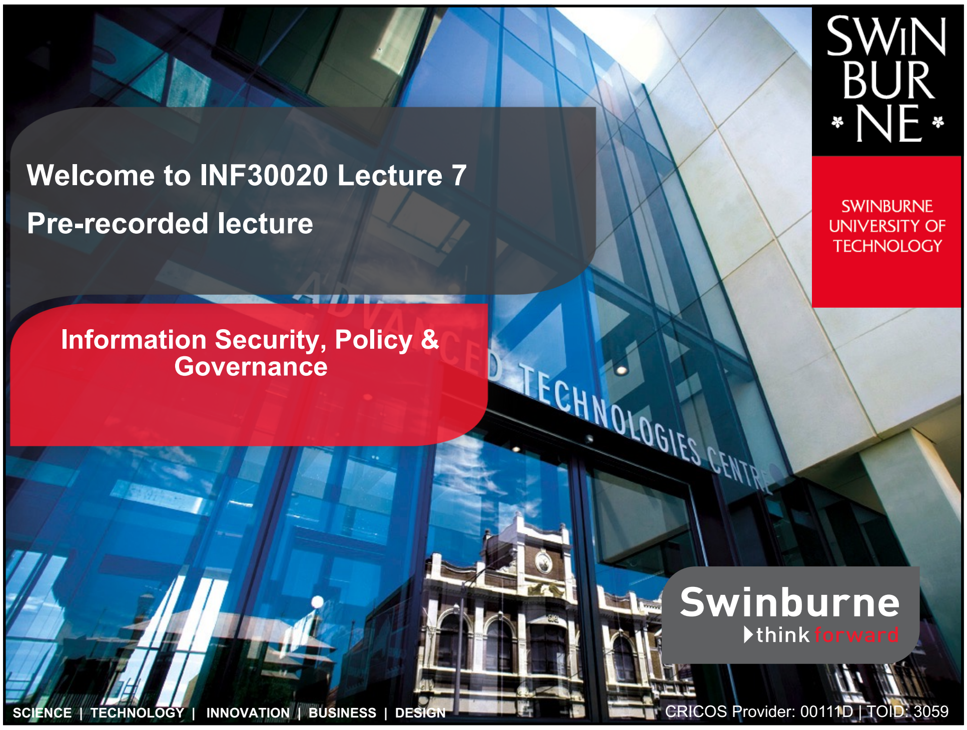


Welcome to INF30020 Lecture 7

Pre-recorded lecture

Information Security, Policy & Governance

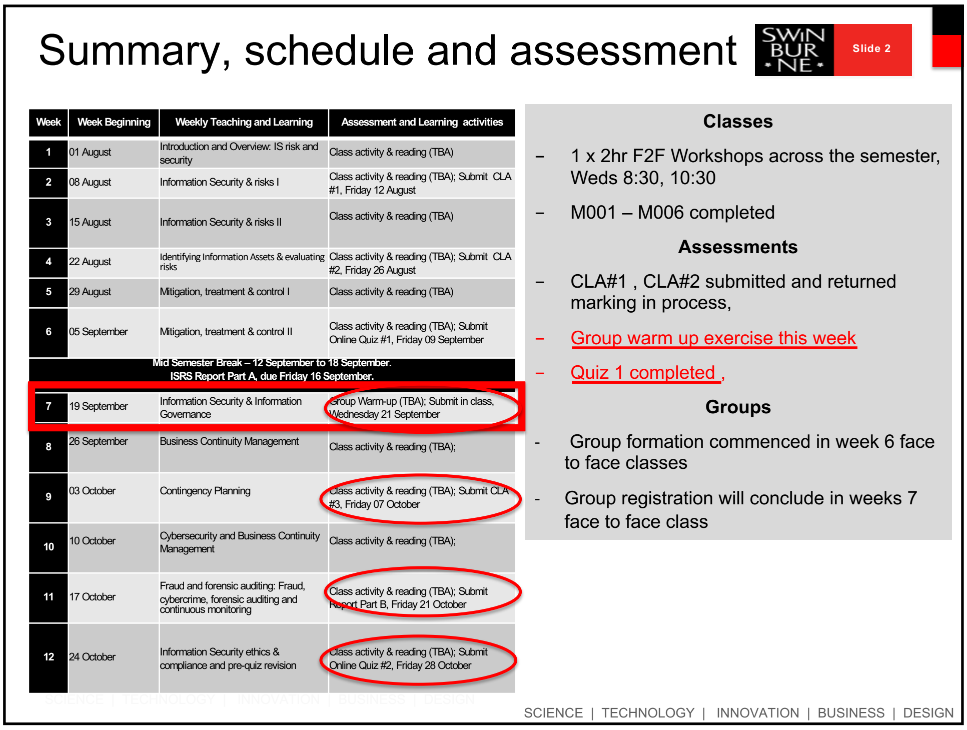
SWINBURNE UNIVERSITY OF TECHNOLOGY

Swinburne
think forward

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

CRICOS Provider: 00111D | TOID: 3059

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	Identifying Information Assets & evaluating risks	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

Classes

- 1 x 2hr F2F Workshops across the semester, Weds 8:30, 10:30
- M001 – M006 completed

Assessments

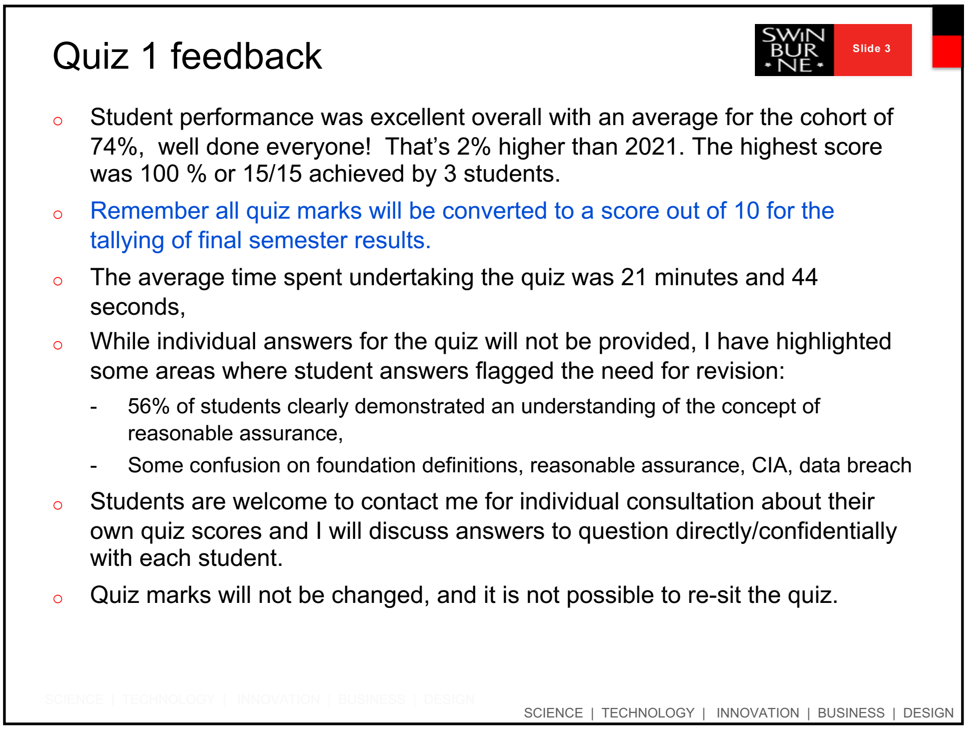
- CLA#1 , CLA#2 submitted and returned marking in process,
- Group warm up exercise this week
- Quiz 1 completed ,

Groups

- Group formation commenced in week 6 face to face classes
- Group registration will conclude in weeks 7 face to face class

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

2



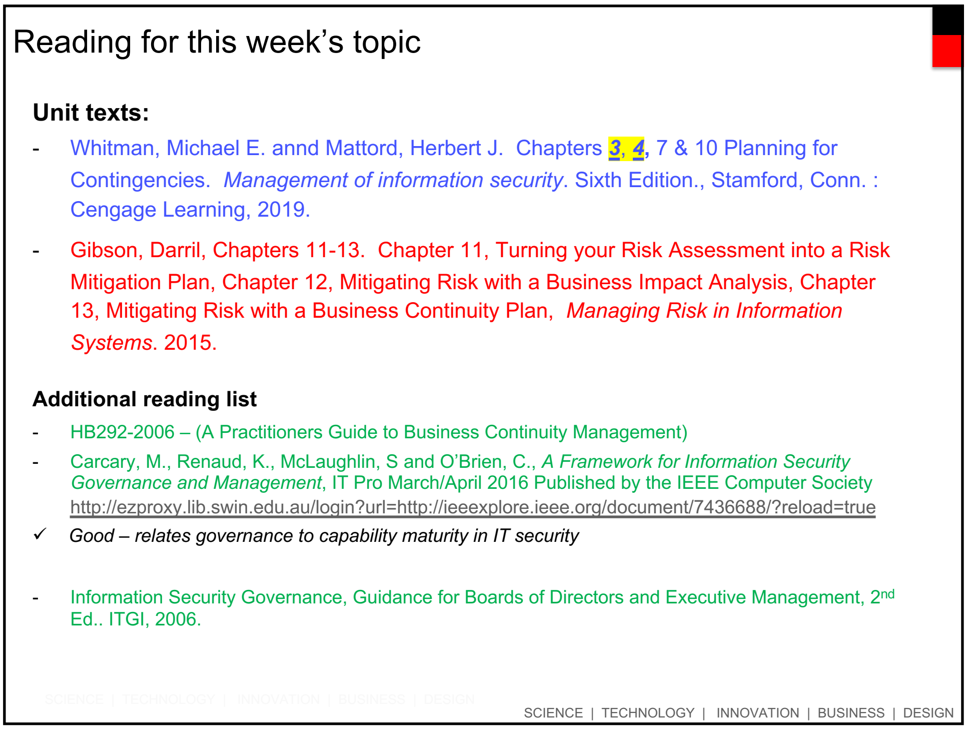
Quiz 1 feedback

SWIN BUR NE Slide 3

- Student performance was excellent overall with an average for the cohort of 74%, well done everyone! That's 2% higher than 2021. The highest score was 100 % or 15/15 achieved by 3 students.
- Remember all quiz marks will be converted to a score out of 10 for the tallying of final semester results.
- The average time spent undertaking the quiz was 21 minutes and 44 seconds,
- While individual answers for the quiz will not be provided, I have highlighted some areas where student answers flagged the need for revision:
  - 56% of students clearly demonstrated an understanding of the concept of reasonable assurance,
  - Some confusion on foundation definitions, reasonable assurance, CIA, data breach
- Students are welcome to contact me for individual consultation about their own quiz scores and I will discuss answers to question directly/confidentially with each student.
- Quiz marks will not be changed, and it is not possible to re-sit the quiz.

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

3



Reading for this week's topic

Unit texts:

- Whitman, Michael E. annd Mattord, Herbert J. Chapters 3, 4, 7 & 10 Planning for Contingencies. *Management of information security*. Sixth Edition., Stamford, Conn. : Cengage Learning, 2019.
- Gibson, Darril, Chapters 11-13. Chapter 11, Turning your Risk Assessment into a Risk Mitigation Plan, Chapter 12, Mitigating Risk with a Business Impact Analysis, Chapter 13, Mitigating Risk with a Business Continuity Plan, *Managing Risk in Information Systems*. 2015.

Additional reading list

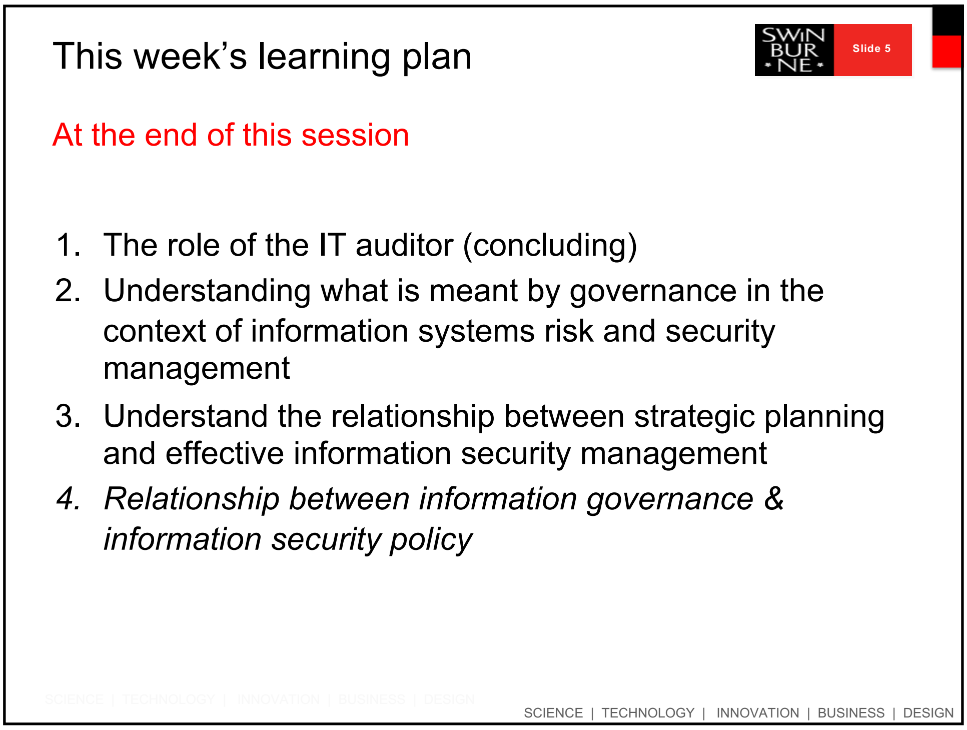
- HB292-2006 – (A Practitioners Guide to Business Continuity Management)
- Carcary, M., Renaud, K., McLaughlin, S and O'Brien, C., *A Framework for Information Security Governance and Management*, IT Pro March/April 2016 Published by the IEEE Computer Society http://ezproxy.lib.swin.edu.au/login?url=http://ieeexplore.ieee.org/document/7436688/?reload=true

✓ *Good – relates governance to capability maturity in IT security*

- Information Security Governance, Guidance for Boards of Directors and Executive Management, 2nd Ed.. ITGI, 2006.

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

4



This week's learning plan

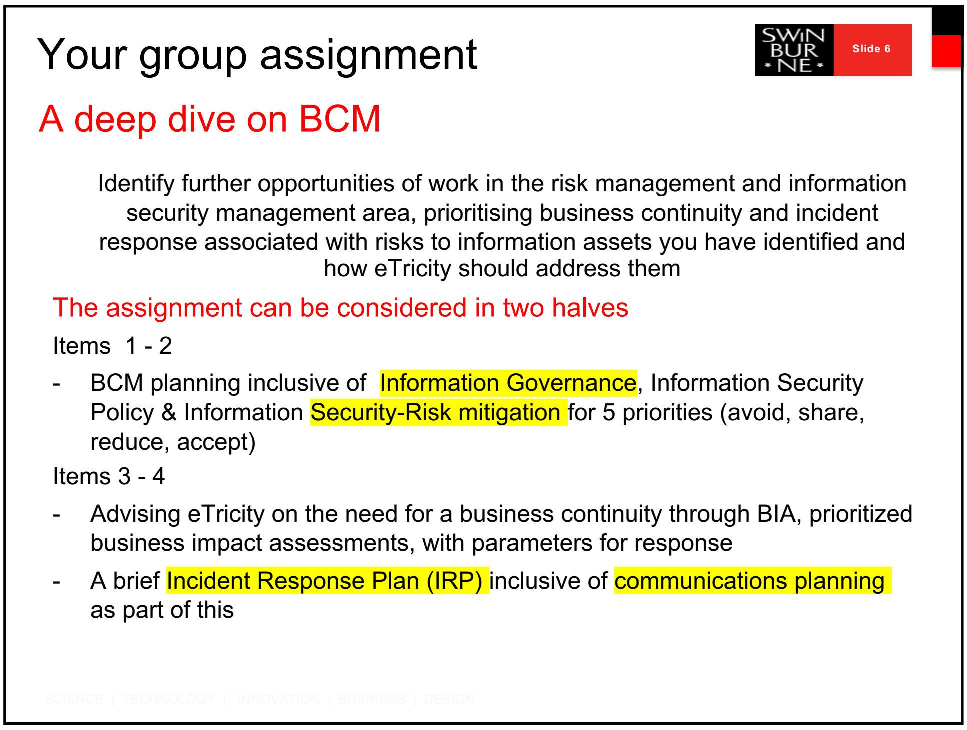
Slide 5

At the end of this session

1. The role of the IT auditor (concluding)
2. Understanding what is meant by governance in the context of information systems risk and security management
3. Understand the relationship between strategic planning and effective information security management
4. *Relationship between information governance & information security policy*

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

5



Your group assignment

Slide 6

A deep dive on BCM

Identify further opportunities of work in the risk management and information security management area, prioritising business continuity and incident response associated with risks to information assets you have identified and how eTricity should address them

The assignment can be considered in two halves

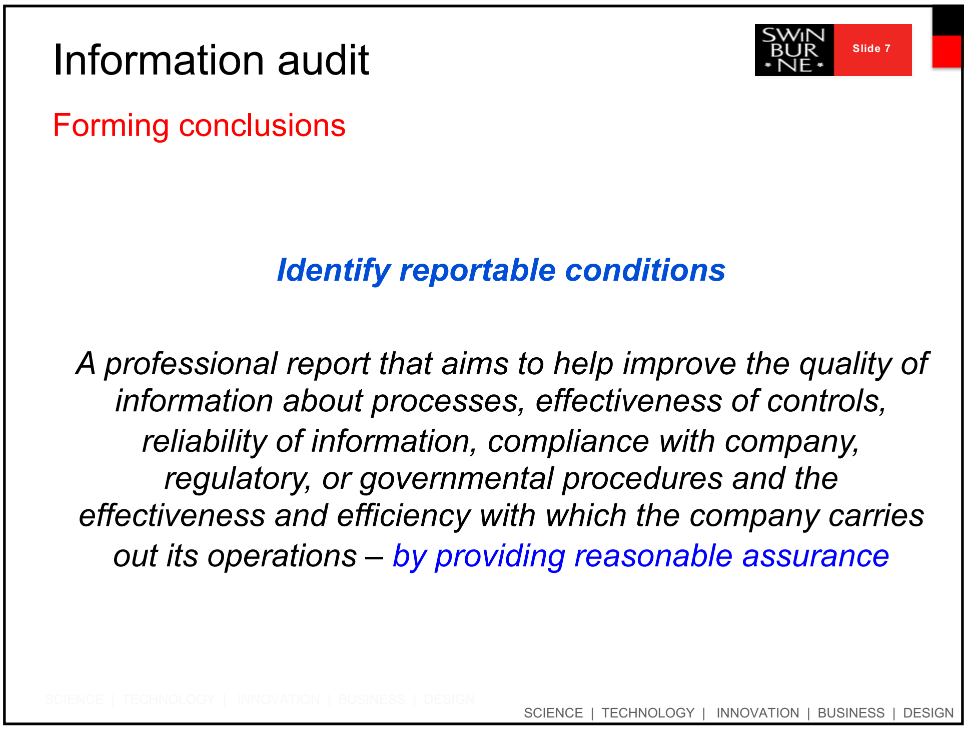
Items 1 - 2

- BCM planning inclusive of Information Governance, Information Security Policy & Information Security-Risk mitigation for 5 priorities (avoid, share, reduce, accept)

Items 3 - 4

- Advising eTricity on the need for a business continuity through BIA, prioritized business impact assessments, with parameters for response
- A brief Incident Response Plan (IRP) inclusive of communications planning as part of this

6



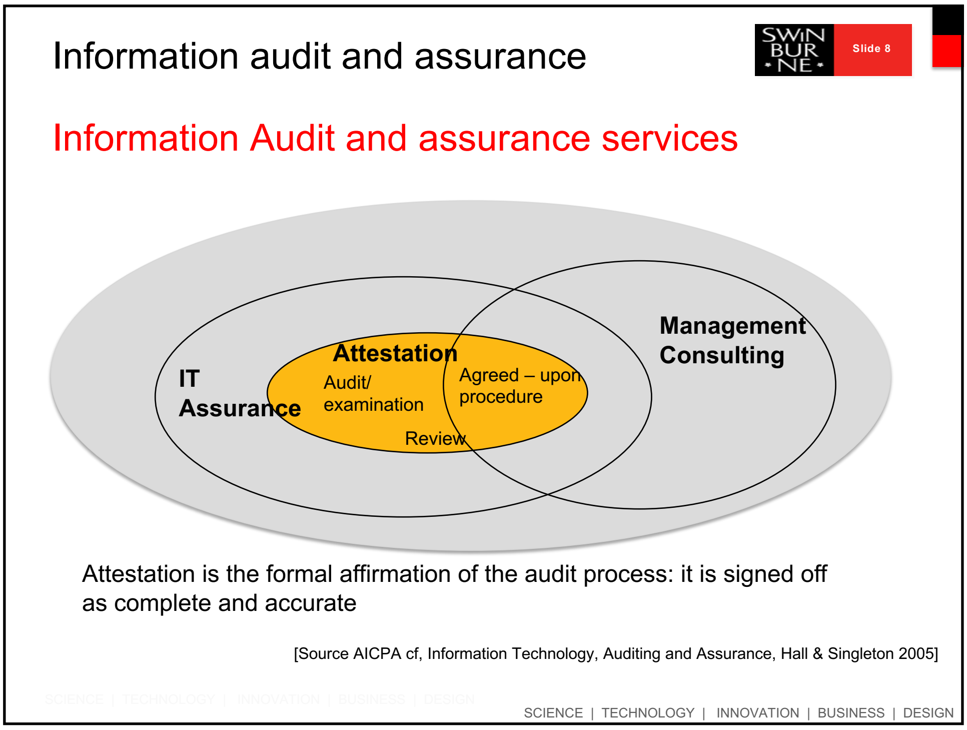
Information audit

Slide 7

Forming conclusions

Identify reportable conditions

A professional report that aims to help improve the quality of information about processes, effectiveness of controls, reliability of information, compliance with company, regulatory, or governmental procedures and the effectiveness and efficiency with which the company carries out its operations – by providing reasonable assurance



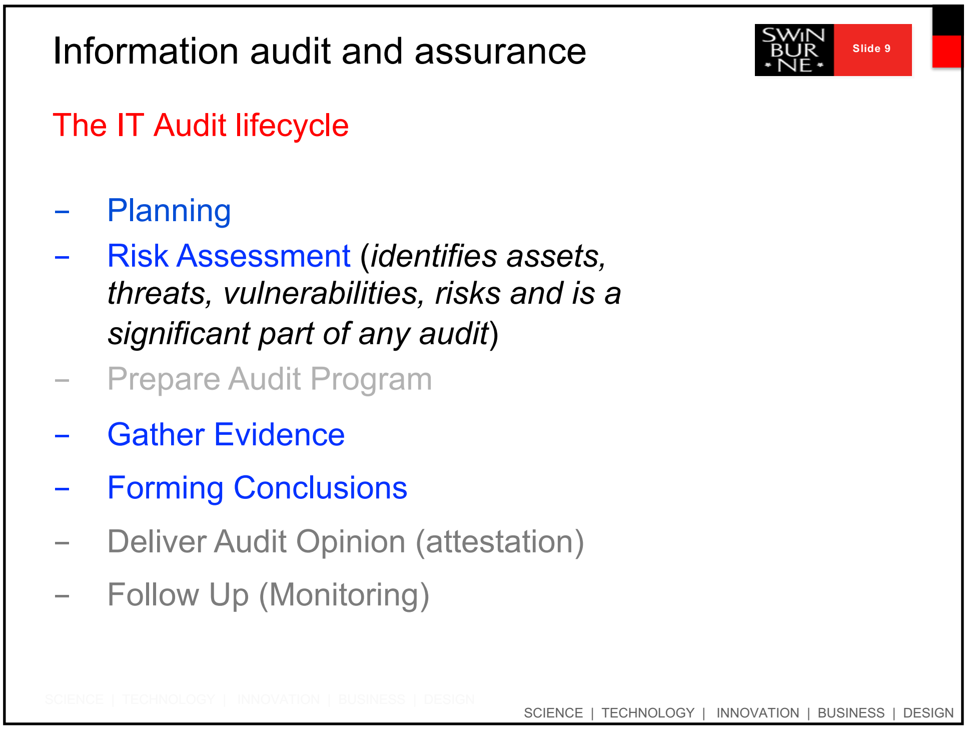
Information audit and assurance

Slide 8

Information Audit and assurance services

Attestation is the formal affirmation of the audit process: it is signed off as complete and accurate

[Source AICPA cf, Information Technology, Auditing and Assurance, Hall & Singleton 2005]

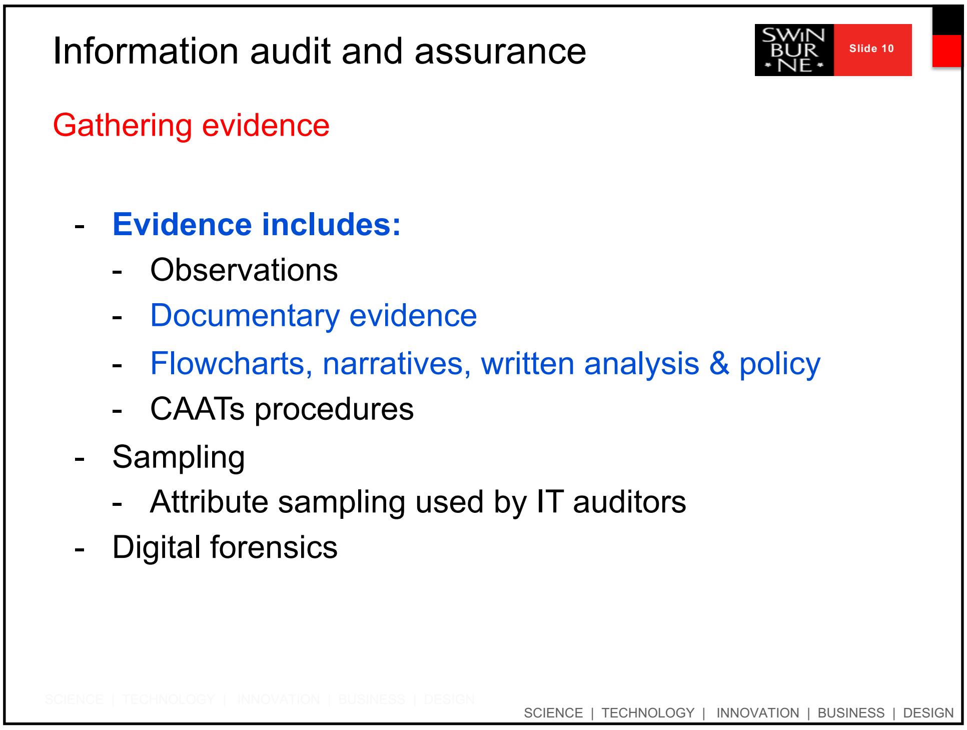


Information audit and assurance

Slide 9

The IT Audit lifecycle

- Planning
- Risk Assessment (*identifies assets, threats, vulnerabilities, risks and is a significant part of any audit*)
- Prepare Audit Program
- Gather Evidence
- Forming Conclusions
- Deliver Audit Opinion (attestation)
- Follow Up (Monitoring)

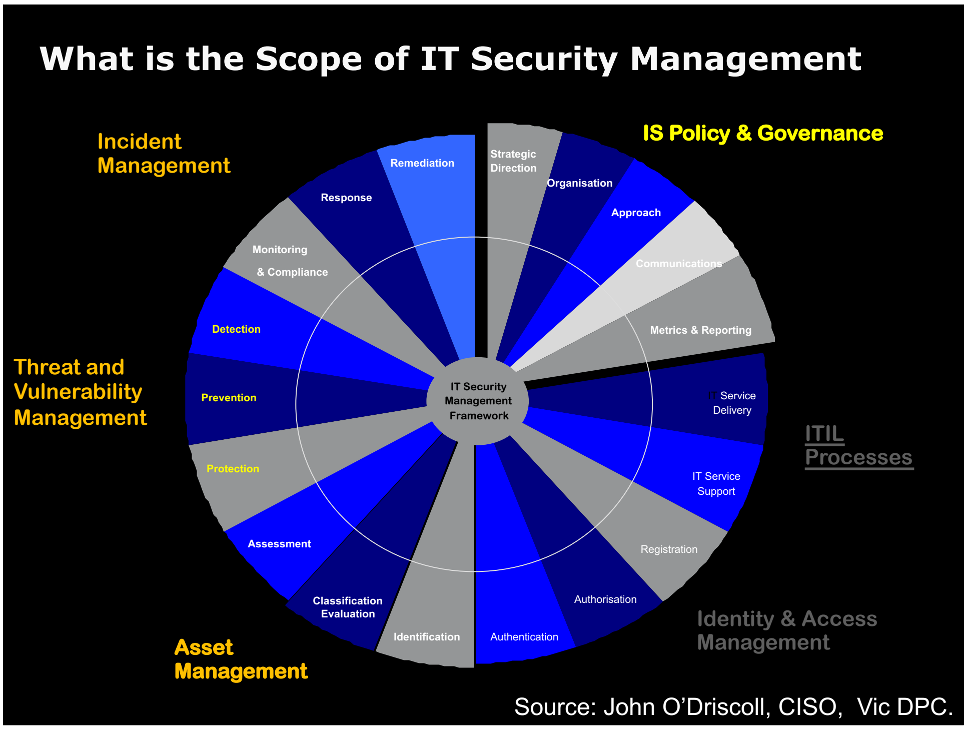


Information audit and assurance

Slide 10

Gathering evidence

- **Evidence includes:**
  - Observations
  - Documentary evidence
  - Flowcharts, narratives, written analysis & policy
  - CAATs procedures
- Sampling
  - Attribute sampling used by IT auditors
- Digital forensics



What is the Scope of IT Security Management

Incident Management

Remediation

Response

Monitoring & Compliance

IS Policy & Governance

Strategic Direction

Organisation

Approach

Communications

Metrics & Reporting

Threat and Vulnerability Management

Detection

Prevention

Protection

IT Security Management Framework

IT Service Delivery

IT Service Support

ITIL Processes

Registration

Authorisation

Authentication

Identity & Access Management

Assessment

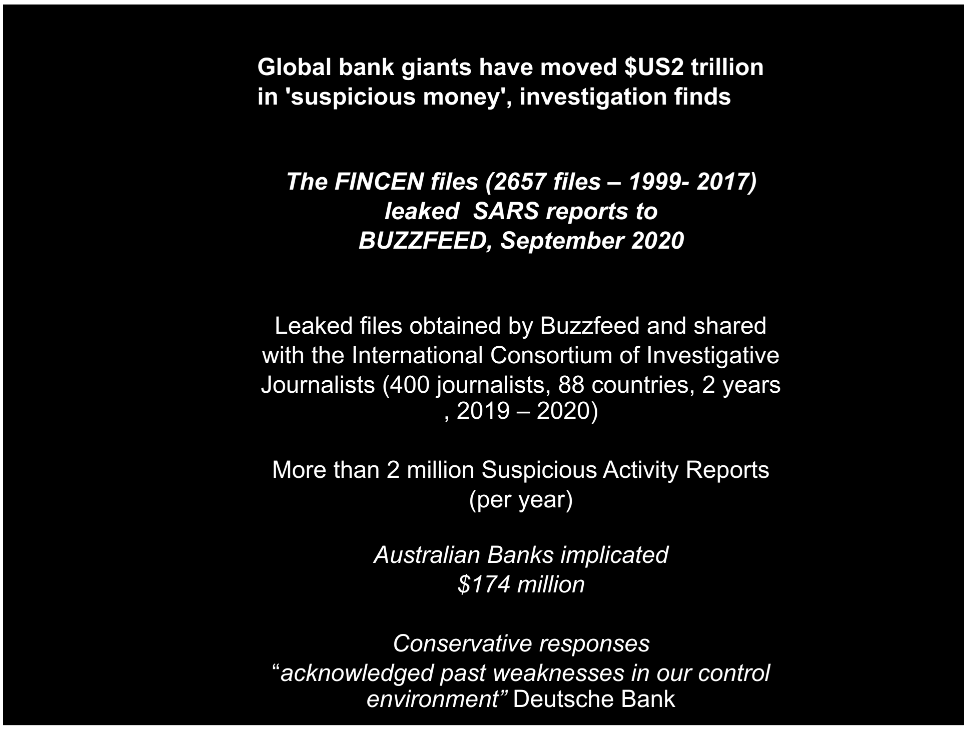
Classification Evaluation

Identification

Asset Management

Source: John O'Driscoll, CISO, Vic DPC.

11



Global bank giants have moved $US2 trillion in 'suspicious money', investigation finds

The FINCEN files (2657 files – 1999- 2017) leaked SARS reports to BUZZFEED, September 2020

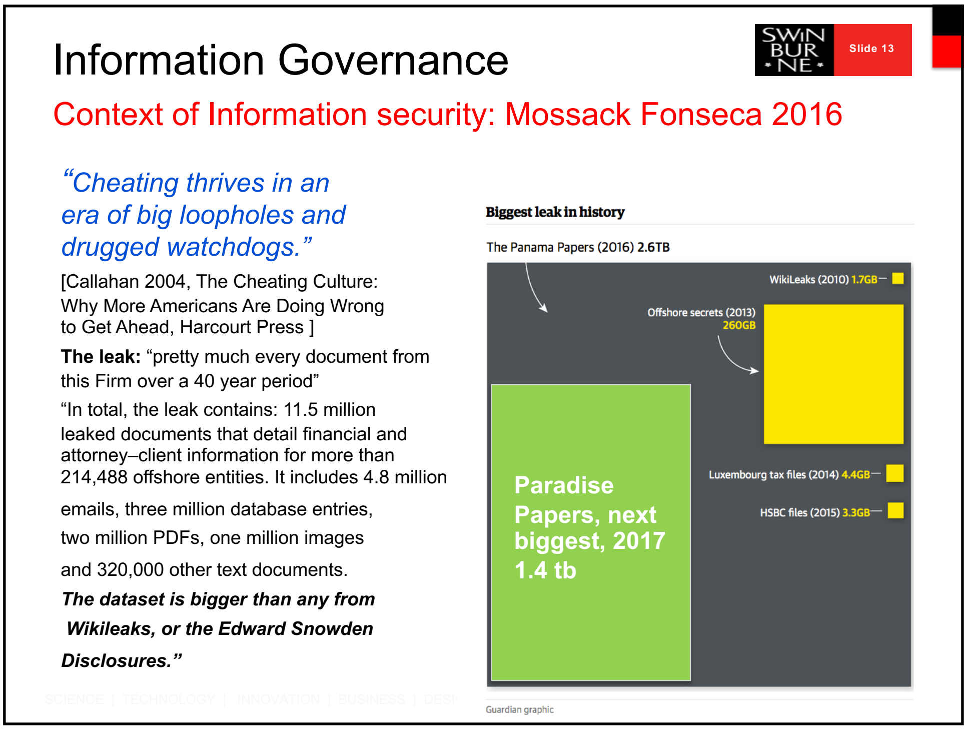
Leaked files obtained by Buzzfeed and shared with the International Consortium of Investigative Journalists (400 journalists, 88 countries, 2 years , 2019 – 2020)

More than 2 million Suspicious Activity Reports (per year)

Australian Banks implicated $174 million

Conservative responses
"acknowledged past weaknesses in our control environment" Deutsche Bank

12



Information Governance

Slide 13

Context of Information security: Mossack Fonseca 2016

"Cheating thrives in an era of big loopholes and drugged watchdogs."

[Callahan 2004, The Cheating Culture: Why More Americans Are Doing Wrong to Get Ahead, Harcourt Press]

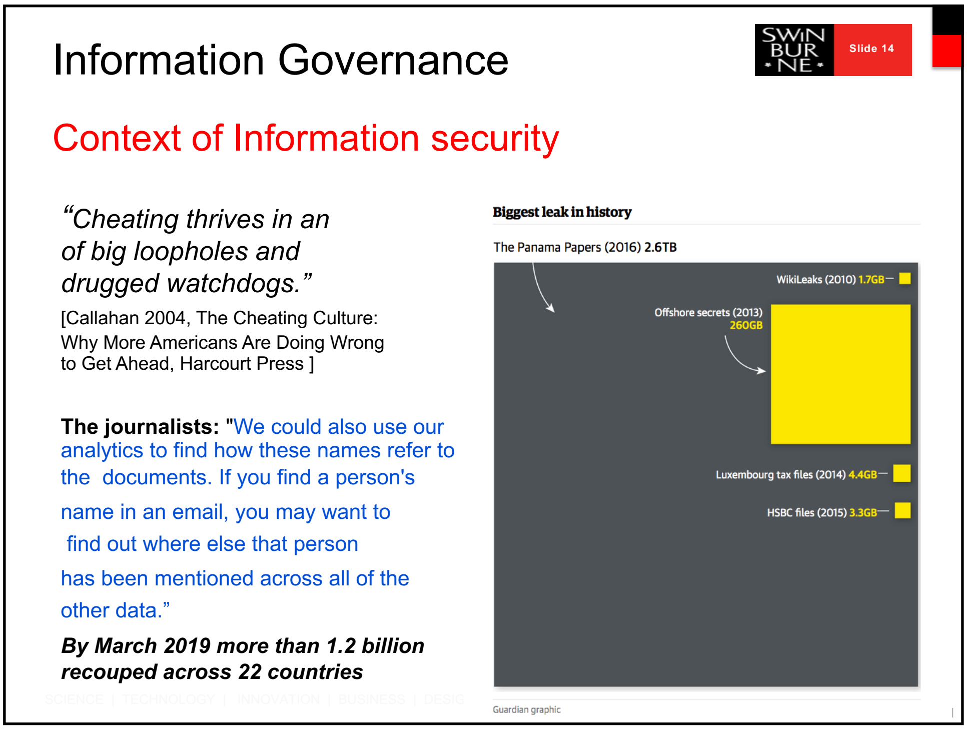
The leak: "pretty much every document from this Firm over a 40 year period"

"In total, the leak contains: 11.5 million leaked documents that detail financial and attorney–client information for more than 214,488 offshore entities. It includes 4.8 million emails, three million database entries, two million PDFs, one million images and 320,000 other text documents. ***The dataset is bigger than any from Wikileaks, or the Edward Snowden Disclosures."***

Biggest leak in history
The Panama Papers (2016) 2.6TB
WikiLeaks (2010) 1.7GB
Offshore secrets (2013) 260GB
Luxembourg tax files (2014) 4.4GB
HSBC files (2015) 3.3GB
Paradise Papers, next biggest, 2017 1.4 tb

Guardian graphic

13



Information Governance

Slide 14

Context of Information security

"Cheating thrives in an of big loopholes and drugged watchdogs."

[Callahan 2004, The Cheating Culture: Why More Americans Are Doing Wrong to Get Ahead, Harcourt Press]

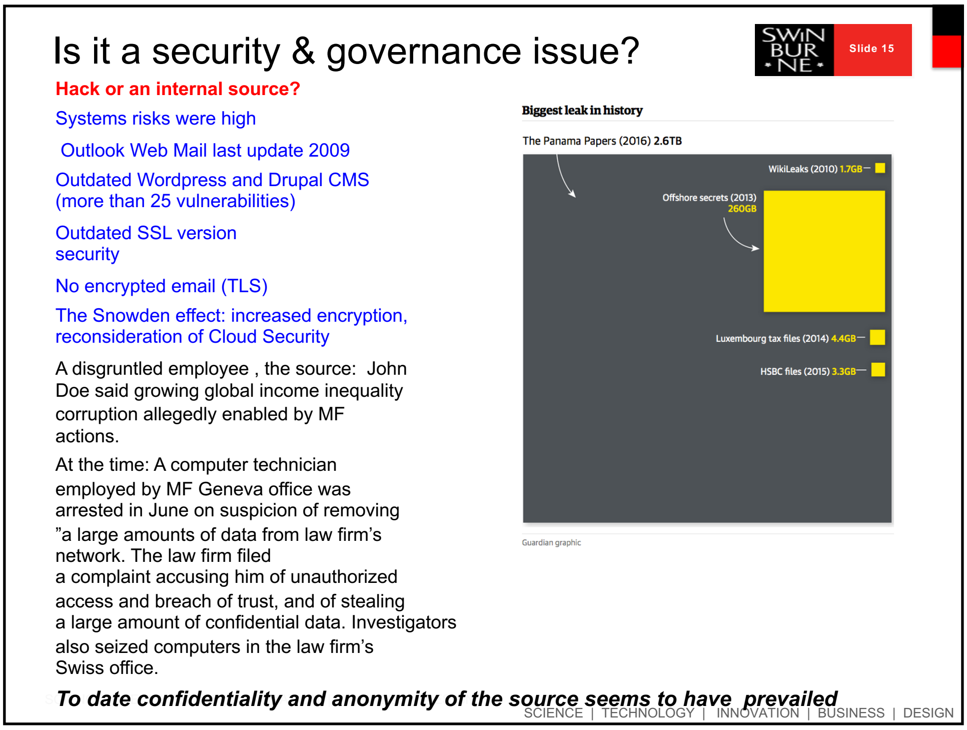
The journalists: "We could also use our analytics to find how these names refer to the documents. If you find a person's name in an email, you may want to find out where else that person has been mentioned across all of the other data."

By March 2019 more than 1.2 billion recouped across 22 countries

Biggest leak in history
The Panama Papers (2016) 2.6TB
WikiLeaks (2010) 1.7GB
Offshore secrets (2013) 260GB
Luxembourg tax files (2014) 4.4GB
HSBC files (2015) 3.3GB

Guardian graphic

14



Is it a security & governance issue?

Slide 15

Hack or an internal source?

Systems risks were high

Outlook Web Mail last update 2009

Outdated Wordpress and Drupal CMS (more than 25 vulnerabilities)

Outdated SSL version security

No encrypted email (TLS)

The Snowden effect: increased encryption, reconsideration of Cloud Security

A disgruntled employee , the source: John Doe said growing global income inequality corruption allegedly enabled by MF actions.

At the time: A computer technician employed by MF Geneva office was arrested in June on suspicion of removing ”a large amounts of data from law firm’s network. The law firm filed a complaint accusing him of unauthorized access and breach of trust, and of stealing a large amount of confidential data. Investigators also seized computers in the law firm’s Swiss office.

Biggest leak in history

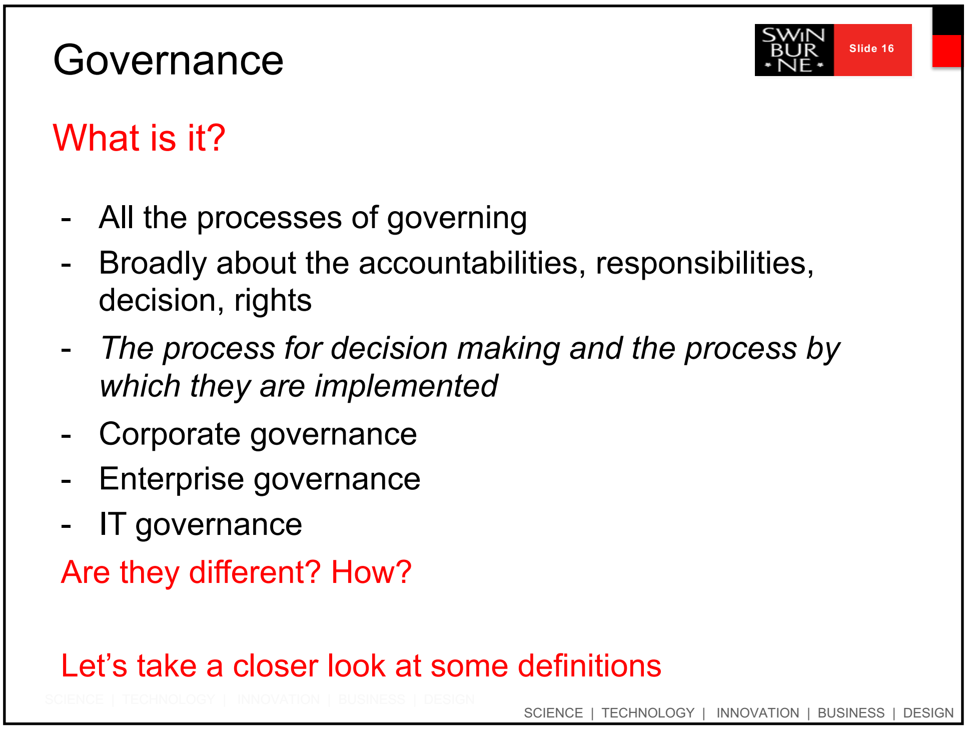
The Panama Papers (2016) 2.6TB
WikiLeaks (2010) 1.7GB
Offshore secrets (2013) 260GB
Luxembourg tax files (2014) 4.4GB
HSBC files (2015) 3.3GB

Guardian graphic

To date confidentiality and anonymity of the source seems to have prevailed

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

15



Governance

Slide 16

What is it?

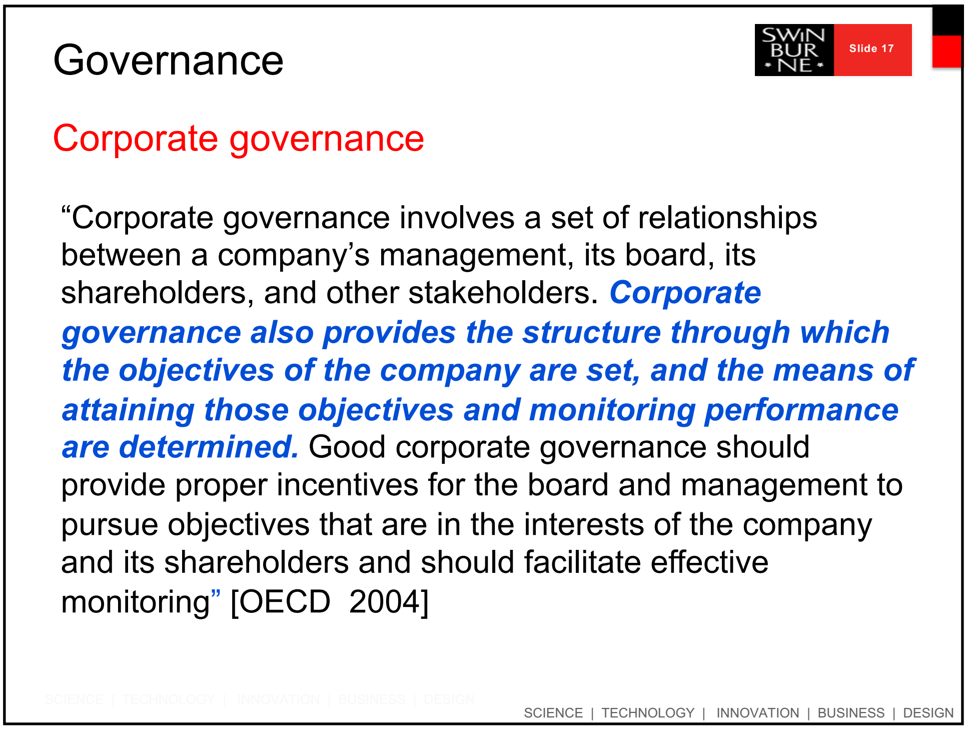
- All the processes of governing
- Broadly about the accountabilities, responsibilities, decision, rights
- *The process for decision making and the process by which they are implemented*
- Corporate governance
- Enterprise governance
- IT governance

Are they different? How?

Let’s take a closer look at some definitions

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

16



Governance

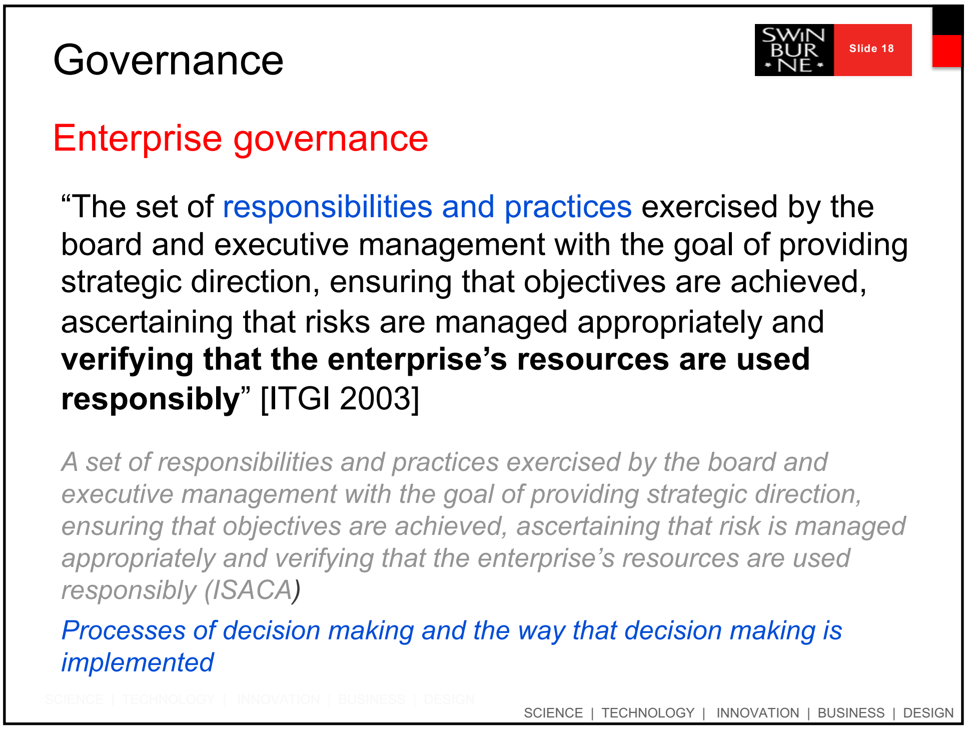
Slide 17

Corporate governance

"Corporate governance involves a set of relationships between a company's management, its board, its shareholders, and other stakeholders. ***Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined.*** Good corporate governance should provide proper incentives for the board and management to pursue objectives that are in the interests of the company and its shareholders and should facilitate effective monitoring" [OECD 2004]

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

17



Governance

Slide 18

Enterprise governance

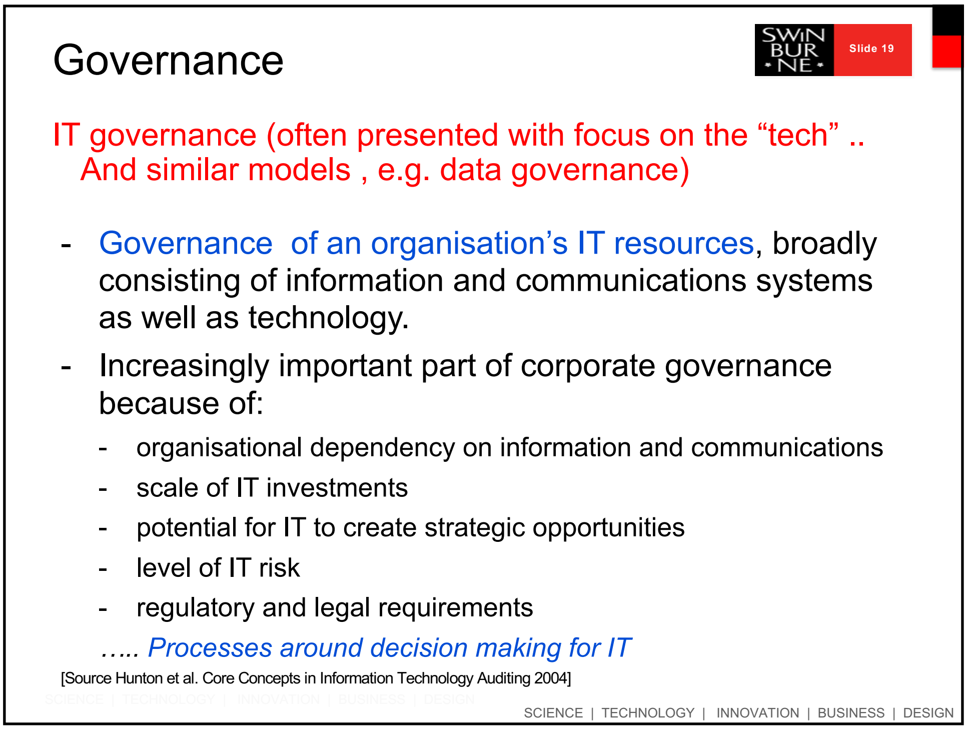
"The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and **verifying that the enterprise's resources are used responsibly**" [ITGI 2003]

A set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risk is managed appropriately and verifying that the enterprise's resources are used responsibly (ISACA)

Processes of decision making and the way that decision making is implemented

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

18



Governance

Slide 19

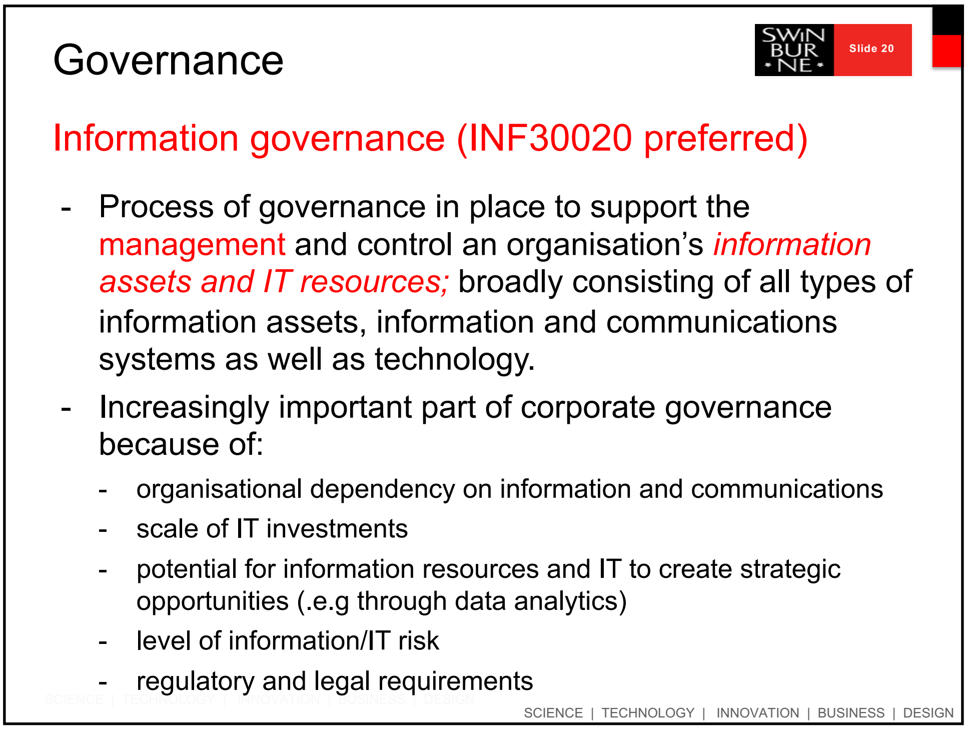
IT governance (often presented with focus on the “tech” .. And similar models , e.g. data governance)

- Governance of an organisation’s IT resources, broadly consisting of information and communications systems as well as technology.
- Increasingly important part of corporate governance because of:
  - organisational dependency on information and communications
  - scale of IT investments
  - potential for IT to create strategic opportunities
  - level of IT risk
  - regulatory and legal requirements

….. *Processes around decision making for IT*

[Source Hunton et al. Core Concepts in Information Technology Auditing 2004]

19



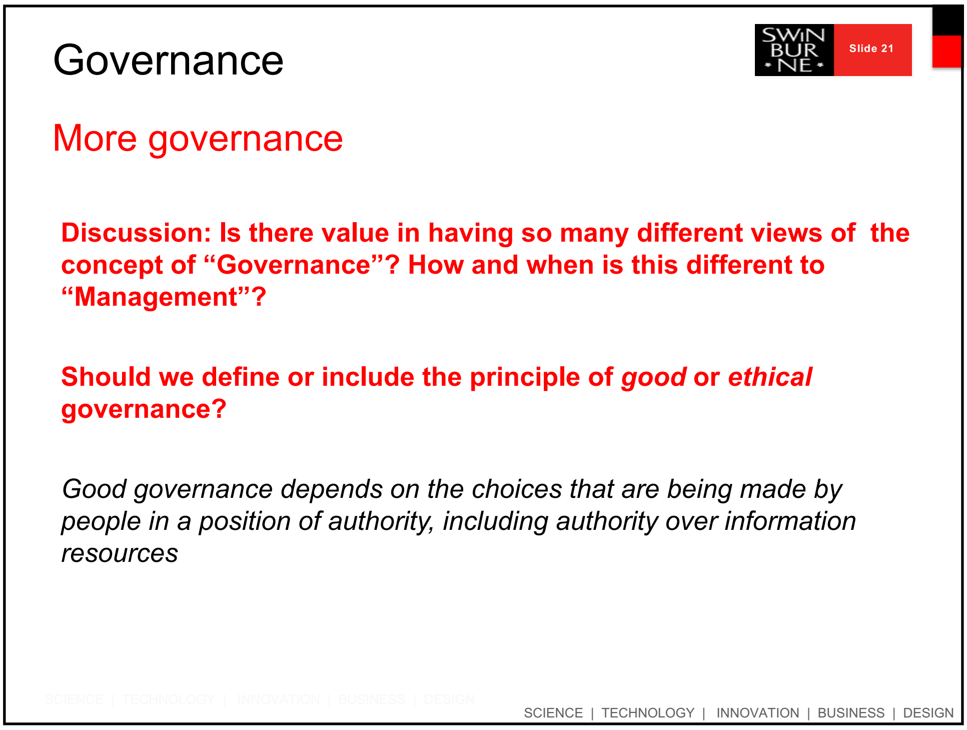
Governance

Slide 20

Information governance (INF30020 preferred)

- Process of governance in place to support the management and control an organisation’s *information assets and IT resources;* broadly consisting of all types of information assets, information and communications systems as well as technology.
- Increasingly important part of corporate governance because of:
  - organisational dependency on information and communications
  - scale of IT investments
  - potential for information resources and IT to create strategic opportunities (.e.g through data analytics)
  - level of information/IT risk
  - regulatory and legal requirements

20



Governance

Slide 21

More governance

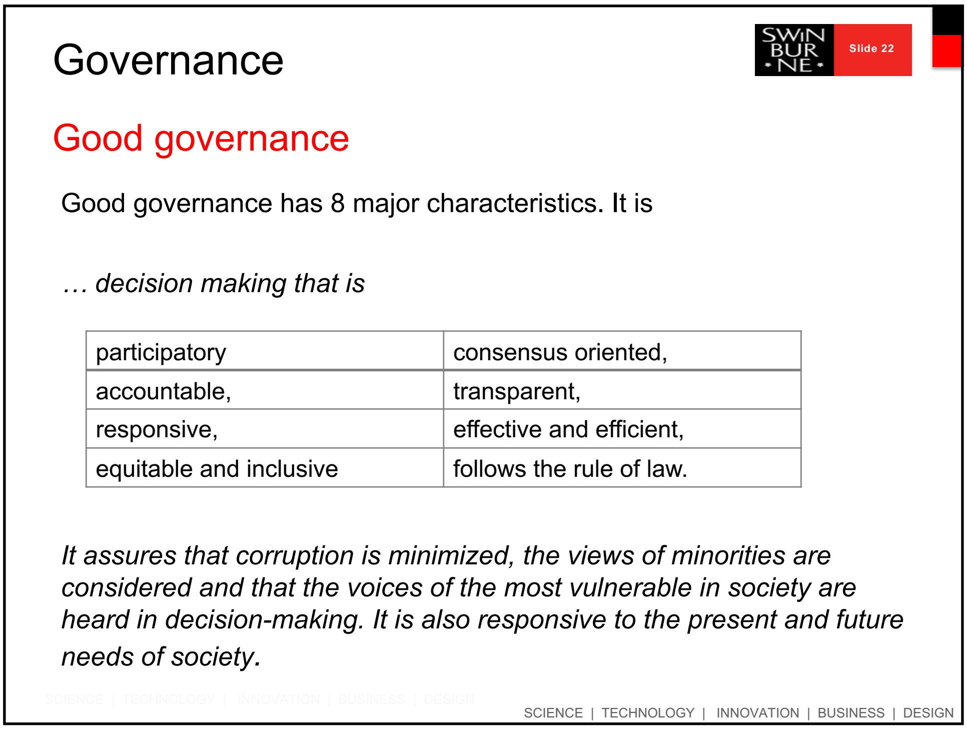
Discussion: Is there value in having so many different views of the concept of "Governance"? How and when is this different to "Management"?

Should we define or include the principle of *good* or *ethical* governance?

Good governance depends on the choices that are being made by people in a position of authority, including authority over information resources

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

21



Governance

Slide 22

Good governance

Good governance has 8 major characteristics. It is

… decision making that is

participatory	consensus oriented,
accountable,	transparent,
responsive,	effective and efficient,
equitable and inclusive	follows the rule of law.

It assures that corruption is minimized, the views of minorities are considered and that the voices of the most vulnerable in society are heard in decision-making. It is also responsive to the present and future needs of society.

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

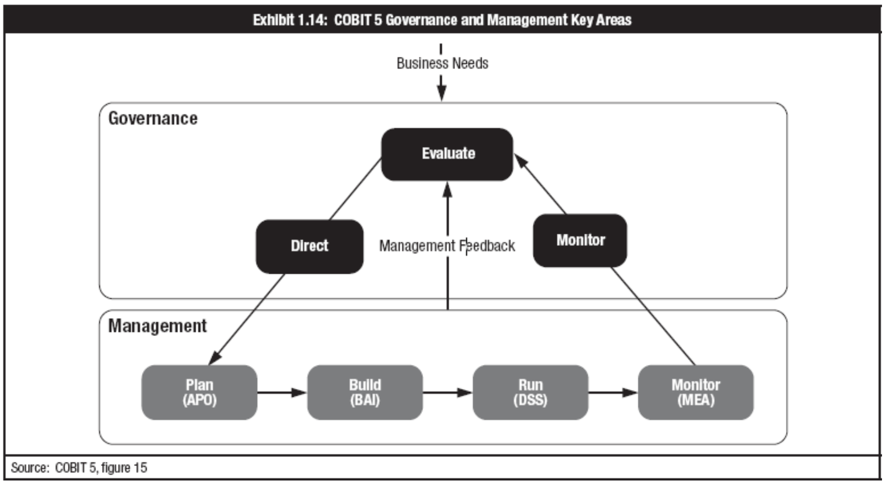
22

Governance

Slide 23

Is there a difference between *governance* and *management*?

Exhibit 1.14: COBIT 5 Governance and Management Key Areas



Business Needs

Governance

Evaluate

Direct

Management Feedback

Monitor

Management

Plan (APO)

Build (BAI)

Run (DSS)

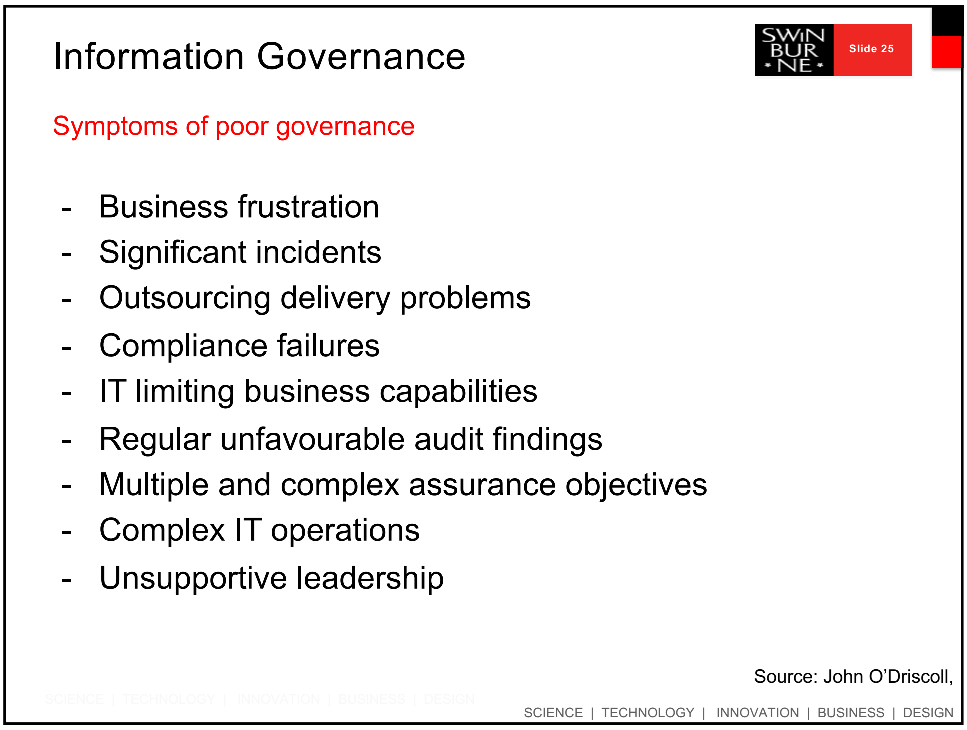
Monitor (MEA)

Source: COBIT 5, figure 15

Differences

- *Governance* refers to oversight and decision-making related to strategic direction, financial planning, bylaws and the set of core policies that outline the organization's purpose, values, and structure. **Governance decisions should provide guidelines about *how to go about business* for management.**

- *Management* refers to the routine decisions and administrative work related to the daily operations of the organization. **Management decisions should support or implement goals and values defined by governing bodies (such as the Board of Directors) and documents (such as the bylaws).**



Information Governance

Slide 25

Symptoms of poor governance

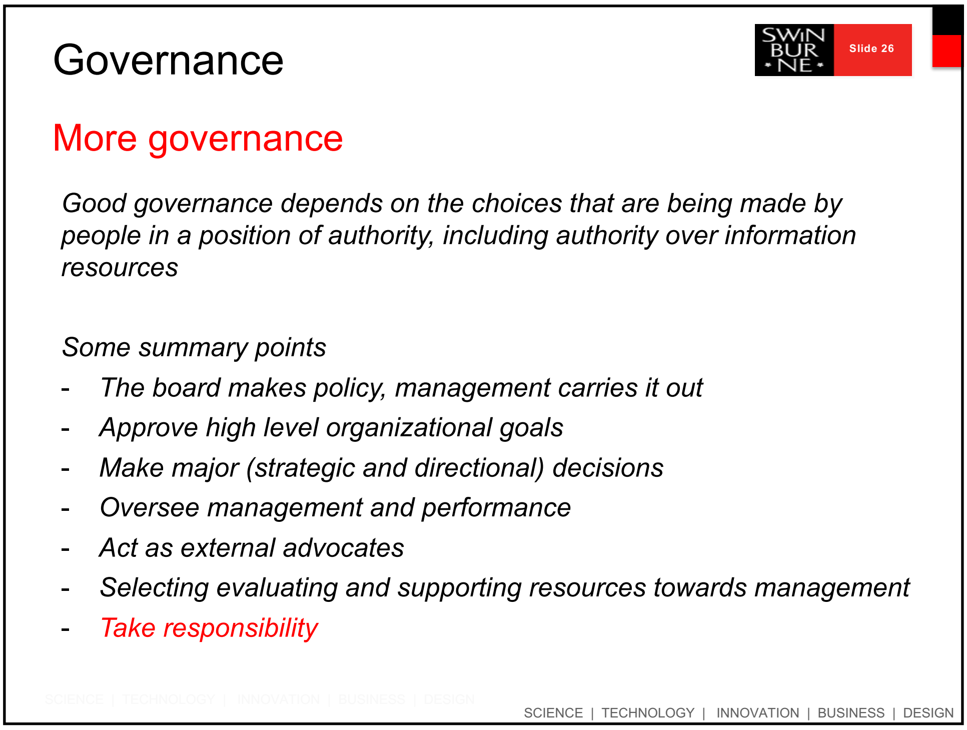
- Business frustration
- Significant incidents
- Outsourcing delivery problems
- Compliance failures
- IT limiting business capabilities
- Regular unfavourable audit findings
- Multiple and complex assurance objectives
- Complex IT operations
- Unsupportive leadership

Source: John O'Driscoll,

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

25



Governance

Slide 26

More governance

Good governance depends on the choices that are being made by people in a position of authority, including authority over information resources

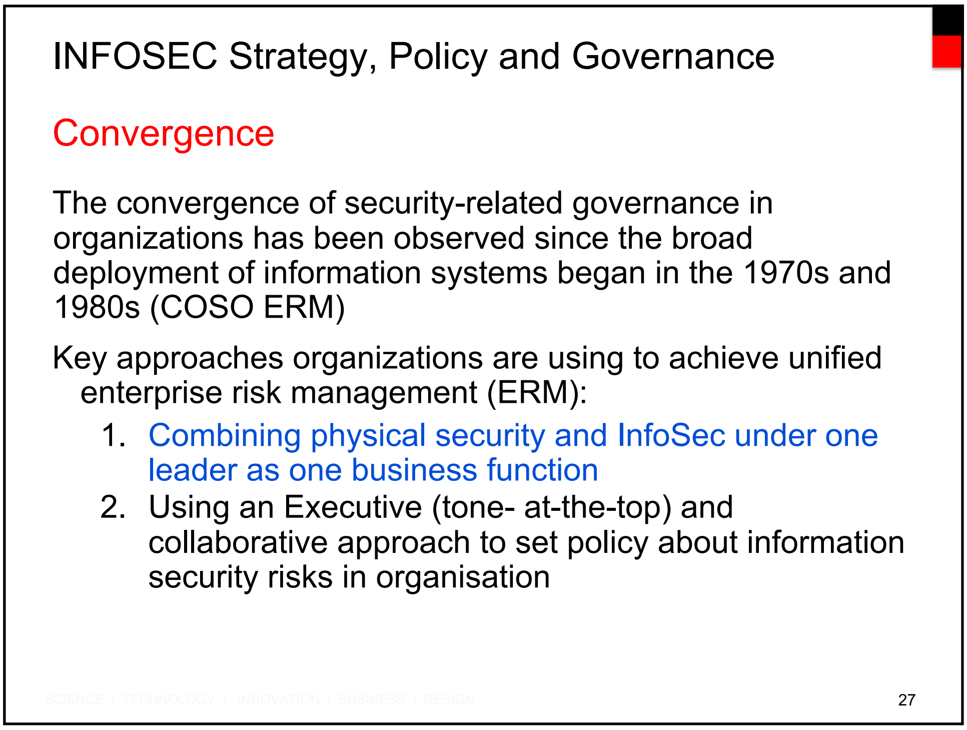
Some summary points

- *The board makes policy, management carries it out*
- *Approve high level organizational goals*
- *Make major (strategic and directional) decisions*
- *Oversee management and performance*
- *Act as external advocates*
- *Selecting evaluating and supporting resources towards management*
- *Take responsibility*

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

26



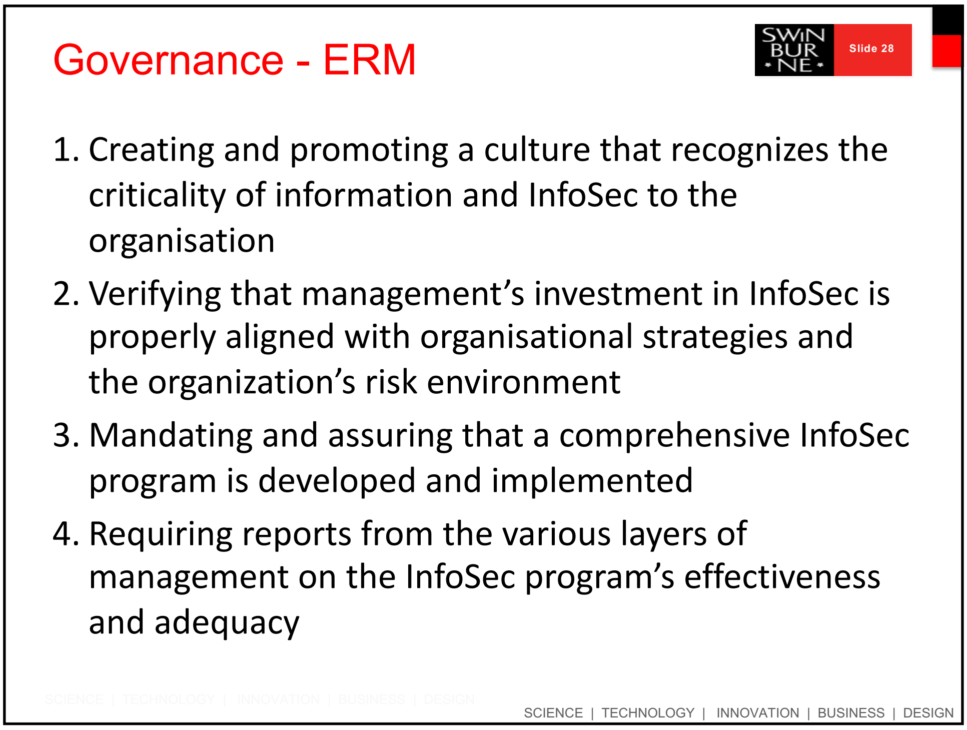
INFOSEC Strategy, Policy and Governance

Convergence

The convergence of security-related governance in organizations has been observed since the broad deployment of information systems began in the 1970s and 1980s (COSO ERM)

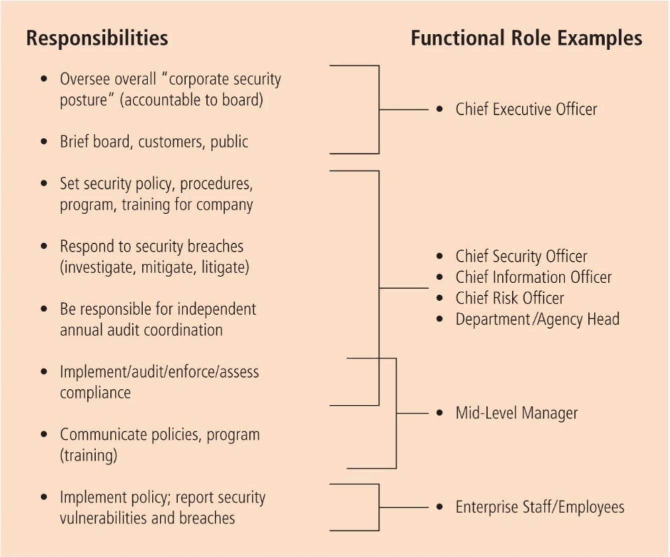
Key approaches organizations are using to achieve unified enterprise risk management (ERM):

1. Combining physical security and InfoSec under one leader as one business function
2. Using an Executive (tone- at-the-top) and collaborative approach to set policy about information security risks in organisation



Governance - ERM

1. Creating and promoting a culture that recognizes the criticality of information and InfoSec to the organisation
2. Verifying that management's investment in InfoSec is properly aligned with organisational strategies and the organization's risk environment
3. Mandating and assuring that a comprehensive InfoSec program is developed and implemented
4. Requiring reports from the various layers of management on the InfoSec program's effectiveness and adequacy



Responsibilities

- Oversee overall "corporate security posture" (accountable to board)
- Brief board, customers, public
- Set security policy, procedures, program, training for company
- Respond to security breaches (investigate, mitigate, litigate)
- Be responsible for independent annual audit coordination
- Implement/audit/enforce/assess compliance
- Communicate policies, program (training)
- Implement policy; report security vulnerabilities and breaches

Functional Role Examples

- Chief Executive Officer
- Chief Security Officer
- Chief Information Officer
- Chief Risk Officer
- Department/Agency Head
- Mid-Level Manager
- Enterprise Staff/Employees

Figure 3-5 Information security governance responsibilities[10]

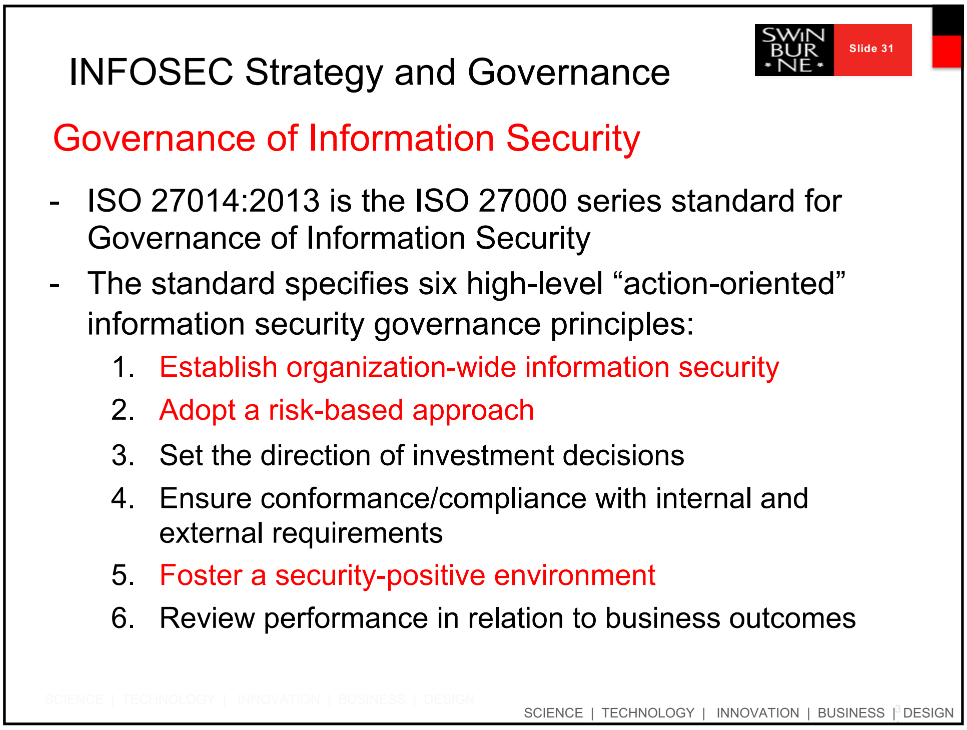
Source: IT Governance Institute.

Strategy, Governance & Management

Swinburne

Scope of IT Security Management

- The CIO and CISO roles include translating overall strategic planning into tactical and operational information security plans
- CISO usually reporting directly to the CIO or the Board. CIO charges the CISO and other IT department heads with creating and adopting plans that are consistent with and supportive of information governance & IT strategy aligned to organisational strategy
- CISO ensuring that the InfoSec plan directly supports the entire organization and the strategies of other business units, beyond the scope of the IT plan, and is implemented



Slide 31

INFOSEC Strategy and Governance

Governance of Information Security

- ISO 27014:2013 is the ISO 27000 series standard for Governance of Information Security
- The standard specifies six high-level “action-oriented” information security governance principles:
  1. Establish organization-wide information security
  2. Adopt a risk-based approach
  3. Set the direction of investment decisions
  4. Ensure conformance/compliance with internal and external requirements
  5. Foster a security-positive environment
  6. Review performance in relation to business outcomes

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

31

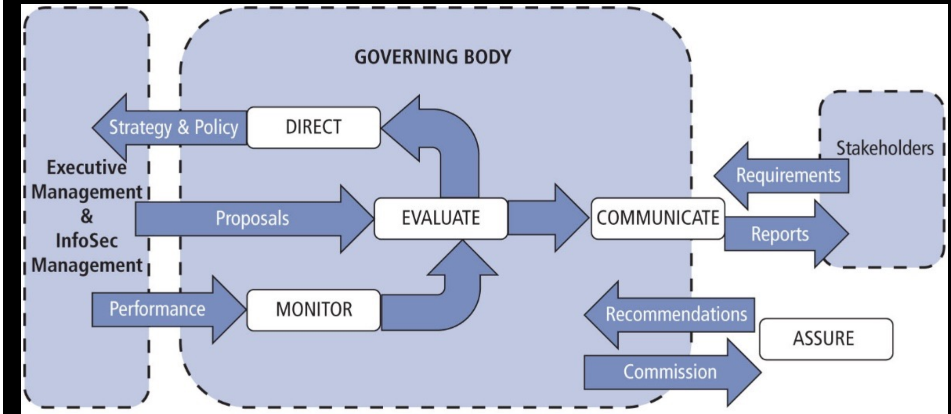
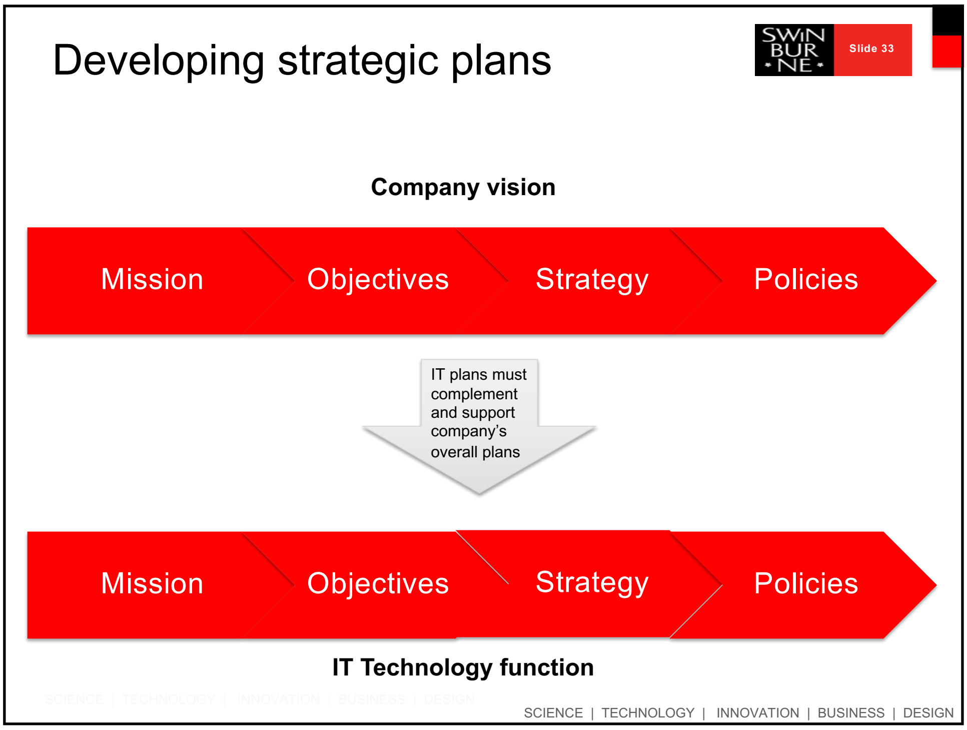


Figure 3-7 ISO/IEC 27014:2013 governance processes[19]

Source: R. Mahncke, Australian eHealth Informatics and Security Conference, December 2013.

32



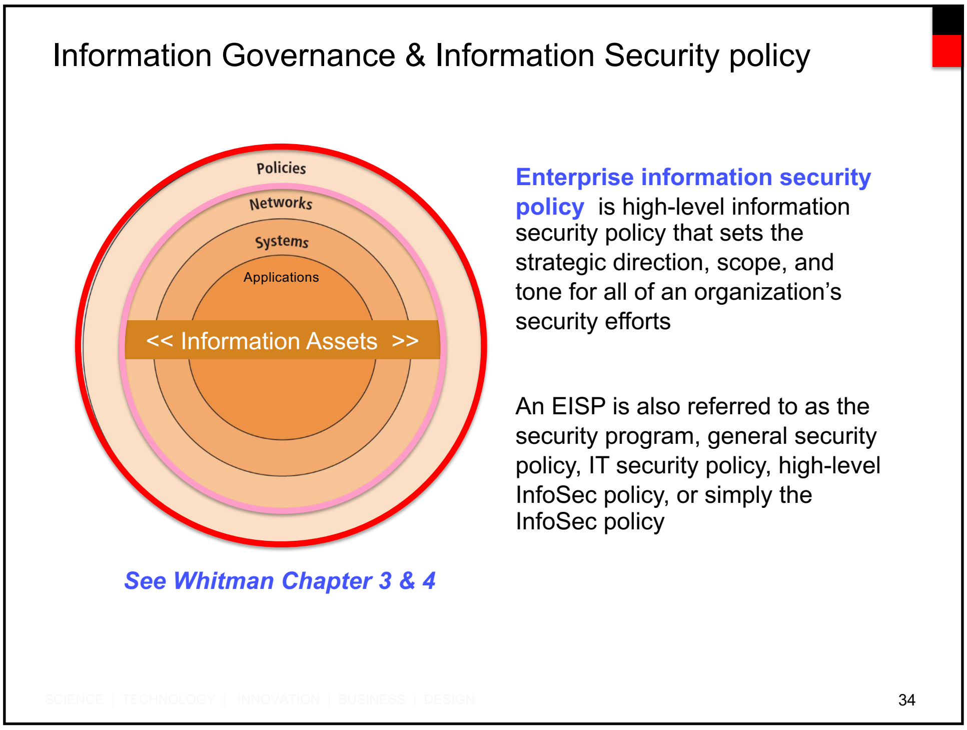
Developing strategic plans

Company vision

IT Technology function

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

33



Information Governance & Information Security policy

See Whitman Chapter 3 & 4

Enterprise information security policy is high-level information security policy that sets the strategic direction, scope, and tone for all of an organization's security efforts

An EISP is also referred to as the security program, general security policy, IT security policy, high-level InfoSec policy, or simply the InfoSec policy

34

34

1. State the purpose: importance of InfoSec to the organization’s mission and objectives
2. Set an overview structure of the InfoSec organization and individuals who fulfill the InfoSec role
3. Provide fully articulated responsibilities for security that are shared by all members of the organization

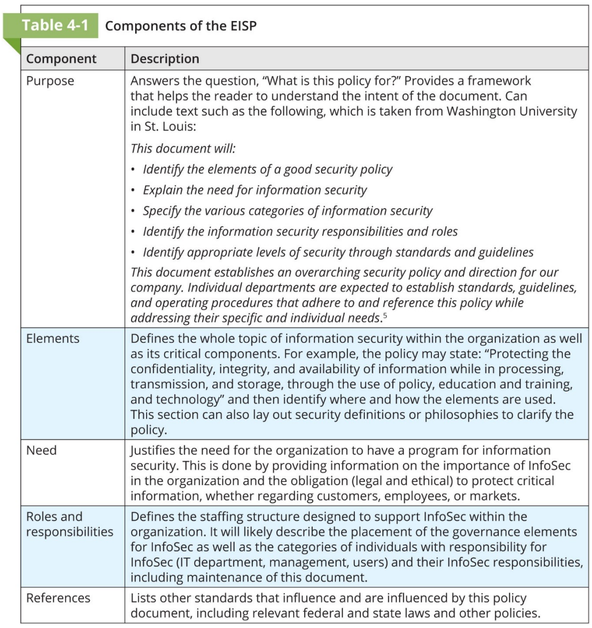


Table 4-1 Components of the EISP

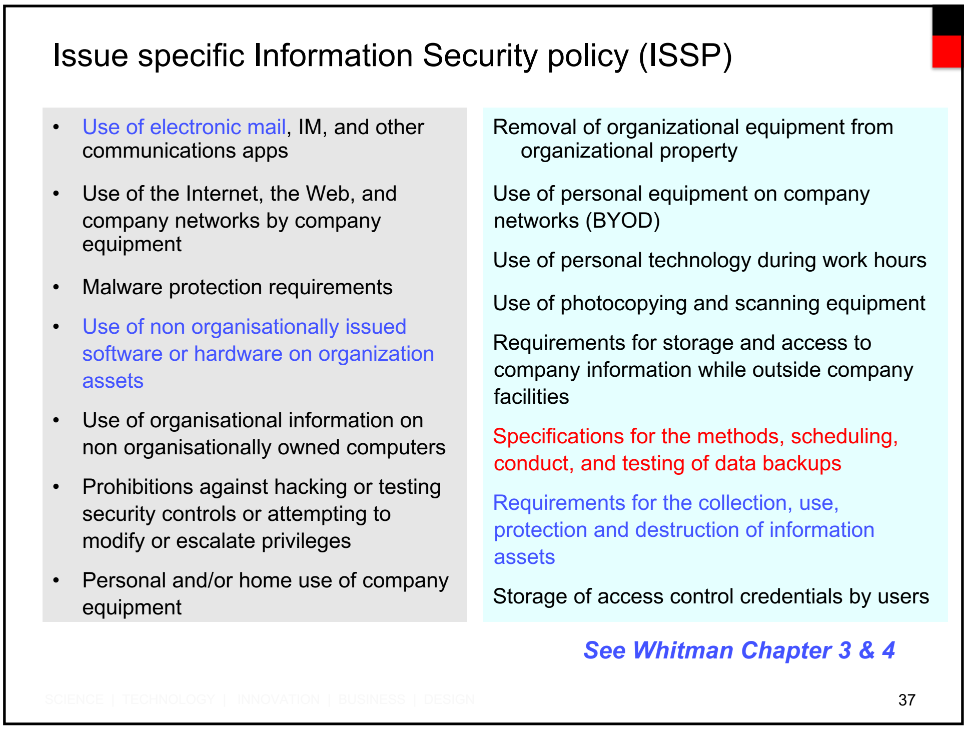
Component	Description
Purpose	Answers the question, “What is this policy for?” Provides a framework that helps the reader to understand the intent of the document. Can include text such as the following, which is taken from Washington University in St. Louis: *This document will:* • *Identify the elements of a good security policy* • *Explain the need for information security* • *Specify the various categories of information security* • *Identify the information security responsibilities and roles* • *Identify appropriate levels of security through standards and guidelines* *This document establishes an overarching security policy and direction for our company. Individual departments are expected to establish standards, guidelines, and operating procedures that adhere to and reference this policy while addressing their specific and individual needs.*[5]
Elements	Defines the whole topic of information security within the organization as well as its critical components. For example, the policy may state: “Protecting the confidentiality, integrity, and availability of information while in processing, transmission, and storage, through the use of policy, education and training, and technology” and then identify where and how the elements are used. This section can also lay out security definitions or philosophies to clarify the policy.
Need	Justifies the need for the organization to have a program for information security. This is done by providing information on the importance of InfoSec in the organization and the obligation (legal and ethical) to protect critical information, whether regarding customers, employees, or markets.
Roles and responsibilities	Defines the staffing structure designed to support InfoSec within the organization. It will likely describe the placement of the governance elements for InfoSec as well as the categories of individuals with responsibility for InfoSec (IT department, management, users) and their InfoSec responsibilities, including maintenance of this document.
References	Lists other standards that influence and are influenced by this policy document, including relevant federal and state laws and other policies.

EISP ***See Whitman Chapter 3 & 4***

Issue specific Information Security policy (ISSP)

- An organizational policy that provides detailed, targeted guidance to instruct all members of the organization in the use of a resources
  - ✓ *e.g. fair and responsible use policies, BYOD policies,*
- Every organization’s ISSPs should:
  - ✓ Address specific technology-based systems
  - ✓ Require frequent updates
  - ✓ Contain a statement on the organization’s position on an issue

See Whitman Chapter 3 & 4



Issue specific Information Security policy (ISSP)

- Use of electronic mail, IM, and other communications apps
- Use of the Internet, the Web, and company networks by company equipment
- Malware protection requirements
- Use of non organisationally issued software or hardware on organization assets
- Use of organisational information on non organisationally owned computers
- Prohibitions against hacking or testing security controls or attempting to modify or escalate privileges
- Personal and/or home use of company equipment

Removal of organizational equipment from organizational property

Use of personal equipment on company networks (BYOD)

Use of personal technology during work hours

Use of photocopying and scanning equipment

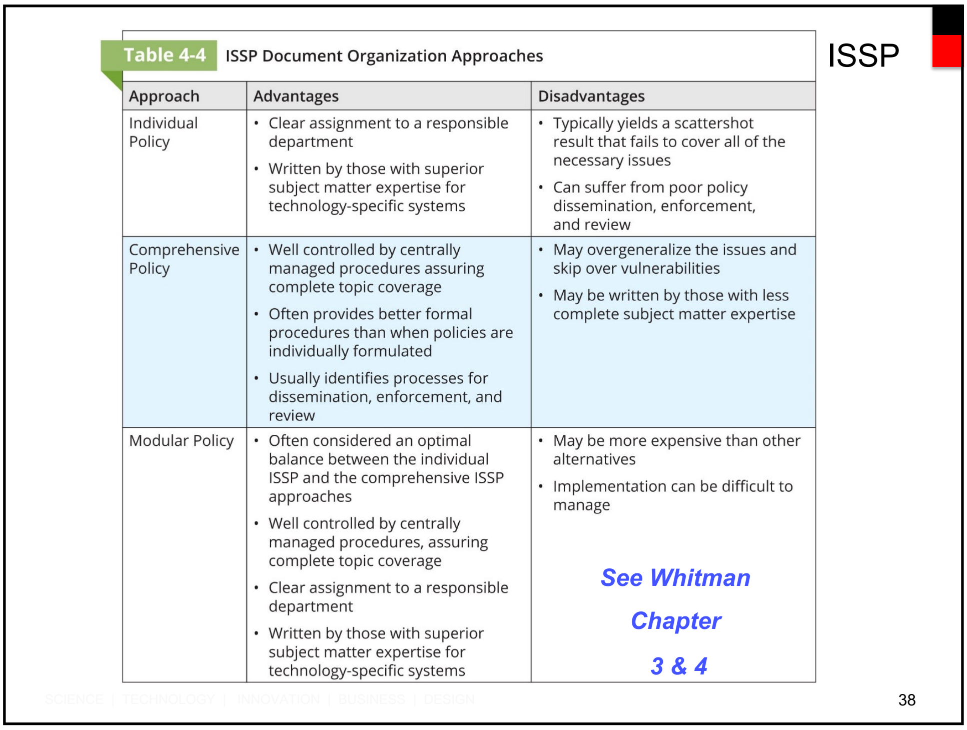
Requirements for storage and access to company information while outside company facilities

Specifications for the methods, scheduling, conduct, and testing of data backups

Requirements for the collection, use, protection and destruction of information assets

Storage of access control credentials by users

See Whitman Chapter 3 & 4

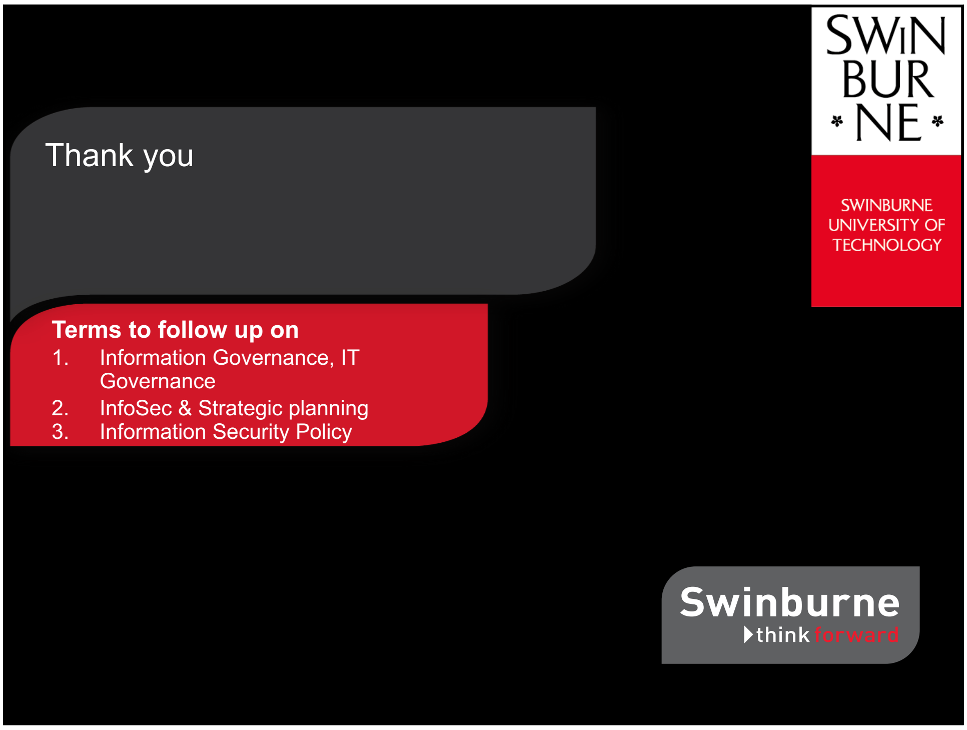


ISSP

Table 4-4 ISSP Document Organization Approaches

Approach	Advantages	Disadvantages
Individual Policy	• Clear assignment to a responsible department • Written by those with superior subject matter expertise for technology-specific systems	• Typically yields a scattershot result that fails to cover all of the necessary issues • Can suffer from poor policy dissemination, enforcement, and review
Comprehensive Policy	• Well controlled by centrally managed procedures assuring complete topic coverage • Often provides better formal procedures than when policies are individually formulated • Usually identifies processes for dissemination, enforcement, and review	• May overgeneralize the issues and skip over vulnerabilities • May be written by those with less complete subject matter expertise
Modular Policy	• Often considered an optimal balance between the individual ISSP and the comprehensive ISSP approaches • Well controlled by centrally managed procedures, assuring complete topic coverage • Clear assignment to a responsible department • Written by those with superior subject matter expertise for technology-specific systems	• May be more expensive than other alternatives • Implementation can be difficult to manage

See Whitman Chapter 3 & 4



Thank you

Terms to follow up on

1. Information Governance, IT Governance
2. InfoSec & Strategic planning
3. Information Security Policy

SWINBURNE UNIVERSITY OF TECHNOLOGY

Swinburne think forward