THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE

BISM3205: Business Information Security

Week 03: Planning for Security (Ch. 4)

Part 1: Security Governance Frameworks

Part 2: Three Lines of Defense vs. Five Lines of Assurance

Semester 1, 2023

THE UNIVERSITY OF QUEENSLAND AUSTRALIA | CREATE CHANGE

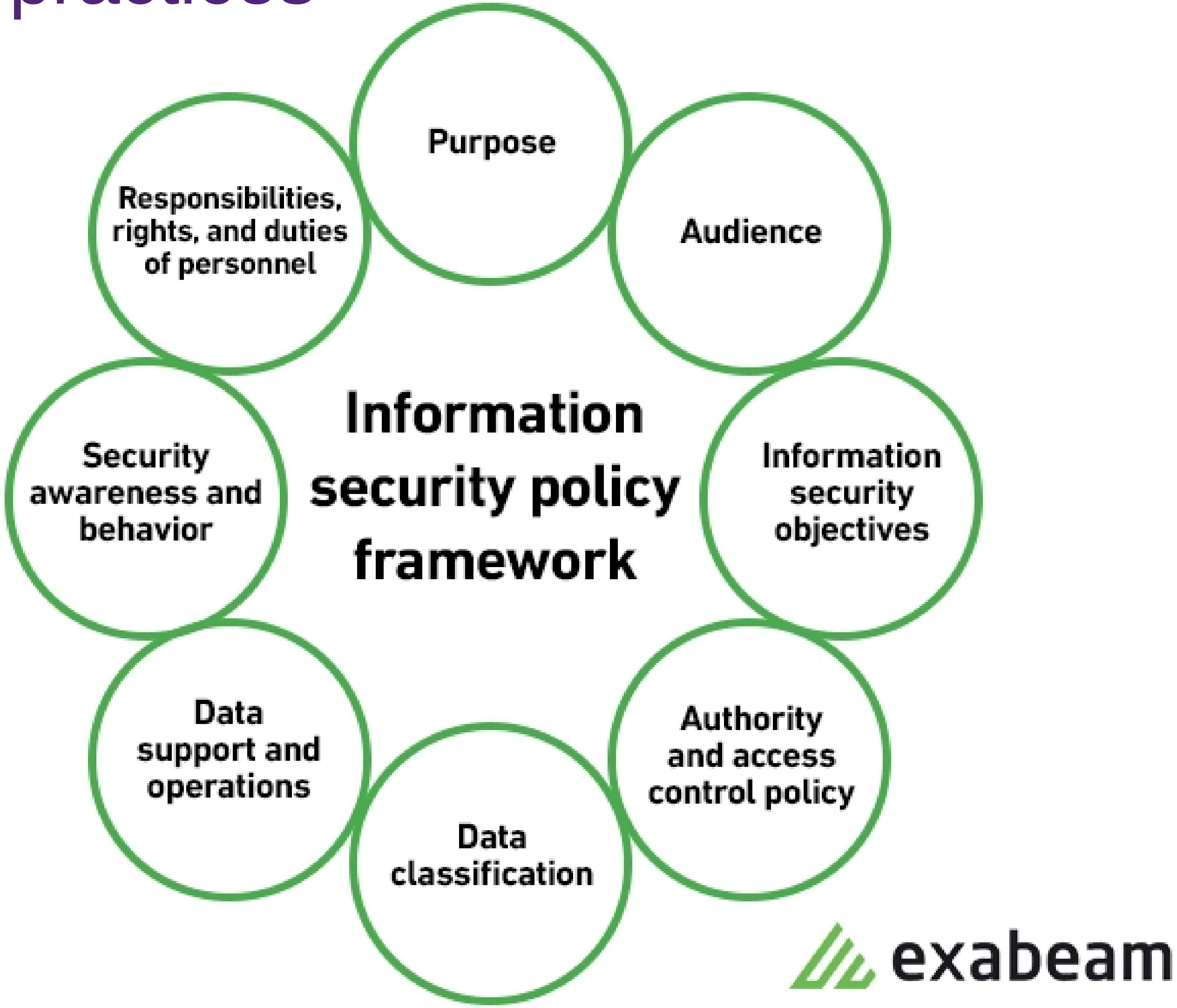
Part 1: Security Governance Frameworks

Policies produce standards and practices

- Policy is the fundamental start in information security

- It is the domain of senior management

- Senior management obviously has the power within the organisation, the capacity to apply proper resourcing, numbers of people, dollars invested in programmes etc.



Information security policy framework

Purpose

Audience

Information security objectives

Authority and access control policy

Data classification

Data support and operations

Security awareness and behavior

Responsibilities, rights, and duties of personnel

Information Security Planning and Governance

- Corporate governance is the set of processes, customs, laws and institutions which affect the way an organisation is directed, administered and controlled
- IT Governance is an integral part of CG and ensures the **effective** and **efficient** use of IT in **enabling** an organisation to achieve its goals.
- Security governance is the system by which security-related activities are directed and controlled
- IT governance and security governance are part of the higher corporate governance and security governance is not only part of IT governance but also corporate governance. The reason is that legal/regulatory dimensions also fall into the area of the broader corporate Governance
- Security is not just an IT issue. It affects every aspect of an organisation

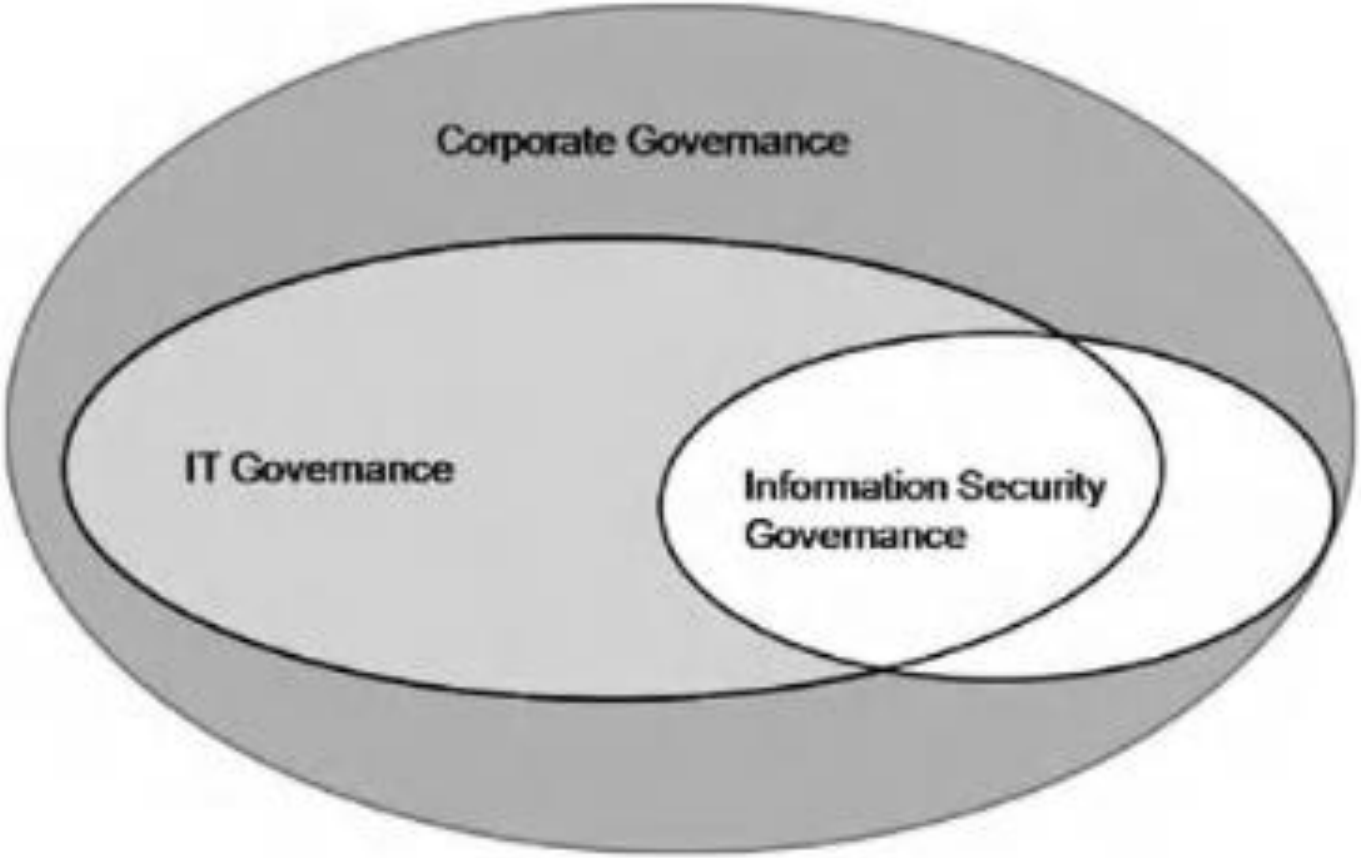


Image: NIST SP 800-100, Information Security Handbook

Five goals of Information Security Governance

- **Strategic alignment** – Information Systems Security should coordinate with business strategy, it needts to fit within it and support it
- **Risk management** – manage and mitigate risks (lecture next week)
- **Resource management** – using Information Systems Security knowledge and infrastructure effectively (personnel, time and money)
- **Performance measurement** – The enterprise needs metric against which to judge security policy to ensure that organisational objectives are achieved
- **Value delivery** – Resources expended on security should be constrained within overall enterprise resource objectives and security investments need to be managed to achieve optimum value

IT Governance Institute, *Information Security Governance Guidance for Boards of Directors and Executive Management*.

Security governance components (explained in detail on next slides)

1. Strategic planning
2. Organisational structure
3. Establishment of roles and responsibilities
4. Integration with the enterprise architecture
5. Documentation of security objectives in policies and guidance

NIST SP 800-100

1. Strategic planning

Enterprise strategic planning

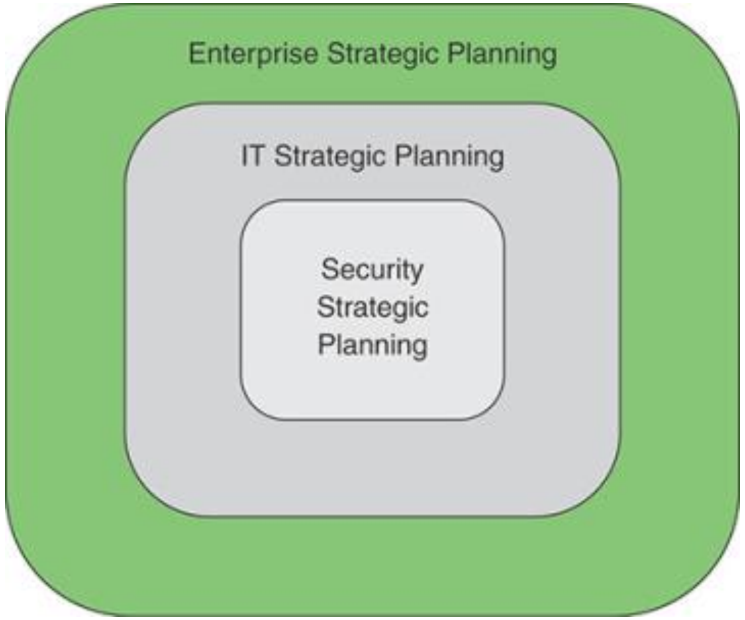
- Defining long-term goals for the organisation
- Development of strategic plan to achieve those goals

IT strategic planning

- Alignment of IT management and operation with enterprise strategig planning
- IT management guided by strategic planning to meet challenges (e.g., new technologies introducing new risks)

Security strategic planning

- Alignment of security management and operation with **both**
- IT‘s delivery of value to organisation includes risk mitigation



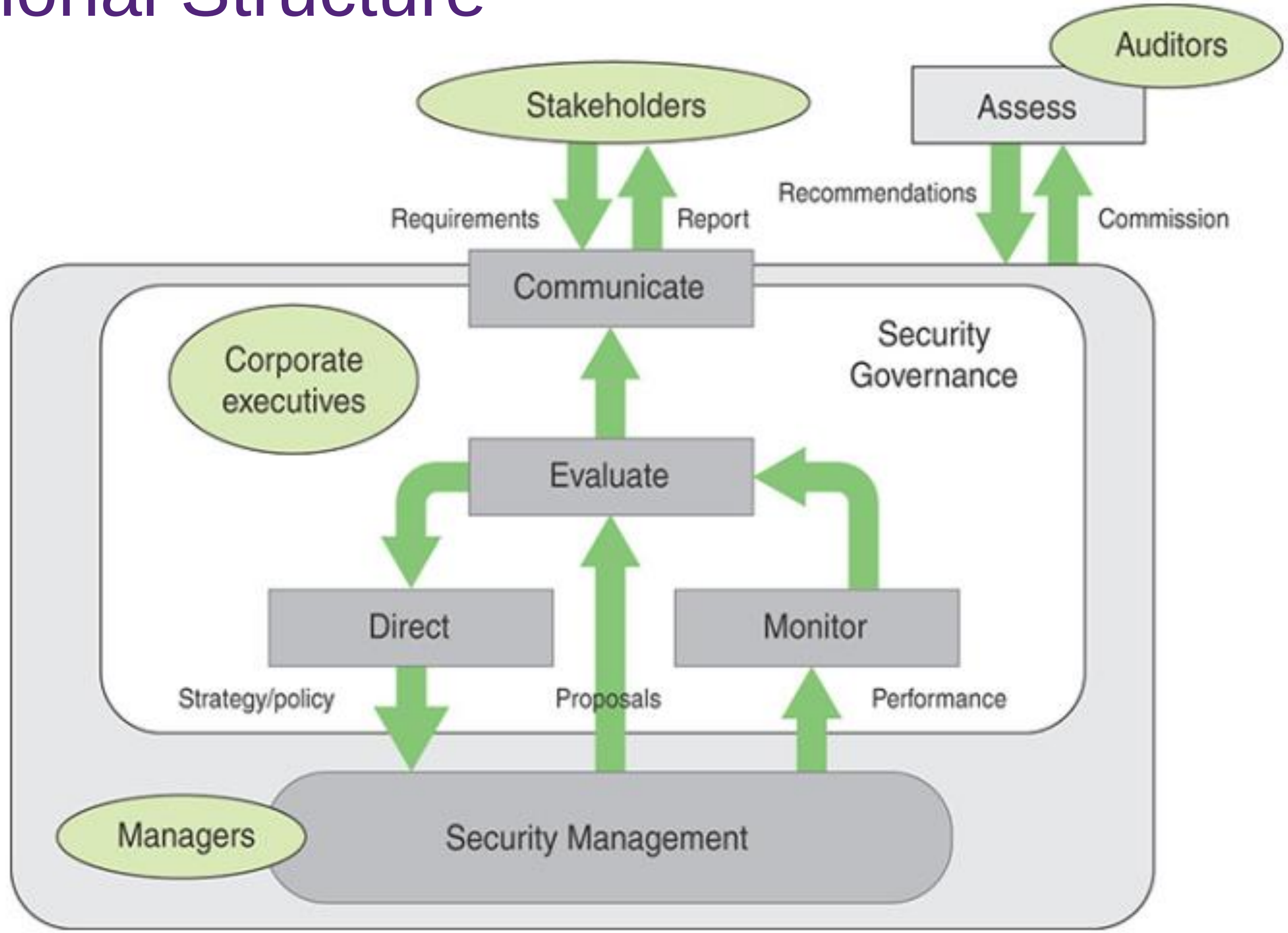
REMEMBER: security is a concern at all levels of an organisation’s governance and decision-making processes, and security strategic planning is an essential component of strategic planning.

https://www.informit.com/articles/article.aspx?p=2931571&seqNum=3

Example: Elements of a strategic plan document

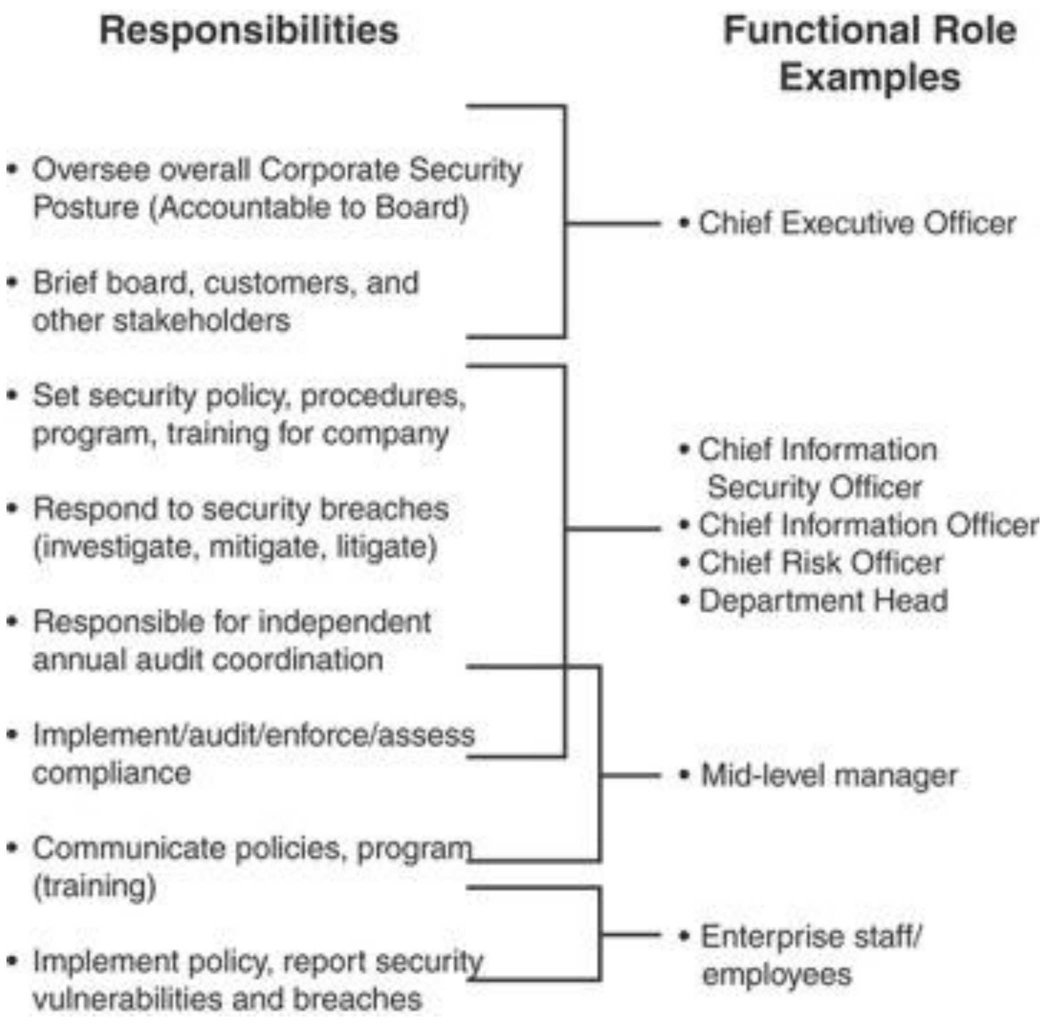
Section	Description
Definition	
Mission, vision, and objectives	Defines the strategy for aligning the information security program with organisational goals and objectives, including the role of individual security projects in enabling specific strategic initiatives.
Priorities	Describes factors that determine strategy and the priorities of objectives.
Success criteria	Defines success criteria for the information security program. Includes risk management, resilience, and protection against adverse business impacts.
Integration	Strategy for integrating the security program with the organisation’s business and IT strategy.
Threat defense	Describes how the security program will help the organisation defend against security threats.
Execution	
Operations plan	An annual plan to achieve agreed objectives that involves agreeing on budgets, resources, tools, policies, and initiatives. This plan (a) can be used for monitoring progress and communicating with stakeholders and (b) ensures that information security is included from the outset in each relevant project.
Monitoring plan	This plan involves planning and maintaining a stakeholder feedback loop, measuring progress against objectives, and ensuring that strategic objectives remain valid and in line with business needs.
Adjustment plan	This plan involves ensuring that strategic objectives remain valid and in line with business needs as well as procedures to communicate the value.
Review	
Review plan	This plan describes procedures and individuals/committees involved in regular review of the information security strategy.

2. Organisational Structure



ITU X.1054

3. Establishment of roles and responsibilities



Responsibilities

- Oversee overall Corporate Security Posture (Accountable to Board)
- Brief board, customers, and other stakeholders
- Set security policy, procedures, program, training for company
- Respond to security breaches (investigate, mitigate, litigate)
- 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 Information Security Officer
- Chief Information Officer
- Chief Risk Officer
- Department Head
- Mid-level manager
- Enterprise staff/ employees

- ❖ The responsibility for information security should also be placed at the manager level that is responsible for the business process.
- ❖ The responsibility for information security should ***not*** be placed at the *Information and Communications Technology (ICT)* department as they typically do not know all characteristics of the business processes!
- ❖ The *security officer* is ***not*** responsible for information security but making sure that others take on their responsibility

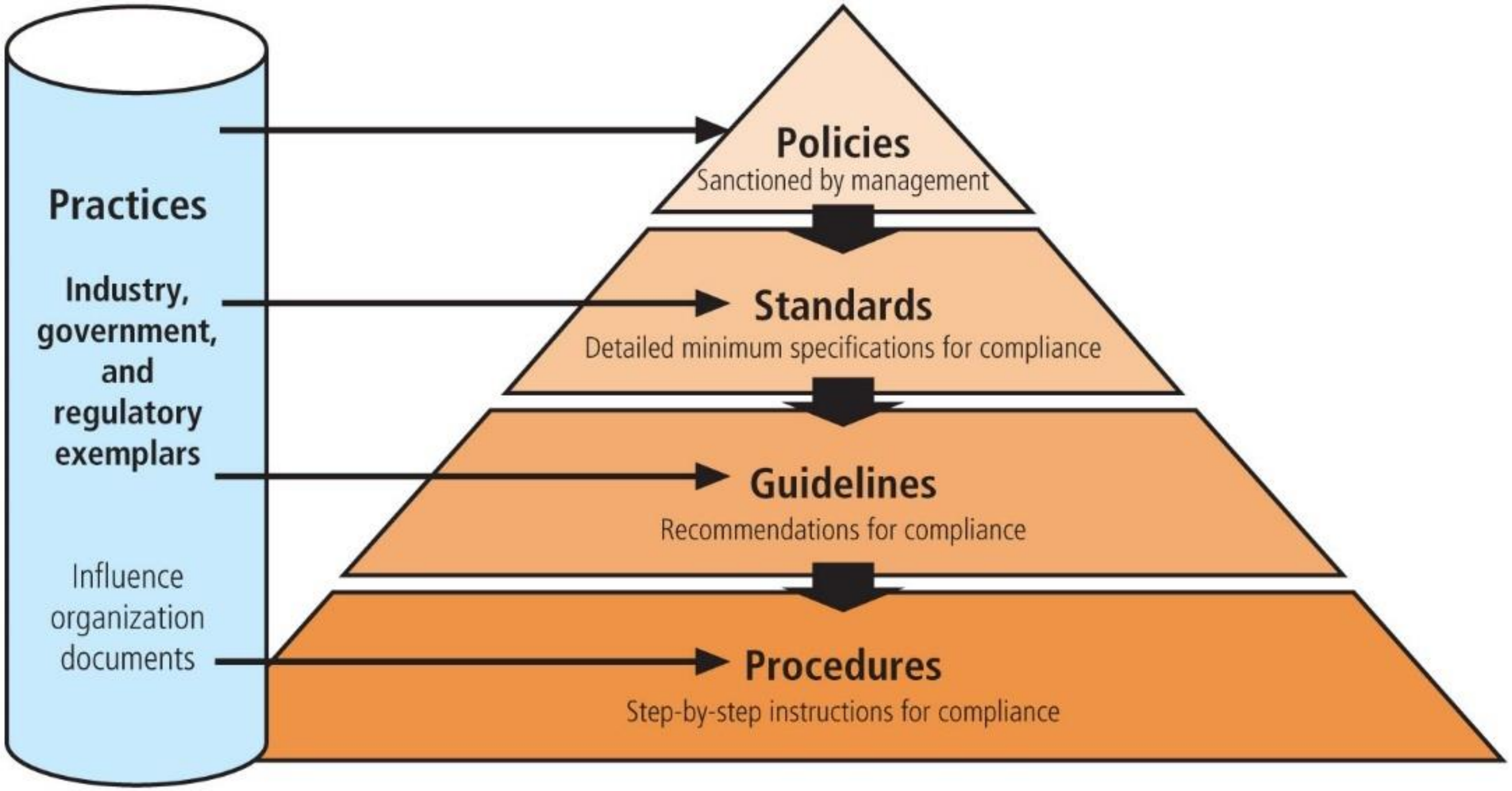
Source: Corporate Governance Task Force Report, "*Information Security Governance: A Call to Action*," April 2004, National Cyber Security Task Force.

4. Integration with the enterprise architecture: Information security policies, standards, and practices

- Communities of interest must consider **policies as the basis for all information security efforts**
- Policies direct how issues should be addressed and technologies used
- Policies should never contradict law
- Security policies are the least expensive controls to execute but most difficult to implement properly
- Shaping policy is difficult

- **Policy**: course of action used by organisation to convey instructions from management to those who perform duties
- **Standards**: more detailed statements of what must be done to comply with policy
- Practices, procedures, and guidelines effectively explain how to comply with policy
- **For a policy to be effective**, it must be properly disseminated, read, understood, and agreed to by all members in the organisation and uniformly enforced

Information security policies, standards, guidelines and procedures


Practices
Industry, government, and regulatory exemplars
Influence organization documents
Policies
Sanctioned by management
Standards
Detailed minimum specifications for compliance
Guidelines
Recommendations for compliance
Procedures
Step-by-step instructions for compliance

Information security policies, standards, and practices (examples)

- **Policy**: Employees must use strong passwords on their accounts. Passwords must be changed regularly and protected against disclosure

- **Standard**: (Provides specifics to help employees comply with policy) Password length – must include at least 1 lowercase, 1 upper case, one digit, one special character – not written down – changed every 90 days – not held on insecure media.

- **Practice**: US-CERT* recommends: 15 characters for admin accounts; use alphanumeric passwords and symbols; cannot reuse previous passwords; no personal information; minimum password length of 8 characters for standard users; - and more

- **Guidelines** (provide examples/recommendations): In order to create strong yet easy-to-remember passwords (NIST SP 800-118): Mnemonic Method; altered passphrases

*CERT = Computer Emergency Response Team. US-CERT is an agency within Department of Homeland Security. They offer best practices, advice to the broader community.

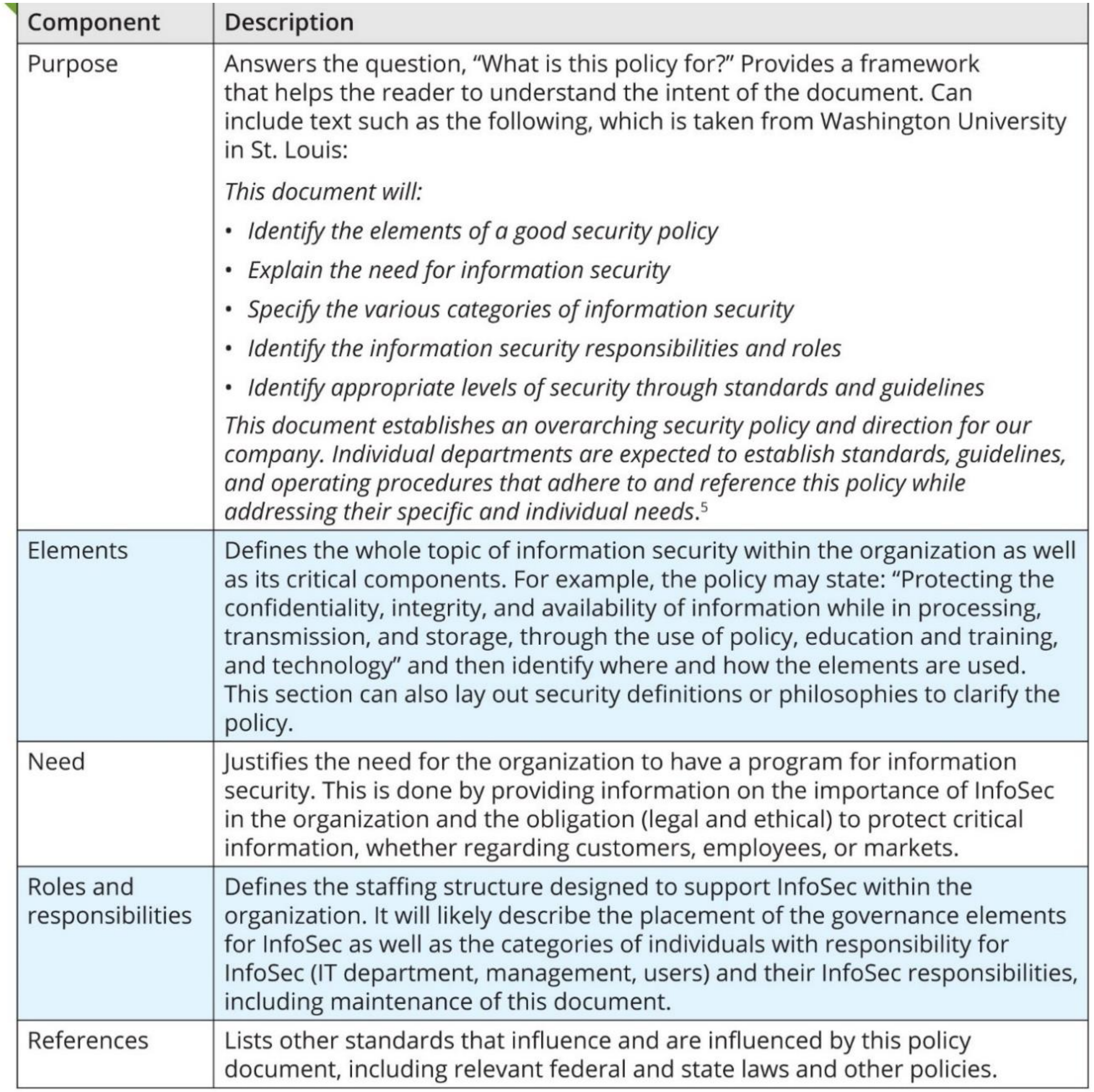
5. Documentation of security objectives in policies and guidance

Enterprise Information Security Policy (EISP)

- **Sets strategic direction, scope, and tone for all security efforts within the organisation**
- Executive-level document, usually drafted by or with CIO of the organisation
- Typically addresses compliance in two areas:
  - Ensure meeting requirements to establish program and responsibilities assigned therein to various organisational components
  - Use of specified penalties and disciplinary action for non-compliance

- **EISP elements:**
  - An **overview of the corporate philosophy** on security
  - Information on the **structure** of the information security organisation and **individuals** who fulfill the information security role
  - Fully **articulated responsibilities for security** that are **shared by all members** of the organisation (employees, contractors, consultants, partners, and visitors)
  - Fully **articulated responsibilities for security** that are **unique** to each role within the organisation

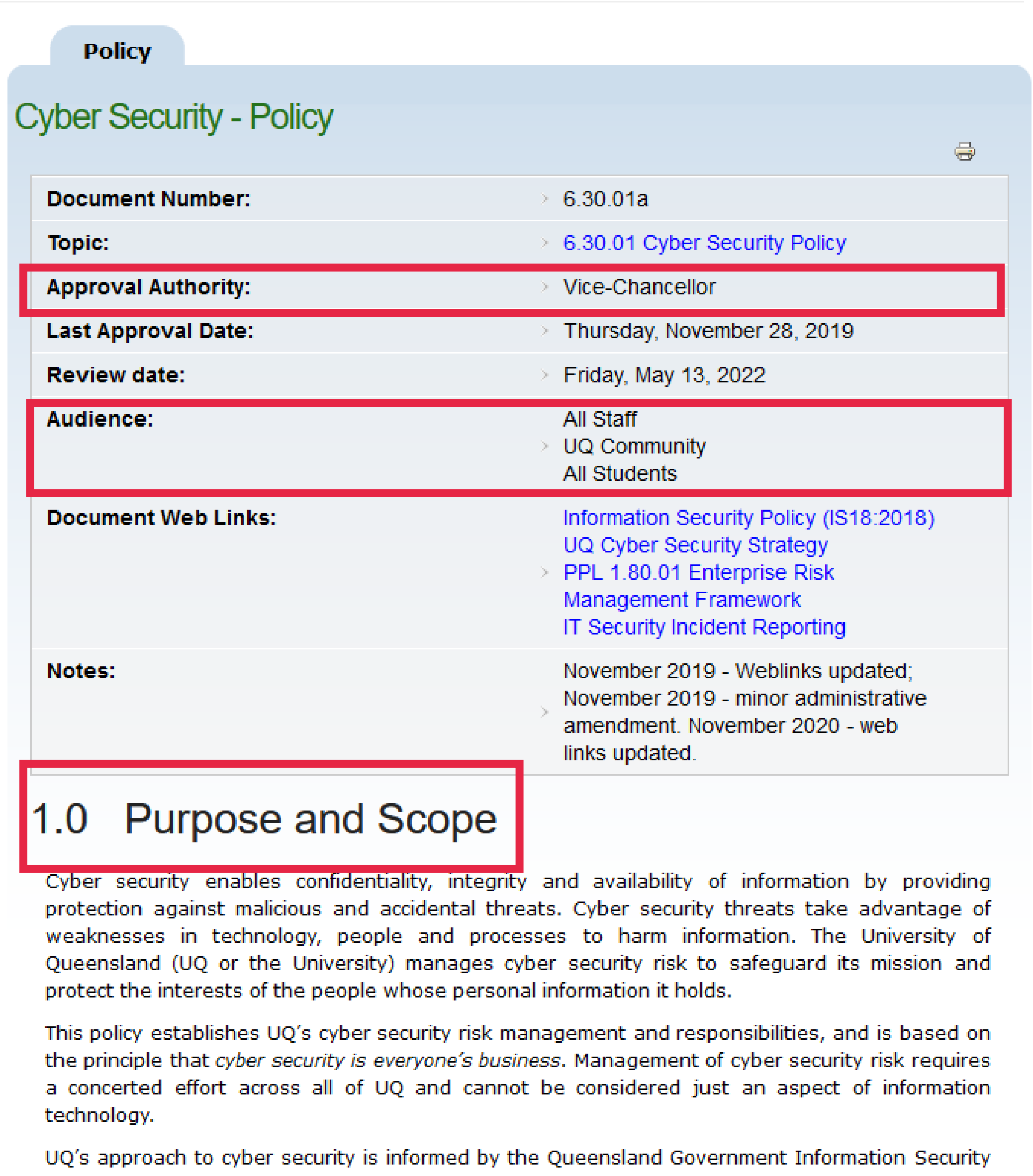
Components of the Enterprise Information Security Policy (EISP)



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.

Just an overview!

Example UQ



Policy

Cyber Security - Policy

Document Number:	6.30.01a
Topic:	6.30.01 Cyber Security Policy
Approval Authority:	Vice-Chancellor
Last Approval Date:	Thursday, November 28, 2019
Review date:	Friday, May 13, 2022
Audience:	All Staff UQ Community All Students
Document Web Links:	Information Security Policy (IS18:2018) UQ Cyber Security Strategy PPL 1.80.01 Enterprise Risk Management Framework IT Security Incident Reporting
Notes:	November 2019 - Weblinks updated; November 2019 - minor administrative amendment. November 2020 - web links updated.

1.0 Purpose and Scope

Cyber security enables confidentiality, integrity and availability of information by providing protection against malicious and accidental threats. Cyber security threats take advantage of weaknesses in technology, people and processes to harm information. The University of Queensland (UQ or the University) manages cyber security risk to safeguard its mission and protect the interests of the people whose personal information it holds.

This policy establishes UQ's cyber security risk management and responsibilities, and is based on the principle that *cyber security is everyone's business*. Management of cyber security risk requires a concerted effort across all of UQ and cannot be considered just an aspect of information technology.

UQ's approach to cyber security is informed by the Queensland Government Information Security

Enterprise Information Security Policy (EISP)

https://ppl.app.uq.edu.au/content/6.30.01-cyber-security-policy

Issue-Specific Security Policy (ISSP) (1/2)

- **Addresses specific areas of technology** (e.g., e-mail, Internet use, anti-malware configuration of computers)
- Requires frequent updates
- Contains statement on organisation’s position on specific issue

Three approaches when creating and managing ISSPs:

- Create a number of **independent ISSP documents**
- Create a **single comprehensive ISSP document**
- Create a **modular ISSP document**

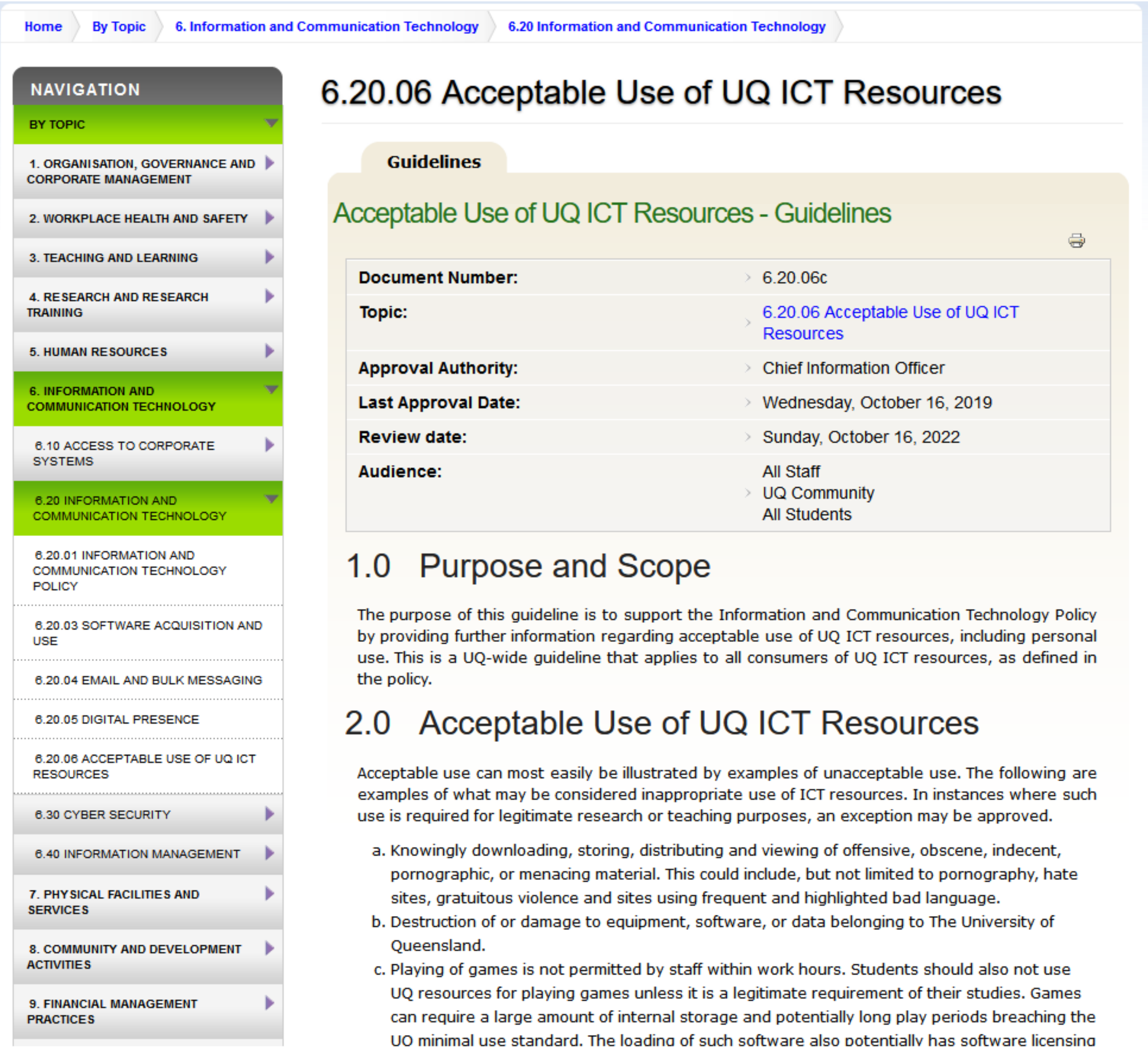
Issue-Specific Security Policy (ISSP) (2/2)

Components of the policy

- **Statement of Purpose** (scope, technology addressed, responsibilities)
- **Authorized Access and Usage of Equipment** (user access, fair/responsible use)
- **Prohibited Use of Equipmen**t (misuse, criminal, copyright, etc.)
- **Systems Management** (e.g. monitoring of employees – virus protection)
- **Violations of Policy** (procedures for reporting violations, penalties)
- **Policy Review and Modification**
- **Limitations of Liability** (cannot protect employees – may assist in prosecution)

Example UQ

Acceptable Use Policy at UQ



Home
By Topic
6. Information and Communication Technology
6.20 Information and Communication Technology
NAVIGATION
BY TOPIC
1. ORGANISATION, GOVERNANCE AND CORPORATE MANAGEMENT
2. WORKPLACE HEALTH AND SAFETY
3. TEACHING AND LEARNING
4. RESEARCH AND RESEARCH TRAINING
5. HUMAN RESOURCES
6. INFORMATION AND COMMUNICATION TECHNOLOGY
6.10 ACCESS TO CORPORATE SYSTEMS
6.20 INFORMATION AND COMMUNICATION TECHNOLOGY
6.20.01 INFORMATION AND COMMUNICATION TECHNOLOGY POLICY
6.20.03 SOFTWARE ACQUISITION AND USE
6.20.04 EMAIL AND BULK MESSAGING
6.20.05 DIGITAL PRESENCE
6.20.06 ACCEPTABLE USE OF UQ ICT RESOURCES
6.30 CYBER SECURITY
6.40 INFORMATION MANAGEMENT
7. PHYSICAL FACILITIES AND SERVICES
8. COMMUNITY AND DEVELOPMENT ACTIVITIES
9. FINANCIAL MANAGEMENT PRACTICES
Guidelines

6.20.06 Acceptable Use of UQ ICT Resources

Acceptable Use of UQ ICT Resources - Guidelines

Document Number:	6.20.06c
Topic:	6.20.06 Acceptable Use of UQ ICT Resources
Approval Authority:	Chief Information Officer
Last Approval Date:	Wednesday, October 16, 2019
Review date:	Sunday, October 16, 2022
Audience:	All Staff UQ Community All Students

1.0 Purpose and Scope

The purpose of this guideline is to support the Information and Communication Technology Policy by providing further information regarding acceptable use of UQ ICT resources, including personal use. This is a UQ-wide guideline that applies to all consumers of UQ ICT resources, as defined in the policy.

2.0 Acceptable Use of UQ ICT Resources

Acceptable use can most easily be illustrated by examples of unacceptable use. The following are examples of what may be considered inappropriate use of ICT resources. In instances where such use is required for legitimate research or teaching purposes, an exception may be approved.

a. Knowingly downloading, storing, distributing and viewing of offensive, obscene, indecent, pornographic, or menacing material. This could include, but not limited to pornography, hate sites, gratuitous violence and sites using frequent and highlighted bad language.

b. Destruction of or damage to equipment, software, or data belonging to The University of Queensland.

c. Playing of games is not permitted by staff within work hours. Students should also not use UQ resources for playing games unless it is a legitimate requirement of their studies. Games can require a large amount of internal storage and potentially long play periods breaching the UQ minimal use standard. The loading of such software also potentially has software licensing

https://ppl.app.uq.edu.au/content/6.20.06-acceptable-use-uq-ict-resources

Systems-Specific Security Policy (SysSP)

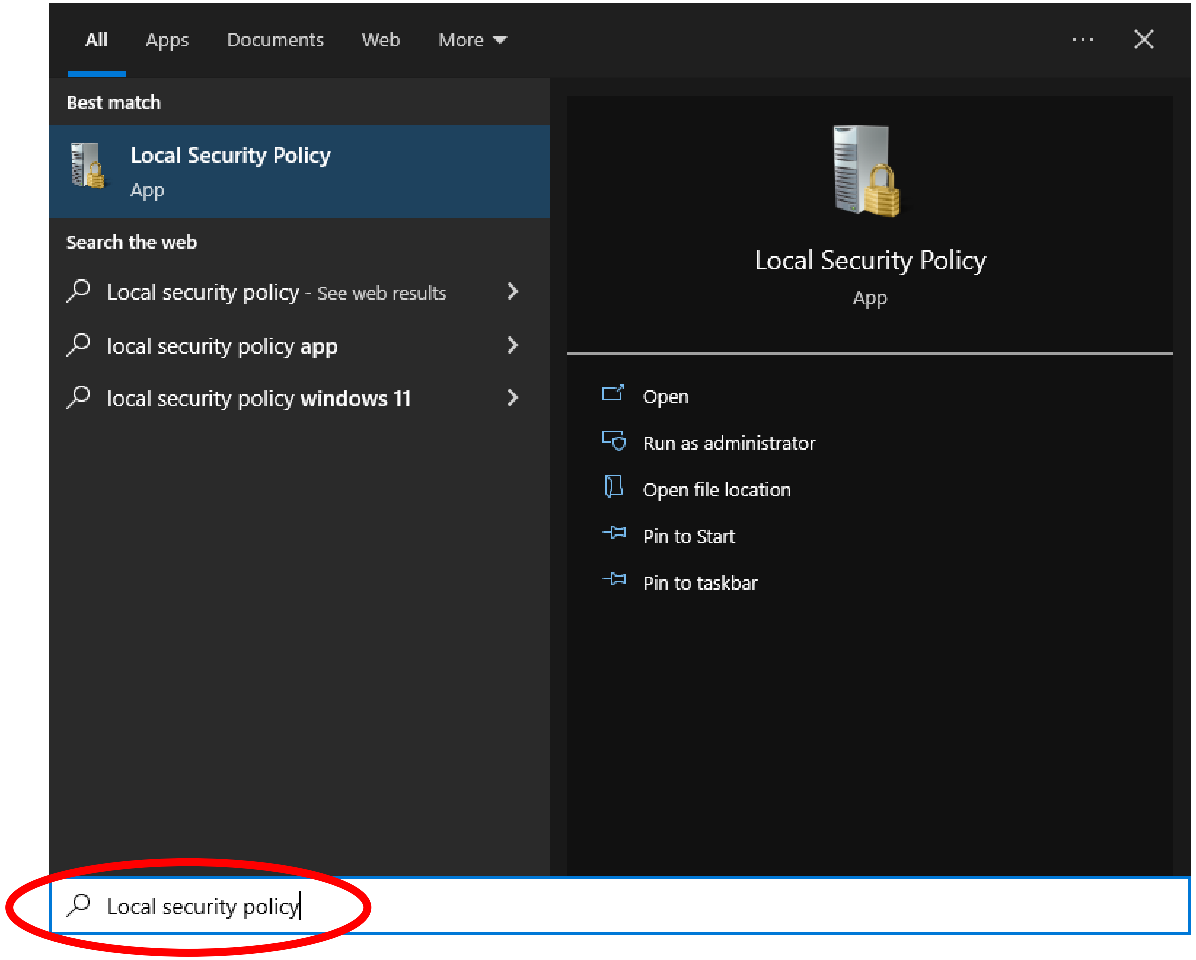
- SysSPs frequently function as standards and procedures used **when configuring or maintaining systems**

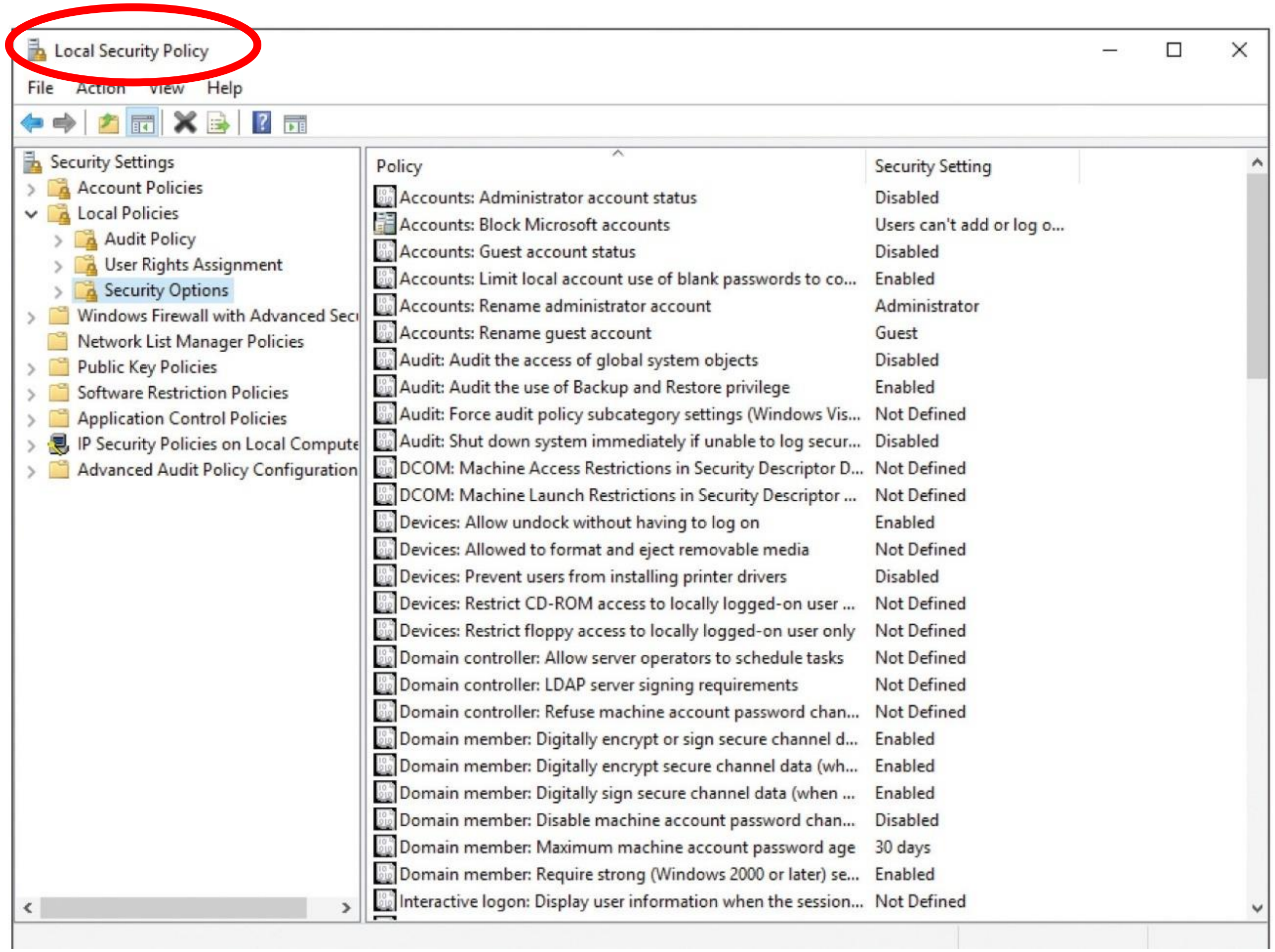
- Systems-specific policies fall into two groups
  - **Managerial** guidance (most often lead to "technical specs")
  - **Technical** specifications

- Example (Access Control Lists or ACLs)
  - ACLs can restrict access for a particular user, computer, time, duration—even a particular file
  - ACLs focus on the organisational asset. Capability tables focus on users
    - Who can access the system (individual identity or group membership)
    - What authorized users can do (Read, Write, Create, Modify, Delete)
    - When authorized users can access the system
    - Where authorized users can access the system from (local/remote)

Example: Local security policy setting on PC

Windows 10




Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

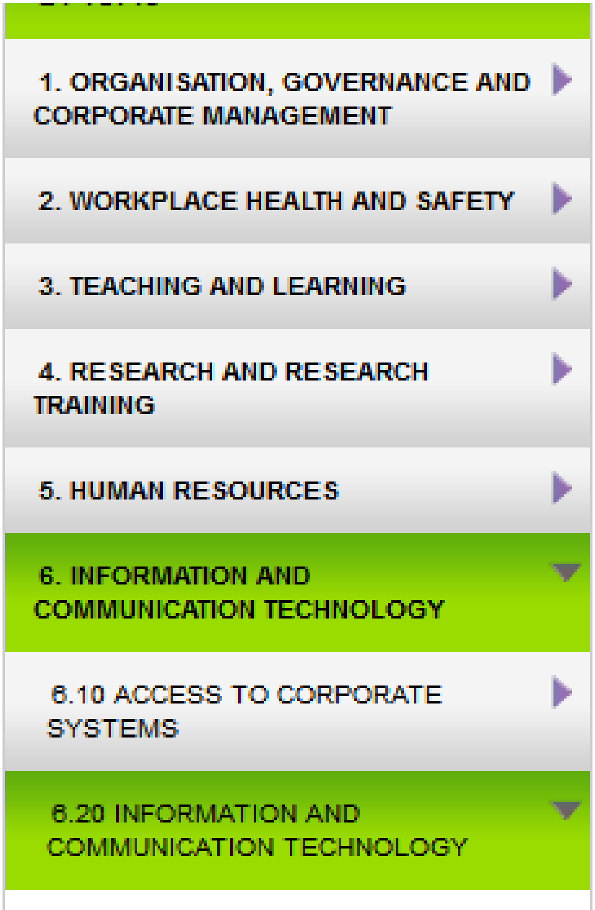
Policy	Security Setting
Accounts: Administrator account status	Disabled
Accounts: Block Microsoft accounts	Users can't add or log o...
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to co...	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Enabled
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Disabled
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Disabled
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Enabled
Domain member: Digitally encrypt secure channel data (wh...	Enabled
Domain member: Digitally sign secure channel data (when ...	Enabled
Domain member: Disable machine account password chan...	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
Interactive logon: Display user information when the session...	Not Defined

Policy Management

- Policies must be managed as they constantly change
- To remain viable, security policies must have:
  - Individual responsible for the policy (policy administrator)
  - A schedule of reviews
  - Method for making recommendations for reviews
  - Specific policy issuance and revision date

Have a look at one of UQ‘s policies: can you identify who is responsible? The revision dates?

Who is responsible? The revision dates?



1. ORGANISATION, GOVERNANCE AND CORPORATE MANAGEMENT

2. WORKPLACE HEALTH AND SAFETY

3. TEACHING AND LEARNING

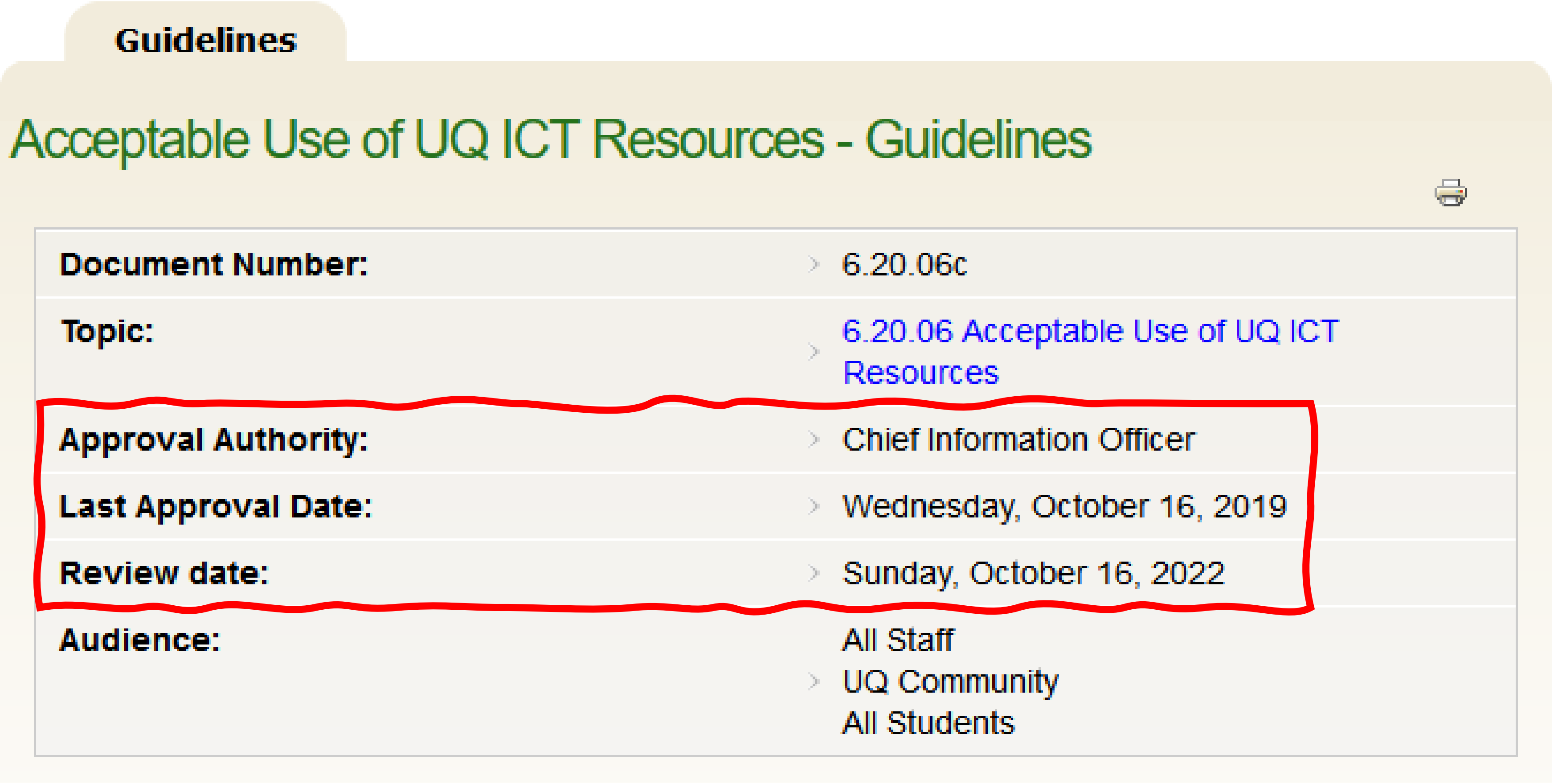
4. RESEARCH AND RESEARCH TRAINING

5. HUMAN RESOURCES

6. INFORMATION AND COMMUNICATION TECHNOLOGY

6.10 ACCESS TO CORPORATE SYSTEMS

6.20 INFORMATION AND COMMUNICATION TECHNOLOGY



Guidelines

Acceptable Use of UQ ICT Resources - Guidelines

Document Number:	6.20.06c
Topic:	6.20.06 Acceptable Use of UQ ICT Resources
Approval Authority:	Chief Information Officer
Last Approval Date:	Wednesday, October 16, 2019
Review date:	Sunday, October 16, 2022
Audience:	All Staff UQ Community All Students

Security education, training, and awareness program (SETA)

- Once general security policies exist, implement a **security education, training, and awareness (SETA)** program**.**
- SETA is a **control** measure designed to **reduce accidental security breaches**.
- Security education and training builds on the general knowledge the employees must possess to do their jobs, familiarizing them with the way to do their jobs securely
- The SETA program consists of: **security education**; **security training**; and **security awareness**

Comparative Framework of SETA

	Awareness	Training	Education
Attribute	Seeks to teach members of the organisation ***what*** security is and what the employee should do in some situations	Seeks to train members of the organisation ***how*** they should react and respond when threats are encountered in specified situations	Seeks to educate members of the organisation as to ***why*** it has prepared in the way it has and why the organisation reacts in the ways it does
Level	Offers basic ***information*** about threats and responses	Offers more detailed ***knowledge*** about detecting threats and teaches skills needed for effective reaction	Offers the background and depth of knowledge to gain ***insight*** into how processes are developed and enables ongoing Improvement
Objective	Members of the organisation can ***recognize*** threats and formulate simple responses	Members of the organisation can mount effective responses using learned ***skills***	Members of the organisation can engage in active defense and use ***understanding*** of the organisation's objectives to make continuous improvement
Teaching methods	• Media videos • Newsletters • Posters • Informal training	• Formal training • Workshops • Hands-on practice	• Theoretical instruction • Discussions/seminars • Background reading
Assessment	True/false or multiple choice (identify learning)	Problem solving (apply learning)	Essay (interpret learning)
Impact time frame	Short-term	Intermediate	Long-term

The Information Security Blueprint

- **After policy/standard development – then develop blueprint** (what is a 'blueprint' - what are we talking about here?)
- Should **specify tasks to be accomplished and the order** in which they are to be realized
- Should also serve as **scalable**, **upgradeable**, and **comprehensive plan** for information security needs for coming years
- We should look to **recognised standards** to assist!

The ISO 27000 Series

1. One of the most widely referenced and often discussed security models
2. **ISO27002** provides a common basis for developing organisational security:
   - Via a list of 14 control areas, addresses 39 control objectives and more than 110 individual controls
3. ISO27002 is a (long) list of IS controls – experience shows that **‘just’ implementing controls is not enough – we need very good ‘security management’**
4. Therefore, the ISO27002 is complemented with **ISO27001** which describes ‘security management’.
   - It is fundamental that ISO27001 considers that IS Security is seen as a continual improvement process – and not as implementing a security product.
5. **ISO 27001/27002 together function as a framework for information security:**
   - Organisational security policy is needed to provide management direction and support – its purpose is to give recommendations for IS security management.

REMEMBER: ISO 27001 provides information on how to implement ISO 27002 and how to set up an information security management system (ISMS).

The ISO 27000 Series (cont‘d)

- Based on the ideas of quality management systems (ISO 9001).
  - ISO 9001 has become the most widely used and implemented quality management system in the world.
- Many such management systems exist, e.g.:
  - Information Security management (ISO 27001)
  - Digital certificate management (ETSI TS 101 456)
  - Environment management (ISO 14001)
  - Occupational Health & Safety management (BSI OHSAS 18001)
- As with all management systems also an organisation’s ISO 27001 implementation can be formally certified.

REMEMBER: The key purpose of the ISO 27000 series is to give recommendations for IS management with the goal of **certification**.

The ISO 27000 Series (cont'd)

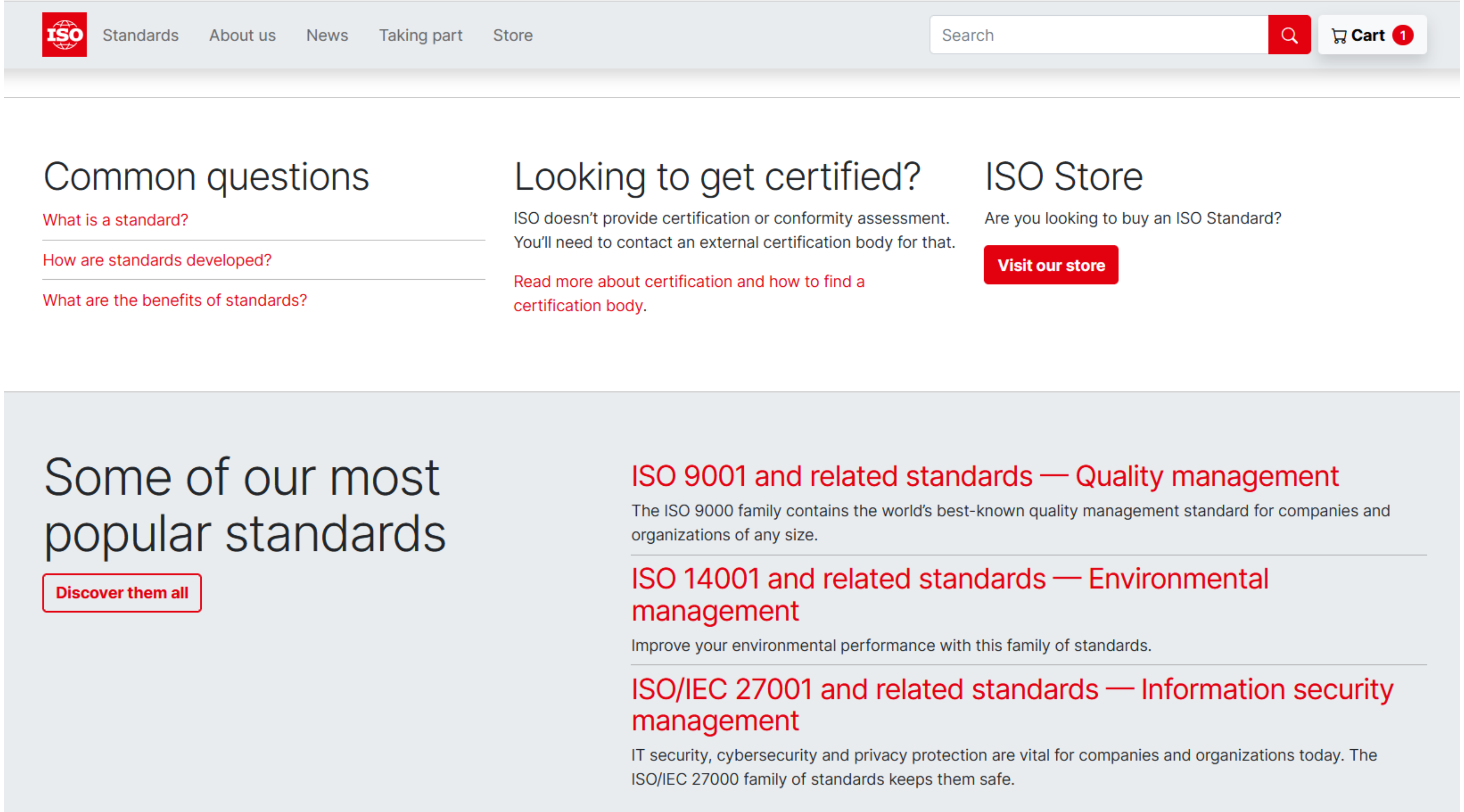
- ISO/IEC 27000 - Information security management systems; overview and **vocabulary**
- <u>**ISO/IEC 27001**</u> - Information technology; security techniques; information security management systems – **27001 focuses on processes for security**!
- <u>**ISO/IEC 27002**</u> - Code of practice (**controls**) for information security management - **27002 focuses on the controls for security!**
- ISO/IEC 27003 - Information security management system implementation guidance

- ISO/IEC 27004—Information security management; measurement
- ISO/IEC 27005—Information security risk management
- ISO/IEC 27006—Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007—Guidelines for information security management systems auditing (focused on the management system)

… and many more standards for IS security!

The ISO 27000 Series (cont‘d)

https://www.iso.org/home.html (is on landing page!)



Common questions

What is a standard?

How are standards developed?

What are the benefits of standards?

Looking to get certified?

ISO doesn’t provide certification or conformity assessment. You’ll need to contact an external certification body for that.

Read more about certification and how to find a certification body.

ISO Store

Are you looking to buy an ISO Standard?

Visit our store

Some of our most popular standards

Discover them all

ISO 9001 and related standards — Quality management

The ISO 9000 family contains the world’s best-known quality management standard for companies and organizations of any size.

ISO 14001 and related standards — Environmental management

Improve your environmental performance with this family of standards.

ISO/IEC 27001 and related standards — Information security management

IT security, cybersecurity and privacy protection are vital for companies and organizations today. The ISO/IEC 27000 family of standards keeps them safe.

The ISO 27000 Series (cont‘d)

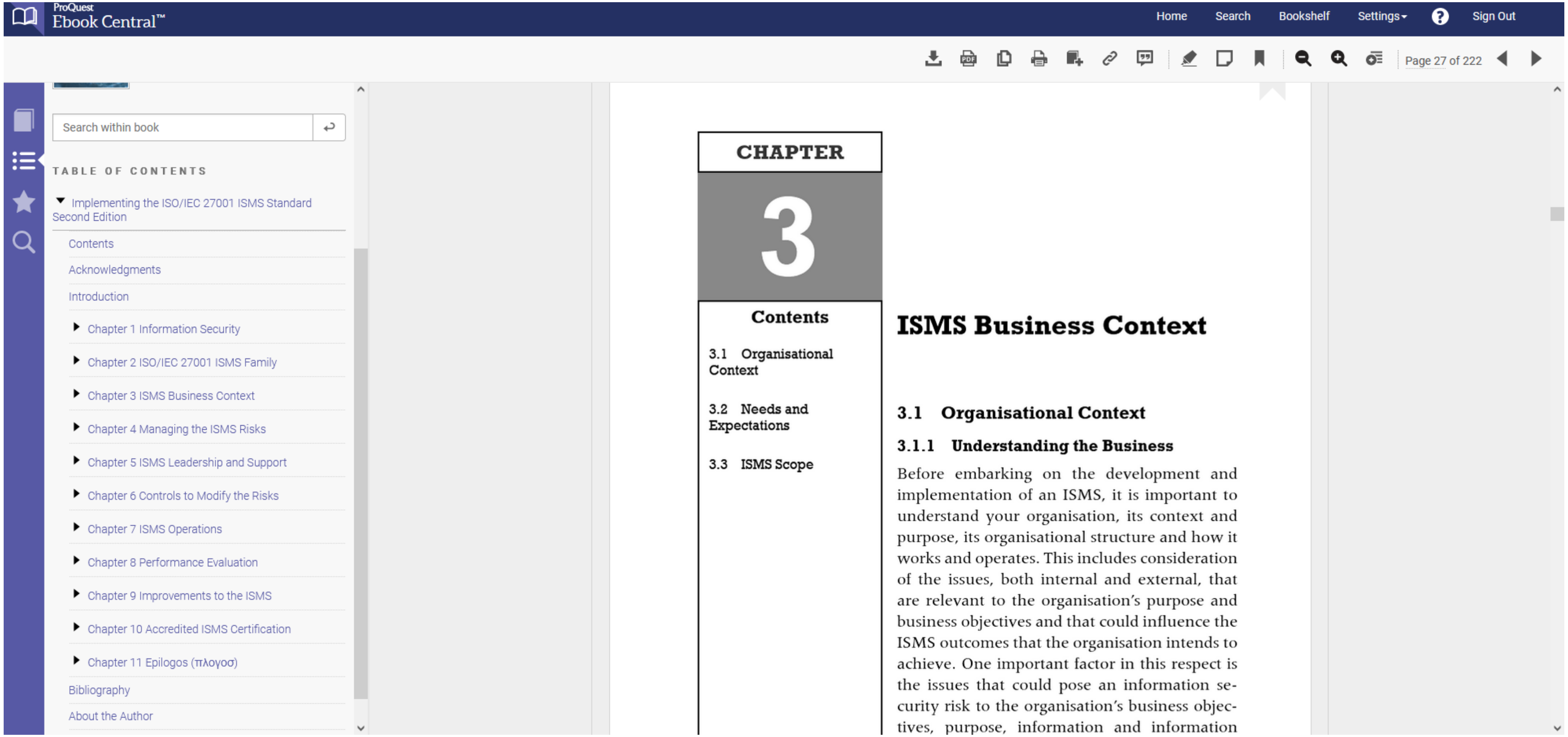


TABLE OF CONTENTS

Implementing the ISO/IEC 27001 ISMS Standard Second Edition
Contents
Acknowledgments
Introduction
Chapter 1 Information Security
Chapter 2 ISO/IEC 27001 ISMS Family
Chapter 3 ISMS Business Context
Chapter 4 Managing the ISMS Risks
Chapter 5 ISMS Leadership and Support
Chapter 6 Controls to Modify the Risks
Chapter 7 ISMS Operations
Chapter 8 Performance Evaluation
Chapter 9 Improvements to the ISMS
Chapter 10 Accredited ISMS Certification
Chapter 11 Epilogos (πλογοσ)
Bibliography
About the Author

CHAPTER

3

Contents

3.1 Organisational Context
3.2 Needs and Expectations
3.3 ISMS Scope

ISMS Business Context

3.1 Organisational Context

3.1.1 Understanding the Business

Before embarking on the development and implementation of an ISMS, it is important to understand your organisation, its context and purpose, its organisational structure and how it works and operates. This includes consideration of the issues, both internal and external, that are relevant to the organisation's purpose and business objectives and that could influence the ISMS outcomes that the organisation intends to achieve. One important factor in this respect is the issues that could pose an information security risk to the organisation's business objectives, purpose, information and information

Access from UQ Library

The ISO 27001 & 27002 – a *framework*

The 27001 & 27002 combine to function as a framework – not as ‘project-based point solutions.

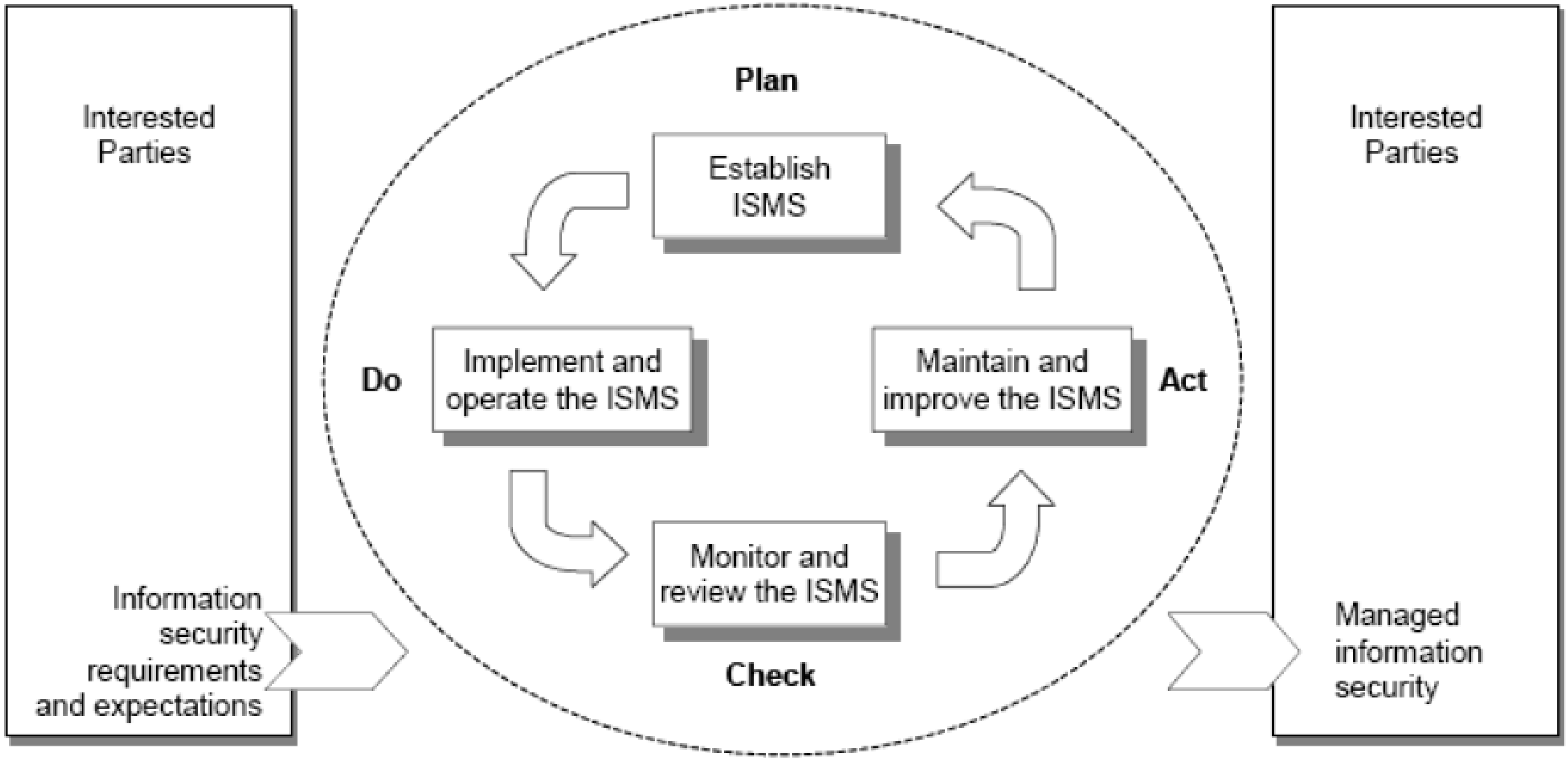
In the later parts of the seminar we consider a standard for information security for any business processing MasterCard, Visa Card etc. And this standard is termed PCI-DSS.

If a business is going to do credit card transactions, debit cart transactions with Visa MasterCard and the like, they must comply with the PCI-DSS.

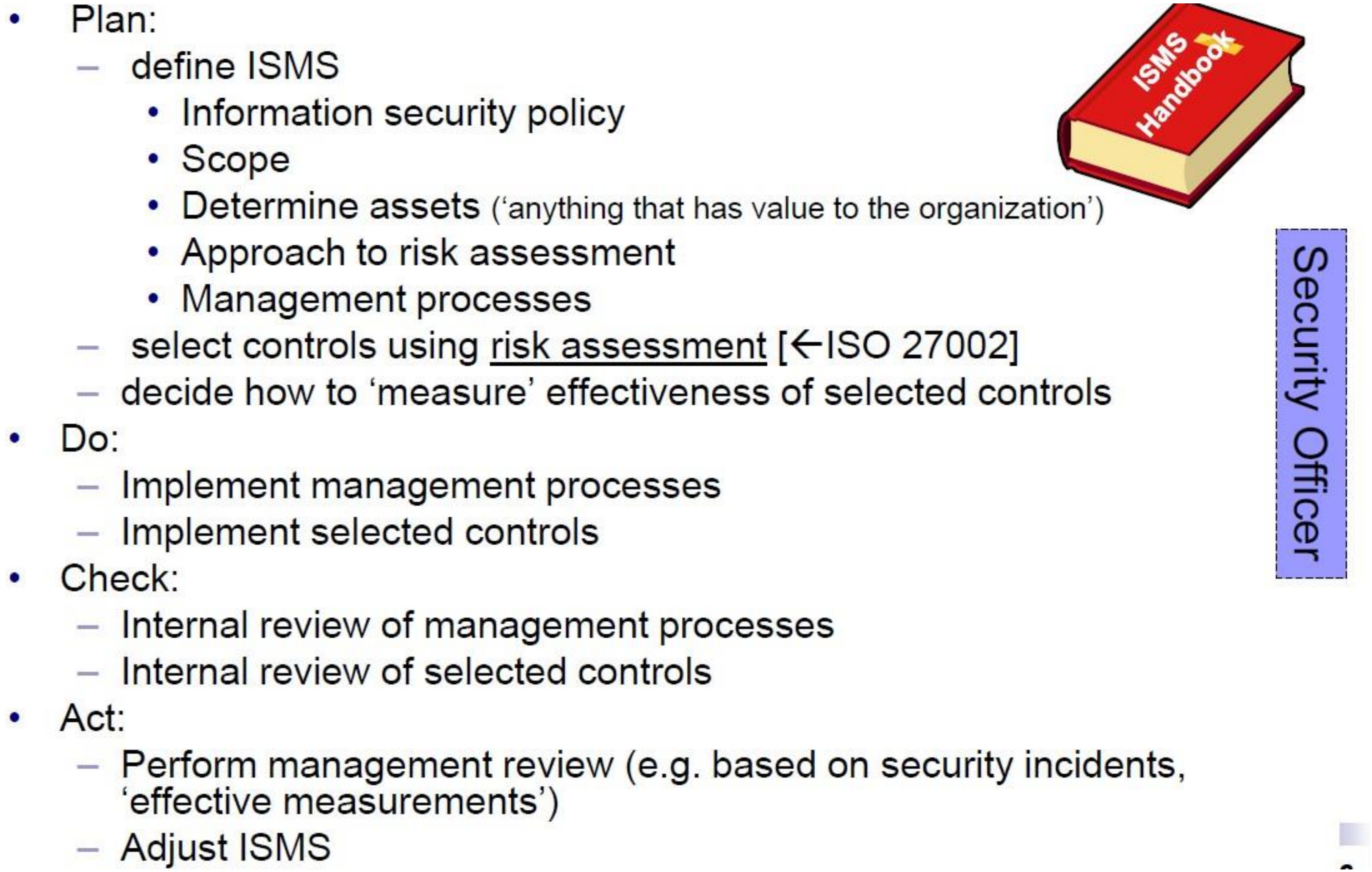
If a security breach occurs and the auditors find the business was not in compliance with the standard, the credit card companies will sue that business, and they will sue the business very savagely.
So this would be a standard. You sign a contract, if you breach the contract, you pay the penalty for non-compliance.

The approach of the ISO is a framework. There is no signing up to it. There‘s no penalties for non-compliance. They are literally issued to try and help improve information security.

The ISO 27001: The Plan Do Check Act (PDCA) model applied to Information Security Management System (ISMS) processes

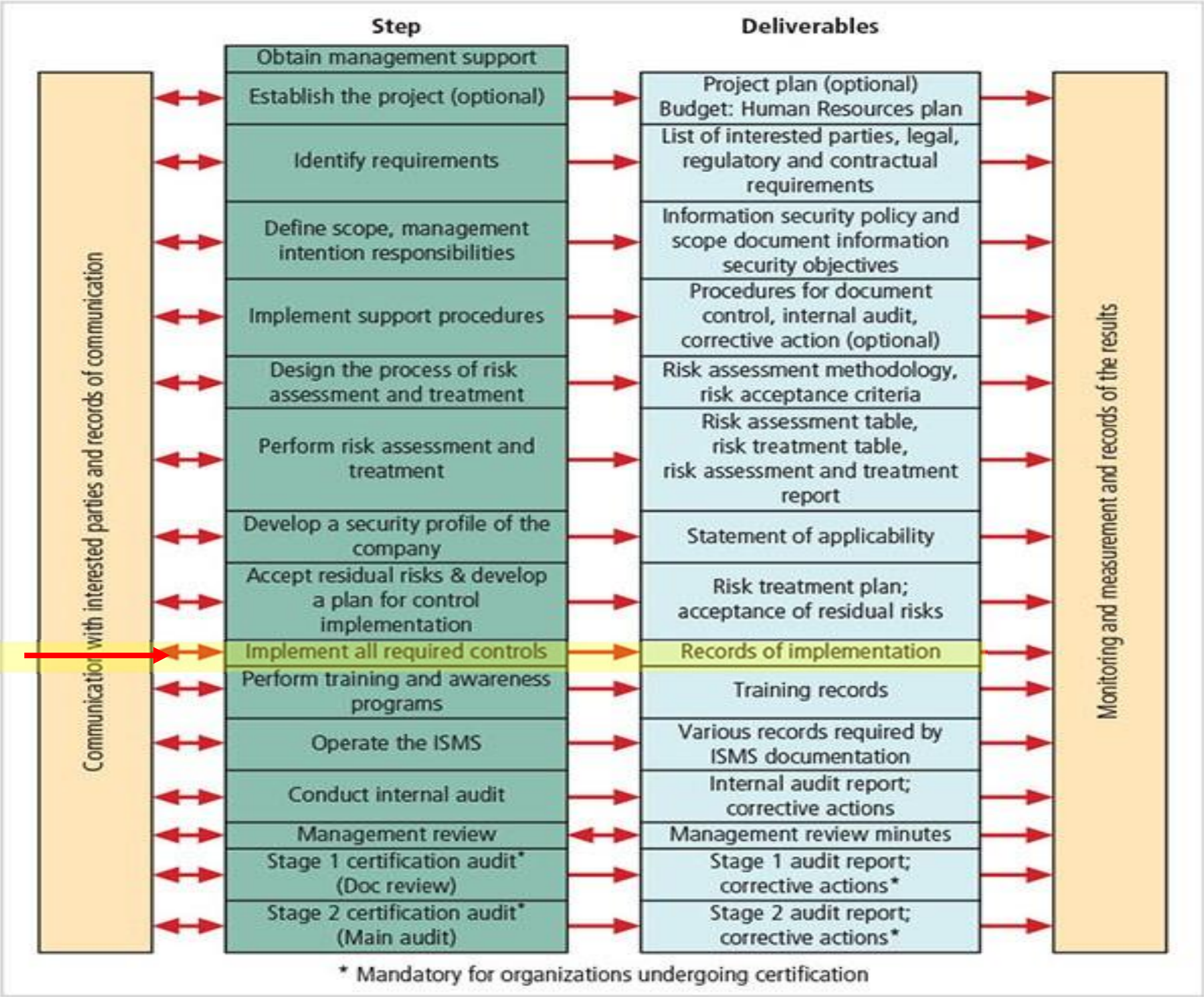

Interested Parties
Information security requirements and expectations
Plan
Establish ISMS
Do
Implement and operate the ISMS
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check
Interested Parties
Managed information security

The ISO 27001: 2013 (more detailed view)



- Plan:
  - define ISMS
    - Information security policy
    - Scope
    - Determine assets (‘anything that has value to the organization’)
    - Approach to risk assessment
    - Management processes
  - select controls using risk assessment [←ISO 27002]
  - decide how to ‘measure’ effectiveness of selected controls
- Do:
  - Implement management processes
  - Implement selected controls
- Check:
  - Internal review of management processes
  - Internal review of selected controls
- Act:
  - Perform management review (e.g. based on security incidents, ‘effective measurements’)
  - Adjust ISMS

The ISO 27001: 2013 – major process steps



Step	Deliverables
Obtain management support	
Establish the project (optional)	Project plan (optional) Budget: Human Resources plan
Identify requirements	List of interested parties, legal, regulatory and contractual requirements
Define scope, management intention responsibilities	Information security policy and scope document information security objectives
Implement support procedures	Procedures for document control, internal audit, corrective action (optional)
Design the process of risk assessment and treatment	Risk assessment methodology, risk acceptance criteria
Perform risk assessment and treatment	Risk assessment table, risk treatment table, risk assessment and treatment report
Develop a security profile of the company	Statement of applicability
Accept residual risks & develop a plan for control implementation	Risk treatment plan; acceptance of residual risks
Implement all required controls	Records of implementation
Perform training and awareness programs	Training records
Operate the ISMS	Various records required by ISMS documentation
Conduct internal audit	Internal audit report; corrective actions
Management review	Management review minutes
Stage 1 certification audit* (Doc review)	Stage 1 audit report; corrective actions*
Stage 2 certification audit* (Main audit)	Stage 2 audit report; corrective actions*

Communication with interested parties and records of communication
Monitoring and measurement and records of the results

* Mandatory for organizations undergoing certification

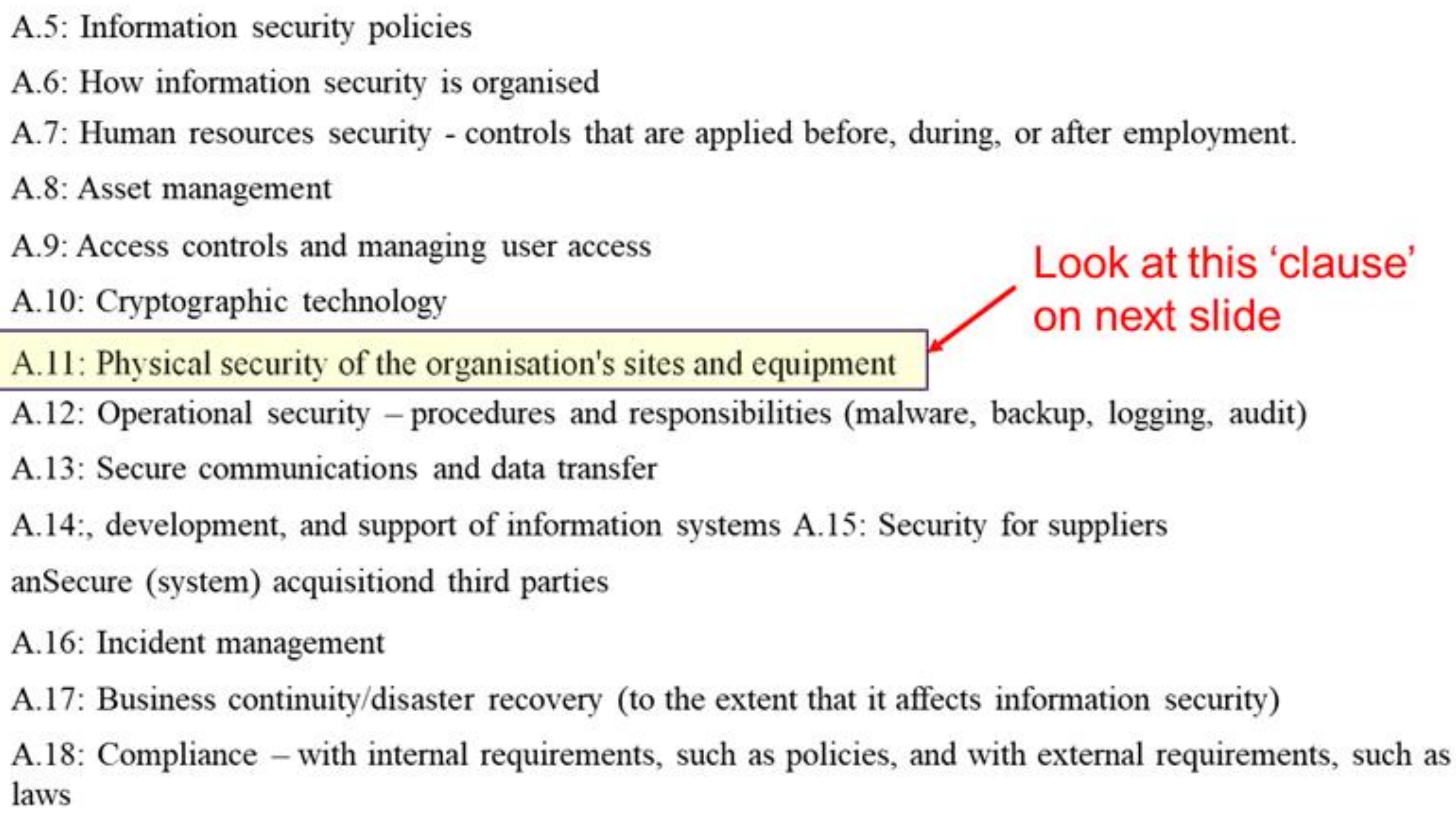
This links with 27002

This is project management 101.

1. We establish the project, we identify the requirements, we define the scope.
2. We design the process of risk assessment and treatment.
3. We implement all required controls that come from that (this is the part where 27001 links across to 27002)

The ISO 27002: 2013 – content (1)

The ISO 27002 has five introductory chapters – followed by 14 main control clauses that then describe general controls. The numbering below reflects the numbering of control clauses in the standard.



A.5: Information security policies

A.6: How information security is organised

A.7: Human resources security - controls that are applied before, during, or after employment.

A.8: Asset management

A.9: Access controls and managing user access

A.10: Cryptographic technology

A.11: Physical security of the organisation's sites and equipment

A.12: Operational security – procedures and responsibilities (malware, backup, logging, audit)

A.13: Secure communications and data transfer

A.14:, development, and support of information systems A.15: Security for suppliers

anSecure (system) acquisitiond third parties

A.16: Incident management

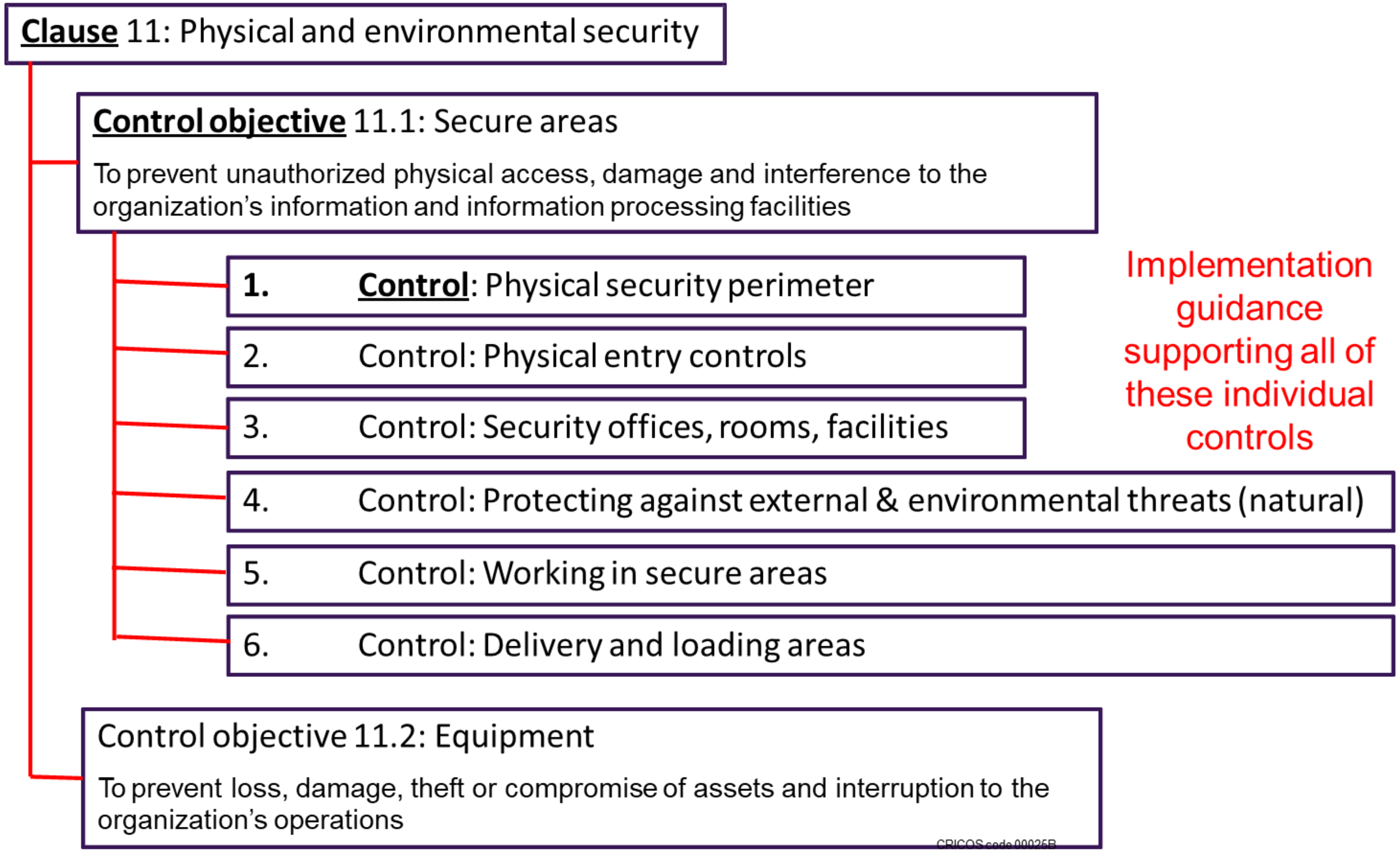
A.17: Business continuity/disaster recovery (to the extent that it affects information security)

A.18: Compliance – with internal requirements, such as policies, and with external requirements, such as laws

Look at this 'clause' on next slide

Example

ISO27002 A.11: Physical security of the organisation's sites and equipment



Clause 11: Physical and environmental security

Control objective 11.1: Secure areas

To prevent unauthorized physical access, damage and interference to the organization’s information and information processing facilities

1. **Control**: Physical security perimeter
2. Control: Physical entry controls
3. Control: Security offices, rooms, facilities
4. Control: Protecting against external & environmental threats (natural)
5. Control: Working in secure areas
6. Control: Delivery and loading areas

Implementation guidance supporting all of these individual controls

Control objective 11.2: Equipment

To prevent loss, damage, theft or compromise of assets and interruption to the organization’s operations

Variations on ISO2700x for the medical sector (IS)

- There is also an ISO standard (27799) variant on the ISO 27002 for the medical sector ‘Health informatics - Information security management in health using ISO/IEC 27002 (https://www.iso.org/standard/62777.html)

- It applies to **health information in all its aspects**, whatever form the information takes (words and numbers, sound recordings, drawings, video, and medical images), whatever means are used to store it (printing or writing on paper or storage electronically), and whatever means are used to transmit it (by hand, through fax, over computer networks, or by post), as the information is always appropriately protected.

- By implementing ISO 27799:2016, healthcare organisations and other custodians of health information will be able **to ensure a minimum requisite level of security** that is appropriate to their organisation's circumstances and that will maintain the confidentiality, integrity and availability of personal health information in their care.

NIST security models (very important also)

- Documents available from Computer Security Resource Center of the National Institute of Standards and Technology (NIST)

  - SP 800-12, *The Computer Security Handbook*
  - SP 800-14, *Generally Accepted Principles and Practices for Securing IT Systems*
  - SP 800-18, *The Guide for Developing Security Plans for IT Systems*
  - SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*
  - SP 800-30 (Revision 1), *Risk Management Guide for Information Technology Systems*

- ***All these standards are freely available (in PDF) from https://www.nist.gov/***

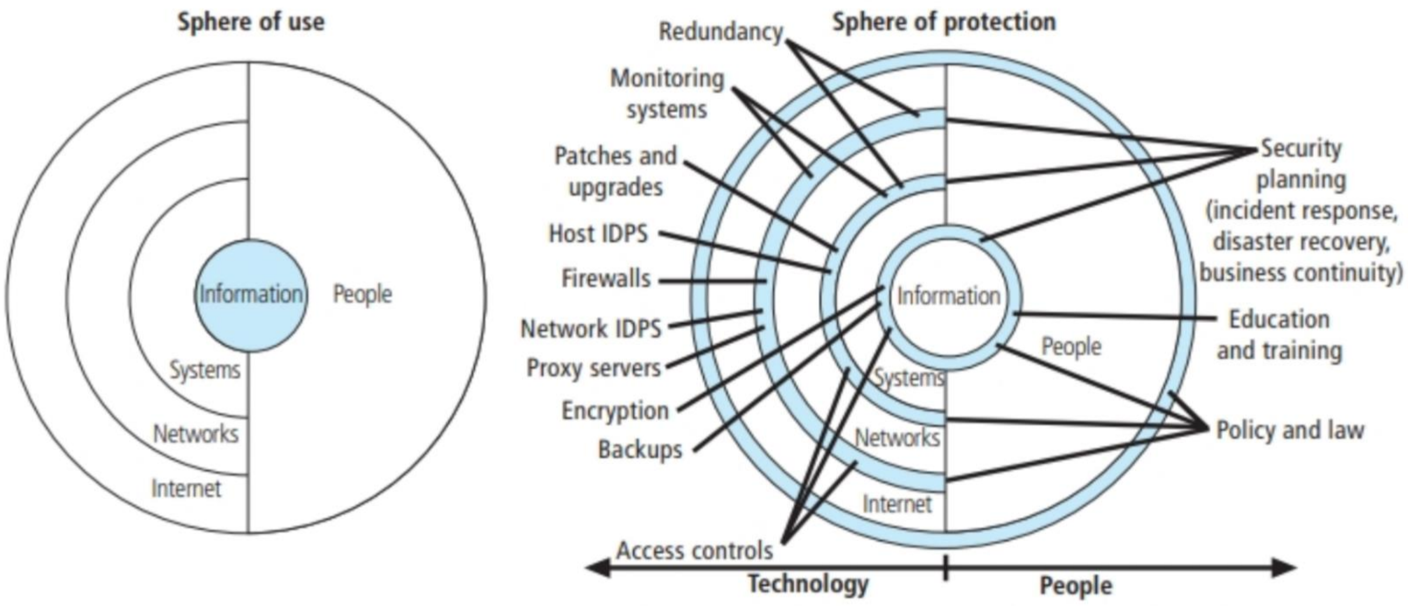
… and there are many more standards for IS security (https://csrc.nist.gov)!

Design of security architecture

Once we have decided to use a particular standard, we have to set the **foundation of the security framework**

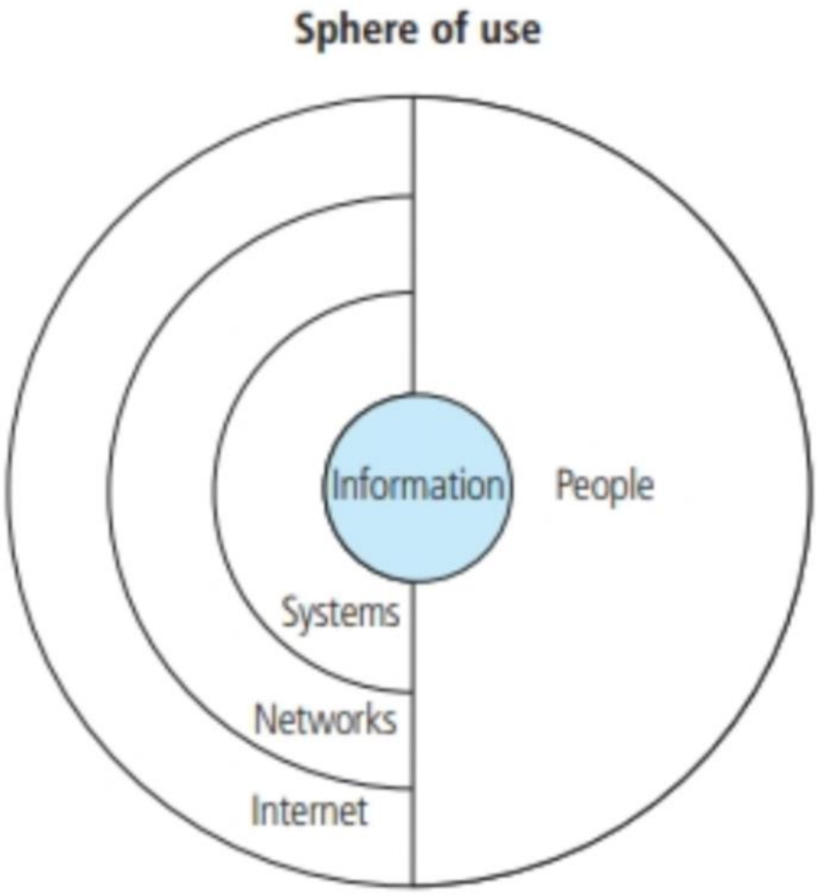
Levels of controls

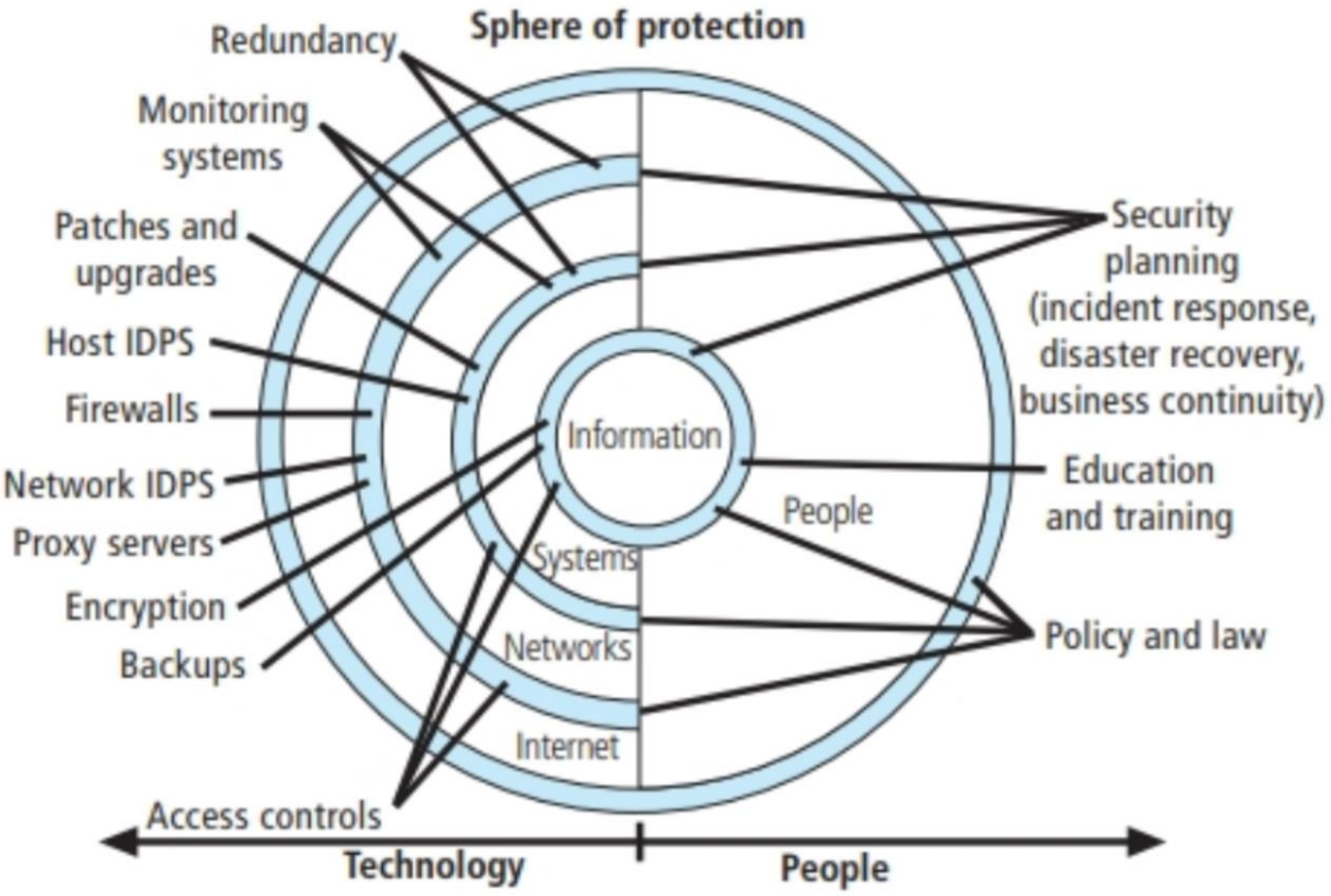
- **Management controls** cover security processes designed by strategic planners and performed by security administration
- **Operational controls** deal with operational functionality of security in organisation (personnel/physical security, education, equipment maintenance)
- **Technical controls** address technical implementations related to designing and implementing security



Note: IDPS is an abbreviation of "intrusion detection and prevention systems".

Different kind of controls that relate to the areas





Note: IDPS is an abbreviation of "intrusion detection and prevention systems".

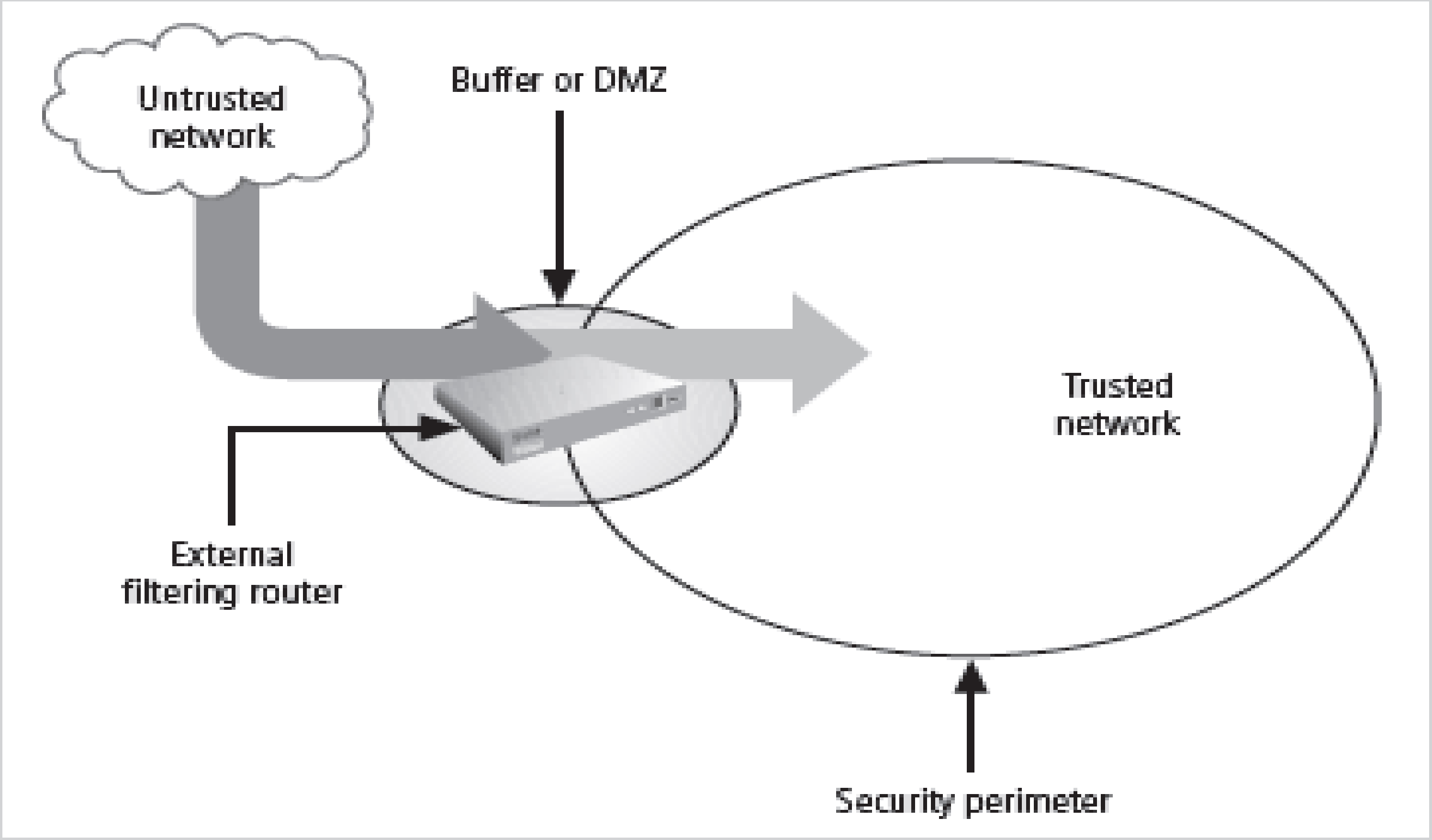
Design of security architecture (continued)

- **Defense in depth**
  - Implementation of security in layers
  - Requires that organisations establish multiple layers of security controls and safeguards
- **Security perimeter**
  - Border of security protecting internal systems from outside threats
  - Does not protect against internal attacks from employee threats or on-site physical threats

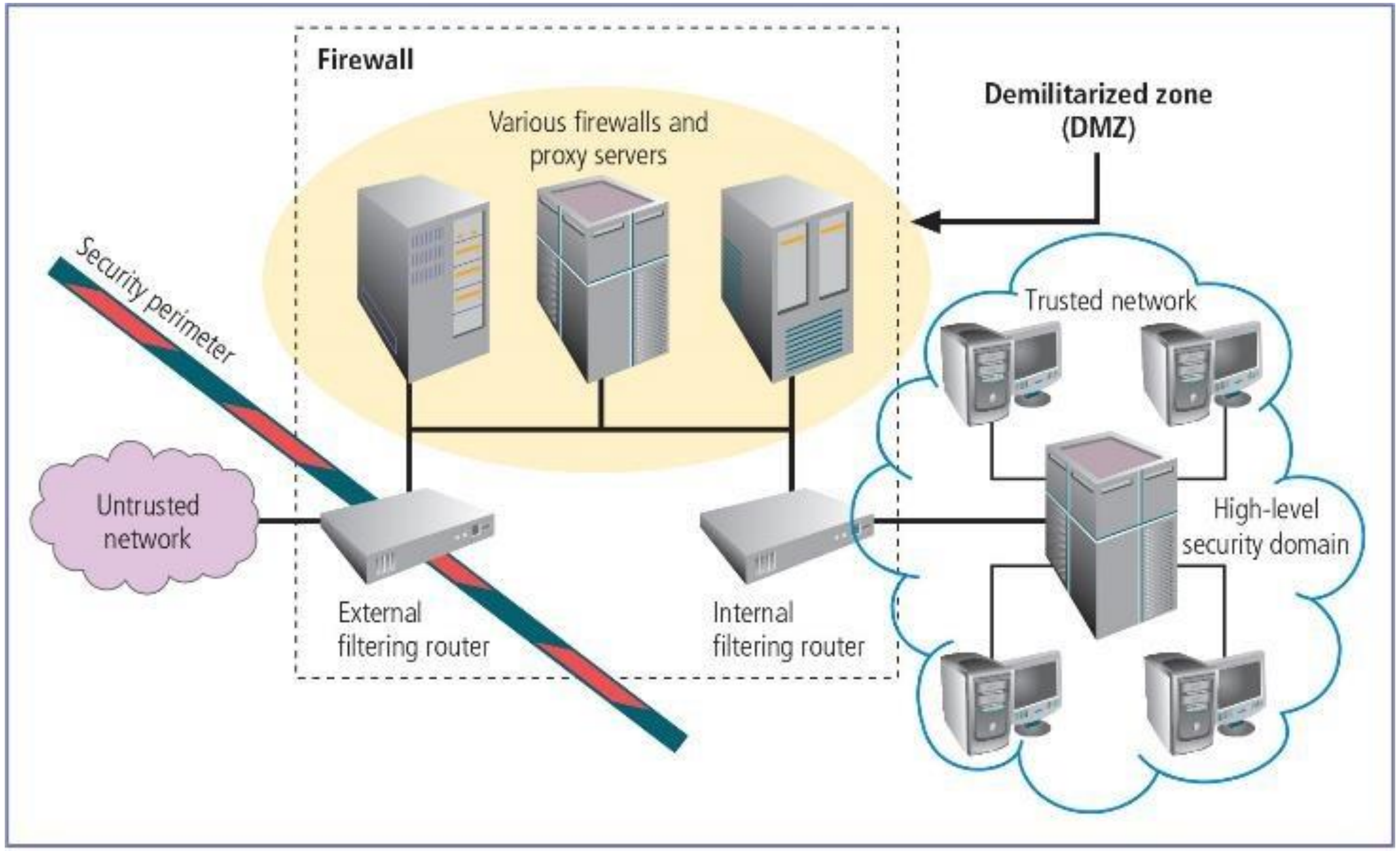
Diagrams and concepts explored later in course – introduced here

- **Firewall**: device that selectively discriminates against information flowing in or out of organisation
- **DMZs**: no-man's land between inside and outside networks where some place Web servers
- **Proxy servers**: performs actions on behalf of another system
- **Intrusion detection systems (IDSs)**: An effort to detect unauthorized activity within inner network, or on individual machines, organisation may wish to implement an IDS

Security perimeters



Security perimeters


Firewall
Various firewalls and proxy servers
Demilitarized zone (DMZ)
Security perimeter
Trusted network
Untrusted network
High-level security domain
External filtering router
Internal filtering router

We shall consider these in more detail in future weeks

Summary of Part 1

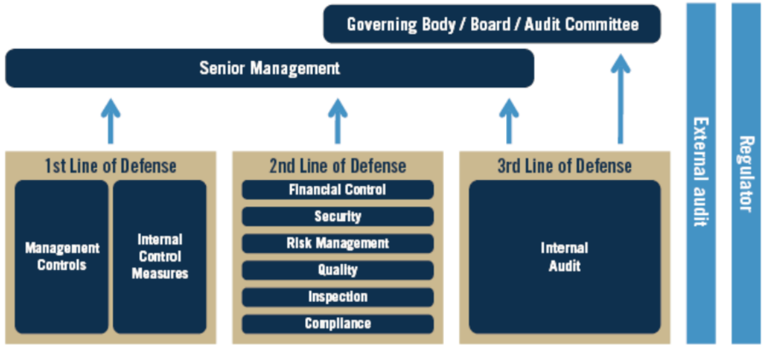
- InfoSec governance: the application of corporate governance principles to InfoSec
- Management must use policies as the basis for all InfoSec planning, design, and deployment
- Three types of ISP: enterprise, issue-specific, systems-specific security policies
- ISP is best disseminated in a comprehensive security education, training, awareness (SETA) program
- InfoSec frameworks (ISO27000 series, NIST) are published to be used as best practices
- Defense in depth: One foundation of security architectures is the layered implementation of security

THE UNIVERSITY OF QUEENSLAND AUSTRALIA | CREATE CHANGE

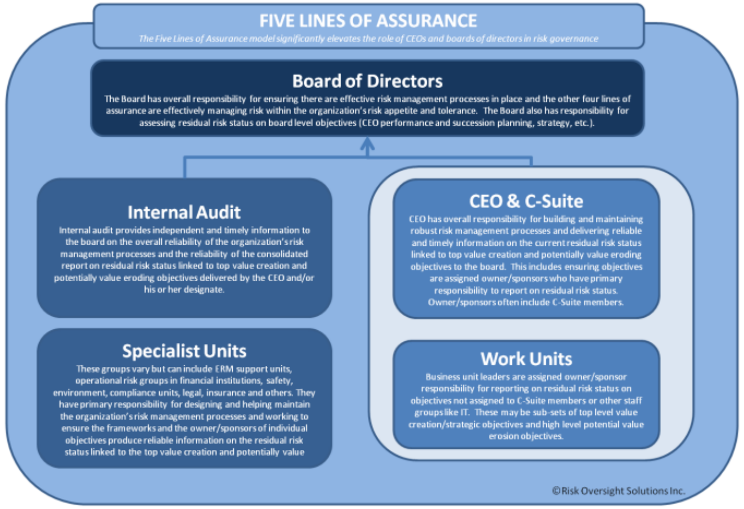
Part 2: Three Lines of Defense vs. Five Lines of Assurance

Why care about governance frameworks?

The Three Lines of Defense Model



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*



FIVE LINES OF ASSURANCE

The Five Lines of Assurance model significantly elevates the role of CEOs and boards of directors in risk governance

Board of Directors

The Board has overall responsibility for ensuring there are effective risk management processes in place and the other four lines of assurance are effectively managing risk within the organization's risk appetite and tolerance. The Board also has responsibility for assessing residual risk status on board level objectives (CEO performance and succession planning, strategy, etc.).

Internal Audit

Internal audit provides independent and timely information to the board on the overall reliability of the organization's risk management processes and the reliability of the consolidated report on residual risk status linked to top value creation and potentially value eroding objectives delivered by the CEO and/or his or her designate.

CEO & C-Suite

CEO has overall responsibility for building and maintaining robust risk management processes and delivering reliable and timely information on the current residual risk status linked to top value creation and potentially value eroding objectives to the board. This includes ensuring objectives are assigned owner/sponsors who have primary responsibility to report on residual risk status. Owner/sponsors often include C-Suite members.

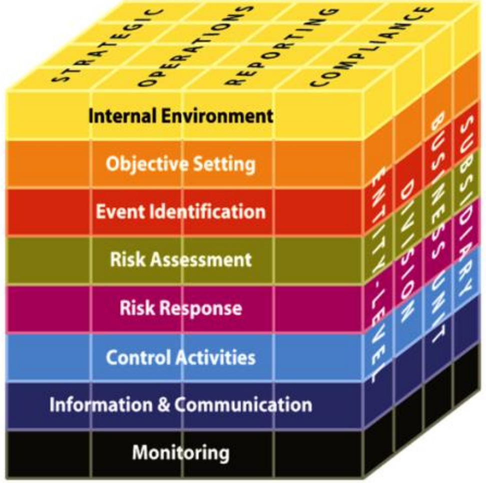
Specialist Units

These groups vary but can include ERM support units, operational risk groups in financial institutions, safety, environment, compliance units, legal, insurance and others. They have primary responsibility for designing and helping maintain the organization's risk management processes and working to ensure the frameworks and the owner/sponsors of individual objectives produce reliable information on the residual risk status linked to the top value creation and potentially value

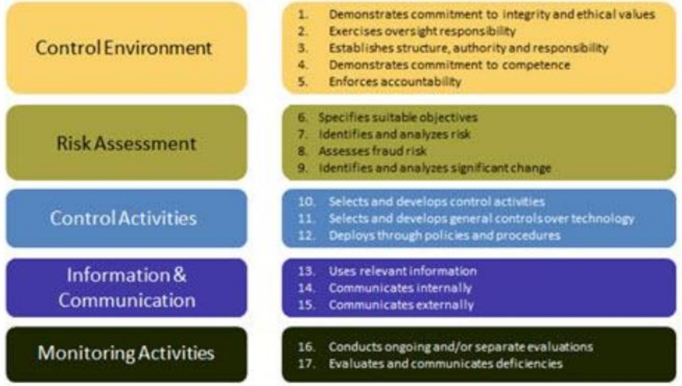
Work Units

Business unit leaders are assigned owner/sponsor responsibility for reporting on residual risk status on objectives not assigned to C-Suite members or other staff groups like IT. These may be sub-sets of top level value creation/strategic objectives and high level potential value erosion objectives.

©Risk Oversight Solutions Inc.



Principles for Effective Internal Control

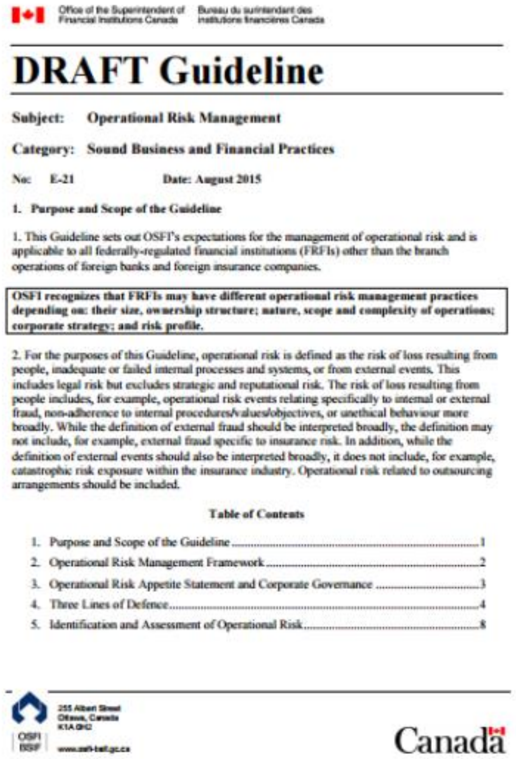


Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Source: Risk Oversight Solutions Inc.

Why care about governance frameworks?

SOMETIMES THEY ARE LEGISLATED



Office of the Superintendent of Financial Institutions Canada
Bureau du surintendant des institutions financières Canada

DRAFT Guideline

Subject: **Operational Risk Management**

Category: **Sound Business and Financial Practices**

No: **E-21** **Date: August 2015**

1. Purpose and Scope of the Guideline

1. This Guideline sets out OSFI's expectations for the management of operational risk and is applicable to all federally-regulated financial institutions (FRFIs) other than the branch operations of foreign banks and foreign insurance companies.

OSFI recognizes that FRFIs may have different operational risk management practices depending on: their size, ownership structure; nature, scope and complexity of operations; corporate strategy; and risk profile.

2. For the purposes of this Guideline, operational risk is defined as the risk of loss resulting from people, inadequate or failed internal processes and systems, or from external events. This includes legal risk but excludes strategic and reputational risk. The risk of loss resulting from people includes, for example, operational risk events relating specifically to internal or external fraud, non-adherence to internal procedures/values/objectives, or unethical behaviour more broadly. While the definition of external fraud should be interpreted broadly, the definition may not include, for example, external fraud specific to insurance risk. In addition, while the definition of external events should also be interpreted broadly, it does not include, for example, catastrophic risk exposure within the insurance industry. Operational risk related to outsourcing arrangements should be included.

Table of Contents

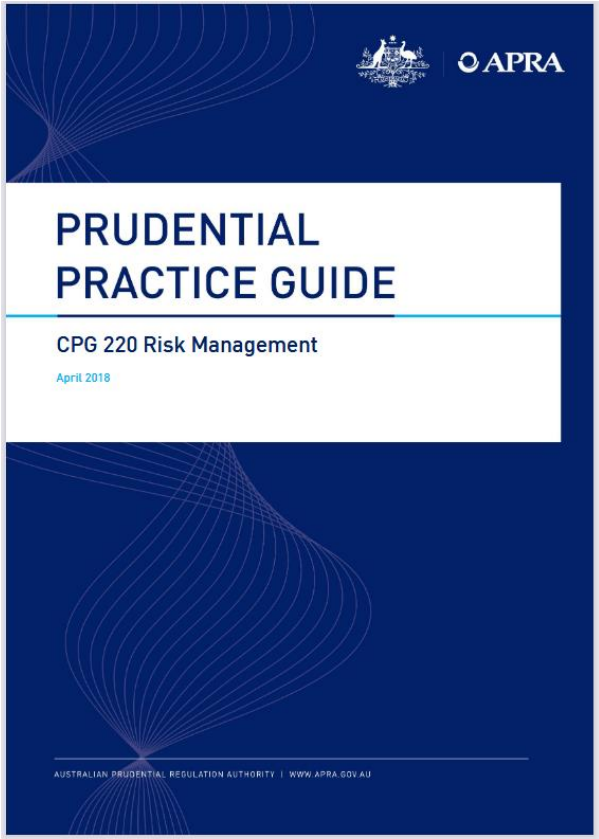
1. Purpose and Scope of the Guideline 1
2. Operational Risk Management Framework 2
3. Operational Risk Appetite Statement and Corporate Governance 3
4. Three Lines of Defence 4
5. Identification and Assessment of Operational Risk 8

OSFI
BSIF

255 Albert Street
Ottawa, Canada
K1A 0H2

www.osfi-bsif.gc.ca

Canada



APRA

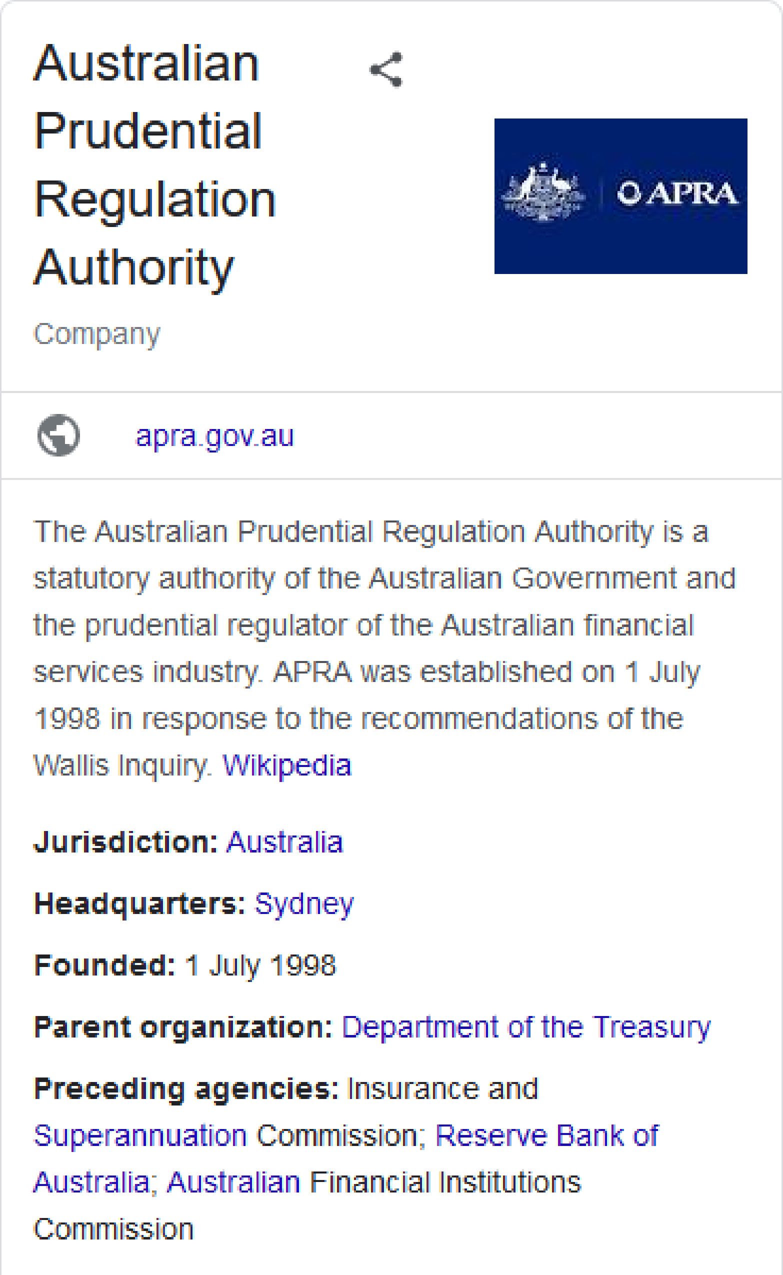
PRUDENTIAL PRACTICE GUIDE

CPG 220 Risk Management

April 2018

AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY | WWW.APRA.GOV.AU

Source: Risk Oversight Solutions Inc.



Australian Prudential Regulation Authority

Company

apra.gov.au

The Australian Prudential Regulation Authority is a statutory authority of the Australian Government and the prudential regulator of the Australian financial services industry. APRA was established on 1 July 1998 in response to the recommendations of the Wallis Inquiry. Wikipedia

Jurisdiction: Australia

Headquarters: Sydney

Founded: 1 July 1998

Parent organization: Department of the Treasury

Preceding agencies: Insurance and Superannuation Commission; Reserve Bank of Australia; Australian Financial Institutions Commission

3LoD for Cyber Security

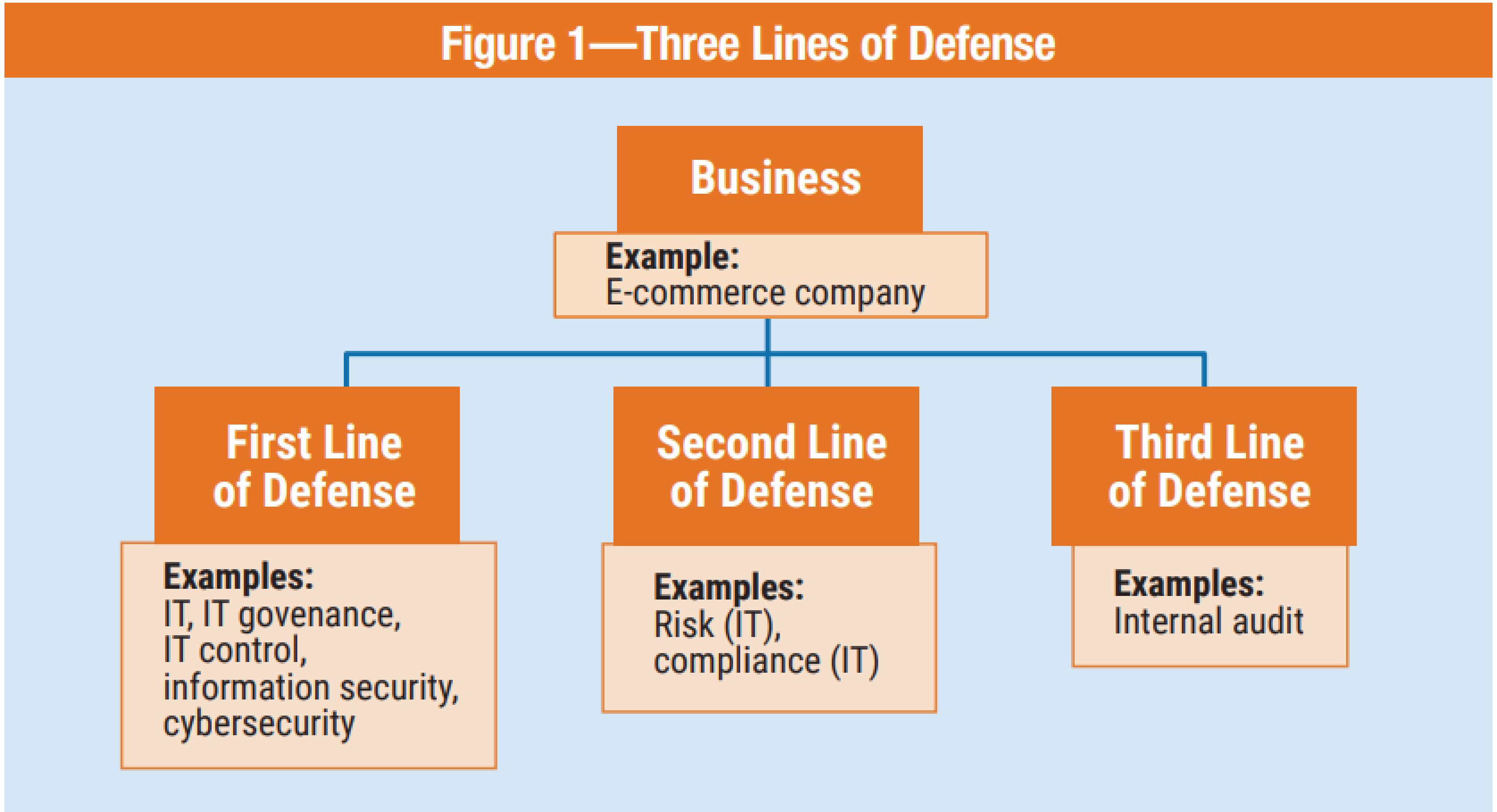


Figure 1—Three Lines of Defense

Business

Example:
E-commerce company

First Line of Defense

Examples:
IT, IT govenance, IT control, information security, cybersecurity

Second Line of Defense

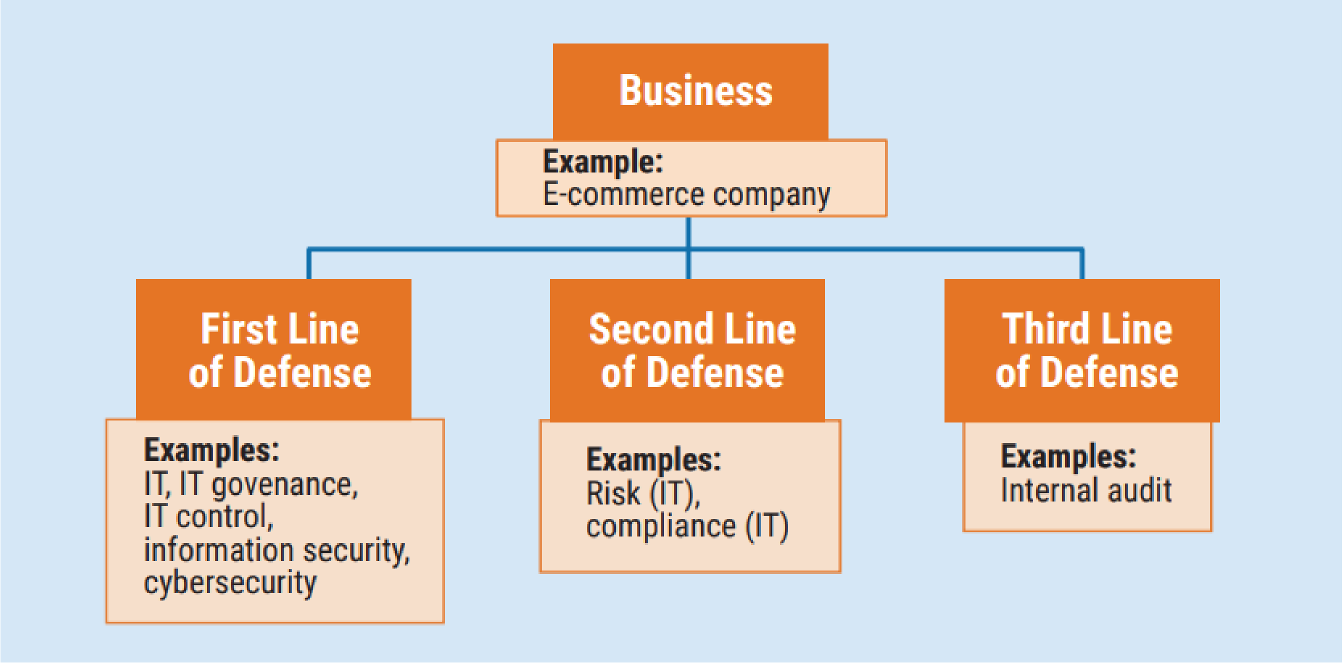
Examples:
Risk (IT), compliance (IT)

Third Line of Defense

Examples:
Internal audit

Ho (2018), https://www.isaca.org/resources/isaca-journal/issues/2018/volume-4/roles-of-three-lines-of-defense-for-information-security-and-governance

Figure 1—Three Lines of Defense



Business

Example:
E-commerce company

First Line of Defense

Examples:
IT, IT govenance,
IT control,
information security,
cybersecurity

Second Line of Defense

Examples:
Risk (IT),
compliance (IT)

Third Line of Defense

Examples:
Internal audit

First LoD is the function that **owns** and **manages** risk. Within the first LoD, businesses can set up control functions (e.g., IT control, which reports to the IT department) to faciliate the management of risk.

Second LoD is the independent control function (e.g., IT risk, IT compliance) that **oversees risk** and **monitors the first LoD controls**. They can challenge the effectiveness of controls and management of risk across the organisation.

Third LoD is **internal audit**, which **provides independent assurance**. It provides the *well-informed sense of assurance* that the risks and controls are in balance. It provides evidence, that risks and controls are in balance. They evaluate how effective the other two lines of defense are. How effective are our controls, how effective is our risk management.

Owners and Key Activities of the First Line of Defense

- Operational managers that own and manage risks and controls
- Implement corrective actions to address process and control deficiencies

Common first line of defense activities:

- Administer security **procedures**, **training**, and **testing**
- Maintain secure device **configurations**, up-to-date software, and **security patches**
- Deploy intrusion **detection systems** and conduct **penetration testing**
- Securely configure the **network** to adequately manage and protect network traffic flow
- **Inventory** information assets, technology devices, and related software
- Deploy **data protection** and loss prevention programs with related **monitoring**
- Restrict least-privilege **access roles**
- **Encrypt** data where feasible
- Implement **vulnerability management** with internal and external scans
- **Recruit** and retain certified IT, IT risk, and information security talent

Owners and Key Activities of the Second Line of Defense

- **IT risk management** and **IT compliance** functions
- Play key role in an organisation‘s security posture and program design
- Responsible for:
  - Cybersecurity-related risk assessment and alignment with organisation‘s risk appetite
  - Monitoring risks and changes to laws and regulations
  - Collaborating with the first-line functions to ensure appropriate control design

Owners and Key Activities of the Second Line of Defense

Common Second Line of Defense Activities:

- **Design** cybersecurity policies, training, and testing
- Conduct cyber **risk assessments**
- Gather cyber threat **intelligence**
- Classify data and design least-privilege **access roles**
- **Monitor incidents**, key risk indicators, and remediation
- Recruit and retain certified IT risk talent
- **Assess relationships** with third parties, suppliers, and service providers
- Plan/test business continuity and participate in disaster recovery exercises

Owners and Key Activities of the Third Line of Defense

- **Internal audit function** assesses whether IT governance supports organisation‘s strategies and objectives
- Coordinates with second LoD, particularly cybersecurity function
- Can be consulted regarding:
  - The relationship between cybersecurity and organisational risk
  - Prioritizing responses and control activities
  - Auditing for cybersecurity risk mitigation across all relevant facets (e.g., privileged access)
  - Assurance in remediation activities
  - Raising risk awareness and coordinating with cybersecurity risk management
  - Validating that cybersecurity provisions are included in the organisation‘s business continuity plans

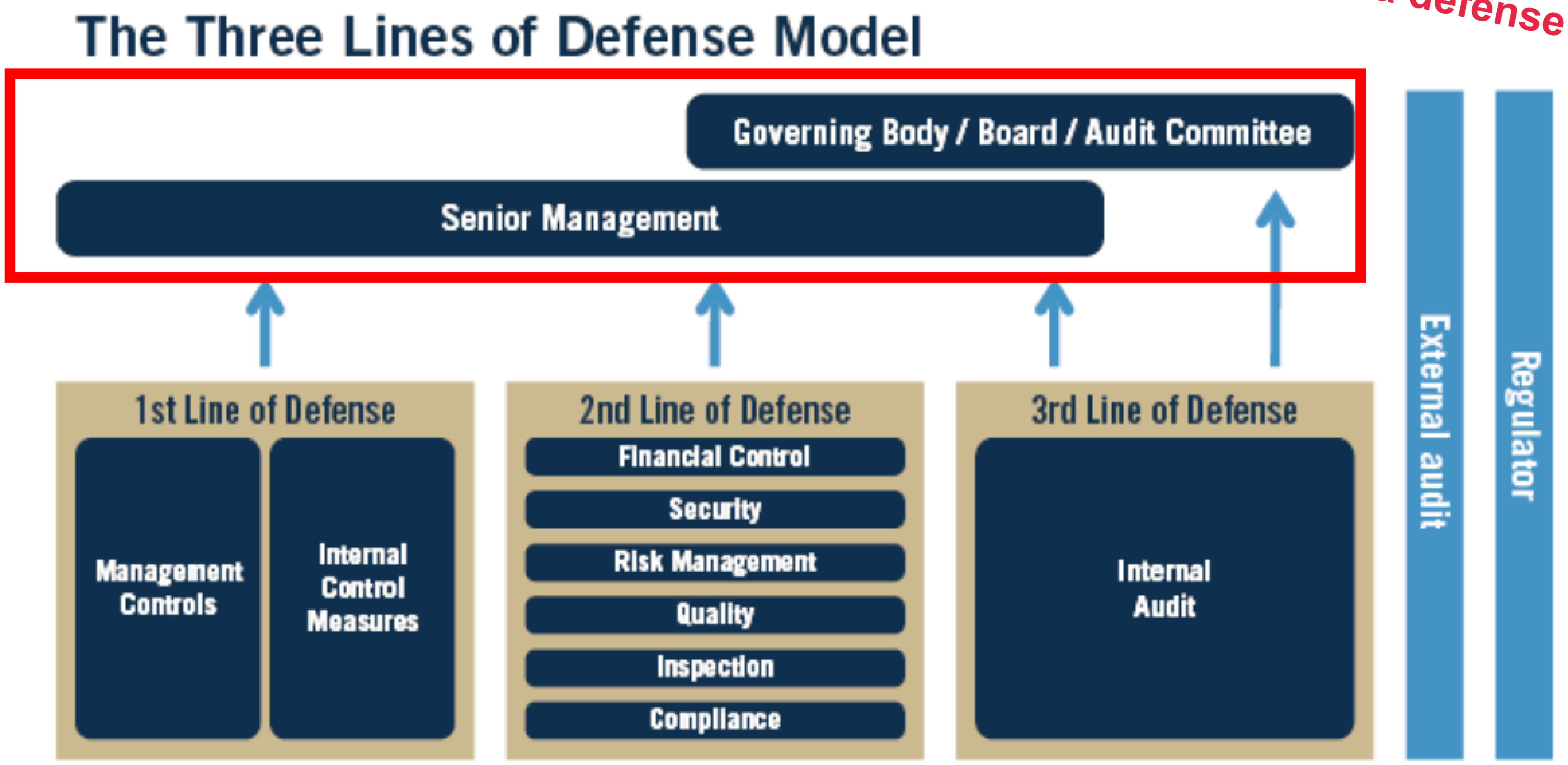
Owners and Key Activities of the Third Line of Defense

Common Third Line of Defense Activities

- Provide independent **ongoing evaluations** of preventive/detective measures related to cybersecurity
- **Evaluate IT assets** of users with privileged access for standard security configurations
- **Track diligence** of remediation
- **Conduct cyber risk assessments** of service organisations, third parties, and suppliers

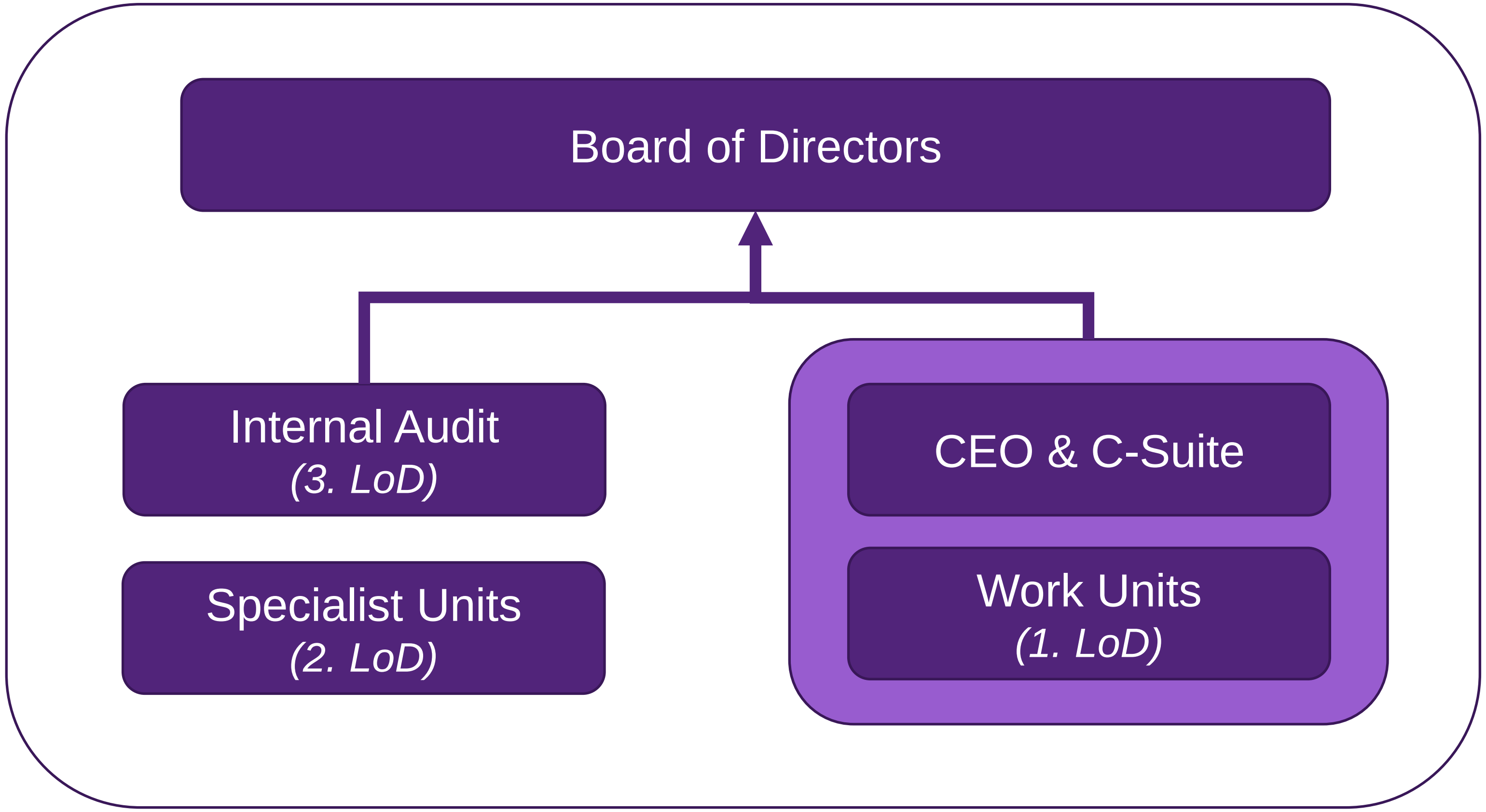
General 3LoD

Problem: Senior management and board of directors are not considered to be a part of a defense line!



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

Overview of Five Lines of Assurance Model (5LoA)



Board of Directors

Internal Audit
(3. LoD)

Specialist Units
(2. LoD)

CEO & C-Suite

Work Units
(1. LoD)

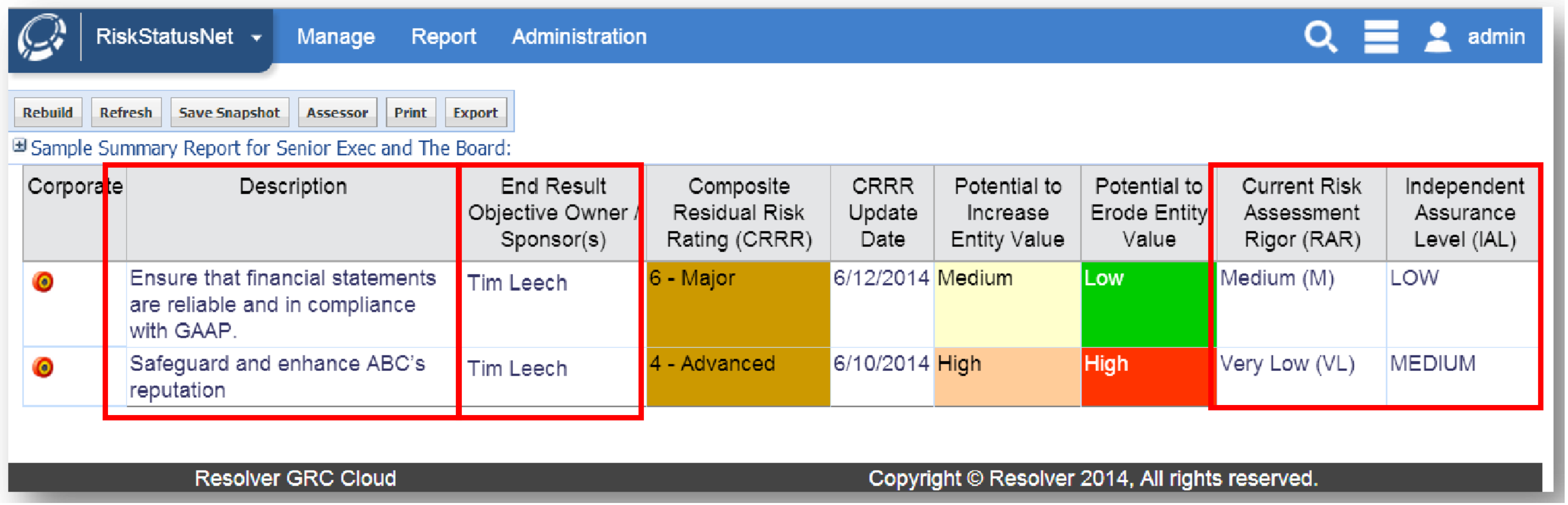
Overview of Five Lines of Assurance Model (5LoA)

- The word "defense" has a sort of negative feel to it. Risk managers are often seen as the "office of no" but risk avoidance as we will see is only one form of treating risk
- So moving away from this negative stereotype the people who promoted this model, wanted the risk management unit to be seen as a function that has potential to help management to increase the certainty that key objectives in an organisations will be obtained, while still operating within an acceptable level of risk. So here it is about assurance, about value-creation objectives rather than preventing value erosion
- How to make sure value is created with appropriate risk levels rather than focusing on avoiding risks at all costs

So, the 5LoA model significantly elevates two roles. The role of CEOs and the role of the Boards of Directors in risk governance - the C-Suite (everyone with a C or Chief in the title, e.g. CIO, CISO, CRO etc.

Core Elements of 5LoA

- Uses an "objectives register" as a foundation *(see figure below)*
- Clear accountability on who is responsible for reporting on residual risk status
- Risk assessment rigour and independent assurance requirements defined by C-suite and the board



⊞ Sample Summary Report for Senior Exec and The Board:

Corporate	Description	End Result Objective Owner / Sponsor(s)	Composite Residual Risk Rating (CRRR)	CRRR Update Date	Potential to Increase Entity Value	Potential to Erode Entity Value	Current Risk Assessment Rigor (RAR)	Independent Assurance Level (IAL)
●	Ensure that financial statements are reliable and in compliance with GAAP.	Tim Leech	6 - Major	6/12/2014	Medium	Low	Medium (M)	LOW
●	Safeguard and enhance ABC's reputation	Tim Leech	4 - Advanced	6/10/2014	High	High	Very Low (VL)	MEDIUM

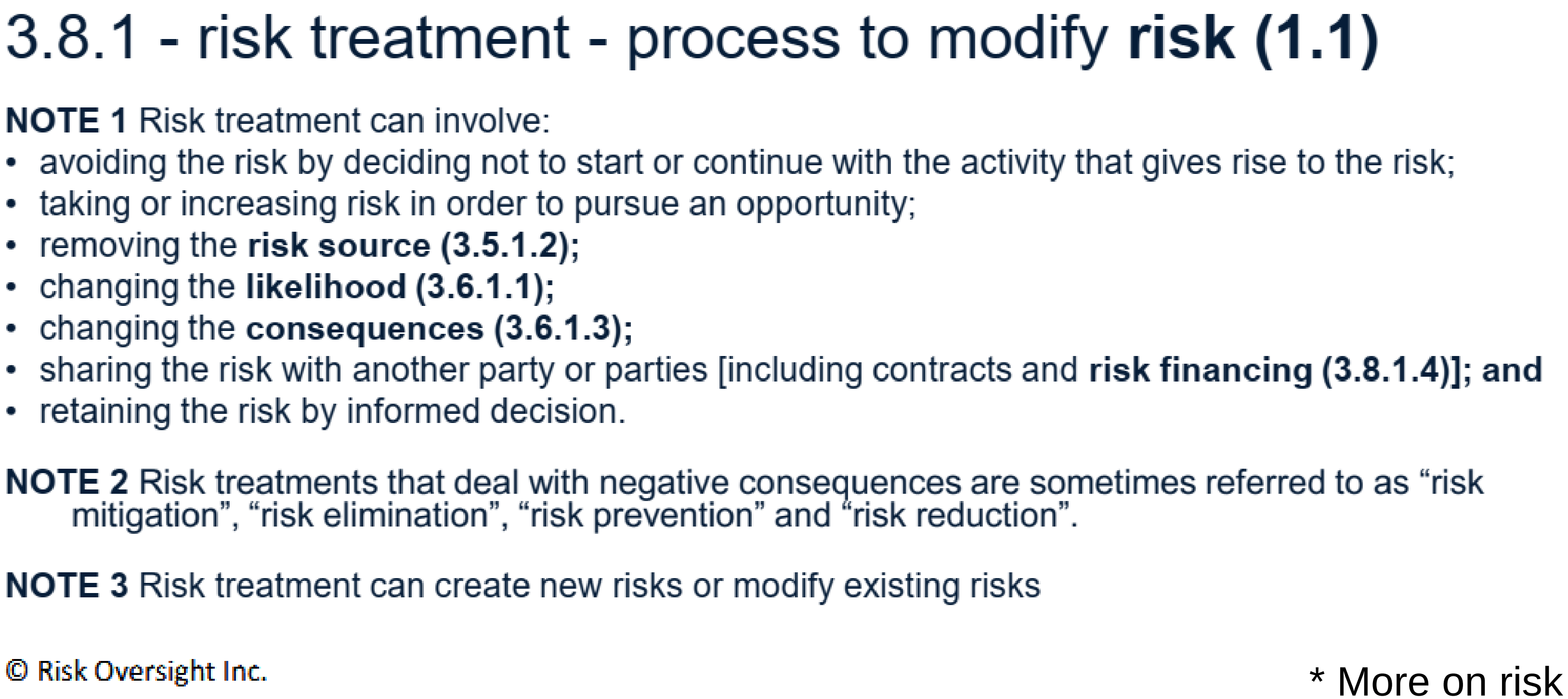
Resolver GRC Cloud

Core Elements of 5LoA

Active board/senior management involvement and clarity around their responsibility as the “ultimate line of defence“

Core Elements of 5LoA

Requires the full range of risk treatments* be identified and assessed not just “internal controls“



3.8.1 - risk treatment - process to modify **risk (1.1)**

NOTE 1 Risk treatment can involve:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing risk in order to pursue an opportunity;
- removing the **risk source (3.5.1.2);**
- changing the **likelihood (3.6.1.1);**
- changing the **consequences (3.6.1.3);**
- sharing the risk with another party or parties [including contracts and **risk financing (3.8.1.4)]; and**
- retaining the risk by informed decision.

NOTE 2 Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.

NOTE 3 Risk treatment can create new risks or modify existing risks

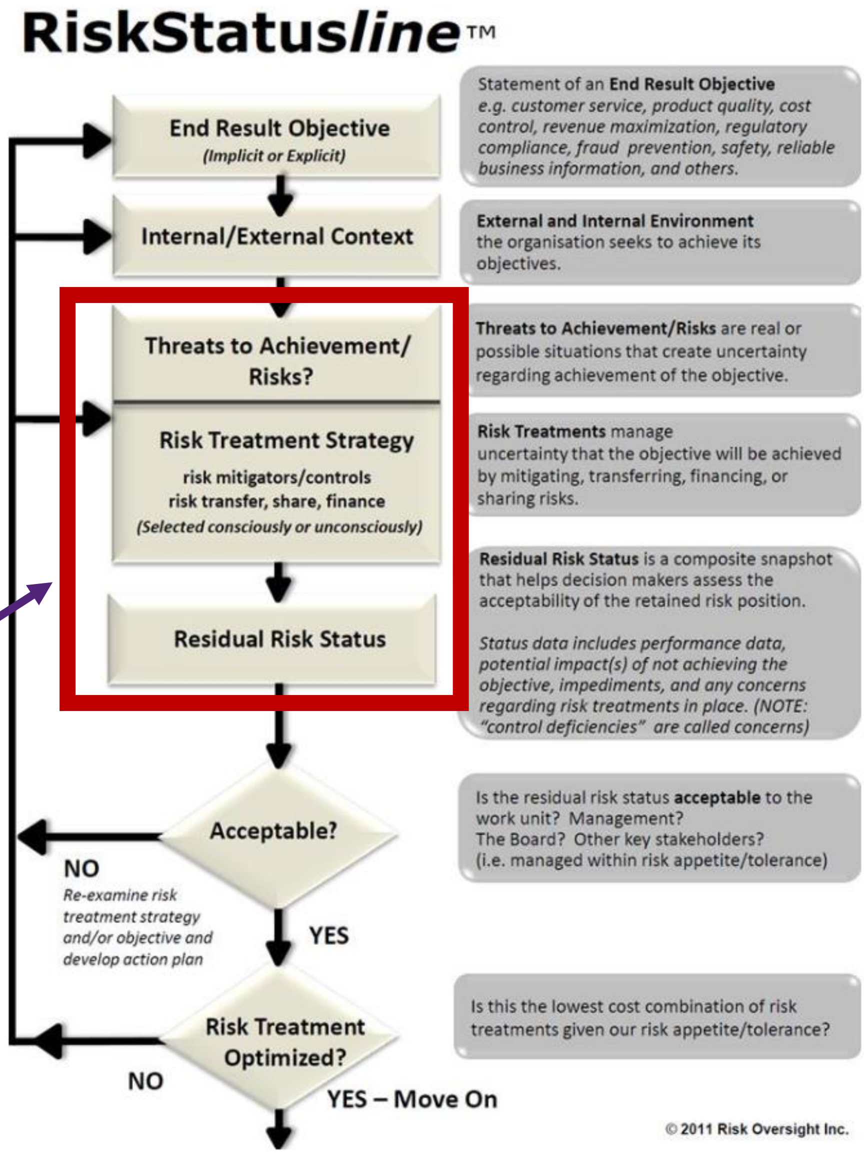
© Risk Oversight Inc.

* More on risk treatment in our risk management (part 2) module

Core Elements of 5LoA

- Primary focus is on the acceptability of residual risk status
- Specific consideration whether risk treatments are optimized

Risk Assessment and Risk Treatment will be our focus in the next two weeks.



RiskStatus*line*™

End Result Objective
(Implicit or Explicit)

Statement of an **End Result Objective** *e.g. customer service, product quality, cost control, revenue maximization, regulatory compliance, fraud prevention, safety, reliable business information, and others.*

Internal/External Context

External and Internal Environment the organisation seeks to achieve its objectives.

Threats to Achievement/ Risks?

Threats to Achievement/Risks are real or possible situations that create uncertainty regarding achievement of the objective.

Risk Treatment Strategy
risk mitigators/controls
risk transfer, share, finance
(Selected consciously or unconsciously)

Risk Treatments manage uncertainty that the objective will be achieved by mitigating, transferring, financing, or sharing risks.

Residual Risk Status

Residual Risk Status is a composite snapshot that helps decision makers assess the acceptability of the retained risk position.

Status data includes performance data, potential impact(s) of not achieving the objective, impediments, and any concerns regarding risk treatments in place. (NOTE: "control deficiencies" are called concerns)

Acceptable?

NO
Re-examine risk treatment strategy and/or objective and develop action plan

YES

Is the residual risk status **acceptable** to the work unit? Management? The Board? Other key stakeholders? (i.e. managed within risk appetite/tolerance)

Risk Treatment Optimized?

NO

YES – Move On

Is this the lowest cost combination of risk treatments given our risk appetite/tolerance?

© 2011 Risk Oversight Inc.

And no, you don't self-isolate for two weeks if you're infected.

```
                end;                   func, std::vect
            write(Endtext);
        end.
        CREATE TABLE product(
            class MultinomialNB(object):
            def __init__(self):
        2})
                self.X = None
                self.y = None
            def __loading(self):
                self.list_labels = cl.Counter(se
        int acc(std::function<int(int, int)> fun
            auto it = operands.begin();
            int result = func(*it, *(++it));
            if (operands.size() > 2) {
                for (++it; it!=operands.end(); +
                    result = func(result, *it);
                }
            }
            return result;     CDog& operator=(C
```

Thank you