CMP4103
Computer Systems and Network Security

CISSP®

Diarmuid Ó Briain

CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

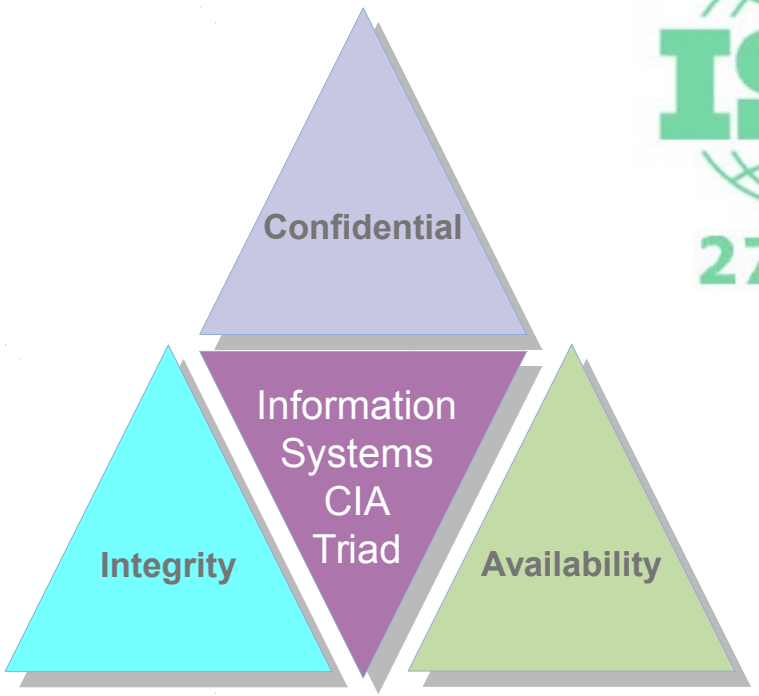
Course sections

- Lecture set 1 — Information Security, Governance & Risk Management
- Lecture set 2 — Security Architecture and Design
- Lecture set 3 — Cryptography
- Lecture set 4 — Physical Security and Access Control
- Lecture set 5 — Virtualisation
- Lecture set 6 — Systems: Threats, Vulnerabilities and Risks
- Lecture set 7 — Secure Software Development
- Lecture set 8 — Network Security and Penetration Testing
- Lecture set 9 — Project Management
- Lecture set 10 — Legal, Regulations, Investigations and Compliance
- Lecture set 11 — Business Continuity and Disaster Recovery Planning
- Lecture set 12 — Operations Security

ITIL
The IT Infrastructure Library

OGC

ISO
27000



COSO
COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

OGC

ISO 27000

Management Frameworks

COBIT

COSO

CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

ITIL
The IT Infrastructure Library

Management Frameworks

A management system is the framework of processes and procedures used to ensure that an organisation can fulfil all tasks required to achieve its objectives.

ISO/IEC 27000

- Information Security Management System (ISMS):
  - ISO/IEC 27000-series

27001	Information Security Management System (ISMS) Requirements
27002	Code of practice for Information Security
27003	Information Security Management – System implementation guidance
27004	Information Security Management – Measurement
27005	Information Security Management – Risk management
27006	Guidelines for Information Security Management – Systems auditing

- This is an evolving list with new 27000 series standards being added to take account of changing needs, for example 27017 covers Information security management for cloud systems.

ISO/IEC 27001 – Management Requirement

- Systematic examination of the organisation's information security risks, taking account of the threats, vulnerabilities and impacts.

- Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that it deems unacceptable.

- Adopt an overarching management process to ensure that the information security controls continue to meet the organisation's information security needs on an ongoing basis.

ISO/IEC 27001 Controls

- Controls – Management and Operational

Management	Context of the Organisation
	Leadership
	Planning
	Support
	Operation
	Performance evaluation
	Improvement

Operational	Management direction for information Systems
	Organisation of Information Security
	Human Resource Security
	Asset Management
	Access Control
	Cryptography
	Physical and Environmental Security
	Operations Security
	Communications Security
	System acquisition, Development and Maintenance
	Supplier relationships
	Information Security Incident Management
	Information Security aspects of Business Continuity
	Compliance

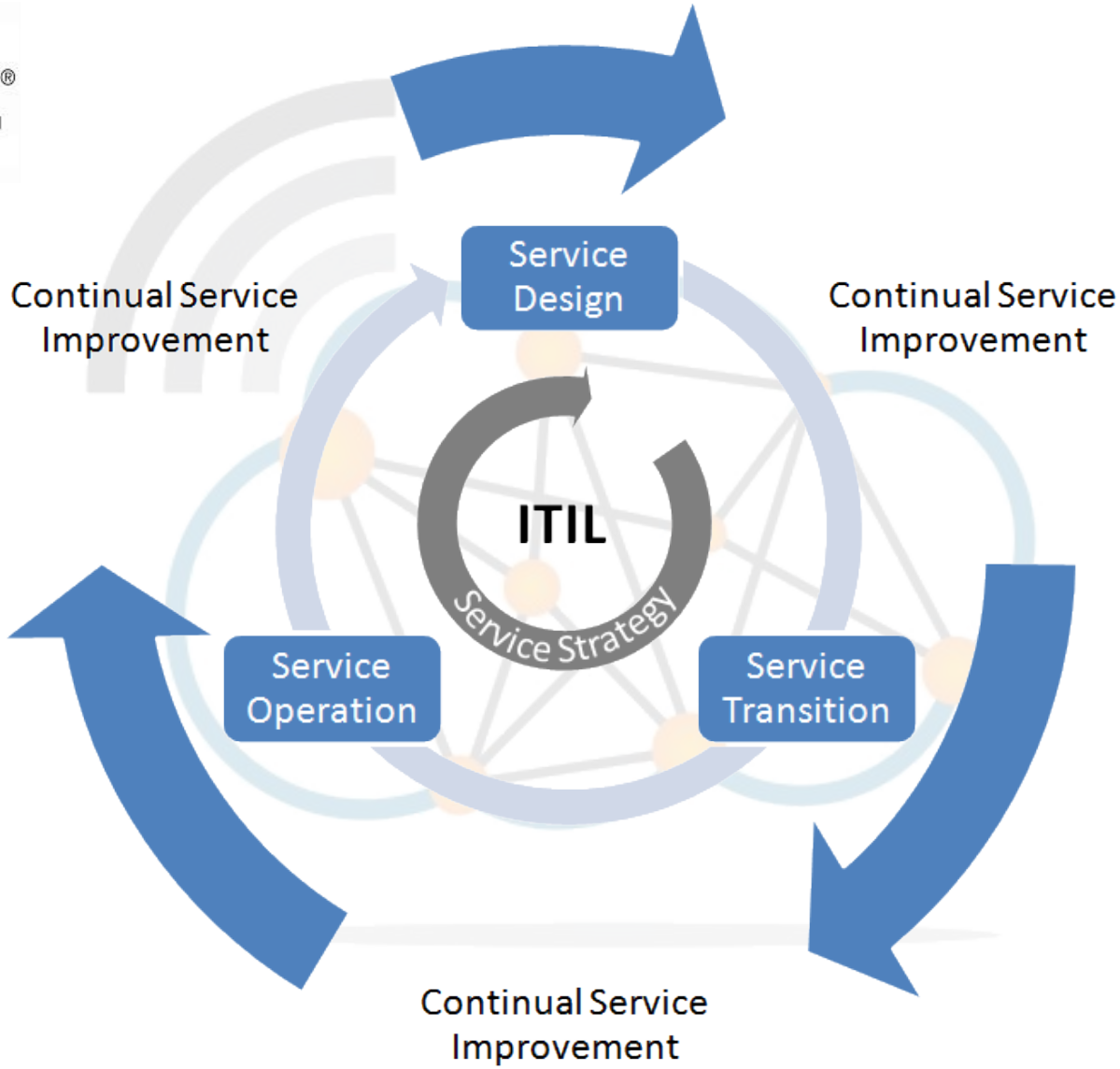
Implementation stages for ISMS

- Define Information Security Policy
- Define scope of ISMS
- Perform risk assessment
- Manage risks
- Select controls
- Prepare statement of applicability

IT Infrastructure Library (ITIL)

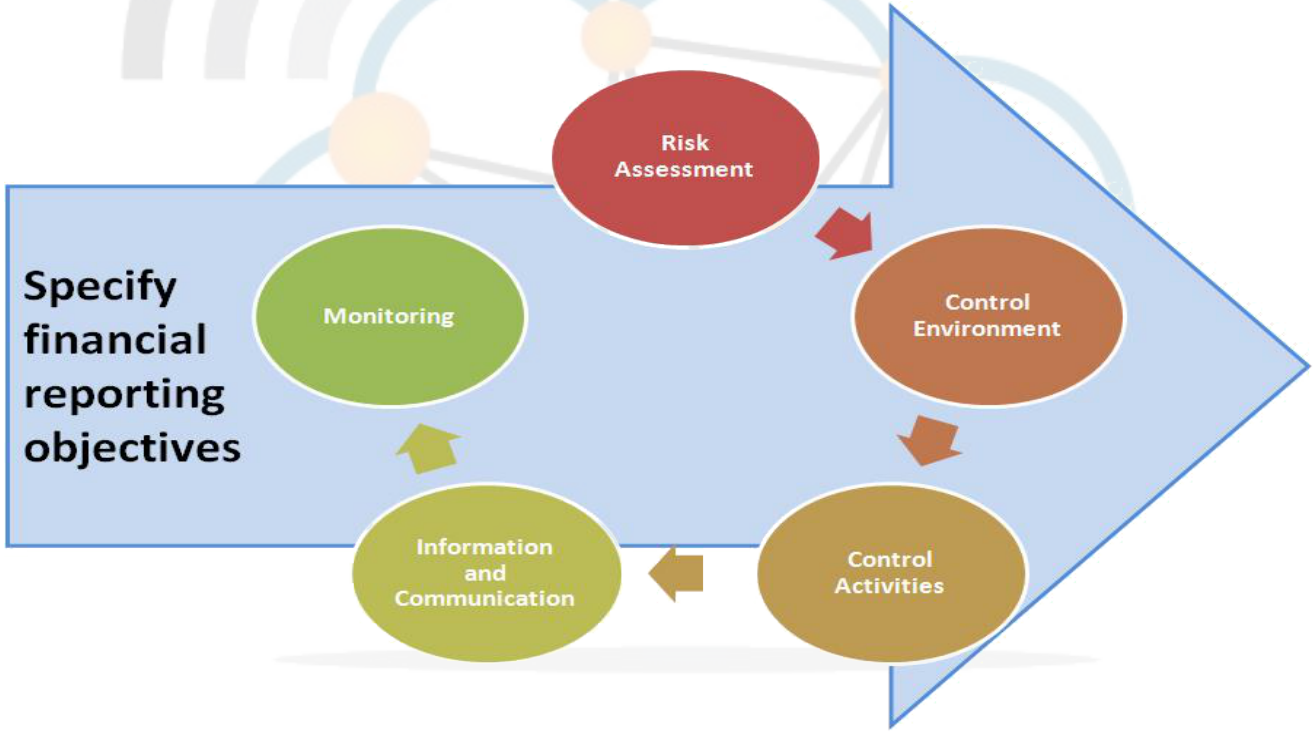
- Information Technology Infrastructure Library (ITIL)
  - UK Office of Government Commerce (OGC).
- Set of concepts and policies for:
  - Management
  - Administration
  - Development
  - Operation
- Library sections
  - Service Strategy
  - Service Design
  - Service Transition
  - Service Operation
  - Continual Service Improvement

IT Infrastructure Library (ITIL)



Committee of Sponsoring Organisations (COSO)

- Committee of Sponsoring Organisations of the Treadway Commission (COSO)
- Enterprise Risk Management Integrated Framework



COSO ERM Objectives

The four objective categories are:

- **Strategy**
  - High-level goals, aligned with and supporting the organisation's mission
- **Operations**
  - Effective and efficient use of resources
- **Financial Reporting**
  - Reliability of operational and financial reporting
- **Compliance**
  - Compliance with applicable laws and regulations

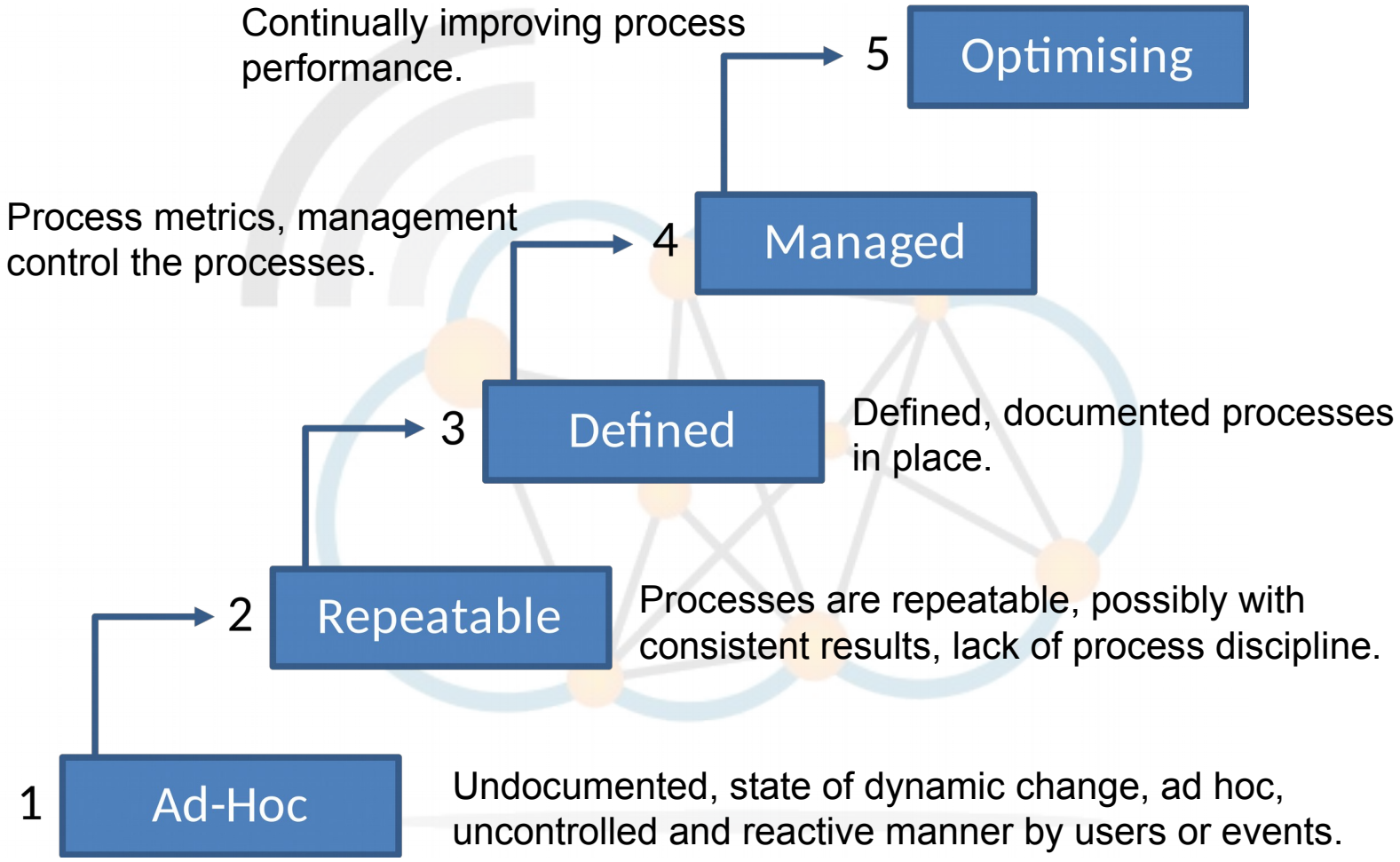
COSO ERM Components

- Internal Environment
- Objective Setting
- Event Identification
- Risk Assessment
- Risk Response
- Control Activities
- Information and Communication
- Monitoring

Capability Maturity Model

- CMM is a useful general theoretical model, to aid in the definition and understanding of an organisation's process capability maturity.
- For software development, the CMM has been superseded by Capability Maturity Model Integration (CMMI).

Capability Maturity Model



Capability Maturity Model Integration

- **CMMI for Acquisition**
  - Designed for businesses that focus on working with suppliers to assemble a product or deliver a service.
- **CMMI for Development**
  - Designed for businesses that focus on developing products and services.
- **CMMI for Services**
  - Designed for businesses that focus on working with suppliers to assemble a product or deliver a service.

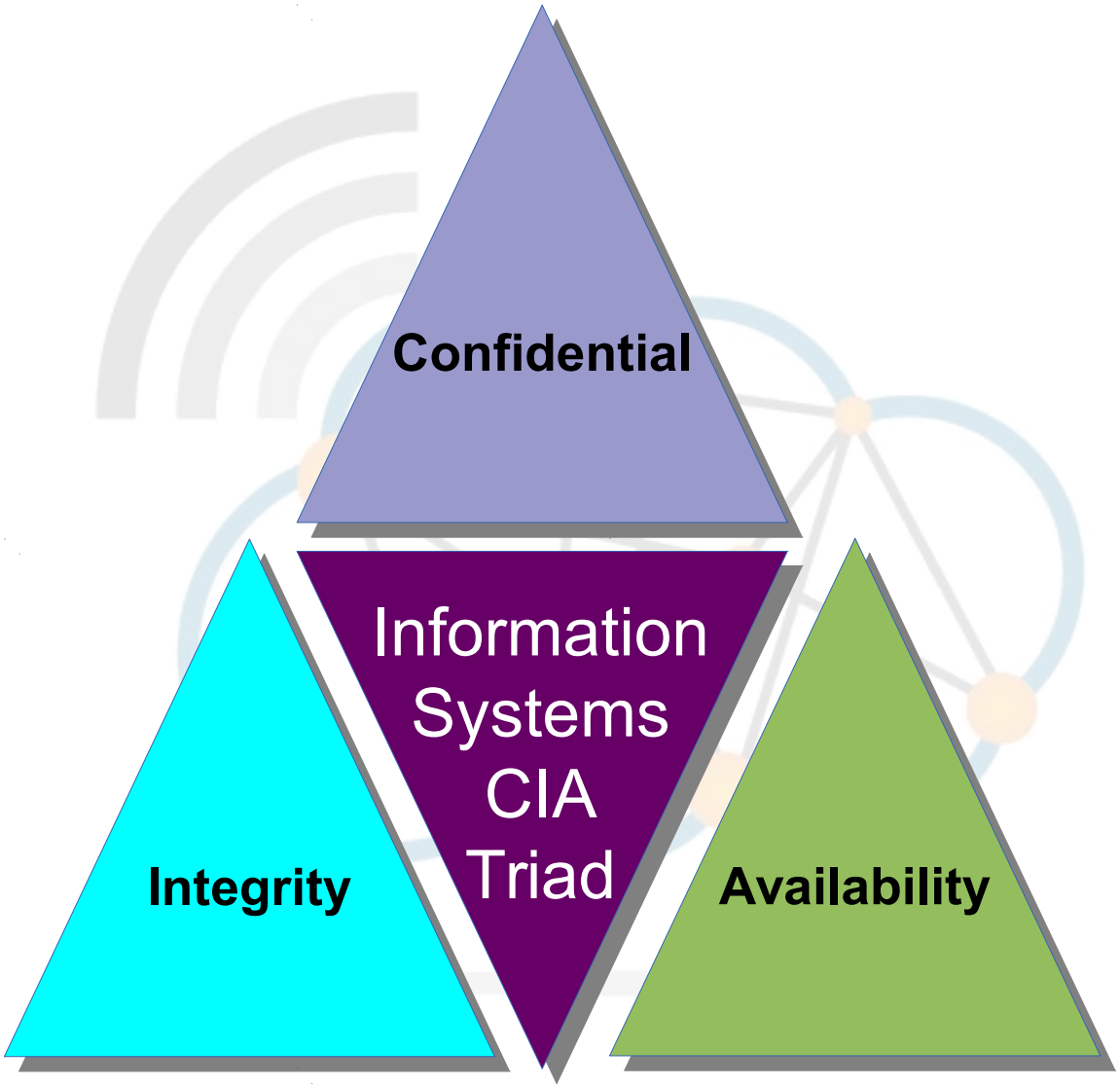
Information Security

CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

CIA Triad

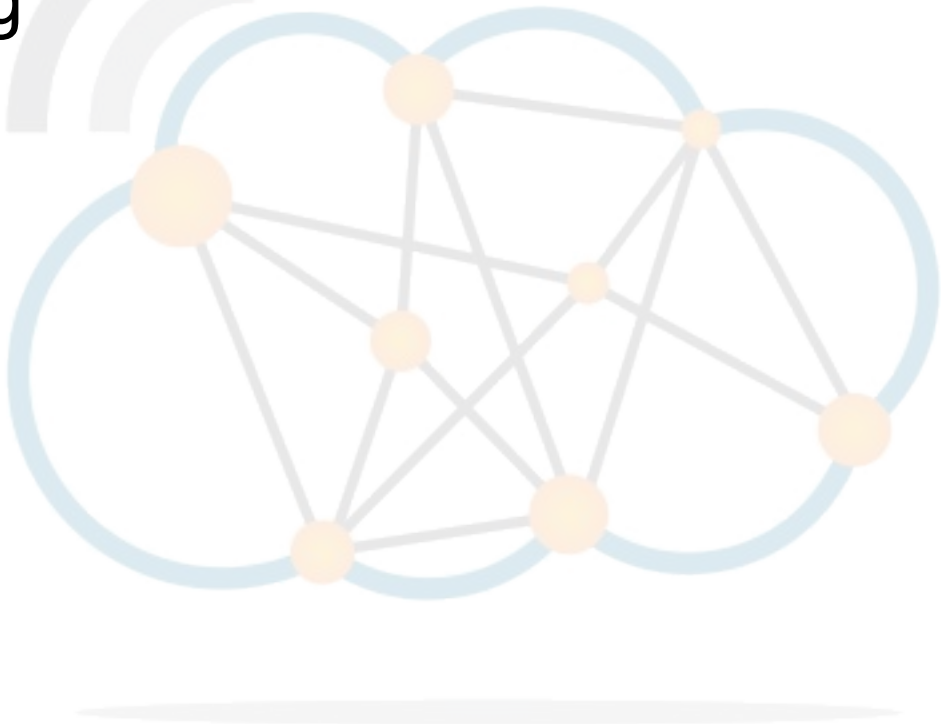

Confidential
Information Systems CIA Triad
Integrity
Availability

Other security concepts

- Privacy
  - Prevention of unauthorised access
  - Freedom from being observed or monitored without consent
- Identification
  - Subjects present their Identification before access is permitted
- Authentication
  - Subjects claimed Identification is valid
- Authorisation
  - Subjects claimed Identification is valid and they are permitted access to a specific object
- Auditing
  - Subjects held accountable for their actions
- Accountability
  - Subjects held accountable for their actions
- Non-repudiation
  - Subject cannot deny the event occurred

Protection mechanisms

- Defence in depth
- Abstraction
- Data hiding
- Encryption



Change control process

- Record/classify
- Assess
- Plan
- Build/test
- Implement
- Close / Gain acceptance

Data Classification

- Data Classification
  - Assign a level of sensitivity to data as it is being created, amended, enhanced, stored, or transmitted
- Classification
  - Determines how data is controlled / secured
  - Indicative of its value in terms of Business Assets
  - Differentiate little value, highly sensitive and confidential
- When data is stored, whether received, created or amended, it should always be classified into an appropriate sensitivity level

Military Classification Scale

- Top Secret
- Secret
- Confidential
- Restricted
- Sensitive But Unclassified (SBU) US only
- Unclassified

Commercial Data Classification Scale

- Confidential
- Private
- Sensitive
- Public

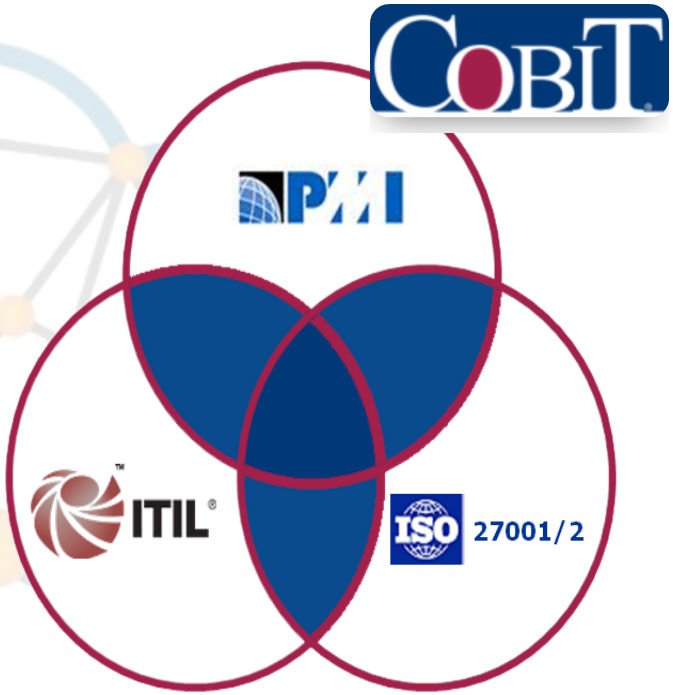
Control Objectives for Information & related Technology (CobiT)

ISACA®
Trust in, and value from, information systems

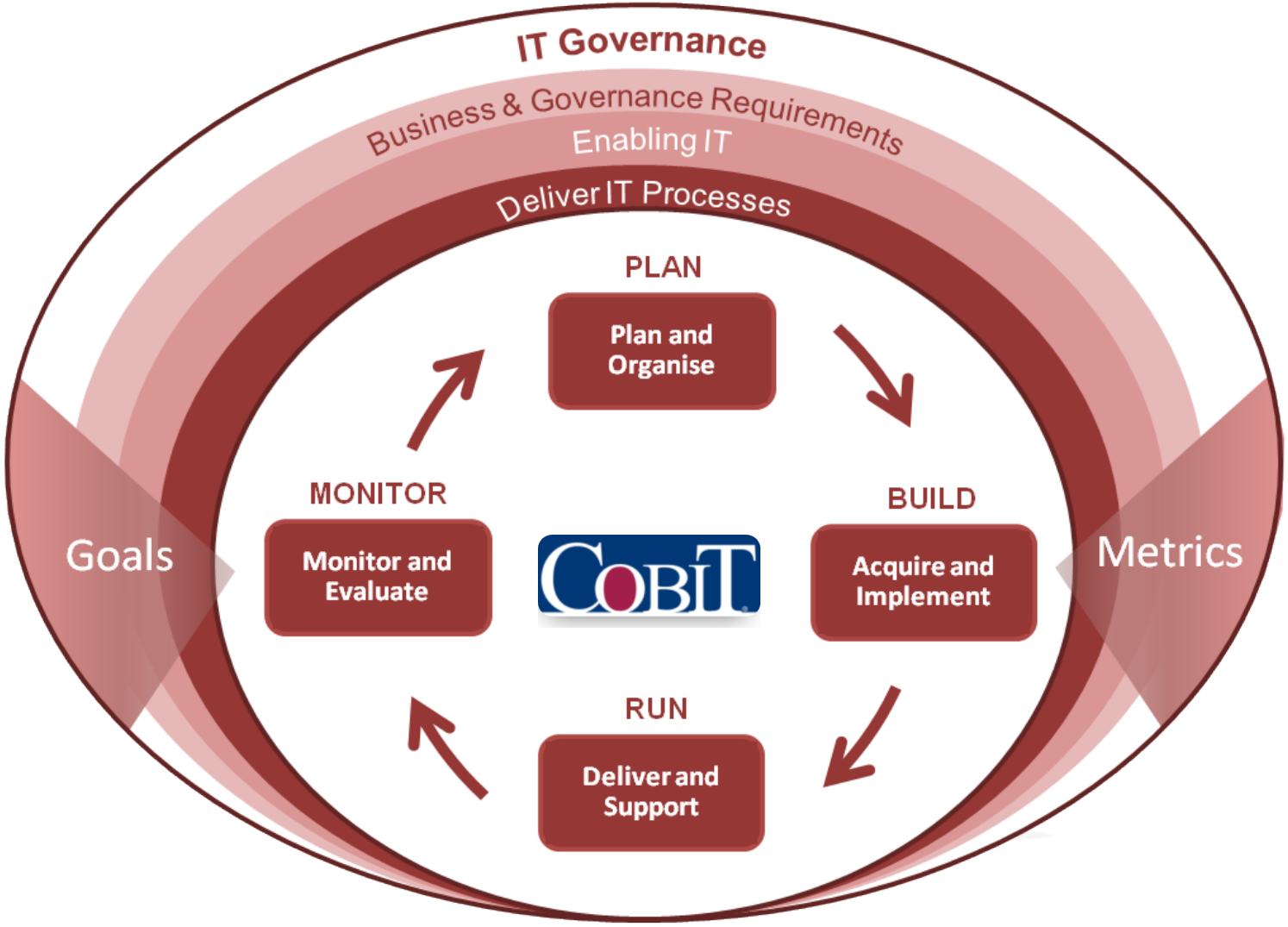
IT GOVERNANCE INSTITUTE®

- CobiT is a framework for IT management
- Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI)
- CobiT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to develop IT governance and control in a company

CobiT IT Governance



CobiT IT governance framework



Employment
Policies and Practices

CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Hiring new staff

- Creating a Job Description
- Setting a classification for the job
- Screening candidates
- Hiring and Training the selected candidate

Job description

- The Job Description should contain the following:
  - Separation of Duties (SoD)
  - Job Responsibilities
  - Job Rotation
  - Knowledge Redundancy

Screening and background checks

- Group exercise

- You are taking on a new employee after an interview process

  - What checks do you think are important ?

Screening and background checks

- Verification of academic credentials
- Discussions with business, professional, and personal references and verify references
- Drug screens and physical medical exams
- Testing to confirm skills and knowledge
- Internet Search
- Criminal background checks
- Credit Checks

Employee agreements

- Group exercise

- You have decided to employ someone after a lengthy process and have completed your background checks

  - What checks do you think are important elements of the employee agreement ?

Employee agreements

- The job position
- Whether the position can be changed by the employer
- The length of the agreement
- The salary, bonus and benefits
- Whether the employee gets stock or stock options in the company
- When the employee can be terminated for good cause
- What "good cause" means in terms of the role
- When the employee can be terminated without good cause and what severance payment will be due
- The employee's job responsibilities
- The employee's confidentiality obligations
- Where and how disputes will be handled

Non Disclosure Agreements (NDA)

- An **NDA** is a contract signed by employees and/or 3rd parties agreeing not to disclose proprietary information to anyone outside the company.

- Prevents outside parties you're working with from revealing inside information with anyone else, or employees from using confidential information to benefit anyone other than your company.

- A **Non-compete Agreement** or Clause, is a term used in contract law under which an employee agrees not to pursue a similar profession or trade in competition against the employer.

Employee termination

- **Employee Termination** is the end of an employee's duration with an employer.
- Depending on the case, the decision may be made by the employee, the employer, or mutually agreed upon by both.
- It is essential to integrate IT into the process:
  - Prompt notification of termination
  - Prudent revocation of access
  - Pre-emptive Preservation of Data

Information Security Management

CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Security roles

- Senior Manager
- Security Professional
- Data Owner
- Data Custodian
- User
- Auditor

Security Management Planning

- Strategic Plan
  - Long term, horizon plan. It should include:
    - Goals
    - Missions
    - Objectives
    - Risk Assessment

Security Management Planning

- Tactical Plan
  - Medium term plan on how the Goals and Objectives of the Strategic Plan should be achieved. These include:
    - Project Plans
    - Acquisition Plans
    - Hiring Plans
    - Maintenance Plans
    - Support Plans
    - System Development Plans

Security Management Planning

- Operational Plan
  - Short term plans that are specific to actions being carried out to achieve Strategic and Tactical goals and objectives. The operational plans include:
    - Resource planning
    - Budgets
    - Staff Assignment
    - Implementation procedures

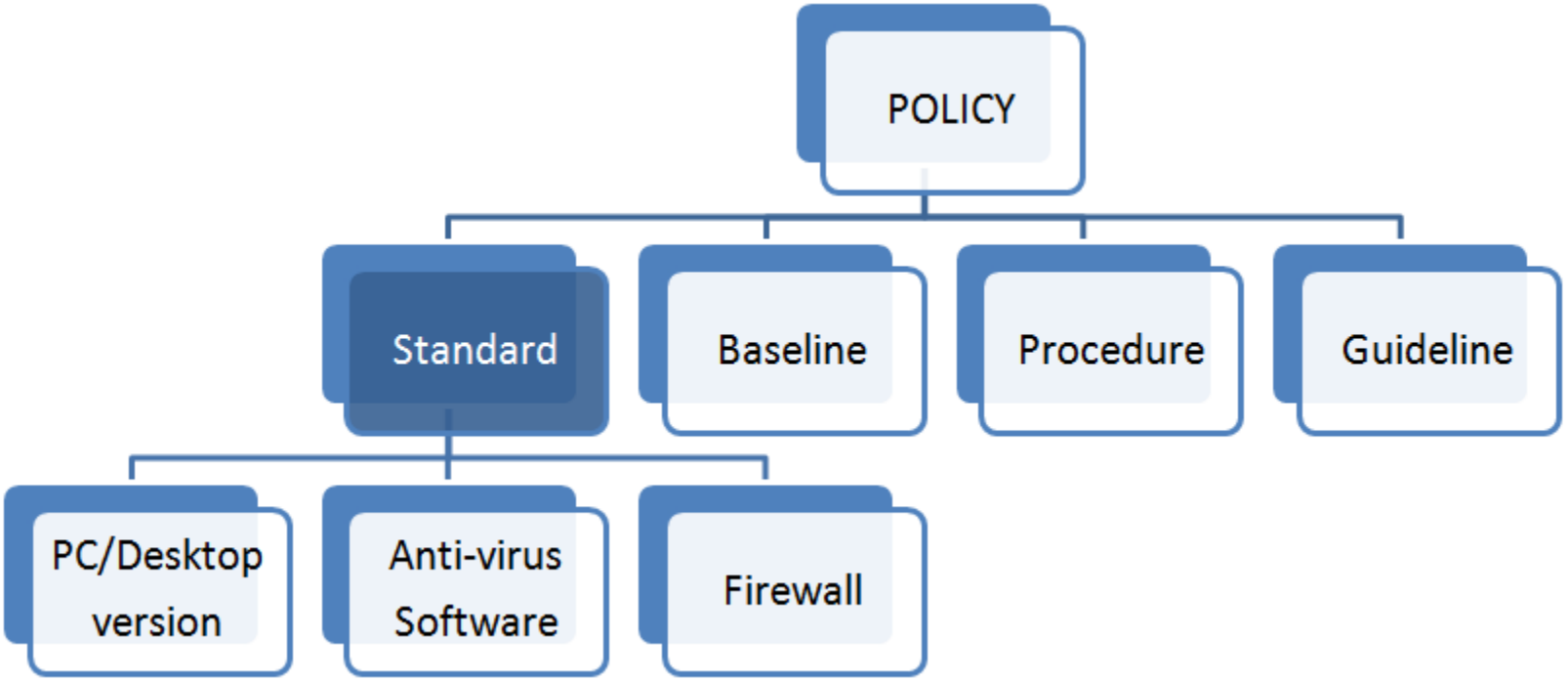
Information Security Documents

- **Policies**
  - high-level statements or rules about protecting people or systems.
- **Standards**
  - low-level prescription for the various ways the company will enforce the given policy.
- **Procedures**
  - step-by-step method to implementing various standards.

Information Security policy

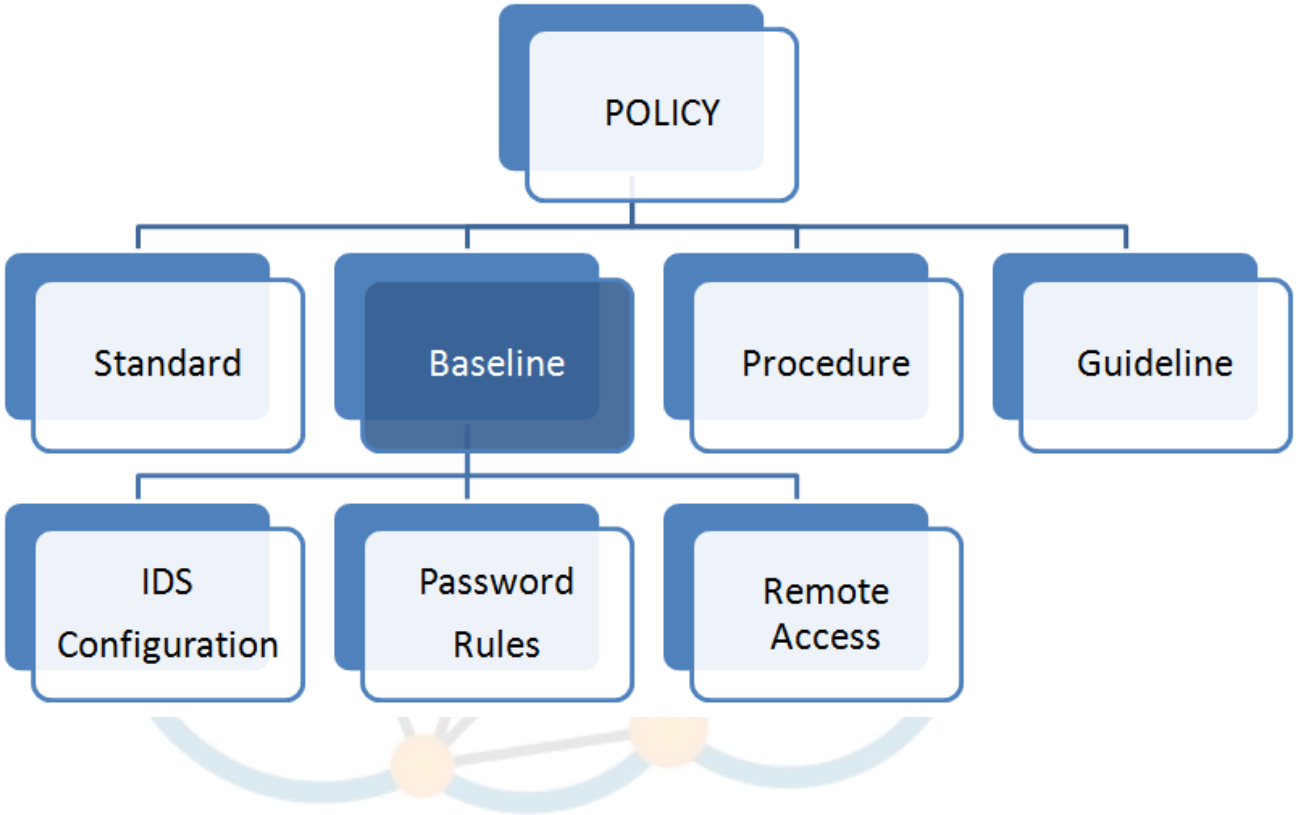
- Policies should include:
  - Title
  - Number
  - Author
  - Publish Date
  - Scope
  - Policy Text
  - Sanctions
  - Sponsor

Information Security standards



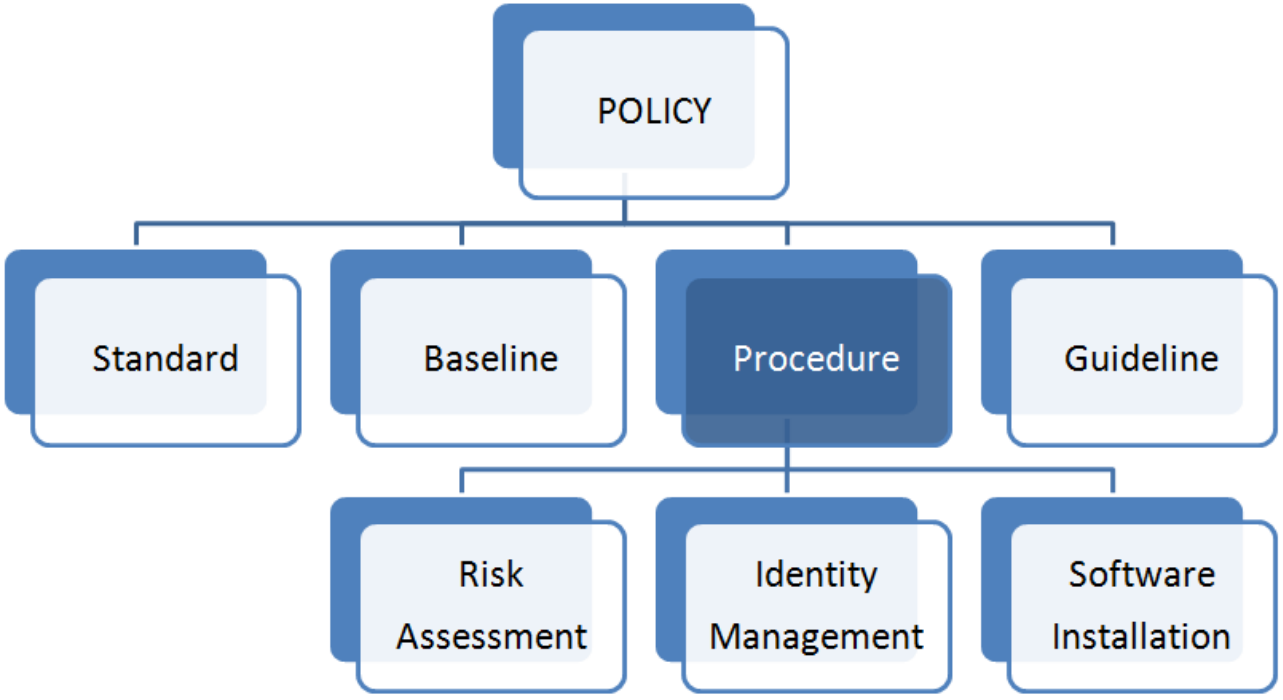
- Define compulsory requirements for use of equipment and software plus security controls.

Information Security baseline



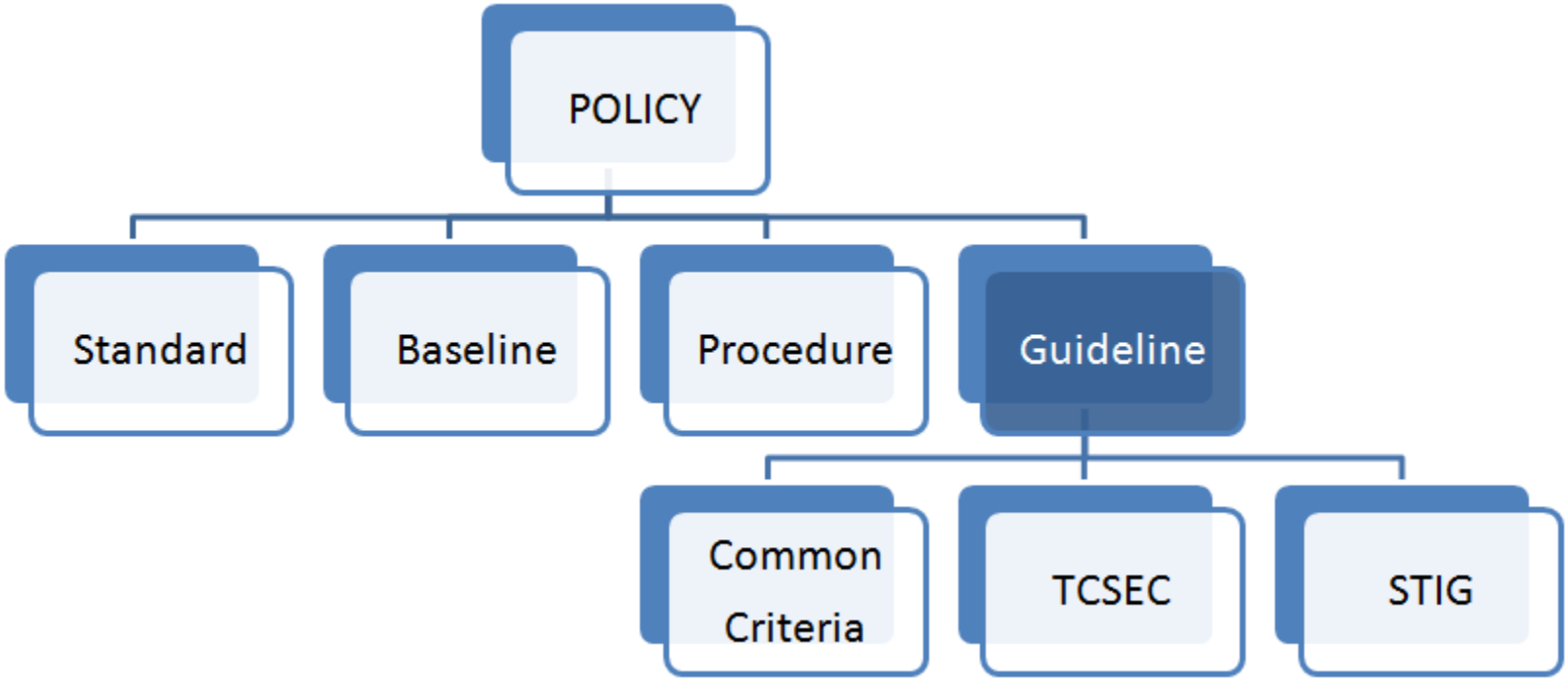
- Security Baselines are the minimum level of security that all organisations systems must meet.

Information Security procedures



- Security Procedures are detailed step by step documents that describe the exact actions to implement a security mechanism, control or solution.

Information Security guidelines



- Security Guidelines define how both standards and baselines should be implemented.
- Common Criteria, Trusted Computer System Evaluation Criteria (TCSEC) and Security Technical Implementation Guides (STIG).

Risk

CISSP®

Diarmuid Ó Briain

CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Risk

- Individual exercise
- In terms of a business
  - What do you consider to be **risk** ?

Risk Management

- What is Risk?

- Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organisation.

- THREAT → VULNERABILITY → IMPACT

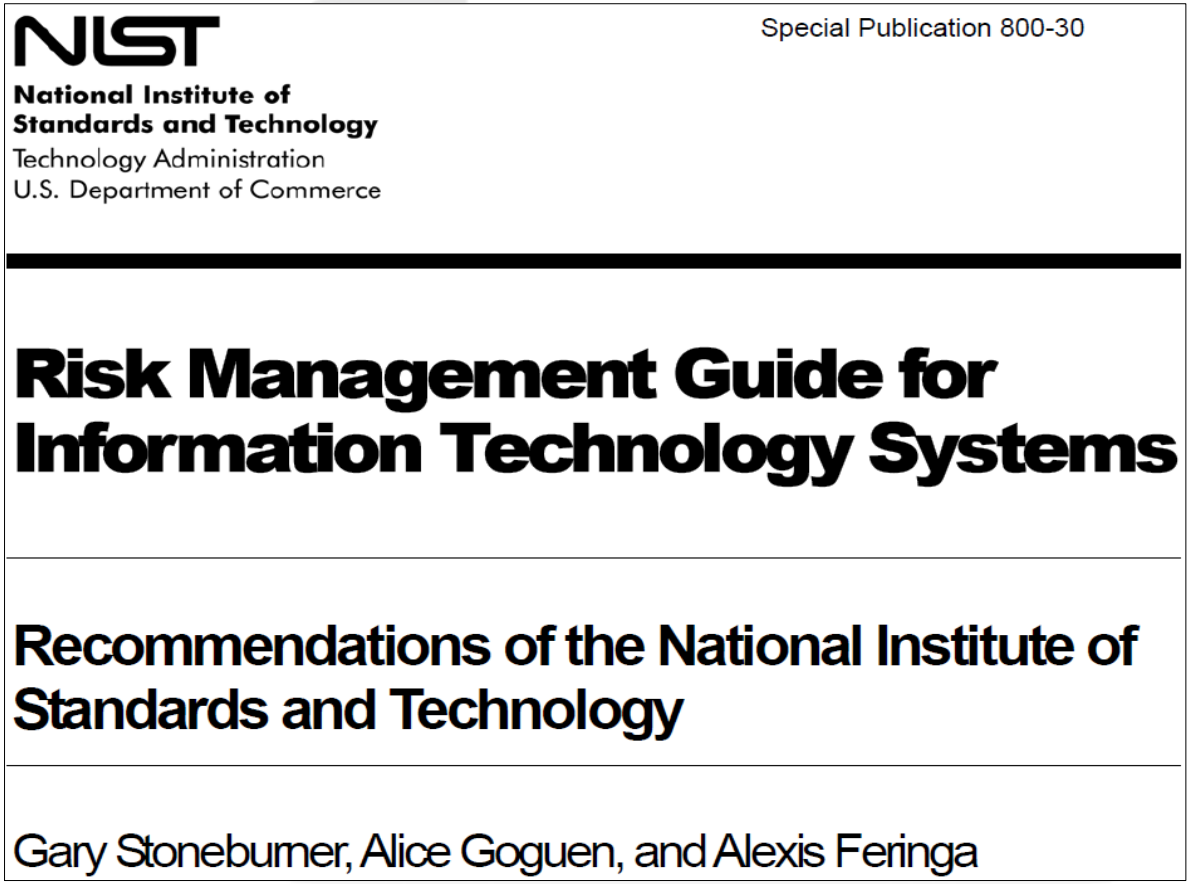
Risk Assessment Process

- Risk assessment is a process as opposed to a once off event.
- Technology and processes change, risk assessments need to be conducted periodically.
  - Phase 1: Preliminary Risk Assessment
  - Phase 2: Risk Analysis of Critical Areas and Processes
  - Phase 3: Organisation-Wide Risk Assessment

Risk Terminology

- Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organisation.

Risk Assessment



NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-30

Risk Management Guide for Information Technology Systems

Recommendations of the National Institute of Standards and Technology

Gary Stoneburner, Alice Goguen, and Alexis Feringa

NIST SP 800-30 - Methodology

- System Characterisation
- Thread Identification
- Vulnerability Identification
- Control Analysis
- Likelihood Determination
- Impact Analysis
- Risk Determination
- Control Recommendations
- Results Documentation

NIST SP 800-30 – Risk Mitigation

- Risk Assumption
- Risk Avoidance
- Risk Limitation
- Risk Planning
- Research and Acknowledgement
- Risk Transference

Risk Log

- Identify Risks.
- Perform Qualitative/Quantitative Risk Analysis.
- Plan Risk Responses.

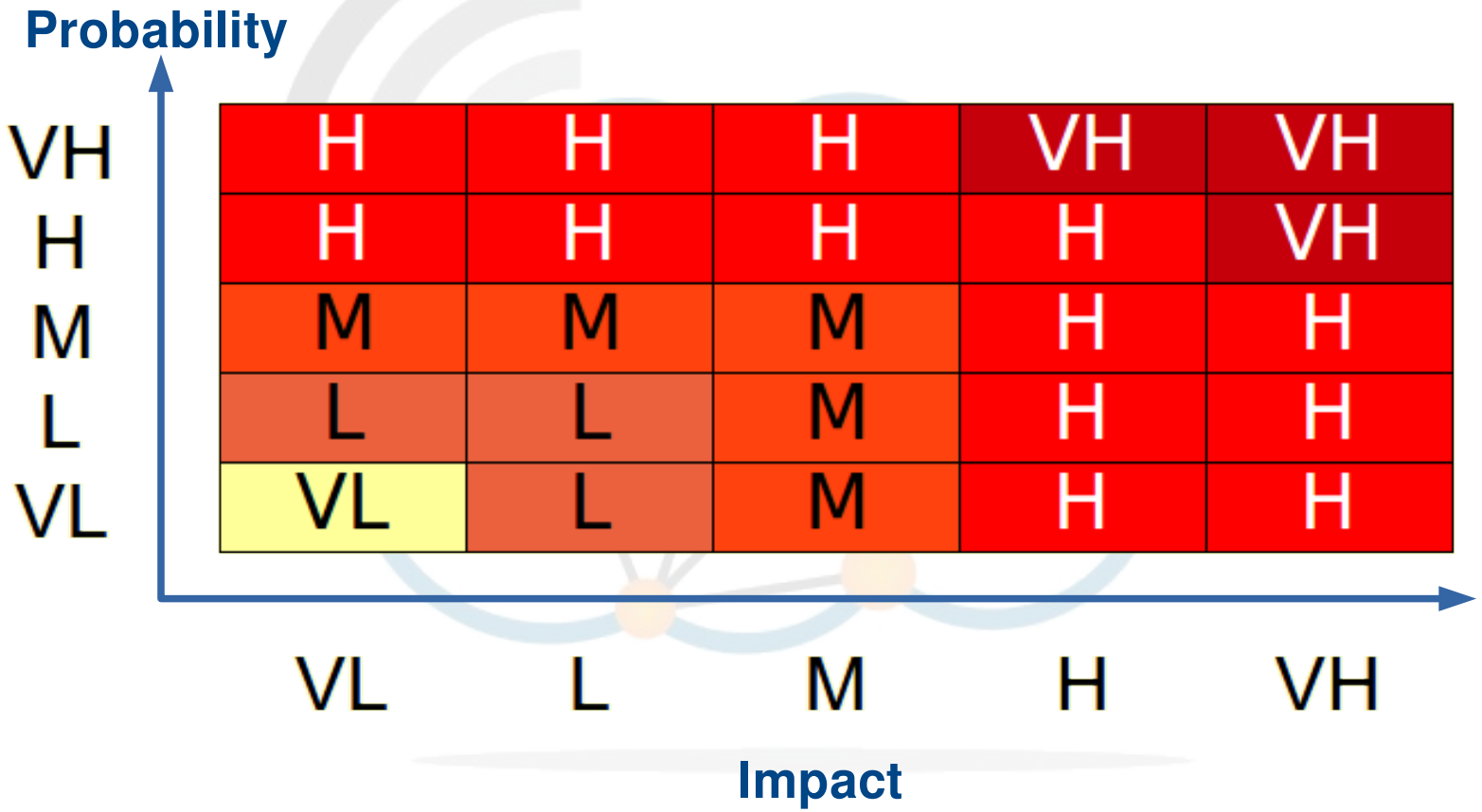
< Project title > RISK LOG

Summary			Description					Preventative Actions			Contingency Actions		
ID	Date Raised	Raised By	Description of Risk	Description of Impact	Probability Rating	Impact Rating	Priority Rating	Preventative Actions	Action Resource	Action Date	Contingency Actions	Action Resource	Action Date

VL = 'Very Low'
L = 'Low'
M = 'Medium'
H = 'High'
VH = 'Very High'

Risk Log

- Probability and Impact Matrix Tool



Risk Assessment

NIST Special Publication 800-39

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Managing Information Security Risk

Organization, Mission, and Information System View

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

March 2011

NIST SP 800-39

- Flagship document of the information security standards and guidelines.
- Provides guidance for an integrated, organisation-wide programme for managing information security risk to organisational operations, organisational assets, individuals and other organisations.
- Provides a structured, yet flexible approach for managing risk that has a broad base, with the specific details of assessing, responding to, and monitoring risk on an ongoing basis provided by other supporting NIST security standards and guidelines.

Quantitative Risk Analysis

- Quantitative risk analysis attempts to **assign monetary values** to the components of the risk assessment and to the assessment of the potential loss.
- Asset valuation
  - Value retained from the cost of creating the information asset
  - Value retained from past maintenance of the information asset
  - Value implied by the cost of replacing the information
  - Value from providing the information
  - Value acquired from the cost of protecting the information
  - Value to owners
  - Value of intellectual property
  - Value to adversaries
  - Loss of productivity while the information assets are unavailable
  - Loss of revenue while information assets are unavailable

Asset valuation

- An organisation must be able to place a dollar value on each information asset it owns, based on:
  - How much did it cost to create or acquire?
  - How much would it cost to recreate or recover?
  - How much does it cost to maintain?
  - How much is it worth to the organisation?
  - How much is it worth to the competition?

Exposure factor (EF)

- Loss Potential or the percentage of loss an organisation would realise if a risk was realised.

- **Single Loss Expectancy (SLE)**
  - The monetary value expected from the occurrence of a risk on an asset.
  - SLE = AV x EF
- **Annualised Rate of Occurrence (ARO)**
  - An estimate based on the data of how often a threat would be successful in exploiting a vulnerability.
- **Annualised Loss Expectancy (ALE)**
  - A calculation of the single loss expectancy multiplied the annual rate of occurrence, or how much an organisation could estimate to lose from an asset based on the risks, threats, and vulnerabilities. It is:
  - ALE = SLE x ARO
- **Annual Cost of Safeguard (ACS)**
  - This is the cost of the researched safeguard.
- **Cost Benefit Analysis (CBA)**
  - CBA determines whether or not a control alternative is worth its associated cost. CBAs may be calculated before a control or safeguard is implemented, to determine if the control is worth implementing, or calculated after controls have been implemented and have been functioning for a time:
  - CBA = (ALE(prior) – ALE(post)) – ACS

Performing a quantitative risk analysis

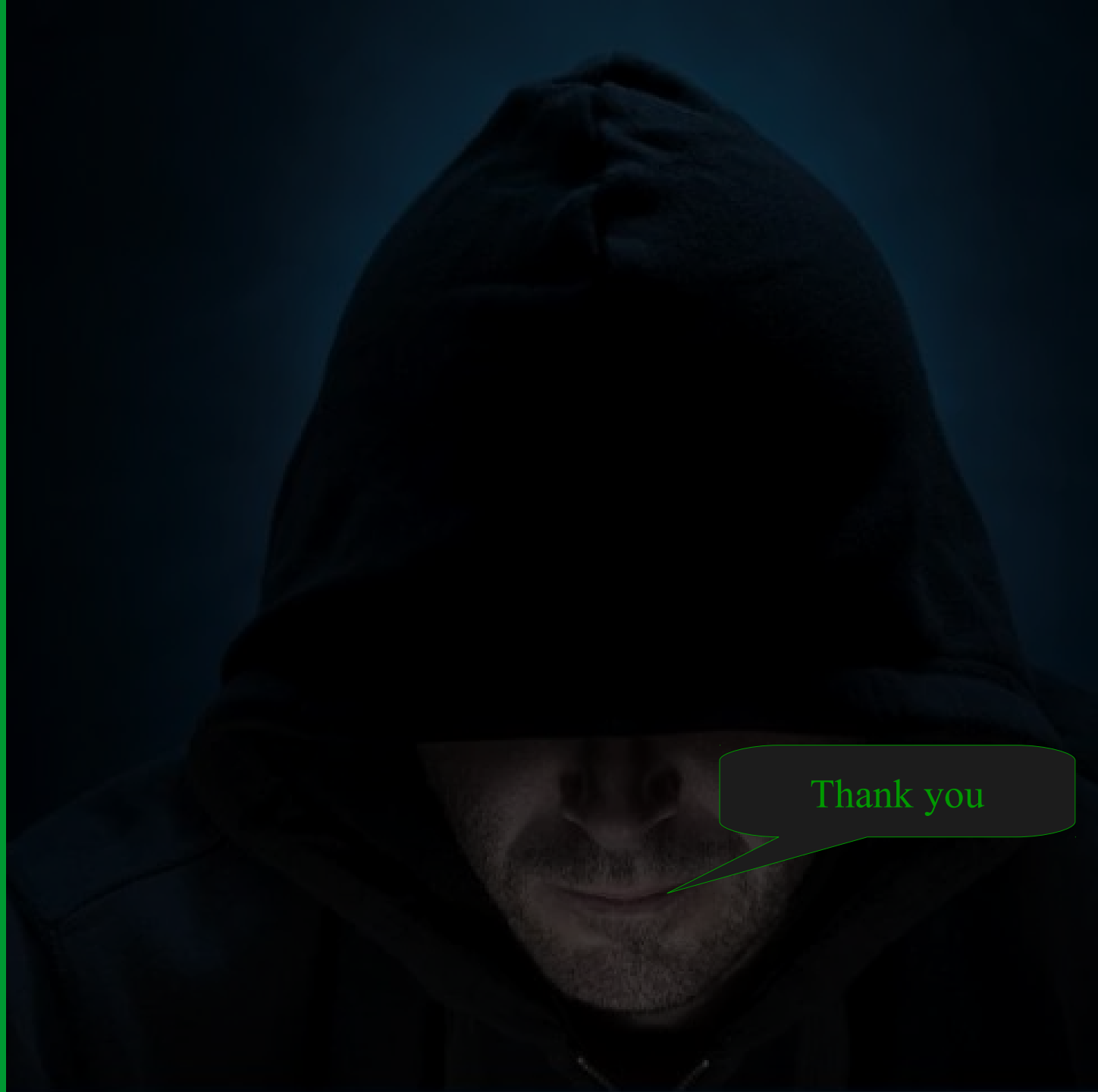
- Create an inventory of assets and assign a value [**Asset Value (AV)**].
- Conduct a risk assessment and vulnerability study to determine the risk factors for each asset. For each threat calculate the **Exposure Factor (EF)** and **Single Loss Expectancy (SLE)**.
- Perform threat analysis to determine the likelihood of the threat occurring in a single year – **Annualised Rate of Occurrence (ARO)**.
- Determine the **Annualised Loss Expectancy (ALE)** for each risk factor.
- Research **countermeasures** for each threat and calculate the change to the ARO and ALE if they were deployed.
- Perform a **Cost/Benefit Analysis (CBA)** of the countermeasures and choose the most appropriate response to each threat.

Qualitative Risk Analysis

- Relative measure of risk or asset value based on ranking or separation into descriptive categories such as low, medium, high; not important, important, very important; or on a scale from 1 to 10.
- Techniques used to assess the risk and produce a Risk Registrar.
  - Brainstorming
  - Delphi Technique
  - Storyboarding
  - Focus Groups
  - Surveys
  - Questionnaires
  - Check Lists
  - Interviews

Delphi Technique

- Systematic, interactive forecasting method which relies on a **panel of experts**.
  - The experts answer questionnaires in two or more rounds.
  - After each round, a facilitator provides an anonymous summary of the experts' forecasts from the previous round as well as the reasons they provided for their judgements
  - Experts are encouraged to revise their earlier answers in light of the replies of other members of their panel.
  - During this process the range of the answers will decrease and the group will converge towards the "correct" answer.
  - Process is stopped after a pre-defined stop criterion (e.g. number of rounds, achievement of consensus, stability of results) and the mean or median scores of the final rounds determine the results.



Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Class Assignment

You have been selected to act as the Chief Information Security Officer (CISO) for an firm called "***Mtoto Lishe Limited***" established in Ntinda, Nakawa, Kampala who have recently been formed to exploit research from the Makerere University College of Health Sciences (CHS) on baby food. The company was recently added to the Uganda Securities Exchange (USE) with a symbol of MTOL and the company has been valued at Ugx 8 billion.

This discovery from CHS is considered a commercial secret and the information is sought after for commercial purposes by a number of pharmaceutical firms from around the world.

As part of the Senior Management Team (SMT) you have been tasked to:

- Assist with the selection of an appropriate management framework to deal with sensitive data.
- Develop a mind-map to outline the policies, standards, baselines, procedures and guidelines necessary for the Information Security Management System (ISMS).
- Perform a high level risk assessment for company data.
- Determine an appropriate data classification system for the company.
- Define an appropriate Information Security organisation for the company,
- Organisation chart.
- Assist Human Resources (HR) with appropriate interview and potential employee selection criteria.