# Information security management, standards and compliance.

Ali E. Abdallah
Professor of Information Security
Birmingham City University
Email: Ali.Abdallah@bcu.ac.uk

# Lectures are part of the project:

## ConSoLiDatE
## Multi-disciplinary Cooperation for Cyber Security, Legal and Digital forensics Education

Funded by

The Higher Education Academy

December 2014-March 2016

BIRMINGHAM CITY University

Queen Mary University of London

# Digital evidence: high profile cases

## Phone Audit trail

**Senior Surrey Police officers probed over Dowler hacking** BBC

-


NEWS OF THE WORLD

UK / 28 June 2012

… admitted **hacking** the 13-year-old's mobile **phone** but it remains unknown whether two missing **messages** were **deleted** deliberately, as previously suggested,…

## Phone Audit trail

**Denham 'crash for cash' men jailed for Baljinder Gill death** BBC

London / 15 February 2013

Three **men** who deliberately caused a car **crash** that led to another collision in which a woman died have been **jailed**. **Baljinder Gill** died when her

# Digital evidence: high profile cases

## Audit?

**Hezbollah suspects to be tried over Rafik Hariri Murder** BBC

Middle East / **17 August 2011**

… **evidence** from **phone** records, an indictment says . Lebanon has not been able to arrest the men, who will**be tried** in absentia. **Hezbollah** leader...

## Can you trust the integrity of your Audit?

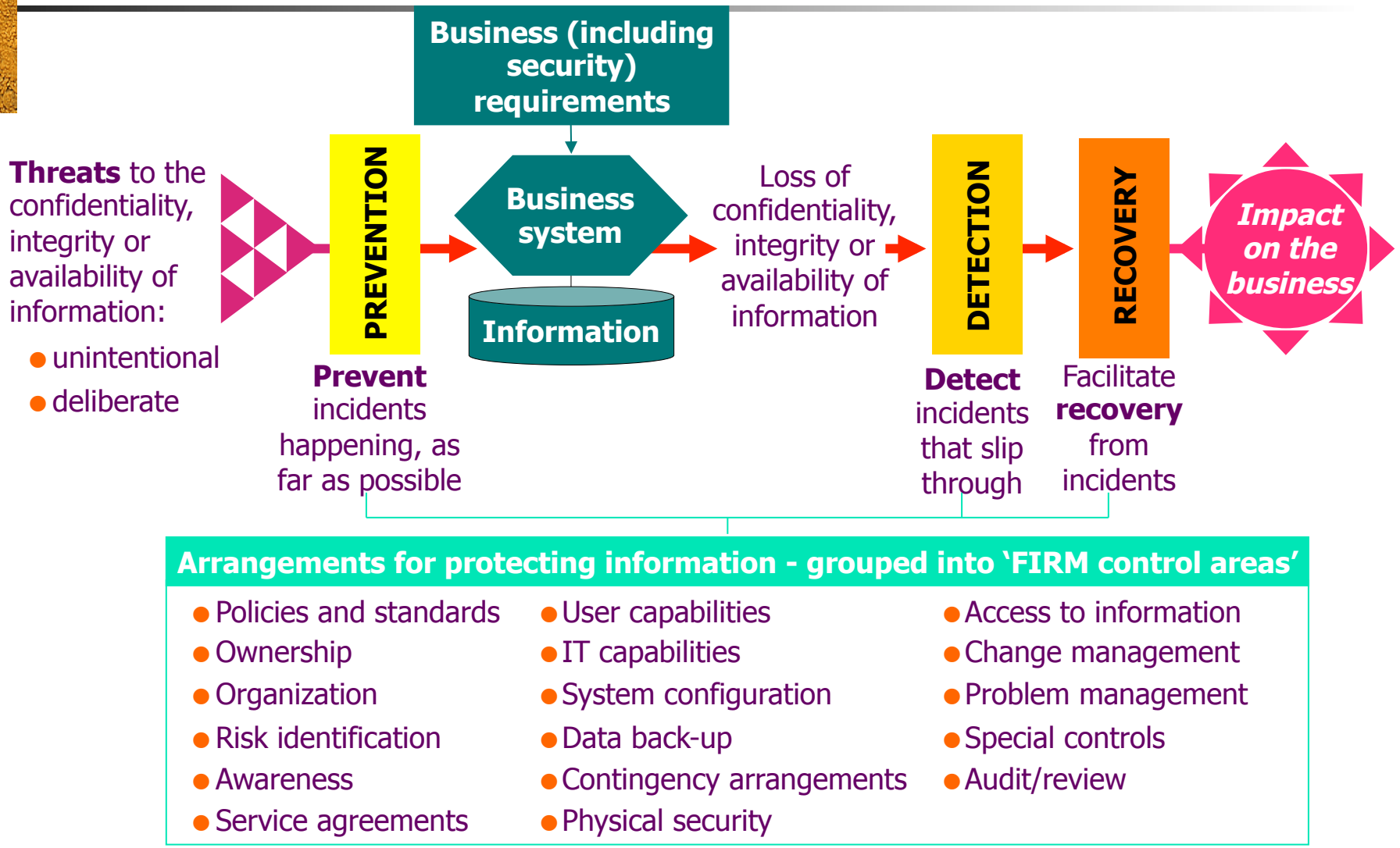
**Israel Prisoner X: Ben Zygier 'leaked Mossad secrets'** BBC


Middle East / **18 February 2013**

… **spy** agency because it believed he had leaked secrets.. **Israel** secretly imprisoned an **Australian** man who worked for its **Mossad spy** agency because…

It said he set up a communications company in Europe for Mossad, which exported electronic components to Arab countries and Iran.

# Getting information risk under control



# Questions

- What good practices are available to manage information security?
- What are ISO 27000s family of standards?
- What are the objectives of ISO 27001?
- What are certification, accreditation and compliance about?

# Overview

- Introduction
  - History, structure and concepts
    - BS 7799, ISO 17799 and ISO 27001
  - Information Security Management Systems
  - The meaning of Compliance, and the value of Certification
  - Motivation – legal, regulatory and other drivers
  - Understanding and meeting Real World Business Objectives
  - Approaches to Compliance, tools and some pitfalls
- Summary and Questions

# Brief History

## BS 7799 Part 2 (now ISO 27001) has always been a 'management system' standard

| | |
|---|---|
| 1993 | DTI Code of Practice for Information Security Management |
| 1995 | Code of Practice for Information Security Management (BS 7799-1:1995) |
| 1999 | Code of Practice for Information Security Management (BS 7799-1:1999) |
| 1999 | Specification for Information Security Management Systems (BS 7799-2:1999) |
| 2000 | Code of Practice for Information Security Management (BS ISO / IEC 17799:2000) |
| 2002 | Information Security Management Systems – Specification with guidance for use (BS 7799-2:2002) |
| 2005 | Code of Practice for Information Security Management (BS ISO / IEC 17799:2005) |
| 2005 | Information Security Management Systems – Requirements (BS ISO / IEC 27001:2005) |

# ISO 27000 family of standards

27000: Principles and Definitions

- 27001: (formerly BS7799-2) *(Nov 2005)*
- 27002: (formerly BS7799-1 / ISO17799) *(June 2007)*
- 27003: Implementation Guidelines *(Dec 2008)*
- 27004: ISMS Metrics and Measurement *(Dec 2009)*
- 27005: Risk Management (BS7799 part 3) *(2010)*

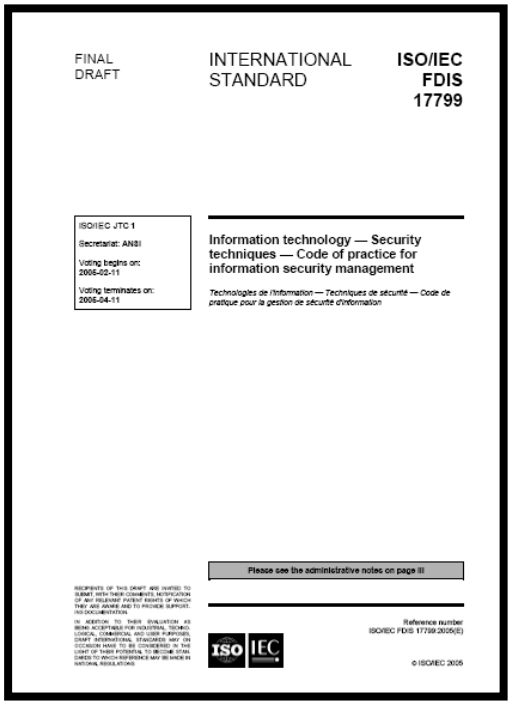
# ISO 27000 family of standards

- 27006: guidelines for the accreditation of organizations offering ISMS certification. *(2010)*
- 27007: Guidelines for Information Security Management Systems Auditing *(2010)*
- 27008: Guidelines for ISM auditing with respect to security controls *(April 2008)*
- 27799: Information security management in health using ISO/IEC 17799 *(April 2009)*

# BS ISO/IEC 17799:2005

## Information Security 'Disciplines' :

- Security Policy
- Organisation of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- IS Acquisition, Development and Maintenance
- Information Security Incident Mgmt
- Business Continuity Mgmt
- Compliance



FINAL DRAFT

INTERNATIONAL STANDARD

**ISO/IEC FDIS 17799**

ISO/IEC JTC 1

Secretariat: ANSI

Voting begins on: 2006-02-11

Voting terminates on: 2006-04-11

**Information technology — Security techniques — Code of practice for information security management**

*Technologies de l'information — Techniques de sécurité — Code de pratique pour la gestion de sécurité d'information*

Please see the administrative notes on page III

Reference number ISO/IEC FDIS 17799:2005(E)

© ISO/IEC 2005

# BS ISO/IEC 17799:2005

- 11 Sections
- 39 main security categories
- 133 controls

Each main security category contains:

a) a control objective stating what is to be achieved; and

b) one or more controls that can be applied to achieve the control objective.

Control descriptions are structured as follows:

Control

Defines the specific control statement to satisfy the control objective.

Implementation guidance

Provides more detailed information to support the implementation of the control and meeting the control objective. Some of this guidance may not be suitable in all cases and so other ways of implementing the control may be more appropriate.

Other information

Provides further information that may need to be considered, for example legal considerations and references to other standards.

# BS ISO/IEC 17799:2005

Control Objective ....

## 8.1 Prior to employment[3]

Objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

Security responsibilities should be addressed prior to employment in adequate job descriptions and in terms and conditions of employment.

All candidates for employment, contractors and third party users should be adequately screened, especially for sensitive jobs.

Employees, contractors and third party users of information processing facilities should sign an agreement on their security roles and responsibilities.

Control ....

### *8.1.1 Roles and responsibilities*

Control

Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy.

Guidance ....

Implementation guidance

Security roles and responsibilities should include the requirement to:

a) implement and act in accordance with the organization's information security policies (see 5.1);

b) protect assets from unauthorized access, disclosure, modification, destruction or interference;

c) execute particular security processes or activities;

d) ensure responsibility is assigned to the individual for actions taken;

e) report security events or potential events or other security risks to the organization.

Security roles and responsibilities should be defined and clearly communicated to job candidates during the pre-employment process.

Additional information ....

Other Information

Job descriptions can be used to document security roles and responsibilities. Security roles and responsibilities for individuals not engaged via the organization's employment process, e.g. engaged via a third party organization, should also be clearly defined and communicated.

# BS ISO/IEC 27001 – the objective

An organization needs to identify and manage many activities in order to function effectively. Any activity using resources and managed in order to enable the transformation of inputs into outputs can be considered to be a process. Often the output from one process directly forms the input to the next process.

The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management, can be referred to as a "process approach".

The process approach for information security management presented in this International Standard encourages its users to emphasize the importance of:

a) **understanding an organization's information security requirements** and the need to establish policy and objectives for information security;

b) **implementing and operating controls to manage an organization's information security risks** in the context of the organization's overall business risks;

c) **monitoring and reviewing the performance and effectiveness of the ISMS**; and

d) **continual improvement** based on objective measurement.


INTERNATIONAL STANDARD

ISO/IEC 27001

First edition
2005-10-15

Information technology — Security techniques — Information security management systems — Requirements

*Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information — Exigences*

Reference number
ISO/IEC 27001:2005(E)

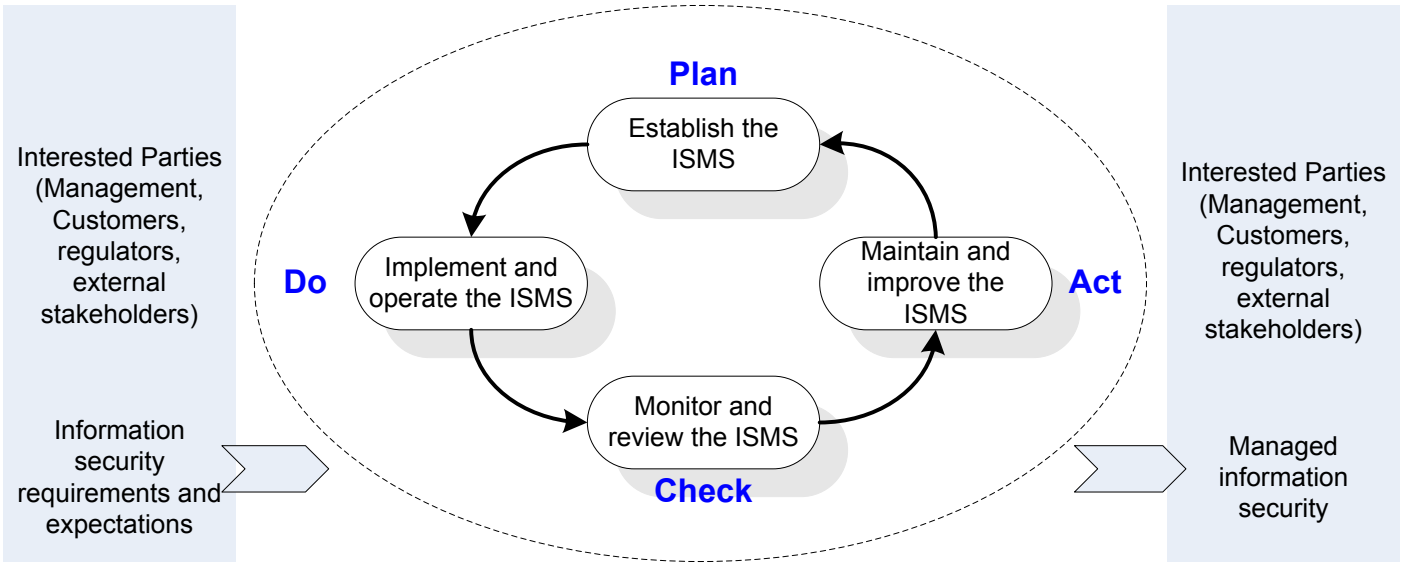
© ISO/IEC 2005

# What Compliance with ISO 27001 is really about …

ISO 27001 is a Management System for information security

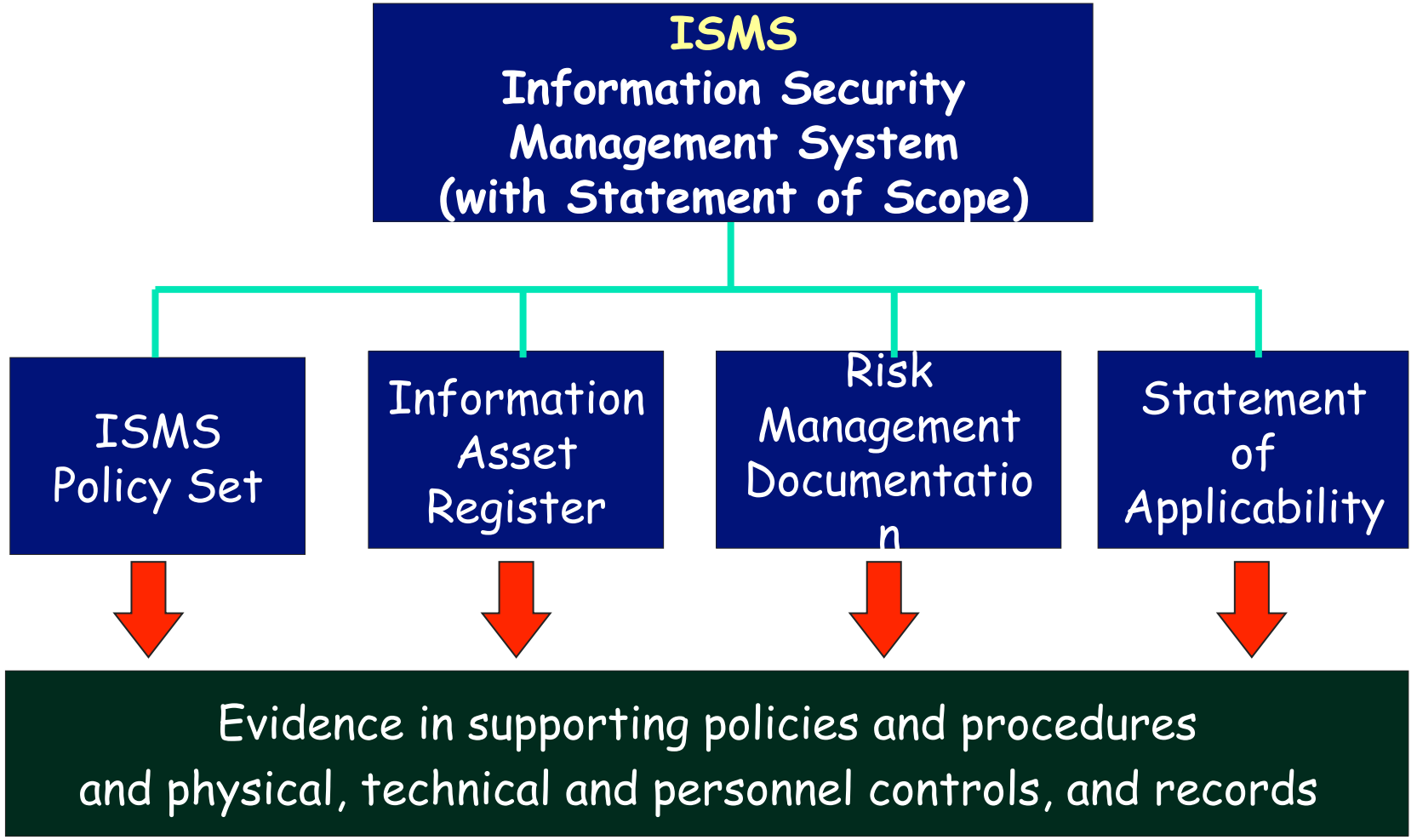
- Compliance focuses on assessing the effectiveness of this management system ('the ISMS')
  - Not an IT Security Review or Audit and shouldn't be seen as such
- It's really about Risk Management, NOT Risk Avoidance
  - Taking a risk based approach to information security
  - Treating risks appropriately
  - Ensuring a framework for risk is in place

# BS ISO 27001 - Plan-Do-Check-Act




| | |
|---|---|
| **Plan (establish the ISMS)** | Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives. |
| **Do (implement and operate the ISMS)** | Implement and operate the ISMS policy, controls, processes and procedures. |
| **Check (monitor and review the ISMS)** | Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review. |
| **Act (maintain and improve the ISMS)** | Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS. |

# What does an ISMS look like?



# What does an ISMS look like in action?

**ISMS documentation set**

ISMS policy
Risk management docs
Statement of Applicability
Asset registers
Policies, procedures and standards applicable to scope (local & corporate)
SLAs, contracts and other evidence

Driven by 'process' documentation

Business processes

**Events**

Security incidents
Suspected weaknesses
Malfunctions

Audit observations
Testing findings
Spot check findings

'Evidential' documentation

Recording and analysis

Report(s) into forum

Review and update ISMS

# What does it mean in action?

- Defined and agreed objectives
  - Demonstrate fit with real business objectives
  - legal, regulatory, contractual obligations, SLA's, Service Measures
- Senior management support and resources
- Responsibility defined, agreed and accepted
  - For controls, processes and the ISMS itself
- ISMS processes defined – and implemented
- Cultural changes – awareness, rigour, evidence
- Communication of objectives, policy, responsibility
  - Staff, contractors, customers, auditors etc
- Demonstrable compliance with all aspects of the ISMS – PDCA
- Same for Compliance and Certification!!!

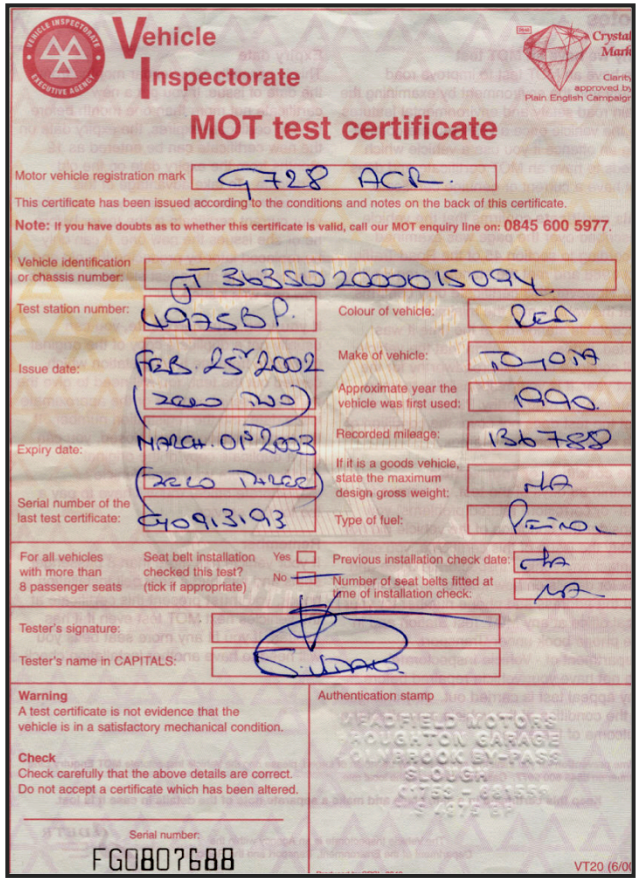
# BS 7799 Terminology

- Compliance
- Certification
- Accreditation
- Accredited versus non-Accredited Certification
- Role of UKAS
- See www.xisec.com for help to certify organisations

# Why do we need Assurance?

- Anybody can say that they comply with ISO 27001
(or any other Standard)

- The need to <u>demonstrate</u> compliance will lead to significant improvements in information security management.



Vehicle Inspectorate

MOT test certificate

Motor vehicle registration mark: G728 ACR

This certificate has been issued according to the conditions and notes on the back of this certificate.

Note: If you have doubts as to whether this certificate is valid, call our MOT enquiry line on: 0845 600 5977.

Vehicle identification or chassis number: JT 3635D 2000015094

Test station number: 49756P

Colour of vehicle: RED

Issue date: FEB 25 2002 (2002 20)

Make of vehicle: TOYOTA

Approximate year the vehicle was first used: 1990

Recorded mileage: 136785

Expiry date: MARCH 01 2003 (2003 20)

If it is a goods vehicle, state the maximum design gross weight: NA

Serial number of the last test certificate: 409313193

Type of fuel: PETROL

For all vehicles with more than 8 passenger seats: Seat belt installation checked this test? (tick if appropriate) Yes ☐ No ☒

Previous installation check date: NA

Number of seat belts fitted at time of installation check: NA

Tester's signature:

Tester's name in CAPITALS:

Warning
A test certificate is not evidence that the vehicle is in a satisfactory mechanical condition.

Check
Check carefully that the above details are correct. Do not accept a certificate which has been altered.

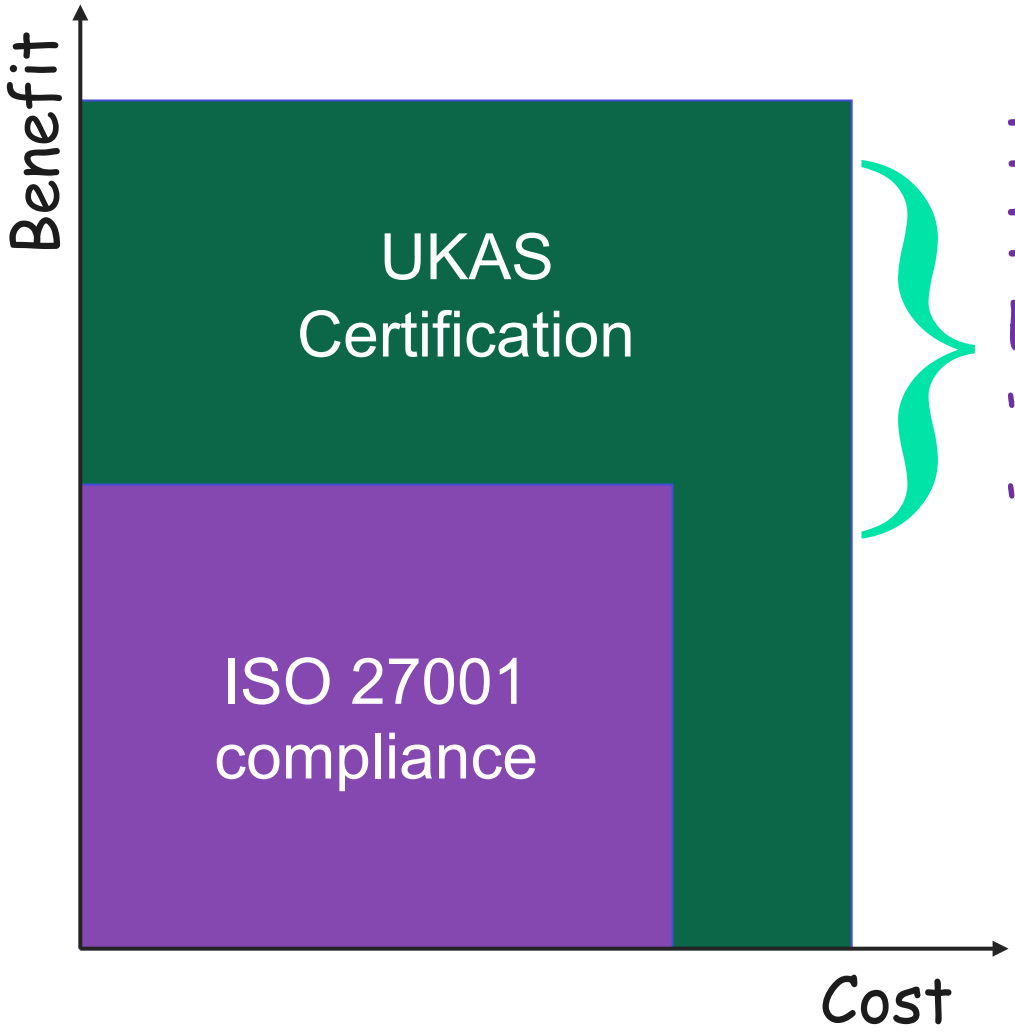
Serial number: FG0807688

Authentication stamp

MEADFIELD MOTORS
BROUGHTON GARAGE
OLYBROOK BY-PASS
SLOUGH

VT20 (6/0

# Compliance versus certification




Independent confirmation
Internal confidence
External recognition
'Customer' assurance
'Benchmark' status

# Motivation – Legal Requirements

## Sarbanes Oxley (SoX) – for companies with US listings

The Management of companies must state who will be *'establishing and maintaining an adequate internal control structure and procedures for financial reporting'*

"Section 404 - Sarbanes Oxley Act"

The recommended internal control framework requires that a formal risk assessment be performed to evaluate the internal and external factors that impact an organisation's performance. The results of the risk assessment will determine the controls that need to be implemented.

Sarbanes-Oxley

Financial and Accounting Disclosure Information

# Motivation – Regulatory Requirements

## FSA

*'A firm to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems and to provide information to demonstrate compliance with this principle'*

" FSA Handbook, Chapter Two, Principle Three requires"

## Basel II

*Operational risk is 'the risk of direct or indirect loss resulting from inadequate or failed internal processes, people or systems, or from external events'*

"Bank of International Settlements"

# Turnbull - Key Quotations

"The guidance is based on the adoption of a risk-based approach to establishing a sound system of internal control and reviewing its effectiveness. This should be incorporated by the company within its normal management and governance process. It should not be treated as a separate exercise undertaken to meet regulatory requirements."

"Internal Control: Guidance for Directors on the Combined Code"

"A thorough and regular evaluation of the nature and extent of the risks to which the company is exposed… to help manage and control risk rather than to eliminate it."

"Internal Control: Guidance for Directors on the Combined Code"

"Since profits are, in part, the reward for successful risk-taking in business, the purpose … is to help manage and control risk appropriately rather than to eliminate it."

nternal Control: Guidance for Directors on the Combined Code"

THE INSTITUTE OF CHARTERED ACCOUNTANTS IN ENGLAND & WALES

# Business Objectives

- To win business - competitive advantage
- To keep business – keeping up with competitors
- To demonstrate improved security through effective risk management
- Government mandates
- Industry peer pressure (e.g. Telcos)
- Trading partners demanding evidence of information security best practice
- Mounting concerns over legal action
- Increasing regulation and corporate governance (FSA, Basel II, SOX, HM Treasury)

# Business Objectives

**Marketing**


***Smile*** **- The Internet Bank from The Co-operative Bank**

**Assurance**


**A major UK Government Department**

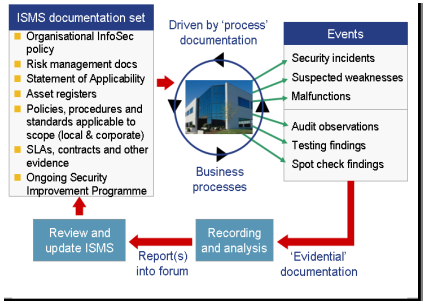
# Approach

Scope → Gap Analysis

ISMS Policy

Info Asset Register

Risk Assessment and Treatment




Action Plan

Compliant

Security Improvement Programme

(Policy, Procedures, and controls…)

Final Review

Initial Statement of Applicability

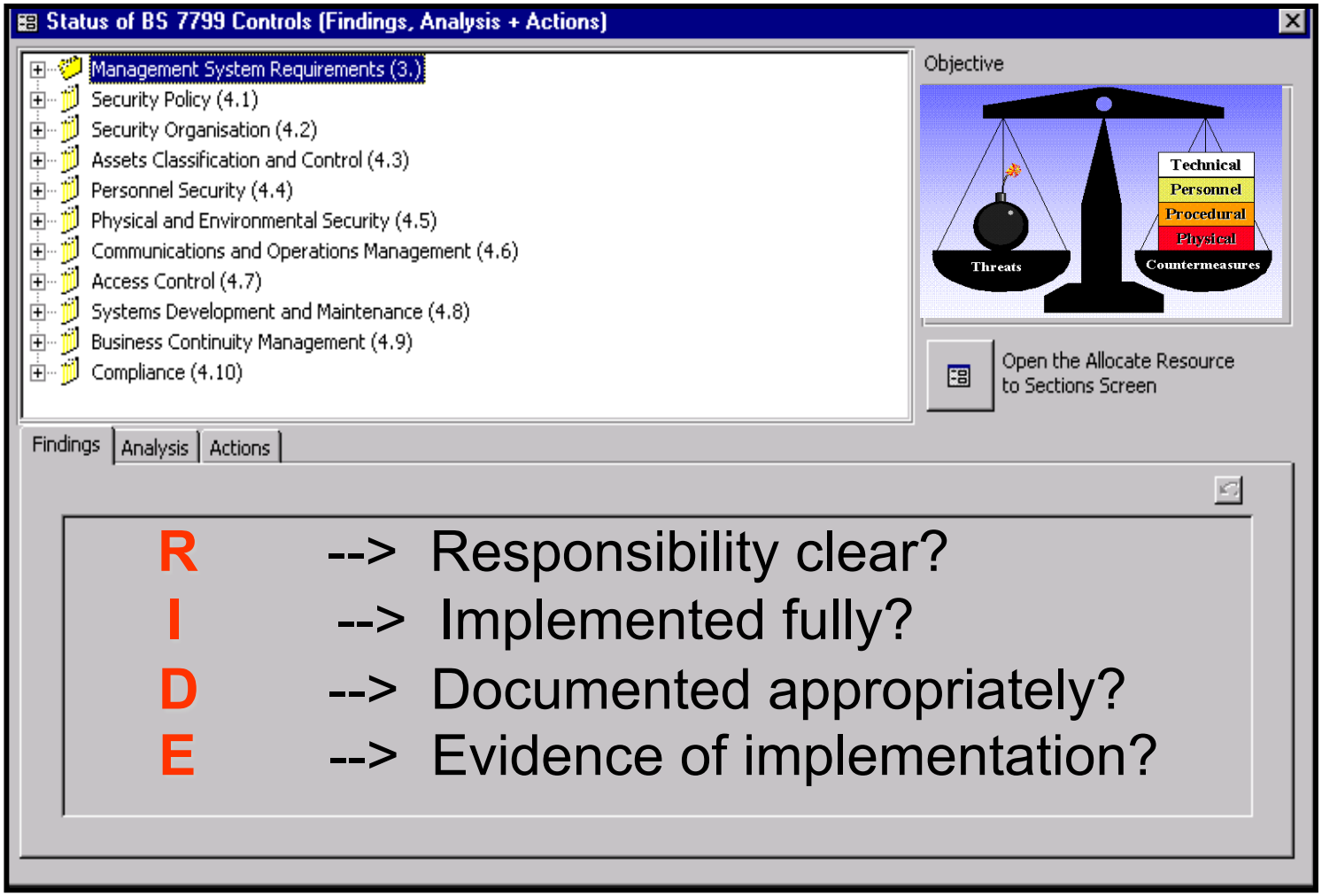
Complete SoA

# Defining the Scope

Identify key/critical business process(es)

- Determine ISMS boundary
- For each ISMS, identify:
  - business functions included
  - key information types and flows
  - supporting IT
- relevant staff
  - locations / physical environments.
- Also identify all third parties.

# Gap Analysis - Asking the Right Questions



# Extract of a Gap Analysis

| | | |
|---|---|---|
| **A.5.2** | **Information classification**<br><br>**Objective: To ensure that information assets receive an appropriate level of protection.**<br>*Information should be classified to indicate the need, priorities and degree of protection.*<br>*Information has various degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. An information classification system should be used to define an appropriate set of protection levels, and communicate the need for special handling measures.* | |
| | **Findings** | **Analysis and Required Actions** |
| **A.5.2.1** | **Classification guidelines**<br>*Classifications and associated protective controls for information shall be suited to business needs for sharing or restricting information and the business impacts associated with such needs.*<br><br>Penzance Tuffe have implemented a classification scheme for the Sales and Marketing area as a result of the company sensitive information that is processed by the sales force.<br><br>Information in the customer database, sales documentation, and product pricing documents are all confidential and may only be viewed by the sales administration team and the sales teams in accordance with their access rights.<br><br>There is only one classification – Confidential, and all documents are considered to be confidential. It was noted that there are some documents that may only be viewed by Janice Power and her regional managers. This includes the commission statement, sales targets and budgets and should not be divulged to the sales teams. There is a concern that the policy is not as granular as it should be to cater for information that needs to be restricted within the area. | The requirement for a classification scheme is understood, however, the fact that there is only one classification is restrictive. Consideration should be given to updating the policy so that another classification that can be applied to confidential information within the area that can only be seen by senior management and others as necessary.<br><br>There is a danger that the sales force are not differentiating between documents and a blanket classification of confidential is not promoting good conduct in the management of documents.<br><br>There is no apparent marking system for 'personal' or 'management in confidence' information such as staff records and staff appraisals. This needs to be addressed urgently. |
| **A.5.2.2** | **Information labeling and handling**<br>*A set of procedures shall be defined for information labelling and handling in accordance with the classification scheme adopted by the organisation.*<br><br>The sales force laptops are configured to label all documents sent to the sales administration team as confidential. It was noted that while all documents are labelled as confidential they are not necessarily handled as confidential and the policy has no advice on this. Some documents are left in in-trays overnight and are not locked away. | The policy should be reviewed to ensure that handling of information is well understood.<br><br>Confidential documents must be locked away overnight. |

# Example Information Asset Register (IAR)

**Annex A Section 7**

| Title | Type | Description | Owner | Classification |
|---|---|---|---|---|
| **Xpresso private key** | Electronic-stored | The private key used by the Java Applet to verify the identification of the Xpresso box in the setting up of the SSL session. | Technology Services Manager | Secret |
| **Co-operative Bank digital certificate private key** | Electronic-stored | Digital certificate private key, used in the encoding of the Java Applet | Technology Services Manager | Secret |
| **Customer authentication data** | Electronic-transient | The customer user ID, password and SPI data entered by the customer for authentication | Technology Services Manager | Secret |
| **Financial and business plans** | Paper / Electronic-stored | Business sensitive information including business risk assessments and marketing information, maintained for the Lincoln business process | Lincoln Business Manager | Management in Confidence |
| **Contract Documents** | Paper / Electronic-stored | Service Lev… …ements, …racts and related correspondence for the third party suppliers to Lincoln, currently Brokat and Planet ISP | Lincoln Business Manager | Management in Confidence |
| **Minutes of business review meetings** | Paper / Electronic-stored | Minutes of the monthly Lincoln business review meetings | Lincoln Business Manager | Management in Confidence |
| **Security Incident Reports** | Paper / Electronic-stored | Reports produced in relation to the channel due to identified incidents, weaknesses and malfunctions | Controller, Operational Risk | Management in Confidence |

# The SOA

| BS 7799 Section | Outline of requirement | Interpretation | Cross Reference |
|---|---|---|---|
| **A.3** | **Security Policy** | | |
| A.3.1 | **Information security policy**<br>*Objective: To provide management direction and support for information security.* | | |
| A.3.1.1 | **Information security policy document**<br>A policy document shall be approved by management, published and communicated, as appropriate, to all employees. | employs a layered approach to security policy, standards and procedures. Forming the top layer, a high-level security policy covers all Information Security aspects for . This document is structured to reflect the format of BS 7799. Individual Information Security policy documents are then written for individual business systems. These include a specific Information Security Policy for . The purpose of the business specific standards is to interpret policy as necessary and describe the detailed standards that must be applied by the business unit.<br>At the lowest level the 'Information Security, Your Responsibilities' booklet is given to all employees as part of their induction, including operators and technical operations staff. This constitutes the basic guidance given to all staff and contains instruction on the information security requirements they must meet for all systems. | Information Security Standards, Reference 8P.<br>Information Security Policy , Reference 1P.<br>'Information Security – Your Responsibilities' booklet, Reference 5P. |

Findings and Analysis column replaced by Cross References

# Roles of the SOA

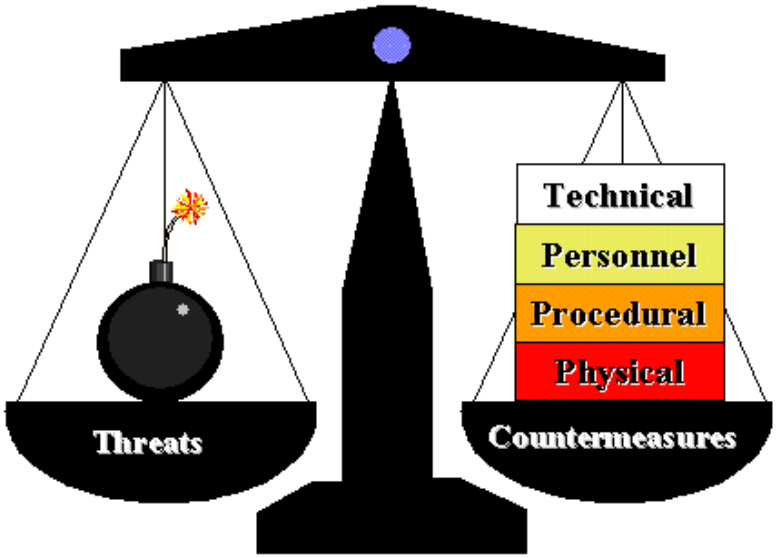
1. Statement of Interpretation of the BS7799 / ISO 27001 objectives and controls as applied in your environment
2. High level information security policy, in the many areas covered by ISO 27001
3. Basis for Service Level Agreements - Statements of broad responsibility for the ISO 27001 control areas, e.g. for supporting information security aspects such as physical and human resources security
4. Baseline for Internal Audits - 'Invert' to develop the internal audit checklists used in ongoing compliance audits against BS7799 / ISO 27001
5. A 'Roadmap' - To present the information required by the external auditors, stating clearly the locations of the evidence of compliance

# What is Risk Management?

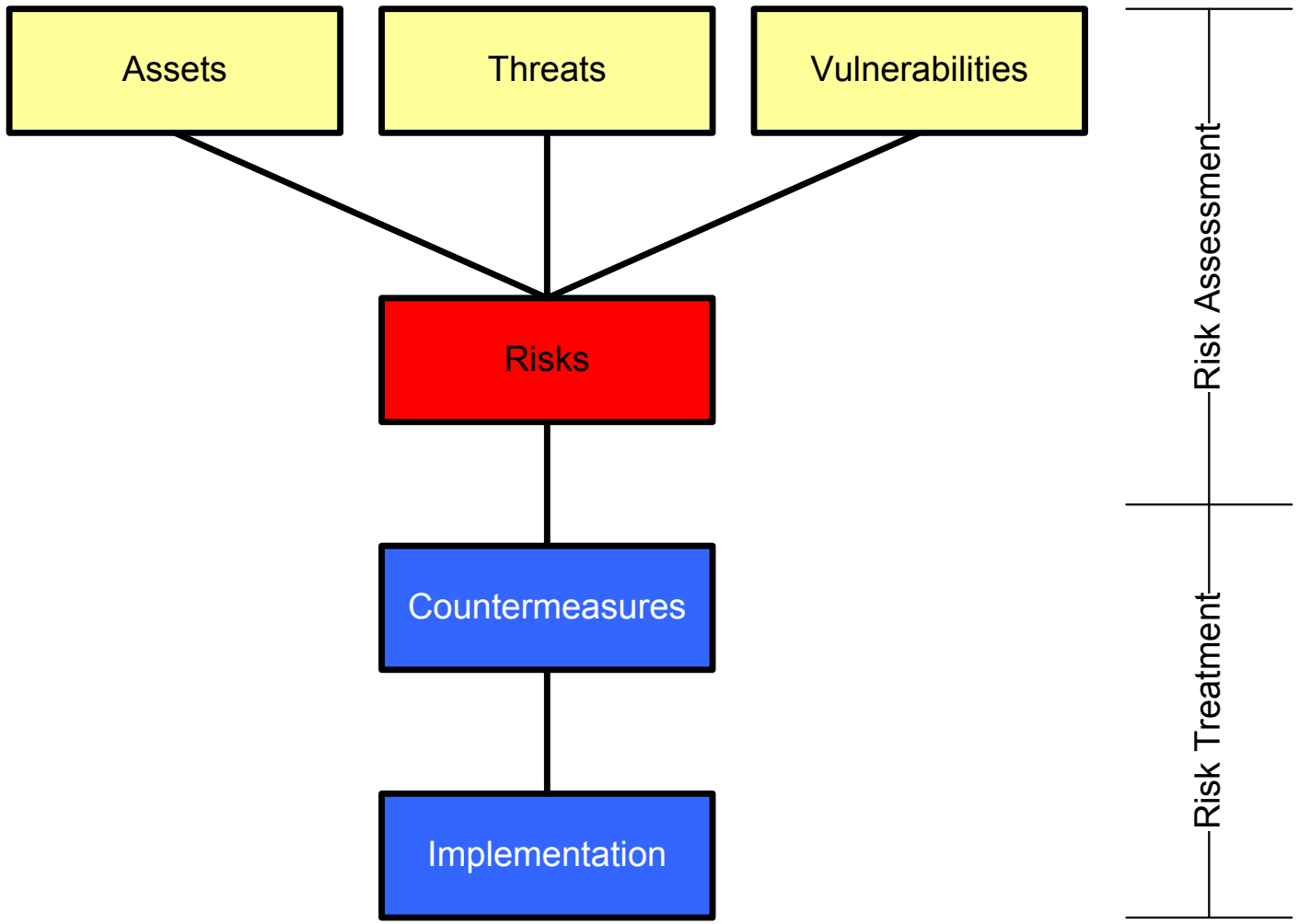
- Risk is defined as: an uncertainty of outcome, usually something which will prevent an organisation from meeting its objectives in some way
- ISO 27001 definition:
  **Risk management = Risk assessment + Risk treatment**
- Risk assessment identifies a 'risk' when a threat could affect an asset (to which it is vulnerable), leading to a potential business impact
- Risk '<u>treatment</u>' is concerned with selecting countermeasures (CMs) to counter these threats, and making risk management decisions

# Generic Steps

1. Identify assets
2. Identify asset dependencies
3. Business Impact Assessment (Asset Valuation)
4. Threat Assessment
5. Determine levels of risk (Risk Assessment)
6. Countermeasure Selection
7. Map to ISO 27001
8. Risk Treatment



# CRAMM methodology



# Risk Treatment

| Measure | Example approaches |
|---|---|
| Eliminating or avoiding the risk | E.g. Abandon or replace the objective associated with the risk in question |
| Sharing the risk | Share in full or in part with third party, e.g. for outsourcing |
| Reducing the possibility | Changing approach, acting to reduce threat or mitigate the occurrence |
| Reducing the consequences | Develop contingency plans |
| Tolerating the risk | Perhaps because the cost of mitigation is too high. Monitor only. |

# Risk Acceptance Register

**PENZANCE TUFFE**

**RISK ACCEPTANCE REGISTER**

| Statement No. | Owner | Description | Date Recorded | Next Review | Status |
|---|---|---|---|---|---|
| 1 | Ivor Natitude | No contract with 'Green Fingers' | 1 Sep '00 | 1 Nov '00 | OPEN |
| 2 | Doris Fence | Firewall not state of the art | 20 Oct '00 | 1 Mar '01 | OPEN |
| | | | | | |

- **NEW** risks that have been identified but not formally accepted
- **OPEN** risks formally accepted and for which there is a Risk Acceptance Statement signed by senior management
- **CLOSED** resolved to the satisfaction of the Forum
- **WITHDRAWN** risks that are overtaken by events, or otherwise cease to be of concern

# Flexible control areas

*Scorecards can be presented with control areas that match the structure of your chosen standard of practice*

## 17 control areas

1. Policies and standards
2. Ownership
3. Organization
4. Risk identification
5. Awareness
6. Service agreements
7. User capabilities
8. IT capabilities
9. System configuration
10. Data back-up
11. Contingency arrangements
12. Physical security
13. Access to information
14. Change management
15. Problem management
16. Special controls
17. Audit/review

## ISO27001:2005 native structure

1. Security policy
2. Organization of information security
3. Asset management
4. Human resources security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Information systems acquisition, development and maintenance
9. Information security incident management
10. Business continuity management
11. Compliance

## COBIT

1. Define a Strategic IT Plan and direction
2. Define the Information Architecture
3. .
4. .
5. .

34 control objectives

33. Ensure Regulatory Compliance
34. Provide IT Governance

## PCI DSS

1. Build and Maintain a Secure Network
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

# Questions???