

---

# *ISO/IEC 17799*

## The Standard for Information Security

Dr Michael John Nash, Director

A contribution to EBU NMC Seminar

Geneva, 16 and 17 June 2004

# Contents

---

- ⌘ What is ISO/IEC 17799? BS 7799?
- ⌘ What is an Information Security Management System?
- ⌘ What do I have to do to be 7799 compliant?
- ⌘ Why should I bother?
- ⌘ What's new?

# ISO/IEC 17799 and BS7799-2

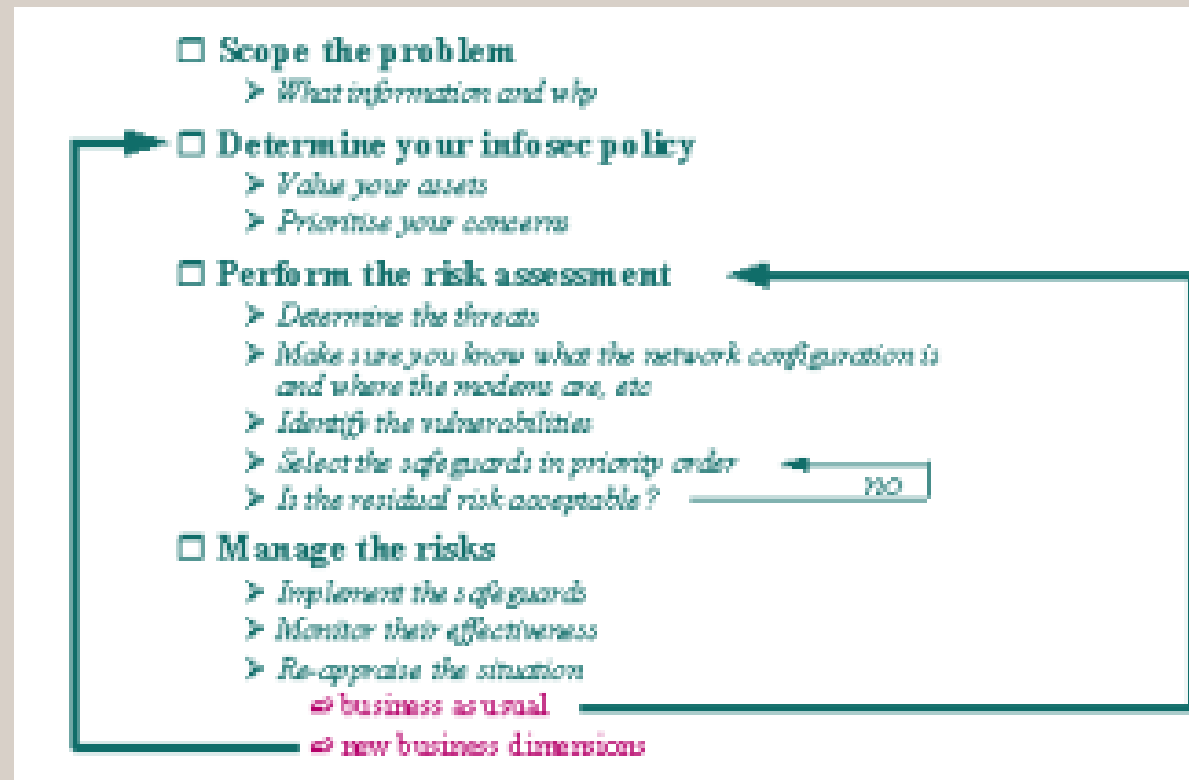
---

- ⌘ IS 17799 is a *catalogue of good things to do*
- ⌘ BS 7799 Part 2 is a *specification for an ISMS (Information Security Management System)*
- ⌘ ISMS compliance can be **independently assessed**



# What is an ISMS?

■ The means by which management can monitor and control information security, to reduce the business risk to an acceptable level and ensure that security continues to fulfil their corporate, customer and legal requirements.



# History

## Today

- IS 17799 Four years old
- hundreds certified worldwide
- Well established IUG
- Part 2 revised 2002
- IS 17799 revision in progress

## 1999 - 2001

- BS7799:1999 Published
- First Certificates
- Part 1 Submitted to ISO
- ISO/IEC 17799 Published
- Part 2 Under Revision

## 1997-1998

- Dutch Certification Scheme
- BS7799 Part 2
- c:cure Scheme Designed
- Pilot Certifications
- Revision of Part 1 Starts

## 1993-1995

- PD0003 Code of Practice
- BS7799:1995
- ISO Fast Track Fails
- International Take-up

## 1987

- DTI CCSC Project Begins
- Product Criteria (ITSEC)
- Users' Guide (BS7799)

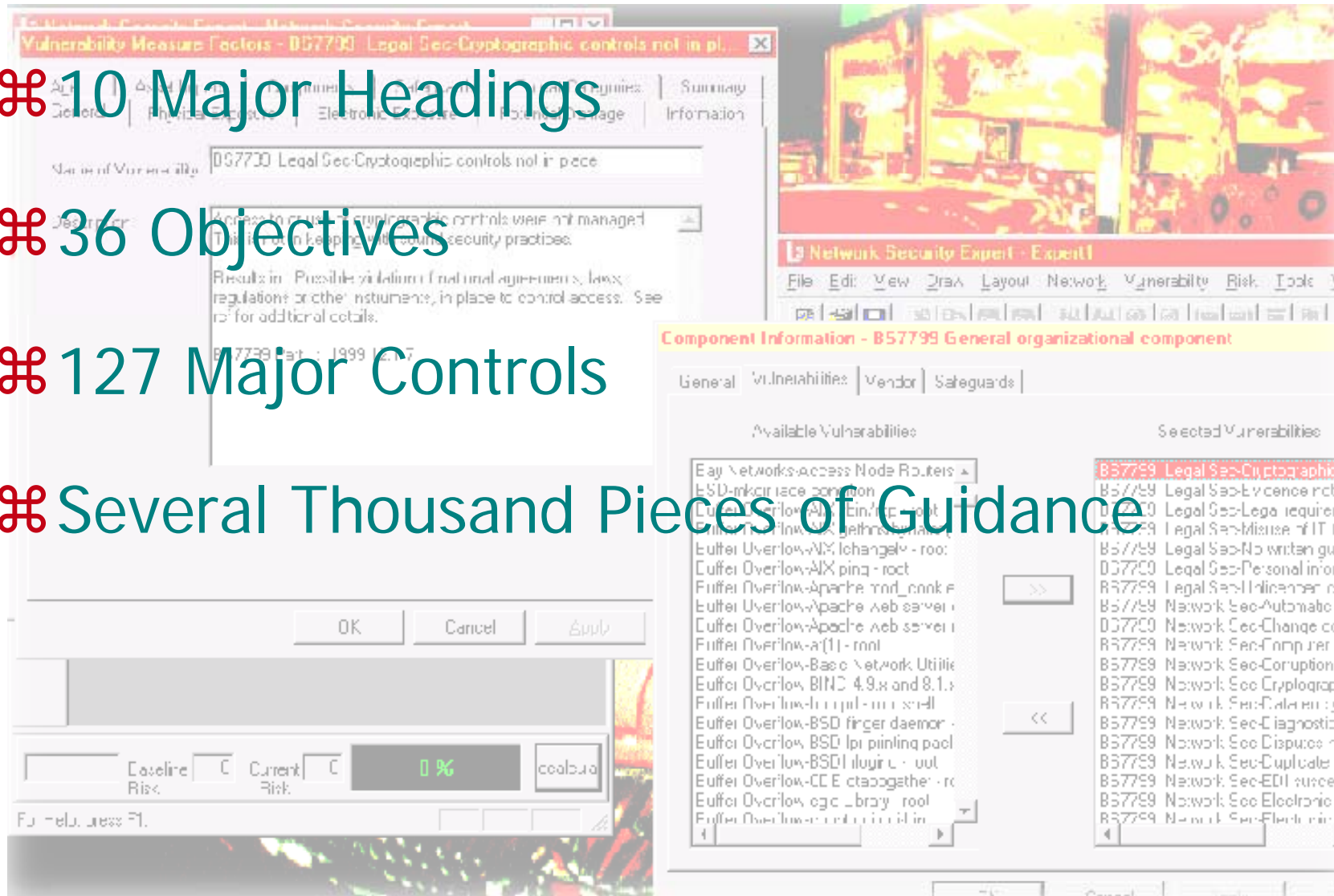
# ISO/IEC 17799 Layout

⌘ 10 Major Headings

⌘ 36 Objectives

⌘ 127 Major Controls

⌘ Several Thousand Pieces of Guidance



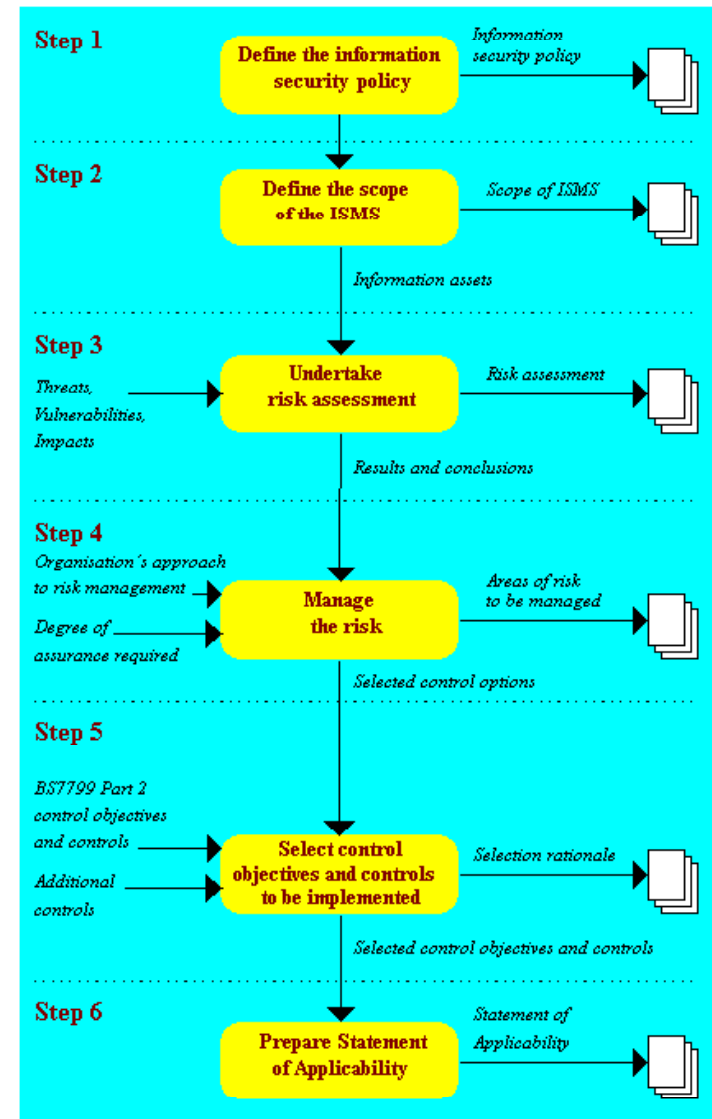
# *The 10 Major Headings*

---

- ⌘ Security Policy
- ⌘ Security Organisation
- ⌘ Asset Classification and Control
- ⌘ Personnel Security
- ⌘ Physical and Environmental Security
- ⌘ Comms and Operational Management
- ⌘ Access Control
- ⌘ Systems Development and Maintenance
- ⌘ Business Continuity Management
- ⌘ Compliance

# BS 7799-2

- ⌘ Requirements for an ISMS
- ⌘ Based on the PDCA (“Plan-Do-Check-Act”) model
- ⌘ Same model as ISO 9001, ISO 14001 etc.
- ⌘ ISO/IEC 17799 Controls (in imperative format)





# Shall and Should

---

## Security requirements in third party contracts

Arrangements involving third party access to organizational information processing should be based on a formal contract containing, or referring to, all of the necessary requirements to ensure compliance with the organization's security policies and The contract should ensure that there is no misunderstanding between the organization and the third party. Organizations should satisfy themselves as to the indemnity of the The following terms should be considered for inclusion in the contract:

- a) The general policy on information security;
- b) Asset protection, including:
  - i. procedures regarding protection of organizational assets, information and software;
  - ii. procedures to determine whether any compromise of the assets, or modification of data, has occurred;
  - iii. controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during, the contract;
  - iv. integrity and availability;
  - v. restrictions on copying and disclosing information;

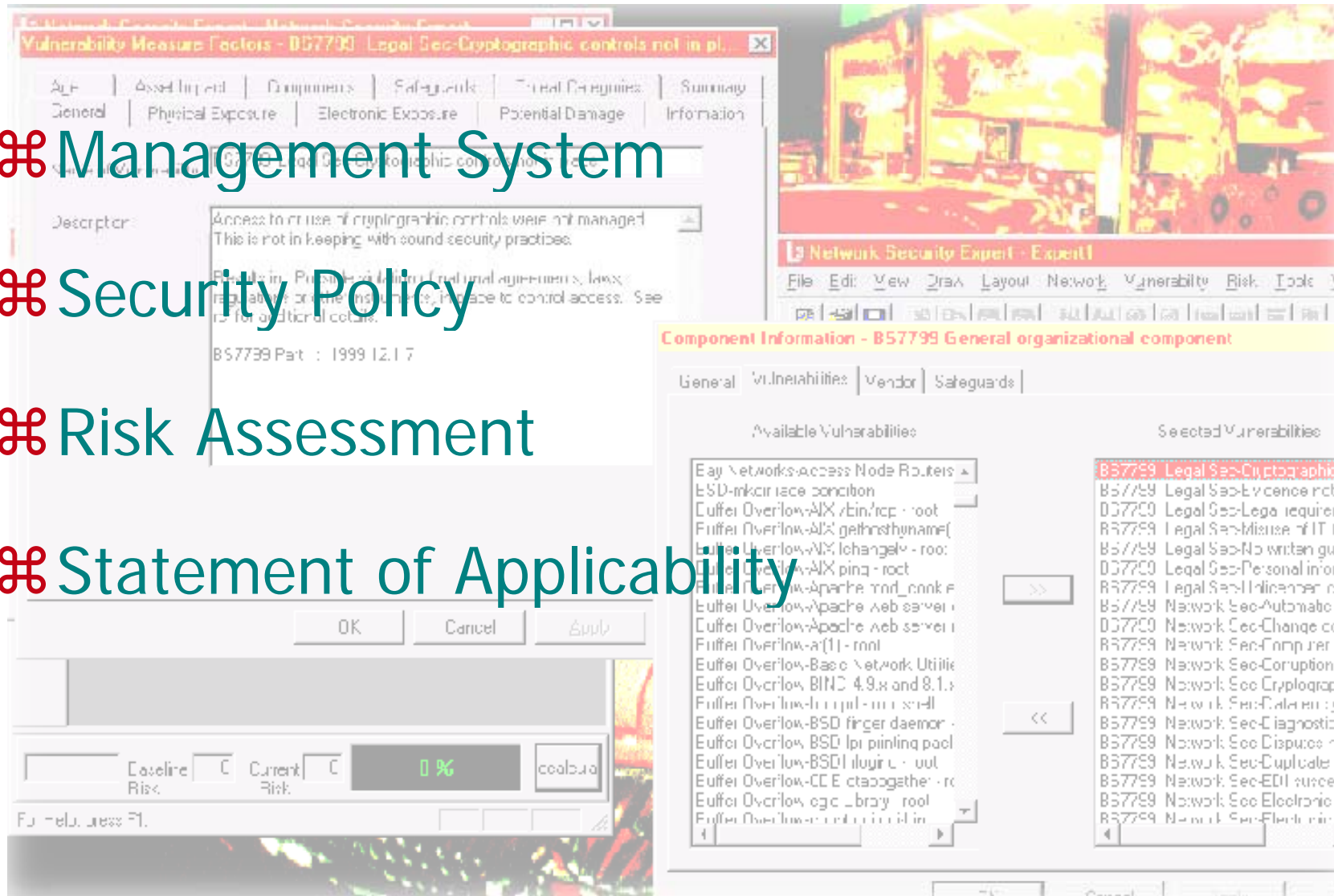
# Complying with BS 7799-2

⌘ Management System

⌘ Security Policy

⌘ Risk Assessment

⌘ Statement of Applicability



The screenshot displays a vulnerability assessment tool interface. The main window is titled "Vulnerability Measure Factors - BS7799 Legal Sec-Cryptographic controls not in pl...". It has tabs for "General", "Physical Exposure", "Electronic Exposure", "Potential Damage", and "Information". The "General" tab is active, showing a "Descriptor" field with the text: "Access to or use of cryptographic controls were not managed. This is not in keeping with sound security practices." Below this, there is a "Results in" field with the text: "Results in: Possible violation of national agreements, laws, regulations or other instruments, failure to control access. See reference for additional details." and a version number "BS7799 Part : 1999 12.1.7".

Overlaid on the main window is a "Component Information - B57799 General organizational component" window. It has tabs for "General", "Vulnerabilities", "Vendor", and "Safeguards". The "Vulnerabilities" tab is active, showing a list of "Available Vulnerabilities" and "Selected Vulnerabilities".

Available Vulnerabilities	Selected Vulnerabilities
Easy Networks-access Node Routers	B57799 Legal Sec-Cryptographic
ESD-mkdir race condition	B57799 Legal Sec-Evidence protect
Buffer Overflow-AIX rbin/tcp - root	D07790 Legal Sec-Legal require
Buffer Overflow-AIX gethostname()	R57799 Legal Sec-Misuse of IT fe
Buffer Overflow-AIX lchangelv - root	B57799 Legal Sec-No written gu
Buffer Overflow-AIX ping - root	D07790 Legal Sec-Personal infor
Buffer Overflow-Apache mod_cooki	R57799 Legal Sec-Indicenter cr
Buffer Overflow-Apache web server	B57799 Network Sec-Automatic
Buffer Overflow-Apache web server	D07790 Network Sec-Change co
Buffer Overflow-a(1) - root	R57799 Network Sec-Comp rari
Buffer Overflow-Basic Network Utilitie	B57799 Network Sec-Corruption/
Buffer Overflow-BIND 4.9.x and 8.1.x	B57799 Network Sec-Cryptograph
Buffer Overflow-burpup - root shell	R57799 Network Sec-Data en: cy
Buffer Overflow-BSD finger daemon	B57799 Network Sec-Diagnostic
Buffer Overflow-BSD lpr printing pool	B57799 Network Sec-Dispute res
Buffer Overflow-BSD1 ilugit.c - out	B57799 Network Sec-Duplicate L
Buffer Overflow-CC E ctacogather - ro	B57799 Network Sec-EDI suscep
Buffer Overflow-egc -library root	B57799 Network Sec-Electronic
Buffer Overflow-ent -root in	R57799 Network Sec-Electronic

At the bottom of the main window, there is a "Baseline Risk" section with a "Current Risk" section showing a green bar at 0%.

# *Security Policy*

---

## **4.1 Security Policy**

### **4.1.1 Information security policy**

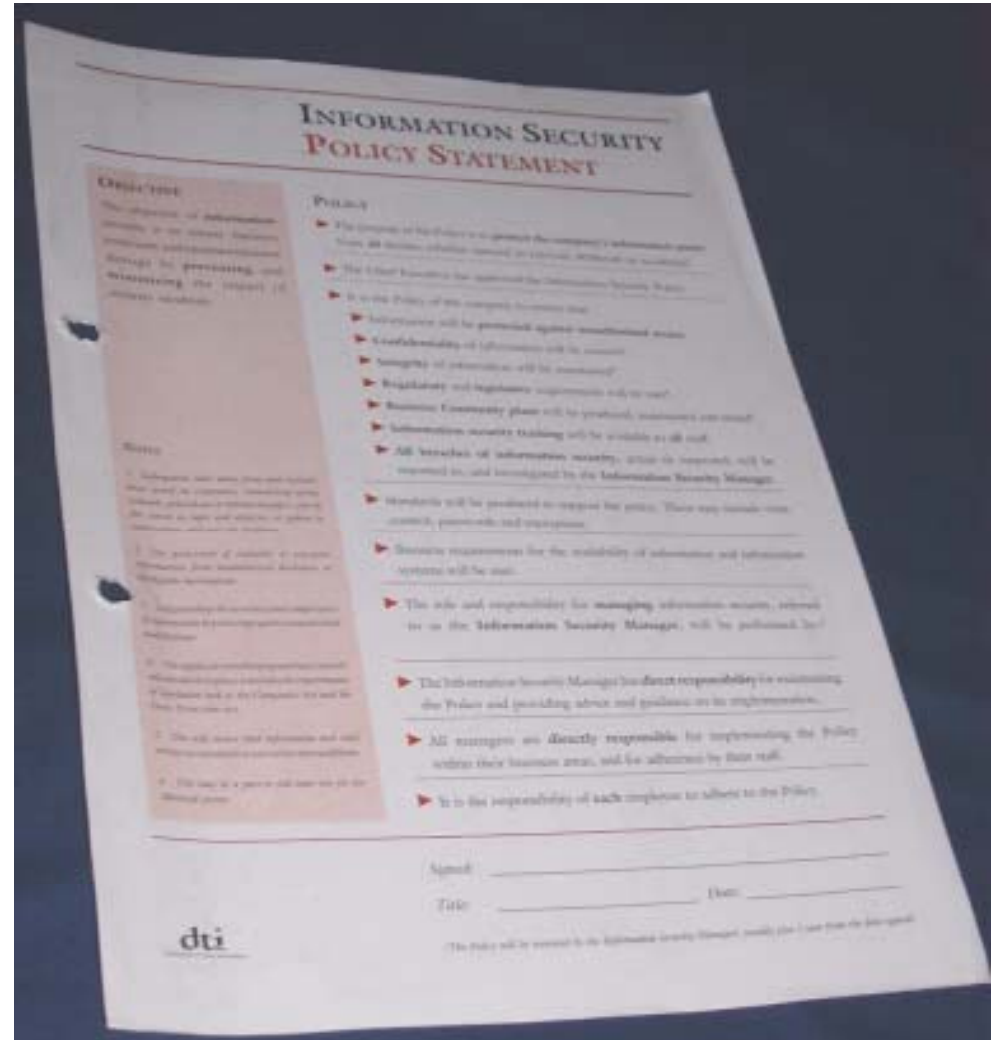
**Control objective:** To provide management direction and support for information security

#### **4.1.1.1 Information security policy document**

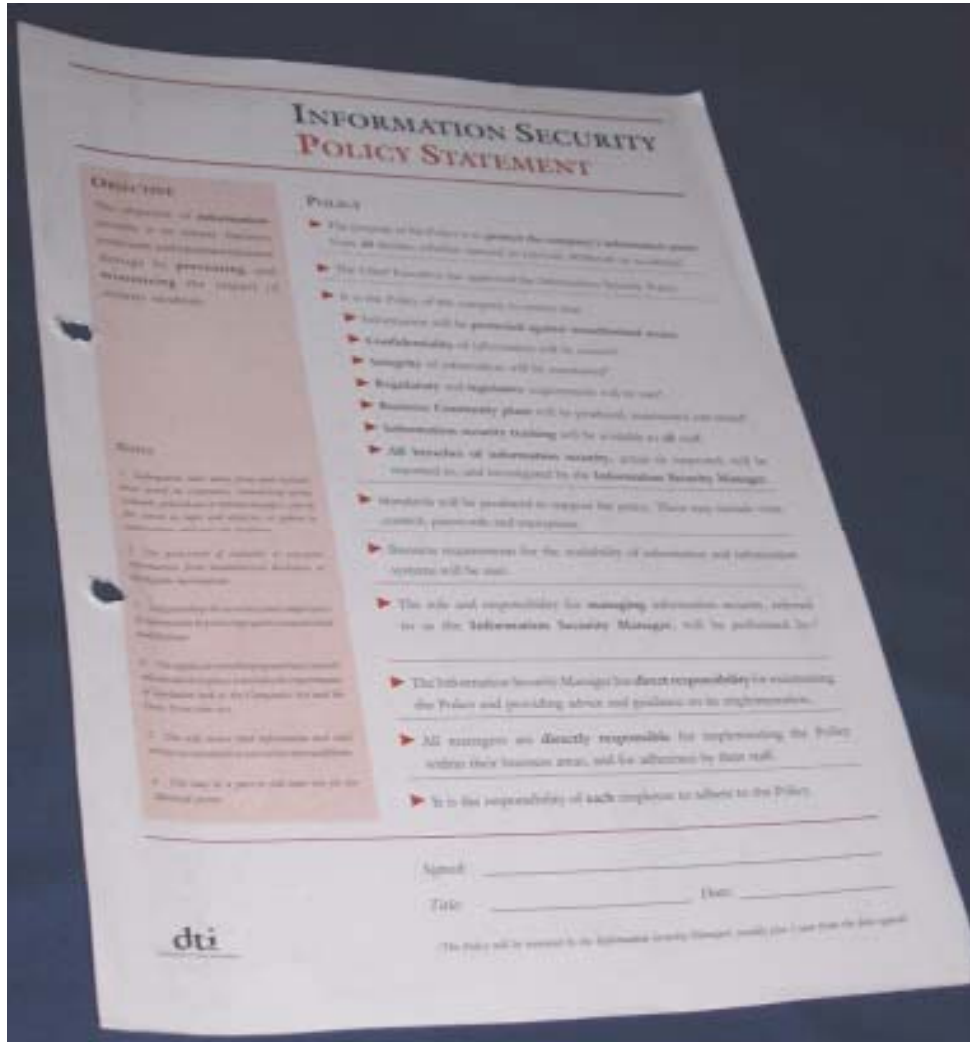
A policy document shall be approved by management, published and communicated, as appropriate, to all employees.

# Security Policy

- ⌘ Scope
- ⌘ Confidentiality
- ⌘ Integrity
- ⌘ Availability
- ⌘ Accountability
- ⌘ Assets
- ⌘ Risk Assessment
- ⌘ Regulatory/Legal



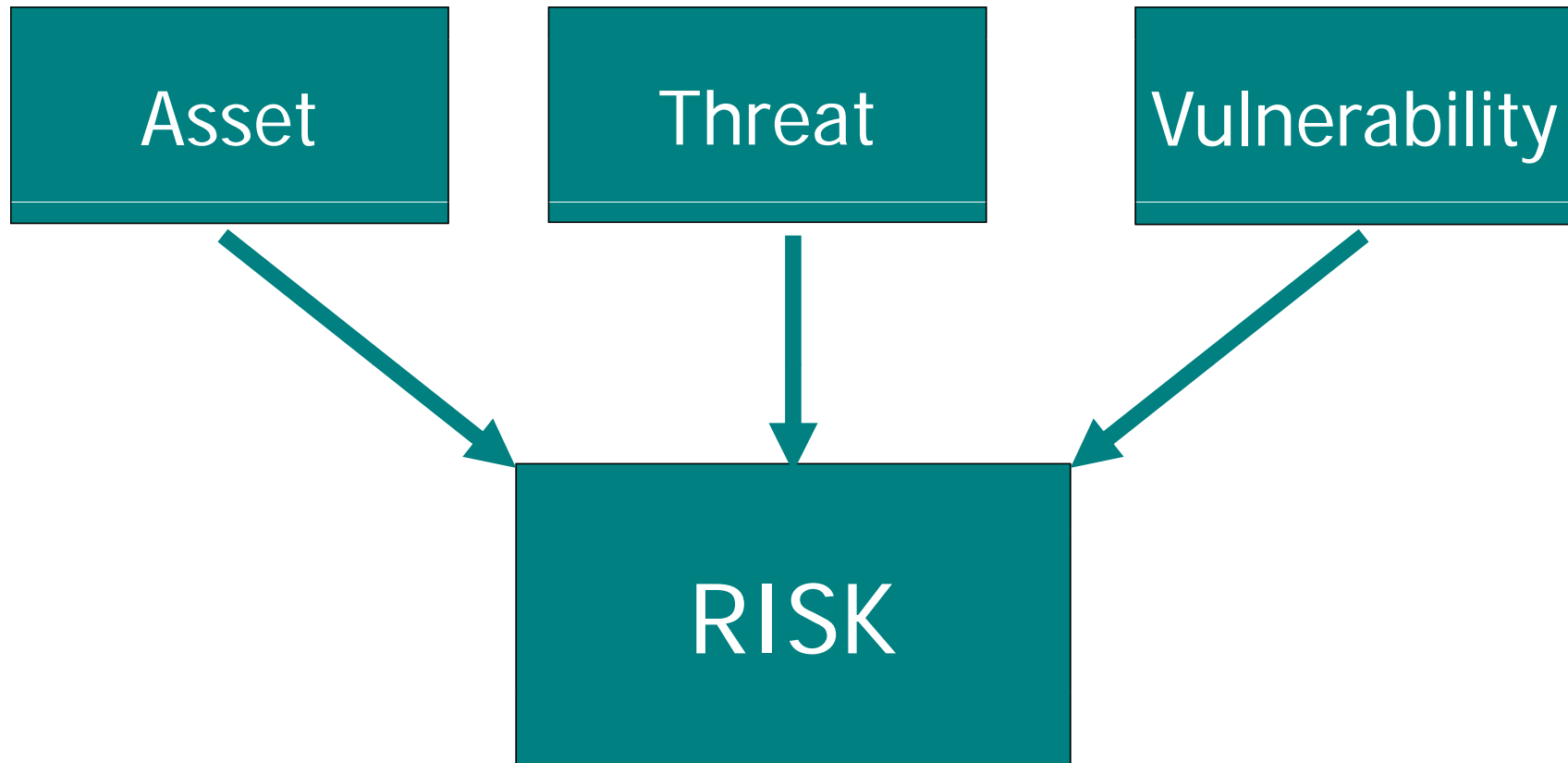
# Security Policy



- ⌘ CISO
- ⌘ ISMS Forum (TOR)
- ⌘ Managers, Staff
- ⌘ Suppliers
- ⌘ Training
- ⌘ Dispensations
- ⌘ Best Practice
- ⌘ Independent Review

# *Risk Assessment*

---



# Statement of Applicability

## 4.5.3 General controls

Control objective	To prevent compromise or theft of information and information processing facilities			References
Requirement	Applicability	Zone	Justification/comments	References
BS 7799-1 §7.3.1 Clear desk and clear screen policy	partial	all	Necessary to prevent the accidental disclosure of CONFIDENTIAL and HIGHLY CONFIDENTIAL information and to prevent authorised access to computer equipment. A clear desk policy only applies to CONFIDENTIAL and HIGHLY CONFIDENTIAL documents, fax machines and printers. There is no controlled stationery.	Exist, but need to be enforced more rigorously
BS 7799-1 §7.3.2 Removal of property	partial	all	Necessary to prevent the removal of HIGHLY CONFIDENTIAL discs from Zone 1 FM. Precautions against the unauthorised removal of property is not a threat as it might be in the case of a military secrets.	See 7.2.6 above, but need permission to remove other kit (eg portables, phones etc)

⌘ Identifies actual security controls

⌘ Must consider all 7799-2 listed controls

4.6 ← include or exclude with justification

## 4.6.1 Operational procedures and responsibilities

Control objective	To ensure that the correct and secure operation of information processing facilities			References
Requirement	Applicability	Zone	Justification/comments	References
BS 7799-1 §8.1.1 Documentation of operating procedures	yes	all	Necessary requirement for compliance with Part 2 §3.4.	Being audited at current date
BS 7799-1 §8.1.2 Operational change control	yes	all	Necessary requirement for compliance with Part 2 §3.5, and to prevent the unauthorised release of software into Zone 1.	Being audited at current date
BS 7799-1 §8.1.3 Incident management procedures	yes	all	Necessary to provide feedback on the effectiveness of the information security systems and to trigger remedial action and, when necessary, crisis management, damage limitation and recovery actions.	To be developed

⌘ Select applicable controls by business and risk analysis

# *Statement of Applicability*

---

## **4.4.1.4 Terms and conditions of employment**

Non-applicable. This is covered by the oath.

## **4.4.2 User training**

**Control objective:** To ensure that users are aware of information security threats and concerns, and are equipped to support organisational security policy in the course of their work

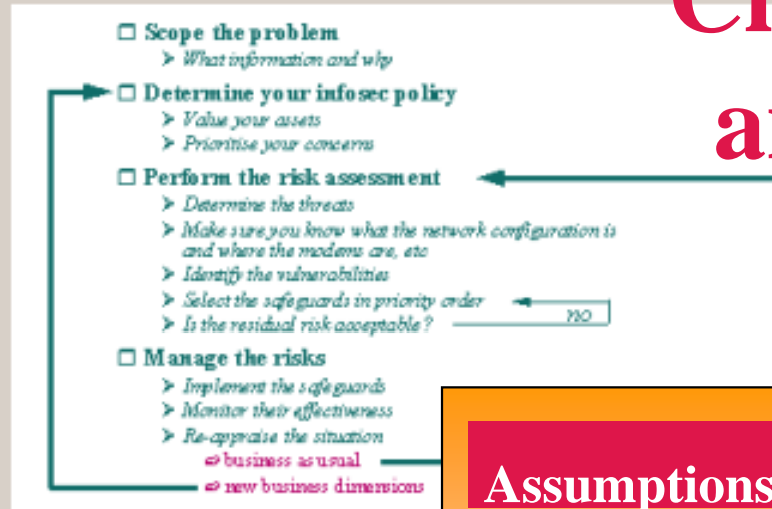
### **4.4.2.1 Information security education and training**

Applicable. Its purpose is induct new staff into the security-minded culture of the company, reinforce that on a regular basis to existing staff and keep staff up to date as security procedures change to meet new requirements. New staff complete 1~2 hours on



# Management System

■ The means by which management can monitor and control information security, to reduce the business risk to an acceptable level and ensure that security continues to fulfil their corporate, customer and legal requirements.



**Check in place and effective**

**Assumptions**

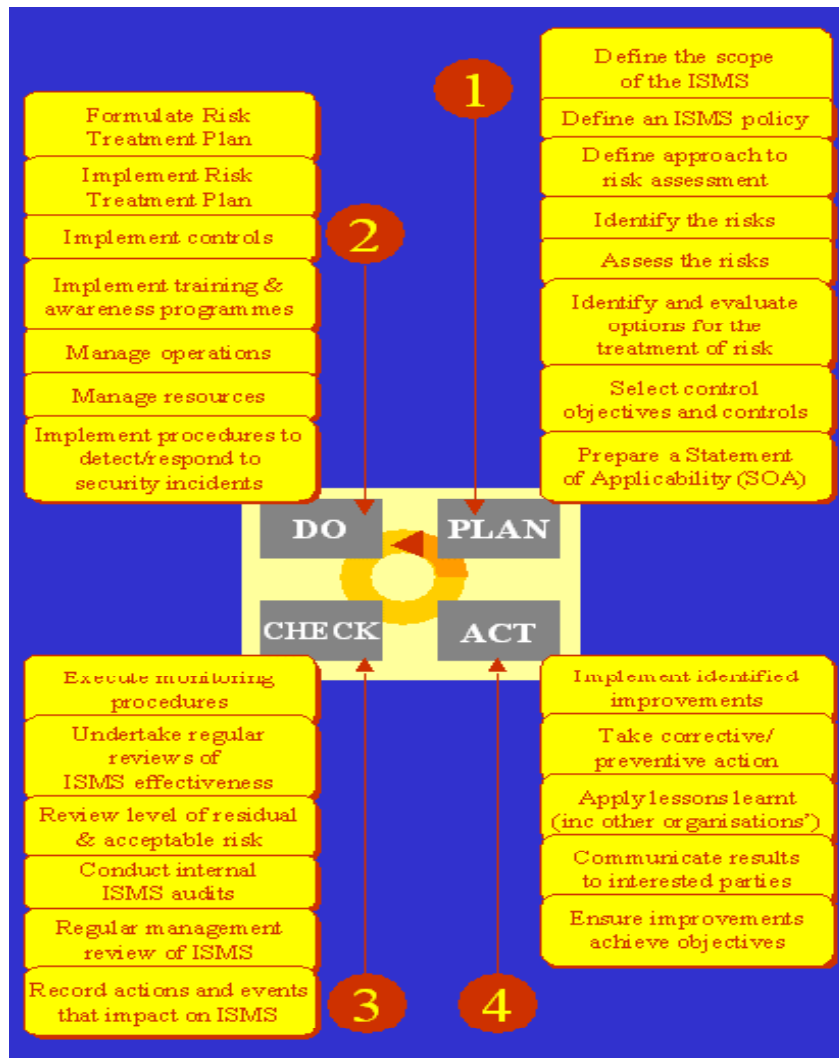
**BS 7799 Controls**

**Residual Risks**

**Monitor and control**

**Continue to be acceptable**

# The Continuous Process



# Why bother?

☘ Information Security forms part of Internal Control, as defined by OECD – important in today's business world

☘ ISO/IEC 17799 is a good cookbook

☘ PDCA provides a good methodology for managing and measuring security

☘ In the Digital Age, physical security is not enough

☘ You can get a recognised and independent certification against BS 7799

Interested?

# *Changes to 17799*

---

- ⌘ ISO/IEC 17799 revision in process
  - ← *Massive interest*
  - ← *Thousands of comments and ideas*
  - ← *One significant change?*
  
- ⌘ ISO/IEC JTC1 considering a certification standard
  - ← *North American resistance*
  - ← *Delaying tactics*
  - ← *Meanwhile BS7799-2 used in over 40 countries*

# *In closing*

---

- ⌘ Information Security matters
- ⌘ If you don't manage it, you don't control it
- ⌘ BS 7799 is your management tool

■ Reducing business risk to an acceptable level and ensuring that security continues to fulfil corporate, customer and legal requirements.



# *ISO/IEC 17799*

**The Standard for Information Security**

**Gamma Secure Systems Limited**  
**<http://www.gammasl.co.uk>**