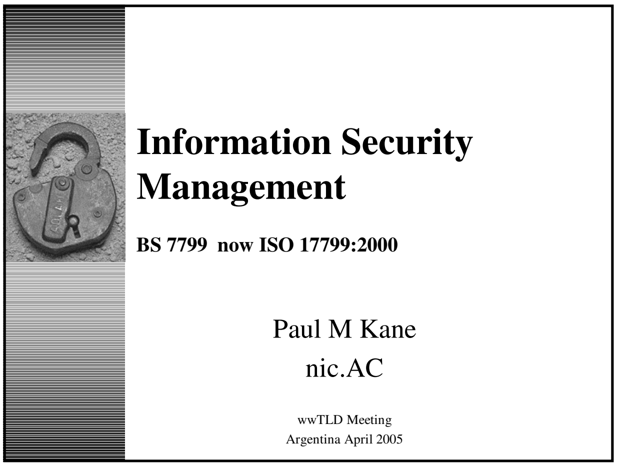
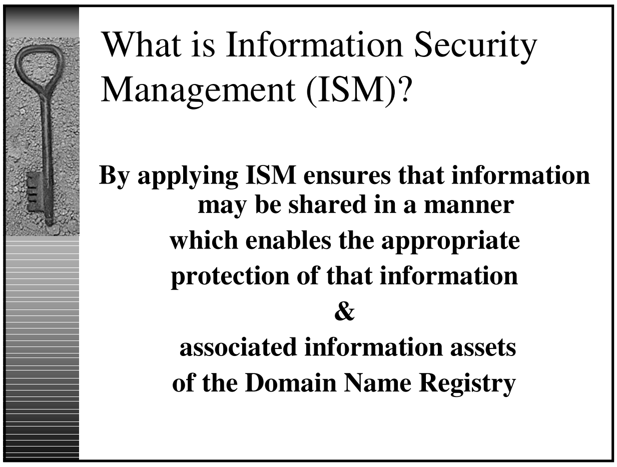


Information Security Management

BS 7799 now ISO 17799:2000

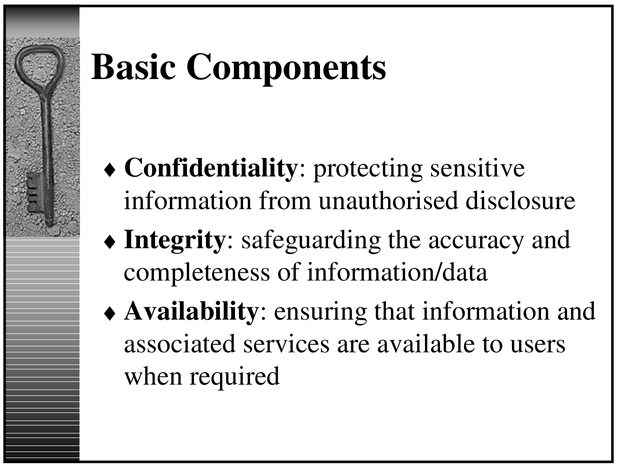
Paul M Kane
nic.AC

wwTLD Meeting
Argentina April 2005



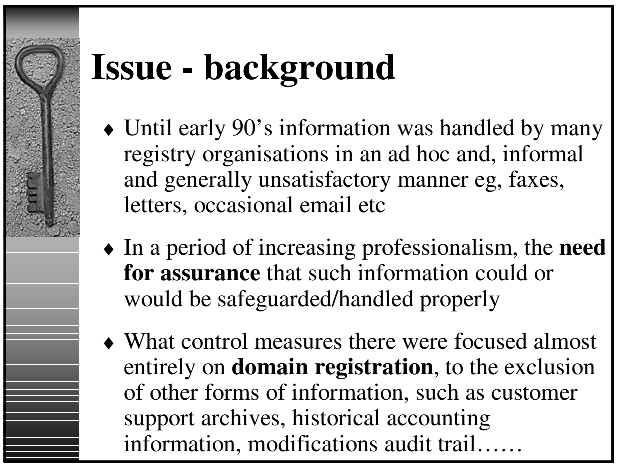
What is Information Security Management (ISM)?

By applying ISM ensures that information may be shared in a manner which enables the appropriate protection of that information & associated information assets of the Domain Name Registry



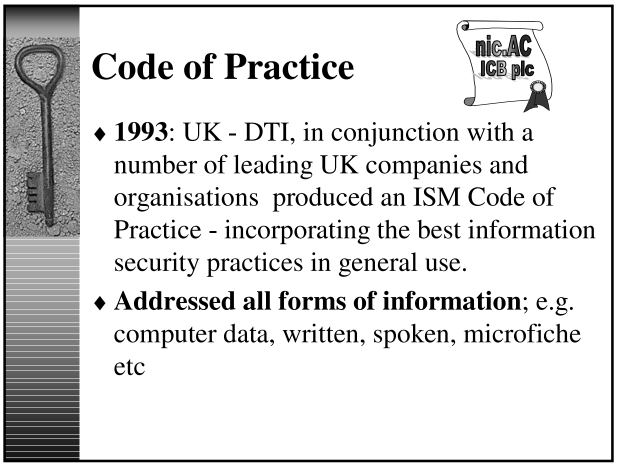
Basic Components

- ♦ **Confidentiality**: protecting sensitive information from unauthorised disclosure
- ♦ **Integrity**: safeguarding the accuracy and completeness of information/data
- ♦ **Availability**: ensuring that information and associated services are available to users when required



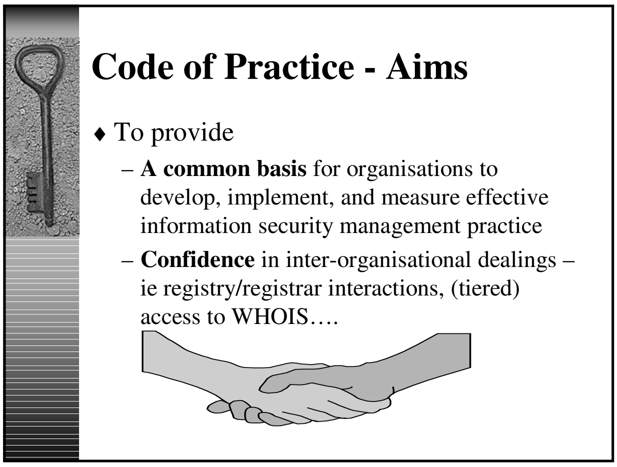
Issue - background

- ♦ Until early 90's information was handled by many registry organisations in an ad hoc and, informal and generally unsatisfactory manner eg, faxes, letters, occasional email etc
- ♦ In a period of increasing professionalism, the **need for assurance** that such information could or would be safeguarded/handled properly
- ♦ What control measures there were focused almost entirely on **domain registration**, to the exclusion of other forms of information, such as customer support archives, historical accounting information, modifications audit trail……



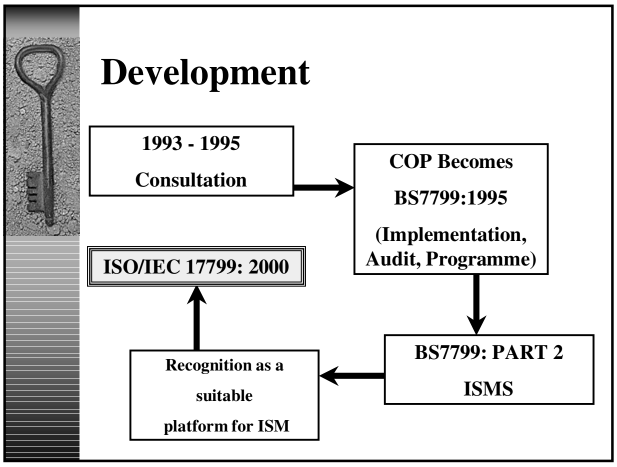
Code of Practice

- ♦ **1993**: UK - DTI, in conjunction with a number of leading UK companies and organisations produced an ISM Code of Practice - incorporating the best information security practices in general use.
- ♦ **Addressed all forms of information**; e.g. computer data, written, spoken, microfiche etc



Code of Practice - Aims

- ♦ To provide
  - – **A common basis** for organisations to develop, implement, and measure effective information security management practice
  - – **Confidence** in inter-organisational dealings – ie registry/registrar interactions, (tiered) access to WHOIS….



Development

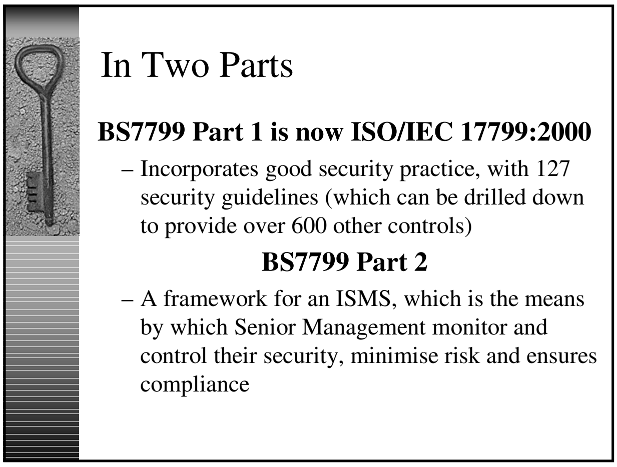
1993 - 1995 Consultation

COP Becomes BS7799:1995 (Implementation, Audit, Programme)

BS7799: PART 2 ISMS

Recognition as a suitable platform for ISM

ISO/IEC 17799: 2000



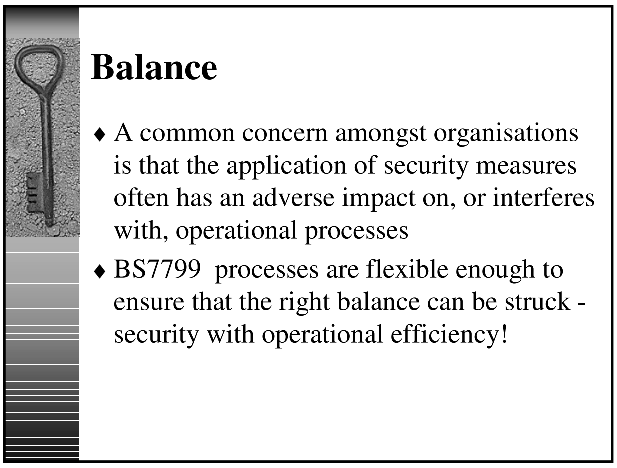
In Two Parts

BS7799 Part 1 is now ISO/IEC 17799:2000

– Incorporates good security practice, with 127 security guidelines (which can be drilled down to provide over 600 other controls)

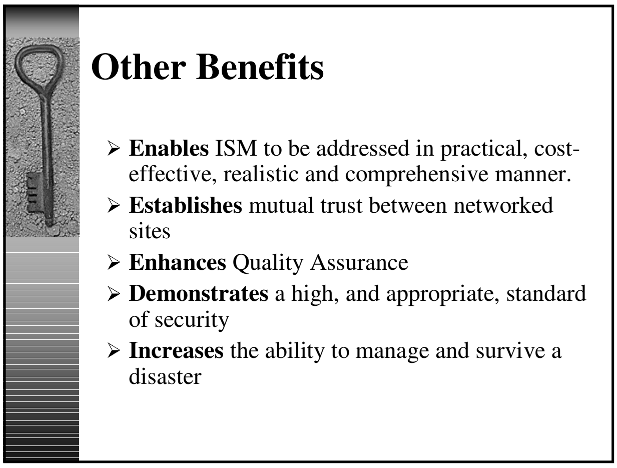
BS7799 Part 2

– A framework for an ISMS, which is the means by which Senior Management monitor and control their security, minimise risk and ensures compliance



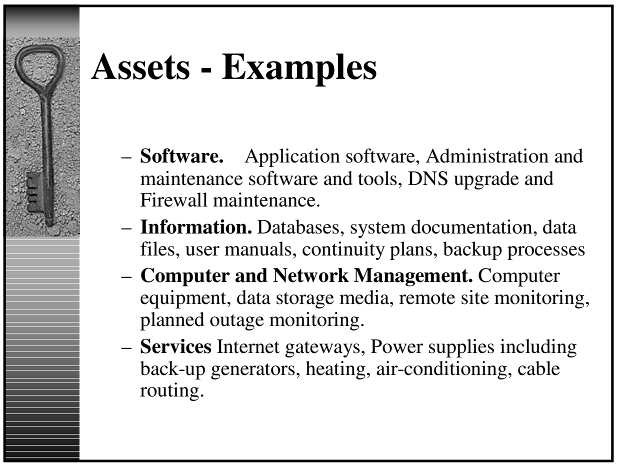
Balance

- ♦ A common concern amongst organisations is that the application of security measures often has an adverse impact on, or interferes with, operational processes
- ♦ BS7799 processes are flexible enough to ensure that the right balance can be struck - security with operational efficiency!



Other Benefits

- ➢ **Enables** ISM to be addressed in practical, cost-effective, realistic and comprehensive manner.
- ➢ **Establishes** mutual trust between networked sites
- ➢ **Enhances** Quality Assurance
- ➢ **Demonstrates** a high, and appropriate, standard of security
- ➢ **Increases** the ability to manage and survive a disaster



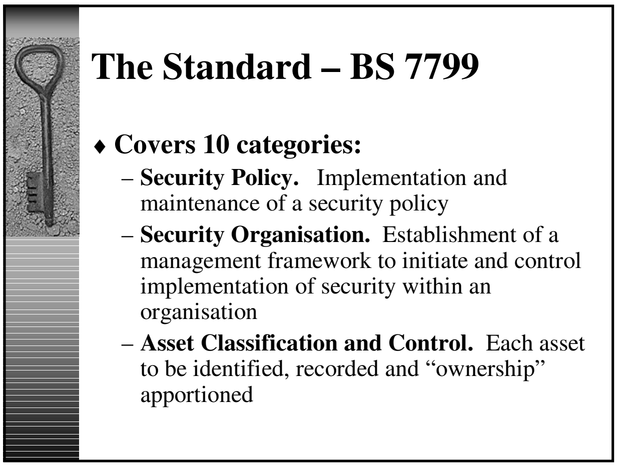
Assets - Examples

– **Software.** Application software, Administration and maintenance software and tools, DNS upgrade and Firewall maintenance.

– **Information.** Databases, system documentation, data files, user manuals, continuity plans, backup processes

– **Computer and Network Management.** Computer equipment, data storage media, remote site monitoring, planned outage monitoring.

– **Services** Internet gateways, Power supplies including back-up generators, heating, air-conditioning, cable routing.



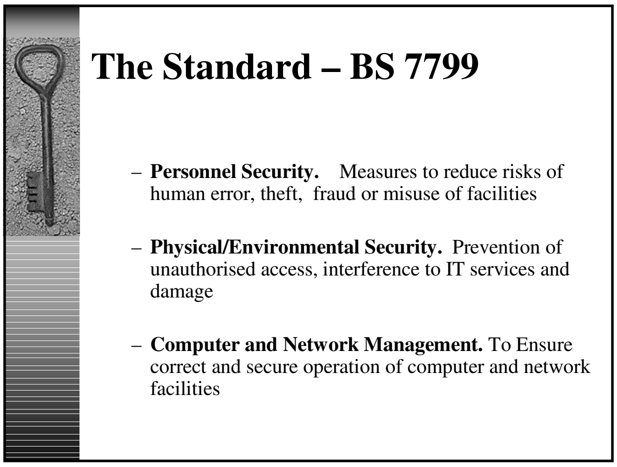
The Standard – BS 7799

♦ **Covers 10 categories:**

– **Security Policy.** Implementation and maintenance of a security policy

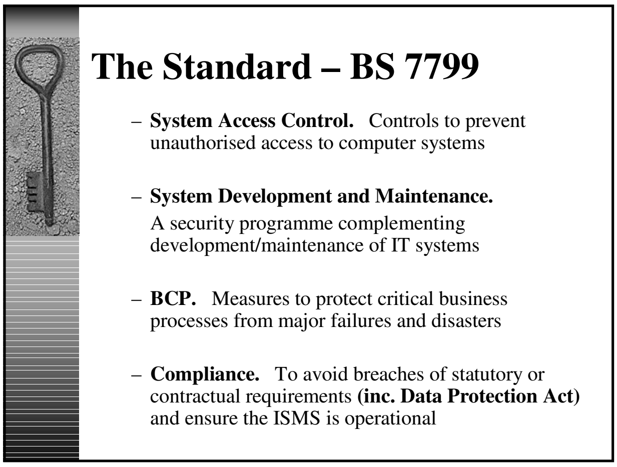
– **Security Organisation.** Establishment of a management framework to initiate and control implementation of security within an organisation

– **Asset Classification and Control.** Each asset to be identified, recorded and “ownership” apportioned



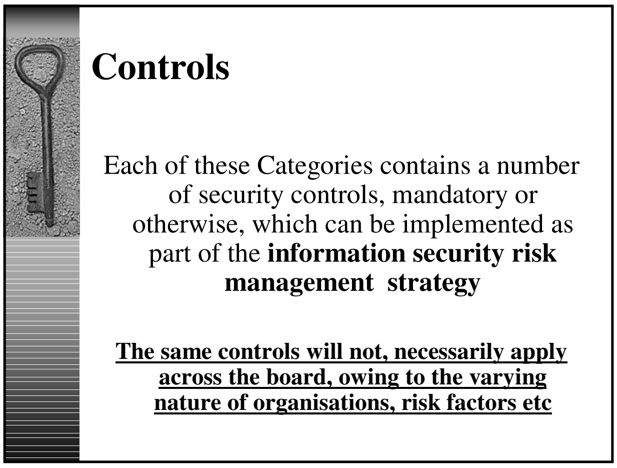
The Standard – BS 7799

- **Personnel Security.** Measures to reduce risks of human error, theft, fraud or misuse of facilities
- **Physical/Environmental Security.** Prevention of unauthorised access, interference to IT services and damage
- **Computer and Network Management.** To Ensure correct and secure operation of computer and network facilities



The Standard – BS 7799

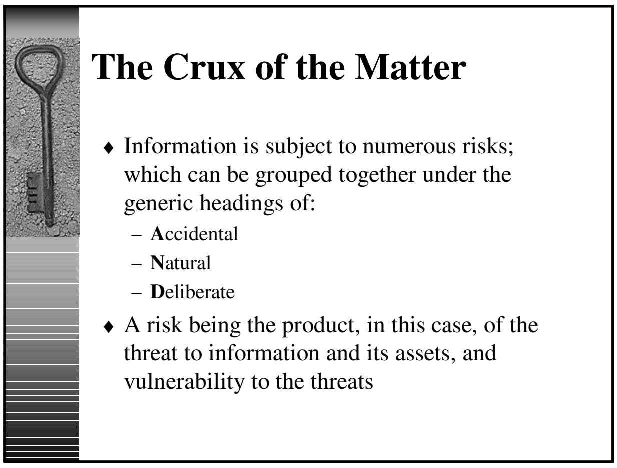
- **System Access Control.** Controls to prevent unauthorised access to computer systems
- **System Development and Maintenance.** A security programme complementing development/maintenance of IT systems
- **BCP.** Measures to protect critical business processes from major failures and disasters
- **Compliance.** To avoid breaches of statutory or contractual requirements **(inc. Data Protection Act)** and ensure the ISMS is operational



Controls

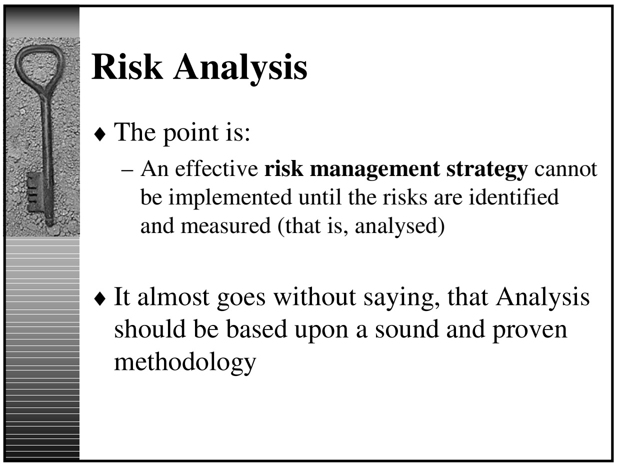
Each of these Categories contains a number of security controls, mandatory or otherwise, which can be implemented as part of the **information security risk management strategy**

The same controls will not, necessarily apply across the board, owing to the varying nature of organisations, risk factors etc



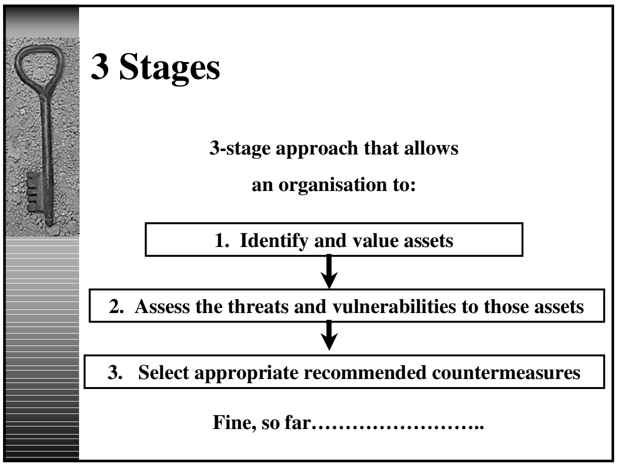
The Crux of the Matter

- Information is subject to numerous risks; which can be grouped together under the generic headings of:
  - **A**ccidental
  - **N**atural
  - **D**eliberate
- A risk being the product, in this case, of the threat to information and its assets, and vulnerability to the threats



Risk Analysis

- The point is:
  - An effective **risk management strategy** cannot be implemented until the risks are identified and measured (that is, analysed)
- It almost goes without saying, that Analysis should be based upon a sound and proven methodology



3 Stages

3-stage approach that allows

an organisation to:

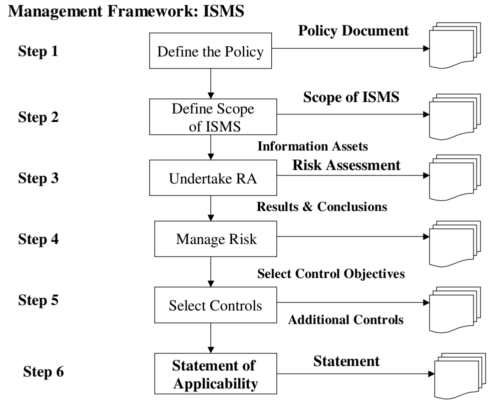
1. Identify and value assets

2. Assess the threats and vulnerabilities to those assets

3. Select appropriate recommended countermeasures

Fine, so far……………………..

Management Framework: ISMS



Step 1
Define the Policy
Policy Document

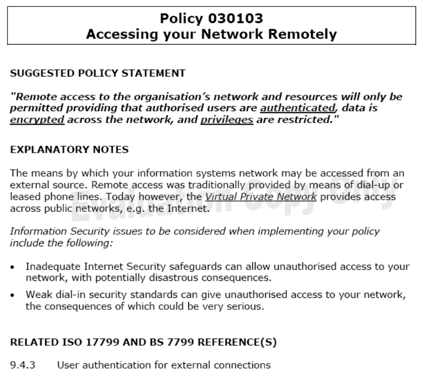
Step 2
Define Scope of ISMS
Scope of ISMS
Information Assets

Step 3
Undertake RA
Risk Assessment
Results & Conclusions

Step 4
Manage Risk
Select Control Objectives

Step 5
Select Controls
Additional Controls

Step 6
Statement of Applicability
Statement



Policy 030103
Accessing your Network Remotely

SUGGESTED POLICY STATEMENT

"Remote access to the organisation's network and resources will only be permitted providing that authorised users are authenticated, data is encrypted across the network, and privileges are restricted."

EXPLANATORY NOTES

The means by which your information systems network may be accessed from an external source. Remote access was traditionally provided by means of dial-up or leased phone lines. Today however, the *Virtual Private Network* provides access across public networks, e.g. the Internet.

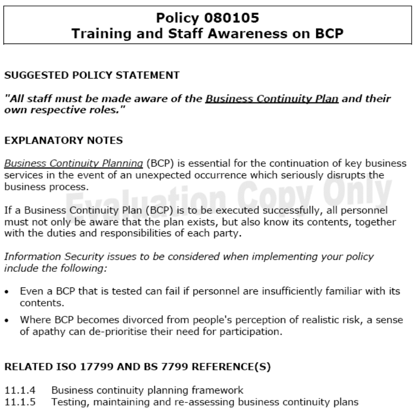
Information Security issues to be considered when implementing your policy include the following:

- Inadequate Internet Security safeguards can allow unauthorised access to your network, with potentially disastrous consequences.
- Weak dial-in security standards can give unauthorised access to your network, the consequences of which could be very serious.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.4.3 User authentication for external connections

♦ Extract of Policy Statement Publication from www.computer-security-policies.com - all rights recognised



Policy 080105
Training and Staff Awareness on BCP

SUGGESTED POLICY STATEMENT

"All staff must be made aware of the Business Continuity Plan and their own respective roles."

EXPLANATORY NOTES

Business Continuity Planning (BCP) is essential for the continuation of key business services in the event of an unexpected occurrence which seriously disrupts the business process.

If a Business Continuity Plan (BCP) is to be executed successfully, all personnel must not only be aware that the plan exists, but also know its contents, together with the duties and responsibilities of each party.

Information Security issues to be considered when implementing your policy include the following:

- Even a BCP that is tested can fail if personnel are insufficiently familiar with its contents.
- Where BCP becomes divorced from people's perception of realistic risk, a sense of apathy can de-prioritise their need for participation.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

11.1.4 Business continuity planning framework
11.1.5 Testing, maintaining and re-assessing business continuity plans

♦ Extract of Policy Statement Publication from www.computer-security-policies.com - all rights recognised

Considerations for Registry Managers……

- Physical threats – Fire, Flood, Bomb, Fiber cut, building security ……
- Logical threats – Data Corruption, Connectivity loss, Hackers, Disc failures, Server failures….
- Not so logical – Neighbourhood catastrophe, Economic, Political ……
- Diversify locations – maintain multiple locations, replicate data, systems and staff, make sure each location can mitigate each other's risk
- Expect the unexpected – practice/train staff for "what if" situations, have muliple staff aware of each others tasks, avoid single points of failure

And then……..

- Think of the unexpected some more then ….. Practice some more
- Review and Maintain
- Simple, isn't it?
- No, it is appreciated that compliance with BS7799 is a **significant** undertaking
- But, as the benefits themselves are significant…it is not only good practice, but makes good sense to adopt the standard

What are the Benefits –

Why think about it?

- **Define responsibilities, assess risk, cheaper Insurance premiums;**
- **Higher quality of service to LIC as processes thought through with risk assessments;**
- **Continuous assessment and more efficient operations**
- **Higher staff moral and greater sense of knowing what to do in the event of a crisis**
- **Is it necessary to seek ISO17799 Accreditation? – some Registries have done it but it is not essential to be accredited but useful to follow the guidelines.**