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

ISO/IEC 17799: 2000

Recognition as a suitable platform for ISM

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

BS7799: PART 2 ISMS

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 Crux of the Matter

- Information is subject to numerous risks; which can be grouped together under the generic headings of:
  - Accidental
  - Natural
  - Deliberate
- 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**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Define the Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Define Scope of ISMS</td>
</tr>
<tr>
<td>Step 3</td>
<td>Undertake RA Risk Assessment</td>
</tr>
<tr>
<td>Step 4</td>
<td>Manage Risk</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select Control Objectives</td>
</tr>
<tr>
<td>Step 6</td>
<td>Statement of Applicability</td>
</tr>
</tbody>
</table>

**Policy Statement**

**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 two business services, in the event of an unexpected occurrence which seriously disrupts the business process.

A Business Continuity Plan (BCP) is an essential requirement, 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:

- A BCP that is tested is useful if personnel are sufficiently familiar with its contents.
- Where BCP becomes dependent on people’s perception of residual risk, a series of quality use plan should be prioritized for participation.

**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 multiple staff aware of each others tasks, avoid single points of failure

**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.