Overview of ISO17799 security standard

Massimo Nardone, TKK, S-38.153 Security of Communication Protocols

Security aspects by area

- **Network**
- Logging/Auditing of network devices
  Firewall (types, management, procedures)
  Remote Access
  Passive intrusion detection
- **Services/Applications**
- Account authorization
  Account termination
  Accounts Lockout and Password Settings
  Intrusion Detection
  Data handling requirements
  Application misuse protection – viruses, buffer overflows etc.
  CM Controls
  Logging/Auditing
- **Platforms/Servers/Devices**
- Patch levels and procedures to update as new ones are released
  Account authorization and termination
  Accounts Lockout and Password Settings
  Intrusion Detection
  Data handling requirements
  Logging/Auditing
- **Data handling**
- Notebooks and laptops
  VPN issues
  Home workers
  E-mail encryption
  Anti-virus
- **Corporate image/liabilities**
- Internet monitoring
  Email monitoring
  Mail relaying
  Spam
- **Other**
- Incident Response
  DRP
  Backups
  Physical Security

Security Standards

- **BS7799, ISO 17799**
- **Common Criteria**
- **TCSEC, ITSEC**
- **SSE-CMM**
- **GASSP**
- **COBIT**
- **Open Web Application Security Project**
- **etc**

Introducing ISO 17799: What is it?

- **“A comprehensive set of controls comprising best practices in information security”**
- **Basically… an internationally recognised generic information security standard (policy)**

Introducing ISO 17799

ISO/IEC 17799 Information Security Standard comes in two parts:

- **ISO/IEC 17799:2000 (Part 1)** is the standard code of practice and can be regarded as a comprehensive catalogue of good security things to do.

- **BS7799-2:2002 (Part 2)** is a standard specification for an Information Security Management Systems (ISMS). An ISMS is the means by which Senior Management monitor and control their security, minimising the residual business risk and ensuring that security continues to fulfil corporate, customer and legal requirements.

Background to BS 7799

- Department of Trade and Industry's Code of Practice for Information Security Management issued September 1993
- BS 7799 published in September 1995
- Objectives are to;
  - Provide a common basis for Information Security Management in organisations
  - Provide confidence in inter-organisational trading

Why BS7799?

- Benefits
  - A good structure to start with
  - Understood across industry
  - Certification possibilities

- Weaknesses
  - Inconsistencies in level of detail
  - Very much a guideline as opposed to an actual standard
  - Areas missing

The History of BS7799 1/2

- First published as Department of Trade and Industry's Code of Practice in UK
- Rebadged and published as Version 1 of BS7799 published in Feb 1995
- NOT widely embraced - for various reasons, including:
  - not flexible enough
  - simplistic ‘key control’ approach
  - other more pressing issues (eg: Y2k, EMU, etc)

The History of BS7799 2/2

- **Major revision of BS7799... Version 2 published in May 1999**
- **Formal certification and accreditation schemes launched in the same year**
- **Supporting tools start to appear**
- **Fast track ISO initiative accelerated**
- **Published as ISO standard**

BS 7799 Sections

BS 7799 is organized into 10 sections:

1. Business Continuity Planning
2. System Access Control
3. System Development and Maintenance
4. Physical and Environmental Security
5. Compliance
6. Personnel Security
7. Security Organisation
8. Computer & Network Management
9. Asset Classification and Control
10. Security Policy

BS 7799 Key Controls

- Information Security Policy document
- Allocation of Information Security responsibilities
- Information Security education and training
- Reporting of security incidents
- Virus controls
- Business Continuity Planning process
- Control of proprietary software copying
- Safeguarding of organisational records
- Data Protection
- Compliance with security policy

BS 7799 for Auditing

- **Product Auditing:** Based on the Security Model BS7799 and ISO/IEC 17799.

  Auditing a network might involve the following:
  - Doing penetration testing of firewalls.
  - Port scanning.
  - Installing intrusion detection software.
  - Analysing and reporting on Internet attack paths.
  - Evaluating service access within your local LAN.
  - Tracking your administrators' maintenance activities.
  - Trying password cracking on all authentication services.
  - Monitoring the activity of legitimate user accounts.

- **Security Audit Tool: COBRA, C&A Systems Security Ltd**

BS 7799 for Security Policy

When creating a new policy ensure it covers all ISO 17799 issues

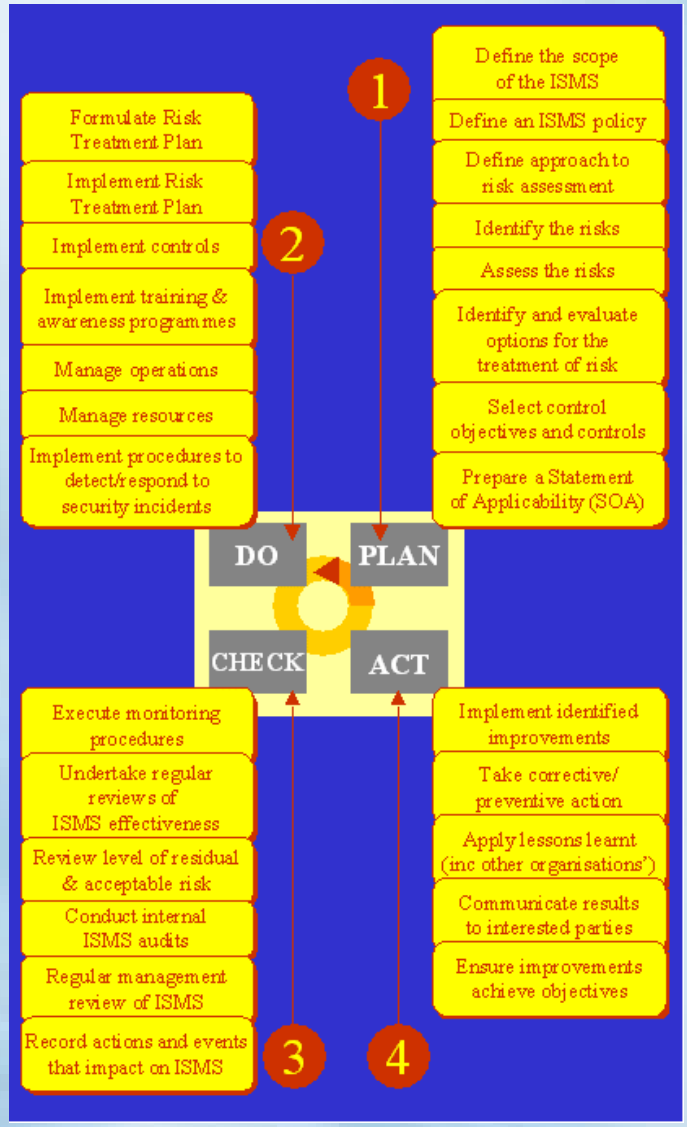
Security Policy covered areas:

- Risk Assessments
- Password Policies
- Administrative Responsibilities
- User Responsibilities
- E-mail Policies
- Internet Policies
- Disaster Recovery (Backup and Restore)
- Intrusion Detection

BS 7799 for ISMS Policy

An Information Security Management System (ISMS) developed according to ISO 17799 and BS 7799-2 is one of the best ways to control the specific risks associated with information systems, thus increasing their reliability.

Here the major steps towards BS7799-2 compliance: The standard is predicated on the Plan-Do Check-Act cycle (established over 50 years ago in Japan).



The future of 17799

- **The Revision of ISO/IEC 17799:**
  ISO/IEC 17799:2000 is under revision and is expected to be complete in the late 2004 early 2005 timeframe. The most significant change is expected to be in the layout of the controls, to clearly distinguish between the requirements, implementation guidance and further information.

- **The Development of Part 3?**
  Will there be a Part 3? and if so what will it be about? There has been speculation about the development of a Part 3 since June/July 2002, based on the observation that ISO 9000 has four parts and BS7799-2:2002 is closely related to ISO 9001:2000. A new Part 3 could therefore be concerned with the continual improvement of an ISMS (similar to the intent of ISO 9004), but other topics have been identified, such as auditing and integrating ISMS with other management systems.

Questions?