

## ISO 17799

International Organization for Standardization  
Information Technology – Code of Practice for  
Information Security Management



# Agenda

- ISO Definition
- History of ISO 17799
- ISO 17799 Certification
- Scope of ISO 17799
- ISO Control Objectives



# ISO Definition

- **The International Organization for Standardization (ISO)** is a worldwide federation of national standards bodies from more than 140 countries



# ISO Definition

- Information Security
  - Preservation of:
    - Confidentiality
      - Ensuring that information is accessible only to those authorized to have access
    - Integrity
      - Safeguarding the accuracy and completeness of information and processing methods
    - Availability
      - Ensuring that authorized users have access to information and associated assets when required



# History of ISO 17799

- 1989 – BS PD 0003, A code of practice for information security management
- 1995 – Updated and re-issued as BS 7799
- 1998 – Part 2 of BS 7799 issued
- 1999 – First major revision to BS 7799-1
- 2000 – ISO 17799 was identical in technical content to BS 7799-1
- 2002 – Major revision to BS 7799-2



# History of ISO 17799

- Based on British Standard BS 7799
  - Replaced BSI 7799-1
  - BSI 7799-2 still exists and is current
    - Updated September 2002
  - Part 2 describes how to build and assess a security management system



# ISO Certification

- Certification is not possible
- Unlike other ISO standards
  - ISO 17799 does not have mandatory requirements
  - ISO 17799 does not provide sufficient detail to base certification upon
- Can be certified against BS 7799-2



# Scope of ISO 17799

- Give recommendations for information security management
- Intended to provide a common basis for developing standards
- Comprehensive list of good security things to do
- Recommendations should be viewed in accordance with applicable laws and regulations (Such as GLB Act)



# Scope of ISO 17799

- Developing Your Own Guidelines
  - “This Code of Practice may be regarded as a starting point for developing organization specific guidance”
  - “Not all of the guidance and controls in this Code of Practice may be applicable”



# Scope of ISO 17799

- 10 Control Objectives
- 127 Security Controls
- 5000 Controls and Elements of Best Practice



# Scope of ISO 17799

- 10 Control Objectives
  - Organizational Security Policy
  - Organizational Security Infrastructure
  - Asset Classification And Control
  - Personnel Security
  - Physical And Environmental Security
  - Communications And Operations Management
  - Access Control
  - Systems Development And Maintenance
  - Business Continuity Management
  - Compliance



# Scope of ISO 17799

- Control Objective
- Control
  - Control satisfies the requirements of the objective
- Implementation Guidance
  - Advice and help on implementation of the control
- Other Information
  - Other supporting help and information



# ISO Control Objectives

- Security Policy
  - Information Security Policy
    - To provide management direction and support for information security.



# ISO Control Objectives

- Organizational Security
  - Information Security Infrastructure
    - To manage information security within the organization.
  - Security of Third Party Access
    - To maintain the security of organizational information processing facilities and information assets accessed by third parties.
  - Outsourcing
    - To maintain the security of information when the responsibility for information processing has been outsourced to another organization.



# ISO Control Objectives

- Asset Classification and Control
  - Accountability for Assets
    - To maintain appropriate protection of organizational assets.
  - Information Classification
    - To ensure that information assets receive an appropriate level of protection.



# ISO Control Objectives

- Personnel Security
  - Security in Job Definition and Resourcing
    - To reduce the risks of human error, theft, fraud or misuse of facilities.
  - User Training
    - To ensure that users are aware of information security threats and concern, and are equipped to support organizational security policy in the course of their normal work.
  - Responding To Security Incidents And Malfunctions
    - To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents.



# ISO Control Objectives

- Physical and Environmental Security
  - Secure Areas
    - To prevent unauthorized access, damage and interference to business premises and information.
  - Equipment Security
    - To prevent loss, damage or compromise of assets and interruption to business activities.
  - General Controls
    - To prevent compromise or theft of information and information processing facilities.



# ISO Control Objectives

- Communications and Operations Management
  - Operational Procedures and Responsibilities
    - To ensure the correct and secure operation of information processing facilities.
  - System Planning and Acceptance
    - To minimize the risk of systems failures.
  - Protection Against Malicious Software
    - To protect the integrity of software and information.



# ISO Control Objectives

- Communications and Operations Management (continued)
  - Housekeeping
    - To maintain the integrity and availability of information processing and communication services.
  - Network Management
    - To ensure the safeguarding of information in networks and the protection of the supporting infrastructure
  - Media Handling and Security
    - To prevent damage to assets and interruptions to business activities.



# ISO Control Objectives

- Communications and Operations Management (continued)
  - Exchanges of Information and Software
    - To prevent loss, modification or misuse of information exchanged between organizations.



# ISO Control Objectives

- Access Control
  - Business Requirement for Access Control
    - To control access to information.
  - User Access Management
    - To prevent unauthorized access to information systems.
  - User Responsibilities
    - To prevent unauthorized user access.
  - Network Access Control
    - Protection of networked services.



# ISO Control Objectives

- Access Control (continued)
  - Operating System Access Control
    - To prevent unauthorized computer access.
  - Application Access Control
    - To prevent unauthorized access to information held in information systems.
  - Monitoring System Access and Use
    - To detect unauthorized activities.
  - Mobile Computing and Teleworking
    - To ensure information security when using mobile computing and teleworking facilities.



# ISO Control Objectives

- Systems Development and Maintenance
  - Security Requirements of Systems
    - To ensure that security is built into information systems.
  - Security in Application Systems
    - To prevent loss, modification or misuse of user data in application systems.
  - Cryptographic Controls
    - To protect the confidentiality, authenticity or integrity of information.



# ISO Control Objectives

- Systems Development and Maintenance (continued)
  - Security of System Files
    - To ensure that IT projects and support activities are conducted in a secure manner.
  - Security in Development and Support Process
    - To maintain the security of application system software and information.



# ISO Control Objectives

- Business Continuity Management
  - Aspects of Business Continuity Management
    - To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.



# ISO Control Objectives

- Compliance
  - Compliance with Legal Requirements
    - To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.
  - Reviews of Security Policy and Technical Compliance
    - To ensure compliance of new systems with organization security policies and standards.
  - System Audit Considerations
    - To maximize the effectiveness of and to minimize interference to/from the system audit process.



# Resources

- BSI Group  
[www.bsi.org.uk](http://www.bsi.org.uk)
- International Organization for Standardization  
[www.iso.org](http://www.iso.org)
- American National Standards Institute  
[www.ansi.org](http://www.ansi.org)



# Questions?

Patrick A. Morin, CPA, CISM  
Principal

Baker Newman & Noyes

Information Technology Consulting Division

(800) 244-7444

[pmorin@bnn CPA.com](mailto:pmorin@bnn CPA.com)

