

# ISO/IEC 17799 Revision

by J.J. Lee, BSI Korea

- 11 Main categories 39 Clauses 133 Controls
- Risk Assessment and Treatment
- Control Description
- More Detail

## □ 11 Main category 39 Clause 133 Control

OLD	New
Security Policy	Security Policy
Organizational Security	Organizing information Security
Asset classification and Control	Asset Management
Personnel security	Human Resource Security
Physical and Environmental Security	Physical and Environmental Security
Communication and Operations Management	Communication and Operations Management
Access Control	Access Control
System Development and Maintenance	Information Systems Acquisition, Development and Maintenance
	Information Security Incident Management
Business Continuity Management	Business Continuity Management
Compliance	Compliance

## ❑ **Security Policy**

OLD :

Review and evaluation -> Only Policy Review

NEW :

Review and evaluation -> The result of Management Review

## ❑ **Organizing Information Security**

Confidential Agreement from Personnel Security

Management Commitment vs. Security Forum

3<sup>rd</sup> Party -> External Party

Addressing security when dealing with customers

## □ **Asset Management**

Ownership of Asset

-What to do

-Who is

Acceptable Use of Assets

## □ Human Resource Security

### 8.1 Prior to employment

- Role and Responsibilities

- Screening

- Term and Conditions of Employment

### 8.2 During employment

- Management Responsibilities

- Information Security Awareness Education and Training

- Disciplinary Process

### 8.3 Termination or Change of employment

- Termination Responsibilities

- Return of Assets

- Removal of Access Rights

## **Physical and Environmental Security**

Power supplies -> Supporting utilities

Clear Desk and Clear Screen Policy is Access Control

## □ **Communication and Operation Management**

Thirdparty Service Delivery management

Service Delivery

Monitoring and Review of Thirdparty Services

Managing Changes to Thirdparty Services

Control against Mobile Code

Information Exchange Policies and Procedure

Security of E-Mail -> Electronic Message

## Access Control

‘Duress Alarm’ -> ‘Incident report ‘

## ❑ Information system Acquisition, Development , Maintenance

The Depth of the Cryptographic Controls

Covert channels and Trojan code -> Information Leakage

Vulnerability Management

## □ Information Security Incident Management

### 13.1 Reporting Information Security Event and Weakness

13.1.1 Reporting Information Security Event

13.1.2 Reporting Security Weakness

### 13.2 Management of Information Security Incident and Improvements

13.2.1 Responsibilities and Procedure

13.2.2 Learning from Information Security Incidents

13.2.3 Collection of Evidence

## □ Control Description

Control

Implementation Guidance

Actions that should be undertaken to implement the control

Other Information

Explanation related to the implementation of the control