International Standards and Information Safety

Understanding the role of international standards in information security and reviewing key frameworks like ISO 17799 and ISO 15408 that provide a basis for managing and evaluating IT security.

The Foundation of Security Standards

The Challenge

As networks and electronic services grew, standardization became critical. Computer information security emerged when data value became significant, intensifying with network development and electronic service demand.

The Solution

International standards create a common basis for interaction between manufacturers, consumers, and security experts—establishing shared language and frameworks for protecting digital assets.

Three Key Stakeholders

Consumers

Need methodology to choose products meeting their needs and a safety rating scale. Require tools to formulate requirements to manufacturers.

Manufacturers

Develop IT products with security features. Balance security requirements with functionality, usability, and compatibility demands.

Security Experts

Evaluate and certify IT products. Assess security levels and verify compliance with established standards and criteria.

Core Components of Information Security Management

01

Define Security Goals

Determine information security objectives for computer systems aligned with organizational needs.

02

Create Management System

Establish an effective information security management system with clear policies and procedures.

03

Establish Indicators

Calculate qualitative and quantitative indicators to assess conformity with security goals.

04

Deploy Tools

Use security tools to ensure protection and assess current status of information assets.

05

Manage Continuously

Apply management techniques to objectively assess and manage company information security.

ISO/IEC 17799 (BS 7799)

Information Security Management Code of Practice

Developed from British standard BS 7799-1:1995, this international standard represents a new generation of information security frameworks. Revised in 2002 with substantial updates focusing on security culture.

BS 7799-2:2000 defines functional specifications for corporate information security management systems and regulates audit procedures.

Key Coverage Areas

- Security policy development
- Organization of security
- Asset classification
- Personnel management
- Physical security
- Access control
- Business continuity

ISO 17799 Comprehensive Framework

Security Policy

Company information security policy and strategic direction

Audit

Internal security audits and compliance verification

Access Control

System access management and authentication

Organization

Enterprise information security structure and responsibilities

Asset Management

Classification and management of information resources

Personnel

Human resources management and security awareness

German BSI Standard

Guidelines for IT Protection at Basic Security Level

Detailed Methodology

General methodology for managing information security, including organization and implementation guidance.

IT Components

Descriptions of modern IT components, hardware, software, and network technologies from leading suppliers.

Comprehensive Catalogs

Over 600 items each in detailed catalogs of security threats and control measures.

Unlike ISO 17799, BSI provides detailed review of particular information security management issues, covering organizational and technical protection levels, emergency response, and business continuity.

ISO 15408: Common Criteria

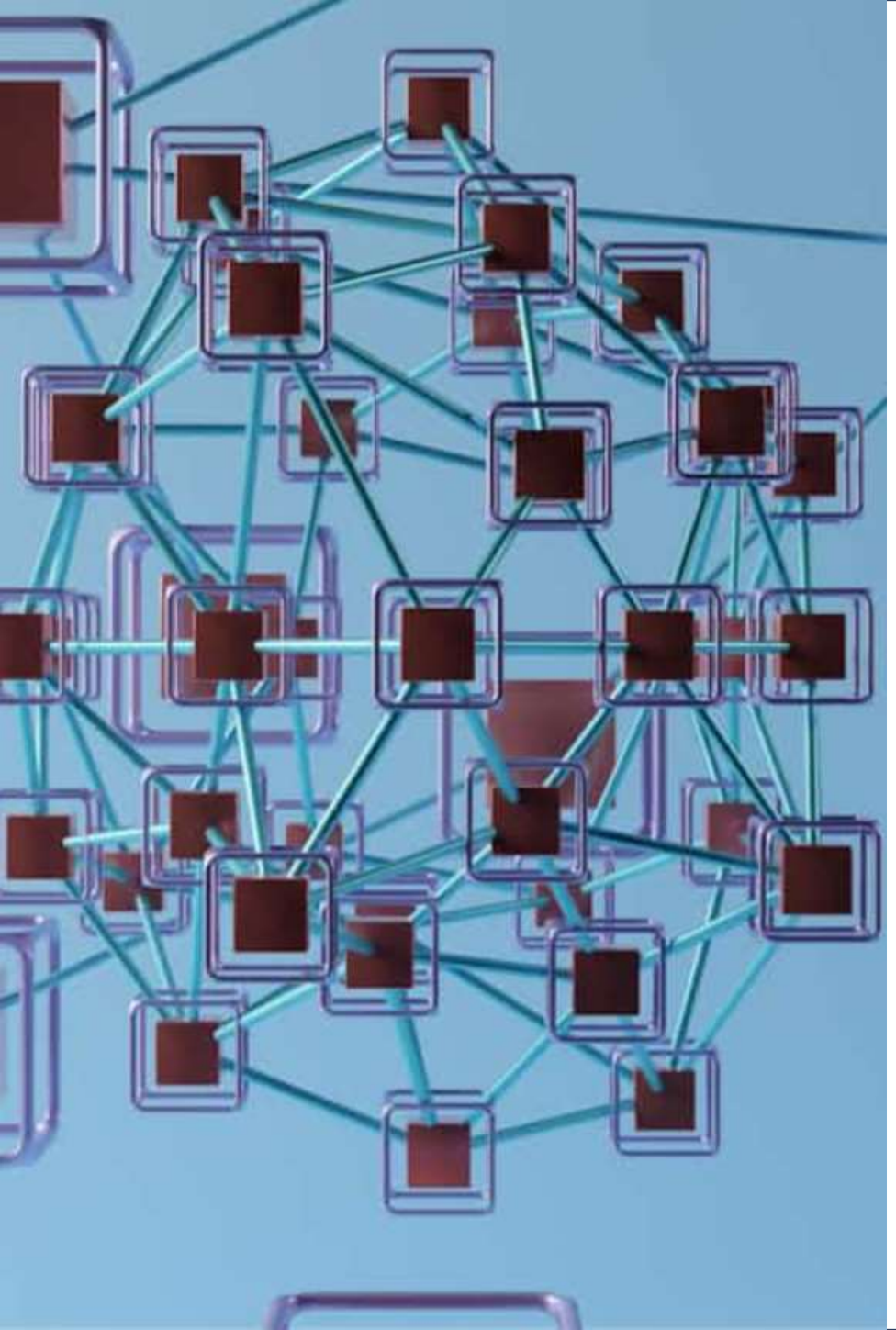
General Information Technology Security Evaluation Criteria

Development History

Developed over a decade starting in 1990 by leading security agencies from USA, Canada, Germany, Netherlands, England, and France. Approved June 8, 1999 as ISO/IEC 15408. Summarized Orange Book, European and Canadian criteria, embodying best practices into real structures.

Key Advantages

- Complete safety requirements and systematization
- Flexibility in application across diverse IT products
- Openness for further development and adaptation
- International-level IT standardization
- Unified secure information space creation



Common Criteria Security Concept

1

Information Security Definition

Combination of confidentiality and integrity of processed information, plus availability of resources.

2

Protection Means

Counter threats relevant to operating environment and implement adopted security policy.

3

Security Features

IT products include features countering threats and addressing vulnerabilities in design, production, and operation.

4

Certification Process

Confirms adequacy of protective equipment to threats and risks at global level.

Key Takeaways

Standards Create Common Ground

International standards establish shared frameworks for manufacturers, consumers, and security experts to interact effectively.

ISO 17799: Management Framework

Provides comprehensive code of practice covering security policy, organization, access control, and business continuity.

BSI: Detailed Methodology

German standard offers over 600 cataloged threats and controls with specific guidance for IT components.

ISO 15408: Global Evaluation

Common Criteria enables international certification, creating unified secure information space for IT products.

Review questions:

1. What is the main objective of information security standards?
2. What are some of the key issues addressed in the ISO/IEC 17799 (BS 7799) standard?
3. How does the German BSI standard differ from ISO 17799, according to the text?
4. What is the "Common Criteria" (ISO 15408) standard used for?
5. Who are the three main groups of specialists that the "Common Criteria" (ISO 15408) was developed to serve?

Recommended literature list:

1. Calder, A., & Watkins, S. (2008). IT Governance: A Manager's Guide to Data Security and ISO 27001/ISO 27002. Kogan Page Publishers.

2. International Organization for Standardization. (2005). ISO/IEC 17799:2005: Information technology — Security techniques — Code of practice for information security management. ISO.

3. International Organization for Standardization. (2009). ISO/IEC 15408: Information technology — Security techniques — Evaluation criteria for IT security (Common Criteria). ISO.

4. Bundesamt für Sicherheit in der Informationstechnik (BSI). (2008). BSI-Standard 100-1: Information Security Management Systems. BSI.