

BS7799-2 to ISO 27001 transition arrangements

With the release of ISO 27001, BS 7799 Part 2 has been withdrawn just as BS 7799 part 1 was withdrawn and replaced by ISO 17799.

The accredited certification bodies have transition arrangements to handle the replacement of BS 7799-2 by ISO 27001. If your organization already has its BS 7799-2 certificate (well done!) contact your certification body to check how they plan to handle the process of moving to the new ISO standard. Your BS 7799-2 certificate will probably be replaced by an ISO 27001 certificate at the time of your next full certification visit.

Introduction

ISO/IEC 17799:2005, the [latest version](#) of the ISO standard “Information technology - Security techniques - **Code of practice for information security management**”, to give it its full title, is an internationally-accepted standard of good practice for information security. Thousands of organizations worldwide follow ISO 17799, with [over 2,000](#) of them in effect being certified compliant using [ISO 27001](#) (previously known as BS 7799-2).

A brief history of ISO 17799

DTI Code of Practice

The history of ISO 17799 traces back to a code of practice published by the UK Department of Trade and Industry, itself based heavily on an internal security standard used by an oil company.

BS 7799

The code of practice was formally released by the British Standard Institute (BSI) as **BS 7799** in 1995.

ISO 17799:2000

After a difficult period of international consideration and review, BS 7799 was finally adopted by ISO and was released as ISO 17799 in 2000.

ISO 17799:2005

ISO 17799 was revised and reissued in June 2005. Advice on risk and incident management was consolidated into two new sections. Please see below for further information.

ISO 27002:2007?

ISO 17799 is due to be renamed ISO/IEC 27002, bringing it into line with the other [ISO 27000 series standards](#) “from Q1 2007” (according to Robert Whitcher of BSI). This is currently expected to be a straight number change not an update although these things have a habit of changing.

Scope of ISO 17799

Like governance, information security is a broad topic with ramifications in all parts of the modern organization. It is relevant to all types of organization including commercial enterprises of all sizes (from one-man-bands up to multinational giants), not-for-profits, charities, government departments and quasi-autonomous bodies - in fact any organization that handles and depends on information. The specific information security requirements may be different in each case but the point of ISO 17799 is that there is a lot of common ground.

Relationship to ISO 27001

[ISO 27001](#) defines the requirements for an Information Security Management System (ISMS), in turn using ISO 17799 to incitate suitable information security controls within the ISMS. [ISO 27001](#) is essentially a direct replacement for BS 7799 part 2. It incorporates a summary of ISO 17799:2005 controls as an appendix.

Structure and format of ISO 17799:2005

ISO 17799 is a generic, advisory document. It lays out a well structured set of controls to address information security risks, covering confidentiality, integrity and availability aspects. Organizations that adopt ISO 17799 must assess their own information security risks and apply suitable controls, using the standard for guidance. Strictly speaking, none of the controls are mandatory but if an organization chooses not to adopt something as common as, say, antivirus controls, they should certainly be prepared to demonstrate that this decision was reached through a rational process, not just an oversight.

39 control objectives

After the introduction, scope, terminology and structure sections, the remainder of ISO 17799:2005 specifies some 39 control objectives to protect information assets against threats to their confidentiality, integrity and availability. In effect, **these control objectives comprise the functional requirements specification for an organization’s information security management architecture.**

Few people would quarrel with most of the control objectives, or, to put that an other way, it would be difficult to argue that the organization should *not* conform with the stated objectives in general. However, a few are not applicable in every case, and the generic wording of the standard does not necessarily reflect the organization’s precise requirements.

In our experience, the control objectives make an excellent starting point to define a set of “axioms” or high level principles for information security policies with only slight re-wording.

Hundreds of specific controls

ISO 17799 refers to hundreds of best-practice information security control measures that organizations should consider to satisfy the stated control objectives. The standard does not mandate specific controls but leaves it to the user organizations to select and implement controls, using a risk-assessment process to identify the most appropriate controls for their specific requirements. They are also free to select controls not listed in the standard, just so long as their control objectives are satisfied. **We treat the ISO standard as a generic controls menu from which organizations select their own meals.**

Not mandating specific controls is a master stroke that makes the standard broadly applicable even as the technology and security risks change, and gives users tremendous flexibility in the implementation. Unfortunately, it also makes it difficult for the certification bodies to assess whether an organization is fully compliant with the standard, hence there are no formal certificates against ISO 17799 itself. Organizations may instead get their information security governance/management processes certified against [ISO 27001](#) which describes the process for assessing risks and selecting, implementing and managing specific security controls from ISO 17799.

Contents of ISO 17799:2005 (outline)

Section 0: Introduction

Starting from ‘What is information security?’, the introduction explains how to make use of the standard.

Section 1: Scope

The standard gives information security management recommendations for those who are responsible for initiating, implementing or maintaining security.

Section 2: Terms and definitions

“Information security” is explicitly defined as the “preservation of confidentiality, integrity and availability of information”. These and other related terms are further defined.

Section 3: Structure of this standard

This page simply explains that the guts of the standard contain control objectives, suggested controls and implementation guidance.

Section 4: Risk assessment and treatment

ISO 17799:2000 hardly mentioned the important topic of information security risk management - it was relegated to a brief entry in the introduction. ISO 17799:2005 promotes the coverage to a main section containing a whole page and a half ... still woefully inadequate for such a complex subject but we can only hope that future versions will expand further

and/or refer to other useful resources (see the [other standards page](#) for some suggestions such as ISO/IEC TR 13335-3 noted in section 12.1.1).

Section 5: Security policy

Management should define a policy to clarify their direction of, and support for, information security.

Section 6: Organization of information security

A suitable information security governance structure should be designed and implemented.

6.1 Internal organization

The organization should have a management framework for information security. Senior management should provide direction and commit their support, for example by approving information security policies. Roles and responsibilities should be defined for the information security function. Other relevant functions should cooperate and coordinate their activities. IT facilities should be authorized. Confidentiality agreements should reflect the organization's needs. Contacts should be established with relevant authorities (*e.g.* law enforcement) and special interest groups. Information security should be independently reviewed.

6.2 External parties

Information security should not be compromised by the introduction of third party products or services. Risks should be assessed and mitigated. when dealing with customers and in third party agreements.

Section 7: Asset management

The organization should be in a position to understand what information assets it holds, and to manage their security appropriately.

7.1 Responsibility for assets

All [information] assets should be accounted for and have a nominated owner. An inventory of information assets (IT hardware, software, data, system documentation, storage media and ICT services) should be maintained. The inventory should record ownership and location of the assets, and owners should identify acceptable uses.

7.2 Information classification

Information should be classified according to its need for security protection and labeled accordingly.

Section 8: Human resources security

The organization should manage system access rights *etc.* for 'joiners, movers and leavers', and should undertake suitable security awareness, training and educational activities.

8.1 Prior to employment

Security responsibilities should be taken into account when recruiting permanent employees, contractors and temporary staff (*e.g.* through adequate job descriptions, pre-employment screening) and included in contracts (*e.g.* terms and conditions of employment and other signed agreements on security roles and responsibilities).

8.2 During employment

Management responsibilities regarding information security should be defined. Employees and (if relevant) third party IT users should be made aware, educated and trained in security procedures. A formal disciplinary process is necessary to handle security breaches.

8.3 Termination or change of employment

Security aspects of a person's exit from the organization (*e.g.* the return of [information] assets and removal of access rights) or change of responsibilities should be managed.

Section 9: Physical and environmental security

Valuable IT equipment should be physically protected against malicious or accidental damage or loss, overheating, loss of mains power *etc.*

9.1 Secure areas

This section describes the need for concentric layers of physical controls to protect sensitive IT facilities from unauthorized access.

9.2 Equipment security

Critical IT equipment, cabling *etc.* should be protected against physical damage, fire, flood, theft *etc.*, both on- and off-site. Mains power supplies and cabling should be secured. IT equipment should be maintained and disposed of securely.

Section 10: Communications and operations management

This lengthy section describes security controls for systems and network management.

10.1 Operational procedures and responsibilities

IT operating responsibilities and procedures should be documented. Changes to IT facilities and systems should be controlled. Segregation of duties should be applied where relevant (*e.g.* access to development and operational systems should be segregated).

10.2 Third party service delivery management

Security requirements should be taken into account in third party service delivery (*e.g.* IT facilities management or outsourcing), from contractual terms to ongoing monitoring and change management.

10.3 System planning and acceptance

Covers IT capacity planning and production acceptance processes.

10.4 Protection against malicious and mobile code

Describes the need for anti-malware controls, including user awareness. Security controls for mobile code 'associated with a number of middleware services' are also outlined.

10.5 Back-up

Covers routine data backups and rehearsed restoration.

10.6 Network security management

Outlines secure network management, network security monitoring and other controls. Also covers security of commercial network services such as private networks and managed firewalls *etc.*

10.7 Media handling

Operating procedures should be defined to protect documents and computer media containing data, system information *etc.* Disposal of backup media, documents, voice and other recordings, test data *etc.* should be logged and controlled. Procedures should be defined for securely handling, transporting and storing backup media and system documentation.

10.8 Exchange of information

Information exchanges between organizations should be controlled, for example through policies and procedures, and legal agreements. Information exchanges should also comply with applicable legislation. Security procedures and standards should be in place to protect information and physical media *in transit*, including electronic messaging (email, EDI and IM) and business information systems.

10.9 Electronic commerce services

The security implications of eCommerce (online transaction systems) should be evaluated and suitable controls implemented. The integrity and availability of information published online (*e.g.* on websites) should also be protected.

10.10 Monitoring

Covers security event/audit/fault logging and system alarm/alert monitoring to detect unauthorized use. Also covers the need to secure logs and synchronize system clocks.

Section 11: Access control

Logical access to IT systems, networks and data must be suitably controlled to prevent unauthorized use.

11.1 Business requirement for access control

The organization's requirements to control access to information assets should be clearly documented in an access control policy, including for example job-related access profiles (role based access control).

11.2 User access management

The allocation of access rights to users should be formally controlled through user registration and administration procedures (from initial user registration through to removal of access rights when no longer required), including special restrictions over the allocation of privileges and management of passwords, and regular access rights reviews.

11.3 User responsibilities

Users should be made aware of their responsibilities towards maintaining effective access controls *e.g.* choosing strong passwords and keeping them confidential. Systems and information should be secured when left unattended (*e.g.* clear desk and clear screen policies).

11.4 Network access control

Access to network services should be controlled, both within the organization and between organizations. Policy should be defined and remote users (and possibly equipment) should be suitably authenticated. Remote diagnostic ports should be securely controlled. Information services, users and systems should be segregated on networks (*e.g.* into separate logical domains). Network connections and routine should be controlled where necessary.

11.5 Operating system access control

Operating system access control facilities and utilities (such as user authentication with unique user IDs and managed passwords, recording use of privileges and system security alarms) should be used. Access to powerful system utilities should be controlled and inactivity timeouts should be applied.

11.6 Application and information access control

Access to and within application systems should be controlled in accordance with a defined access control policy. Particularly sensitive applications may require dedicated (isolated) platforms, and/or additional controls if run on shared platforms.

11.7 Mobile computing and teleworking

There should be formal policies covering the secure use of portable PCs, PDAs, cellphones *etc.*, and secure teleworking ("working from home" and other forms of mobile working).

Section 12: Information systems acquisition, development and maintenance

Information security must be taken into account in the processes for specifying, building/acquiring, testing and implementing IT systems.

12.1 Security requirements of information systems

Automated and manual security control requirements should be analyzed and fully identified during the requirements stage of the systems development or acquisition process, and incorporated into business cases. Purchased software should be formally tested for security, and any issues risk-assessed.

12.2 Correct processing in application systems

Data entry, processing and output validation controls and message authentication should be provided to mitigate the associated integrity risks.

12.3 Cryptographic controls

A cryptography policy should be defined, covering roles and responsibilities, digital signatures, non-repudiation, management of keys and digital certificates *etc.*

12.4 Security of system files

Access to system files (both executable programs and source code) and test data should be controlled.

12.5 Security in development and support processes

Application system managers should be responsible for controlling access to [development] project and support environments. Formal change control processes should be applied, including technical reviews. Packaged applications should ideally not be modified. Checks should be made for information leakage *e.g. via* covert channels and Trojans if these are a concern. A number of supervisory and monitoring controls are outlined for outsourced development.

12.6 Technical vulnerability management

Technical vulnerabilities in systems and applications should be controlled by monitoring for the announcement of relevant security vulnerabilities, and risk-assessing and applying relevant security patches promptly.

Section 13: Information security incident management

Information security events, incidents and weaknesses (including near-misses) should be promptly reported and properly managed.

13.1 Reporting in information security events and weaknesses

An incident reporting/alarm procedure is required, plus the associated response and escalation procedures. There should be a central point of contact, and all employees, contractors *etc.* should be informed of their incident reporting responsibilities.

13.2 Management of information security incidents and improvements

Responsibilities and procedures are required to manage incidents consistently and effectively, to implement continuous improvement (learning the lessons), and to collect forensic evidence.

Section 14: Business continuity management

This section describes the relationship between IT disaster recovery planning, business continuity management and contingency planning, ranging from analysis and documentation through to regular exercising/testing of the plans. These controls are designed to minimize the impact of security incidents that happen despite the preventive controls noted elsewhere in the standard.

Section 15: Compliance

15.1 Compliance with legal requirements

The organization must comply with applicable legislation such as copyright, data protection, protection of financial data and other vital records, cryptography restrictions, rules of evidence *etc.*

15.2 Compliance with security policies and standards, and technical compliance

Managers and system owners must ensure compliance with security policies and standards, for example through regular platform security reviews, penetration tests *etc.* undertaken by competent testers.

15.3 Information systems audit considerations

Audits should be carefully planned to minimize disruption to operational systems. Powerful audit tools/facilities must also be protected against unauthorized use.