

## ISO-17799 – STANDARD FOR INFORMATION SECURITY: A WELCOME BOON FOR SECURITY MANAGEMENT AND AUDIT

LAWRENCE CAPUDER

Imagine — no, fantasize — as an IT audit security or audit professional that your organization has taken on a dedicated commitment toward information security, its risk assessment, design, implementation, and testing. This commitment is felt by all levels — from the board of directors to senior management, all the way down to the computer console operator. Try to visualize the impact on your job duties and status, and the compliance with major regulatory directives, such as the:

- Sarbanes–Oxley Act (for publicly financed companies)
- Health Insurance Portability and Accountability Act (HIPAA) (for organizations dealing with health issues)
- Gramm–Leach–Bliley Act (for financial institutions)

Such could be the result if an organization had a successful implementation of ISO-17799. What is an *information security management system* (ISMS)? What are the ISO-17799 and BS 7799-2 standards? What does it take to implement them and seek certification under BS 7799-2? What are their objectives? What are the experiences of a company that has been an early adopter? This article attempts to answer these questions.

### THE CONCLUSION

An auditor or security professional should seriously consider encouraging his or her organization to seek certification to the BS 7799-2 standard, whether the organization is already exploring the idea or the initiative comes from the auditor and security professionals. Of course, this should only be the case if senior management and the board of directors are supportive of the project. The standards consider “visible support and commitment from management” to be a *critical success factor*.

### IN THIS ISSUE

- ISO-17799 – Standard for Information Security: A Welcome Boon for Security Management and Audit
- The Twelve Principles of Trusted Solutions

**Editor**  
RICHARD O'HANLEY

**Editor Emeritus**  
BELDEN MENKUS, CISA



Perhaps it did not go far enough and should suggest that this comes from *all levels of management*.

The standards provide a useful framework for information security management so that an organization does not have to start from scratch. They also provide a practical methodology for implementation. The organization will need to decide whether it has sufficiently expert and available resources for implementation or it will need to hire a consultant. Whether to seek certification is up to the organization, which may be satisfied that the standard is well implemented and that internal audits show good compliance.

**MOST PEOPLE  
MISTAKENLY  
BELIEVE THAT  
ISO-9001 IS ONLY  
FOR  
MANUFACTURING  
CONCERNS, BUT  
EVEN SERVICE  
ORGANIZATIONS  
HAVE SOUGHT  
AND EARNED  
CERTIFICATION.**

### THE BSI AND ITS STANDARDS

The British Standards Institute (BSI) is probably best known for its ISO-9001 — Quality Management Systems certification program. Perhaps the reader might remember passing by a factory proudly displaying its banner announcing its ISO-9001 compliance. Most people mistakenly believe that that program is only for manufacturing concerns, but even service organizations, such as the American Institute of Certified Public Accountants (AICPA), have sought and earned the ISO-9001 certification.

The BSI's other standards include:

- ISO-9100 Aerospace Quality
- ISO-13485 Quality Management Systems for Medical Device Manufacturers
- ISO-14001 Environmental Management Systems
- ISO-16949 Automotive Quality Systems
- ISO-18001 Occupational Health and Safety

Don't ask how the BSI comes up with its numbering scheme — to be catchy and easy to remember doesn't seem to be one of its objectives. The BSI also suggests that it may be more efficient to combine quality, environmental, or occupational health and safety into an *integrated management system*.

---

**If you have information of interest to EDPACS, contact Richard O'Hanley, Editor, Auerbach Publications, 29 W. 35th Street, 7th Floor, New York, NY 10001 (rohanley@crcpress.com).** EDPACS (ISSN 0736-6981) is published monthly by Auerbach Publications, CRC Press LLC, 2000 NW Corporate Blvd., Boca Raton, FL 33431. Periodicals postage is paid at Boca Raton and additional mailing offices. The subscription rate is \$245/year in the U.S. Prices elsewhere vary. Printed in USA. Copyright 2004 EDPACS is a registered trademark owned by CRC Press LLC. All rights reserved. No part of this newsletter may be reproduced in any form — by microfilm, xerography, or otherwise — or incorporated into any information retrieval system without the written permission of the copyright owner. Requests to publish material or to incorporate material into computerized databases or any other electronic form, or for other than individual or internal distribution, should be addressed to Auerbach Publications, Editorial Services, 2000 NW Corporate Blvd., Boca Raton, FL 33431. All rights, including translation into other languages, reserved by the publisher in the U.S., Great Britain, Mexico, and all countries participating in the International Copyright Convention and the Pan American Copyright Convention. Authorization to photocopy items for internal or personal use, or the personal or internal use of specific clients may be granted by CRC Press LLC, provided that \$20.00 per article photocopied is paid directly to Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923 USA. The fee code for users of the Transactional Reporting Service is ISSN 0736-6981/04/\$20.00+\$0.00. The fee is subject to change without notice. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged. Product or corporate names may be trademarks or registered trademarks, and are only used for identification and explanation, without intent to infringe. POSTMASTER: Send address change to EDPACS, Auerbach Publications, CRC Press LLC, 2000 NW Corporate Blvd., Boca Raton, FL 33431.

Important to note is that all the standards include provisions for the need for both:

- External certification — by BSI personnel or those authorized by BSI
- Internal audit

The latter requirement either creates an entirely new breed of auditors or expands the scope of the traditional internal audit department significantly.

One of BSI's new and less widely known programs, especially in the North America, is its ISO-17799 standards for Information Security Management Systems (ISMS) — the current version is BS ISO/IEC 17799:2000 (hereafter referred to as: ISO-17799). The BS 7799-2:2002 (hereafter referred to as BS 7799-2) standards provide requirements as to how an auditor is to determine whether an organization is a compliant *information security management system* and therefore worthy of BSI certification. The latter standards also provide a listing of desirable control objectives.

One way of looking at the difference between ISO-17799 and BS 7799-2 is that:

- ISO-17799 provides a generic implementation framework.
- BS 7799-2 is a normative standard in which a reader will find the word “shall” a lot, because the organization “shall” do this and do that in order to be worthy of being certified under the standard. These criteria are the ones used by the certification auditor as a measuring stick.

Whether a company wishes to proudly announce its compliance with BS 7799-2 might totally depend on the nature of its business and its motivation for seeking the certification. For example, an IT service organization that serves multiple clients may be required to have an SAS-70 Auditor's Report (third party review). However, it may choose to voluntarily seek certification to BS 7799-2 as a marketing differentiator — a fact that it can include in its advertising and marketing brochures, unlike SAS-70 Report information, which has substantial usage and distribution restrictions.

On the other hand, a bank may seek the certification to BS 7799-2 in an effort to satisfy itself that its information security controls are well-designed and effective. This bank may be reluctant to publicize its certification out of fear that doing so would make it a target for hackers. Hackers love the challenge of “We've got a tight ship” so that they (the hackers) can say, “Oh, yeah? Let me find some chinks in that armor! I'm getting bored with organizations that only have ordinary security.”

## CONTENT AND QUALITY

Note the use of the term “information security” up to this point instead of “information technology security.” The cover of BS ISO/IEC 17799:2000 is entitled “Information

*AN IT SERVICE  
ORGANIZATION MAY  
CHOOSE TO  
VOLUNTARILY SEEK  
CERTIFICATION TO  
BS 7799-2 AS A  
MARKETING  
DIFFERENTIATOR.*

---

*EACH SERVICED ORGANIZATION HAS THE RESPONSIBILITY TO READ THIS REPORT TO BETTER UNDERSTAND CONTROLS AND CONTROL WEAKNESSES AT THE OUTSOURCING ORGANIZATION.*

technology — Code of practice for information security management.” This comes across as being somewhat ambiguous, starting with a reference to information technology but later using the term “information security management.” The BSI intends for the latter term to be operative because in the introduction to these standards, it states that “Information can exist in many forms.” It goes on to explain that “information security” should account for information that is electronic, paper, spoken, filmed, or transmitted. This revelation opens up the discussion beyond which many IT departments typically focus, and rightfully so. Many other departments will become part and parcel of the entire process from risk analysis to implementation to testing.

The reader can purchase paper copies of both the ISO-17799 and BS 7799 standards for \$150 directly from BSI Americas at [http://www.bsitraining.com/infosecurity\\_standards.asp](http://www.bsitraining.com/infosecurity_standards.asp). A CD-ROM version with the standards in Adobe Acrobat is available at a slightly higher price. Even if an organization is not thinking of implementing the standards, they represent good reference materials to have on hand.

Paging through the standard, an IT audit or security professional would certainly find an experience of “preaching to the choir.” Its content certainly reads very similar to Certified Information Systems Auditor (CISA) or Certified Information Systems Security Professional (CISSP) review materials.

The content is fairly comprehensive, although BSI points out that organizations may need to adapt it to their specific needs, adding and taking away as needed. Such is the nature of a standard meant for all types of organizations throughout the world.

The major weakness this author found was in terms of outsourcing standards. ISO-17799 places major emphasis on a contract with the outsourcing organization that requires them to have good security and includes a “right to audit clause.” This may all be fine and good, but in the United States, as this article earlier mentioned, outsourcing organizations are required to provide SAS-70 Service Organization Auditor Reports. Each *serviced* organization has the responsibility to read this report to better understand controls and control weaknesses at the outsourcing organization. Then they must analyze their controls related to preparation of data sent to the service organization and the interface between them.

The BSI means for ISO-17799 to be a global document, allowing worldwide acceptance. However, the author’s copy was written in British English, which, sporadically, is quite different from American English. For example, be prepared for “equipment sitting” as opposed to “equipment placement.” The reading of the standard, or most all of BSI’s documents, probably should not be done in one long sitting — they are certainly much drier than the latest fiction novel. BSI’s Business Development Manager assures the author that the documents that American implementers receive — either from materials

direct from their Web site or those received at BSI seminars — will be an *American translation*.

## ISO-17799 OBJECTIVES

ISO-17799 defines information security as:

Preservation of *confidentiality, integrity* and *availability* of information.

Confidentiality is straightforward, related to how only authorized users have access to information. Also straightforward is availability, relating to access to information and its equipment as needed.

Integrity may not be so simple. Integrity involves “safeguarding the accuracy and completeness...” By contract, the AICPA has its SysTrust Services, which also adds insuring proper *authorization* and *timeliness* as important objectives of integrity. Sarbanes–Oxley 103 (a)(2)(A)(iii)(II)(bb) also stresses the importance of proper authorization for financial statement integrity. The Statement on Auditing Standards (SAS) 55 provides requirements for an organization’s external financial audit and states that the auditor must test management’s various financial statement assertions, including:

1. Existence or occurrence
2. Completeness
3. Rights and obligations
4. Valuation or allocation
5. Presentation and disclosure

The conclusion here is that audit and security professionals should look carefully at the integrity objectives of the standards versus others that they must also work with — external financial statement audit, Sarbanes–Oxley, GLB, HIPAA, miscellaneous regulators, state regulations, local regulations, etc. *Controls flow from objectives*; and if one of the objectives is missing, then controls are almost certainly to be missing.

For example, the Sarbanes–Oxley Act deals with published financial reporting of publicly financed companies. Financial statements and the accounting and operational systems that generate them are a subset of an organization’s information management system. Therefore, the information security of all these subsets would be covered by an organization’s proper implementation of ISO-17799.

However, Sarbanes–Oxley places many more requirements than the information security of the accounting system in its broadest sense and the external audit of this system. The external auditor is not likely to find *totally sufficient* the work done literally to fulfill ISO-17799 standards, even with the caveat of an outside certification, to fulfill the requirements of Sarbanes–Oxley’s Section 404 — Management’s Assertion of Internal Controls.

---

*AUDIT AND  
SECURITY  
PROFESSIONALS  
SHOULD LOOK  
CAREFULLY AT THE  
INTEGRITY  
OBJECTIVES OF THE  
STANDARDS  
VERSUS OTHERS  
THAT THEY MUST  
ALSO WORK WITH.*

**AN ORGANIZATION SHOULD CONSULT WITH ITS EXTERNAL AUDITOR ABOUT THE IMPACT OF ISO-17799 ON THE EXTERNAL FINANCIAL REPORTING AUDIT — ESPECIALLY VIS À VIS SARBANES-OXLEY.**

Sarbanes–Oxley and ISO-17799 are likely to have a large majority of internal controls overlap. Also, to properly implement, both would find an organization looking carefully at internal control policies, performing an internal control risk assessment, as well as performing detailed documentation and testing of internal control procedures.

The bottom line is that an organization should consult with its external auditor about the impact of ISO-17799 on the external financial reporting audit — especially vis à vis Sarbanes–Oxley — both in terms of work expended by the organization’s personnel and those of the external auditor.

## THE PROCESS

Appendix B of BS 7799 provides an overall simple but seemingly effective implementation model based on the Deming Wheel or PDCA cycle — Plan, Do, Check, Act. Like the systems development life cycle (SDLC), this process is continuous and circular.

During the Plan phase, the organization defines its information systems policy, defines the scope of its information security management system (ISMS), performs its risk identification and assessment, and, from that, develops a risk treatment plan.

During the Do phase, the organization musters its resources and training, then implements its risk treatment project based on the risk treatment plan.

During the Check phase, the organization performs a variety of forms of checking procedures, including routine checking, self-policing procedures, benchmarking, internal audit — specifically of information security, management review, and trend analysis.

During the Act phase, the organization takes the results of its Check phase and resolves nonconformity issues and designs and carries out corrective and preventive actions.

## ISO-17799 IMPLEMENTATION CONSIDERATIONS

Once an organization has made the decision to implement ISO-17799’s information security management systems standards, it must develop an implementation strategy. The following is a discussion of implementation issues to consider.

### Go It Alone Strategy

An organization may decide that it has sufficient in-house expertise in information security management systems and project implementation, as well as sufficient time available by these personnel to be spent on implementation tasks. It may decide to hire someone or a group of people with these tasks to serve as internal consultants. ISO-17799 is a relatively new standard, so a bevy of experts in this arena does not exist.

However, the standard is not so complex as to preclude an overall expert in information security to “wrap his arms around it” and develop a project plan and a proper information security management system framework.

The standard, of course, recommends a *management information security forum*. This multidiscipline steering committee would oversee the project plan, implementation issues, and internal control problems. It also recommends internal audit involvement, but that topic is discussed in a subsequent section.

## Implementation Manuals

The British Standards Institute (BSI) has prepared a five-booklet set of implementation manuals:

1. Preparing for BS 7799-2 Certification
2. Guide to BS 7799 Risk Assessment and Risk Management
3. Are You Ready for Your BS 7799 Audit?
4. Guide to the Implementation and Auditing of BS 7799 Controls
5. Guide on the Selection of BS 7799 Controls

All five manuals cost \$200 from the BSI Americas Web site ([http://www.bsitraining.com/infosecurity\\_publications.asp](http://www.bsitraining.com/infosecurity_publications.asp)).

Some of the information is a duplicate of that provided in the ISO-17799 and BS 7799 standards, but, in general, provides additional, more detailed, and useful information. The BSI Americas Web site ([http://www.bsitraining.com/infosecurity\\_publications.asp](http://www.bsitraining.com/infosecurity_publications.asp)) provides more information on these manuals.

## BSI Seminars

The BSI offers two seminars on ISO-17799:

1. ISO-17799 — Understanding an Information Security Management System — two days
2. ISO-17799 — Information Security Management System Implementation — five days

It also offers a five-day course entitled “BS-7799-2:2002 — Information Security Management System Auditor.” All three courses are available as regularly scheduled public events or can be arranged as on-site training. More information is available at the BSI Americas Web site ([http://www.bsitraining.com/infosecurity\\_training.asp](http://www.bsitraining.com/infosecurity_training.asp)).

## Implementation Consulting

Using a Web search engine to find “ISO-17799” and “implementation consultant” (or [s]) yielded mostly European references. Only the Web site <http://www.qualitydigest.com/pdfs/0201ISO-DIR.pdf> contained one reference for ISO-17799 training and one for implementation consulting. Yes, this standard is new to the Americas.

*ISO-17799 IS NOT SO COMPLEX AS TO PRECLUDE AN OVERALL EXPERT IN INFORMATION SECURITY TO “WRAP HIS ARMS AROUND IT” AND DEVELOP A PROJECT PLAN AND A PROPER INFORMATION SECURITY MANAGEMENT SYSTEM FRAMEWORK.*

IF WELL-DONE AND  
THOROUGH —  
AT LEAST  
THEORETICALLY —  
AN INDEPENDENT  
REVIEW OF  
INFORMATION  
SECURITY SHOULD  
HELP REDUCE THE  
SCOPE OF THE  
REGISTRAR'S AUDIT.

Another option is to call BSI Americas toll-free at 1-800-862-4977 or standard line 1-703-437-9000 to ask for recommended implementation consultants. The reader can also reach them by e-mail at [inquiry@bsiamericas.com](mailto:inquiry@bsiamericas.com).

An organization must be sure to verify the qualifications of a proposed consultant. It is advisable to ask them for credentials of the consultants who would be working on the assignment, references, and fee schedules. And then have a general discussion with them about their perspective on ISO-17799 and their implementation philosophy — see if they seem to know what they are talking about and whether their approach is good for the organization.

### THE ROLE OF INTERNAL AUDIT

BSI's information security management system standards provide plenty of job security for internal information technology auditors.

Section 4.1.7 of the ISO-17799 calls for an *independent review of information security*. Such a review is important to give management confidence that its information security policies are being followed and are feasible and effective. It also helps prepare an organization for the certification auditors or registrars, as BSI likes to call them. If BSI follows the practice of external financial auditors, the registrar will want to review the work of the internal audit function; and, if well-done and thorough — at least theoretically — this should help reduce the scope of the registrar's audit.

The standard states that such a review can be carried out by an internal audit department, independent manager, or a hired expert consultant.

Section 6.4 of the BS 7799-2 standard is devoted to *Internal ISMS Audits*. It says that the organization shall perform internal information security management system audits at planned intervals. It emphasizes the importance of the internal auditor's impartiality, in many of the same terms as the Institute of Internal Auditor's (IIA) International Standards of Professional Practice.

BS 7799-2 recognizes audit as part of the continual improvement process. However, when listing internal controls, it does not recognize that internal audit itself is an internal control, as recognized by other disciplines. Also, it does not encourage the involvement of internal auditors on systems development teams, so that their expertise can help design internal controls into new applications.

### READY FOR BS 7799-2 CERTIFICATION

As a practical matter, in North America, if an organization wishes to request a certification audit, it should call BSI Americas. In Europe, many BSI-licensed auditors or registrars

exist; but until ISO-17799 grows in popularity, organizations will need to rely on BSI Americas.

The “Preparing for BS 7799-2 Certification” implementation manual emphasizes that certification:

...does not imply that the organization has achieved specific levels of information security related to its services. Evidence may be presented to the certification auditors that such levels have been met via separate evaluation of its products but such evaluation is not part of the certification process.

Stage 1 and Stage 2 certification audits exist:

- Stage 1 audit.* This audit is always performed before a Stage 2 audit. It consists of a document review and its objective is to determine whether the organization is ready for a Stage 2 audit. The auditor presents a report at the end of the audit with his findings. These findings also help select Stage 2 audit team members.
- Stage 2 audit.* This comprehensive audit verifies whether the organization is following the “shall’s” of BS 7799-2. Oral and written reports are likely throughout the audit, but the final report must be timely so as to give the organization’s management time to address the issues raised so that the organization can meet certification requirements.

The actual decision regarding certification is not made in the audit report or by the auditors involved. Rather, the certification body reviews the certification audit report and other relevant information to make its decision.

To remain certified, the organization must receive periodic surveillance audits. The typical interval for such audits is every six months and is not a full-blown recertification. The reassessment is full-blown and occurs every three years.

## CASE STUDY

[Because of its security policy, the insurance company that is the subject of this case study has asked to remain anonymous.]

The holding company of a large insurance company directed the subsidiary to implement an effective information security management system. In 1995, the insurance company chose BS 7799 — predecessor to both the current ISO-17779 and BS 7799-2 — as its standard to help insure the primary objectives of information protection, confidentiality, and availability.

The subsequent time has been spent implementing the standard and continually refining it. As this article is published, the company is preparing for its certification audit under the current BS 7799-2. As such, it is one of the early adopters of both of the current standards.

Of course, the company appointed someone to be a project manager for information security management systems implementation. The author of this article interviewed him for

---

*ORAL AND WRITTEN  
REPORTS ARE  
LIKELY  
THROUGHOUT THE  
AUDIT, BUT THE  
FINAL REPORT MUST  
BE TIMELY SO AS TO  
GIVE THE  
ORGANIZATION'S  
MANAGEMENT TIME  
TO ADDRESS THE  
ISSUES RAISED SO  
THAT THE  
ORGANIZATION CAN  
MEET CERTIFICATION  
REQUIREMENTS.*

---

THE COLLECTIVE  
IMPACT OF SEVERAL  
RECENT  
REGULATIONS WAS  
TO STRENGTHEN  
THE RESOLVE AND  
EMPHASIS OF THE  
ISO-17799  
PROGRAM.

this article. The project manager described the most important critical success factor for implementation as *governance practice* — the project must garner the support, cooperation, and efforts of management at all levels.

Overall organizational support for the project was good, then happened the Enron and Worldcom financial scandals and ensuing regulations — Sarbanes-Oxley Act, Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act (HIPAA) — not to mention various miscellaneous federal, state, and local regulations. The collective impact of all these regulations was to strengthen the resolve and emphasis of the ISO-17799 program. The Internal Audit Department spearheaded the Sarbanes-Oxley Act implementation; and the Regulatory Compliance Department took responsibility for the Gramm-Leach-Bliley Act, HIPAA, and other regulations. The ISO-17799 project manager remains in virtual constant contact with these two departments to coordinate the implementation and minimize the overlap-redo between the various projects. Of course, the Internal Audit Department also assists in performing internal audits required by the ISO-17799 standard.

The company chose to hire implementation consultants to help develop the framework from which their information security policies and risk analysis approach flow. Basically, the company and its consultants took the ISO-17799 document and tailored it to its organization and its industry — adding and deleting as necessary. The project manager expressed that the organization was quite glad to have the ISO-17799 document to start with — that way, the organization was not beginning from scratch.

Why is the company seeking official certification by the British Standards Institute audit when it does not plan to publicize this fact? The project manager explained that the company is merely seeking independent verification of what it has sought to establish internally. ■

---

*Lawrence Capuder operates his own consulting practice focusing on information technology security and auditing, internal auditing, and strategic management. He has clients in over twenty countries on four continents, including Big Four CPA firms, Fortune 500 companies, banks, central banks and the World Bank and US Agency for International Development. He has written dozens of professional journal articles, spoken at global conferences and presented seminars in many parts of the world.*