November 2002

International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management

Frequently Asked Questions

Introduction

The National Institute of Standards and Technology's (NIST's) Information Technology Laboratory developed this Frequently Asked Questions (FAQ) in response to the high level of interest in this activity. The FAQ addresses a number of questions being asked by persons in both government and industry about ISO/IEC 17799:2000, *Code of Practice for Information Security Management*. This document is for background information purposes only and does not serve as an official US Government position.

What is ISO/IEC 17799:2000?

ISO/IEC 17799 is a code of practice. As such, it offers guidelines and voluntary directions for information security management. It is meant to provide a high level, general description of the areas currently considered important when initiating, implementing or maintaining information security in an organization. The document does not currently cover all areas of importance but is undergoing a thorough revision. The joint project editors for this revision are Oliver Weissman from Germany, and Angelika Plate from the UK.

What does ISO/IEC 17799:2000 cover?

ISO/IEC 17799:2000 addresses topics in terms of policies and general good practices. The document specifically identifies itself as "a starting point for developing organization specific guidance." It states that not all of the guidance and controls it contains may be applicable and that additional controls not contained may be required. It is not intended to give definitive details or "how-to's". Given such caveats, the document briefly addresses the following major topics:

- Establishing 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, and

- Compliance.

ISO/IEC 17799:2000 does not provide definitive or specific material on any security topic. It provides general guidance on the wide variety of topics listed above, but typically does not go into depth. ISO/IEC 17799 does not provide detailed conformance specifications necessary for an organizational information security management program. It does not provide enough information to support an in-depth organizational information security review, or to support a certification program like the ISO 9000 process quality certification program. Appropriately revised, ISO/IEC 17799 could be useful as a high-level overview of information security topics that could help senior management to understand the basic issues involved in each of the topic areas. ISO/IEC 17799 should be augmented by more technical guidance in order to be used effectively for a security review.

Is there a Part 2 of ISO/IEC 17799:2000, as there is of the UK's BS 7799?

At this time, ISO/IEC JTC 1 has no plans to generate a part 2 of ISO/IEC 17799 as a future work item.

How does ISO/IEC 17799:2000 relate to ISO/IEC 15408:1999, the Common Criteria for IT Security Evaluation?

ISO/IEC 17799: 2000 is a management standard, and deals with an examination of the non-technical issues relating to installed IT systems. These issues have to do with such matters as personnel, procedural, and physical security, and security management in general.

The Common Criteria standard is a technical standard. It is intended to support the specification and technical evaluation of IT security features in products. Normally, the products are evaluated as part of the development/production cycle. The Common Criteria standard also has a major usage as a structure, syntax and catalog of information technology specifications that can be used to describe user technical requirements for security in products.

To see how the Common Criteria can help organizations face their security challenges, please refer to NIST Special Publication 800-23, Guide to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, which can be downloaded at the following website:

http://csrc.nist.gov/publications/nistpubs/index.html

What is the US position on ISO/IEC 17799:2000?

The current US position is strongly in favor of the major revision of the document, which is currently underway. While there was no official US government position expressed,

US TAG members from both the Commerce Department (via NIST) and Department of Defense (via the Defense Information Systems Agency) supported the US position.

What is NIST's position regarding ISO/IEC 17799:2000?

The objectives outlined within 17799 could be revised to provide general guidance on the commonly accepted goals of today's information security management professionals. Therefore this document, once revised, may serve as a practical guideline for developing effective security management practices, in an effort to achieve confidence in inter-organizational dealings. One would have to supplement it with detailed technical guidance in order to use it for security reviews. It is important to note that security policies and practices may be largely dependent upon laws, regulations and organizational decisions around acceptable risk and appropriate risk mitigation. No policy or practice, even if implemented exactly as planned, can ensure that an organization's information is 100% secure.

For the detailed information necessary to develop organizational and technical security standards, one can turn to a wide variety of documents published by NIST, ANSI and ISO/IEC.

There are a wide variety of helpful security publications available at the NIST website:

http://csrc.nist.gov/publications/nistpubs/index.html.

Numerous guidance documents can be freely downloaded there. The following documents in the NIST Special Publication 800-series, may be particularly useful for organizational information security management:

- SP 800-12, Computer Security Handbook
- SP 800-14, Generally Accepted [Security] Principles & Practices
- SP 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model
- SP 800-18, Guide for Developing Security Plans
- SP 800-23, Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
- SP 800-24, PBX Vulnerability Analysis: Finding Holes in your PBX Before Someone Else Does
- SP 800-26, Security Self-Assessment Guide for Information Technology Systems
- SP 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- SP 800-30, Risk Management Guide for information Technology Systems
- SP 800-34, Contingency Plan Guide for Information Technology Systems
- SP 800 –37, Draft Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems
- SP 800-40, Procedures for Handling Security Patches
- SP 800-41, Guidelines and Firewalls and Firewall Policy

- SP 800-46, Security for Telecommuting and Broadband Communications
- SP 800-47, Security Guide for Interconnecting Information Technology Systems
- SP 800-50, Building an Information Technology Security Awareness and Training Program (DRAFT)
- SP 800-42, Guideline on Network Security Testing (DRAFT)
- SP 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices (DRAFT)
- SP 800-4A, Security Considerations in Federal Information Technology Procurements (REVISION)
- SP 800-35, Guide to IT Security Services (DRAFT)
- SP 800-36, Guide to Selecting IT Security Products (DRAFT)
- SP 800-55, Security Metrics Guide for Information Technology Systems (DRAFT)
- SP 800-37, Guidelines for the Security Certification and Accreditation (C&A) of Federal Information Technology Systems (DRAFT)

The ISO/IEC TR 13335 Guidelines for the Management of IT Security (GMITS) series of Technical Reports are particularly useful. All five parts are presently available from ANSI.

To order, go to ANSI at:

http://www.ansi.org/

Then click on the INCITS logo: 

The following information is provided for ordering the GMITS series of Technical Reports:

Document Number: INCITS/ISO/IEC TR 13335-1-1996
Title: Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security
$18.00

Document Number: INCITS/ISO/IEC TR 13335-2-1997
Title: Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security
$18.00

Document Number: INCITS/ISO/IEC TR 13335-3-1998
Title: Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security
$18.00

Document Number: INCITS/ISO/IEC TR 13335-4-2000

Title: Information technology -- Guidelines for the management of IT Security -- Part 4: Selection of safeguards
$18.00

Document Number: ISO/IEC DTR 13335-5-2001
Title: Information technology -- Guidelines for the management of IT Security – Part 5: Management guidance on network security
$18.00

Some of these Technical Reports are now under revision. GMITS Part 1 is submitted as an new project for an international standard with a title change to "Management of information and communications technology security Part 1: Concepts and models for information and communications technology security management". Status information on the revisions and the new project proposal is available from NCITS T4:

http://www.ncits.org/tc_home/t4htm/index.htm

Go to Technical area - List of projects and look for TR 13335. The best way to get the latest copies of these revisions would be to join NCITS T4 (See the last question.).

As a US person, how can I participate in the ISO/IEC 17799:2000 revision process?

The US TAG to ISO/IEC JTC 1 SC 27 is the National Committee for Information Technology Standards (NCITS), Technical Committee T4, Security Techniques. Technical Committee T4, Security Techniques, participates in the standardization of generic methods for information technology security. This includes development of: security techniques and mechanisms; security guidelines; security evaluation criteria; and identification of generic requirements for information technology system security services. As the US TAG to ISO/IEC JTC 1 SC27, T4 provides recommendations on US positions to the JTC 1 TAG.

The Chairman of NCITS Technical Committee T4 is Rowena Chester, University of Tennessee. For information on joining T4 send email to Rowena Chester at:

mailto:roc2@cornell.edu

The NCITS Technical Committee T4 web site is:

http://www.ncits.org/tc_home/t4.htm

Membership information for NCITS and the JTC 1 TAG are available on their websites.

The NCITS web site is:

http://www.ncits.org/

The US Technical Advisory Group to JTC 1 (JTC 1 TAG) web site is:

http://www.jtc1tag.org/