

ISO 17799: Pay Attention to this One

Executive Insight Series

Jonathan G. Gossels

Introduction

For years, organizations have been searching for an objective benchmark to measure the security of potential business partners and to distinguish the quality of their own services. While not perfect, ISO 17799 is emerging as the standard of choice because it overcomes many of the critical deficiencies of SAS 70. Specifically, it provides a comprehensive set of security-related topics and an objective means of measuring compliance.

The certification mechanisms prescribed by the standard are largely unworkable and will not make economic sense for most organizations to pursue. Nevertheless, if *compliance* rather than *certification* is your goal, ISO 17799 will serve as a sound security-baseline for many organizations.

This brief paper is intended to give you insight into ISO 17799 and how it might be relevant to your organization.

What is ISO 17799?

ISO 17799 was first published by the International Organization for Standardization (ISO) in 2000. It is derived from the 1999 version of an earlier U.K. standard, called BS7799.

ISO 17799 is a comprehensive security standard, focusing primarily on control

requirements. The standard contains ten major sections. Each is described briefly below.

Security Policy

A surprisingly weak section of the standard, this section requires a written security policy and an ongoing process for its review and evaluation.

Organizational Security

The Organizational Security section cover three main categories:

- Information security infrastructure
- Security of third party access
- Outsourcing

The Information Security Infrastructure category is itself broken into seven sub sections.

Asset Classification and Control

Recognizing that not all information assets are equal, the Asset Classification and Control section of the standard addresses classification of assets so that information assets receive an appropriate level of protection. It also addresses asset inventory and labeling.

Personnel Security

The behavior of people is an essential element of any security environment. The Personnel Security section deals with many issues. The main headings are:

- Security in job definition and resourcing
- User training

- Responding to security incidents and malfunctions

Physical & Environmental Security

The Physical and Environmental Security section addresses secure areas, equipment security, and general controls.

Communications and Operations Management

The Communications and Operations Management section includes the following topics:

- Operational procedures and responsibilities
- System planning and acceptance
- Protection against malicious software
- Housekeeping (e.g., back ups and logging)
- Network management
- Media handling
- Exchanges of information and software with other organizations

Access Control

The Access Control section describes control issues related to:

- Business requirements for access control
- User access management
- User responsibilities
- Network access control
- Application access control
- Monitoring system access and use
- Mobile computing and teleworking

System Development and Maintenance

The System Development and Maintenance section describes control issues related to:

- Security requirements of systems
- Security in application systems
- Cryptographic controls
- Security of file systems
- Security in development and support processes

Business Continuity Management

The Business Continuity Management section identifies measures to mitigate potential disruption of business activities and critical business processes caused by major failures or disasters.

Compliance

The Compliance section places the technical requirements of the standard in the full legal, regulatory, and business context. Specifics include:

- Compliance with legal requirements
- Reviews of security policy and technical compliance
- System audit considerations

Context

Interestingly, the perspective of an ISO 17799 analysis is as a service provider to a customer. That means that most organizations will need to do a number of pair-wise assessments. In large organizations that may have many business partners or that utilize a large number of ASPs, this pair-wise assessment requirement becomes impractical. In addition, it makes formal certification exceedingly expensive (see below)

Compliance vs Certification

For a standard that has so much to offer, it is unfortunate that the compliance portion is half-baked. It has two critical flaws:

The first problem is the pair-wise assessment requirements discussed above. Each service-provider / customer relationship must be thoroughly reviewed. The only winners in that model are consulting companies doing the reviews. Economically and practically, that just won't scale.

The second problem is less obvious but more insidious because most organizations seeking certification aren't even aware of it. The standard draws a distinction between the act of assessing whether an IT infrastructure *complies* with the standard and the act of formerly *certifying* compliance.

Only ISO approved companies can certify compliance. While ISO makes a separation of duties argument to justify this restriction, that argument is specious and self-serving. What actually drives this distinction is that ISO is looking to create an ongoing revenue stream from the certification process in the same way it has from its ISO 9000 activities. That makes for nice bonuses for the individuals who run ISO but drives up the cost of certification and restricts the pool of firms available to perform such certification. Agreement to pay fees to ISO becomes the litmus test for potential certifiers, rather than technical qualifications.

Most organizations will gain substantially all of the benefits from the process of assessing their compliance and making changes to address any deficiencies. Except in unusual circumstances, the added cost of formal certification is simply not worth it.

ISO 17799

ISO currently offers the best promise of the long sought objective standard for information security. It will help many organizations realize that there is more to security than simply installing a firewall.

Even with its obvious deficiencies in the area of certification, the process of assessing compliance and working to resolve control weaknesses will benefit most organizations.

How to Get Started

As a final note, clients regularly ask us whether the ISO 17799 review is sufficient by itself or whether it should be combined with a traditional security review. The answer to that question varies.

If the client is looking for a relatively fast assessment of how it measures up and doesn't need a lot of advice on how to remedy deficiencies that are found, an ISO 17799 review is an excellent starting point. If the client needs more help in figuring what to do about its problems, the ISO 17799 review should be performed as an extension to a traditional security review.

