

# Explainer: Security standards and frameworks

Bob Violino

**April 17, 2006** (Computerworld) Many companies are using standards and frameworks to deal with certain aspects of information security. These models can help protect systems and data, but each plays a very different role in an overall security plan.

Some of the most popular ones, including the Control Objectives for Information and Related Technology (Cobit), ISO 27001, the IT Infrastructure Library (ITIL) and Statement on Auditing Standards (SAS) No. 70, offer guidelines for improving some elements of security. But experts say these models are more like pieces of a puzzle than comprehensive security standards.

"All of these frameworks supply IT with repeatable processes that are consistent across the various IT functions" and help technology executives provide better service, says Kimberly Sawyer, vice president of computing and network services at Lockheed Martin Corp.'s IT department, known as Enterprise Information Systems, in Orlando.

But none of the standards alone provides full security, Sawyer says. "They contain various information security concepts that must be interpreted, integrated and incorporated into the daily operations," she says. "Comprehensive security requires discipline and integration across all aspects of planning, service delivery, risk management architecture, tool selection, policy development and audits."

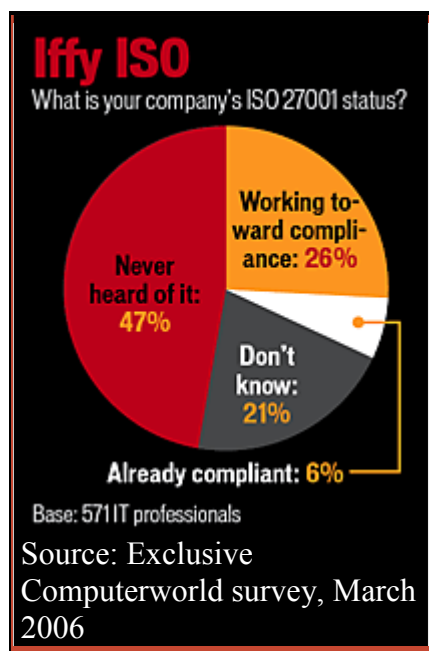
Lockheed Martin is using Cobit, ITIL and ISO 27001 for different purposes: Cobit for measuring and assessing IT controls, ITIL to improve internal IT services, and ISO 27001 for IT governance. Although each helps to bolster security, none is a stand-alone solution, Sawyer says. "IT organizations must integrate the frameworks to ensure [that] best practices are integrated across the information security discipline," she says.

Here's a look at some of the key standards and their roles in a security plan.

## **Cobit**

Developed in 1996 by the Information Systems Audit and Control Association and the IT Governance Institute, Cobit provides a framework for users and IT, security and auditing managers. It's gaining acceptance as a good practice for controlling data, systems and related risks.

"Cobit has enabled us to more systematically approach audit issues to identify root causes of deficiencies," says Sawyer.



The framework includes tools to measure a company's capabilities in 34 IT processes. Among them are a list of critical success factors that provides best practices for each IT process, maturity models to help in benchmarking and performance-measurement elements. The standard is becoming vital as companies strive to comply with regulations such as the Sarbanes-Oxley Act.

"Cobit only has one security module, but when you look at [the standard] from a broad perspective, it addresses a lot of elements of security," says Mike Nelson, president of SecureNet Technologies Inc., a consulting firm in San Ramon, Calif., that focuses on information security. "Where it begins to break down is in providing details of the 'how.' It gives detail of controls and objectives of controls" but doesn't explain how to implement them, he says.

## ISO 27001

ISO 27001 (Information Security Management -- Specification With Guidance for Use) provides more of the detail that's needed, Nelson says. The standard, which is based on an earlier standard, ISO 17799, is designed to help organizations establish and maintain effective information security controls through continual improvements.

Developed in October 2005 by the International Standards Organization, ISO 27001 implements principles of the Organization for Economic Cooperation and Development on governing the security of information and networks. The standard creates a road map for the secure design, implementation, management and maintenance of IT processes in an organization.

"ISO 27001 is a laundry list of controls; it gives more of framework for an effective security program," says Paul Proctor, an analyst at Gartner Inc. in Stamford, Conn. "Cobit and ISO 27001 are the most popular [standards] out there."

## **ITIL**

ITIL is a set of best practices, published as books designed to help reduce the cost of using technology and to improve the quality of services delivered throughout the organization. ITIL consists of rules on how to deliver services more efficiently by improving management processes across IT departments that support networks, applications and databases.

In the late 1980s, the U.K. Office of Government Commerce developed the standards for service providers to follow in delivering IT services to the British government. ITIL covers seven main areas: service support, service delivery, planning to implement service management, infrastructure management for IT and communications technology, applications management, security management, and the business perspective.

"ITIL is strong in process management and delivery but fairly narrowly focused on those areas," says Nelson. "It only peripherally deals with security as a component in service management. From a pure security point of view, it's relatively weak, but it was not designed to address that."

Adds Proctor, "Cobit is better for meeting regulatory [requirements]. ITIL is more of an operations standard, something you use to improve the maturity of your IT operations. We find a lot of companies either choose ITIL or Cobit. Some do both, but that is rare."

Ruben Melendez says ITIL is becoming the standard of choice for many vendors and is useful for improving security. He is president of The Glomark Group Inc., a consulting firm in Columbus, Ohio, that works with IT vendors and end-user organizations to develop return-on-investment strategies. "The companies I've worked with are all ITIL implementers," Melendez says. "We've done a lot of work with [CA] on security-related products. If you look at their literature, when they talk about security, they emphasize ITIL and not the others."

According to Melendez, other vendors pushing ITIL include Microsoft Corp., Intel Corp. and Oracle Corp.

## **SAS 70**

SAS 70 is an auditing standard that was created by the American Institute of Certified Public Accountants (AICPA) in 1992. A SAS 70 audit shows whether an independent accounting and auditing firm has examined a service provider's controls for IT and related processes.

SAS 70 isn't a predetermined set of control objectives or activities. Auditors must follow the AICPA's standards for fieldwork, quality control and reporting and issue a formal report to the service provider that includes the auditor's opinion once the audit is completed.

There are two types of reports: one describes a service provider's controls at a specific point in time, and the other describes the controls and includes detailed testing of the service provider's control activities and processes over a minimum six-month period.

Service providers must demonstrate that they have adequate safeguards when they host or process client information. SAS 70 enables service organizations to disclose their controls to their clients and their clients' auditors in a uniform reporting format.

The benefit to companies is that they receive detailed information about a service provider's controls and an independent assessment of whether the controls are operating effectively. They can present this information to their own auditors when necessary.

SAS 70 lets organizations know if their existing controls are working, but it doesn't tell them if all the right controls are in place, Nelson says.

Each of these standards has a potential role to play in helping organizations protect their systems and data. Companies that are looking to create an overall security strategy need to explore the frameworks to see which provides the best fit.