
How Tripwire Supports Standards Set by the BS 7799/ISO17799

page 2	Introduction
page 2	BS 7799 and the Financial Services Industry
page 3	How Tripwire Supports the 10 Domains of Control
page 4	Change Auditing

There are a lot of changes underway in the areas of information security, legal issues in computing and legislation for information handling and protection in healthcare and other industries. In the healthcare industry, the Health Insurance Portability and Accountability Act (HIPAA) is framing the legal standards for data protection. In Information Security, the British Standards Institute (www.bsi.co.uk) has been working to formalize information security management. The BSI may be best known for the ISO9001 standard, which improved manufacturing processes.

The BS 7799 was issued to provide a set of controls comprising best practices in information security. It is a strong reference point for identifying the range of controls needed for most situations where information systems are used in the business world. The standard has been worked through the ISO acceptance process as the ISO17799 standard.

Business continuity is sustained, in part, by the integrity of its operations, including systems assurance and integrity. Tripwire® Change Auditing solutions extend well past being a security niche product—as a single point of control for detecting change across the enterprise, they enable IT organizations to automate change detection, reconciliation, and reporting. Use of Tripwire software directly supports key controls in the BS 7799.

BS 7799 and the Financial Services Industry

Many regulated industries have looked to the BS 7799 to aid in their pursuit of comprehensive security. Most obvious of these is the financial services industry.

Companies providing financial services understand that computer security is part of information security, and that information security is part of the company's risk management strategy.

Even companies not in the financial services industry can understand the high-stakes risks and are personally affected by the integrity of their own banking institutions.

High-stakes such as:

- One financial services company reported \$40-60 million in “unaccounted wire transfers.” This is an indirect way of saying it was stolen.
- Another financial services company identified unauthorized transfers of \$6 million when each night's settlement was processed. It turned out to be an internal company employee who really worked for a group of organized criminals.
- The SEC imposes high dollar fines, per-hour, or the late reporting of Net Asset Values (NAV) for mutual funds. These are the “stock prices” for mutual funds. A mutual fund company can quickly find itself with multi-million dollar fines for being late with its information.

Understanding the risks are high, change auditing must be a key element of business risk management. Tripwire can directly solve issues surrounding unauthorized change for systems and data—but it can also support efforts across the complete domain of information security.

How Tripwire Supports the 10 Domains of Control

The BS 7799 / ISO17799 is broken into ten domains of control focus. These are:

(1) Security Policy

Every company must have an information security policy outlining their support for, and commitment to, information security. It should set policy direction across the organization. Often, in these policies, data is identified as a corporate asset and must be protected. Tripwire directly supports information protection and integrity.

(2) Security Organization

A security organization must be specifically tasked with the responsibility of information security issues.

(3) Asset Classification and Control

A company and its security organization can only protect what they have identified. Corporate assets should be inventoried and classified so appropriate protection can be applied. In the case of information systems, "mission critical" systems may dictate the use of change auditing solutions such as Tripwire; whereas a temporary testing server may not require such people, process and technology.

(4) Personnel Security

This is focused on reducing the risk of human error, theft, fraud or misuse of resources. A Computer Security Incident Response Team (CSIRT) may be part of this effort. Tripwire software's ability to quickly assess what happened is especially useful in response to security incidents and all associated reporting around them.

(5) Physical and Environment Security

Much of this focus is around physical access controls to prevent unauthorized access, damage, or interference to business. Tripwire software, as part of the desktop standard, will identify when hardware has been changed or removed, and possibly stolen. By watching the Windows registry, stolen memory or downgraded processors are identified quickly.

(6) Communications and Operations Management

This is the area most commonly identified as "computer security." The purpose of this focus is to ensure the correct and secure operation of information processing.

- (a) Operational Change Management is specifically identified as a key component. Tripwire software excels in this area and is used in virtually every installation for configuration and change management on servers.
- (b) Segregation of Duties is an important part of risk reduction. Tripwire software can assist with this human process. As an example, the IT organization behind the New York Stock Exchange uses Tripwire as a hand-off mechanism for each shift change of the operations team on the trading floor.
- (c) Systems Acceptance. Tripwire software is used to identify inconsistency in platforms between development and quality assurance (QA), and between QA and production rollout. Also, the software aids with internal audits to validate a build server process. Once validated, its output systems can be checked via Tripwire software instead of a multi-hour systems audit for each.

(7) Access Control

This section of the BS 7799 identifies the need to control access to information. This includes user management and entitlements or privileges. Tripwire software, as part of the basic system build, can protect changes around the user password and other systems access mechanisms.

(8) Systems Development and Maintenance

The purpose of this area is to ensure that security is built into information systems as part of their complete life cycle—not just added near release. Tripwire software should be an integral part of a repeatable build process and QA/Release engineering. Cryptographic controls are specifically identified in this section of the BS 7799 to protect the confidentiality, authenticity or integrity of information. Tripwire uses cryptographic checksums (hashes) of watched files. These are stored in a flat file data on the system. This database is digitally signed to protect against unauthorized tampering. Tripwire software, while not usually thought of as a cryptographic product, meets many of the needs in this area of the standard.

(9) Business Continuity Management

Business Continuity Management is concerned with counteracting interruptions to business activities and protecting critical business processes from the effects of disaster. This includes systems and data backup/restoration, testing of failure scenarios, and other practices. Tripwire software supports these activities directly as it is often used to reduce recovery time and identify, with “surgical precision”, files with that need to be recovered/restored to bring systems back into a known, good state.

(10) Audit/Compliance

Audit/Compliance ensures that policies, standards and best practices are being pursued within the organization. Tripwire has long been a key part of an auditor’s toolbox. Internal auditors use Tripwire to take a “digital snapshot” of a system and, during subsequent integrity checks, compare against that database to identify unauthorized changes.

Change Auditing

Tripwire is the world leader in Change Auditing solutions that enable enterprises to reduce operational risk and gain control over IT systems. Tripwire software ensures the security of systems, instills accountability for change, and increases the availability of critical IT infrastructure. Comprehensive change auditing requires process, people and technology. Correspondingly, Tripwire Solutions include both software and professional services offerings. Software offerings include Tripwire Enterprise and Tripwire for Servers. Tripwire Professional Services offers a complete set of services to help organizations define change control processes, integrate Tripwire software with existing C/CM systems, as well as Tripwire software implementation and tuning.

To Learn More

For additional information on change and configuration management and change auditing solutions as they relate to IT auditing, regulatory compliance, the IIA and GTAG, best practices such as ITIL/Visible Ops and COBIT, the ITPI and the ITGI, please visit www.tripwire.com/solutions.

TRIPWIRE Audit Change. Prove Control.

www.tripwire.com

US TOLL FREE: 1.800.TRIPWIRE MAIN: 503.276.7500 FAX: 503.223.0182
326 SW Broadway, 3rd Floor Portland, OR 97205 USA

www.tripwire.com/intl/uk

TRIPWIRE UK: +44 207 618 6512 FAX: +44 207 618 8001
78 Cannon Street London EC4N 6NQ UK