

## **Regulatory Compliance and ISO 27001**

### **Executive Summary**

Today's regulatory environment is increasingly complex, the penalties for failure unattractive and the route to effective compliance not clear. ISO 27001 provides a best-practice solution to a range of regulatory issues faced by directors.

### **The Regulatory conundrum**

Organizations have traditionally responded to regulatory compliance requirements on a law-by-law, or department-by-department basis. That was, last century, a perfectly adequate response. There were relatively few laws, compliance requirements were generally firmly established and well-understood, and the jurisdictions within which businesses operated were well-defined.

Over the last decade, all that has changed. Rapid globalisation, increasingly pervasive information technology, the evolving business risk and threat environment, and today's governance expectations have, between them, created a fast-growing and complex body of laws and regulations – such as Data Protection and privacy legislation (e.g. HIPAA, GLBA, DPA) and governance requirements (eg SOX and Turnbull) - that all impact the organization's IT systems. While global companies are in the forefront of finding effective compliance solutions, every organization, however small, and in whatever industry, is faced with the same broad range of regulatory requirements.

These regulatory requirements focus on the confidentiality, integrity and availability of electronically-held information, and primarily – but not exclusively – on personal data. Many of the new laws appear to overlap and, not only is there very little established legal guidance as to what constitutes compliance, new laws and regulatory requirements continue to emerge. Increasingly, these laws have a geographic reach that extends to organizations based and operating outside the apparent jurisdiction of the legislative or regulatory body that originated them.

Regulatory requirements in all these areas concentrate on preserving the confidentiality, integrity and availability of electronic data held by organizations operating within the sector. Regulations, which are technology-neutral, describe what must be done, but not how. Organizations are left to establish, for themselves, how to meet these requirements.

In most instances, there is not yet a body of tested case law and proven compliance methodologies to which organizations can turn in order to calibrate their efforts. There are no technology products which, of themselves, can render an organization compliant with any of the data security regulations, because all data security controls consist of a combination of technology, procedure and human behaviour. In other words, installing a firewall will not protect an organization if there are no procedures for correctly configuring and maintaining it, and if users habitually bypass it (through, for instance, Instant Messaging, Internet browsing or the deployment of rogue wireless access points).

In the face of new, blended, complex and evolving threats to their data, organizations have business and regulatory obligations to protect, maintain and make that data available when it is required. They have to do this in an uncertain compliance environment where the rewards for success don't grab headlines, but the penalties for failure do. Fines, reputation and brand damage and, in some circumstances, jail time for directors are outcomes that every business wants to avoid, and wants to avoid as systematically and cost-effectively as possible.

The adoption of an externally-validated, best-practice approach to information security – one that provides a single, coherent framework that enables simultaneous compliance with multiple regulatory requirements - is, therefore, a solution to which organizations are increasingly turning.

### **ISO 27001**

ISO 27001 provides just such a solution. It focuses on the confidentiality, availability and integrity of data and its key precepts and requirements all occur in the regulatory requirements. Implementation of an ISO 27001 framework enables an organization to comply, at one step (and subject to specific documentation and working practices tailored for each individual regulation), with all the core requirements of information-related regulation anywhere in the world.