

IT compliance and IT security —Part 2

This article is the 2nd in a series by Dr Jörg Hladjk, of Hunton & Williams, on the interrelationship between IT security, compliance and data protection

Today, every organisation has information assets. Typically these assets account for a significant part of the overall value of the organisation and are essential to the ongoing operation of the organisation. For most organisations, the security and protection of information assets is essential to their continuity, integrity and, therefore, existence.

Since information is an important business asset, it needs to be suitably protected. This is especially crucial in the increasingly interconnected business environment. As a result of this interconnectivity, information is exposed to a growing number and a wider variety of threats and vulnerabilities.

International IT security standards recognise that the level of security that can be achieved purely through technical means is limited. The required level of security, established through assessing risk and the associated costs of a breach of security, and weighing this against the costs of implementing additional security measures, should always be driven by appropriate management controls and procedures. Information security management requires, as a minimum, participation by all employees in the organisation. It may also require participation from shareholders, suppliers, third parties and customers, in order to be successful.

What is information security?

There are many definitions of 'information security,' but it can best be described as the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Information security can best be achieved by implementing a suitable set of controls, including policies, processes, procedures, organisational structures, and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the business are met. This should be done in conjunction with other business management processes and not be considered to be a stand-alone project.

What is the interrelationship with data protection?

The use of international security standards can help a business to satisfy the requirements of European data protection laws. These laws provide that information held about people, both customers and employees, is adequately protected and securely maintained. By implementing good information security practices, organisations are better equipped to keep their information accurate and up to date. They can also ensure it is accessed by the right people, and in a secure way. If information security is compromised, the financial cost to the organisation can be significant, but the reputational cost can be life threatening. There are a number of security implications contained within European data protection laws. The following outline will use the UK Data Protection Act 1998 ('the Act') as an example.

The Act applies to computerised records, as well as to certain manual records, involving personal information. At the heart of the Act is a set of eight principles. Good information security practice is implied in all eight, but explicitly in the Seventh Principle, which relates to the prevention of unauthorised or unlawful processing, and of accidental loss, destruction or damage to data. It requires that appropriate technical and organisational security measures are implemented to protect personal information.

Further, given the international context within which personal data flow, the means by which data may legitimately be transferred outside the European Economic Area attract close scrutiny. The Eighth Principle provides that personal information shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an "adequate" level of protection for the data. Technical and organisational security measures are an important part of the assessment of adequacy. Their significance is underscored by the fact that Appendix 2 to the Model Clauses governing controller-to-processor transfers requires a detailed description of the technical and organisational security measures implemented by the data importer. Given the significance of IT security, it is prudent to base IT security management activities on widely

(Continued on page 12)

(Continued from page 11)

accepted international security standards.

Set out below is a short list of some of the typical areas in which IT security requirements should be considered by the business as part its IT compliance and risk management program. The list identifies the relevant IT security standard for each type of activity, although many of these overlap.

IT management

Business that are subject to the US Sarbanes-Oxley Act 2002 (see Part 1 of this article, published in the previous edition, for a discussion of the impact of this legislation on IT security controls) may wish to adopt the control frameworks: the Committee of Sponsoring Organisations of the Treadway Commission (COSO) Internal Control Integrated Framework and the IT Governance Institute's Control Objectives for Information and Related Technology (COBIT).

These two frameworks have different approaches and differ in their goals. The CoSo framework is focussed on the idea that internal control is established by the business' board of directors or management through internal procedures in order to ensure that pre-defined goals are achieved within the organisation. On the other hand, COBIT is focussed on information that could be used to fulfil the business needs and to enable IT resources and procedures to function properly. Further, the objectives of Coso concentrate on efficiency of operations, financial reporting and compliance with laws whereas COBIT also takes into account security and quality management requirements in a number of categories including confidentiality, integrity, availability and reliability. Finally, the frameworks can be distinguished with regard to their users. While Coso addresses the broader management, COBIT is suitable not only for the management, but also for users and auditors. COBIT is clearly related to IT controls for IT compliance projects in order to ensure systems and data security.

According to the IT Governance Institute, the goals of the COBIT framework can be described as follows. Businesses are obliged to fulfil the minimum quality, fiduciary and security

requirements in relation to information assets, just as they would for other types of asset. In addition, management is expected to optimise the use of available resources, including data, application systems, technology, facilities and people. In order to make sure these responsibilities are discharged and objectives achieved, management has the task of understanding the status of its own IT systems and deciding what security and control they should provide. Further, the management has to ensure the existence of an internal control system or framework to support the business processes and to make clear how each individual control activity satisfies the information requirements and impacts in IT resources. The responsibility of management covers IT control, including policies, organisational structures, practices and procedures.

IT services

In the area of service support, the Information Technology Infrastructure Library (ITIL) is generally used. ITIL presents a set of management procedures for IT systems and operations, including security management. The security management procedures enable an organisation to structure all of their IT systems and operations in way that allows them to achieve a high level of security. The underlying concept is delivered by the "code of practice for information security management" commonly known as the ISO/IEC 17799, which is outlined in more detail below. Every information security management system is focused on the value of the information that has to be protected. The concepts used to measure and value the types of business information are confidentiality, integrity and availability. Correlating aspects are data protection, anonymity and verifiability. Looking at the implementation side of an information security management system, two elements must be considered. First, the realization of security requirements defined in a Service Level Agreement (SLA) and other external requirements which are specified in contracts, legislation and other internal or external policies or codes of conduct. Secondly, the realization of a basic level of security. This is necessary to guarantee the continuity of the organisation.. The input for the basic level consists of the SLAs with the specified security requirements, applicable legislative require-

ments and other potential underlying contracts.

IT security

The international standard used today in the area of IT security is ISO/IEC 17799:2005. This standard was published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is entitled "Information technology - Security techniques - Code of practice for information security management." The current standard is a revision of the version published in 2000, which consists of the British Standard (BS) 7799-1:1999.

ISO/IEC 17799 provides best practice recommendations on information security management for use of a business that wants to implement an Information Security Management System. Information security is defined as "the preservation of confidentiality (ensuring that information is accessible only to those authorised to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorised users have access to information and associated assets when required)."

The standard contains twelve main sections, including the following:

- "Risk assessment and treatment—analysis of the organisation's information security risks";
- "Security policy—management direction;
- Organisation of information security—governance of information security";
- "Communications and operations management—management of technical security controls in systems and networks";
- "Access control—restriction of access rights to networks, systems, applications, functions and data";
- "Information systems acquisition, development and maintenance—building security into applications";
- "Information security incident management—anticipating and responding appropriately to information security breaches";

- “Compliance—ensuring conformance with information security policies, standards, laws and regulations.”

Each section specifies information security controls and their objectives. Each control is accompanied by guidance on implementation. Specific controls, however, are not mandated since it is expected that each business will undertake a structured information security risk assessment process to determine its specific requirements before selecting controls that are appropriate to its particular circumstances. In addition, it is also practically impossible to list all possible controls in a general purpose standard. There exist also industry-specific variants of ISO 17799 that are anticipated to give advice tailored to businesses e.g. in the telecoms or financial services sector.

IT service providers

As part of an IT compliance project, a business must also identify its critical third party and outsourcing suppliers using formal IT risk assessment processes. The relevant standards and procedures applied to a specific service need to be defined depending on the scope of that service. Since the adherence to such standards by any service provider may be hard for a business to control, external certification can be used to ensure a certain level of compliance. Such external certification may be provided by a “Statement on Auditing Standards No. 70 Type II reports” (Type II SAS 70). This Type II SAS 70 is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). Type II SAS 70 is generally applicable when an auditor is auditing the financial statements of an entity that obtains services from another organisation. Service organisations that provide such services include application service providers, bank trust departments, internet data centres or other data processing service providers. A Type II SAS 70 audit or service auditor’s examination is widely recognized because it demonstrates that a service organisations’ control activities have been audited, generally including controls over information technology and related processes, including IT security.

To exercise control over and discharge its compliance obligations, a business should request Type II SAS 70 certifications from all their critical IT service providers. A business should also review carefully the scope of any Type II SAS 70 certification to ensure that it matches the specific service and/or product being provided. If certifications are not readily available, alternative procedures should be adopted. It is also necessary for a business to include all relevant standards for service provision in its contracts with the third party service provider and to allow follow up and enforce those standards. Finally, the adoption of international standards such as ISO 9001, ISO 15000 and ISO 17799 as mandatory requirements by all critical IT suppliers is strongly recommended as best practice.

How to implement an Information Security Management System?

To implement an Information Security Management System (ISMS) as described above, a business needs to follow at least the following five main steps:

Design and Layout of the ISMS: At this stage, a business would determine its policy and objectives regarding information security, assess its security risks, evaluate various ways of handling these risks, and select controls from the various international security standards that reduce risks. Hereby, a business should remember to compare the cost of risk control against the value of the information and other risks to its business.

Implementation of the ISMS: In this phase, a business should implement the selected controls to manage risks. This would involve setting up procedures and instructions for management and for Compliance/IT department, raising awareness through training, assigning roles and responsibilities, and implementing any new systems. Close coordination with other compliance functions and projects, such as e.g. with regard to Sarbanes Oxley and Basel II requirements is required.

Review of the ISMS: This will help the business to ensure that the ISMS continues to manage the risks to its

data. This includes monitoring how effective the IT controls are in reducing the risks, reassessing the risks taking account of any changes to the business, and reviewing policies and procedures.

Certification of the ISMS: If available and useful in a commercial sense, the business should consider to have the security system or parts of it, such specific applications, certified.

Improvement of the ISMS: A security system needs to be maintained by improving existing controls, as well as putting into practice new controls if new threats or changes in the IT infrastructure occur.

Conclusion

Any business, which has an ISMS in place, should be well placed to respond positively to Data Protection Authorities in the context of notification of processing or transfers of personal data abroad. Security standards such as ISO 17799 can be used by any businesses irrespective of size or sector. The standard, will not render the business immune from security breaches, but they will reduce the risk of security breaches. Businesses will also be in a better position to minimize damage, cost and disruption if security breaches do occur. The use of COBIT, ITIL and ISO 17799, can help businesses to meet the information security requirements of data protection laws, in particular in an international context. There are distinct advantages to be gained by identifying and protecting the assets of a business. The advantage of using COBIT, ITIL and ISO 17799 is, that they are business-led best practice on information security management, providing ready-made guidance and processes for managing risks to information security. As well as helping to satisfy the technical and organizational security requirements of the data protection laws, third party service provider certification, e.g. with SAS 70 Type II can demonstrate to trading partners and to supervisory authorities that the business goes a step beyond general IT security compliance.

Dr. Jörg Hladjk
Hunton & Williams
