

IT compliance and IT security— Part I: Why is it necessary to comply with legal requirements?

This article is the first in a series of articles, by Jörg Hladjk of Hunton & Williams, that will address the interrelationship between IT security, compliance and data protection. This first part explains the concept of IT compliance, why it is important to comply with best practice and provides an overview of how compliance may be achieved

ImmEDIATE access to the latest data is essential for business. The Internet and other networks ensure that data are readily accessible. But easy access to data carries with it certain risks, including the risk of unauthorised access.

According to research by Gartner in 2006, 80 percent of companies will have suffered an application security incident by 2009. Recent examples of security breaches that go beyond application security incidents include Nationwide in the UK, which was fined £980,000 by the UK's Financial Services Authority because Nationwide's risk assessment and IT security procedures were considered to be inadequate. Another example involved Vodafone in Greece, where the Hellenic Authority for Information and Communication Security and Privacy fined Vodafone €76 million following a security breach and wiretapping incident.

These examples demonstrate that any weak link in a company's array of IT security procedures and IT infrastructure may jeopardize a company's confidential data. The failure to assure the integrity and consistency of controls over data processing and other IT systems could ultimately have a significant effect on the company's image or, more significantly, the value of its corporate assets.

What is IT compliance?

IT compliance is a key element of a business' risk management profile and a crucial aspect of good corporate governance. The broader concept of corporate governance captures the need for businesses to identify, understand and comply with the considerable number of laws, regulations and standards which affect how a business operates. The particular regulations concerning IT compliance focus on electronic data processing, networks and IT infrastructure.

Becoming compliant requires a business to adopt best practice

procedures including internal controls to protect IT systems, processes and ultimately the value of corporate assets. A plethora of statutory and supervisory regulations dealing with risk management have been introduced, tightened and enhanced in recent years. These include Basel II and Sarbanes-Oxley, but also laws on control and transparency in business, corporate governance codes, data protection and telecommunication laws as well as specific IT requirements.

The Sarbanes-Oxley Act of 2002 is a United States federal law passed in response to a number of major corporate and accounting scandals including those affecting Enron and WorldCom. Although the Act is focused on financial reporting, it has given IT issues increased importance. IT controls such as security, incident management, disaster recovery and electronic records management can have a direct or indirect impact on the financial reporting process and they do affect the reliability and security of systems in which companies keep their financial records. There are several titles and sections in the Sarbanes-Oxley Act that have a direct impact on internal controls, including IT controls.

IT compliance is by no means restricted to particular regulated sectors, and IT security requirements are no longer referable only to data protection laws.

Why is IT compliance necessary?

Businesses tend to comply with the legal requirements which form part of the IT compliance landscape because of the risk of sanctions being imposed in the event of breach. The sanctions may be either criminal or civil, or both. For example, data protection laws provide for both prison sentences and fines in certain narrowly defined circumstances. In addition, if necessary IT secu-

(Continued on page 4)

(Continued from page 3)

riety measures are not implemented, or not implemented appropriately, there may be liability to third parties with the prospect of paying damages.

Further, legislation—such as Basel II in the financial services sector—presume a high level of IT compliance to enable businesses to complete specific required assessments and reporting.

Sarbanes Oxley is similar: sanctions are robust in the first instance, and become even more draconian if wilfulness or an intention to deceive can be proven. A CEO or CFO who submits an inaccurate certificate is subject to a fine of up to US \$1 million and imprisonment for up to ten years. However, if the inaccurate certification was submitted ‘wilfully,’ the fine may be increased to as much as US \$5 million and the maximum prison term may be raised to twenty years. Further, auditors must maintain and preserve audit work papers for five years, which raises significant document-management issues. Non-compliance with this requirement can result in an additional fine and/or imprisonment for up to 10 years. The fact that these penalties carry serious personal sanctions for senior management acts as a significant deterrent and has resulted in IT compliance being taken more seriously within organisations.

Typical examples of IT compliance

The following are typical examples of areas that companies consider as part of their IT compliance and risk management programme:

- **IT requirements for risk management**

In Germany, the Federal Financial

Supervisory Authority (Bundesamt für Finanzaufsicht, “BaFin”) has developed “*Minimum Requirements For Risk Management*” which are binding on financial services providers. The requirements are used to define minimum standards which must be implemented by financial institutions as part of their risk management processes.

“*IT compliance is by no means restricted to particular regulated sectors, and IT security requirements are no longer referable only to data protection laws.*”

IT security is explicitly mentioned in Section AT 7.2 (Technical facilities and related processes) of the Requirements. Among other IT requirements, these state that the IT systems (hardware and software components) and the related IT processes have to ensure data integrity, availability, authenticity and confidentiality. In order to ensure this, the IT systems and the related IT processes have to be based

on established standards as a general principle.

According to the supplementary documentation, these standards for IT systems include, among others, the Basic IT Protection Manual of the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik - BSI) and the ISO 17799 international security standard of the International Standards Organisation.

The use of established standards does not mean that standard software or hardware has to be used—as a general rule, financial institutions use a significant amount of bespoke software. Further, best practice dictates that the IT systems must be extensively tested before they are used for the first time and after any material changes have been made. They must then be approved by both the staff responsible for the relevant processes and the staff responsible for the systems. As a general rule, the production and testing environ-

ments have to be kept separate.

Finally, enhancements and changes to technical specifications (e.g. the adjustment of parameters) should involve both the staff responsible for the relevant processes and the staff responsible for the systems. Technical approval need not be user-specific.

- **User and access administration**

In the compliance framework, identity management plays an important role in tracking which user has accessed systems and what systems each is permitted to access. Ideally, the technical setup follows standards and best practices for IT management such as ISO 17799, the Control Objectives for Information and related Technology (COBIT) and the Information Technology Infrastructure Library (ITIL). Provided these standards have been implemented correctly, conflicts with data protection laws may be avoided.

- **IT security for data**

Integral to compliance with the array of laws and regulations mentioned above will be the ability of an organisation to produce and retain secure data for audit, accounting and also legal purposes.

In the UK, the rules of civil procedure require that electronic records form part of the document disclosure process during preparation for trial. The significance which may be attributed to any record will be materially affected by the authenticity of the document (including the manner in which it has been created and stored) which, in turn, presupposes secure IT systems. Therefore, it is crucial to be able to prove the authenticity of data, the correct running of systems and to demonstrate that rights to access and modify data are tightly controlled and operate in accordance with carefully documented procedures.

Some laws, like Sarbanes Oxley, require organisations to retain information for a number of years following the end of the relevant fiscal period. This means that organisations will need to assess whether their systems can retrieve the necessary data, such as email, and this, in

turn, may have implications for the way in which email is stored, with its authenticity preserved.

Companies must ensure that all relevant data are backed up and that they may be accessed and searched when required. In addition, some laws require strong authentication controls such as encryption and user level logging of access and data amendment.

At the same time, data protection laws mandate certain security requirements such as access controls and processes to prevent denial of service, together with a means of recording and mirroring data. The key elements of compliance with ISO 17799 require business continuity planning, system access controls, system development and maintenance, physical and environmental security, compliance, personnel security, computer and operations management, asset classification and a controls and security policy.

How can IT compliance be achieved?

- **Impact assessment:** An impact assessment is invariably the starting point. Relevant questions to be asked include what are the applicable laws and regulations in each jurisdiction and what do they require an organization to do to its existing IT systems in order to achieve compliance?
- **Systems due diligence:** In parallel, it is important to prepare and verify an inventory of existing IT systems, ensuring that the specific purpose of each system is clearly understood. As part of this investigation, existing compliance programmes should be identified and assessed. In the absence of a comprehensive, holistic strategic approach to compliance, new systems may spring up in isolation and outside the organisation's compliance regime.
- **Analysis of competing regulatory requirements:** Regulatory frameworks such as Basel II have to be implemented in accordance with other competing regulatory

requirements, such as data protection, competition and tax laws as well as the requirements of corporate governance. A careful analysis, identifying overlapping or complementary rules and provisions, is crucial for successful IT compliance.

- **Contract audit:** A company should carry out an audit of existing contracts relevant to the IT system to ensure that they exist, that their terms are consistent with what is required by the supervisory framework and that any onerous terms are identified and their risks mitigated where possible. The manner in which contractual risk and liability are dealt with will form part of a bank's or financial institution's operational risk analysis. Both new and existing contracts will need to be reviewed with a focus on system procurement and integration projects, maintenance and disaster recovery relationships and outsourcing arrangements.

The increasing complexity of regulation and risk management requirements emphasises the need for an organisation to examine closely the adequacy of its current IT systems and how they fit within the wider compliance framework.

The willingness of the service provider to be contractually obliged to assist the organisation in meeting its security objectives and regulatory obligations is becoming an important feature of vendor-customer relationships.

Conclusion

The laws and regulatory requirements outlined in this first part of this article series are leading to significant changes in the manner in which businesses handle their IT compliance risks. The main objective of these IT control requirements is to ensure that risks are made transparent and that sufficient controls are implemented so that problems may be identified and dealt with as early as possible. Increasingly, personal responsibility is attributed to individuals within the organisation as a means of ensuring that

these issues receive senior management attention.

The principles-based approach which underpins the regulatory framework places additional responsibility on management; no comprehensive catalogue of the individual legal and regulatory issues which must be addressed can simultaneously address the organisational and business risks which form a crucial part of the overall IT risk and compliance framework of every business.

As a part of the overall compliance solution, the establishment of a comprehensive Information Security Management System is key. Further, strong IT security management in many cases improves IT security more efficiently and for a longer period than simply investing in security technology.

The second part of this series will consider some of the main international IT security standards, explain their scope and identify their data protection relevance.

Dr. Jörg Hladjk
Hunton & Williams
jhladjk@hunton.com
