New Minimum Standards for IT Security in the European Union –"EuroSOX" to be Implemented

Martin Braun

Martin's work out of Frankfurt involves outsourcing and technology transactions, data privacy and IT security, open source software licensing and e-commerce issues. He serves clients in the telecommunications, biotechnology, pharma, agriculture and new media industries.

49 697 941 2101

mbraun@mayerbrown.com

Legal requirements regarding IT security have been on the agenda of companies doing business in Europe for many years. The need to give serious consideration to these security obligations is currently reaffirmed by Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts, which is commonly referred to as "EuroSOX." Each member state of the European Union ("EU") has to pass national legislation to implement its requirements by June 29, 2008.

Primarily Statutory Audit Requirements

Like the Sarbanes-Oxley Act in the US, EuroSOX aims to strengthen the transparency and accountability of existing financial control and management systems. Primarily, this directive harmonizes requirements regarding education, approval, independence and registration of persons and audit firms who are authorized to perform statutory audits. Additionally, EuroSOX aims to create a high-level harmonization of statutory audit requirements for certain types of companies across the European Union.

Direct Impact on IT Security

These statutory audit requirements have a direct impact on companies' IT systems. The directive confirms that auditors are required to assess the affected companies' systems of internal controls and confirm the existence of a functioning audit committee, as part of the general risk management strategy. With information technology being a critical component of virtually all companies, IT systems and the security of such IT systems are a vital part of all risk assessment and management. At the same time, at each individual company, internal control and risk management systems themselves rely on the applicable company's IT systems. Unlike the Sarbanes-Oxley Act in the US, EuroSOX does not contain detailed obligations — each company will have to determine which measures are required and appropriate to ensure compliance.

Which Companies are Affected by the Directive?

EuroSOX does not apply to all companies in Europe. Primarily, the directive harmonizes the framework for auditors and their qualifications. At the same time, the directive also defines certain minimum standards for statutory audits of so-called "public-interest entities." Public-interest entities are defined as:

- entities governed by the law of a member state of the EU whose transferable securities are admitted to trading on a regulated market of any member state of the EU,

- credit institutions (as further defined in Art. 1 N° 1 of Directive 2000/12/EC), and
- insurance companies (as further defined in Art. 2 Para 1 of Directive 91/674/EWG).

Individual member states of the EU are free to extend EuroSOX obligations to other companies within their jurisdiction, and they may also, within certain limits set by the directive, choose to exempt certain public-interest entities from the minimum standards.

Companies to whom the directive is not directly applicable will very likely be affected by the directive as well, because public-interest entities will very likely require their suppliers and partners to comply with EuroSOX obligations (e.g., in the context of outsourcing relationships).

Standards in Europe are Already High

EuroSOX was passed on the assumption that companies generally have effective systems of internal control and risk management. These systems exist because of the already considerable number of laws and regulations relating to internal control and/or risk management. As an example, in Germany, such laws include the Federal Data Protection Act (*Bundesdatenschutzgesetz*), the German tax code (*Abgabenordnung*), provisions regarding management liability in the event of insufficient risk management in the German Stock Corporations Act (*Aktiengesetz*), and the Basel II requirements.

In addition, documents such as the International Standards on Auditing, International Accounting Standards, International Financial Reporting Standards and related Interpretations establish general requirements for statutory audits, including as related to

EuroSOX was passed on the assumption that companies generally have effective systems of internal control and risk management.

information technology and IT security. There is a good chance that most of the EuroSOX requirements are covered by these requirements already. Similarly, companies that are already in compliance with the Sarbanes-Oxley Act in the US will very likely only have to make limited changes, as EuroSOX appears not to contain any obligations that exceed those of the Sarbanes-Oxley Act.

Sanctions

Non-compliance with EuroSOX has severe consequences: auditors may refuse to issue audit reports due to these heightened requirements, and company executives may face personal liability under national laws if the internal control systems or risk management systems are considered to be inadequate.

Suggested Steps

For the coming months, it is advisable for companies to do the following:

- Review in detail whether the Directive is applicable to your company and how your company might be affected indirectly by the Directive;
- Closely monitor implementation measures of EuroSOX requirements in the countries relevant to your business;
- Review existing documentation of IT and telecommunications systems at your company;
- Review your company's existing strategy regarding certification under IT security standards such as ISO/IEC 27001:2005;
- Review existing agreements with your company's suppliers and business partners and consider amending contract templates in order to be able to impose IT security and compliance requirements; and
- Review or audit compliance with existing IT security and data protection requirements, particularly in relation to national data protection laws.

Conclusions

EuroSOX needs to be a top priority on the agenda of CIOs and internal legal departments, particularly because of the significant sanctions faced in the event of non-compliance. At the same time, the scope of actual changes due to implementing these requirements in the individual countries is likely to be rather limited, as many companies are already subject to similar obligations. ◆