

# Regulatory Compliance

## USA

The Sarbanes-Oxley Act (SOX)

The Sarbanes-Oxley Act (SOX) was signed into law on 30th July 2002, and introduced highly significant legislative changes to financial practice and corporate governance regulation. It introduced stringent new rules with the stated objective: "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws".

The act is actually named after its main architects, Senator Paul Sarbanes and Representative Michael Oxley, and of course followed a series of very high profile scandals, such as Enron. It is also intended to "deter and punish corporate and accounting fraud and corruption, ensure justice for wrongdoers, and protect the interests of workers and shareholders" (Quote: President Bush).

The Sarbanes-Oxley Act itself is organized into eleven titles, although sections 302, 404, 401, 409, 802 and 906 are the most significant with respect to compliance (Sarbanes Oxley section 404 seems to cause most concern) and internal control. In addition, the Act also created a public company accounting board.

Currently, the Sarbanes-Oxley Act requires Canadian companies that trade on U.S. stock exchanges to hire external auditors to audit their internal control systems and file a report of the findings

## CANADA

The Personal Information Protection and Electronic Documents Act (PIPEDA)

The Personal Information Protection and Electronic Documents Act (PIPEDA) is a new law that protects personal information in the hands of private sector organizations and provides guidelines for the collection, use and disclosure of that information in the course of commercial activity. The Act, based on ten privacy principles developed by the Canadian Standards Association, is overseen by the Privacy Commissioner of Canada and the Federal Court. As of January 1, 2004, all Canadian businesses are required to comply with the privacy principles set out by PIPEDA. The Act covers both traditional, paper-based and on-line business.

There are steps organizations must take to be privacy compliant. Under PIPEDA, personal information must be:

- collected with consent and for a reasonable purpose
- used and disclosed for the limited purpose for which it was collected
- accurate
- accessible for inspection and correction
- stored securely

PIPEDA defines personal information as "information about an identifiable individual" that includes any factual or subjective information, recorded or not, in any form. For example, the following would be considered personal information:

name, address, telephone number, gender; identification numbers, income or blood type; credit records, loan records, existence of a dispute between a consumer and a merchant, and intentions to acquire goods or services.

Under PIPEDA personal information does not include the name, business title, business address, or business telephone of any employee, i.e. information on a business card.

The legislation also covers sensitive personal information, which may include health or medical history, racial or ethnic origin, political opinions, religious beliefs, trade union membership, financial, information and sexual preferences.