



International Regulations (Privacy Laws and Data Protection) *by Norm Meier*

Over the past several years, a variety of regulations have been developed which have become a major focus to BCM programs for both national and multi-national companies. These regulations fall into two very broad categories:

- Privacy and Data Protection (*require protection of private and personally identifiable information*)
- Corporate Governance and compliance

These regulations come from two primary sources, the specific government (*i.e. USA, Australia, Canada as well as various States within a country*) or international stock exchanges such as the London, the US SEC (Securities and Exchange Commission), the European Union Data Protection Directive, the Canadian Personal Information Protection and Electronic Documents Act, or the Australian Securities and Investments Commission (ASIC). Many of the new regulations have expanded the civil penalties to criminal consequences for non-compliance.

The primary regulations within the US and their 'compliance' dates are:

- Graham-Leach-Bliley Act (GLBA) for financial institutions: May 2003
- HIPAA for organizations dealing with health information: April 2005
- Sarbanes Oxley (SOX) for public companies with SEC: June 2004 (or June 2005 for public companies below \$75M market cap)
- NFPA 1600 (*acknowledged by the US Congress, the Department of homeland Security, the 9-11 Commission, and ANSI as the National Preparedness Standard and high importance to the private sector*): No 'compliance' Date ...undergoing enhancements for 2007 edition.

Several States within the US have chosen to adopt their own versions of HIPAA and GLB that mirror or expand the federal regulations as well as developing SOX-type regulations that enter the non-public company area. An example here is California's Senate Bill (SB1386) which applies to any company with personal information on California residents.

SOX has become a 'defacto' international 'regulation' because it applies to many multi-national US firms and their divisions overseas as well as divisions of non-US companies registered with the SEC. It is connected to the recently updated FCPA of 1977. Although SOX only applies to public companies, the 'intent-to-comply' bar has been raised for private and nonprofit organizations as well.



SEPTEMBER 18-24, 2005

Australia's Commonwealth Criminal Code has been updated (2002) to address the officers and directors of a failed company that did not have a proper risk management plan in place. This upgrade also provides severe penalties for cyber terrorism and hacking, one of the common threats for BCM and DR programs. ASIC's CLERP 9 (Corporate Law Economic Reform Program) regulation became effective July 2004 and focuses on Audit Reform and Corporate Disclosure (similar aspects to SOX).

International standards such as those of Australia/New Zealand Standard 4360 (Risk Management) and its corresponding Handbook (HB221) of business continuity guidelines; London Stock Exchange's 'Turnbull Guidelines' and the Australian Stock Exchange 'Principles of Good Corporate Governance' as well as the established COSO and Basil Guidelines for the international financial markets.

There is a common thread to all these new regulations, rules and guidelines and those are elements fundamental to a solid BCM program:

- Risk assessment
- Control environment and activities
- Policies and procedures
- Internal and external communication plans
- Training
- Monitoring the program

What it does differently is force the BCM professional to be aware of regulations not only in their country but any country their organization and its supply chain does business in.

As a business continuity professional, a regular, independent 'report card' assessment of your business continuity program is becoming important and should include compliance and regulatory focus as well as a focus on crisis communication plans that address all elements of the business continuity program.

Norm Meier is a Fellow of the Business Continuity Institute (FBCI) and is President/Owner of The Catalyst-A Global BCM Consortium. Their specialty is providing Snapshot-in-Time (SiT) Report Cards of an Organization's status on all elements of the BCM program. Clients are International and diverse with representation from transportation, education, financial, cultural (museums, libraries) and manufacturing organizations. The Catalyst is an alliance partner of the Media Skills Network tm. He may be contacted at normmeier@att.net.