

Electronic records compliance management - not if, but when

Innovative processes and systems are now required by financial institutions to ensure day-to-day records are managed in a way that satisfies all regulatory compliance issues.

By David Thompson*

Compliance issues loom large for board members and senior executives from financial institutions throughout Australia. New demands are being placed on organisations today as regulatory bodies, investors, shareholders, customers and employees demand greater accountability, responsibility, auditability and control of the organisation's information, processes and reporting.

An increasing array of regulatory requirements is compelling organisations to preserve and manage electronic records. These include:

- Australian Standard on Compliance (AS3806)
- Basel II
- Commonwealth Electronic Transactions Act 1999
- QLD Recordkeeping (IS40)
- NSW Workplace Surveillance Act 2005
- VIC Crimes (Document Destruction) Act 2006
- Sarbanes-Oxley 2002

For organisations not directly affected by specific regulatory requirements today, corporate governance and litigation concerns are requiring them to implement new, more exacting measures to manage and protect electronic information that may someday be subject to internal and external audit and e-discovery.

One ubiquitous facet of business that has had considerable publicity over the past couple of years is email communication. Many reputations have been tarnished and/or large fines and sanctions imposed because of controversy over emails – involving companies such as Enron, AWB and Morgan Stanley, as well as government agencies such as the CIA to name but a few.

The case of Morgan Stanley

Massive and exponentially growing volumes of email can create an additional set of issues in the event of e-discovery, such as ground-breaking cases like *Perelman vs Morgan Stanley* in which Perelman was awarded \$US1.45 billion in damages after Morgan Stanley was unable to prove convincingly that it had handed over records of all the emails requested.

Subsequent to this, Morgan Stanley reportedly paid a \$US15 million fine to the US Securities and Exchange Commission for its failure to archive emails in compliance with regulatory requirements. This highlights the fact that there is little scope to doubt the importance of email in legal, regulatory and compliance issues.

Even organisations with sophisticated IT infrastructures, which would include Australia's major banks, building societies



Even organisations with sophisticated IT infrastructures, which would include Australia's major banks, building societies and credit unions, face a compliance problem: most of them wouldn't be able to comply with a broad legal discovery order fast and accurately, because they don't archive and manage electronic content in such a way that it can be searched and retrieved in a timely manner.

and credit unions, face a compliance problem: most of them wouldn't be able to comply with a broad legal discovery order fast and accurately, because they don't archive and manage electronic content in such a way that it can be searched and retrieved in a timely manner. In fact, most companies rely on tape backups and think that's enough. But when the company wants or needs to find and retrieve specific historical records (in the event of an audit or litigation for instance) it usually struggles – even when faced with a multi-million-dollar judgment (as in the case of Morgan Stanley). And that should send shivers down the spine of every finance, compliance and IT executive.

The new Crimes (Document Destruction) Act 2006 applies to individuals and companies oper-

ating in Victoria who destroy documents that are considered reasonably likely to be required in legal proceedings, or prevent them from being used in evidence (eg concealed or rendered illegible). This includes emails and their attachments. A crime is also committed if a corporate culture exists within a company that leads to the destruction of the documents.

With more than 80 per cent of company communication now handled via email and instant messages, this should be the first area that directors and managers validate to ensure that appropriate policies and procedures are in place.

Today's management of electronic records

Given a changing regulatory and legal environment, organi-

sations should implement policies and procedures to manage the retention and disposition of their corporate records. A streamlined process that automatically enforces policies is essential to ensure a compliant framework for creating a corporate memory with expert recall for legal discovery and compliant destruction for continual risk mitigation.

In dealing with unstructured data (emails & instant messages), IT departments should ensure all business-related communication is copied to archive before they arrive on the employee's desktop and immediately as they are sent from the employee. These business records can be stored using WORM (write once, read many) technology, so the documents can be accessed but can't be modified.

Ideally, the organisation should implement a centralised

and integrated archive to manage the retention and disposition of these electronic records and make them easy to search and retrieve as needed. Solutions are available where unstructured data is archived with all other electronic record types including desktop documents, ERP systems, images, voice and video, creating a true single repository.

Relying on backup tapes does not address these issues.

A mis-match in records compliance

There is a mis-match between what an organisation requires to manage its business and what the IT department is currently delivering.

IT management needs to be aware of today's requirements for the retention and management of electronic documents; inadequate processes carry risks that the business may not be able to sustain or will take a long time to recover from.

With email being used for most business transactions, companies need to instigate a number of policies and practices.

A water-tight records retention policy is imperative, ideally supplied as a simple, automated, electronic solution with no end user intervention required (i.e. don't leave it up to end-users to decide what to keep and for how long). Alleviating the costs of physical storage, a rules-based storage management solution provides for the automatic flagging of disposal in accordance with statutory retention requirements.

Organisations should investigate implementing a single, integrated platform where both the unstructured and structured data are archived in a central repository, with each record managed throughout its lifecycle.

A full 'search and retrieve' facility

A single archive solution for storage of disparate data isn't much good unless it has a powerful search facility that enables 'one in a billion' emails to be found in minutes, most probably in context with records generated by other applications. There should also be an ability to apply case holds to records, which suspends their usual disposition and prevents them from being destroyed.

A browser-based environment can provide the user with an intuitive and efficient way to search, retrieve, display and process the archived data.

Organisations need to be 'dispute ready' so they can find the records they need accurately and quickly. ■

* DAVID THOMPSON IS THE CHIEF EXECUTIVE OFFICER OF RECORDS COMPLIANCE MANAGEMENT SOFTWARE SOLUTIONS COMPANY, AXIS-ONE PVT LTD.
WWW.AXISONE.COM.AU