



Managing record keeping risk

By Barbara Reed, Director and Kerry Gordon, Director, Recordkeeping Innovation

- Information needs to be managed like any other asset and it is vital to ensure that security standards are sufficient to ensure that leakage or unauthorised use does not take place
- Management oversight and control is essential, but also assign responsibilities clearly
- A degree of human error is inevitable but a culture of accountability is an important safeguard against risk

Managing risk in the complex modern business environment is not easy. The risks associated with record keeping and information management are usually not transparent to corporate risk managers. Record keeping and information risk adds an extra dimension to business risk.

Because business information is vital to conducting transactions, the link between business risk and record keeping risk is very close. But treating record keeping risk as an identifiably separate component of risk enables organisations to become more sophisticated, focused and successful in managing risk.

The responsibility for managing records often falls between executive responsibilities and therefore may not be well managed. From risk management we have learnt of the need to plan for the likelihood of something happening and having plans to manage the consequences of the event. The potential impact of record keeping risks includes economic or financial losses, damage, including reputational damage, injuries and delays. Record keeping risks can also include the failure to share or publish information to prevent an occurrence, as well as the more usual examples of breaching the information security policy.

Records management, accountability and risk are closely aligned. Records are essential for auditing and accountability. When developing a strong record keeping governance framework, there are many risk-based decisions to be taken — some intuitively — but this article clarifies potential risks and shows what needs

to be addressed. It outlines what board members and executives need to know and presents a model for action to address record keeping risks based on international standards. The aim should be to take a simple, self-assessment checklist in order to assess your organisation's preparedness, and to ensure that record keeping governance can be monitored, reviewed and audited, empowering executives to act. This outline is the basis for a more detailed training workshop on how to manage record keeping risk.

What's the problem?

In recent years, greater regulatory and compliance requirements have been imposed on organisations in all aspects of business, from compliance with GST reporting to environmental standards and carbon footprints. There is plenty of evidence that organisations have already failed to meet this rising challenge of managing digital records associated with compliance and accountability requirements. Across Australia, Auditor-Generals' departments have consistently reported that government agencies are not performing well enough. In particular they have highlighted that:

- the management of electronic records in all government agencies (with minor exceptions) is inadequate. In our experience, practice in the corporate environment is even worse than most government agencies
- record keeping needs to be managed more strategically
- a risk-based approach should be adopted, and
- record keeping should be integrated into a larger information environment.

More rigorous regulatory regimes imposed on businesses in recent years (IFRS, Sarbanes Oxley and Basel II to name a few) have increased that compliance burden of Boards and executive officers, but offer little in the way of guidelines of 'what to do'. Few organisations have allocated a role of 'chief information officer', and when they have, this is traditionally a technical not a content expert, so the responsibility for information content is often diffuse or shared across several roles within the executive — often the company secretary, legal manager or risk manager. It can be difficult to determine just who is in charge, and often it's no one in particular. Managing record keeping risks is harder than ever before. Technology improvements have made it both easier, and harder. Technology makes it easier to copy electronic information, distribute and move it, while simultaneously making it more fragile, harder to preserve and protect from obsolescence. While organisations are in the process of changing from hardcopy to an electronic environment, important safeguards and anti-fraud measures that were previously common practice are not translated into the online world.

There has been a focus on IT risks, and while we should not underrate the seriousness of that problem, IT risk (for example, virus protection, backups and logons) is not the same thing as information content risk, although IT security is a critical component of managing record keeping risk.

What are the risks to mitigate and what is the potential impact? Using case studies, what can we learn from past experience?

What are we trying to achieve?

The objectives of any record keeping risk plan are to:

- deliver better outcomes for the organisation
- protect stakeholder and shareowner interests
- identify, prevent, mitigate or effectively constraints threats to an acceptable level, thereby minimising potential losses

- make informed decisions about exploiting opportunities for reuse of information and assets.

Maintaining accurate and reliable business information which provide evidence of activity (records), is a critical part of doing business, doing it efficiently and effectively, and providing trustworthy services. This has been recognised by the UK government which states:

Guardianship and management of information in all aspects (integrity, availability and confidentiality) is crucial to service delivery.¹

The key areas of critical importance for managing record keeping and information risk are:

- governance and cultural change
- ensuring the integrity of records and information, particularly the preservation of key corporate information
- managing human error and behaviours and having an accountable corporate culture
- managing the publication, distribution, use, privacy and protection of records.

Governance and cultural change

Organisations need to manage their information assets, just as they do their other assets — such as personnel, finance, property — by allocating responsibility clearly and ensuring that all staff know what they are expected to do, and how they should contribute their records to the shared corporate pool. Information risks should be identified as a key element of the risk mitigation plan. If there are breaches of records rules, is there a plan of action to address the issue and communicate with any clients or stakeholders who are affected by the problem?

An assessment must be made of the potential impacts on business continuity, reputation or integrity and it is essential for the board to be aware if confidentiality, integrity or the availability of records has been compromised. Ownership and control of records should be clearly

assigned, with particular regard for privacy protection and information security. There is a need to ensure that standards of security are adequate and that robustness of security over both paper and increasing the electronic records is adequate, especially with regard to access, rules for transfer, distribution, and storage. There should be a means of reporting on record keeping compliance and system performance to the board so that any gap can be identified, objectives for risk management are set and progress to achieve agreed risk priorities is known.

Some governance and culture risks to manage are as follows.

- A failure to provide comprehensive oversight and control means anything can go wrong.
- A failure to assign responsibility when something goes wrong means that no one is responsible for addressing the problem, and the problem can be repeated. The agency fails to learn from past mistakes.
- Inadequate safeguards and contractual agreements with third party providers or outsourcing of records functions may lead to record keeping breaches where third party providers let you down.
- When changing or upgrading technology or business processing, ensure the same accountability standards and safeguards are in place and don't let the ease of electronic processing undermine accountability standards.

Barings Bank

In 1995 Barings Bank collapsed when it could not meet enormous trading losses incurred by a rogue trader, Nick Leeson, located in the bank's Singapore office. Leeson had engaged in unauthorised activities, such as changing the trade prices and crediting 'switching' accounts where losses were neither reported nor reconciled. Accounts were not independently audited. Internal audit reports recommending a separation of powers were not actioned.

Ensuring the integrity of records and information, particularly the preservation of key corporate information

Every organisation needs a records management program with a statement of scope and intentions, a budget that is adequate to the tasks, and control over the capture, registration, identification, storage, security, and disposal of all records. A lack of clear expectations, a records policy and procedures that do not include staff can result in wide-ranging consequences, increased risk of fraud or corruption and reduced accountability standards.

Some key risks to manage in the area of record integrity are as follows.

- Non-compliance with corporate standards or the use of personal records systems means a lack of accountability and review.

Victoria Police

In 2009, the Victorian Police Force IT Department was riddled with dodgy multi-million dollar deals, records were in a shambles and staff were cashing in on free hospitality when there was no one in charge, reported the Ombudsman. With a budget of more than \$200 million, IT contracts worth tens of millions of dollars were kept on handwritten notes. There were significant gaps in documentation, records were not dated and not signed, or did not include author details.²

- If an organisation is not ensuring that the requirements for records are known

and that records are retained for the full length of time they are needed, critical information may be wrongly destroyed, not retained, can't be found or accessed to verify statements or decisions.

- Inaccurate information may cause the wrong decision to be taken.
- Key contextual information is lost due to technological obsolescence and causes financial or legal damage or loss of reputation.

Japanese Social Insurance Agency

Failure to manage electronic records for the full length of time that they were needed by the Japanese Social Insurance Agency caused a government crisis in 2007. The introduction of a new pension scheme meant that multiple pension numbers from previous systems were integrated into a single pension number for each person. Records were not properly transferred, so 50 million pension records couldn't be linked to the individuals who had made the payments.³

- The failure to provide appropriate business continuity and disaster recovery can lead to critical information loss or damage after a disaster causing further loss or damage.

Hurricane Katrina

When identity documents were lost during Hurricane Katrina in the US in 2005, victims were ineligible to apply for state benefits, thus compounding losses for individuals already in distress.

Managing human error and having an accountable corporate culture

Sometimes policies and procedures are not enough. Executives need to lead by example and treat record keeping risks with the same level of importance as financial and other risks, with adequate safeguards, separation of powers and monitoring of practices. Staff need to be aware of what they are expected to do, and have a supportive environment for identifying inappropriate or corrupt behaviour by others, including their managers.

Is there a clear understanding of privacy protection, what can be said to clients over the phone, procedures for whistleblowing or escalating problems confidentially? Are sensitive records adequately labelled and have associated business rules governing their storage, copying and distribution to prevent security breaches. When staff fail to meet record keeping standards or do not comply with policy, are there methods to address their poor performance, or is it tolerated and allowed to undermine the good behaviour of other staff?

Accountability and human error need to be managed for these sorts of risks.

- Despite having policy and procedures in place, staff act in error resulting in an unauthorised release of information.
- Despite rules, insiders still do the wrong thing.
- Failures to check usage patterns, unusually high levels or after hour use

of systems can result in facilities being used for improper purposes and with undesirable results.

- Failure to remove access permissions to short term staff at the end of contracts can lead to unauthorised or inappropriate access.

Jake Kovco

A CD containing a draft of the confidential report into the bungled repatriation of the remains of Private Jake Kovco from Iraq was left in the Qantas Club at Melbourne airport. This caused public embarrassment, personal distress and reputational damage as the disc found its way into the hands of talkback radio host Derryn Hinch.

Enron

Through the 1990s, Enron started making deals with limited liability corporations that it controlled, allowing them to hide many of their debts and losses from their financial statements. In reality, Enron was close to bankruptcy, but no one knew, except its accounting firm, Arthur Andersen, and the company executives. In 2001 the scandal was exposed, causing its stock to drop from nearly \$100 a share to less than \$1 a share...

It was the duty of the forensic accountants on the Enron case to look over every accounting record, including the records of its owned limited liability corporations to verify that the numbers say what actually happened ...

Though forensic accounting acts as a prevention of tax fraud within businesses such as Enron, it's not necessarily the solution. The solution is vigilant record keeping and ethics training within businesses.⁴

- The failure to adequately and appropriately destroy electronic records so data cannot be recovered from backup tapes or discarded equipment can result in leakage or exposure of data.

- Failure to adequately protect privacy adequately to prevent identity theft, phishing or hacking can make data records available to persons seeking to fake identities for criminal purposes.

University students' academic results

The NSW Independent Commission Against Corruption (ICAC) was investigating alleged improper use of a computerised student record system of a major Australian university. A key business requirement of the system is to ensure the integrity of university academic results. The system must provide an accurate representation of student results and be protected against alteration or unauthorised deletion. ICAC's investigations revealed that the business information system used to manage student results was not able to meet these key recordkeeping requirements. People were able to access and use the records inappropriately, which resulted in significant fraud. Access rules, which stated that former staff should not be able to continue to access business systems, were not policed. As a consequence inappropriate record access and use occurred. Metadata used to document record access and use was also inappropriately defined and important information, such as who had changed what records, was not captured. As a result the access rules, that were ostensibly in place, were able to be flouted. Record reliability, authenticity and integrity were all therefore compromised.

Managing the availability, publication, distribution, use, privacy and protection of records

Protection from unauthorised disclosure requires clear business rules around who can access and use records. There needs to be an understanding of the clearance process for exceptional use. This includes all phases of the record's life, including disposal and destruction, as can be seen from the example of Moran Health Care

(see box). Sensitive records should be labelled as such. Points of vulnerability need to be identified and staff need training to ensure that they understand their roles. The responsibility for protecting records should be clearly assigned to a data and records protection officer.

Regular monitoring will help to show weaknesses in the security system, and breaches of security should be linked to staff performance management. If security breaches occur, ensure there's a system to document them and use the analysis of what went wrong in future training programs to learn from mistakes.

If information is shared with other organisations, ensure there are clear boundaries and contractual agreements in place so that records continue to receive the same level of protection as they did while they are in your custody. This might include transport and destruction rules and safeguards.

Where the organisation receives requests for information, ensure there's a record of what information has been released and that if required, the released information can be re-produced. Ensure that information released to the public through websites and publications is registered and the date of release tracked.

Some risks to manage in the availability and distribution of records are as follows.

- Sensitive or personally identifying records may be inappropriately disclosed.

Moran Health Care

In May 2009, a taxi driver found hundreds of private documents dumped in Bridge Street, Sydney outside the Moran Health Group office, including property contracts, legal correspondence, wills, title deeds, staff details, payroll and patient information. Moran Group is regulated by the Department of Health and Ageing under the Aged Care Act 1997 and may have been in breach of this Act as well as the requirement to comply with the privacy regulations.⁵

Key Issues Applied Corporate Governance

- Ensure that vulnerable information is identified, labelled and has adequate usage and other business rules clearly associated with the security labels.
- Have security systems been tested and monitored?
- Make sure that you manage and disclose critical case information to protect client rights and entitlements.

Public access via Google

A well known legal publisher entered an arrangement with courts to publish cases online. The cases are inadvertently made available to Google Search (not knowing that you could turn these off). After only a very short time, the publisher was inundated with complaints about the fact that this information is available. It's usually the subject of the information that objects (for example, the barrister who is appalled that the case over his high fees is public, the person appalled that details of domestic violence are available). The implication is that these people might have Google alerts out on their name. Whichever way it arises, the issue of private and public information is raised. When this was taken back to the court in question, their response was that although there was always public access to this material so technically it was public available, there is also the reality of 'practical obscurity' achieved by making access difficult through physical means, and this is what has been changed by widespread digital availability. The material is still available, but only to those who know the URL. It has been blocked from Google searches.

- Are you able to reproduce information or publications that are already in the public domain or from the website?
- Are you able to get the right information to the right people at the right time? If not, the results may be disastrous.

Every organisation needs a records management program with a statement of scope and intentions, a budget that is adequate, and control over the capture, registration, identification, storage, security, and disposal of all records. A lack of clear expectations, a records policy and procedures that do not include staff can result in increased risk of fraud or corruption and reduced accountability standards.

Detroit Airport bomb plot

Christmas Day 2009. The US Government had enough information to prevent the alleged bomb plot, but failed to 'connect the dots'. US President Barack Obama admitted 'This was not a failure to collect intelligence; it was a failure to integrate and understand the intelligence we already had.'

What to do

This is a checklist of what to do to address record keeping risk.

1. Assess the importance of the organisation's record holdings.
2. Assess all the record keeping risks, sensitivity and points of vulnerability.
3. Develop a plan for managing risks, including proactive mitigation steps and what to do if things go wrong.
4. Inform staff of their roles and responsibilities to manage record keeping risks, and make it a performance measure.
5. Acquire the right skills and capability to manage records through a program of systematic control.

6. Ensure that record keeping standards are embedded in business processes, there are sufficient points of review and auditing standards are met.
7. Ensure processes are monitored, checked and reviewed. New risks can emerge from different sources and in countless numbers of ways. Risk management requires a continuous improvement approach.
8. Keep management informed of the record keeping risks, in the same way they receive regular updates on personnel and finance.
9. Take on an incident management approach and ensure a prompt response to mitigate the impacts of risks. Security breaches will occur. Organisations need to detect and respond promptly to minimise the harm.

To improve management of your organisation's record keeping risks, ensure that you understand the nature of the risks to your business and make sure that record keeping risks are adequately identified and covered in your risk management plans.

Barbara Reed and Kerry Gordon can be contacted on (02) 9267 3700 or by email at mail@records.com.au.
www.records.com.au

Notes

- 1 UK Government, 2008, *Managing Information Risk: A Guide for Accounting Officers, Board Members and Senior Information Risk Owners*, http://www.coal.gov.uk/media/A3D/15/Information_and_Risk.pdf [19 February 2010]
- 2 AAP and Cooper M, 'Police IT department 'riddled with dodgy deals'', 2009, *The Age*, 12 November, www.theage.com.au [10 February 2010]
- 3 UK Government, op cit, p 27
- 4 Sherwood C, 2008, 'About Enron and Financial Accounting', www.ehow.com/about_4614281_enron-forensic-accounting.html [10 February 2010]
- 5 Jensen E, 2009, 'Patients' documents found in city street', *Sydney Morning Herald*, 25 May, www.smh.com.au [10 February 2010] ■