iQ

InfoRMAA Quarterly

IS THERE LIGHT AT THE END OF THE DIGITAL PRESERVATION TUNNEL?

EDMS/EDRMS
The Good, the Bad, the Ugly

90 QUESTIONS
You Should Ask Vendors

EMAIL HEAVEN & EMAIL HELL

INTERNET SECURITY
The Looming Threats

RIM RELICS
A Luftwaffe Album

DIGITAL RIGHTS MANAGEMENT
Does it Tie Your Hands Behind Your Back?

INTERVIEW WITH A GURU
We Talk Digital With Recordkeeper Chris Hurley

iQ

infoRMAA Quarterly

CONTRIBUTIONS & EDITORIAL ENQUIRIES
Articles, reports, reviews, news releases, Letters to the Editor, and content suggestions are welcomed by the Editor, whose contact details are above.

ADVERTISING
Comperation Group Pty Ltd
Aarti Karande
(02) 9954-9000
aartis@comperation.com

ANNUAL SUBSCRIPTIONS
$75.00 (plus GST) per annum for all issues (incl postage), from:
Membership & Financial Services
RMAA Office
GPO Box 1059 BRISBANE QLD 4001
P: 1800 242 611   **F**: 1800 333 802

***IQ* ONLINE ARCHIVE**
Every article published in *InfoRMAA Quarterly* since 1984 is available online to RMAA members at the *IQ* Online Archive.
To access, simply log on to www.rmaa.com.au and go to the *IQ* Archive.

RMAA WEBSITE
http://www.rmaa.com.au

In This Digital Issue

Front Cover:
Is there light at the end of the digital preservation tunnel? Two international experts discuss the issues, starting on page 38.

Together, We Can Do It!

Just, as in every busy work day we have to address a range issues, for this, my very first President's Page in *IQ*, I'd like to discuss three different subjects relating to records and information management. Yet they all share a common theme - of what we can achieve TOGETHER.

As this edition of the journal is focused primarily on the **digital world**, I'll begin with digital records. There are so many benefits to implementing sound records management practices and procedures for digital records. For example, they help us fulfill legal mandates, facilitate records retrieval, identify strategies for preserving records, reduce the costs of storing obsolete records, and ensure the creation and management of accurate and reliable records.

As several articles in this edition of *IQ* point out, questions hang over the long-term preservation of digital records. Maintaining access to digital records over time will be a shared responsibility. Establishing and operating effective recordkeeping systems and good business practices are best achieved through a multidisciplinary approach.

Effective teams would include individuals with expertise in archives and records management, information technology, data and information management, business system analysis and design, auditing and risk management, and the law. I firmly believe that by working together, we can overcome the short-term problems and create long-term solutions.

THE PROFESSION MUST BELIEVE IN ITSELF AND BUILD ON ITS QUALITIES

As a group, we are able people who serve our clients and employers well, and through them, society. Society changes and we change with it. We must not apologise for being records managers. We should be proud of what we do. Unfortunately, it appears that we have got into the habit of believing our own bad press. Only a tiny proportion of record managers cause serious problems but we all feel it very badly when it occurs. We take it personally.

This is both a strength and a weakness. It's great that we care so much. How many other professions truly do? But sometimes we forget all the good we do, the quality of service we give and the value for money we offer.

Look at what we have. We are well known for our independence. We have high ethical standards and we offer the public unrivalled protections. Keeping the trust of our clients and employers is equally as important to us as the records we keep. We possess great skills which we use to the benefit of our clients, employers and society. Above all our values are human ones - we understand, we help and we protect.

Together, we can build on all these qualities. The ways in which we educate for the future, the development of standards as we adapt to extraordinary advances in technology and much-needed legislation are all leading the profession to think in new ways about what record managers are and how we should operate.

The RMAA can and should help the profession with these new ways of thinking. Collectively we must provide demonstrably useful services to benefit records and information professionals and add value to your membership of the Association. We are stronger together than as individuals.

23rd INTERNATIONAL CONVENTION, SEPTEMBER 2006, CAIRNS, QUEENSLAND

That strength is never more apparent than at our international conventions, where we come together to share our knowledge and experience. These events reward us not only in terms of professional development, but also in terms of networking opportunities.

This will be a recurring message from me, but one that is important to you, your organisation, your profession and your Association - make every effort to join us this year. The 2006 Convention in Cairns from September 17-20 will provide a unique opportunity for delegates to survey the past, examine the present, and look to the future, as records meet the reef.

The programme promises to be challenging and diverse and will feature both Australian and international speakers. Events will include a welcome reception, convention dinner, and farewell cocktail party. The vendor showcase offers more educational opportunities and hands-on introductions to the latest products and services for effectively managing records and information.

To assist you obtaining approval to attend, a template 'Letter of request to attend' has been posted to the RMAA website. Use it as a base to gain approval from your manager to attend this very exciting and diverse programme in September.

As always, I invite you to contact me on any issues that you wish to raise. TOGETHER, we can ensure that the Association, and the profession, move in the right direction.

Kemal Hasandedic
National President, RMAA

Kemal Hasandedic,
RMAA's National President

From the CEO

I know that CPD is a recurring theme from me, but it's one that I feel passionate about and can't stress enough.

The world in which all professionals practice is changing. Global competition has never been more intense, clients are more demanding, and digital technology offers new ways of working. The knowledge base of professionals has increased.

With such changes come new opportunities; new clients, new markets, new areas of practice and new work methods. Above all, such changes demand new knowledge, new skills, and increasingly a commitment to lifelong professional learning.

For many professionals, this commitment is manifested in an active involvement in Continuing Professional Development (CPD). An increasing number of professionals recognise the benefits of adopting a more planned and structured approach to professional development.

Not only is it important to keep up-to-date and know *what*, but also to know *why*, and *how* to deal with a new professional or managerial issue. In the knowledge-intensive world of the professions, some have argued that the only real source of sustainable competitive advantage is the ability to learn faster than the competition.

In many professions and countries it has been formally recognised for over 20 years, whilst in others it is at a more embryonic stage of development. Whatever its nomenclature, the continuation of professional or personal development is an aspect of life that is avidly followed by those wishing to ensure that they remain at the forefront of their chosen profession.

WHY CPD IS IMPORTANT

Firstly, it should be emphasised that the concept of CPD is not new. Effective professionals in all fields have always realised the importance of new knowledge, improved skills and the development of personal qualities.

In effect, CPD is simply part of good professional practice. What is new, is the greater importance and relevance of CPD to professional success. The growing importance of CPD can be attributed to the following.

Competence: It has been estimated that the knowledge gained in some degree courses has an average useful lifespan of about four years. While this will vary according to the discipline, it does nevertheless highlight the increasing need to maintain an active interest in keeping up to date with changing technology, legislation and operational procedures.

If, at the same time, professionals have expectations of increased managerial responsibility, the need to acquire new skills and knowledge is even more acute.

Consumerism: The development of a more affluent consumer society has also resulted in a better informed and more sophisticated public. One consequence of this trend is that the public expects a higher duty of care and level of service from their professional advisors than in the past.

Again, the skills acquired during an initial training period or during higher or further education may not equip new staff for this role.

Litigation: The professions are increasingly at much higher risk from claims of negligence than in the past. Professional indemnity (PI) insurance premiums have risen considerably in recent years.

CPD may not totally eliminate PI claims; however, if sceptics are worried by the cost of CPD, such claims may help emphasise the potential cost of ignorance! Some evidence is also emerging that insurance companies may be willing to slightly reduce PI premiums, if a structured CPD programme is available to staff.

Standards : A primary role of professional bodies is to safeguard standards of competence. CPD has a key part to play in the communication of agreed standards and in ensuring that members comply with specified procedures.

Quality Management System : The increasing emphasis on quality management systems and the ethos of continuous improvement has also increased the relevance of CPD. Training and education are key elements of quality assurance processes.

Competitiveness : Whether in the private or, increasingly, in the privatised public/state sector, the competitive market edge must be partly or totally focused on client care/service quality and technological innovation. Both demand a high investment in developing people skills if they are to be effective.

The RMAA has a CPD scheme that is compulsory for all Professional Members and Fellows, and whilst optional for all other members I encourage all of you to step up to the plate, take control of your own professionalism and join in the scheme.

Details are available on the website (www.rmaa.com.au) or by contacting myself at kate.walker@rmaa.com.au. Further learning is here to stay.

Kate Walker
RMAA CHIEF EXECUTIVE OFFICER

Kate Walker,
CEO of the Records Management Association of Australasia

From
the Editor's
D E S K

IN THE DIGITAL WORLD

With RIMs confronted by rapid and unprecedented change in their work environment, we've dedicated this issue of *IQ* to problems and opportunities in the digital world.

Just as Off the Record columnist Kenneth Tombs warns of the dangers of becoming locked into soon-to-be-outdated digital technologies, several authors deal with thorny issues about EDMS/EDRMS, and we offer a list of 90 basic questions software system customers should ask vendors. We also take a look at a new implementation at the University of Western Sydney and also discuss EDMS software and compliance.

Is there light at the end of the digital preservation tunnel? With the future of e-records dependent on the technology that supports them, we look at the critical issue of digital preservation from two different expert perspectives - one Australian, the other taking in the international experience. We also look at digital rights management, email, Internet security, and efficient intranet searching.

We have two *IQ* Interviews, both, coincidentally, with a Chris. We lead off with Chris Hurley, RM's sometimes controversial knight in shining armour, and follow him with Chris Lynch, new Managing Director for Australia/New Zealand of US software house Interwoven, which has launched a new EDRMS product on the A/NZ market.

And, in RIM Relics, we publish rare 1939-45 photographs by a secretary to Hermann Goering, the second-highest man in Germany's Nazi hierarchy, from a private collection.

Talking about RIM Relics, a reader has made some interesting observations in relation to our 'Hiroshima Context' RIM Relics story in the latest issue of *IQ*, (November 2005). We were wondering about the connection between the sketch of the Aussie digger at Kure, Japan, and Hiroshima, site of the first 1945 A-bomb attack.

The reader points out that the port and naval base of Kure is only a short distance from Hiroshima, and this is where Australian occupation troops assigned to the Hiroshima area would have landed.

They also noted that in the SBS TV documentary 'Submariners' aired in January, a female crew member of the Australian submarine HMAS *Rankin* docked at Kure visited the A-bomb museum at Hiroshima.

KEEP THOSE SUBMISSIONS COMING

Even if you've never written an article before, if there's a RIM-related subject you have strong views about or experience with, or you have an interesting case study, send it in.

Apart from gaining enormous satisfaction from seeing your work published, articles by RMAA members in the journal contribute to their status upgrades and put them in the running for the Objective *IQ* Article of the Year Award.

There is also the possibility of your article subsequently being picked up by an overseas journal. In January, the Records Management Society of Great Britain sought permission to republish in their journal, the *Bulletin*, nine articles which appeared in *IQ* last year. Of course, both *IQ* and the authors involved were delighted to give their permission for the articles in question to also be published in the UK.

In May's *IQ* we're covering issues that affect the individual RIM. For example, we're publishing a US study that poses the question, 'Do RIMs have a distinct personality?' We'll also look at RIM education and training. If you've a view to put about personal development, email me a query or submit an article. Editorial deadline for the May issue is April 1. By the way, I'll be overseas for most of March – so I won't be able to respond to March emails until my return.

For our August issue we're looking for material dealing with policy, law and compliance. If you've something to say on those subjects, email me to discuss your idea.

We're especially interested in securing case studies for our special issue of *IQ* later in the year. Thank you to the readers who have already contacted us regarding case study submissions. If you have been involved in, or are involved in a project of potential interest to your colleagues in the industry, contact us today.

See you back here in May - which, don't forget, is Information Month.

Stephen Dando-Collins
Editor
IQ Magazine
PO Box 317
Potts Point NSW 1335 Australia
editor.iq@rmaa.com.au

'Dear
Editor…'

www.codafile.com

**Your 'one stop shop'
for a total records management solution...**

Serving the industry since 1976, Codafile Records Management is today recognised as a leading authority in providing records management, technology and storage solutions. Whether you are planning a move, upgrading existing premises, or want to improve productivity and save valuable floor space, Codafile's team of experienced consultants can help ensure you achieve your objectives.

If you are looking for ways to improve your organisation's records management process, call Codafile toll free today on: 1800 263 234 (Australia) or 0800 263 234 (New Zealand) or visit www.codafile.com.

Codafile™
INNOVATIVE RECORDS MANAGEMENT

■ RECORDS MANAGEMENT CONSULTING ■ FILETRAK SOFTWARE ■ CODAPRINT LABEL SOFTWARE
■ CABINETS ■ CODAFILE LATERAL FILES ■ CUSTOMISED FILES ■ FILING STORAGE PACKAGES

Internet Security Problems: The Worst is Yet to Come!

Experts within government and commerce are predicting that cyber attacks will soon become far more sophisticated, widespread, and damaging. Such predictions are ringing alarm bells at security agencies and in businesses that rely on the Internet.

Last October, PBS's Nightly Business Report in the US told of a WebNet survey by the University of California at Berkeley which showed that 30% of respondents has ceased making purchases online due to fears about their credit card details falling into the wrong hands. Another large proportion of respondents had cut back their online purchases.

The Internet has been hailed as the greatest thing for business since sliced bread. Some media commentators were predicting in the 1990s that online shopping would eventually destroy retail as we know it, with shopping centres becoming ghost towns as we all bought our every need online.

Those commentators failed to take into account the human need to touch, feel, and sample products ranging from fruit to a new car. They also failed to realise that where goes business there goes the criminal. And criminal minds are hard at work finding every loophole in Internet security, for profit, for pleasure, and for more destructive motives.

On November 29 last year, *PC World* reported that Scott Borg, Director of the US Cyber Consequences Unit, an agency within the Department of Homeland Security behemoth, told the Security Conference of the E-Government Institute in Washington DC that, while past cyber attacks had generally been the work of individuals, criminal organisations and terrorist groups would orchestrate devastating future attacks.

Borg told the conference that most existing viruses and worms knocked out computer networks for two or three days. Coordinated attacks by cyber teams using the Internet against the likes of the electrical grid or banking industry had the potential to have much wider, longer-lasting affects, he said. A core industry that was knocked off the net for more than three days would suffer hugely – "Gigantic numbers, really fast," said Borg, who is an economist by training.

At the same conference, Howard Schmidt, a former cybersecurity executive with eBay and Microsoft and one-time White House advisor, agreed that criminal hackers will be a major problem in coming years.

The views of Borg and Schmidt are backed by the latest Internet Security Threat Report released by Symantec, leading cybersecurity providers whose range of products include Norton ant-virus software.

Carried out in the first half of 2005 and drawn from 24,000 sensors in 180 countries, Symantec's latest Threat Report, published last December, concluded that attackers are moving away from broad-scale network attacks and toward more focused attacks on desktop computers.

'The new threat landscape,' says Symantec, 'will likely be dominated by emerging threats such as bot networks, customisable modular malicious code, and targeted attacks on Web applications and Web browsers.'

Using tens of thousands of remotely controlled infected computers, a 'botter' can shut down a targeted organisation's computers - or, as is thought to be increasingly the case, to extort large sums with the threat of such a shutdown.

Symantec observed a dramatic rise in bot attacks and DoS (Denial of Service) attacks in the first half of last year – bot attacks were double those of the previous six months. Malicious code attacks which threatened confidential information were also way up.

According to Symantec, Mozilla Web browsers including Firefox showed the highest vulnerability to attack, with 25 vendor-disclosed vulnerabilities during the survey period, compared to 13 for Microsoft's Internet Explorer, which was down from 31 in the previous period.

With two-thirds of the Global 2000 companies expected to adopt Voice over Internet Protocol (VoIP) as an alternative to analogue phone systems by the end of 2006, Symantec warns that Internet vulnerabilities will cause criminals and terrorists to increasingly target VoIP, for profit, and to create mayhem.

All enterprises, say Symantec, should be deploying anti-virus software, firewalls, and intrusion detection, and be actively monitoring their Internet environments around the clock against attack

Be warned. The crooks and the kooks are out there. They are targeting the Web. And your desktop is the new battleground in the war on crime, and the war on terror. IQ

How secure is your computer system?

For more on the Symantec Threat Report visit: www.symantec.com, and, www.securityresponse.symantec.com/avcenter/vinfodb.html

Email Heaven, and Email Hell!

With the proliferation of PDAs, it has never been easier to send and receive emails. That, to some executives today, is heaven. Problem is, many people have failed to realise that the emails that they or colleagues casually dash off become records that can later surface to embarrass them, or, worse, to incriminate them.

As Forrester's Robert Markham noted at the RMAA Convention in Perth last September, the big growth area in records management is email management. At the same Convention, PROV's Andrew Waugh pointed out that 40% of government e-documents in Australasia today are emails.

With mobile phones being email capable, and with PDAs spreading through corporate and government executive ranks like cane toads in the tropics, there is no escaping emails. Just as there is no escaping the repercussions when embarrassing or incriminating emails appear in the media or in the hands of lawyers in court.

Michael Brown, former head of the US Government's Federal Emergency Management Agency (FEMA) found that out the hard way last year following Cyclone Katrina, which was a disaster for Brown as well as for US Gulf Coast states.

Brown's emails via his BlackBerry to FEMA's Deputy Director of Public Affairs, Cindy Taylor, which were subsequently obtained by the press via FOI, portrayed a man more interested in his media image and where to find a sitter for his pet dog than in managing disaster relief.

Meanwhile, giving evidence in the One.Tel case in Sydney in November, former News Limited chief Lachlan Murdoch found that even with frequent memory lapses he could not avoid cold hard facts emerging via News Limited emails produced in court.

In a Florida, USA court case reported by Forbes magazine in October last year, accountancy firm KPMG was charged with improperly destroying electronic and hard copies of 800 emails relating to a tax shelter plan developed for clients. Surviving emails, described as smoking guns by prosecutors, recorded the document purge and its motivation – the prevention of future litigation.

In another KPMG email in the Florida case, one executive had casually informed 33 recipients that the firm had purposely given the Internal Revenue Service an incomplete list of tax shelter clients.

Another KPMG executive responded, by email, to question the wisdom of putting such 'sensitive' information in print.

As Forbes magazine writer Janet Novack remarked about the case, while KPMG's tax shelters weren't too bright, its internal emails on the shelters were dim-witted. And five of the eight KPMG executives indicted had legal degrees!

This leads to the inevitable question - how could apparently very smart people like Michael Brown and the KPMG executives be so dumb when it comes to emails? Didn't they realise their emails were going to become a record which could later be accessed by others? Obviously not.

There are some hard lessons for email users to learn. Just as HRH Prince Charles and several Australian politicians had to learn the hard way in times past that a mobile phone conversation is not a secure communication but is a broadcast into which eavesdroppers can tap, so email users have to learn that emails are neither private nor confidential.

The intimacy and ease of use of the email lull users into a false sense of security. It doesn't occur to many users that people other than the designated recipient may be able to read their message at some future time due to legal discovery, or FOI, or through a whistleblower or leaker.

To avoid, humiliation, defamation, and/or incrimination, the biggest favour you can do colleagues in your organisation is to remind them that their emails become records the moment they send them. And remind them that when they put their name to an email, they, and their organisation, become responsible for every word they've committed to screen.

It's advice that might prevent the heavenly attributes of email from becoming the stuff of hellish nightmares. iQ

The ubiquitous BlackBerry has made it possible to send and receive emails almost anywhere. It has also made it possible for individuals to create a record that will later surface to haunt them

A Shred of Evidence? Victorian Government Acts on Document Destruction

MELBOURNE: In an Australian first, Victorian Attorney-General Rob Hulls has introduced new legislation into Victorian state parliament designed to prevent the shredding of documents which may be of use in court.

As the Melbourne *Herald Sun* reported last November 11, the new legislation is a sequel to a 2002 civil case in which Supreme Court judge Geoffrey Eames awarded $700,000 compensation to the late Rolah McCabe after she sued British American Tobacco, blaming them for her lung cancer.

The Court of Appeal later overturned Judge Eames' decision, ruling that the destruction of documents by the defendant's law firm had not been unlawful as it occurred before legal proceedings were instituted.

The reforms follow recommendations tabled in 2004 by the Victorian Parliament's Law Reform Committee and a report by Crown Counsel Professor Peter Sallmann, 'Document Destruction and Civil Litigation in Victoria'.

In a media release on November 9, Victorian Attorney-General Rob Hulls said, "The intentional destruction of documents that may be used in court raises fundamental questions going to the heart of the integrity of our legal system."

The new legislation, introduced into state parliament by the Attorney-General in the third week of November, makes the intentional destruction of documents to prevent their use in cases already underway a new offence under the Crimes Act.

Under the new provisions, in addition to a jail term, individuals would be fined up to $62,886 and corporations as much as $314,430 if convicted of intentional document destruction.

In addition, the existence of direct instructions to destroy evidence will not be necessary to convict a corporation under the new provisions. It will only be necessary to prove that the culture of a corporation permitted the destruction of documents that are likely to be required in evidence, putting the onus on corporations to retain potentially incriminating documents.

"The new offence will not impact on normal document destruction processes," Attorney-General Hulls noted in his media statement. He added: "Corporations have an obligation to ensure document management policies are responsible."

The Attorney-General's media spokesperson, Liz Armitage, told *IQ* as we were was going to press in January that it is not possible to say when the new legislation will be debated in the Victorian Parliament or to forecast when it might come into law, as the parliamentary programme was "still being worked on."

Brambles Strips Down to Records and Pallets

SYDNEY: Brambles Industries, once a key player in the transport sector, is selling off all of its businesses other than the Recall document management operation and the CHEP pallets business, both of which are considered to offer the company its most profitable future.

The *Sydney Morning Herald* (November 29, 2005) reported that Brambles announced the divestment over the next 12 months of all its subsidiaries other than Recall and CHEP, as it unifies into one company listed on the Australian Stock Exchange, with a subsidiary listed on the London Stock Exchange.

*Australasian Transport New*s (November 29, 2005) said that the divestment will involve the sell-off of the Cleanaway business in Australia, Asia and the UK, as well as the sale of Brambles Industrial subsidiaries Interlake,

Eurotainer, and TCR.

In a statement to investors, Brambles CEO David Turner said that the company will concentrate on the two parts of the business with the highest expected ongoing growth prospects.

CHEP leads the world in its field, distributing over 265 million pallets and containers annually to 300,000 customers worldwide via 500 service centres in 42 countries. Brambles considers Recall a major player in document and information management - Recall operates from 200 locations in 42 countries.

But how serous is Brambles about retaining Recall, which has absolutely no fit with CHEP? News Limited news service News.Com reported on December 1 that this question was posed to CEO David Turner by AAP. Turner responded by refusing to rule out the possible sale of Recall. But, Turner told AAP, the medium term outlook for Recall was strong. "We are absolutely committed to make this business work," he said.

As reported in the November 2005 issue of *IQ*, last October Brambles announced the purchase of AUSDOC Information Management from ABN AMRO for $260 million.

This latest divestment move could mean that Brambles will focus even more heavily on document and information management, and may even sell CHEP if the right buyer comes along. Or, it will fatten up its Recall and AUSDOC document and information businesses with a view to a combined sale and a renewed, cashed-up transport focus.

Either way, the move signals a strong belief in the future growth prospects of RIM-related business.

Victoria's 2005 Hamer Awards Presented

MELBOURNE: The 2005 Sir Rupert Hamer Awards for excellence in government recordkeeping were presented in a ceremony at Queen's Hall, Parliament House, Melbourne, on December 14.

The awards, presented by Glenyys Romanes, MP at the December function, are conducted by the Public Record Office of Victoria (PROV) in association with the Public Records Advisory Council (PRAC), with sponsorship from the Victorian Branch of the RMAA.

The 2005 Inner Budget Agency winner was Victoria Online, Multimedia Victoria, for 'Victoria Online Thesaurus Development'. Winner of the Local Government Agency award was Yarra City Council, for 'City of Richmond – That Was Then,' a virtual exhibition.

A Special Award for Significant Innovation, as decided by the PRAC subcommittee, was presented to the PROV for its Digital Archive Project.

A Certificate of Commendation was presented to the Department of Human Services, Capital Management Branch, (Inner Budget Agency), for 'E-Information Management, F: Drive Review'.

Regional/Rural Agency Certificates of Commendation went to the Department of Primary Industries - Tatura, for 'Review and Improvement of Community Surface Water Management Systems', and to the Gannawarra Shire Council for 'Records Management Procedures and Strategy Development'.

Indigenous Recordkeeping & Archives Scholarship Renewed

MELBOURNE: The Caulfield School of Information Technology is again offering a scholarship for indigenous Australians and Torres Strait Islanders to undertake a masters degree or graduate diploma specialising in recordkeeping and archives.

Monash University's Professor **Sue Mckemmish**

The 2006 scholarship will cover the full cost of course fees for the Master of Information Management and Systems (MIMS) or the Graduate Diploma in Information Management and Systems (GDIMS).

The scholarship came as a result of the 1997 Bringing Them Home Report into the 'Stolen Generation' by the Australian Human Rights & Equal Opportunities Commission.

Bringing Them Home recommended that indigenous archivists be involved in archival projects that enable indigenous people to locate records, and also that scholarships be provided for indigenous archivists who wish to gain professional qualifications. In 2005, the scholarship was awarded to two recipients.

The 2006 scholarship is jointly sponsored by Monash University, the National Archives of Australia, and the Public Record Office of Victoria.

Professor Sue McKemmish of Monash University told *IQ* that she is hopeful that the scholarship will also receive the support of the RMAA and the ASA.

More information on the 2006 scholarship can be obtained from Ms Victoria Humphreys, Academic Programme Support Officer at Caulfield School of IT, at victoria. humphreys@infotech.monash.edu.au. Or, visit the Monash website: www.sims. monash.edu.au/events/shcolarships/indig-archives/index.html.

Defence & ATO Slammed for Poor Recordkeeping

CANBERRA: In his report for 2005, the Federal Auditor-General, Ian McPhee, has castigated Australian government departments for failures in business support systems and recordkeeping.

The Melbourne *Age* reported on December 30 that the Auditor-General found 18 breaches of the Constitution by various government departments in relation to expenditure activities.

But Mr McPhee reserved special criticism for the Australian Taxation Office (ATO) and Department of Defence (DoD). The ATO had errors totalling $7 billion in its 2004-05 financial statements, while the Auditor-General says he could not "validate" $4.43 billion in DoD recorded assets or $900 million in stated liabilities.

"Shortcomings are evident in a number of key operational and business

support systems and processes, in particular logistics and asset management, finance and personnel," the Auditor-General said of the DoD.

"In addition, recordkeeping practices need considerable improvement."

80-20 Launches Leaders4 GRC Solution

MELBOURNE: **Australian specialist governance, risk and compliance software house 80-20 has unveiled its latest offering, a new version of its Leaders Online GRC product.**

Leaders4 is the culmination of a multi-million dollar R&D investment and was partly funded through a $2.5 million Federal Government R&D grant.

Leaders4 includes new tools for board information management, risk management, compliance management, reporting, and Sarbanes-Oxley compliance – the company is growing its presence in the US market.

John DeGroot, Compliance Manager with Hydro Tasmania, is quoted in an 80-20 press release as saying that he has seen a preview of Leaders4. "The enhanced compliance frameworks and incident management capabilities will enable us to standardise government and compliance management processes around this solution," said DeGroot.

80-20 will ship Leaders4 with support for Windows Server 2003 R2, Microsoft's most productive platform to date for powering applications, networks and Web services.

Queensland Signs Up for Combined Whole of Government EDRMS

BRISBANE: **After a detailed review of EDRMS solutions, the Queensland Government, through CorpTech, its provider of corporate applications and related**

system support services, has opted for a system which combines software from Hummingbird, Red Dot, and Synercon.

Synercon Director **Conni Christensen** with the Executive Director of CorpTech, **Geoff Waite**

The solution tendered by LogicaCMG, the international IT services company, combines Hummingbird ECM software, content management software from subsidiary RedDot, and a.k.a. taxonomy management and records retention software from independent Sydney firm Synercon Management Consulting.

The whole of government approach is designed to standardise records management across all Queensland Government agencies and improve consistency of information management.

Synercon director Conni Christensen told *IQ* that the use of Synercon's Australian a.k.a. software will facilitate Queensland state government agency compliance with regulatory requirements for records management. The 3-year-old a.k.a product is used by the ABC, BP, and Westpac among other major Australian and New Zealand enterprises.

Synercon also launched a.k.a. on the North American market last year, via the ARMA Conference in Chicago.

Objective the Transparent Choice for NSW Regulator

ITSRR Chief Executive **Carolyn Walsh**

SYDNEY: **The New South Wales Independent Transport Safety and**

Reliability Regulator (ITSRR) has chosen Objective to supply an EDRMS to enhance its transparency and credibility as a regulator.

The ITSRR is a two-year-old statutory authority whose roles include administering rail safety regulations, advising the state government on the reliability of all public-funded transport within NSW, and to coordinate safety regulation with ferry operator NSW Maritime and the Ministry of Transport (buses).

Carolyn Walsh, Chief Executive of the ITSRR, told *IQ*: "ITSRR required a business tool that would instill confidence in its staff, the rail industry and the travelling public by assuring them of information integrity and credibility. As a regulator, credibility is paramount. It is essential for ITSRR to operate in a transparent and accountable manner."

In addition, the final report of the Special Commission into the 2002 Waterfall rail disaster had recommended that the ITSRR establish an electronic document control system to enable the monitoring of safety issues relating to the state's rail system.

The Objective EDRMS will allow ITSRR field officers who work remotely around NSW to rapidly access documents such as accident investigation reports, policy documents, and details of operator safety management systems from a central repository, using handheld devices.

ITSRR will also use the system to review and approve policy documents, to process travel approvals, to action correspondence and reconciliations, and to manage audits, inspections and investigations.

The ITSRR contract comes at a time when Objective has been ranked in the Deloitte Technology Fast 50 list for the fourth time in 5 years after achieving 122% revenue growth over the past 3 years.

Southland To Get New Library & Archives

INVERCARGILL: **City administrators have borrowed NZ$1.8 million to purchase and adapt a city centre building for a new combined provincial library and archive for public and community records.**

Invercargill's daily newspaper, the

Southland Times, reported on November 26, 2005: "Bureaucracy rather impelled progress on the matter in response to the Public Records Act which requires local government to more appropriately archive its own records. It made sense to combine the facility to house corporate and community records."

The new building will be refurbished and opened to the public in 2007. The city will employ a full-time archivist and develop an acquisitions policy, the newspaper said.

The city's Information Services manager Marianne Foster told the *Southland Times* that the existing library contained, "a lot of donated material which, because we haven't had the time to actually go through it individually, we probably don't even know the worth of some of it".

RMAA Accredits Open Polytechnic

WELLINGTON: The RMAA has awarded its first education and training accreditation in New Zealand to the Open Polytechnic, a distance learning and campus tertiary education establishment based in Lower Hutt.

The accreditation was confirmed by the

Open Polytechnic's
Lois Robertson

RMAA National Board in December and applies to the institution's Level 6 Diploma in Records and Information Management (DipRIM), over the next 5 years.

The Polytechnic's DipRIM Programme Leader, Lois Robertson, told *IQ*, "We see it as a very good thing, a really positive step building stronger links with the records community."

RMAA NZ Branch President, Douglas Wilson, ARMA, currently studying for the Polytechnic DipRIM, commented: "I'm very pleased to see a New Zealand education supplier receive this accolade. I've seen for myself the value of the diploma course. It's a first for the country and a great step forward for

the NZ Branch."

RMAA CEO Kate Walker, MRMA, described the award as "an excellent addition to the growing collection of accredited courses of the RMAA". She added, "This announcement is not only exemplary of Open Polytechnic's dedication to providing consumers access to quality information, but it is also a testament to the teamwork among the RMAA."

Open Polytechnic has been marketing its RIM courses aggressively and successfully. A month before gaining RMAA endorsement, the institution's School of Information and Social Sciences appointed a new lecturer, Kay Sanderson, for its Information and Library Studies, headhunting her from Archives N.Z. where she had lead the NRAM (National Register of Archives and Manuscripts) project.

For more information: www. openpolytechnic.ac.nz

PRA Health Records Privacy Fears Scotched by Archives Chief

WELLINGTON: Surprise comments by New Zealand's Privacy Commissioner regarding the new Public Records Act (PRA) brought a swift defence from the head of the PRA's sponsoring agency, Archives New Zealand.

On National Radio's breakfast programme on October 28, Privacy

Archives New Zealand's Chief Archivist **Dianne Macaskill**

Commissioner, Marie Schroff alleged that as a result of the April, 2005 Act, "uncertainty" surrounded the future management of New Zealanders' personal health records held by local health authorities.

She went on, "The risk of access by other people, other than the individuals' representatives, certainly has the capacity

to undermine peoples' willingness to seek medical or legal help. So, I do have a concern about the possibility of access to such information once the material has been transferred to Archives."

In a media release later the same day, Chief Archivist Dianne Macaskill countered,"Personal health information will not be publicly available. This is protected by both the Privacy Act and the Health Information Privacy Code. The Public Records Act does not override them.

"Under the Act, records created 25-plus years ago are required to be either transferred to Archives New Zealand or destroyed if they are no longer required for business purposes. We are currently working with (district health boards) to identify which classes of records are of long-term value and should be transferred and archived. We will not require any records to be transferred until this has been resolved."

100,000 Records Released for Katrina Inquiry

NEW ORLEANS: The Governor of Louisiana, Kathleen Blanco, has released more than 100,000 documents relating to the government response to Hurricane Katrina last August.

According to Associated Press, (December 5, 2005), the documents joined a smaller records release from Mississippi and some 1,000 emails from the Federal Emergency Management Agency (FEMA) in providing a House of Representatives committee looking into the hurricane response with a detailed insight into how and why the government response was so lacking.

House committee spokesman Robert White told AP that the emails in particular pointed to major problems if coordination and communication. Even when the problems and requirements were effectively communicated, FEMA lacked the ability to adequately respond to the demands of the disaster.

The Louisiana documents record delays in federal response, and, sometimes, a complete lack of response. AP says they reflected partisan battles between Governor Blanco, a Democrat, and the Republican White House of George W Bush - which was subsequently

accused of lethargy over the disaster relief effort.

Disasters Boost Demand for Medical Records Backup

KANSAS CITY: The loss of tens of thousands of medical records to Hurricane Katrina in the Gulf Coast states and severe flooding in New England has caused a boom for US companies in the offsite storage business.

Thomas Handler, Research Director with technology consultant Gartner Inc told the *Columbia Daily Tribune* (November 13, 2005) that the 2005 hurricanes have forced healthcare groups to catch up with other industries that protect their records.

Alpha Systems, a Pennsylvania company that provides records backup for the medical and legal sectors, told the *Tribune* that it was expanding capacity to meet demand following the hurricanes and in the wake of severe flooding of hospitals in New England.

Commenting about most hospitals, Brett Griffith, President of Alpha Systems, told the *Tribune*: "They'll typically use their basements for storage because it's cheap, and that's the first part that floods."

The *Tribune* reported that, in New Orleans, unlike most other civil medical patients, 3,500 HIV-positive patients had their records preserved because they had been backed up electronically on servers in the nearby city of Baton Rouge.

In Kansas City, national medical records backup specialist Cerner Corp was planning to build a second data center to meet what it expected would be a huge jump in demand for medical records backup.

Vietnam War Trigger Cast Into Doubt by Top Secret Document FOI Release

WASHINGTON DC: The National Security Agency (NSA), **the largest US intelligence agency, has released 140 formerly top secret documents which cast doubt on the so-called Gulf of Tonkin Incident, a trigger for US military involvement in Vietnam in the 1960s.**

The documents, released on December 1 last, include reports, histories, chronologies, signals intelligence (SIGINT), and records of interview relating to the August 2-4, 1964 incident. According to the Baltimore *Sun* (December 2, 2005), the records prove that the rationale for the Vietnam War was faked.

The records show that on August 2, 1964, the destroyer USS *Maddox* was attacked by North Vietnamese torpedo boats in the Gulf of Tonkin.

The administration of Lyndon B Johnson was to claim that the North Vietnamese launched another attack on US ships in the Gulf of Tonkin two days later.

Johnson and Secretary of Defence Robert MacNamara used this as the excuse for subsequent US air strikes against North Vietnam and a request to Congress for a resolution which gave the White House freedom of action in Vietnam. The escalation took American, Australian and New Zealand troops to war in Vietnam.

The *Sun* reports that the released records show that the second attack never took place. At best, the North Vietnamese were attempting to recover vessels damaged in the first attack, but US signals intelligence wrongly labelled their actions as another attack.

In an eerie echo of misinterpreted 'WMD' intelligence that took the US and Australia to war in Iraq in more recent times, the 1964 Johnson White House interpreted the SIGINT as showing a second attack, and pressed the military response button. The rest, as they say, is history.

The NSA had for years been resisting the release of the Gulf of Tonkin records. The release was ultimately made possible by determined FOI requester Matthew M Aid, whose campaign for the declassification of the Gulf of Tonkin records was backed by the *New York Times*.

For more on this story, visit the George Washington University National Security Archive, at www.gwu.edu/-nsarchiv.

Microsoft Offers Free Security and Tune-up Package

SEATTLE: Microsoft has launched its OneCare online security and tune-up package with a free test version.

OneCare is Microsoft's attempt to muscle in on the Internet software services market dominated by Google and Yahoo and the online security market where the likes of Symantec Corp currently have a stranglehold.

The *Washington Post* reported last November 30 that the OneCare test version, offered free at http://ideas.live.com, was designed to automatically update itself online to deal with the latest security threats and also perform other PC tune-ups to keep computers running smoothly.

OneCare will form part of Windows. Live, an upcoming suite of online products with an as yet undisclosed price tag which Microsoft hopes will keep Windows customers loyal to MS products.

Secure PDFs Now 'Guaranteed' in Europe

LONDON: Document security specialist GeoTrust has launched new software in Europe which they claim guarantees PDF documents have come from a verified sender and have not been tampered with.

The GeoTrust software integrates with Adobe's LiveCycle Document Security server, and is designed to allow PDF documents to distributed securely.

TechWorld (29 November 2005), reports that recipients can view the documents on any Adobe Acrobat reader.

Using True Credentials, the high-end version of the system, large volumes of PDFs can be created, sent and verified without human intervention.

A special accelerator card placed in a server increases throughput by thousands of documents per second. A low-volume version, My Credential, uses USB tokens which plug into the PC on which the PDFs are created.

Records Reveal Soviet Nuclear Attack Plan

WARSAW: **The Polish Government has released 1,700 Warsaw Pact documents from its military archives, revealing Soviet plans for nuclear counter-attacks in the event of a NATO first strike against Soviet territory.**

The London *Guardian* reported (November 25, 2005), that the records released on November 24 included details of a 1979 Warsaw Pact plan entitled 'Seven Days to the River Rhine' which detailed a Soviet response to a NATO nuclear strike.

The plan called for nuclear counter-strikes against targets in West Germany, the Netherlands, Belgium and Denmark, followed by a land force drive west to reach the Rhine within a week of the NATO attack.

Other papers in the release included the Soviet operational plans for the 1968 invasion of Czechoslovakia, and details of the Soviet massacre of Polish strikers at Szczecin (Stettin) in 1970.

Indian Stock Exchange Automates Web Publishing

MUMBAI: **The National Stock Exchange of India (NSE), leading Indian stock exchange and 3rd largest stock exchange in the world, has acquired Interwoven's web content management (WCM) software to manage its Web publishing.**

Established in 1994, the NSE operates a fully automated screen-based trading system and is required to publish key investor information on its Web site at the end of each trading day. Previously, the NSE Web team had updated information manually, struggling with an escalating volume of content as well as versioning and workflow issues.

After evaluating a number of systems, NSE chose the Interwoven WCM solution, influenced by the fact that it is widely used in the financial services market worldwide. The solution will enable NSE to automatically update investor information. Relevant business users across the organisation will also be able to directly contribute Web content, without the need of assistance from IT.

In a joint press release with Interwoven, NSE say they also plan future rollouts such as multi-lingual sites using their new WCM system.

Thai Hospital Injects Aussie Solution into System

BANGKOK: **Siriraj Hospital, Thailand's largest and oldest hospital, is to install an administrative, clinical and electronic records solution developed by Australian company IBA Health Limited.**

Siriraj Hospital services 80,000 inpatients and 1.6 million outpatients each year, and is part of the University of Mahidol's Faculty of Medicine.

The IBA Health solution will not only support in-house administration at the hospital but will enable the coordination of healthcare records throughout the region. The $6.6 million IBA Health contract, announced December 5, will involve a 2-year rollout and will be supported by a maintenance contract worth $1 million annually.

IBA Health has its administration and billing software in 420 hospitals worldwide. For more information, see: www.ibatech.com/Main.asp.

Fiji Government Launches RIM Initiatives

SUVA: **The Fiji Government is launching a number of RIM initiatives in 2006, including a new National Archives building and website, and new records legislation**.

Speaking in the 2006 Budget debate on November 15, Minister for Information, Communication and Media Relations, Marieta Rigamoto, told parliament that the Government would build a new 3-level National Archives building worth Fiji$3.8 million, on a site adjacent to the current National Archives in Suva.

A Website was being developed by the National Archives, and records would progressively be digitised. A revised Fiji Public Records Act was soon expected to become law, and the Government was looking at the "eventual introduction" of a Freedom of Information bill.

The Minister said the FOI legislation "will probably revolutionise recordkeeping and records management in government departments " in Fiji. IQ

RIM's
Knight in Shining Armour
Talks Digital

CHRIS HURLEY has been at the forefront of archives and recordkeeping change in a career extending over several decades in both Australia and New Zealand. Here, he shares his thoughts with *IQ* about the challenges facing RIM professionals in the digital age.

IQ: Chris, what, in a nutshell, is recordkeeping?

CH: What makes it different from other arms of RIM is the link between documentation and action. A record doesn't just carry data. Like all information, the content of a record means something.

A record is special because its meaning comes, in part at least, from the connection the record has with an event or circumstance. Keeping records is about establishing, maintaining, and interpreting that connection.

IQ: You have worked at the highest levels of records management/archiving in the public sector in Australia and New Zealand, and now operate in the private sector. Do records and information management practitioners in the public and private sectors have to possess different mindsets?

CH: When I moved across, I thought so. Now, I find that the work is fairly similar. The drivers are different, there are different

business objectives, our message has to be tailored differently, and our employers respond to different stimuli and have different priorities. But what we do and why is just the same.

IQ: A US study being published in the next issue of *IQ* found that records managers and archivists responded so similarly that the study's authors say they can be categorised together, as opposed to other RIM practitioners. In your experience, do records managers and archivists share similar qualities?

CH: Many do. And I've said for a long time that they are one and the same. I have belonged to both ASA and RMAA for over 25 years. In that broad community, there are still some who aren't comfortable in moving between the two. I am comfortable, and I know that there are a lot who now think and act the same.

IQ: That same US study found that records managers and archivists in North America are more emotionally stable than academic reference librarians and catalacatalogers, are more optimistic, are less tough minded and are more into teamwork. Does this surprise you?

CH: I don't know much about academic libraries, so I can't comment on their neuroses. I'm not sure that being emotionally stable and optimistic during the lingering crisis precipitated in all these professions by computerisation is necessarily a good thing.

It might mean we are becalmed in a backwater while the librarians are engaging in a healthy struggle with reality at the expense of their sanity. I hope not.

IQ: Are the individuals responsible for new information and knowledge management projects responding adequately to recordkeeping needs in the digital environment?

CH: That's difficult to answer, because I don't know anyone who is knowledgeable across the whole sector. My impression - it's only that - is

IQ: Does Internet blogging represent a new, additional avenue for records management? Or will it simply multiply the amount of useless information that RIMs will have to one day sift though to establish legitimate records worthy of retention?

CH: Most information isn't worth keeping – even for a short while. In New Zealand, the motto of the National Archives was 'preserving the nation's memory'. I thought this odd because in practice their role is destroying the nation's memory. Like everyone else they destroy more than they keep. Their role is to preserve what's left of the nation's memory.

It's already too late if you have to sift through useless information to find what's worth keeping. The right approach is to analyse work and specify documentation requirements as part of the rules governing business processes.

"What memory of this business process do I want?" and, "What memory do I keep?" should be one question not two. The question "How long?" is supplementary. This isn't happening. Perhaps it's time to become emotionally unstable.

IQ: How vital is risk analysis to records protection and security?

> ‘ **Successful EDRM is about what IT doesn't do or know how to do** ’

that recordkeeping needs in the digital environment are still hardly being met at all. There's been some magnificent work done both theoretically and practically, but it isn't taking across the board.

A good deal of success has been achieved with policies, procedures, and standards. Design work has led to some effective products, but take-up is patchy, and implementation is where it falls down most of the time. Some people will even tell you that most EDRM projects fail.

IQ: Some RIMs complain that their IT departments don't understand records management, don't want to understand it, and make unilateral decisions which impact adversely on the RIM's role and their organisation's ability to meet future RM and compliance needs. Has the IT Department become the enemy of the RIM?

CH: I think this is the commonly held perception in the world of EDRM, and it is often the case. IT has different assumptions, different objectives, and different methods. Moreover, successful EDRM is about what IT doesn't do or know how to do: implementation and maintenance.

IT designs tools around defined business processes. EDRM uses tools to manage changing and variable business processes. Probably the biggest single disappointment of the last fifteen years has been the failure to develop business analysis beyond widget-making and to apply that technique to ordinary everyday work.

CH: Risk analysis lies at the bottom of everything we do. What to make, what to keep, for how long, how to maintain it, how to protect it, what access controls to run - the whole catastrophe.

IQ: With the growing convergence of RM with business systems, is it necessary for organisations to formulate entirely new documentation strategies?

CH: Documentation strategies are in short supply in both the public and private sectors. There are fragments, but very few that look across an entire organisation. Those fragments derive from an enormous variety of assumptions and objectives that are far from uniform. Just asking to see a documentation strategy will produce wildly different results in different organisations.

The most comprehensive - in terms of coverage - are probably the archives statutes. These are still so retarded as to be almost dysfunctional for that purpose. I can say that because I designed three of them.

They are still locked into the 'cabbage-patch syndrome' - records are discovered every morning under cabbage leaves formed by business in ways we know not of.

Yes, documentation strategies are needed, but they won't often be new - in the sense of an advance on something else - because most of them will have to be developed for the first time.

IQ: Do stand-alone RM applications have a future?

CH: No. They're already dead, or soon will be. Most of the majors are already integrating with other functionality. RM functionality needs to be relaunched inside desktop applications. Interestingly, things like workflow are being looked at by standard desktop applications, such as Microsoft. Ultimately, RM functionality has to be desktop too.

The question to ask of any EDRM implementation is this: exactly what functionality do we get for our money, what additional things can we do in this application, that is additional to what we have in the desktop? The difference between the two lists and the money you are investing is the basis for the ROI. When the difference is nil, we'll know we are where we need to be.

IQ: In your experience, do company boards and senior government administrators understand the importance of recordkeeping in their organisations?

CH: Some do, many don't. The fact is that we don't project a clear-cut, coherent, enduring image to anyone – including senior managers in both the public and private sectors. We send out mixed messages.

They don't understand the importance of recordkeeping because they don't understand what recordkeeping is. Not surprising, we can't agree about that even amongst ourselves.

There is an understanding of the importance of some of the things recordkeeping can do. But we are not seen as solution-providers in that space. They don't necessarily think of us as the solution.

If they have a legal problem, they think of lawyers. If they have a problem around evidence, reliable documentation, authenticity, memory, whatever it is we offer, they don't necessarily think: 'recordkeeper'.

IQ: Have you found that, with the digital revolution, records managers are increasingly expected to become involved in areas which are not reflective of the traditional RM skill-set, and for which their existing training and experience doesn't fully equip them?

CH: The days of a registry in which documents went in one door and came out another as files are - of course - long gone. Technology, the disappearance of middle management - whose job was to enforce process rules - the ubiquity of desk-top users, and the continued disconnect between RIM and IT pose problems that still have to be overcome.

As David Bearman told us many years ago, our methods must change, but what we are trying to do remains the same. RM can only be a contributing factor in business-focused solutions for documenting activity and maintaining evidence. But its intellectual integrity remains unchanged. It is not yet clear how this "traditional" skill-set will be learned or deployed within IM teams.

IQ: Will recordkeeping as we know it survive into the future without substantial re-skilling?

CH: The fundamentals will stay the same. It is a skill, however, not necessarily a role. People who learned those skills in the paper world are retiring and their robust re-engineering into the digital world is still incomplete. The skills might even

be lost for a while, but they will be rediscovered. We are recordkeeping mammals. Fire-making probably didn't just arise once and only in one place.

IQ: Should tertiary institutions be introducing a whole new era of records and information management studies?

CH: Tertiary education is in a fragile state and I think survival for them means responding to various agendas – not necessarily a reform agenda for the re-establishment of recordkeeping in cyberspace. I hope, whatever happens, there will continue to be opportunities to study and research recordkeeping in the tertiary institutions.

IQ: There have been calls, from the likes of Sue Myburgh of Adelaide University, for all RIM professionals to pull down the barriers that divide the different information and knowledge management sectors, to create a single metacommunity. What are your thoughts on that?

CH: While I think the barriers between records management and archives should be pulled down, I'm not so sure about other barriers. We are part of the world of IM and KM, the same way Maori are part of New Zealand.

But integration is not necessarily a good thing - for Maori or for recordkeepers - if it swamps your identity. Again, this is about barriers between skills, roles, and responsibilities – not jobs.

> "**The dust hasn't yet settled on what it means to be a recordkeeper in cyberspace**"

IQ: Has the industry, and the professional associations within it, clearly articulated the roles and responsibilities of recordkeepers?

CH: Not as clearly, or as extensively, as I would like. The fact that things aren't as I would wish is no great problem. What concerns me is that this is not high on the professional radar. Such an articulation has to be a collective thing. If the result of collaborative reflection isn't what I agree with, so be it. But I don't think it's being given enough attention.

IQ: Does the industry have good checks and balances?

CH: No, hardly any. Checks and balances for what? You need to have articulated roles and responsibilities before you can even start to answer that question.

We have standards and codes of ethics which, in my view, don't provide bench-marks against which our own behavior can be measured, no monitoring to speak of, and no enforcement mechanisms even if there were.

IQ: Just how accountable should a recordkeeper be?

CH: Accountability means many things. I am currently concerned with is our own professional accountability - the checks and balances extended over individual and institutional

behavior to satisfy the community that pre-determined standards of professional best practice are being monitored.

IQ: You have been having a stoush with the Australian Society of Archivists lately, in relation to the 'Heiner Affair'. Briefly, what's the difference of opinion all about?

CH: The Heiner Affair has a long and complicated history. In 2004, I was invited to speak at the ASA Conference. Nothing I said was very new. I used Heiner to illustrate what I've just said – in that context, archivists aren't accountable because they have no benchmarks against which to measure their behavior.

What was new was a critique of a submission on Heiner the ASA Council had made earlier in the year to a Senate Committee. ASA said my paper was defamatory and are refusing to publish it in the Conference Proceedings.

Material which is prima facie defamatory is published all the time; the question is whether an action is likely to succeed. The opinion on which they relied declined to take a view on whether an action would be likely to succeed.

I obtained an opinion from a QC who examined the materials and said that he could not imagine how the available defences against an action for defamation would not prevail. I then published the paper on Mike Steemson's website: www.caldeson.com/RIMOS/archivists01.html.

As of today (December 16, 2005), they are still considering their position in consultation with a third set of lawyers.

IQ: Should there be legislation in Australia and New Zealand that frees government archivists and records managers from penalty if they refuse to obey government instructions to destroy particular documents when they believe those instructions to be unethical?

CH: There has been such legislation for some time, in Tasmania. I've rather lost touch, but I had the impression that similar provisions were included in at least one other jurisdiction. Theoretically, no statutory power should be subject to government direction, but, in the absence of something explicit, that principle of administrative law can be a shaky ground on which to take a stand.

IQ: Is there any other RIM-related legislation that you would like to see introduced?

CH: There are two kinds of RIM-related legislation, just like there are two kinds of statute. Most legislation, even if it has limited ambit, applies to all the world. Companies law, privacy law, the law of evidence, and the Crimes Acts, for example, are all RIM-related in the sense that they contain important and relevant provisions.

But they are different from archives laws which apply only to government agencies. With the possible exception of public access provisions which I've been doing my best to have written out of them, archives laws are, for all practical purposes, housekeeping rules for the internal operations of government – like public sector legislation and financial regulations.

Governments promulgate housekeeping rules in legislation because that's all they know how to do. Archives laws are like the internal decisions of the board or directives of the CEO within a company.

In the wake of Enron and the like we've seen more of compliance benchmarks with teeth imported from overseas - like SOX and BASEL II. I'd like to see more homegrown corporate regulation like that, not necessarily only legislation, not just imported from overseas, via our need to trade internationally.

In a word, more of the same kind of benchmarking accountability that we, as a profession, lack.

IQ: What advice would you give someone just starting out in recordkeeping today?

CH: Be prepared for an uncertain future. The dust hasn't yet settled on what it means to be a recordkeeper in cyberspace. Understand the basics and hold to them and be ready to embrace new methodologies and functions as part of a team. Keep looking for systems and methods that integrate recordkeeping with business processes, and put your money on those.

IQ: Where to next for Chris Hurley? Are there more metaphorical mountains you want to climb, more battles to fight?

CH: Very few mountains left, and, I hope, no more battles. The future is never certain. I had thought my position at Archives New Zealand was my pre-retirement job, but it turned out otherwise.

Here at the Commonwealth Bank we are doing some interesting things and, so long as that lasts, it will probably keep me busy until it becomes time for me to retire. After that, I hope to go on working in my own time and at my own pace and take up indexing part-time.

IQ: Thank you, Chris. IQ

GUFF ON THE GURU

Chris Hurley, ARMA has been the Information and Archives Specialist, Document and Content Management, with the Commonwealth Bank of Australia, in Sydney, since 2003. Previously, he worked with the Australian Archives, was Keeper of Public Records at the Public Record Office of Victoria, and was with Archives New Zealand, serving as New Zealand's Acting Chief Archivist for two years.

Chris has post-graduate diplomas in education from the University of Sydney, librarianship (University of New South Wales), and archives studies (University of London).

He has spoken and written extensively throughout Australasia on recordkeeping issues. His essay 'Recordkeeping, Document Destruction, and the Law,' won the Archives and Records Association of New Zealand (ARANZ) Michael Standish Prize in 2003.

An outspoken champion of recordkeepers and an advocate for recordkeeping standards and legislation, he has been involved in the drafting and review of archives legislation federally, and in NSW, Queensland, and New Zealand.

Chris would like to point out that the views he expresses in this interview are his own and do not necessarily represent those of his employer.

Why Things Are Look

Not that long ago, Interwoven was seen as a specialist software supplier to the legal sector. But as the company's new MD for Australia/New Zealand, CHRIS LYNCH, tells *IQ*, Interwoven is rapidly becoming a major player in government and corporate circles, with new products and fresh ideas.

Interwoven Managing Director **Chris Lynch**

IQ: Chris, You joined Interwoven last October, having previously been MD of Hummingbird in Australia. Did this involve a culture change?

CL: Interwoven is a very talented and focused organisation. The senior Management team are very "hands on". Which has made the transition much easier.

IQ: 2005 seemed to be a big year for Interwoven in the Asia Pacific region.

CL: Yes, we have had a fabulous year. James Murray, the VP for APAC, moved down to Singapore from the U.K early in the year. Under his direction we posted record revenue results right across the region.

We're now focusing on Enterprise Content Management solutions rather than single point solutions. Our customers are now seeing Interwoven as a strategic partner that can cater to all their ECM needs. Of course we primarily sell now on point solutions, but users want the box ticked on ECM

IQ: How long has Interwoven been in the Australia/New Zealand marketplace? And how would you characterise the company's presence here?

CL: We have now been operating in Australian for 5 years. As far as our reputation is concerned, Interwoven is seen as a company that truly delivers best of breed technologies. We often say, "We measure our success by our customer's success". We are constantly getting fabulous feedback from our customers on how they use our technology.

As far as our solutions are concerned we have a leader's reputation in Web content across all industries, and in document management we are seen as a leader in professional services and a new up and coming player in government and banking and finance. Our latest records management product integrated with WorkSite is being received with a great degree of excitement.

IQ: Who would you rate as your key competitors?

CL: We have two sets of competitors. In regards to DM/RM, it's Documentum, Objective and Hummingbird. On the Web

king Up at Interwoven

content side, its Documentum and Vignette.

CL: WorkSite has been a very successful product in the professional services, legal, accounting and government sectors. It is a mature and robust offering that is very quick to deploy and easy to adopt, which provides our customers with rapid return on their investment.

Team site has also been very well accepted. It has a very strong following in government, in 18 government departments and 7 Universities. And in the commercial sector, where we will continue to expand our global dominance in banking and finance.

IQ: In the US, readers of Law Office Computing magazine recently voted WorkSite the top document management solution in the legal sector. Do you have a strong emphasis on the legal market here?

related content.

Scrittura provides customers to automate yet another high value content-centric process in the OTC derivatives space.

IQ: In 2005, DFAT in Canberra launched a 2,500-seat WorkSite rollout. Did that contract mark a breakthrough for Interwoven in terms of Australian federal government departments?

CL: In many ways yes, it was the first large government department to reject "traditional" DM systems and move to a more commercial solution, based on recommendations from our local users in banking and legal. It has been a great success, and they are now evaluating our records management solution.

IQ: What does WorkSite do that other solutions don't?

CL: WorkSite ranks high in ease of deployment, integration with the Microsoft stack, performance and scalability. It's not necessarily "what we do" but "how we do it" that makes the difference.

Many EDRMS projects fail because the systems are too complex to deploy or too hard for users to adopt. WorkSite has

> **'Many EDRMS projects fail because the systems are too complex to deploy or too hard for users to adopt '**

CL: Talking awards, we also won the eLoties award in Britain for the best email management product.

We do dominate the legal market internationally. Seven of the top 10 law firms worldwide and 14 of the top 20 law firms in Australia are WorkSite customers. Many of these have switched from competitive systems. Interwoven has enabled law firms to move to a truly electronic file, which drives greater productivity and compliance.

IQ: Last August, Interwoven announced the acquisition of Scrittura, a financial services solution provider with an emphasis on over-the-counter derivatives trading. Does this mean there will now be an Interwoven focus on the financial industry here?

CL: Financial services along with legal and professional services and government are key vertical markets for Interwoven. Some of the biggest brands in the financial services space use Interwoven software for managing Web-content, and business

cracked the code along both these dimensions.

Unique however is the concept of "Matter or Deal Centricity" where all matters are kept together in spaces pertaining to work tasks or projects. All documents including email are found within these matters.

IQ: Interwoven's ECM solutions now integrate with Microsoft's SharePoint Portal Server. What does this mean for records and information managers?

CL: Worksite augments Sharepoint by delivering high-end ECM capabilities through the Sharepoint interface. Organisations can have the rich data aggregation capabilities of Sharepoint Portal server and yet still have a single point of control for all corporate documents and emails. We believe we have the best integration of all ECM players.

IQ: Last year, Interwoven got into bed with Sun Microsystems, who now package Interwoven's enterprise content management software with Sun's system software, servers, and storage.

WHY THINGS ARE LOOKING UP AT INTERWOVEN: Continued from page 21

Does this indicate a shift in industry dynamics, with content requirements now driving storage decisions, rather than the other way around?

CL: We feel privileged that Sun has made Interwoven its ECM partner of choice. Enterprises worldwide are very focused on driving new levels of productivity and compliance through investments in content-centric applications. Applications drive infrastructure purchases, whether it is software platforms like databases or hardware platforms like servers and storage.

IQ: Email management is now driving many RIM solution investment decisions. What does Interwoven have to offer RIMs looking for email solutions that provide archiving, records management, and search capabilities that address compliance and discovery requirements?

> **'Getting end users to adopt without loss of productivity is a critical element of enforcing a sustainable compliance policy'**

CL: Interwoven is widely used to manage email content. It is probably the primary reason many of our customers buy WorkSite today. Some of the unique capabilities we provide include a consistent way of filing and accessing documents as well as emails.

We enable users to classify and file large volumes of emails efficiently. We provide tight integration with Outlook, Notes and Groupwise. We provide a powerful search capacity, of emails and even attachments.

You get single instance storage of email, and the ability to automatically declare email as records and apply retention schedules. Our architecture is capable of scaling up to very large volumes of email content. And you can get offline access to email filed into the records system.

IQ: How does Interwoven's new RM 5.0 records management solution address retention policy?

CL: IRM 5.0 allows records managers to set up retention policy based on time, events or a combination of the two. These retention polices are applied to all content across media types including paper and electronic content.

A retention policy consists of one or more lifecycle milestones. For example, a retention policy could include a milestone to archive the content two years after the last activity, and another milestone to destroy the content five years later.

These retention polices can be applied to any level in the file plan independent of media type.

IQ: How much control can a records manager exercise over enterprise compliance policies using Interwoven's RM 5.0?

CL: Records managers can use IRM 5.0 to define the enterprise file plan and to enforce proper retention policies across media types. Most importantly, through its integration with WorkSite, IRM 5.0 enables records managers make the capture of electronic content transparent and seamless for the end user. That's a key challenge for traditional records solutions.

Getting end-users to adopt without loss of productivity is a critical element of enforcing a sustainable compliance policy.

IQ: In the last issue of *IQ* we discussed the growing problem of loss of government reports on the Web. Do you see the latest WCM software offering solutions to those problems?

CL: By definition, a good DM system such as WorkSite and the new RM product combined with a good publishing WCM solution like TeamSite is going to manage this problem.

A WCM system on its own without DM and RM is not the solution. The real solution is a true ECM system such as ours that looks after a document from life till death. Including, of course, its forays onto the Web.

IQ: Where do you see Interwoven's future in Australia and New Zealand?

CL: We are excited about our future here. And we should be - our customers tell us we are providing what they want! Sure, it's nice to be supported by analysts, and by the press as well. But we listen to our customers, and they tell us we are doing it right.

As we move from the legal market to finance and banking, government and corporate, we hear the same thing. We are providing what users want. Probably, short term, the release of our new records management product is going to have the biggest immediate impact.

IQ: Thank you, Chris. Every success in your new role. ⬛

A Record of Growth

New Interwoven A/NZ MD **Chris Lynch** brings a wealth of experience to the position including more than a decade spent in executive sales, channel, and operational management roles with companies including Hummingbird, Norada, and Software Spectrum.

Prior to joining Interwoven, he ran Hummingbird's Australia/New Zealand operations for over five years, starting his career at the company as the national sales manager. While at Hummingbird, Lynch was instrumental in growing the business by 25 percent year-over-year across key vertical markets including manufacturing, government, enterprise, and legal. Lynch expanded Hummingbird's sales team and partner channel, resulting in strong market presence, particularly in the utilities and financial services markets.

Interwoven has an expanding presence in Australia/ New Zealand. Its several hundred customers include the NSW RTA, NSW Health, Macquarie Bank, Qantas, leading Australian law firm Clayton Utz, and Blake Dawson Waldron, an international law firm with offices in Australia, England, and China.

EDRMS: The Good, the Bad, the Ugly

By Stephen Macintosh

After a decade as a manager and consultant involved with EDRMS implementations in State, Federal and international public sector organisations, STEPHEN MACINTOSH discusses what recordkeepers can bring to a EDRMS project, outlines his experiences in EDRMS teams, and reveals some of the pitfalls of a badly implemented EDRMS.

Identifying evidence of business activities that are conducted electronically, then capturing and managing that evidence, is the central challenge of all modern recordkeepers.

An environment where the majority of business is being conducted using electronic media requires a robust Electronic Document and Records Management System (EDRMS), which is fully integrated into an organisation's business processes.

The Good

I suppose the good news with regard to recordkeepers and any EDRMS project is that they have a lot of extremely valuable perspectives, methodologies, and tools to bring to any information management working group.

Firstly, they bring what Australasian RIM guru Chris Hurley describes, in a paper he gave at the 2004 RMAA conference as, 'The knowledge that records aren't exactly the same as other kinds of information - they exist in an information environment but they have unique characteristics as well.' My experience is that projects without this knowledge tend to founder.

Projects produce the best results where there is an annoying records person constantly and fearlessly trying to ensure that the project results in an EDRMS that can seamlessly capture and manage the evidence that is produced by business activities, in amongst the much broader information

management purposes that they support.

Secondly, recordkeepers can bring a comprehensive and flexible methodology to any information management project. DIRKS is a methodology for designing and implementing a recordkeeping system. It originated in Australia and is part of the Australian Standard for Records Management, AS ISO 15489 Information and documentation - Records Management.

DIRKS has its origins in business systems analysis that have been in use in the information management field for many years. The methodology is divided into 8 principal steps that, when completed, will enable recordkeepers to present a comprehensive schema and plan, to identify and manage evidence organically produced by an organisation's business activities.

Because DIRKS is comprehensive, any combination of its 8 steps can be applied to information management projects. For example, if there is a need to understand the business, regulatory or social context within which an organisation operates, a recordkeeper can use step A, or if a recordkeeper needs to understand the recordkeeping requirements of an organisation, they will apply step C.

Over the past 5 years, different constituencies have applied DIRKS in different ways, but the overall consensus among people I have spoken to has been that it provides a solid set of conceptual and practical tools to develop a thorough, respected and valued recordkeeping system.

One aspect, in particular, that I have found most exciting is the respect I have received from other information management professionals when I have been able to present a logical and

implement an EDRMS."

The third piece of good news is that recordkeeping tools, as well as laying the groundwork for a solid recordkeeping system, have, in my experience, many ongoing applications for the wider management of an organisation's information.

For example, I have found, again and again, that a Business Classification scheme, created by use of the DIRKS methodology, has been used as a business analysis tool to critically assist in the planning for a range of business systems.

I have found that risk managers can use the recordkeeping risk analysis, which comes from the third step of DIRKS, in many other parts of an organisation's information management processes, such as e-mail procedures.

I have also seen a functional analysis provide a rational and consistent means of understanding and conceptualising an organisation's business.

As a final note with regard to these good factors - they are all underpinned by recognition of the need to work closely and collaboratively, with other information professionals, and, most importantly, have a clear understanding of the unique knowledge, methodologies and tools recordkeepers bring to the information management milieu.

I also need to say that the dialogue between recordkeepers and other Information professionals can be improved by all parties developing a better understanding of each other's jargon.

For example, Chris Hurley recently wrote to me, saying, 'To an IT person, I have discovered, a record is "unstructured data", and our stuff is not metadata it's an attribute. To DM,

> ## 'A few of my colleagues have been daunted by or dismissive of DIRKS'

comprehensive schema of an organisation's business activities.

I also have observed that a few of my colleagues have been daunted by, or dismissive of, DIRKS because it is a rigorous and time-consuming methodology. It is worth noting, then, that this rigour is typical of most business system analysis methodologies, and that such rigour wins a lot of creditability in the information management milieu.

Indeed, as I will discuss later, in my experience recordkeepers who do not have a solid understanding, and respect for, business processes in their organisation find it very difficult to advocate a recordkeeping perspective and are quickly marginalized by other information managers.

Perhaps one of the most satisfying exchanges I ever had with an IT person was when he conceded that our EDRMS project was all about capturing evidence in a way that allowed people to get on with their work. We also agreed that a lot of these metadata capture and production processes could be automated.

What flummoxed him, however, was how we were going to identify the evidence that needed to be captured and how we were going to work out how long we needed to keep that evidence for. I was able to say, in triumphant pomposity, "Over the past 18 months we have carried out a DIRKS process and we can now give you the conceptual tools you will need to

classification structure is about taxonomies, not an evidential chain. To business analysts, it is all about identifying a work process that is already in place, rather than designing one for corporate application.'

The Bad

The bad, or dark, or lost side of EDRMS implementation happens when recordkeepers are ignorant of, or have forgotten, the fundamental knowledge, methodologies and tools that they bring to an EDRMS project.

Ignorance, on the part of management, has a lot to do with some truly silly appointments. It needs to be understood that if a person does not know what a record is, does not understand functional analysis and cannot see and coherently explain the fundamental practical and conceptual value to an organisation of a solid recordkeeping system, then they probably shouldn't be appointed to a senior records management position.

Such people may have truly impressive qualifications in IT or librarianship, but if they don't understand and/or have some experience in recordkeeping, their tenure is unfortunate for themselves, the organisation or, as is usually the case, both.

Having made this rather opinionated statement, however, I need to qualify it by saying that if, upon appointment, an IT manager or librarian recognises that they have a fundamental skill

gap, and put in the work and humility needed to close it they can be perfectly good records managers. The variation on this theme is that they take on a truly managerial role and appoint and listen to someone with the specialist subject knowledge.

The key to success for such people is humility and a capacity to listen. The other key is, as will be discussed later, not to fall into the arms of a range of carpetbaggers who are only too ready to profit from the vanity and ignorance of a wrongly appointed records manager.

The real problems start when such a person is given the complex task of selecting and implementing and EDRMS. If that person does not understand the crucial operational recordkeeping requirements associated with an EDRMS. But they do appreciate EDRMS as a generic information management tool. The outcome, in my experience, is usually an awful mix whereby neither the information management nor recordkeeping requirements are met.

Another outcome can also be that the system is simply ignored by users and becomes just another icon on their desktop. This tends to happen when there is no, or only very superficial, business analysis done.

None of the hard analytical work - that recordkeepers are often in a unique position to do - is done. Instead the rationale for the EDRMS is lost in waves of IT and librarianship jargon.

It is also important to note that, in my experience, such people shy away from doing any of the rigorous work in setting up a recordkeeping system that I referred to earlier. They are, however, very attracted to all sorts of marginal, if quite often fun, activities such as having their staff embark in wealth creation courses, or employing executive coaches for their staff so as they can become organisational leaders.

One of my favourites, though, is when a confused manager sent away her staff, each Wednesday, to a toastmaster's course. There were some great speeches and, after the initial fear of public speaking was overcome, we all had a wonderful time. I think the idea was to turn us all into great advocates. I can't say for sure, because the reasons why we were doing this were

IT's section's every whim.

Or they will set off on a course of grand empire building that invariably means they spend most of their time charging at windmills and fighting glorious organisational battles whose outcome is, at best, counter productive and, at worst, disastrous.

The simple fact is that if recordkeepers start out confused and unclear as to what they want from, or what they need to contribute to, an EDRMS implementation, constructive outcomes will be very difficult, if not impossible, to achieve.

I probably need to stop demonizing these "Claytons" records managers! At the end of the day, the problem is a combination of flawed recruitment practises, for which these poor souls (Clayton's records managers) can't possibly be blamed, and the inability of the recordkeeping profession to decide on and promote what are the essential skills a recordkeeper needs to have.

The Ugly

The ugly side of all these shenanigans is the simple fact that, because of dubious implementations, organisations are still very vulnerable to a range of risks. Some of these risks are litigious, and some mean that the documentation of key functions gets carried out poorly, or not at all.

An ineffective or nonexistent EDRMS also is integral in creating an environment that is very vulnerable to corruption.

Let us also not forget that there is a range of businesses, I call them carpetbaggers, who are making a lot of money out of these misadventures. They thrive when Clayton's records managers are appointed to senior positions.

Moreover, they become another source for the, often huge, waste of money and resources associated with flawed EDRMS implementation.

They are also usually the first people to offer and yet another solution to the many problems that they have been a bridesmaid to creating.

Recordkeepers are not IT professionals, or librarians, or senior executives, or trainers, or even change managers. They can, however work with and contribute to all of the above

> **❝ Because of dubious implementations, organisations are still very vulnerable to a range of risks ❞**

hidden under a gentle cloud of New Age jargon.

The other thing to note is that, because this particular manager also had a distinct Stalinist management style, none of us were game enough to ask for clarification. New Age gobbledegook meets Joseph Stalin. Who ever said that recordkeeping was boring?

Perhaps the two saddest parts of these flawed implementations is that they are difficult to remedy over time. They create a culture of confusion and mean that the evidence of an organisation's business is, sometimes for generations, not captured or managed.

Secondly, they often leave the records section with a terrible reputation among users and fellow information professionals. In my experience, this tends to happen because a "Claytons" records manager will completely acquiesce to the

professions' fine endeavours.

At the end of the day their primary focus is to bring a unique set of knowledge, skills and tools to the important task of identifying, capturing and managing evidence of an organisation's business.

It is this unique set, first and foremost, that they should confidently and passionately bring to any EDRMS implementation project.

The Call

I would suggest that the vital knowledge, skills, passion and commitment many recordkeepers bring to the task of EDRMS implementation needs to be better understood and recognised.

I realise that to other information professionals reading the last paragraph it may sound a shade triumphalist, so to these

EDRMS: THE GOOD, THE BAD, THE UGLY: Continued from page 26

readers I would say, on behalf of my rather quirky profession, recordkeeping:

We don't have all the answers but we know a lot about evidence and our involvement will improve the result of an EDRMS project .

Keeping records is just a part of what information systems need to be.

We don't just advocate dedicated recordkeeping applications but also incorporation of recordkeeping functionality into information systems where required.

This is my call - for the recognition of the unique value recordkeepers bring to any EDRMS implementation. iQ

The Author

RMAA member **Stephen Macintosh** has been involved in the recordkeeping profession for some 10 years. In that time he has developed and implemented recordkeeping tools for Federal, State and International public sector organisations. This has included time with the International Monetary Fund, The Human Rights and Equal Opportunity Commission, and NSW Railcorp. Last November he took up the post of Archivist with the Reserve Bank of Australia.

Stephen's article 'Making DIRKS Work,' which appeared in the November 2004 issue of *IQ*, was a Highly Commended entry in the 2004-2205 Objective IQ Article of the Year Award.

Stephen told *IQ*, "It has been a fascinating, absorbing and delightful privilege to be involved in developing strategies for capturing evidence, against the backdrop of monumental technological, organisational and social change."

If readers of this latest EDRMS article wish to discuss its contents, Stephen can be reached at stedel@mail2me.com.au

A MURDER MADE EDRMS LAW

In February, 2000, 9-year-old Victoria Climbie died at London's St Mary's hospital. Her mother and de facto father were later convicted of murder. That case generated an inquiry, which in turn sparked legislation requiring local councils to adopt electronic recordkeeping. But few are meeting the requirements.

The Victoria Climbie Inquiry found that while Victoria had 128 separate injuries and had been abused for months, medical and welfare workers and the Metropolitan Police were guilty of a failure of duty of care.

Victoria had been frequently hospitalised. She had received social worker attention. Police had issued a protection order, then withdrew it. But, critically, local council social workers had not shared records that would have alerted others involved that little Victoria was being seriously abused.

As a result of the Inquiry, the British Government introduced its Electronic Social Care Records (eSCR) initiative in January, 2004. This required local authorities to commence storing new social welfare case records electronically by October, 2005, to aid information access and sharing. And councils must implement an EDRMS across the whole organisation by October this year.

But, Simon Foster of Diagonal Solutions told the RMS *Bulletin* last December, few local authorities have met the first eSCR deadline. Most, he says, still lack the most basic of eSCR plans, and have no chance of meeting this October's EDMRS deadline.

Is this the result of neglect? Or is the task overwhelming councils? In UK local government, social services departments generate vastly more records than any other. And those records must be kept for the 'client's' lifetime – up to 75 years.

Many British councils have computerised some social care records. But only structured data is currently accessible. Unstructured data such as emails, which frequently contain case correspondence that rings alarm bells, isn't.

While eSCR is an excellent concept, and enterprise-wide EDMRS an admirable goal, the reality is that without a massive injection of government money and expertise the October EDMRS deadline is unachievable. And more Victoria Climbies could die because of failures in recordkeeping. iQ

90 Questions
you should be asking EDMS VENDORS
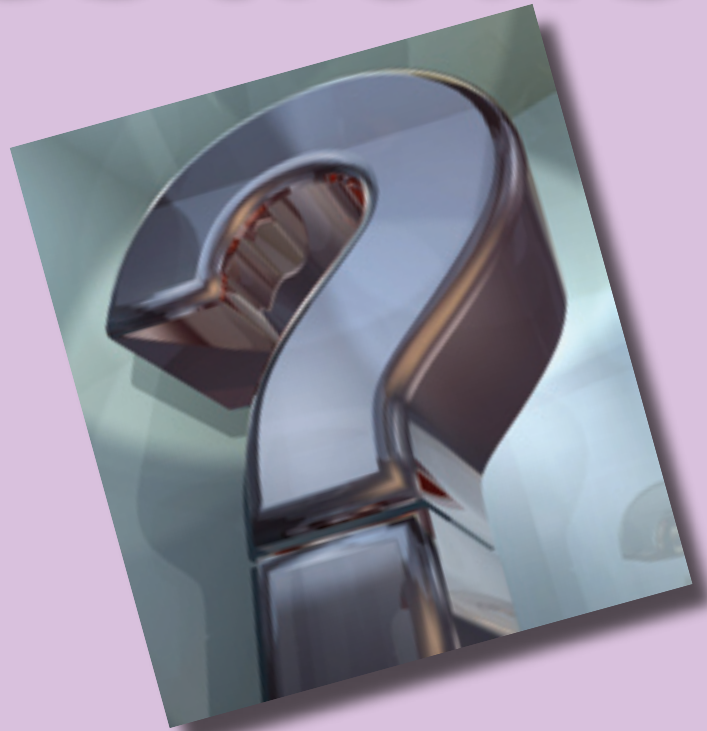
Choosing the right EDMS for your organisation can be an exercise fraught with conflicting claims by vendors and sleepless nights for buyers. Based on extensive professional evaluation, *IQ* presents a range of questions that you should be asking vendors before signing on the dotted line.

New electronic document management systems are frequently coming onto the market. And, over the past year, several major software houses have entered the rapidly expanding RM field for the first time.

The latest offerings boast enhanced capabilities to handle paper and e-records, to provide email management, and to deal with compliance requirements. So, what is the right system for you? The answer can only be arrived at by asking questions. A lot of questions.

Naturally, when you consider any vendor's EDMS offering, you will ask the basic question about the system's integration capabilities, and the partnerships the vendor has with other suppliers for specialist services. You will also ask about the operating software and databases involved. And cost, usually calculated on a per-seat basis, will always be a key factor.

But over and above the basics, there are numerous other operational questions that must be asked if you are to determine the suitability of an offering for your organisation's needs. As a guide, *IQ* presents what we've called the Emery EDMS Evaluator, based on the framework used by leading US EDMS consultant Priscilla Emery in THE RECORDS MANAGEMENT REPORT, (see page 30 for details).

Most of the following questions require a simple YES or NO answer, and you might employ a points system in your evaluation of a vendor's product, giving a point for each YES. Other questions require multiple answers, in which case you could give one point for each attribute you check off.

But the points system can be misleading. For example, you may not consider the first category, Certifications, important, and not bother scoring it. Or, even if a product scores well on Certification that may not interest you as much as later evaluation scores.

How important is certification? In the US, Department of Defence (DoD) certification is considered the gold standard in EDMS. But just because a product doesn't possess DoD certification doesn't mean it isn't DoD compliant. It could mean that the vendor didn't want to part with the US$22,000 certification fee. Or the product could be in the year-long certification queue.

In Britain, TNA/Public Records Office certification was the EDMS equivalent of an Academy Award, but last year the TNA phased out certification, to the astonishment of many in the UK RIM industry. Indications are that the TNA may link with a European Union certification approach by 2007.

In the end, the importance and relevance of Certification is for you to decide. Likewise, you may not care that a particular EDMS only supports 3 of 9 email management systems as long as it supports the one you are currently using or opt for. So, even though a product only scores 3 of a possible 9 points in

that category, it may be just right for your needs.

This questionnaire is not exhaustive. There will be questions that relate to your specific organisation that will need to be addressed. Like every purchase, it all comes down to individual needs and preferences. But you can do worse than use this questionnaire as your starting point.

THE QUESTIONS

CERTIFICATIONS

Does the product have the following?
1.   DoD 5015.2 Certification
2.   DoD 5015.2 Certification including Ch 4 - Managing Classified Records
3.   UK TNA/Public Records Office Certification
4.   Victorian Electronic Records Strategy (VERS) Compliance
5.   ISO 15489 Compliance
6.   RDIMS Certification
7.   21 CFR Part II Compliance
8.   Section 508 Compliance
9.   Other (eg, DOMEA, Germany)?

RECORD/FILE PLAN MANAGEMENT

Does the product...?
10. Create unlimited levels in the classification plan?
11. Support hierarchical and/or functional classification file plans?
12. Allocate records to organisational units?
13. Create custom records metadata for any record type?
14. Support electronic records?
15. Support paper records?
16. Support images?
17. Support CDs
18. Support URLs?
19. Support Microfilm?
20. Support Other elements?
21. Have flexible search terms including record metadata?
22. Use Favorites, Picklists and inheritance for classification?
23. Establish Thesaurus terms for enforcing naming conventions?
24. Identify and manage Vital Records?
25. Mark Official Records with limited access?
26. Allow multiple file classifications to be assigned to a single record?

27. Support bi-directional cross referencing of records?
28. Provide automatic or assisted classification of records?
29. Provide automatic filing and classifying from other systems?

RETENTION and DISPOSAL MANAGEMENT

Does the product...?
30. Manage active, inactive and total retention periods?
31. Support time and/or event-driven retention periods?
32. Automatically calculate transfer and destruction dates for all records in the repository?
33. Change disposition for groupings of records or individual records?
34. Capture applicable legislative citations supporting each retention period?
35. Create disposal reports, including destruction certificates?
36. Provide automatic workflow process for record destruction?
37. Ensure deleted records are destroyed?
38. Assign multiple retention schedules to a single record?
39. Provide e-mail notification of disposition results?

CIRCULATION MANAGEMENT

Does the product...?
40. Allow users to request records that they have been given permission to access?
41. Create colour and barcode labels for physical records?
42. Enable batch printing of labels?
43. Check in/check out records using barcodes?
44. Generate lists of records for pulling from shelves?
45. Support Bring Forwards, Reservations and Recurring Reservations of records?
46. Support passing of checked-out records to another user?
47. Audit reports?
48. Generate Return notices for records?
49. Provide additional features?

HOLD MANAGEMENT

Does the product...?
50. Allow Create, Apply, View and Remove Holds for individual or multiple records in the repository?
51. Provide definition of types of holds and length of time holds?
52. Assign multiple holds to selected records as required?
53. Ensure records cannot be deleted from the system until the hold has been removed?
54. Resume assigned retention and disposition cycle for records once holds have been removed?
55. Maintain complete audit of who assigned and removed holds from records?

STORAGE MANAGEMENT

Does the product...?
56. Track all types and sizes of storage containers within storage locations?
57. Define storage facilities, down to shelf dimensions?
58. Transfer boxes to storage, tracking location of boxes throughout the transfer process?
59. Check in/out all media types to users?
60. Report on total and free space available across all storage facilities?
61. Integrate with Third Party Storage providers?
62. Support accessions for transferring of physical records to external care takers?
63. Enable records to automatically inherit the location from their present container object?
64. Provide additional features?

EMAIL MANAGEMENT

Does the product...?
65. Provide Level of Content Filtering at Header Level, Message Text and/or Attachments?
66. Provide Autoclassification of email into a repository?
67. Provide Encryption Keys for selected messages?
68. Provide Instant Message Archiving?
69. Provide electronic signatures?

70. Provide Certified Receipt/Delivery?
71. Provide a Hosted Email Repository?
72. Archive to another vendor's DM repository?
73. Provide email locking to a Records Repository?
74. Provide a Rule-based Destruction Schedule?
75. Provide Secure Email Tools?
76. Provide Email Audit Trails?
77. Provide Email Storage Management?
78. Provide Email User Profiling?
79. Provide Email Repository Search?
80. Provide additional email management/RM management integration tools?

EMAIL SYSTEMS SUPPORT

Does the product support the following email systems?
81. Microsoft Exchange?
82. Microsoft Outlook?
83. Lotus Notes?
84. Novell Groupwise?
85. Hotmail?
86. AOL Mail?
87. YAHOO! Mail?
88. Earthlink WebMail?
89. Sendmail?

DIGITAL RIGHTS MANAGEMENT

90. Does it have the capacity to detect DRM and to strip the DRM from a document if required?

Add questions that are specific to your organisation to this list, and ask away. Good luck, and may the EDMS you choose give you and your organisation the tools you need. IQ

Sources

All categories and questions in this questionnaire bar the last are based on those used by US RIM consultant and author Priscilla Emery in THE RECORDS MANAGEMENT REPORT (CMSWatch, 2005).

The full Enterprise Search version of that Report, covering all major EDMS products currently on the market, can be purchased for downloading in PDF format at www.cmswatch.com. For more information, email info@cmswatch.com.

The last category and question have been added by *IQ* in the light of growing concerns regarding DRM, and are based on the advice of VERS Technical Research Manager Andrew Waugh.

Log It, or Lose It!
Part 3

By Anastasia Govan, ARMA

Since November 2004, *IQ* has followed the Northern Territory PowerWater Corporation's 10-step EDMS implementation. In this final installment of a three-part series, we look at the last two steps - full implementation and external audit.

PowerWater Corporation (PWC) provides electricity generation, power transmission and distribution networks, water and sewerage, rural and remote services, and retail services across the Northern Territory from 15 locations. With assets worth in excess of $1.2 billion, the Corporation employs 680 people.

Sponsored by the Northern Territory's Information Act, which was enacted in 2003, the PWC embarked on a three-stage Information Governance Compliance Programme.

The final part of that programme was the selection and implementation of an Electronic Document Management System, with completion to take place by December, 2005. The chosen system was Tower's TRIM Context.

The Final Project Steps

Step 9: Full Implementation (Rollout and Training)

Planning can be the most daunting stage of any IT project, but the most important is the investment in human resources at the training and rollout stage.

You need to invest in your project staff daily to keep their spirits high, keep them cohesive and seeing the value of continuing to work for the end rollout goal of process cost efficiencies within the organisation during the rollout. It's a high pressure environment to work in.

You also need to invest heavily in training the organisation's staff - allocating more dollars than hardware and software if you can. This requires repeat bouts of structured initial training for staff as they cutover to the new system.

It also requires ongoing visits to individual work areas, to reinforce the change and provision of fortnightly ad hoc hands-on training in groups, where staff can choose to attend if they need to brush up on a specific topic.

At PowerWater Corporation the training programme also included retraining of some staff due to re-implementation of desktop interfaces to a more user friendly format.

The initial cutover training can become part of the organisation's online intranet-delivered orientation package, with follow-up visits and hands-on training by the Records Management Unit once the EDMS project is over.

Step 10: The Final Evaluation

By now your team is probably very glad to see the end of an enlightening journey. PowerWater was on track to conclude its formal implementation at the end of the year.

After this, capitalisation of the project by the finance team and another external audit concluded the formalities, with training and software upgrades being transferred to the operational areas of the IT and Records units.

As I outlined earlier in the series, it had been a challenging road. But, for PWC and all of us involved, it had been well worth the journey. IQ

The Author

Anastasia Govan, ARMA, is currently Principal Consultant of Inforg in Darwin, NT, (inforg@austarnet.com.au). A full biography accompanies her first article in this series, in *IQ*'s November 2004 issue, (page 22). Part 2 in the series appeared in the February 2005 issue of *IQ*.

UWS TAKES THE PLUNGE

By Julia Barbatano with Michael Smith

After putting several toes in the EDRMS water, the University of Western Sydney (UWS) has taken the plunge to embrace a unified enterprise-wide solution, becoming a leading institution in best practice for managing and sharing corporate knowledge.

The introduction of TOWER Software's TRIM Context as the UWS EDRMS is empowering the university's staff, improving access to corporate knowledge; maintaining corporate history; and most importantly, is unifying the organisation's vast array of document based information.

The Challenge

UWS is one of the largest universities in Australia. Its 6 campuses across 11 different sites in Greater Western Sydney offer undergraduate and postgraduate programs in more than 100 course areas, and provide academic services to over 36,000 enrolled students.

The large number of students and the wide geographical spread of campuses caused the university concern about the challenges and complexities of daily business document sharing. In 2001, the University's IT Directorate conducted an investigation into enterprise application architectures.

The investigation concluded that there was need for a unified system to more efficiently share business documents between all campuses and departments. The new system had to provide:

- Document check-in and check-out;
- Automated version control;
- Interest profiles and document subscriptions;
- Templates;
- Categorisation and metadata;
- Inter-campus and intra-campus document sharing;
- Single user directory;
- Portable and off-line documents;
- Multi-format viewing and document preview;
- Web browser access and multi-platform access;
- Desktop application integration;
- Search interface;
- Document archiving and retention;
- Workflow engine;
- Collaboration capabilities;
- Integration with existing systems;
- Web publishing integration;
- Document naming enforcement;
- Document Capture and scanning.

While this functionality would address the document sharing issue, the system also had to be easily adapted to the university's existing IT architecture, including a network spreading over 9,000 square kilometres.

TRIM Context was already being used by small sections throughout the university for managing paper records, so a decision was made to investigate whether the full functionality of TRIM Context could meet the University's entire information management requirements.

The investigation was performed by an independent consultant, who concluded that TRIM Context would meet the information management requirements as identified by the study, whilst retaining the flexible architecture required for in-house applications.

Sign off was given for TRIM Context to be implemented as the information management solution that would support business processes at UWS.

The Implementation

The University's Records Management Policy devolved to each organisational unit the responsibility for managing its own records. For the implementation, one or more staff from each unit were nominated to coordinate the overall management of records for that unit.

With the delegation of responsibility to the business units, it was important that prior to the rollout, each unit completed an information management analysis. The outcome of this process was a 'Records Information Form' (RIF) which became the blueprint for how files would be created in and managed throughout the recordkeeping continuum.

The user desktop rollout commenced in 2003. The University implemented a Standard Operating Environment on all user desktops and then deployed the TRIM client remotely.

This made for a consistent deployment and also made the delivery of future application upgrades a particularly simple process for administrators and users. Remote deployment was critical in selection of the application, as the university's IT Department is centrally controlled.

The Architecture

TRIM Context is a D-COM multi-tiered application that has a solution for even the most complex customer sites. The strength and flexibility of its architecture is such that it can enhance performance at sites with WAN issues (due to bandwidth and network latency).

The university has a high bandwidth optical fibre network, so the IT Directorate did not need to consider this feature. A centrally located server has been implemented to manage all the components.

The Benefits

UWS began the staged rollout of the system in August 2004. Michael Smith, Manager, Records and Archive Management Services, is pleased with the results to date.

"The introduction of TRIM Context as the University information management system has not only achieved the initial business requirement of sharing documents across campuses, but has also provided other business benefits," he says.

"The University's introduction of TRIM Context has assisted in the compliance with information management legislation such as the NSW State Records Act, 1998, privacy legislation, and Freedom of Information."

Michael says that in an organisation as large and geographically spread as the University of Western Sydney it would have been impossible to meet compliance obligations without a system such as the TOWER Software solution.

Yet, compliance, while important at the organisational level, is not necessarily the highest priority to an individual user. Michael says users are seeing the benefits of improved access times, the reduction in duplication of documents being stored, document security, information sharing, and version control.

"It's not only the users who are seeing these benefits,"

Michael explains, "but also the University's clients - the students. The University now scans and registers student forms in TRIM Context."

Having the forms made available electronically through the EDRMS has meant improved service to students.

"A form can now be submitted at a Student Centre one day and be available to any Student Centre staff - with appropriate access - the following day."

The 'student forms scanning' project has resulted in savings in the resources required for form processing.

Another scanning project that has taken place is in the Capital Works area of the university. This area has scanned approximately 11,000 plans into the system, providing instant access to water, electrical, structural and other plans in an emergency, eliminating the time-consuming task of searching for the paper plans.

The Future

With the success of the unification of corporate knowledge Michael says the University will further expand its use of TRIM Context to include a single centralised file for each student.

This would integrate it with the university's student system, and similar integration with the university's personnel system is also planned. The integration would incorporate the creation, management and closure of student and staff files.

UWS are also investigating the use of TRIM Context within the Media Unit. As it can store any form of digital media this would allow the Media Unit to store and manage their digital photos.

University of Western Sydney RAMS staff, from front to back, **Barry Flanagan**, **Joanne Martin** and **Sharon Flynn**

Photograph courtesy of the *Hawkesbury Gazette*

Conclusion

Formal records management in the University of Western Sydney previously occurred in small pockets of workers, but with the introduction of the enterprise-wide EDRMS system this is now a unified process.

Staff are more empowered through the effective management of the information that supports their business processes. In the ten months since the rollout of the TOWER Software solution commenced, the University of Western Sydney achieved many business benefits.

The university is now looking to further expand the uses of TRIM Context to provide additional benefits and efficiencies to both their staff and student clients. It is anticipated that the solution will be fully rolled out to all areas of the University by mid 2006.   iQ

The Authors

Julia Barbatano is a Product Marketing executive with TOWER Software in Sydney.

Michael Smith is the Manager, Records & Archives Management Services (RAMS), with the University of Western Sydney.

Will All RM Software Deliver on Compliance Needs?

By Priscilla Emery

Legislation around the world has made RM integral to compliance activities. But, with most vendors claiming their EDMS software will support all your compliance needs, a US EDMS expert warns that compliance requirements frequently go beyond the typical RM implementation.

Compliance is a multi-faceted issue. Overall, it is imperative that internal users be compliant with defined records retention and disposition policies.

To some degree, electronic records management systems can aid in enabling quicker and more productive interaction with records but they can also aid in determining active compliance with an RM programme and any auditing activities that may be required as a result.

As a subset of overall compliance come industry-specific or government-mandated regulations that require monitoring and auditability of compliance activities. Government and regulatory compliance are not new issues in the records management space but the consequences of non-compliance have become graver and more expensive.

In addition, the number of regulations has increased dramatically over the last several years making the tracking of these regulations a full-time job in some companies, creating a new 'C' level position – the Chief Compliance Officer.

Couple that with the exponential growth of electronic record volume and the need for software to track and enable defined regulations becomes readily apparent. Just about every vendor will tout its ability to support everything from Sarbanes-Oxley to HIPAA regulations.

However, there are no certification specifications or procedures for any of these compliance activities at this point. So how does a user know if their software is compliant with these regulations? By working with internal compliance officers, legal counsel and internal users to define what compliance really means with regard to specific documents and records.

Those specifications may overlap with the basic functional specifications of a generic records management system but there may be special retention needs within the file plan definition phase or in the reporting phase that go beyond the typical RM implementation.

For example, although records management can play a significant role in Sarbanes-Oxley compliance most of this activity is associated with financial reporting and monitoring financial processes making workflow activities and processes monitoring more important features to focus on than just records retention.

Therefore, you would want to make sure that the RM product can work well with process monitoring software if it doesn't incorporate that function already.

The bottom line is that there is no substitute for doing your homework and understanding your organisation's specific requirements. Although government certifications are becoming a qualifier for many implementations *(DoD in the US and TNA in the UK, for example)* they are by no means the sole requirement during the product selection process. iQ
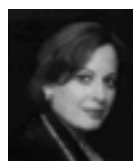
The Author

Priscilla Emery is the Florida-based President and founder of e-Nterprise Advisors and has provided market research and analysis services to Fortune 1000 and high technology companies.

With more than 30 years of technology experience, her areas of expertise include imaging, document, records and email management, and other technologies in the enterprise content management (ECM) landscape.

Prior to establishing e-Nterprise Advisors, she was Senior Vice President of Information Products and Services for AIIM International.

Prior to her position with AIIM, Ms Emery was Vice President and Director of Gartner's Electronic Workplace Technologies research centre and New Science's Intelligent Document Management Service.

She is also the author of the *Records Management Report 2005*, (CMS Watch), a comprehensive analysis of EDMS software currently on the market, which can purchased at www.cmswatchstore.com.

This article is an extract from 'Certifications and Compliance: There is a Difference,' published by the *Sarbanes-Oxley Compliance Journal* in November 2005, and is reprinted in *IQ* with permission.

RIM WORLD OBSERVATIONS
by Kenneth Tombs

OFF the RECORD

Dig-Pres: Ten Years On – Ten Years Back!

"I stand on the terrace of this 200-year-old Arabic sandstone farmhouse, staring across the plain to the town of Zebbug a few kilometres' distant... This landscape has remained unchanged for thousands of years and it is easy to visualise how Gozintian [Maltese] society formed, its origins and its influences displayed through this rich and three-dimensional picture of life as it currently is…"

It's probably just as well my flowery 1995 article, the result of an unusual outbreak of romanticism/idealism, died a death. Clearly, being on an island enjoying myself (er, working), spurred my literary tendencies.

A further 1995 textual failure was 'A Diminished Role for Standards in Archive Sourced Electronic Research Materials' for Oxford University Press. I am not sure who was the more embarrassed, editor Dr Eddy Higgs for his reviewers rejecting my sentiments, or me for having embarrassed him. A good bloke, Eddy, if you ever come across him. At the UK PRO, he held the digi-pres poison chalice for a while.

These articles grew from my drawing together an embryonic preservation strategy for the UK National Archive (nee Public Record Office) from the suggestions of Rick Barry, Tony Hendley and Geoff Rothenburg. The rest, as they say, is history, as EROS emerged (Electronic Records from Office Systems) soon after, and digital preservation was underway at least in the UK.

Everyone was involved: IT gurus, librarians, NARA and the Nixon Watergate tapes, Mark Fresko, Jose Luis Borbinha and many others. From this arose DGXIII-powered (Brussels) initiatives, collectively building a view of how to preserve our governments' histories.

They were heady days. Emulators, change programmes, training and awareness sessions, accession programmes, conferences, EDRMs, simulators, Bundling (overtaken by PDF), virtual storage, optical juke-boxes, and many more wondrous terms and technologies. We even had the then political fresher Geof Hoon (now leader of the House of Commons) lending his political weight to electronic preservation.

Everywhere we turned, up popped someone with a new idea, a white paper, some potential practice or an experiment to try, and perhaps naively we expected things to happen, and quickly.

The reality has turned out quite positive. EDRM suppliers actually seem interested in their customers. Archivists and librarians talk to each other occasionally. A few archives even have machines to stuff their documentary electrons into!

Yet, we don't have a shared attitude towards Government records away from the Anglophile world. In some respects, we have gone backwards, with Governments now apparently much less concerned whether the official record survives or not.

Arguably, Europe has taken the first step towards a world class government when agreeing that Turkey may join. But, in a hundred years time, will we look back and see great political voids in our decision-taking map of the world?

We prevaricated politically over large-scale digital preservation systems for half a decade, and may find ourselves lumbered with soon-to-become-obsolete high-overhead technologies. Public records are a big game, no doubting that. By the nature of the beast they should tend towards well proven machinery. Yet we must remain wary of getting locked into technologies because we feel we have solved the problem. Complaisance might just kill us.

Over the last few weeks I have been testing text-extraction, taxonimising (good grief!) and natural language processing tools for a client project. Yes, I got paid-to-play. I am amazed at how effective and accurate they have become, with such simplicity of use. More important is how little these tools cost per seat, in lacking massive computer and time overheads.

Ten years ago, national archives took some heavy pressures to move from the totality of paper to the hybrid electronic. How much pressure would it take today to move on to less intrusive and overhead-laden ways of knowing what we should keep? Is it timely to get involved with the next generation of text tools so the archives and records community can shape exactly what it needs next?

Rose-coloured retrospectives are fine, but we must look forward again, and anticipate - history shows it really does take a long time to progress. Technology isn't quite so forgiving as paper when you turn on the power switch and the valves don't glow! iQ

The Author

Kenneth Tombs worked for major ICT suppliers in Britain before establishing an education company. Ken works extensively with the UK Office of Government Commerce and service providers. He is also a director of Document Law and of the Performance Trust. His forthcoming book Making Out With Decisions is 'an irreverent miscellany with pictures' on the practical aspects of making a choice. He can be contacted at: ken.tombs@warmfuzzies.co.uk.

Does
DIGITAL RIGHTS MANAGEMENT

Tie Recordkeepers' Hands Behind their Backs?

By Stephen Dando-Collins

Is DRM a curse, or a cure? Recent revelations about Sony BMG's surreptitious use of digital rights management on music CDs have sparked a major debate about its pros and cons. According to some authorities, DRM can only have a negative impact on records and information management.

Enterprise content management can be broken down into five categories – records management, document management, Web content management, digital asset management, and digital rights management.

In its most celebrated guise, digital rights management involves implantation of encryption in products such as videos, music CDs, and digital photographs, to prevent unauthorised use and copying.

With movie and music piracy a huge worldwide problem for producers, it made sense to the manufacturing and legal communities to go down that road to cure the problem by creating so-called 'copy protection.'.

Enter Sony BMG's XCP. Last November, Associated Press revealed that Sony had apologised for secretly introducing its XCP 'copy protection program' to 52 of its music CDs. XCP incorporates a cloaking feature which hides files on users computers to prevent the copying of its product.

Problem number one: Sony didn't tell its customers about XCP, making it a Trojan. Problem number two: after there was a public outcry, and Sony made a patch available to its customers so they could uninstall XCP from their computers, it was soon found that the 3.5mb patch could open up the computer to a host of other Trojans. The State of Texas considered XCP so malicious it sued Sony BMG.

In January, Sony BMG offered affected customers refunds and replacement CDs which did not contain their XCP copy protection.

There are lessons here for RIMs. For, DRM has begun to find its way into the RIM world. The British Library, in its secure electronic delivery service, used DRM to manage worldwide access to numbers of rare documents which, for legal reasons, could only previously be accessed via a personal visit to the Library's document centre.

In the US, the American Dental Schools (ADS) use DRM for DVD textbooks which 'expire' after a set time.

The former use seems worthy, the latter questionable – not only does it spell the end for second-hand books, future researchers would be prevented from accessing material that was subject to DRM if the ADS model were to be broadly adopted.

Meanwhile, DRM was incorporated into the 2002 Sarbanes-Oxley Act (SOX) in the US as a key part of corporate compliance policies, to protect corporate documents from unauthorised tampering, and creating an audit trail. Again, a seemingly worthy application.

But what happens, as in the Sony XCP case, when the application proves to be flawed? Worse, what if the application is malicious - so-called malware? In Europe, DRM schemes have a host of opponents, who have labelled DRM 'e-Slavery'.

Online encyclopaedia Wikipedia, in its definition of digital rights management, notes, 'All forms of DRM depend on the device imposing restrictions that cannot be legally disabled or modified by the user. In other words, the user has no choice.'

Professor Ross Anderson, of Cambridge University's Computer Laboratory, author of the book Security Engineering, is, with Cambridge colleagues, a leading adversary of DRM.

Cambridge University's Professor **Ross Anderson** is a vocal critic of digital rights management.

In his 2004 paper 'Cryptography and Competition Policy – Issues with "Trusted Computing"', (www.cl.cam.ac.uk/users/rja14#Econ), Professor Anderson expressed grave misgivings about the Microsoft 'Trusted Computing' (TC) initiative, another variant of DRM.

'Given the claims by TC supporters,' he wrote, 'that TC will create value for customers, and the clear expectation that it will also create value for vendors, and all the fog of impassioned argument about the rights and wrongs of digital rights management, perhaps the test of whether the consumers end up better or worse off may be the most simple and practical way to arrive at a consistent and robust policy decision on TC.'

I recently spoke to Professor Anderson, and suggested that he might feel both concern and vindication as a result of the Sony XCP revelations.

"Damn right!" Anderson responded. "We predicted that a move to 'trusted computing' would lead to the appearance of 'trusted malware' that would be harder to get rid of. The only thing we didn't expect was that the culprit would be Sony rather than Microsoft."

The problem with DRM doesn't stop with CDs and DVDs. There are potentially grave implications for records and information management.

In 2003, Microsoft incorporated DRM functionality into its Office suite, enabling desktop users to place severe restrictions on the documents and communications they create.

At the Records Management Association of Australasia's Convention in Perth, Western Australia last September, Andrew Waugh, Technical Research Manager with the Public Record Office of Victoria's VERS Centre of Excellence, warned his audience to avoid DRM like the plague. It should not be turned on in any organisation, he said, and email containing DRM should be bounced right back.

Waugh discusses DRM in his article on digital preservation starting on page 38 of this issue of *IQ*, but for this DRM-specific article I asked Waugh to elaborate on his concerns about the potential for DRM to have a negative impact on recordkeeping.

"Digital rights management technology is normally used to prevent people from making illegal copies of songs and videos," he recently told me. "But it can be used to control the display of any digital content including emails and reports."

Yes, but to intellectual property owners - and every organisation owns intellectual property - this would be a plus, surely? Scottish firm LockLizard (www.locklizard.com) is one of a number of companies around the world marketing DRM software to 'protect your intellectual property from unauthorised use and misuse.'

LockLizard says that, using their products, you can 'publish your PDF documents and software applications using the Internet and other media including CDs, disks and email, knowing you have full control over them at all times.'

LockLizard says their Safeguard product controls who can view a document, and for how long - both online and offline - and limits the copying and saving of documents. It also provides immediate termination of access to documents if a customer fails to pay.

Which all sounds fine, in theory, if you are an intellectual property owner.

Ah, says PROV's Andrew Waugh, what if you are the recipient of material containing DRM?

"Under DRM," he told me, "you could receive an email and act on it, and then the sender could unilaterally destroy your copy of the email.

"The DRM would also have prevented you from printing out a copy of the email for your files, or saving it to your electronic recordkeeping system.

"You would be left with no evidence about why you acted. DRM consequently has the potential for destroying the basis for your recordkeeping system."

There can be no doubting that DRM has the capacity to cause RIMs significant headaches in the future.

Meanwhile, *TechWeb News* reported on November 21 that analysts at Gartner in the US had soon found an easy cure to Sony's XCP program, which took 5 years to develop – stick a piece of opaque tape the size of a fingernail on the out edge of the affected CD.

Solutions to larger RIM problems caused by DRM may be harder to find, just as DRM itself may be harder to detect in the future. iQ

The Author

Stephen Dando-Collins is the Editor of *IQ*. He is also the Managing Director of editorial consultancy Fame & Fortune and the author of a number of books on subjects ranging from sociology to business and history.

DIGITAL PRESERVATION: THE VIEW FROM VERS

By Andrew Waugh

Digital technology has drastically changed how we record information. This article by the Technical Research Manager with the Public Record Office of Victoria's VERS Centre for Excellence gives an overview of current activities in digital preservation and discusses how you can begin to preserve the digital records held by your organisation.

While the paperless office has not yet arrived, the preparation of work has largely gone electronic. Reports, for example, are written using Microsoft Word, information is published on the Web, and communication with colleagues and, often, the public, is via email. This change has posed a massive challenge to accurately recording what organisations did, and why.

Digital preservation is a very broad area. A workshop sponsored by the NSF and Library of Congress in 2003[1] identified four broad research challenges in digital archiving.

Technical architectures for archival repositories. This challenge focused on the development and testing of a range of digital archival systems and services. One emphasis was on scalability of the systems and their cost of operation.

Collection management and processes. This challenge focused on organisational processes dealing with managing a digital collection. This included curatorial processes, preservation methods, and aggregating items into collections.

Digital archiving tools and techniques. This challenge focused on technical aspects of managing a digital collection. This included the accession of digital objects into the collection, standards, the persistent naming of objects. And managing the evolution of the archive over time.

future in an unaltered, authentic state.

'On the other hand, doing so inevitably requires come alteration. All the methods described in this paper entail altering or replacing hardware, software, or data, and sometimes more than one of these.'

In the work discussed in this section, there is clear emphasis that digital preservation is a complex task that must be supported both organisationally and technically. Preservation requires management of the digital objects, and this management is primarily embodied in a sophisticated digital archive that holds the digital object.

This approach to preservation raises challenges for organisations (and individuals) that do not have the resources to obtain or operate such a digital archive. The remainder of this article will discuss simple steps that will assist in the preservation of digital objects outside a digital archive.

Preservation in the Small

To understand the challenges of preserving digital records for 100 years or more it is necessary to understand how information is stored and displayed in a computer. There are four basic challenges to preserving digital records.

Media preservation. The challenge is in ensuring that the computer files are not lost due to failure or obsolescence of the media on which the files are stored.

> ' Sooner or later these programs will cease to function, and access to the records will be lost '

Organisational, economic, and policy issues. This challenge focused on the business case, including economic and business models and cost/benefit/value metrics.

A good overview of the major international preservation projects can be found in The State of Digital Preservation: An International Perspective, 2002[2]. These projects include the National Digital Infrastructure Initiative (NDII)[3], a massive US digital archive based in the Library of Congress, Nedlib[4], a significant digital archive constructed by the National Library of the Netherlands to store electronic publications, and Pandora[5], the National Library of Australia's digital archive of significant Australian websites.

In Australia, the National Archives of Australia (NAA) have been working on a digital preservation submission and archiving project[6,7], and the Public Records Office of Victoria (PROV) has just commissioned a digital archive to support VERS (Victorian Electronic Record Strategy)[8].

The national, state and territory archival and records authorities in Australia and New Zealand are cooperating on the Australian Digital Recordkeeping Initiative (ADRI). ADRI is planning to work on guidelines for preservation formats, migration strategies and processes for agencies' preservation and retrieval from defunct systems or media.

Work will also be carried out on standards for describing digital records, preservation formats, digital repositories, and the authenticity of digital records.

Thibodeau[9] discusses the advantages and limitations of the various technical approaches to preservation and concludes with the observation: 'There is an inherent paradox in digital preservation. On the one hand, it aims to deliver the past to the

Program preservation. The challenge is ensuring that a program is available to read the computer files and 'display' their contents to users.

Contextual preservation. The challenge is knowing how an individual digital record relates to other digital records.

Integrity preservation. The challenge is in being able to demonstrate whether a digital record has been modified, and if so, how it was modified and who modified it.

Media Preservation

Information is normally stored as one or more computer files; for example, a report might be stored as 'reprt.doc'. Such files are physically stored on media such as hard discs, magnetic tape, CDs, or DVDs.

The first preservation challenge is that these pieces of media have a finite and relatively short lifespan. A hard disc, for example, might have a life of four or five years before failing.

The second issue is that storage technology as a whole has a relatively short life; a CD may still be readable in twenty years, but will CD readers still be available, and could they be plugged into the then current computers?

The key to solving the challenge of the short life of media is to separate the concept of the computer file from the media on which it is stored. Preservation of electronic records is not about preserving the media on which these records were initially stored.

Instead, the focus should be on preserving the record itself, and accurately copying the record – in the shape of a file – from one piece of media to another. In the archival literature this copying is known as 'refreshing' the media.

Accurately copying the record requires management of

the media. The management involved depends on whether the media is stored online - on hard discs on file servers as part of the normal computing environment – or offline on removable media – eg, CDs, DVDs, or tapes.

When records are stored as part of the normal computing environment, the media management would normally be a function of the IT department. As part of the normal, day to day operations, an IT department should back up the contents of media to protect against the failure of individual pieces of media – eg, disc crashes. And accurately copy the contents of media when one technology is being replaced by another. And recover from a catastrophic failure of the computing infrastructure – a fire, for example.

The key duty of a records manager is to ensure that these processes are accurately carried out.

Where records are stored offline the management task is more significant. Recommendations for the care and handling of CDs and DVDs can be found in Byers[10]. For tape, a good place to start is the fact sheets produced by the Association of Moving Image Archivists (AMIA)[11]. Although these deal with video tape, the issues are very similar to digital storage tapes.

Irrespective of the media format, it is recommended that you systematically sample your collection of offline media and attempt to read data from the sampled media. This assists in detecting slow deterioration of the media.

In comparing an online and offline storage solution, you should carefully consider the whole-of-life costs. This not only includes the original cost of the media and readers, but the cost of managing the media and eventual refreshing.

Due to recent advances in disk storage technology, large capacity disk (online) storage has dropped in price. The cost of storage in the PROV Digital Archive is currently around $70,000 for each terabyte, which includes off-site replication and the storage of multiple copies.

> **When selecting an EDMS careful attention should be paid to the interface used to enter metadata when registering an electronic record**

Program Preservation

Unlike a paper record, a user cannot just 'read' a digital record. To see or hear a digital record a user must run a program to interpret the contents of the file and 'display' the information in it. A user, for example, would run Microsoft Word to interpret the contents of the '.doc' file and display the report.

The preservation challenge here is that sooner or later these programs will cease to function, and access to the records will be lost. The programs will eventually cease to function because they depend on a computing environment – a particular design of hardware and operating system.

Over time this environment changes and, eventually, will sufficiently change so that the program will not run. For example, will we be able to run Microsoft Word in 20 years time to display the contents of the '.doc' files?

Preservation Problems in a Digital World

Essentially, there are two core approaches to program preservation: migration and emulation. Migration involves converting from one data format to another. Emulation involves writing a program to reproduce the execution of obsolete hardware or software.

A preservation approach may involve a mixture of migration and emulation. For example, VERS migrates electronic records to a long-term preservation format, eg PDF, and then depends on emulating the display software in the future. In practice, current preservation strategies depend on migration as emulation is still in the research phase.

We (PROV VERS Centre of Excellence) recommend that organisations that need to keep electronic records choose a small number of long term preservation formats such as TIFF, JPEG, or PDF. All records that need to be kept for more than a short period should be saved in one of those formats.

Each additional long-term preservation format chosen increases the long-term management cost as viewing software will need to be obtained for each format and, ultimately, each record in a particular format may need to migrated to another format.

When choosing a long-term preservation format there are several criteria to base a decision on. In order of importance these are:

Published specifications. The long-term ability to write new software to display a format depends on access to accurate specifications of the format. As an archive, PROV is building up a library of the specifications that it uses.

Formally published specifications are preferred as these are legally deposited in a library. International standards such as JPEG are preferred, however VERS accepts proprietary or industry specifications, provided the specification is complete, easily obtainable, and accurate.

Independent implementations. A format that has been independently implemented by several vendors is preferred over one that has only been implemented by one. Independent implementations help ensure that the published specification is accurately implemented.

Industry usage. It is preferable to choose a format that is widely used – it is likely to have a longer life before becoming

obsolete. When it does become obsolete, there are likely to be several migration tools to convert the format to a new one.

PROV accepts the following long-term preservation formats: PDF for document-like objects and plain text, and TIFF and JPEG for images. (*PROV is also adopting the new PDF/A format*.)

The International Association of Sound and Audiovisual Archives has published guidelines on recommended audio formats[12]. The Dutch National Archives have undertaken experiments in preserving various types of electronic records and have published their findings for databases[13], spreadsheets[14], text documents[15], and email[16].

A long-term preservation format for the Web is problematic, mainly because a Web page can link to objects in any format. For actual Web pages, archives such as Pandora save the native Web page itself.

The weakness of any migration approach is the loss of information if the migration is not accurate. This issue can be addressed in two ways. The first is that a well-chosen long-term

Contextual Preservation

Even retaining the ability to display the contents of a file does not exhaust the preservation problems. A document only tells a part of the story; for example, reading a single email from a lengthy exchange is likely to be of limited help and could be quite misleading.

To understand the whole story it is necessary to know the context of the record: what the record is, eg, title and subject, and who created the record and why. And, how does it relate to other records? This context needs to be preserved along with the content of the record.

Unfortunately, computer systems are generally not designed to store this contextual information let alone preserve it for long periods. Losing the context of a record is the cause of the common user experience of 'losing' files on the file server, or looking at a list of files in a directory and not knowing what the file is.

The answer to preserving context is to associate metadata with the electronic record. Normally this requires a system to

> ❝ We believe that DRM will become a significant issue for most organisations over the coming decade ❞

preservation will minimise the number of migrations required and hence minimises the potential for loss of information. The second is to preserve the original data file; this allows a re-migration if a better preservation approach is developed in the future.

One potential strength of emulation is the ability to preserve the experience of creating the record. Emulation, for example, would allow a future researcher to open up a report using the same Microsoft Word program that the creator used when writing the report. While this feature is very valuable to cultural institutions that preserve the experience of using artifacts, we believe that it is less relevant to archives.

Migration, on the other hand, allows organisations to preserve, as far as possible, the original appearance of the record, with this appearance being rendered by contemporary programs.

manage the electronic records and the associated metadata. However, this system does not have to be sophisticated.

In Victoria, a number of agencies use their departmental computer file server as a simple electronic record management structure pending an EDMS. Two policies need to be developed to do this: a recordkeeping file classification scheme, and a computer file naming convention.

The file classification scheme is developed in preparation for the EDMS, usually using a functional analysis methodology such as DIRKS. The file classification scheme is used to set up the directories in the file server.

The file naming convention is used to title the computer files on the server. For example, the Word file containing this paper might be named 'RMAA presentation-v2-20050710-ajw.

doc'. A typical file naming convention includes a meaningful title, a version number, a date, and the initials of the creator.

Use of the file server as a simple management system in this way has a number of advantages. It allows some management of electronic records immediately, it gets the agency staff used to the file classification scheme, and it organises the electronic records in preparation for the eventual deployment of an EDMS.

Of course, we do not recommend the use of a file server as a long-term solution, because it does not support organised management and disposal of electronic records, nor does it ensure record integrity or authenticity.

We expect the long-term solution for contextual preservation for most organisations will be the deployment of an EDMS with appropriate recordkeeping functionality. From the point of long-term preservation of electronic records, the most important features of an EDMS are these.

1. The ability to capture and manage electronic records from a range of corporate information systems. Easy capture from the corporate email system is probably the highest priority in most organisations as, otherwise, emails are isolated in a proprietary system and must be managed there.

2. The ability to control modifications to electronic records, and, where modifications are allowed, to record what was modified, who modified it, and where the modification occurred. This will be discussed further in the next section on integrity preservation.

3. The ability to record metadata and associate it with electronic records. Good collections of metadata can be found in VERS, and in the National Archives of Australia recordkeeping Metadata standard[17]. For governments, the minimum level of metadata should be the AGL standard[18].

When selecting an EDMS, careful attention should be paid to the interface used to enter metadata when registering an electronic record. Our experience is that it can be difficult to convince users to enter meaningful metadata at all, and a poorly designed user interface increases this difficulty.

4. The ability to automatically convert documents to a long term preservation format. The reason this fir this had been discussed in the previous section on program preservation.

5. The ability to detect and/or remove digital rights management (DRM) controls from registered records. We believe that DRM will become a significant issue for most organisations over the coming decade.

DRM systems allow the original creator of an electronic document to control who may subsequently access it; for example, the sender of an email can effectively delete it from the receiver's system after the receiver has read and acted upon it. DRM clearly destroys an organisation's ability to document and defend its actions.

We recommend that any EDMS should detect the presence of DRM and, at least, bring this to the attention of the user. Ideally, an EDMS would be capable of stripping the DRM from the document.

6. The ability to export the registered electronic records, including the metadata. When commissioning a new system, little thought is often given to its eventual decommissioning. When the system is decommissioned, it will be necessary to

extract the registered records from it – including the metadata – and to transfer them to its replacement system.

This transfer is likely to be a point of great risk to the records. If the transfer is not easy, it is possible that the records will simply be abandoned in the obsolete system as not worth the cost of transferring. Even if records are transferred, there may be issues about the cost and quality of the transformation.

We recommend that the issues of decommissioning the system be considered up front when the system is being selected and commissioned.

Integrity Preservation

The final preservation problem is proving the integrity of the electronic record; that is, that the record has not been altered since it was created.

While there were centuries of experience in demonstrating the integrity of paper records, we have little experience in demonstrating this for electronic records. Current computer file systems provide little support for demonstrating integrity, and for this reason loss of integrity can occur immediately after the electronic record is created.

An EDMS assists in ensuring integrity by controlling access to electronic records and documenting any modifications that are carried out. The documentation is usually captured in an audit log. When evaluating an EDMS, it should be remembered that the ability to check integrity is dependent on the ability to extract information from the audit log

Two particular issues should be considered. The first issue is the granularity of the entries in the audit log. In many EDMS, a single recordkeeping event - such as modification - is represented in the audit log by the sequence of low-level action, such as checking in and out of versions. The high-level events must reconstructed from the sequence of low-level events.

The second issue of the ease of isolating the events that relate to a particular electronic record, or series.

VERS detects unauthorised modifications to digital records by signing the VEO with a digital signature. This allows the integrity of the record to be validated at any time, and it can be validated completely independently of the system that is holding the records.

Conclusion

There are many activities that organisations can do right now to help ensure the long term preservation of electronic records.

An EDMS can be used to support long term preservation of electronic records. In particular, an EDMS can protect the integrity of the electronic record, transform the content into a long-term preservation format, and store metadata that describes the context of the electronic record.

Even if an organisation does not have an EDMS, actions can be taken to assist long-term preservation. A file classification can be adopted in the file server and users can be encouraged to save electronic records in a long-term preservation format.

Readers interested in further reading on digital preservation should consult PADI[19], the annotated bibliography maintained by the National Library of Australia. There are three e-journals devoted to digital libraries and related information: *Ariadne*[20], *D-Lib Magazine*[21], and *RLG DigiNews*[22]. iQ

The Author

Andrew Waugh is Technical Research Manager with the Public Record Office Victoria's VERS Centre of Excellence in Melbourne. The PROV is a corporate member of the RMAA.

This paper was presented by Andrew at the 23rd RMAA International Convention in Perth, Western Australia, in September, 2005.
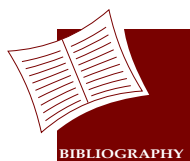
BIBLIOGRAPHY

1. The National Science Foundation (et al), It's about Time: Research Challenges in Digital Archiving and Long Term Preservation, Workshop on Research Challenges in Digital Archiving and Long-term Preservation, April 12-13, 2002, http://www.digitalpreservation.gov.repor/NSF LC Final Report pdf, visited 25 July 2005.

2. Council on Library and Information Resources, The State of Digital Preservation: An International Perspective, 2003, http://www.clir.org/pubs/abstract/pub107abst.html, visited 25 July 2005.

3. Campbell, L, Update on the National Digital Infrastructure Initiative, in the State of Digital Preservation, loc cit.

4. Van der Werf, Experience of the National Library of the Netherlands, in the State of Digital Preservation, loc cit.

5. Web, C, Digital Preservation – a Many-Layered Thing: Experience at the National Library of Australia.

6. National Archives of Australia, Digital Preservation Project, http://ww.naa.gov.au/recordkeeping/preservation/digital/summary.html, visited 25 July, 2005.

7. SourceFORGE, XENA http://xena.sourceforge.net/, visited 25 July, 2005.

8. Public Record Office Victoria, VERS, http://www.prov.vic.gov.au/vers/vers/. Visited 25 July 2005.

9. Thibodeau, K, Overview of Technological Approaches to Digital Preservation and Challenges in Coming Years, in The State of Digital Preservation, loc cit.

10. Byers, F, Care and Handling of CDs and DVDs, CLIR/NIST, 2003, ISBN 1-932326-04-9, http://www.itl.nist.gov/div895/carefordisc/, visited 25 July 2005.

11. Association of Moving Image Archivists, Videotape Preservation Fact Sheets, http://www.amianet.org/publication/resources/guidelines/videofacts/intro.html, visited 25 July 2005.

12. International Association of Sound and Audiovisual Archives, Guidance on the Production and Preservation of Digital Audio Objects, 2004, self-published.

13. Digital Preservation Testbed, From digital volatility to digital permanence, Preserving database, Dutch National Archives, 2003, ISBN 90-807758-1-9, http://www.digitaleduurzaamheid.nl/bibliotheek/docs/volatility-permanence-databases-en.pdf, visited 25 July 2005.

14. Digital Preservation Testbed, From digital volatility to digital permanence, Preserving spreadsheets, Dutch National Archives, 2003, ISBN 90-807758-1-9, http://www.digitaleduurzaamheid.nl/biliotheek/docs/volatility-permanence-spreadsh-en.pdf, visited 25 July 2005.

15. Digital Preservation Testbed, From digital volatility to digital permanence, Preserving text documents, Dutch national Archives, 2003, ISBN 90-807758-1-9, http://www.digitaleduurzaamheid.nl/bibliotheek/docs/volatility-permanence-textdocs-en.pdf, visited 25 July 2005.

16. Digital Preservation Testbed, From digital volatility to digital permanence, Preserving email, Dutch National Archives, 2003, ISBN 90-807758-1-9, http://www.digitaleduurzaamheid.nl/bibliotheek/docs/volatility-permanence-email-en.pdf, visited 25 July, 2005.

17. National Archives of Australia, Recordkeeping Metadata Standard for Commonwealth Agencies, 1999, ISBN 0 642 34407 8, http://www.naa.gov.au/recordkeeping/control/rkms/summary.html, visited 25 July, 2005.

18. National Archives of Australia, AGLS Metadata Element Set Part 1:Reference Description, 2002, ISBN 0 642 34491 4, http://www.naa.gov.au/recordkeeping/gov online/agis/metadata element set.html, visited 25 July, 2005.

19. National Library of Australia, PADI, Preserving Access to Digital Information, http://www.nla.gov.au/padi/ visited 25 July, 2005.

20. UKOLN Araidne http://www.ariadne.ac.uk/ visited 25 July, 2005.

21. CNRI D-Lib Magazine http://www.dlib.org/ visited 25 July 2005.

22. RLG RLG DigiNews http://www.rig.org/en/page.php?Page ID=12081 visited 25 July, 2005.

FUTURE-PROOFING DIGITAL MATERIAL:

Is There Light at the End of the Tunnel?

DR ROBERT SHARPE of UK RIM consultancy Tessella describes, from practical experience, how in recent years a number of mainly academic and government organisations in the UK, the US and the Netherlands have been at the forefront of digital preservation challenges, allowing a body of knowledge and experience to be developed that can give other organisations the confidence to address the issue.

The advances of computer technology offer many new opportunities but also new challenges. One of the most important challenges is ensuring that digital information we create and store today will remain accessible for as long as we may need it. The challenges involved are considerable since the aim is to ensure that in the future we can read any electronic record … 'born digital' or scanned … regardless of the original format, software application, operating systems and hardware used to create it. Failure to address this issue could lead to irrevocable loss of both our cultural heritage and the intellectual property of organisations.

Tessella has played a key role in a number of the most practical of these initiatives, and as a result believe that it is possible to take steps to safeguard the digital knowledge of an organisation and thus preserve digital records using today's technology.

Such a solution will not be complete and some further experimentation and research is required, but this can occur in parallel with active preservation measures. The alternative would be to wait, but the greater the time lag between creation and facing the issues involved, the greater the risk of information loss or excessive expense in order to be able to retrieve such information.

Taking pro-active measures also allows organisations to gain invaluable experience of the processes involved whilst evolving a more complete solution to their digital preservation problems.

This philosophy leads to the recommended solution consisting of modular parts based around a framework. The framework gives the required structure to product and process, whilst the modularity allows third-party solutions to be added as time goes by, thereby leveraging digital preservation solutions achieved elsewhere.

What's the Problem?

In today's society an increasing amount of information is being created and stored digitally. In addition, the number of ways in which this information can be stored is increasing, with new software products or new versions of existing products constantly coming onto the market. All of this means that there is a large quantity of digital records, potentially containing information of vital corporate or societal importance, in an ever expanding number of formats.

However, these formats rapidly become obsolete, and as hardware and operating systems move on, digital files can become unreadable. In many cases the format can be read by newer software but even then some of the information in that file may be altered or lost in the transformation. This means that most organisations' own information which is in danger of

Solving this problem was a not a trivial exercise, but was completed successfully after considerable effort (including experience and input from the original record creators). For more details on this task, see <www.nationalarchives.gov.uk/ preservation/research/domesday.htm/default.htm>.

Although the records are now safe, for another 15 years maybe, the amount of effort required to preserve a relatively small amount of information shows it is not practical to rely on such methods for all digital records.

Does it Affect My Organisation?

The question every organisation needs to ask itself is whether the usefulness of its digital material will outlast the lifetime of the software used to create or read it. Such application software will rely on an operating system and hardware, and this typically has a lifetime of just a few years. Thus, the answer to this question is almost certainly: yes!

All organisations are threatened with the loss of information, which will be very expensive to recreate, but it is mainly those that are required to save data for a long time that have been at the forefront of addressing the challenges of digital preservation. These organisations include:

Scientific organisations that collect large amounts of data over a long period of time. For instance, if a mission is sent to collect data from a remote planet, it is definitely worth going to

> **The longer the problem is put off, the greater the risk of losing information**

becoming inaccessible only a relatively short time after it was created.

Digital records can also be endangered because of the way in which they are stored: the media can deteriorate or became difficult to read owing to the obsolescence of the associated hardware. This is in sharp contrast to paper records which, provided they are stored in the appropriate conditions, are likely to remain readable for a very long time.

The Domesday Book Dilema

A case study illustrates the problem well. The Domesday Book, William the Conqueror's survey of England in 1086, is still readable today in the UK National Archives at Kew, London. A modern, digital version of the 'Domesday Book' was created by the BBC children's program Blue Peter to celebrate the 900th anniversary of the original.

Children were invited to submit digital material about their community, which was stored on the latest technology to guard against obsolescence: 12" laser disks. Just fifteen years later, serious action had to be taken to save these records from being lost for a number of reasons.

Firstly, the media has become very difficult to read with relatively few laser disk readers still in working order. Fortunately, the time-gap from creation was still sufficiently small that some readers still existed, so this problem could be solved. This allowed the files to be extracted in binary format onto more modern media.

The next challenge was to interpret this so that it was not just a meaningless string of 1s and 0s, as the digital files could not be interpreted by any modern software.

the expense of preserving the data. One of the advantages that scientific organisations have is that they can often dictate their own data formats.

Universities and academic research organisations. A lot of money is spent generating and gathering research information, and such institutions have a duty to keep it for future generations of researchers. For example, a number of university libraries are creating digital collections of thesis abstracts, and in some cases are saving full theses (again, aided by the fact that they are able to dictate the format).

Regional, national and international libraries responsible for maintaining collections of new materials: almost all of which are now produced digitally. These organisations have a difficult job although most of the materials they receive will be from a relatively few sources (e.g. the publishing industry) and will be in well-defined formats.

Regional, national and international archives responsible for maintaining government records. Like libraries, these organisations face the issue that almost all of their future ingest material is now being produced digitally. In this case there is also likely to be a wide variety of formats with little uniformity.

Some standardisation may be possible, but this can never be 100% effective since it is likely that there will be a requirement to archive information that has originated from outside the influence of these standards

Companies in regulated industries, notably in the pharmaceutical and nuclear sectors. These industries have a duty to preserve information often in a wide variety of formats, some of which (such as data output from a given piece of equipment) rapidly become obsolete.

What Can We Do About It?

The result of the research and active preservation measures performed by the types of organisations described above means that it is now possible to plot a roadmap, which other organisations can follow to solve the digital preservation problem.

Not all parts of this roadmap are well defined and, even in the better defined areas, it is expected that the tools needed to perform the job will need to continue to evolve to meet the challenges of preserving information stored in tomorrow's formats.

However, it is possible to take active measures today to preserve current digital content. This is important since, as the BBC Domesday project shows, the longer the problem is put off, the greater the risk of losing information or incurring excessive expense in an attempt to preserve material.

This article outlines a digital preservation solution, including specific knowledge gained by Tessella from working on a number of archival projects for The National Archives, the Dutch Government, the US National Archives and Records Administration, and pharma and scientific organisations.

The solution is based upon the Open Archival Information System (OAIS) framework (described below) and projects undertaken for the organisations listed.

Open Archival Information System: a Solution Framework

In order for different organisations to share digital preservation experiences and learn from each other, it is essential that each solution can be compared.

However, digital archiving is a relatively young discipline and, as such, standards are in their infancy. Nonetheless, ISO are encouraging the development of good practices and have endorsed NASA's Reference model for an Open Archival Information System (OAIS) (see http://ssdoo.gsfc.nasa.gov/nost/isoas/overview.html).

OAIS splits the problems of archiving into six functional entities as shown in figure 1. These are

1. Ingest. This covers the issue of getting records into an archive, including the capture of appropriate metadata to allow them to be found, extracted and meaningfully used in many years' time.
2. Data Management. This covers the controlled editing of data input into the system.

3. Storage. This covers the issue of physically storing records in an archive, including the creation of an appropriate backup policy, regular media migration etc.
4. Access. This covers two related aspects: finding records within the archive and disseminating them to consumers. This includes ensuring that the appropriate information is only disclosed to appropriate users of the system.
5. Preservation Planning. This involves ensuring that the contents of an archive remain more than just a meaningless bit-stream.
6. Administration. This covers the running of the system itself including its maintenance

Tessella has experience of building practical archival solutions that cover each of these functional entities. In particular, Tessella has built both the UK Digital Archive and a file format repository (called PRONOM) to the UK National Archives' specification after open tenders. This article discusses the key lessons learnt as a result of this experience.

Figure 1: Schematic view of the OAIS model

Ingest

For a digital archive to be effective, material must be ingested into the archive. This requires material to be selected, stored in an appropriate structure, and described by appropriate metadata.

Selection of records

Before archiving a set of potential records, it is necessary to decide whether they are worth keeping. One option, of course, is to archive everything. However, the cost of archiving is large: archiving a file is a commitment to keep it for an exceedingly long time (potentially in perpetuity) in a managed, well-maintained environment. In some cases it may not be possible to archive everything for security, intellectual property, legal or other reasons.

The ideal situation would be to review all material, decide what needs to be archived and reject the rest. However, manual selection is also an expensive process. Thus, it is currently only practical to select records at a high level (e.g. to accept all records associated with one project and reject all records associated with another).

Longer term, it is likely that tools to help with this selection will evolve, using technologies that can assess the usefulness of potential records based on their characteristics or derived content. These tools may need to decide not just which files to keep, but also which parts of an individual file to keep.

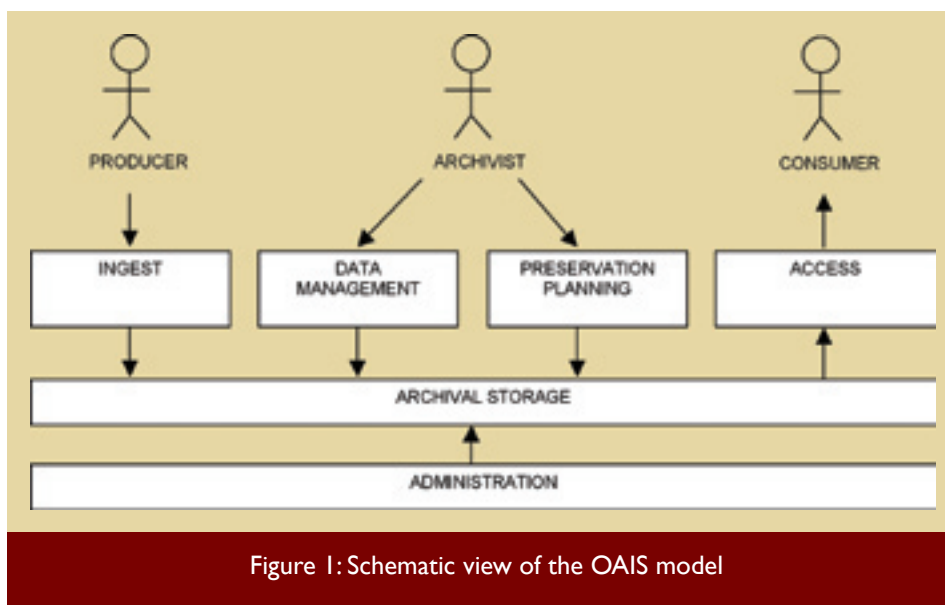For example, imagine archiving the records created by

a prominent individual. In the world of paper records, a selection decision might be taken to archive official documents but exclude, say, post-it notes. However, in the world of digital records, this distinction is potentially more difficult as both these types of records may have been sent by email and thus be stored in a single physical file.

Some current digital archives will only select records for preservation if they are created in (or first converted to) a set number of formats. This can work well if it is possible to tie the archival system to the system used to create and manage these records.

A demonstration of this principle was created by the Dutch Government's Tested project where Tessella produced an email add-in to Microsoft Outlook that allowed users to make use of their email almost as normal, but saved sent and received emails as XML documents, thereby ensuring that the format of the files was fit for future preservation.

Another example is a project to archive thesis abstracts (e.g. a Scandinavian project called DiVA uses custom-created input forms to capture the records to be archived).

However, it is reasonable to assume that data record producers will continue to use technology (and thus file formats) that match the purpose for which they are creating the record. It is thus unlikely that long-term preservation will be a major factor in this decision. Hence, a generic archival solution, although it can influence formats, will realistically be unable to impose absolute restrictions.

The Structure of Records

Records tend to be hierarchical in nature. The ingest process has to allow archivists to choose the most appropriate logical

- **Records of the Committee**
  - **Sub-committee1**
    - **Agendas**
      - **Agenda 1**
      - **Agenda 2**
      - **. . .**
    - **Minutes**
      - **Minutes 1**
      - **Minutes 2**
      - **. . .**
  - **Sub-committee2**
  - **. . .**

Figure 2: Possible conceptual structure of a record

structure for records. For example, an accession such as the records of a committee might be logically structured as shown in figure 2.

The records to be archived will consist of physical files, which may also have a hierarchy that will need to be preserved. For example, if a snapshot of a website is archived, it is important to preserve the folder structure so that the internal links of the site will continue to work.

The physical hierarchy is more a function of current technology than conceptual content structure. For example, the minutes of a set of meetings could be stored as:

• A series of word processor documents. In this case there is likely to be one physical file per meeting
• A dedicated database to hold all the minutes of the meetings. In this case there might be a single physical file covering the entire set of meetings
• Part of a large enterprise-wide database. In this case, the record might be a part of a series of files associated with a record at a higher level of a conceptual record hierarchy

Thus, it is important to realise that the conceptual and physical hierarchies need not be intricately linked. Therefore, it is important to allow archivists to assign a conceptual hierarchy to the records in an accession independently of the physical hierarchy of that accession.

This implies that an archive should allow some files to be shared between records even if they are not associated with a higher-level record. (In this case, although the file can be retrieved as a part of any of these records, it should still only be stored once to prevent version discrepancies).

Metadata Extraction

As part of the ingest process, it is necessary to ensure that appropriate metadata is captured. This metadata falls into two main broad categories: technical and descriptive.

Technical metadata allows future consumers to learn to use the records and enables archivists to take active measures to preserve them. Most of this technical metadata can be derived automatically using appropriate third-party software, e.g. to automatically determine the file format of most of the ingested files.

This can then be matched against known combinations of application software, operating system and hardware that the consumer will need in order to be able to interpret these formats. This mapping can be provided by PRONOM, an on-line repository of formats created for the UK National Archives by Tessella (see below).

Descriptive metadata allows future consumers to understand the records. For paper-based records, archivists have traditionally provided manually-created, detailed descriptive metadata to accompany the records and allowed consumers to find the records they require.

It is obviously possible to do the same for digital records but the sheer quantity of these records (and the fact that it is necessary to use appropriate application software, operating systems and hardware to view them) means that this is potentially a bottleneck in the ingest process.

Ideally, this metadata would be held with the records at the point that they are created, and then updated when they are edited (e.g. through the use of a records management system). However, this is unlikely to be the case for existing digital records.

An alternative is to try to create this metadata at the point of archiving, ideally automatically. However, this is much more difficult than extracting technical metadata owing to the lack of

appropriate software tools and the fact that (as described above) the relationship between a record and its physical file structure is potentially complex.

Such tools would need to, for example, be capable of reliably searching through a number of files to produce a précis of their contents in a few sentences. Also there will be some contextual metadata that should be stored as part of the archival record (e.g. the background to why a certain document was produced or why it became important), which may not be contained in the actual physical files (and thus cannot be extracted).

There are two potential solutions to this problem.
1. Develop better automatic extraction tools. Whilst some progress is being made in this area, the field of data mining is still young and it is likely to be some time before effective tools of this nature become mature
2. Rely less on such traditional finding aids for digital records and use other methods (e.g. an internet-style, content-based search engine). This option exploits one of the advantages of digital records: it is possible to search within such records, and it is a method that is becoming increasingly accepted by end users.

However, even if advanced cataloguing and indexing techniques are used, it will still be preferable to offer the consumer a brief summary of the record so they can assess its potential usefulness before they are required to view, download or request the files making up that record. Also, this style of searching works well for text-based documents but is less easily applicable to images, databases etc.

Data Management

In a digital archive it is important that users are not given unauthorised access to the records. In particular no one should be able to edit the archived files. However, approved users should be able to edit the metadata about the records (e.g. to add extra information or to correct spelling mistakes). All metadata entry and editing should be audited so that it is possible to work out who changed what, and when each change occurred.

In addition:
• Many records will need to be accrued over time, so extra files must be able to be added to an existing series of records
• Migration of files should be allowed. In this case, it is advisable to always retain the original, but, if a record has undergone a series of transformations, it is not strictly necessary to retain every intermediate format. This will be discussed in more detail later
• Some records will contain information that not all users will be authorised to see. In such cases, it may be possible to create a redacted version of the record consisting of files with the secure information removed. This, in essence, leads to the creation of another sibling record of the original. In general, there is no generic way of performing this redaction and thus it may be necessary to return to the original application in order to edit the files

Storage

One of the key aspects of an archive is to ensure that the records are stored securely and safely. Fortunately, the core of this problem is not especially challenging, as millions of organisations that retain their digital information from day

to day can testify. There are, however, some unusual features needed in an archive.

It is important to recognise the difference between the metadata (which can change) and the actual digital files (which are invariant). One way to resolve this issue is to store the metadata and files separately (e.g. in an XML-enabled database and a separate file store respectively). This means that the responsibility of keeping the links between the two must be performed by the archive.

The alternative is to store the metadata and the files together as one object, in order to ensure that they cannot become separated and to simplify backup issues. However, this can lead to the creation of unwieldy large objects, and it makes the editing of these records a potentially complicated process since it involves a large retrieval and subsequent upload, and it is then necessary to perform extra safeguards to ensure that only the metadata has been changed.

Everything that is ingested into the archive must also be backed up and stored off-site. There are a number of options for doing this but all face the same slightly unusual issue: the material to be retained is invariant.

As the archive grows in size, running a full overnight backup of the system, say once a week, may not be a realistic option, and thus appropriate backup policies have to be developed that take into account the ingest rate and the relative difficulty of re-ingesting information (e.g. all information added on a given day). It is also important that the backup policy keeps the metadata and the data synchronised (if these are stored separately)

Creating lots of copies does not by itself ensure that files are safe, hence the storage system needs to actively manage its holdings and ensure each and every file held is being appropriately cared for. This means there needs to be an automated program of checks taking place, e.g. regular checks of checksums, exercising tapes to prevent them from sticking and ensuring regular maintenance occurs before there is a problem. There are a variety of commercial systems on the market that help perform such functions

The amount of information to be stored is often vast. One option to reduce the volume is to perform guaranteed loss-less compression. The argument against it is that this results in a loss of redundancy, so the impact of losing a data bit is high, but a key requirement of an archive should be to ensure that a single bit is never lost: and there should always be another copy of every file from which to restore.

The storage system needs to guarantee that each file

has not been changed whilst it has been in its care. This can be achieved by the creation (and subsequent verification) of checksums for each file.

However, this is really an application-level issue since it is best to create a checksum quickly in the ingest process (so that the protection it offers applies as soon as a file enters the archiving system), and to verify that checksum just before dissemination. Some systems might decide to build-in digital signatures in addition to a checksum.

However, the advantage of relying on just a checksum is that the technology required is simpler and openly available (checksum algorithms are freely published). The advantage of a digital signature is that it provides additional information about who verified the contents of the file, although this can also be provided by the archiving system itself and recorded in an audit trail

Access

Access to an archive involves searching for records and delivering them to the end user. Use of any or all of the services described in this section could incur a fee, and it would thus be the responsibility of the archive software to ensure that appropriate payment was received before allowing access to a fee-bearing service.

Finding records

There are two ways in which consumers can find records: open searching and browsing through catalogue hierarchies. The ability to perform these tasks will depend on the indexing and cataloguing that has occurred as part of the ingest process.

Typically, when searching, users will enter a search criteria and then be presented with a prioritised list of possible 'hits' showing a brief summary of the records that match that criteria. Users will then be able to refine the search to home in on the record they want. Alternatively, users may be able to browse through a catalogue in order to locate records.

Having chosen the record they want to see, the consumer should have the option of viewing more detailed metadata about this record (assuming this descriptive metadata has been created at ingest). As well as allowing the consumer to ensure that they have found the correct record, this information may contain important contextual information that is needed to correctly interpret the contents of the record to be retrieved.

They may also be shown some technical metadata so that they can ascertain whether they are capable of physically using the record (e.g. do they need specialised application software or a long since obsolete operating system?). The issues that this

latter point throws up are discussed in more detail later.

When searching for records, it is quite likely that consumers would want to perform a single search to find all the available material on a given subject, regardless of whether it is stored digitally, on paper, or even in which archive it is stored (e.g. whether it is stored in a national or a regional archive). There are two ways of enabling such a search:

1. Retaining a central index containing all the relevant metadata. This option will probably give consumers the fastest response, but it means that the organisation responsible for maintaining that index has to store a lot of information, ensure that it is all in compatible formats and keep it up to date

2. Distribute the search using Web services. In this case, the archive that receives the consumer's request would send out a series of sub-requests to each registered archive asking it to perform an automated search of its holdings, based on the consumer's criteria, and return a list of hits each with a numerical relevance score.

It would be necessary for all the archives to agree the format of the search criteria (e.g. using an agreed XML schema) and agree a scoring scheme for the hits (although these could then be potentially weighted according to which archive they are stored in).

Once all archives have replied (or a pre-specified timeout has expired) the consumer will be presented with the amalgamated and sorted list of hits. If more detailed metadata is requested on a remote holding, this could be obtained by another Web service request or by re-directing the consumer to that archive

In both cases, the user would probably need to be re-directed to the archiving hosting the material for dissemination.

Disseminating Records

The simplest way of disseminating records is simply to allow the users to download the records (either in their original or a migrated format). However, some downloads will be large so it may be more practical to allow users to request a posted copy (e.g. on a CD).
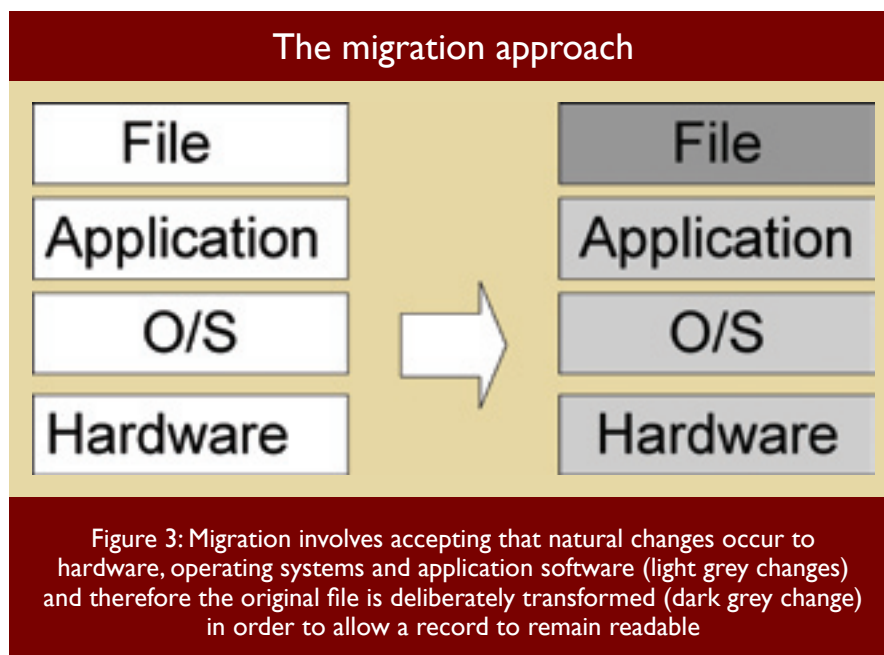
Both of these methods have the disadvantage of requiring consumers to have appropriate client-side application software to interpret the file formats. Thus, a third option is to create presentation-ready versions of records (e.g. converting word processing documents into HTML) and display these directly to the users.

Preservation Planning

It might be tempting to conclude that the lesson to learn from the Domesday projects is that organisations should simply print everything that is important to them and then store the paper records or, if space is a concern, to store the information on microfiche.

However, this would lose many of the potential advantages offered by digital records, such as the ability to maintain security, verify authenticity, as well as the ability to make verifiable copies, easily edit a document (if required) and search within a document. Further, for some records, such as databases or virtual reality models, it is not possible to create a printed version that captures all the relevant information. Better solutions must be found.

These solutions fall into three categories, each of which is discussed below. All solutions have one fundamental thing in common: the original files in a record are always maintained for as long as the record needs to be retained.

Figure 3: Migration involves accepting that natural changes occur to hardware, operating systems and application software (light grey changes) and therefore the original file is deliberately transformed (dark grey change) in order to allow a record to remain readable

The Museum Approach

One possibility would be to maintain the old hardware and software used to create the data in the first place. However, this is not very practical. Such a solution would require the maintenance of every combination of hardware and software required, and the hardware would become increasingly expensive to upkeep and would eventually become irreparable. This is really only an interim measure.

In this technique, a copy of the original is transformed into another, more modern format that can be read by newer application software (potentially running on updated hardware with a newer operating system).

For instance, scientific data in a bespoke binary format may be transformed into a document conforming to an XML schema, which (as it is self-describing and based on very simple low-level technology, i.e. it is fundamentally just a simple text file) is less vulnerable to obsolescence.

In more complex cases it may be necessary to perform a series of transformations over the lifetime of the data, either because of a change in the available application software or because a better transformation engine becomes available. In such cases, it is normally preferable to return to the original file and transform this into the new format, rather than transform it from the previous migration (as this will potentially already have lost some of the information in the original).

To make this approach easier, it would be best to restrict

the number of formats by moving towards standardisation. One example where standardisation has worked is in image formats where specifications such as TIFF have been almost universally adopted by software manufacturers as they have realised that there is a larger overall market if images can be readily exchanged.

In some cases, such as in colour specification, manufacturers have actively collaborated (forming the International Colour Consortium) to make standardisation happen. While standardisation has many attractions, the commercial companies that create the majority of application software in use today are unlikely to follow this route unless there is a competitive advantage to be gained.

Also, it is worth remembering that it is not always trivial to translate records from their current formats into a standard format, as such a transformation may require archivists to make assumptions about the intentions of the original author(s).

Migration need not occur just for preservation purposes, it could also occur to allow easier presentation. For instance, if a digital record consists of Microsoft Word files, a consumer could choose to download the records to their local PC and read them using a locally-installed copy of the software.

An alternative would be to create an HTML rendition of this file and display this to the consumer instead. Third-party products exist that will perform such migrations for a number of formats with a reasonable degree of integrity.

The fact that migration involves a transformation, which may result in loss, means that it is necessary to understand and categorise this loss so that different transformation software can be assessed and compared. The attributes that need to be considered can be split into five categories:

1. Context. This is set by metadata and thus is unaffected by migration (although the migration process should itself be documented)
2. Content. A good transformation should preserve all the content of the original. However, sometimes the new format will not allow information to be kept in exactly the same form
3. Structure. It is important to remember that, if an accession undergoes migration, for either preservation or presentation purposes, the logical (technology-independent) structure will be preserved, but the physical (technology-dependent) structure may be altered as not all

migrations will lead to an exact 1-to-1 file correspondence.

This means that migration is potentially a complex process and as such could be prone to human error (e.g. marking a file incorrectly as having been superseded by a newer version).

4. Appearance. It is quite hard to preserve the look and feel of the original when performing a migration. For most purposes, this may not matter too much but there is not always a clear-cut distinction between appearance and content.

For instance, if an author uses bold or italics at some point in a document, it is probably an emphasis and thus can be interpreted as being part of the content of that document

5. Behaviour. One of the advantages of digital records is that it is possible to manipulate the information within them. For example, database records can be queried to provide new views of the information contained within them or a model can be re-run using different initial parameters.

This aspect of a digital record relies on programming logic embodied in the application software and is thus difficult to preserve by migration. One of the key aspects of preservation planning is ensuring that the strategy for data types is reviewed regularly (e.g. a strategy for a given data type, that is relying on the use of a given piece of application software, will need to be reviewed if support for that application ceases).

The emulation approach

Figure 4: Hardware emulation involves accepting that natural changes occur to hardware but makes no change to the original file, application software or operating system. Enabling the software to continue to run requires the creation of an emulator (dark grey change) to emulate the original hardware on the new hardware

This means that there is a requirement to maintain a repository of information about each file format stored in the archive, to assist archivists in determining its best preservation strategy (e.g. to plan when each format will need to be migrated).

This strategy may evolve with time as better technologies become available. With assistance from Tessella, the UK National Archives has created such a library (called PRONOM), designed to share information with other archiving organisations and to allow anyone to submit information on new formats (see <www.nationalarchives.gov.uk/pronom/>).

The ideal scenario for a large archive would be to automate the migration process. The process would then work something like this:

• An archivist updates the file format repository to state that migration of format XYZ is now required and that the approved policy is to migrate to format ABC using a
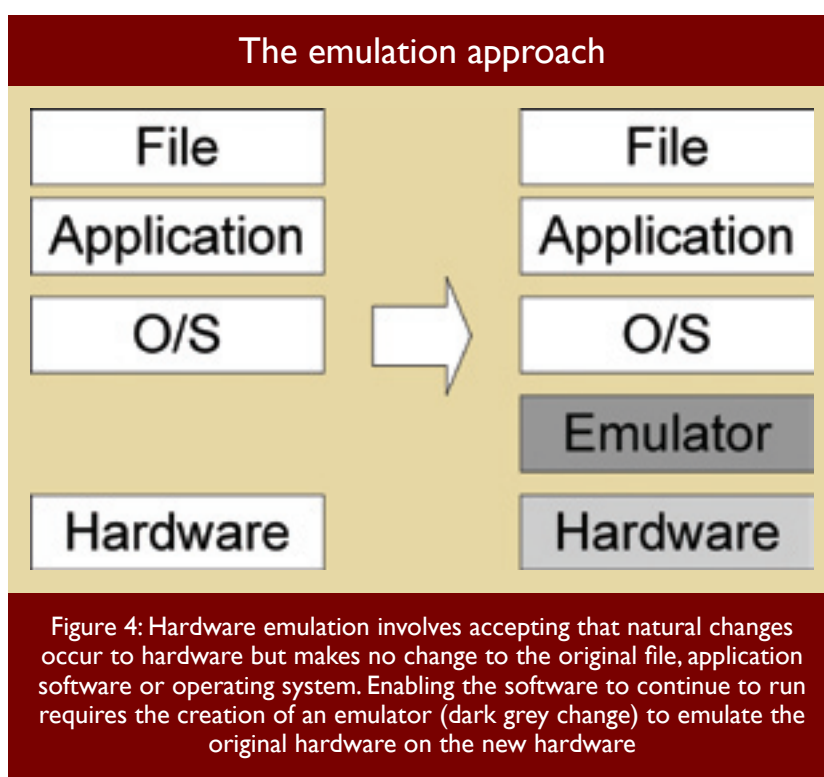
specified piece of software

- The archive automatically detects the update and calculates that this will require x hours' worth of processing time
- The archive schedules this processing to occur at relatively quiet periods (e.g. over the next few nights or a weekend)
- The migration takes place automatically. Humans need only be involved to provide a quality check (although even this process could be assisted by appropriate software tools)
- An alternative to migration is to use emulation. There are variations of this technique but the most promising would seem to be hardware emulation where the original file, application software and operating system are retained but, since it is accepted that hardware will become obsolete over time, the original hardware is emulated in software on new hardware (see figure 4)

This technique potentially has an advantage over migration in that it should allow the look and feel and behaviour of the original application to remain intact (whereas these are potentially lost in migration). This will be especially helpful for records with a high degree of behavioural content (e.g. virtual reality models).

Also, for a given piece of hardware, such an emulator can be written once and re-used by many organisations (although an emulator may need to be re-written when hardware changes again). However, such generic emulators do not yet exist, thus the concept cannot yet be seen to be a proven universal approach.

The approach also means that licensed copies of the original application software (in fact a record may rely on lots of applications to operate as originally intended), and the original operating system, must be retained, including the relevant bug fixes, service releases etc.

It also means that the effort required to access an old record could be considerable, since the original application software and operating system must be installed together with the emulator before the record can be meaningfully interpreted.

There are alternative emulation methods:

Operating system emulation. In this case, we retain the original file and application software and accept 'natural' evolution of both the operating system and the hardware.

Application software emulation. In this case, we retain the original file and accept 'natural' evolution of the application software, operating system and the hardware.

Neither of these seem as feasible as hardware emulation (see the summary of the result of the Dutch Government Digital Preservation Testbed project for more details: <www.digitaleduurzaamheid.nl/bibliotheek/docs/white_paper_emulatie_EN.pdf>).

Administration
Day-to-day running of a digital archive involves many tasks that are very similar to those required to keep any other large software system running. In particular, it is important to remember that all such systems require a combination of process (e.g. standard operating procedures etc.) as well as product (the actual hardware and archiving software).

However, building and maintaining a digital archive also poses some unique maintenance issues that need to be addressed during design and development. These are discussed below.

Future-Proofing
The point of a digital archive is to keep digital material for a long time (potentially in perpetuity). However, one of the reasons that digital preservation is a problem is that the lifetime of most software and hardware is very short: typically just a few years before it becomes obsolete.

It is thus unrealistic to think that the software and hardware required to run the archive will last without needing significant alteration over the lifetime of the archive. To help with this, careful attention must be paid when designing an archive to provide a system that is as future-proof as possible.

Software Issues
The first step is to use a well-established framework as a benchmark for the design of the archive. Users of archives will normally expect an interface based around Web technology (even if the archive is not released on the internet), so assuming that this is the case, an archive should be built using a standard n-tier architecture using one of the two well-established frameworks currently in operation:

- J2EE (Java 2 Enterprise Edition). This is an open standard owned by Sun. This means that application server providers using this framework (e.g. Oracle, BEA and IBM) must guarantee that their servers comply to a basic standard, although they are free to add proprietary extensions. Thus, although porting application servers is not a trivial job, it should be achievable. Most J2EE application servers are available for both Windows and Unix operating systems
- Microsoft's .NET framework. This is not an open standard, but is now well established and is likely to continue to be supported in the foreseeable future. It can currently only be used on the Windows operating system

The following diagram (based on the Tessella design for the UK National Archives' Digital Archive) illustrates the required strict demarcation between the various application layers:

Figure 5 illustrates the second step needed to help future-proof the software in an archive: the design must be exceedingly modular with clearly defined interfaces between each component. This allows one component to be easily swapped with another without affecting the rest of the software.

A third and related feature of digital archive software is that any third-party components used, must have a well-established 'sunset' policy (i.e. before any component is used it must be clear how that component could be retired and swapped with an alternative component).

This can be achieved by wrapping the interface of the component in such a way that it creates a buffer between the main components of the archive and the third-party software, which insulates the former from a change in the latter.

This enables a new version of the same component, or a completely different component that performs the same job, to be switched for the third-party component without affecting the rest of the application. This modular policy must also apply to the interface, with software used to control the storage of the digital files.

Operating System, Hardware and File Storage Issues
Clearly an archive will need to run on real computers and thus

will need to interact with real operating systems and hardware. However, there is no reason for any of the software to be tied to a particular operating system, and this should be avoided. This is one of the main reasons for choosing J2EE over .NET.

A larger issue is the hardware on which the actual files are stored. Migrating data from an old storage medium to another is a well-established technique, but the sheer quantity of material in a digital archive poses some potential problems.

This means that a program of migration will need to be started well before the planned retirement date of any equipment in order to ensure that all the migrations required can occur in time.

Metadata Storage Issues

The metadata about all the records in an archive are best held in XML. This provides a format that is likely to last well into the future and will be readily understood, and is also independent of the exact nature of how it is stored, which will make migration easier.

Such metadata should be captured by the user interface or imported from another source (such as record management system) and converted into an XML file compliant with the archive's XML schema. This is then likely to be appended to automatically extracted information (e.g. virus check details) as the ingest process occurs.

This metadata is probably best stored in its native XML format (e.g. by using an XML-enabled database), although some denormalisation may be required to allow quick access. This metadata can then be extracted for editing purposes or converted to HTML for viewing by the user.

It is also important to have the ability to extract a full accession comprising all its XML metadata and every archived file. This functionality can be used to replicate full records between non-networked digital archive instances or to migrate the data forwards into a new system.

Procurement of Tools

There is a need for many specialist software tools to enable the effective use of digital archives. For instance, the automatic selection of records for ingest, the automatic extraction of descriptive metadata from records at ingest, and the migration from some formats to another all require high-quality software, which is not currently available, to be developed.

There are a number of ways in which this software could be procured by organisations that need to perform archival activities. Organisations could:

Develop bespoke software themselves. This is very expensive and would result in lots of organisations repeatedly procuring similar software.

Rely on open-source software. Open-source software can solve a number of problems but it is important to realise the limitations as well. The kind of software tools needed here must be produced in a timely manner, fit into a controlled framework, be of a verifiably high quality and be supported.

It is possible that open-source software can solve a few of the problems listed above but it is unrealistic to think that all the software required can be procured in this way.

Buy commercial software. The software market for these type of tools is in its infancy, but as the importance of digital preservation begins to be realised more widely, the market is likely to grow.

The digital archives in existence at the time of writing have almost exclusively been built for national archives or national libraries. These institutions do not have the resources to develop their own software, nor can they afford to wait in the hope that open-source software will come along.

However, one pro-active role that such institutions could play is to establish benchmarks for best practice. For instance, if a piece of software is produced that performs a migration from one format to another, these benchmarks could be used to assess the ability of this software to produce a new file that faithfully reproduces various features of the original format.

If such benchmark scores became recognised by the rest of the software world, as a measure of the worth of this software, it would drive manufacturers to improve the software and thus provide an ever-increasing variety of quality archival tools. iQ
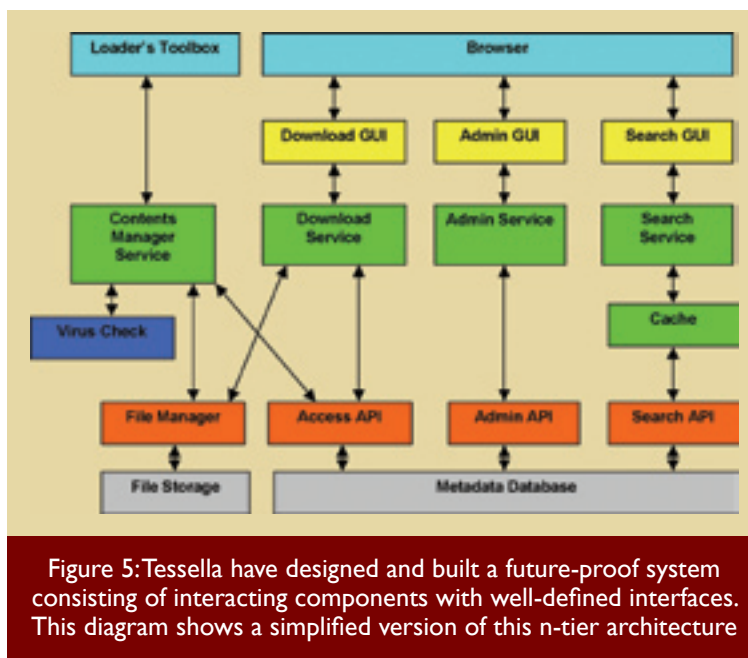
Figure 5: Tessella have designed and built a future-proof system consisting of interacting components with well-defined interfaces. This diagram shows a simplified version of this n-tier architecture

The Author

Dr Robert Sharpe of UK consultancy Tessella has spent the last three years working mainly on digital archiving projects. His contribution to the emerging field of digital preservation includes the specification, design and development of the UK National Archives' Digital Archive and PRONOM systems, consultancy on the US National Archives and Records Administration's Electronic Records Archives system, and consultancy for the Dutch National Archief.

Burned CDs Not a Long-Term Option

Want your self-burned data and images to be preserved long term? A German physicist and data storage expert says that burned CDs only have a very short life span and are not a good storage option.

IT journal *PC World* reported on January 10 that Kurt Gerecke, a senior scientist with IBM Germany, said that, unlike original pressed CDs, burned CDs will not last long. He says that cheap, discount store CDs have a life span of around 2 years, while better quality discs will retain content for up to 5 years before degrading. Neither offer a viable long-term solution.

The digital degradation problem, says Gerecke, is to do with the recording surface on CD-R and CD-RW discs. Made of a layer of dye, this surface is modified by heat to store data – hence the term 'burning'. Over time, the data shifts on the recording surface, until a CD reader's laser beam is unable to read it.

Even hard drives present storage problems, says the German expert. The hard disk is not the problem, it's the disk bearing, which wears out.

CD life can be extended a little by keeping your CDs in a cool dark place. But, says Kurt Gerecke, the best electronic data storage option is magnetic tape, which will last between 30 and 100 years, depending on its quality.

But the key lesson is that no current electronic storage medium has an infinite life span, and a digital migration plan is essential. Gerecke warns that organisations should have "an archiving strategy that allows them to automatically migrate to new technologies."

The alternative is a dead-end. "For those sitting on terabytes of crucial data," says Gerecke, "that could be a colossal problem."

BEST BETS

Make Searching a Sure Thing

By James Robertson

While much can be done to improve the quality of search results, no amount of tweaking of metadata or search configuration will ensure that the most relevant results always appear at the beginning of the list. This is where search engine 'best bets' come in.

Best bets are a hand-created list of key resources for common queries, and they can dramatically improve the search experience, particularly on in-formation-rich sites such as in-tranets.

Presenting Best Bets

In the CSIRO screenshot shown above, the staff member has searched for 'organisational structure'. The first section highlights the intranet page 'CSIRO or-ganisational structure'. Below that, the rest of the 4821 matching search results are presented, most of which just include the words 'organisa-tional structure' somewhere in the page.

This initial featured page is not listed by chance. Instead, the intranet team specifically marked it in the search engine for the phrase 'organisational structure'.

The Value of Best Bets

As the size of the site grows, so does the number of matching search results. The challenge is then to ensure that the most useful pages are listed right at the beginning of the list.

In most cases, however, users are only ever looking for a few key pages. For example, users entering 'annual leave' are either looking for the leave form itself, or the leave policy.

Recognising this, search engine 'best bets' provides a hand-created list of key matches for common searches. These are presented prominently at the beginning of the search results, followed by the rest of the matching pages.

Implementing 'best bets' is one of the most effective ways of improving the quality of search results, as well as allowing the Web team to raise awareness and visibility of key corporate documents and policies.

Creating and Managing Best Bets

Search engine 'best bets' are implemented using a simple database that contains search terms, and matching best bets.

Efforts in creating best bets are then targeted by reviewing the 'most popular searches' report, (see my article Intranet Search Reports at www.steptwo.com.au). Starting with the most popular searches ensures that the greatest value is initially delivered.

Ongoing effort should then be set aside on a monthly basis to review and add entries. This allows the effectiveness of the search to be steadily enhanced over time.

Technology Options

Ideally, the ability to enter and manage 'best bets' is built directly into the search engine. A simple interface should then be provided to cre-ate new entries.

Unfortunately, at the time of writing, few search engines provide support for 'best bets' out of the box. If a new search tool is being purchased, this should therefore be a selection criteria for the chosen product.

When working with an existing search product, it may be necessary to custom-develop the 'best bets' capability. Experience has shown that this is generally not a major piece of coding. It should then be fairly straightforward to implement this as an extra 'layer' on top of the normal search engine results. iQ

The Author

James Robertson is the Managing Director of Step Two Designs, (www.steptwo.com.au), a Sydney-based vendor-neutral consultancy specialising in intranets and content management. James has written extensively on these topics, and has spoken at conferences globally.

Objective Sign On to Again Sponsor *IQ* Article of the Year

After sponsoring the inaugural 2004-2005 *IQ* Article of the Year Award, Objective Corporation has once again become the sponsor of the award for 2005-2006.

The award was inaugurated to encourage RMAA members to put fingers to keyboard to share their thoughts and experiences with *IQ* readers, and to reward them for their article-writing efforts. Publication in *IQ* also contributes to Association member status upgrades.

Tony Walls, Asia Pacific CEO of the Objective Corporation, a leading ECM provider, says that supporting *IQ* and supporting the award are important ways of supporting our industry.

"*IQ* has gone ahead in leaps and bounds over the past year or so, we hope that this award again encourages quality contributions from RMAA members and industry luminaries,"

Objective

**IQ Article of the Year
AWARD**

he remarked.

"Our involvement with the RMAA, with the magazine, and with the award also allows us to keep our finger on the pulse of the industry."

All articles by RMAA members published in the journal between November 2005 and August this year automatically become eligible for the 2005-2006 award. A judging panel will select a shortlist, which will be published in the August 2006 issue.

The winner of the next Objective *IQ* Article of the Year Award will be announced at the 23rd RMAA Convention at Cairns in September, with the details appearing in our November 2006 issue. IQ

2005 Hamer Awards Announced
See Industry News, page 11, for details

Weren't at the 2005 RMAA Convention? See What You Missed, on DVD

22nd RMAA Convention Proceedings
FREE to RMAA members and registered Convention delegates via the RMAA website: www.rmaa.com.au

Order NOW!
Oz Freecall: 1800-242611
NZ Freecall: 0800-400625
Email: admin@rmaa.com.au

R·M·AA
Records Management
Association of Australasia

3 Unforgettable Events on a 2 DVD Set:
The Simkos, the Education V Experience Debate, and Jon Doust's 'Humour in the Workplace'

1 The inspirational and emotional live 'From the Dust of 9/11' presentation by Robert and Alison Simko
2 The great RIM debate – Education versus Experience
3 And Jon Doust's hilarious motivational presentation.

'*One of the funniest thirty-minute motivational presentations you'll see. Move over John Cleese. Jon Doust is terrific!*'
STEPHEN DANDO-COLLINS, EDITOR OF IQ MAGAZINE

$70.00 incl p&p (Plus $7 GST for Australian purchasers)
RMAA members receive a 30% discount = $50.00 incl p&p
(Plus $5 GST for Australian purchasers)

RMAA Snapshot: Kate Walker,
Chief Executive Officer

Kate, who was appointed RMAA CEO on August 1, 2003, has long-standing RIM industry experience, and previously held executive positions on the Association's National Board.

Kate's mandate is to provide executive support to the Board of Directors, to consolidate the strategic objectives set by the Board, and above all, to continue the Association's commitment to representing the unique needs and interests of its diverse membership.

Her qualifications include, Master Business Administration, Bachelor of Science (Business Administration), Advanced Dip Business (Recordkeeping), Advanced Dip Business (Strategic Management), Cert IV Training and Assessment and Company Directorship. She calls beautiful Binalong Bay on Tasmania's East Coast home.

TRUE CONFESSIONS

IQ asked Kate some personal questions:

A little known fact about you? I breed labrador retrievers.

Goal yet to be achieved? A weekend with the family, with the computer turned off.

Word that best describes you? Dedicated.

The thing you like best about your job? The challenge, and impacting the profession.

The thing you least like about your job? Mediocrity. People can be as successful as they want to be, and a little more time and effort can make a huge difference in someone's career.

The most important lesson you've learned? Trust. But verify. And, patience.

Your motto for life? I have two. 'Everybody can say what they want, but everybody can't do what they want'. And, 'The harder I work, the luckier I get'.

Your greatest fear? Not being able to dream.

The award/honor you're most proud of? I'm most proud of earning the respect of the Board and members - for giving them some guidance and the opportunity for the RMAA to develop into a peak professional body.

The book that has influenced you most? The 7 Habits of Highly Effective People, by Stephen R Covey.

Your favourite movie? I don't watch a lot, so haven't got a particular favourite.

Your favorite restaurant/dining experience? Anything seafood or vegetarian.

Your favourite holiday spot:? Binalong Bay in Tasmania's Bay of Fires - recently voted 2nd best beach in the world. When you're hardly ever home, this seems like a holiday spot.

Your favourite way to spend free time? Free time? What's that? But I do try and coach my daughter at athletics, and provide school-based traineeships.

What vehicle do you drive? Subaru WRX.

Your essential business philosophy? Change can be positive. And I like to let people focus on what they do best. I believe that what drives people is the value of loyalty.

Your tip for maintaining a competitive advantage? Be creative, and maintain a sense of urgency about everything you do, and have fun doing it. Also, know the market, and know what to offer prospects that will help them achieve their business goals.

Your personal measurement of success? Employees and members being happy and pushing in the same direction, and the continuous growth of the RMAA for the benefit of the members. **iQ**

CALLING FOR SUBMISSIONS

Publish Your RIM Case Study

The RMAA is seeking records and information management Case Study submissions from government agencies, private companies, academics and individual consultants to be considered for inclusion in a prestigious new sister publication to *IQ* to be published in 2006.

Share your valuable experiences, lessons and insights with your RIM colleagues. All practitioners in the field are welcome to submit proposals. RMAA members whose case studies are published will have the work credited to their CPD status.

Australia and New Zealand are considered RIM world leaders. Here's your chance to show why. If you have recently managed or are managing an interesting RIM implementation or training project or a related project such as disaster recovery, your industry peers will benefit from your experience, while you enhance your reputation.

Interested? You can download a proforma from the RMAA website, www.rmaa.com.au. Or, to discuss a potential submission, contact:

Kristen Keley, RMAA Marketing & Event Manager, marketing@rmaa.com.au
Or, Stephen Dando-Collins, Editor, *IQ* Magazine, editor.iq@rmaa.com.au

R·M·AA
Records Management
Association of Australasia

iQ

A LUFTWAFFE ALBUM

From the Baltic to Berchtesgaden, a Photographic Record of the War of a Secretary to a Nazi Leader

In 1939, 19-year-old Lucy Wolf was conscripted into the Luftwaffe, the German air force. Over the next 6 years she went from a Baltic backwater to the Berlin office of Reich Marshal Hermann Goering, then to Berchtesgaden and arrest by the SS, finally escaping from an American POW camp. As STEPHEN DANDO-COLLINS writes, she recorded those years in an album with photographs little bigger than postage stamps.

In the 1950's, Lucy Wolf migrated to Australia, living in Melbourne, then Tasmania, before finally settling on the Gold Coast. I interviewed her for the local and national press in 1978, and it was then that she shared some of her photographs with me. Her photo album, and the tattered red silk scarf of a downed British bomber pilot, were her only physical mementos from the war years.

She had been conscripted into the Luftwaffe in 1939 at her home town of Wismar on the Baltic, and initially worked as a secretary at the local Luftwaffe barracks. Her father, Fritz Wolf, was a sergeant in the Luftwaffe, playing clarinet in the band of the 61st Flak Regiment. In 1941, Fritz went with his unit to Crete, which Luftwaffe paratroopers had just captured at great cost from Allied troops including Australians and New Zealanders.

In November 1942, Lucy was transferred to the air force high command, the Oberkommando der Luftwaffe, or OKL, at Postdam, outside Berlin. There she became secretary to the chief of the Transport and Supply Department, General Langemeyer. Lucy was promoted to captain. Most OKL secretaries held this rank, to keep them separate from junior ranks due to the top secret nature of their work.

With typical German efficiency, every document that passed through Lucy's hands had to be logged in a record book and signed for, so that document location and movement could be tracked. Working hours were 9.00 am to midnight, seven days a week, with only occasional time off. In the evenings, reports came in from the Luftflotten, the Air Fleets, on every front, detailing movements, losses, etc, which Lucy and her colleagues had to process for High Command meetings next day.

Reich Marshal Hermann Goering, Hitler's number 2, was head of the Luftwaffe and Air Minister, and Lucy saw him regularly at the Potsdam HQ. By late 1942, the German 6th

Army had been surrounded by Soviet forces at Stalingrad, and the Luftwaffe was struggling to keep Goering's promise to Hitler to supply it from the air.

To control Eastern Front air operations, the OKL forward element, code-named Robinson, moved to Goldap in East Prussia, where it operated from an armoured train on a rail siding. Lucy and fellow OKL staff slept in their offices, sustained by a daily ration of champagne from France and midnight fry-ups.

During Operation Kettle, the Stalingrad airlift, more than 540 German aircraft were lost to Russian fighters, flak, and the appalling winter weather. At one point a number of Luftwaffe aircrews refused to fly on what had become a suicide mission, and Goering ordered eight cargo plane crews put before a firing squad for mutiny. Lucy Wolf had to type the order for their execution. Goering refused to sign the order himself; he made the head of the Transport Department, General Langemeyer, do it.

Then, when Stalingrad fell in early 1943, Goering made General Langemeyer the scapegoat for the failure of the airlift, sacking him. The general handed his job over to his deputy, a colonel. But before Langemeyer went home to his estate in Silesia, his staff gave him a farewell party in the snow-covered car park beside the armoured train.

When, in 1978, I sent Lucy Wolf's photographs of that party in the snow to the photographic editor of the London *Daily Telegraph*, he snorted that such a German party was "impossible," ignoring the record of the event which he held in his own hands.

During their time in East Prussia, Lucy and a group of her colleagues were given time off to visit the Kaiser Wilhelm Palace and Goering's private hunting lodge at Rominter Heide

Lucy Wolf in 1939, the photo from her official German ID papers

(Rominten Heath). The lodge featured stuffed wolves shot by Goering as Master of the German Hunt. Its walls were lined with the finest art from across Europe, most of it purloined. The lodge even had a private cinema. The bulky Reich Marshal's cinema chair was so large that Lucy and two of her girlfriends could sit in it together.

As 1943 progressed, the Russians advanced west, and the OKL staff were pulled back to Potsdam. Before long, Lucy was summoned to the Air Ministry in Berlin, where, to her astonishment, she was given the job of secretary to Reich Marshal Goering himself for four weeks while his regular secretary was ill. Lucy found him professional, correct, frustrated by Hitler and those around him, but still able to sit on the corner of a desk and crack jokes.

Shortly after returning to her OKL job, Lucy earned herself a medal. Early one morning, after a full night at her desk, she was cycling through the trees from the camouflaged two-storey OKL building in the forest to the Potsdam hotel where she was quartered. From the trees stepped a British bomber pilot who had been shot down overnight.

He pulled a gun. Lucy pulled her Mauser service pistol. But, using her schoolgirl English, she was able to talk him into handing over his pistol and accompanying her to a nearby guardhouse rather than be shot by a trigger-happy patrol - the forest, home to the top secret OKL, was swarming with troops. Before he was marched off to a POW camp, the grateful airman gave her his red silk scarf as a memento.

Two weeks later, Lucy was summoned back to Goering's office in Berlin – to receive the Iron Cross, Second Class, for 'capturing' the pilot. Goering smiled on seeing her. "You again?" he said.

Soon after, Lucy met a German airman named Ernst on a rare night out at a Potsdam restaurant. His last name was

Above: The document recording **Lucy Wolf**'s May 1, 1945 discharge from the German air force at Berchtesgaden. The stamps and notations were made by German authorities in places she passed through after her escape from an American POW camp.

also Wolf, and they immediately hit it off. A major, he was a night fighter ace and squadron commander. After a whirlwind romance, they had a traditional German wedding at her home town of Wismar, travelling to the church together in an open, horse-drawn carriage as was local tradition. One night two weeks after they were married, Major Wolf was shot down and killed. Mrs Wolf never remarried.

After Stalingrad, she had known that Germany would lose the war. Now she just put her head down and did her job, knowing that people who asked too many questions were arrested and never seen again - as happened to several of her OKL colleagues. In late 1944, she went west with Robinson when it was transferred to the Rhine to oversee the airforce's part in the German offensive that became known as the Battle of the Bulge.

As a part of that offensive, on New Year's Day, 1945, the Luftwaffe launched Operation Floor Slab. Surprising the Allies, the OKL put 1,200 aircraft into the air and destroyed 350 British and American aircraft in a single day. But the Germans lost a similar number of aircraft that day. The Allies could quickly replace their losses, the Germans could not. It was the Luftwaffe's last hurrah.

In February, as all Luftwaffe training schools were closed and their instructors were sent to front line units, and the Russians closed in on Berlin and Potsdam, the OKL was transferred to Berchtesgaden, 1,700 metres up in the mountains of Bavaria. Then, in April, Hitler ordered the OLK back to Berlin. Lucy and her comrades drove for four days and nights in a long truck convoy to reach the capital, only for Hitler to change his mind and order them back to the mountains.

By that time the Russians had surrounded Berlin and the roads south were cut, so the OKL personnel had to fly out. Just one Berlin airport, Gatow, remained open. Lucy was on the second last aircraft to escape the capital. The Ju52 'Auntie' cargo plane ahead of hers was shot down in flames by Russian guns as it struggled into the air - several of Lucy's girlfriends, fellow secretaries, died in the wreckage.

Next page, clockwise from top left: Sergeant **Fritz Wolf**, Lucy's father, in the doorway of a Ju52 'Auntie' transport aircraft, Crete, 1941, after the island had been captured from ANZAC troops. The Luftwaffe barracks at Wismar, 1940. Touring to the Kaiser's palace, East Prussia, 1942. Hermann Goering's hunting lodge, Rominter Heide, East Prussia, during Lucy Wolf's 1942 visit. **Lucy Wolf,** in hooded coat, with fellow OKL staff , Kaiser Wilhelm Palace in East Prussia, 1942; the officer second from left was a **Captain Stumpff**, a fighter pilot shot down and badly burned during the Battle of Britain and later given an OKL desk job. And, the band of the Luftwaffe's 61st Flak Regiment; Lucy Wolf's father was a clarinetist in the band

A LUFTWAFFE ALBUM

A LUFTWAFFE ALBUM

Top, and middle: Lucy Wolf's photographs of the 1943 OKL farewell party for General Langemeyer in the snows of Goldap, East Prussia. London's Daily Telegraph would later declare such a party "impossible". The bareheaded officer clowning in the blanket in the top photograph was the colonel who replaced the sacked general, and became Lucy Wolf's new boss. **Bottom, right: General Langemeyer**, scapegoat for Goering's failed Stalingrad airlift

One of the three engines on Lucy's 'Auntie' was hit and caught fire, but the pilot managed to put it out by diving for the ground, and then flew the plane to Salzburg in Austria. From there, the OKL survivors were trucked back to Berchtesgaden. Both Hitler and Goering had retreats at Berchtesgaden, and Goering joined his staff there.

In April, Goering, who was Hitler's nominated successor, attempted to take over from the Fuehrer and negotiate a surrender with the Allies. In response, Hitler's chief aide Martin Bormann ordered the SS to arrest Goering and his staff. Lucy Wolf was dragged from her bed at the Haus Geiger Hotel at Berchtesgaden by Schmeiser-wielding SS troops.

Lucy spent two weeks as a prisoner of the SS, seeing Goering under SS guard in a railway tunnel sheltering from a USAAF air raid - he was saluted and cheered by his former personnel. While Lucy remained in SS custody, a Luftwaffe flak unit soon freed Goering. He would surrender to the US Army in May.

The Americans were sweeping down through Bavaria, virtually unopposed. When, on May 1, they entered Berchtesgaden, Lucy Wolf and her colleagues were released from SS detention, only to be placed in a US prisoner of war camp in the town. She was formally discharged from the Luftwaffe that day – her discharge notice is shown on these pages.

Soon, bored and worried about their families, Lucy and two fellow Luftwaffe secretaries decided to escape from the POW camp. The three of them drew straws, and the loser (not Lucy) offered 'sexual favors' to a young GI guard, who subsequently let the trio slip out the gate one night, after the German surrender on May 8.

Lucy tried to walk home to Wismar, but on reaching the Elbe on roads clogged with refugees from all over Europe she heard that the Russians were in her home town. So she turned around and headed west, to the North Sea port of Cuxhaven, where an aunt lived. The stamps and notations on her discharge notice chart her course to Cuxhaven.

She remained in Cuxhaven, resorting to black marketeering to survive, and spending a little time in a Hamburg gaol in 1946 after she was caught by British military police. The judge who sentenced her was one of her customers for black market sausages. Goering was also behind bars, at Nuremberg, where he was found guilty of numerous war crimes. He cheated the hangman by taking cyanide on the night of October 15, 1946.

In the early 1950's, Lucy came to Australia as a migrant, and she worked industriously as a secretary for many years. In a final twist of fate, her partner in later life was a former RAF bomber pilot.

Lucy Wolf's photographs, taken on a Balda box camera and reproduced here from the tiny original sepia prints in the photo album - which she had carried all the way across Germany from the POW camp at Berchtesgaden bound by the bomber pilot's red silk scarf - offer a unique record of life on 'the other side'. IQ

The Author

Stephen Dando-Collins is the Editor of *IQ* magazine and the author of 15 books on a variety of subjects including military history. His latest history of the legions of ancient Rome, Cleopatra's Kidnappers, has just been published in Australia and New Zealand by Wiley.

Coming Up

May is Information Awareness Month

In The May 2006 issue of *IQ*…

UP CLOSE & PERSONAL
Issues that affect the individual

- **DO RIMS HAVE A DISTINCT PERSONALITY?**
- **CREATING A PERSONAL CONTINUITY PLAN**
- **SCRAPBOOKING: THE NEW PERSONAL RECORDKEEPING PHENOMENON**
- **HOW YOU CAN GET ROI FROM RIM**
- **EDUCATION, TRAINING AND PERSONAL DEVELOPMENT**

The Copy Deadline for the **May 2006 issue is April 1**

iQ The ONLY industry magazine that reaches EVERY RMAA member in Australia, New Zealand & the Asia/Pacific

RMAA Directory

Email contacts: To contact RMAA National officers by email, use addresses such as president@rmaa.com.au or secretary@rmaa.com.au

To contact officers in RMAA branches, create addresses from branch initials as below, for example, nsw@rmaa.com.au or qld@rmaa.com.au

National

President	Kemal Hasandedic MRMA	Ph: (07) 4773 8418
CEO	Kate Walker MRMA	Ph: 0409 250 795
Postal	PO Box 276 St Helens TAS 7216	

NSW

President	Toni Anderson ARMA	Ph: (02) 9370 2069
Secretary	Christopher Colwell ARMA	Ph: (02) 9210 3546
Postal	GPO Box 1059 Brisbane QLD 4001	

VIC

President	David Moldrich FRMA	Ph: (03) 9609 2198
Secretary	Dragana Mitrovich ARMA	Ph: (03) 9214 5625
Postal	GPO Box 1059 Brisbane QLD 4001	

QLD

President	Philip Taylor MRMA	Ph: (07) 3365 3140
Secretary	Jennifer Curley ARMA	Ph: (07) 3407 4616
Postal	GPO Box 1059 Brisbane QLD 4001	

WA

President	Trissa Dent ARMA	Ph: (08) 9420 3243
Secretary	Jane Lake ARMA	Ph: (08) 6488 1639
Postal	GPO Box 1059 Brisbane QLD 4001	

SA

President	Helen Onopko ARMA	Ph: 0411 420 012
Secretary	Marie Feltus ARMA	Ph: (08) 8406 8363
Postal	GPO Box 1059 Brisbane QLD 4001	

TAS

President	Kate Walker MRMA	Ph: 0409 250 795
Secretary	Kate Walker MRMA	Ph: 0409 250 795
Postal	GPO Box 1059 Brisbane QLD 4001	

ACT

President	Thomas Kaufhold ARMA	Ph: (02) 6206 4772
Secretary	Amanda Harris ARMA	Ph: (02) 6207 6111
Postal	GPO Box 1059 Brisbane QLD 4001	

NT

President	Joan Sohl ARMA	Ph: (08) 8924 7226
Secretary	Loretta Hempsall ARMA	Ph: (08) 8924 7336
Postal	GPO Box 1059 Brisbane QLD 4001	

NZ

President	Douglas Wilson ARMA	Ph: +64 (0)4 803 1351
Secretary	Sue Macpherson ARMA	Ph: +64 (0)4 439 3357
Postal	PO Box 5643 Wellington New Zealand	

SECURELY MANAGING YOUR MOST VALUABLE ASSET: INFORMATION

National Suppliers of:

↘ Secure document management, storage and retrieval

↘ Active file management

↘ Magnetic media management and storage

↘ Cataloguing, indexing and sentencing

↘ Web based order management and reporting

↘ Document imaging, OCR/ICR and e-Forms

↘ Integrated mailroom solutions

↘ Web based hosting and retrieval of documents

↘ Secure document and media destruction

Quality System

Quality Endorsed Company

ISO 9001:2000 Lic 5550
Standards Australia

QUALITY ENDORSED SUPPLIER TO GOVERNMENT AND INDUSTRY

PICKFORDS 1800 181 800
www.pickfords.com.au