



InfoRMAA  
Quarterly

Vol 24 - issue 2 - May 2008 - issn 0816-200x  
AU \$75.00 for four issues (plus GST)

**FIRST AID  
FOR RECORDS**

**You  
Can't Buy  
COLLABORATION**



**PROTECT YOUR ID ONLINE**

**KEYWORD AAA: NEW POSSIBILITIES**

**UN RECORDKEEPING IN WAR-TORN DARFUR**

**SAFETY, SECURITY, PRIVACY**

We Interview Data Security Specialist James Turner

Enterprise Content Management with one surprise.



**People want to use it.**

The greatest challenge of any ECM project is getting everyone to use it. Changing the way people work will always be difficult. At Objective, we concentrate our research and development efforts on addressing this challenge. We've designed software that's easy to use and our solutions help people get their work done faster and easier.

Since 1987, Objective has provided government and top 1000 companies across the globe with ECM solutions that people want to use. Again and again.

When ECM is on your to-do list put Objective on your short list. [www.objective.com](http://www.objective.com)

**Objective**

# iq

## inforMAA Quarterly

Vol 24 – issue 2 – May 2008

OFFICIAL JOURNAL OF THE  
RECORDS MANAGEMENT ASSOCIATION  
OF AUSTRALASIA

### EDITOR: Stephen Dando-Collins

Fame & Fortune Pty Limited, Editorial Consultants

Email: editor.iq@rmaa.com.au

Postal Address: Editor, IQ

PO Box 317 POTTS POINT NSW 1335 Australia

Contributing Editor: Michael Steemson

Art Director: Nathan Devine,

Comperation Group Pty Ltd

### EDITORIAL BOARD

Kristen Keley (SA)

Michael Steemson (NZ)

Philip Taylor (QLD)

### 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.

### COPYRIGHT & REPRODUCTION OF MATERIAL

Copyright in articles contained in *InfoRMAA Quarterly* is vested in their authors. Most editorial material which appears in *IQ* may be reproduced in other publications with permission gained through *IQ*'s Editor.

### ADVERTISING

Comperation Group Pty Ltd

Aarti Karande

(02) 9954-9000

aartis@comperation.com

### ANNUAL SUBSCRIPTIONS

\$75.00 (plus GST) per annum for 4 issues (including postage), from:

### Membership & Financial Services

RMAA Office

PO Box 276 St Helens TAS 7216

P: 1800 242 611 F: 1800 333 802

### IQ ONLINE ARCHIVE

Copies of articles published in *IQ* since 1984 are available at the Members Only section of the RMAA website, in the *IQ* Article Archive. Complete back issues from February 2005 are available electronically at the Members Only section of the RMAA website.

The Members Only section of the website can be accessed with RMAA membership, or, outside Australia and New Zealand, with the purchase of an *InfoRMAA Quarterly* annual subscription.

### DISCLAIMERS

Acceptance of contributions and advertisements including inserts does not imply endorsement by the RMAA or the publishers. Unless otherwise stated, views and opinions expressed in *InfoRMAA Quarterly* are those of individual contributors, and are not the views or opinions of the Editor or the RMAA.

### RMAA WEBSITE

<http://www.rmaa.com.au>

*IQ* Magazine is produced for the RMAA by Comperation Group Pty Ltd, PO Box 391, North Sydney, NSW 2059. Editorial management by Fame & Fortune Pty Limited.

Comperation Group

Bell Awards 2005 Best B2B Magazine (CO magazine), Finalist

Bell Awards Year 2004, Best Small Publisher of the year, Highly Commended



## In This Issue

### President's Page

4

### Kate's Column

5

### Editorial

6

### Industry News

8

### IQ Interview

Data Security: Why Old-Fashioned Ideas  
Just Don't Hack it Anymore: James Turner

12

### Safety, Security, Privacy

How Safe, Secure and Private Are We?  
Finding Answers During Information  
Awareness Month

18

### Protect Your ID Online

20

### Public & Private, Sunshine & Reign

26

### RIM Around the World

When Recordkeepers Are Peacekeepers:  
Managing the Records & Information of a  
UN Mission in War-torn Africa

28

### Collaboration

You Can't Buy Collaboration

37

### RIM Tools

First Aid for Records

40

Keyword AAA: Finding Potential Opportunities  
For its Application Within a Financial Reporting  
Framework

44

### EDRMS

Information Seeking Behaviour of EDRMS  
Users: Implications for Records Management  
Practices. Part 3

48

### Book Review

Who Are You, and What Do You Want?

??

### Awards

56

### RMAA News

58

### RMAA Directory

62

### Front Cover:

May is Information  
Awareness Month. With  
safety, security, and privacy  
of information highlighted in  
this issue, check out Protect  
Your Identity Online: it  
makes fascinating, and scary,  
reading. See page 20.





# Safety: Security: Privacy

How wonderful a world it might be if we could enjoy these 3 concepts and conditions with certainty and conviction.

**D**on't get me wrong. The place we live in does not compare with Afghanistan, Iraq, Burma (yes I am old), Darfur and any number of other countries where the fight for these 3 above mentioned ideals is intrinsic to those peoples' wellbeing.

Do we, as records and information managers, have a role to play in ensuring our collective well-being for those we represent? I have often advocated the importance and value of what we do, and congratulate each and every one of you who fights the good fight. For, as many of us can attest, as a profession, I believe, we are proactive rather than reactive.

But issues that impact on RM such as those enshrined in our holy trilogy - 'transparency, accountability, and my favourite, integrity' - can fall out of the spotlight. We use the Enrons and HIHs as examples of bad practice, but do they still have the same impact they once had? I believe we have to be the champions of ensuring the holy trilogy is current and relevant to our respective organisations, and to the collective.

Queensland, back in the days of 'the white shoe brigade', had the unfortunate situation where government kept files on individuals. Even when the practice was aired publicly, we were assured that those files were destroyed - because they were considered no longer relevant. Imagine the surprise when more of these 'destroyed' files came to light years later! 'Ancient history' many may say. What's the relevance today? Well, we have evidence of poor practice occurring today.

Take the US Patriot Act. Being learned individuals, I'm sure you're well aware of the stated reason behind it - the need to secure the safety and security of US citizens and assets. Note I did not mention privacy.

Our history is littered with examples of the citizenry offering up certain freedoms to our elected leaders in times of crisis, freedoms inherent to our system of values and belief. We expect those leaders to protect us by whatever means necessary.

Fear is, and has, been well used to suborn our personal rights. The challenge is for us to ensure systems of checks and balances are in place to ensure they are not abused 'for the greater good.'

I read recently: 'Some other organisations

are banning Google's innovative tools outright to avoid the prospect of US spooks combing through their data. Security experts say many firms are only just starting to realise the risks they assume by embracing Web-based collaborative tools hosted by a US company, a problem even more acute in Canada where federal privacy rules are at odds with US security measures.'

<http://www.theglobeandmail.com/servlet/story/RTGAM.20080324.wrgoogle24/BNStory/Technology/home> (Accessed 4/4/08.)

Yes, at national and state levels we have privacy principles and legislation in New Zealand and Australia, to protect our personal information and privacy from unauthorised invasion and abuse. Unfortunately, we continue to see headlines about people in public office being dismissed or demoted for infractions of these laws. Our consolation, I guess, is that the systems in place caught these people after the fact. That surely counts for something?

Has your organisation considered the collaborative tools offered by Google? Are there systems in place to ensure the data and information you manage is protected from access and tampering? The answer to this is obvious to me, considering the astute and savvy professionals within our community. But how strong are those same policies and processes when you involve external providers who are given to access your data?

There has been an interesting discussion on the listserv recently, on RFID. Without taking a position, (something totally alien to me, I admit), I will say it was lively and informative. Congrats to all. The importance was in our willingness to ask the question and the generosity of the subscribers to discuss and provide answers. We are fortunate to have the freedom to ask for assistance, and that permits our peers to respond.

Enjoy this issue of *IQ*, and remember that we are the champions to promote and challenge. We can be the vocal minority to remind those around us that safety, security & privacy of our information is our right, to be protected and preserved.

At the same time, let us not forget those in other countries who are less fortunate than us, and vow to help them also protect the safety, security and privacy of their information.

**Kemal Hasandedic,**  
RMAA's National President

**Kemal Hasandedic, FRMA MBII**  
National President and Chair of the Board





**Kate Walker,**  
CEO of the Records  
Management Association  
of Australasia

# From the CEO

I guess the question on everyone's lips is... have the membership fee increased for 2008/2009? Well, the good answer is 'NO', but the even better answer is that we've 'tweaked' the corporate category to allow proxies to attend 'local' events that the nominees are unable to attend.

To see the categories of membership, benefits and FAQ's, please visit the website. Remember, a professional member can still have their membership paid by the employer, and apart from additional discounts, you are taking charge of your own professional development.

Whilst I have spoken before about the value of membership, this edition is a good time to once again provide you with...

## Answers to the Membership Value Question

### What is in it for me?

Since professional associations were first conceived, one of their biggest and most constant challenges has been answering the questions, "Why should I belong? What is in it for me?"

RMAA is no exception. And, in the tradition of professional associations around the world, RMAA answers those questions with a question of its own: "That depends. What do you want?"

### Do you want to become better at your job as a result of access to leading-edge research?

RMAA provides that research, both as an association and through its journals and scholarships. The association has conducted research to benchmark salaries, members, audits, ethics, professional development, etc, which can be used to measure one's own development as well as their organisation's.

Further, RMAA is pursuing publication exchanges with other organisations to increase members' access to the research of others. The RMAA's leading research productions are *IQ* (*infoRMAA Quarterly*) and the online *iRMA*, which bring together existing international standards and case studies into one set of generally applicable and accepted good practices for governing records and information management.

Next up for the RMAA: a series of publications, designed to make valuable toolsets for members and non-members across all jurisdictions and industries. RMAA members not only help create association-generated research, they also receive it first, free or at greatly discounted fees.

### Do you want to support your profession by contributing to the body of work guiding it?

RMAA, through its involvement in Standards Australia (IT21) and, through affiliation with the International Organisation for Standardisation (ISO), defines, develops and promulgates standards and their

associated guidelines and procedures. These standards establish a quality baseline by which other RIM audit and control activities are measured.

### Do you want to increase your value to your employer by expanding your warehouse of skills?

RMAA offers a variety of ways members can add to their RIM governance and control education. Each year, workshops, seminars, conferences and accredited training are held around the world, offering members discounted access to a variety of hot-topic workshops conducted by known instructors.

An International Convention, rounds out the professional development menu each year. RMAA Branches also offer education on a monthly basis, either generated locally or using some of the seminars prepared and packaged by RMAA Headquarters.

Finally, the quarterly *IQ*, provided free to all members, features articles on topics of immediate interest to the records and information management community.

### Do you want to improve your financial position by paying less for publications and events of value to you?

In addition to discounted registration fees to RMAA's many professional development opportunities, the RMAA Shop offers members discounts on its products.

### Do you want to augment your resource base by expanding your network of business contacts?

Membership in one of more than 9 branches and 9 special interest groups (SIGs) with members in numerous countries immediately puts you in contact with a local circle of individuals with similar job responsibilities, questions, concerns and advice.

Expanding the circle outward, attendance at RMAA professional development sessions and conventions brings members face to face with a global community of like minds. And, finally, extending into cyberspace, members can access forums, SIG sites, Internet newsletters, and listservs composed of RMAA members trading questions and counsel on topics of professional interest.

### Do you want to underscore your understanding of the Records and Information Management field by earning a professional credential?

RMAA offers the Professional Member accreditation (ARMA, MRMA, FRMA) designations, which recognise educational and professional involvement achievement in domains of records and information management competence, including standards and practices; organisation and management; processes; integrity, confidentiality and availability; and systems development, acquisition and maintenance, understanding of the intricacies involved in setting up and managing an enterprise wide information.

Continued on page 6

# From the Editor's DESK

May is Information Awareness Month (IAM) across Australia and New Zealand, and in this issue of *IQ* we feature an *IQ* Interview and a number of interesting articles which focus on Safety, Security and Privacy - the theme of IAM in 2008. Our book review is in a similar vein.

The digital world has changed the way we work, spend our leisure time, and, in some respects, how we think. A consistent message that comes through in the Safety, Security, Privacy articles in this issue is that there is a need to protect our information, corporate and private, as never before. The more sophisticated the technology, it seems, the more sophisticated the associated risks. It's a case of 'if you use it, be prepared to lose it.'

This issue also includes an interesting report from Canberra on new possibilities for Keyword AAA, and a discussion of the role of IT and RIM in collaborative projects. We also wrap up the 3-part series reporting a study on EDRMS user behaviour.

And, I defy you not to laugh at least once when you read 'First Aid for Records.' Not at the author, but with him.

We also have an exclusive article from a UN recordkeeper working in Darfur in Africa in the wake of the

civil war there. If you thought your work environment was difficult, put yourself in this RIM's shoes! And, as RMAA President Kemal Hassandedic says in his column in this issue, spare a thought for the people in various parts of the world for whom security, safety and privacy are mere dreams. And spare a thought, too, for the RIMs who are working to turn those dreams into reality. Keeping records, it turns out, is one way to bring justice, peace and freedom to war-torn lands.

## LOOKING FOR SUBMISSIONS ON EDUCATION & TRAINING

We have held over our planned feature on the subject of RIM education and training until *IQ*'s August issue. And we still have capacity for additional editorial submissions on the subject. If you have a case study to tell, a view to express, an educational programme to promote, send me an email to discuss. Advertising space is also available to educational providers.

**Stephen Dando-Collins**

Editor

*IQ* Magazine

editor.iq@rmaa.com.au

## CORRECTIONS

In the February issue of *IQ* we inadvertently attributed authorship of the article 'RMAA Act Branch Helps Shape Territory Records Policy Via ACT Territory Records Advisory Council' to Marian Hoy. The article was in fact written by Veronica Pumpa. Apologies to both.

The Gremlins also found their way into the post nominal department in the February issue, promoting David Pryde to FRMA and demoting Kristen Keley to ARMA. For the record, both David and Kristen are in fact MRMA's.

FROM THE CEO:

Continued from page 5

RMAA Professional members receive a substantial discount on the attendance at professional development events (plus a membership discount).

### **Do you want to position yourself for participation in a global marketplace?**

RMAA's international membership is a perfect place to learn more about cultures, priorities, practices and preferences different from your own. Maybe you do not work in a global business today. But what about tomorrow? Jobs change and employers change. Don't be left behind as the world shrinks.

The wise employee is prepared for possibilities before they become actualities. Membership in RMAA, which has identified for itself a vision of being 'The recognised leader in professional development, research and networking for the benefit of records management professionals' is a good place to start.

### **Do you want to help support the continuation of your profession in the years to come?**

Members' support of the association helps ensure that research takes place, so that the next generation of records and information management specialists take their place in the workforce fully accredited.

### **Do you want to prepare yourself for management responsibility?**

RMAA offers members the opportunity to practice leadership skills through its branches, chapters and its boards, committees and task forces.

Also available to leaders is the RMAA-sponsored Branch Leadership Day, offered in conjunction with each RMAA Convention, at which best practices -- which feature many of the same leadership and management skills required on the job -- are thoroughly reviewed and described.

Information. Standards. Certification. Education. Research. Global Presence. RMAA provides it all.

Why should you belong? Because professional success requires professional resources. As the leading source of records and information and expertise worldwide, RMAA is the professional resource for success in the records and information management field.

**Kate Walker**

FRMA MAICD AMIM MBA BSc  
(BAdm) AdvDipBus (Rkg), DipBus(Adm)  
**RMAA Chief Executive Officer**  
kate.walker@rmaa.com.au

## National

President  
Email Kemal Hasandedic FRMA  
khasandedic@gmail.com

CEO  
Email Kate Walker FRMA  
kate.walker@rmaa.com.au  
Postal PO Box 276 St Helens TAS 7216

Ph: 0409 250 795

## NSW

President  
Email Toni Anderson ARMA  
toni.anderson@asic.gov.au  
Postal PO Box 276 St Helens TAS 7216

## VIC

President  
Postal Debbie Prout ARMA  
PO Box 276 St Helens TAS 7216

## QLD

President  
Email Peta Sweeney MRMA  
psweeney@legalaid.qld.gov.au  
Postal PO Box 276 St Helens TAS 7216

## WA

President  
Email Lisa Read White ARMA  
lisalex@iinet.net.au  
Postal PO Box 276 St Helens TAS 7216

## SA

President  
Email Bonita Kennedy ARMA  
bonita@bigpond.net.au  
Postal PO Box 276 St Helens TAS 7216

## TAS

President  
Email Cathy Fyfe ARMA  
cathy.fyfe@utas.edu.au  
Postal PO Box 276 St Helens TAS 7216

## ACT

President  
Email Stephanie Ciempka MRMA  
Stephanie.ciempka@dest.gov.au  
Postal PO Box 276 St Helens TAS 7216

## NT

Contact  
Email Anastasia Govan MRMA  
agovan@whitehorsestrategic.com  
Postal PO Box 276 St Helens TAS 7216

## NZ

President  
Email Julia Harris ARMA  
Julia.harris@nzqa.govt.nz  
Postal PO Box 5643 Wellington New Zealand

## STAFF

Marketing & Events Manager  
Email marketing@rmaa.com.au

Ph: (08) 8281 3302

Membership & Services Officer  
Email admin@rmaa.com.au

Finance & Administration Officer  
Email finance@rmaa.com.au



# Are You a Fox, a Wolf, or a Puppy?

**CANBERRA:** A survey conducted in Britain and Ireland for Australian ECM vendor TOWER Software entitled 'Document Mayhem in the UK and Republic of Ireland' has found that middle managers stepping into others' shoes are frequently stumped by their predecessor's records management practises.

The quantitative study of 300 respondents in organisations with 50 or more employees, conducted by Dynamic Markets for TOWER Software, categorised middle managers as The Fox, The Wolf, and The Puppy, and found that each category reacts differently when confronted with a records management problem.

According to the researchers, the Fox is a middle manager aged 45+ who is wary of those around him or her and doesn't easily trust colleagues. Wise but devious, and a creature of habit, the Fox is very conscious of organisational politics and potential threats to their own position and advancement. The Fox's paranoia is often driven, say the researchers, by having been made redundant in a previous role, or through having fallen foul of those more sly than them.

The Wolf is more prevalent in the UK than in Ireland. Aged 34 to 45, the Wolf has become a team player, perceiving the route to success to

be via working as a pack. A little braver than the Fox, and feeling less threatened, the Wolf will do what is most efficient to get the job done, without worrying too much about personal gain - the pack will bring rewards to all.

The Puppy is a younger member of the team, aged 33 or under. Puppies fulfil junior management roles, and are often still in training, even if they don't think they are. The playful Puppy makes more mistakes than its elders, and is not always aware of those mistakes. Yet it tries hard to please. But in trying to please they sometimes fall foul of the actions of those around them.

The researchers found that when a manager has to assume the role of another executive in the organisation, either as their replacement or to fill in for them while they are off sick or on leave, 32% were unable to find key files, emails, or documents. And, of those, 87% had experienced negative outcomes as a result.

Those negative outcomes included stress, frustration, arguments, and a bad atmosphere among work colleagues. In fact, 40% of respondents said they had become 'extremely stressed' by the inability to lay their hands on the records in question.

The survey found that foxes are hoarders of

files, documents, and emails that they are meant to share with colleagues. Close to two-thirds of foxes interviewed said that they store files the way they do out of long-term habit, with 20% admitting that they deliberately hide files to protect their creative ideas from colleagues. By comparison, only 6% of wolves and less than 4% of puppies act this way.

Conversely, 75% of both wolves and puppies have found themselves unable to locate the current version of a computer file that colleagues have been working on, while the more experienced foxes only had this difficulty in 38% of cases.

When it came to picking up the phone and calling a colleague, customer or supplier to obtain a copy of a file or document they were unable to track down, respondents in all categories showed similar gumption, with 48% of both wolves and puppies saying they would do it or have done it, and 43% of Foxes saying the same.

Says Geoff Moore, Asia/Pacific General Manager for TOWER Software, in a press release announcing the report's findings, "Time is a precious commodity that most busy employees simply can't afford to waste. It's no wonder that colleagues with



poor information management practice are causing office tension.”

To obtain a copy of the ‘Document Mayhem in the UK and Republic of Ireland’ report, contact any office of TOWER Software in Australia or New Zealand.

## Victorian Government Records Management Hammered in Auditor-General’s Report

**MELBOURNE:** The Victorian Auditor-General has handed down a report into the standard of records management in Victorian Government agencies that contains severe criticism of the way public records have been managed in the state of Victoria, with particular blame being levelled at senior management in government agencies for failing to support records management.

The Victorian Auditor-General’s Office (VAGO) is an independent agency that reports direct to the Victorian Parliament. One of its roles is to report on the way public sector records are managed, and in a wide ranging review, Auditor-General Des Pearson has identified major deficiencies in the way Victorian Government agencies manage their records.

In the report, released in March, the Auditor-General specifically identified the lack of senior management support for records management. He pointed out that most Victorian Government agencies had not adopted a strategic approach to records management, and identified significant records management skills gaps in staff, issues that senior agency managers need to address.

Auditor-General Pearson was also critical of agencies for not being pro-active in relation to the management of electronic records including email and websites.

The Auditor-General found that while most agencies indicated they had established records management objectives and policies, further research has shown that these objectives and policies were of variable quality.

The Public Records Office of Victoria (PROV) was also highlighted as lacking in resources to tackle the many issues associated

with managing public records. The Report calls for a more strategic action from the PROV.

According to the Auditor-General, that action should include collection of comprehensive information on the state of records management across public sector agencies, more active engagement in raising awareness of recordkeeping responsibilities by agencies, ensuring that products and services provided remained up-to-date and were relevant for agencies, and ensuring that core recordkeeping activities such as processing records disposal schedules were conducted efficiently.

In response to the report, the Victorian Government has announced a review of the Public Records Act 1973

The full Auditor-General’s report may be found at URL [http://www.audit.vic.gov.au/reports\\_publications/reports\\_by\\_year/2008/20080312\\_records.aspx](http://www.audit.vic.gov.au/reports_publications/reports_by_year/2008/20080312_records.aspx)

## Scots Think FOI is Dragging Information Out of Government

**EDINBURGH:** A survey conducted for the Scottish Information Commissioner has found that, while 57% of people in Scotland think that public authorities would find a way around their FOI responsibilities if they did not want to reveal particular information, 64% believe that Scottish public agencies were nonetheless becoming more open and accountable as a result of British FOI laws.

The survey was conducted by Progressive Scottish Opinion, and is the fifth annual survey carried out for the Information Commissioner.

The RMS *Bulletin* (March 2008), in publishing the research report’s findings, also reported that 69% of respondents felt that more information was available from public authorities than ever before, and that authorities in Scotland were more open and accountable than their counterparts in the rest of the UK.

Of those respondents who had made an FOI request to public authorities, 73% had received everything they had requested.

On publication of the report’s results, Information Commissioner Kevin Dunion expressed concern that, while public awareness of the benefits of FOI was growing, there was a low awareness among young people, the elderly, and those with disabilities.

“We need to ensure that all groups in society are fully aware of their rights,” said Dunion.

## QSA Releases 2 RM Guides for Public Authorities

**BRISBANE:** Queensland State Archives (QSA) has released two new publications to guide public authority records management, one covering metadata standards, the other, planning for an EDRMS.

The ‘Queensland Recordkeeping Metadata Standard and Guideline’ (the Metadata Standard), is designed to guide public authorities on the recordkeeping metadata required to appropriately identify and manage public records in all formats over time.

The Metadata Standard and 4 related Public Records Briefs can be accessed at [www.archives.qld.gov.au/metadata.asp](http://www.archives.qld.gov.au/metadata.asp).

The new EDRMS Guideline highlights some of the recommended tools and environments that should be in place prior to implementation of an EDRMS. It also outlines a number of the key non-technical issues that should be explored prior to system deployment.

QSA’s EDRMS Guideline is available at [www.archives.qld.gov.au/downloads/eDRMS.pdf](http://www.archives.qld.gov.au/downloads/eDRMS.pdf).

## Objective Solution is Hot Property

**BRISBANE:** Property and investment group FKP Limited is implementing an enterprise-wide ECM solution from Objective Corporation.

With operations across Australia, FKP had found that legacy document systems and business processes had created a situation where growth constraints were occurring.

“The business case for implementing a DMS in FKP has identified over \$1 in tangible benefits and avoided costs,” said Laurie Martyn, Business Systems Project leader with FKP in a press release.

Stage one of the system roll-out has begun in all FKP business units and retirement villages. Stage two will involve all offices and construction sites nationally.

The FKP implementation comes on the back of the announcement that the Western Australian Government’s land and property development arm LandCorp has selected an Objective ECM system to take its records management from hard copy to electronic.

The LandCorp WA decision to implement an ECM system was spurred by the fact that the agency’s workload has increased drastically in recent times, with staff levels increasing by 50% over the past 2 years.

## Objective Just What the Kiwi Doctor Ordered

**WELLINGTON:** The Royal New Zealand College of General Practitioners (RNZCGP) has successfully implemented an ECM solution from Objective Corporation as a part of the organisation's move to enhance its information management.

RNZCGP, in addition to an advocacy role for the country's GP's, provides postgraduate vocational education and professional development. It chose the Objective solution to manage its documents, records and correspondence, and also to handle committee management affairs.

The College's previous hard copy system and 130,000 electronic documents had resulted in silos of material both onsite and in an offsite archival facility.

Within six months of initiation, the new Objective ECM solution had brought all RNZCGP records together in a single accessible location.

## Bundaberg Says There's Nothing Rum About RecFind

**BUNDABERG:** Bundaberg Regional Council, a new Queensland local government authority covering an area famed for its sugarcane and Bundaberg Rum, has rolled out Knowledgeone Corporation's RecFind Corporate as its EDRMS.

Bundaberg Regional Council was created following the 2007 decision by the Queensland Government to push forward with their plan to amalgamate local government authorities and centralise their use of technology. The new council incorporates Burnett, Isis, Kolan, and Bundaberg City Shires.

The new entity went in search of a electronic records and document management solution, and after considering many offerings it chose RecFind from Knowledgeone, an Australian company with an international reputation. Both Burnett and Kolan Shires had previously been using the RecFind Corporate Software Suite

The system was rolled out at Bundaberg in March at the time of the formal creation of Bundaberg Regional Council.

## New ACS Boss Wants Greater Recognition and Collaboration



Kim Denham, new CEO of the ACS

**SYDNEY:** New Chief Executive Officer of the Australian Computer Society (ACS), Kim Denham, has called for proactive involvement of the private sector in the information technology industry.

Ms. Denham, who was recruited by the ACS in Perth, WA after a year-long search for a new CEO, took up her Sydney post at the end of February.

The first female CEO of the Society, Ms Denham has 20 years experience in ICT. Previously she was Information Systems Manager with chemical company CSBP, and has also held senior management roles with Ericsson Australia, West Australian Newspapers, and Tourism WA.

"We (the Australian information technology sector) can be extremely competitive on the world's stage," said Ms Denham after her appointment. "But greater recognition and collaboration from the business community is what's required to allow our sector to flourish."

## Germans Get Tough on Data Retention

**BERLIN:** A new law introduced by the German parliament, the Bundestag, is now in effect, mandating the retention of all telecoms traffic data for six months.

According to the *Information Management Journal* (Jan/Feb 2008) the new law, passed by the Bundestag last November for introduction in

2008, requires all communications providers in Germany to retain the records of all phone calls including numbers called, their date, time, and duration, whether they be via landline, mobile, or voice over Internet protocol (VoIP).

Similar records must also be kept for six months on all emails and on Internet access.

The legislation is similar to that now operating in other European countries introduced following a European Union directive to do so in the wake of 9/11 in the US.

## Archives Employee Stole Historic Documents to Pay Bills

**NEW YORK CITY:** An archivist with the New York State Library has been charged with stealing historic documents and artefacts from the library and selling them on eBay.

Fifty-four-year-old Daniel Lorello was accused of systematically stealing Library content since 2002 – accelerating to 400 items in 2007 when Lorello learned that surveillance cameras were due to be installed at the library.

Pilfered items covered the US Revolutionary, Civil and Mexican wars, World War I, Abraham Lincoln and the Roosevelts.

Associated Press reported that Lorella allegedly sold the items on eBay and at trade shows, spending the proceeds on household bills, house renovations, car bills, school fees, and paying off his daughter's \$10,000 credit card bill.

If convicted, Lorello faces up to 25 years in jail.

## BluePoint IBM Lotus Solution Joins Elite VERS Certification Club

**MELBOURNE:** The Public Records Office of Victoria (PROV) has certified BluePoint Content Manager against all 5 specifications of the Victorian Electronic Record Strategy (VERS) standard.

BluePoint is an Australian-owned vendor based in Melbourne. Its BluePoint Content

Manager is an enterprise-wide solution dedicated to the IBM Lotus platform. It is designed to manage the entire content lifecycle from capture to disposal, supporting content types ranging from documents and records to email and images.

BluePoint Content Manager joins a select few EDRMS products to have obtained VERS certification, and is the first IBM Lotus-dedicated solution with certification.

Said Craig McLaughlin, BluePoint's Operations Manager, in a press release announcing the successful completion of the certification process, "Victorian State and Local Government have a large investment in the IBM Lotus platform."

## Breaches of Britney's and Farrah's Medical File Privacy Lead to Medical Centre Inquiry



US actress **Farrah Fawcett**

**LOS ANGELES:** The medical file of actress Farrah Fawcett revealing information about her treatment for cancer, was leaked to the tabloid magazine *National Enquirer*, the University of California, Los Angeles, (UCLA) Medical Centre has revealed. This was only weeks after a similar breach involving the records of troubled singer/actress Britney Spears.

Fawcett, a Hollywood actress best known for her role in the 1970's Charlie's Angels TV series, had been undergoing cancer treatment at the UCLA Medical Centre since 2006.

NBC News reported on April 3 that that UCLA Medical Centre announced that Fawcett's medical records had been leaked to *National Enquirer* magazine by an employee of the Centre, where Fawcett was undergoing cancer treatment.

The breach was discovered after Ms Fawcett had complained to her doctor at UCLA that the *National Enquirer* had reported the fact that her cancer had returned even before she had a chance to tell family or friends about the recurrence. Fawcett had been declared cancer-free in February 2007 after undergoing treatment at the Centre.

Following the complaint, Medical Centre management then conducted an inquiry which identified a Centre employee who had accessed Ms Fawcett's file without authorisation on several occasions and had subsequently passed the contents onto the magazine. The Centre said that it had disciplined the employee, but did not specify what nature that disciplining had taken.

Only several weeks earlier, in March, the UCLA Medical Centre had sacked 13 employees and disciplined others who had been caught looking at the file of another celebrity patient, Britney Spears.

The *Los Angeles Times* reported that the California Department of Health had immediately announced an inquiry into the way UCLA Medical Centre had handled Ms Fawcett's files. A similar inquiry had been launched by the Department following revelations about the Spears incident.

## DocsCorp Now Integrates With NetDocuments

**SYDNEY:** PDF integration specialist DocsCorp has announced that it has expanded its integration capability to include Sofatware-as-a-Service (SaaS) provider NetDocuments.

NetDocuments provides the legal, real estate, financial and health service professions with a solution offering instant access to collaborative documents and email.

Law firms increasingly demand more from their PDF creation and management software, including collation, redaction, electronic filing, Bates stamping, and document binding.

Integration with DocsCorp's pdfDocs Desktop means that NetDocuments users will be able to pull down documents to their local system, convert them to PDF and push them back as new or related documents. Alternatively, users can save documents into NetDocuments as PDFs direct from MS Word.

## State Dept Employees Fired for Accessing Presidential Candidates' Files

**WASHINGTON DC:** Two contract employees of the US State Department have been fired, and a third employee disciplined, after they were detected looking at the passport files of Senators Hillary Clinton, Barack Obama, and John McCain.


Reporting the incident on March 20, NBC News quoted a State Department spokesperson as saying the breaches of security and of the privacy of the candidates were thought to be the result of 'imprudent curiosity.'

It was revealed that internal monitoring systems are automatically tripped when a State Department employee accesses records of high-profile individuals without authorisation.

A Defence Department spokesperson told NBC News that once the monitoring system is tripped an explanation is immediately sought from the culprit, and if the explanation is unsatisfactory a supervisor is notified.

It was via this system that the Department was alerted to the breach of the Obama files initially, with three separate breaches occurring in January, February and March. Breaches of both the Clinton and McCain files were also subsequently discovered.

The State Department told NBC News that every time an employee logs on, he or she must acknowledge that the records they are accessing are protected by the Privacy Act and are only available on a need to know basis.

Outside contract employees who have security clearance are used by the State Department to design, build and maintain the Department's systems. They also provide support to government employees; in the passport area, they support data entry, file searches, customer service, and quality control. 





In some parts of the world, this would  
be considered a firewall



# DATA SECURITY:

## Why Old-Fashioned Ideas Just Don't Hack it Any More

Specialist IT security industry analyst JAMES TURNER tells *IQ* there are major data security issues that you should know about, and be proactive about. Ignore the warnings, and you run the risk of even becoming an accomplice to the crime of the theft of your own ID.

**IQ:** James, you seem to have had a particularly early introduction to computer hacking and IT security issues.

JT: Yes, my IT journey started back in 1986 when my school set up a dedicated computer room with about 20 PCs. And, luxury of luxuries, one of the PCs had a colour monitor - which we had to book time on. At high school and then at university I worked casually assembling computers and helping schools deploy networks.

My first full time job in IT was in a university library, helping deploy 500 PCs which the computer science students were always trying to hack into! That was back in Windows 95 days.

The web hosting company I went to work for had a dedicated security team and it was here that I got a very fast education in the importance of IT security. Windows 2000 was getting turned into Swiss cheese by network worms and spam was becoming a serious problem.

And I was responsible for explaining to some very backward IT managers why we needed to pay £30,000 for firewalls and keep them in Highly Available pairs.

**IQ:** Is it the 'techie' aspect of IT security that fascinates you, or is there more to it than that?

JT: Well, at first I got interested in security because it was my job. It was about locking down PCs at the university so that



IBRS data security analyst James Turner

the computer science students couldn't hack in. Then it was about protecting a central database for 30 pharmacies around Australia.

We were continually confronted by data integrity and availability issues. Working as a UNIX sysadmin gave me a deep and healthy respect for the powers a systems administrator can have over a computer system. If you tell the machine to kill itself, it will.

Latterly, when I was with a software company, because I was dealing with IT managers from our clients every day I got a lot of exposure to the various challenges they were facing - employee fraud, mistakes, data loss, security policy, reasonable usage of email, employees downloading inappropriate material at work.

I got to see it all, and it's really surprising what a human toll it takes on the people who have to deal with the fallout of these issues.

I like dealing with the concepts of security and looking for better ways of doing things, so this is what I do.

**IQ:** A few years back biometrics were trumpeted as the answer to identity fraud, and anyone with a recently issued passport and who travels overseas is familiar with the use of biometrics in passport control. Is biometrics all it was made out to be? Is it a foolproof way of preventing the use of false ID's?

JT: From an ivory tower perspective, biometrics is sensational. But the part that continually creeps me out is the stories you hear of a

*DATA SECURITY: Continued from page 13*

guy who has his fingers cut off so that the criminals can steal his car.

The problem I have with biometrics is that instead of my password or my swipe card becoming a target of attack or theft, the target becomes me: my voice, my eyes, my fingers, my hand geometry, and so on.

Our signatures on the back of credit cards are an interesting aspect of biometrics; it's a credential we use to authenticate ourselves – even though we know that signature forgery is easy.

It's rare for us to place complete trust in what a person says. So we have contracts and signatures. But paper-based contracts are too limited in an electronic world. I need someone in London or New York to be able to trust me right now, not when the letter arrives in the post next week.

When the trust for a credential is broken, we need to find a new credential. This is much harder when the credential is part of your body.

We clearly need mechanisms to authenticate ourselves on the Internet, but this is an immature area. We're still finding our way.

***IQ: How much potential do biometrics have in the broader field of data security?***

JT: Personally, I think that biometrics should be avoided for authentication. I think many areas are trying to run before they can walk.

An area of IT which I think voice recognition, for example, is better suited to, is for inbound call centres. These places are deploying software which is starting to work out your personality from the words you use.

Just the same, while this may make your customer experience better, you don't want this information about your personality stored. The last thing we want is for an organisation to start linking your personality to your bank account.

***IQ: Do you have an association with the Australasian Consumer Fraud Taskforce, and in particular Scamwatch?***

JT: I'm interested in their work, but we don't have an official association with them.

***IQ: Microsoft tout their BitLocker feature, available in select versions of Vista, as a major advancement in identity management, data security, and asset management. Is it all it's cracked up to be?***

JT: It's an interesting question. I was pretty annoyed when I found out that I couldn't play around with BitLocker because I'm using an older laptop which doesn't have a TPM chip on the motherboard.

That instantly means that any organisation that wanted to use BitLocker not only had to upgrade all their laptops and workstations to Vista - a harrowing thought – but they would also have to update the hardware.

I like having encrypted data on devices which get carried out of the enterprise; but I think the requirement to refresh both the hardware and the software is a large hurdle for most Australian organisations.

***IQ: How effective as an online banking security tool is the use of one-time passwords delivered by SMS? And how does this work?***

JT: This is an area that I really like. I did some research into Internet banking and I ended up changing my bank as a result of what I found.

Some of the banks in Australia got around to issuing their customers with tokens which generate six digit PINs when the customer activates the token. This PIN is what we call strong authentication because it is something that only the customer should have – the token – combined with something the customer knows – their password.

This mechanism is much better than a password, but the problem is that if a hacker managed to compromise your computer, they could sit there in the background, let you authenticate to your bank, and then play merry-hell with your money.

The solution I really like is the one deployed by CBA and NAB. They send their customers an SMS which is unique and linked directly to the exact transaction you wanted to do.

So, if I transfer \$1,000 to my mum, my bank sends an SMS to my phone to authenticate that transaction. I then enter that code and the bank has supportive evidence that it's actually me doing the transfer because I knew my password – something only I should know. And I had the SMS - something I had. The genius is that authentication is on the transaction, not the login.

So, if I get an SMS asking me to authorise a transaction and I'm at a pub with friends then I know that someone is in my accounts. But without my phone they cannot transfer money out because they don't have the SMS.

It's a pretty elegant solution. It isn't fool-proof, but it's certainly better than just a password.

Of course this will all get much better once EVM smartcards roll out. Then you'll be able to stick your credit card, with a microchip, into a reader plugged into your laptop. You'll be able to do transactions with even more confidence.

***IQ: What does the federal government's overhaul of Australia's privacy laws mean for those who have to manage personal data within their organisations?***

JT: Well, this is a 'watch this space' issue. We've yet to see what the final amendments will look like, but I think that will be happening this year. The implications – if the Australian Law Reform Commission's recommendations are accepted – will be profound.

Perhaps the most interesting recommendation was for mandatory notification in the advent of a data breach. What this means is that if the shop down the road has your personal data and they believe it's been compromised, then they are obliged to inform you.

This will be a real pain for many Australian companies, but it

will be a massive step in the right direction and brings us back in line with Europe and the US.

**IQ:** Data Leakage Prevention (DLP) is a new buzz phrase in IT security circles at the moment. What is that all about?

JT: Data Leakage Prevention is my favourite piñata at the moment. It's such a load of nonsense. Once again, we're back in the ivory tower. The technology does what it claims – usually – but what the vendors don't want us to notice are the real issues.

DLP is in its infancy and is very hard to maintain. Any security product which has a substantial requirement for ongoing administration is just too much of a resource black hole for IT departments – particularly with our skills shortage. Resources are better applied elsewhere.

Even the DLP vendors will admit that the majority of data which is inappropriately sent outside an organisation is as a result of a mistake. DLP is basically a band-aid intended to stop employees from making careless mistakes.

What would be much more appropriate is good training on how to do their jobs. Outside of IT they call this Due Care, and it's rather important!

**IQ:** IT security experts talk about 'black lists' and 'white lists'. What's that all about, and are they effective as data security measures?

JT: Black lists and white lists are an interesting area conceptually, but they also are directly applicable to everyday life, as well as IT operations.

A black list is something like the FBI's Most Wanted list. You don't want to be on this list, and if you are, then there are severe limits on what you can do. Black lists are appropriate when you only need to single out a few bad apples from the rest of the barrel.

White lists, conversely, are the list you often want to be on. These are the VIP lists. The reservation you place with a restaurant is a form of a white list. Your driver's licence puts you on a white list of people who are licensed to drive a car.

Only people on the white list are permitted to do something. White lists are appropriate when only a few people need to be singled out from the rest of the crowd for permission or favourable treatment.

In the IT world, we talk about applications, email addresses, IP addresses and users being put on black lists – to block – or white lists – to allow. To date, most of the security tools we hear about – anti-virus, anti-spam, anti-malware – it's all anti-something. It's about blocking and preventing.

The problem is that these products are looking to block items which can actually be the majority. It's like having a bouncer on the door, giving them a list of all the names of people in Australia and having the bouncer check every name against the entire list

when someone wants to come in.

My argument is that we should be looking to use white lists more often in IT security.

In most organisations you don't need to install new applications often. So why not use a white list to mandate what can be done, instead a black list to do the opposite?

**IQ:** Not long ago we ran an article about the data security risks inherent in people using portable electronic devices (PED's) away from their offices. How big a problem is this?

JT: This is a sensationally large issue that not too many people are talking about. The challenge is for IT departments to work with their organisation to work out what PEDs the employees should be permitted to use in the network.

I was just chatting with a friend yesterday about this. It was his last day on the job and he'd taken in a removable hard drive to harvest his data from his work computer and server. My friend's company didn't have a policy around this area. Now I'd trust this guy with my life, but how many times is this happening in companies every day around the country?

**IQ:** Are there a few major rules of thumb that PED users should apply, and questions organisations should ask, to limit the dangers of losing or revealing confidential data via these tools?

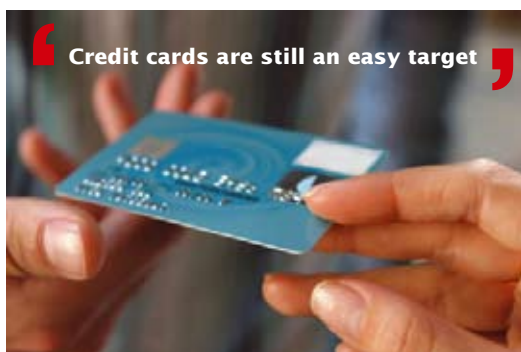
JT: There is technology which could prevent this, but there are more important issues. Does your company have a policy about this, for instance? Do your employees know what data they can carry about on their smartphone? Do your employees understand how serious it could be if they mislaid, or misappropriated, company data?

I was recently told that Australia is the largest market per capita of removable hard drives. This is a serious issue!

**IQ:** We keep hearing horror stories about financial institutions and government agencies around the world losing huge amounts of confidential customer data. Is there a data security device that you would love to see invented that eliminated the risk of this happening?

JT: Well, this is getting into Mission Impossible territory, but a network device which could scan for stolen data and then zero in on the location of the data and the criminals using it would be sensational! I get the impression that some of the law enforcement and defence agencies may already have this capability.

I don't think we can completely stop the data breaches from happening, but if we could shift the risk equation so that the consequences of a criminal using this data were so severe and so inevitable that it became just too risky for a criminal to even bother. That would be great.



**Credit cards are still an easy target**

*DATA SECURITY:* Continued from page 15

**IQ:** People continue to respond to email scams such as fake lottery wins and the famous Nigerian plea for help securing millions of dollars, providing their bank account details and losing their savings. Is there a 'black list' we should all have on our computers to prevent us being scammed?

JT: When people are trained to prevent social engineering – which is what these scams are – we are taught a few basic principles. If it seems too good to be true, it is. If you feel uneasy about something, respect your instincts.

Always, always, always ask to call the person back; get their name and number, then check out the number for the organisation on the white pages. When an organisation calls you, you should not have to authenticate yourself to them, so giving passwords and dates of birth to someone who has called you is silly.

**IQ:** We ran a story several years ago about a major New York bank which lost most of its data on 9/11 because of poor

is extraordinarily high for an analyst firm. This shows the value we deliver in our research and advisory service to Australia. We understand the local issues.

**IQ:** How can good recordkeeping contribute to data security?

JT: Good recordkeeping is essential to most aspects of business function. Security is also a function to support the business. So, let me flip it around and say that good security is vital to accurate recordkeeping.

Having the right person able to make the right change to the right data at the right time; that's a security issue. But it's also directly relevant to record keeping, because I also want to keep an audit trail of who did what, when they did it, how they did it, and who they were authorised by to do it.

**IQ:** What have been the trends in ID fraud and ID security to counter fraud over the past 5 years?

JT: Probably the big one is the increasing acceptance we have for transactions over the Internet. If you think about it, the Internet

## **It's the mistakes, and not the malice, which can carry the greatest risks to data**

backup, while another saved all its data with an emergency backup procedure that electronically transferred it to New Jersey within seconds of the 9/11 attack. What is the biggest mistake organisations make today when it comes to taking steps to secure their data? Inadequate backup? Poor firewalls?

JT: Organisations can make two easy mistakes when it comes to security. The first is not understanding the value of the data and so taking inadequate precautions. The second mistake is in inadequate training. Setting policy is very important, but if people don't understand the need for the policy, or they are not reminded of it regularly then they can try shortcuts.

I'm always reminding people that it's the mistakes and not the malice which can carry the greatest risk to data.

Security, whether it's policy or technology, has to be integrated with the flows. The minute security impinges on processes, people start resenting it, are even tempted to subvert it. Look at airport security. How many people see that as a value-adding aspect of the travel process?

**IQ:** How well does Australia do in the area of data security compared with other developed countries?

JT: It's impossible to measure that comparatively. We do OK for what we have. We can often be told that we're not doing enough to keep up with other countries when it comes to technology adoption. But I think the reality is that Australians are more expedient with their investments.

At IBRS we've got a 92% renewal rate with our clients, which

really only started to get commercial in the mid to late 90s and this means that we're still exploring what we can do.

The more money sloshing through an area, then the more attention it's going to get from criminals. As the famous bank robber said when he was asked why he robbed banks, "Because that's where the money is."

Some of the technology which impresses me is the really high-end analytic software that the banks use to determine, probabilistically, whether the activity in your account is legitimate or not.

So normally you access your Internet banking from a Windows XP machine via an Australian ISP, and you only ever use Bpay. So how come you're now trying to access it from a Linux machine in China, and you're trying to transfer money to Afghanistan? They have this software and it clearly helps.

But there's nothing quite as good as the simple solutions. I think one of the most effective security strategies of the last five years was the release of Windows XP Service Pack 2.

This came out in August 2004 and really helped stabilise much of the madness. XP SP2 delivered enhancements to the Windows firewall, as well as making the firewall active by default. It's going to be interesting to see what Service Pack 3 delivers.

**IQ:** How big is the problem of identity theft?

JT: This is very hard to say, and the answers you get depends on who you talk to. The bottom line for me is that no matter what the fraud rate is per capita, it's still a dreadful inconvenience to each and every victim.



Try telling someone who keeps getting approached by debt collection agencies because their identity has been cloned, that credit card fraud rates in Australia are comparatively low. This is an area where the larger statistics hide the truth. The truth is that any fraud is too much.

**IQ:** Is any area more vulnerable to ID fraud than others?

JT: Credit cards are still an easy target. I've had a taxi try to scam my credit card, and barely a month goes by without me hearing some horror story of a corporate credit card being used to buy a \$4000 handbag in Sydney while the owner is interstate.

**IQ:** What steps can we as individuals take to limit our personal exposure to ID fraud and theft?

JT: People need to keep a closer eye on their credit card. Walk it to the counter to pay in restaurants, be selective over what you use the card for versus paying cash. Have a second credit card with a miniscule limit for Internet purchases.

Get a post box at the post office so you can receive your next credit card in the mail at a secure location. I don't understand why Australia Post doesn't take more advantage of their post boxes.

The bottom line is that it's our own responsibility to take care of our money. It's easy to forget that when we hand someone our credit card, it's as though we were handing them the cash equivalent of our credit limit. What steps should you take before you handed that stranger a few thousand dollars in cash? That's a much easier question to answer for most people.

**IQ:** Thank you, James. Hopefully, our readers will be a lot more security conscious after reading this. 

## An IT Security Identity

After undertaking computer studies at high school and endless tinkering at university, **James Turner** began his IT career in PC support at a university library. He moved on to become a UNIX systems administrator, before working in London for several years as a Hosting Infrastructure Manager.

"It was when I was in London," says James, "that I realised that, while I enjoy the technical side of IT, I am more of a communicator, and I'm much better at demystifying technology for people who weren't propeller-heads."

James was subsequently headhunted by a software company and returned to Australia to work as a customer relationship manager. In 2005 he joined Frost & Sullivan as their Industry Analyst for Security and Services.

"That was a good experience, but I missed talking to IT managers and CIOs who were on the front line. That was, after all, where I'd come from."

At the beginning of 2007 he took his present position at IBRS, in the same capacity. "The depth of experience at IBRS is exceptional. Working with that team is incredibly rewarding."



## HELPING MANAGE INFORMATION EFFECTIVELY

*At Records Solutions we pride ourselves as industry leaders with over 120 years combined experience in the Records, Document, Information and Knowledge Management profession.*

### Our Services Include ...

- ✓ **Records and Information Management Consultancy**
- ✓ **Industry Training**
- ✓ **Records Management Outsourcing**
- ✓ **Archival Services**
- ✓ **Staff Placement**

**Visit Our Website [www.rs.net.au](http://www.rs.net.au)  
Phone: +61 3 9747 3077**

SAFETY, SECURITY,  
PRIVACY



# HOW SAFE, SECURE & PRIVATE ARE WE?

## Finding Answers During Information Awareness Month

By Kristen Keley, MRMA  
RMAA Marketing & Events Manager

May is Information Awareness Month across Australia and New Zealand. The purpose of Information Awareness Month is to increase public awareness of the breadth of the information industry and the importance of properly maintaining good records and information as it relates to everyone from global Corporations through to small business and even the homemaker. In other words, 'connecting information and people'.

**N**ow in its third year, and with the theme of 'Safety, Security, Privacy', the initiative is more relevant in 2008 than ever.

This year's theme is aimed at raising the profile of the importance of good records and information management in light of the increasing prevalence and notoriety of cases involving Identity theft, spam, email scams, sharing of personal information, electronic access of information, electronic banking and credit card fraud. Not simply issues relating to business but also potentially relevant to every individual.

In 2008 the IAM collaborating group welcomed the Public Record Office of Victoria (PROV) as a collaborating body, and were pleased to see that both Archives & Records Association of New Zealand (ARANZ) and Archives NZ have supported the initiative with events during the month.

RMAA are running a Lead-up to IAM tour with international speaker Susan McKinney from the University of Minnesota in the US, joined in many locations by EMC speaker Roger Schmitt from Australia.

A full range of events are being run by RMAA Branches and other collaborating bodies throughout IAM, and you should visit the website: [www.informationawarenessmonth.com.au](http://www.informationawarenessmonth.com.au) to ensure you don't miss out on something special.

Although not one of the collaborating bodies for IAM, the following event came to our attention. Through its focus on disaster preparedness, originally an initiative of the Society of American Archivists, 'MayDay' (May 1) has been adopted by the Collections Council of Australia and is described on their website as follows:

'For the second year in Australia, archives, galleries, libraries,

museums, cultural heritage sites and organisations are urged to perform at least one disaster-preparedness task during the month of May, as MayDay aims to raise awareness about disaster preparedness.

'In 2007, severe flooding on the eastern coast of Australia reminded us of the great risks that natural disasters present to Australian cultural heritage. From the Ash Wednesday bushfires in 1983 and the Canberra bushfires in 2003, to Cyclone Larry in 2006 and other freak weather events, this geologically stable continent is no stranger to environmental emergencies.' Appropriately, 'Mayday' is of course the international distress call.

But there are other types of emergency that we must always be mindful of. From the faulty electrical wiring in the building next door to the impact of burst water mains pipes on basement storage areas – these are real and more likely risks for much of Australia's cultural heritage.


Given human nature, it's easy to put off disaster planning. In 2008, people in cultural heritage organisations are encouraged to act upon one or more of the suggested activities:

- If you have a disaster plan, dust it off and make sure it's up to date or make a timeline for developing one.
- Get to know your local firefighters and police, and invite them to tour your organisation and give you pointers on safety and preparedness.
- Identify the three biggest risks to your collection or heritage site.
- Meet with the people working in the other cultural organisations in your area and find out how you can share resources in the event of a disaster.

Blue Shield Australia has arranged for a series of workshops to be delivered through the Australian Library and Information Association pillar body. Entitled 'Disaster Planning for Cultural Collections', the workshops will be presented in your city by esteemed Conservator, Mr Kim Morris, between May and September.

You can participate in activities associated with 'Business Continuity Awareness Week' between 28 April and 2 May 2008. For more information, go to <http://www.collectionscouncil.com.au>.

The RMAA is a leading IAM partner, and to carry through IAM's Safety, Security, Privacy theme this issue of *IQ* features an illuminating interview with a leading data security expert and a range of authoritative articles on the subject.

This is also a good time to remind you that the RMAA website offers a free copy of our Personal Continuity Plan for maintaining and storing personal and household records in case of disaster. Download your copy today from the RMAA homepage, [www.rmaa.com.au](http://www.rmaa.com.au) 



# PROTECT YOUR ID ONLINE

By Rose Vines

Identity theft is a nasty crime. At its worst, it involves not merely stealing someone's money but also their reputation. It is a crime of stealth: often the victim doesn't know they have been targeted until well after the crime occurs. As both a RIM and an individual Internet user, you need to know how to protect your ID online.

Once an identity thief has enough details about you, he or she can use that information to make purchases, apply for credit, rent property and go about in the world masquerading as you. Your stolen identity can be used as a cover for other illegal activities, too.

Identity thieves operate by stealing personal information – your address, phone numbers, passwords, tax file number, account numbers, purchasing history and so on. They can get that information offline in the ‘real

world’ or online, in the virtual world.

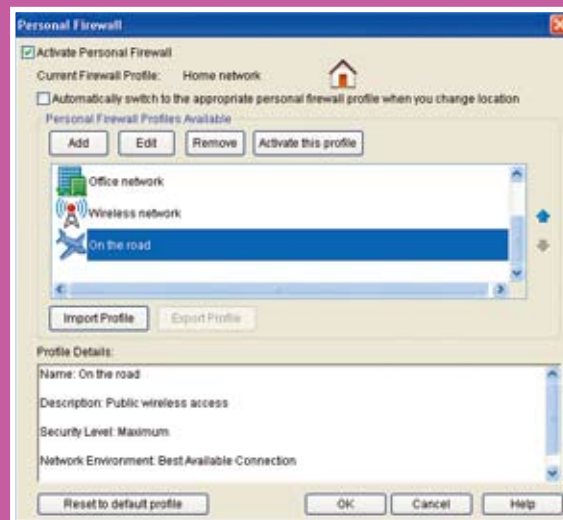
As the number of services and amount of information we store online increases, so, too, does the incidence of identity theft. The Internet is fertile ground for the crime. The interconnectedness of all our computers makes us vulnerable, while the impersonal nature of online transactions provides perfect cover for someone trying to pass as someone else.

The Internet is also a place where fake identities are commonplace: people use them all the time when they participate in social networking sites such as Facebook, enter

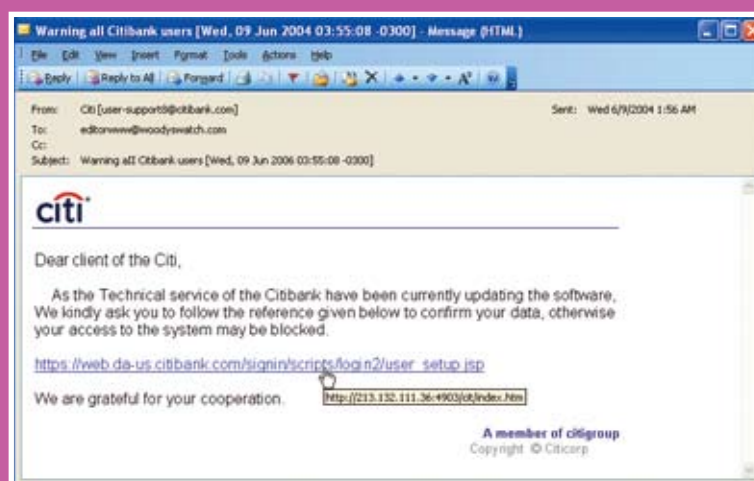




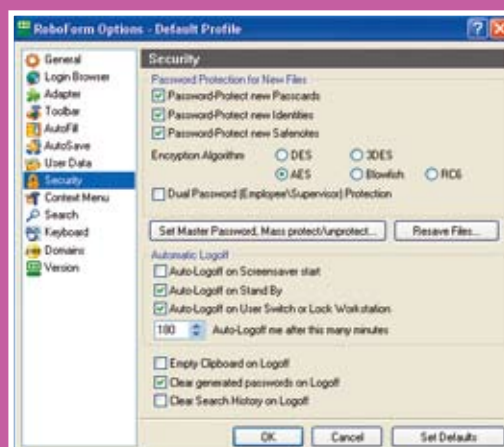




Use your firewall to protect your system at home and on the road.



Phishers often give themselves away by poor grammar and spelling, generic greetings and fake web addresses.



RoboForm simplifies password management, making it easy to create strong, unique passwords for all the sites you use.

PTOTECT YOUR ID ONLINE: Continued from page 20

virtual worlds like Second Life, create accounts on discussion forums, or sign up for online subscriptions.

Most fake IDs – or inaccurate details provided as part of a real ID – are created for innocent reasons: as part of a game, perhaps, or to protect the user's own privacy. For example, you might want to sign up for a site but feel it unnecessary to provide your age or income bracket details on the sign-up form.

The innocent nature of most fake IDs makes us all the more susceptible when someone uses fakery to trick us into sharing information we should keep private. In the real world, there are a myriad cues – visual, tonal, situational – that help us suss someone out and decide whether we can take them at face value, but how do you take someone at 'face value' on the Internet?

It's hard to get solid statistics on the incidence of identity theft in Australia. The National Crime Prevention Program's Identity Theft Kit states, 'The risk of becoming a victim of identity theft in Australia is still relatively small.' However, in 2007 the Office of the Federal Privacy Commissioner, extrapolating from figures obtained in a telephone survey, reported that around two million Australians 'have had their personal details stolen and used fraudulently by a third party.' Hardly a low incidence.

Whatever the figures, everyone agrees on three things: identity theft

is one of the fastest growing of all crimes; being online increases your exposure; and there are simple steps you can take that will greatly reduce your risk of becoming a victim.

### How Online ID Thieves Work

Online identity thieves use a variety of methods to steal personal information:

**Research.** Googling a person is the simplest way to ferret out information about them. Depending on how much – and how carelessly – that person uses the Internet, a Google search can turn up all sorts of information. And Google – or another search engine – is only the first point of call: there are online phone directories, job sites containing resumes, minutes of public meetings and many other sources of information.

For a small fee, anyone can purchase additional, much more 'private' information – such as credit reports – from online investigation firms.

**Mining social networking sites.** When you post information on social networking sites such as Facebook and MySpace or chat in public chatrooms, there's no way to know who's listening in. Even if you limit the information in your membership profiles, the details add up across different sites and in different settings.

**Phishing.** A phisher obtains your personal information by posing as a trusted organisation. The phisher

#### Expert tip 1: Use UAC

**Experienced users have a tendency to ignore warning dialogs, such as Vista's UAC warnings. Don't! The UAC prompts are particularly useful for spotting Trojans and other programs which attempt to install without your permission.**

#### Expert tip 2: Tweak your firewall

**Explore your firewall software. Most firewalls work fairly well using the default configuration, but if you get to know the advanced settings you can often ratchet up your protection a couple of notches while still allowing legitimate programs full Internet access.**

#### Expert tip 3: Take care in public

**Don't use public terminals to access your financial accounts, make online purchases or connect to any password-protected site. Similarly, avoid making such transactions when using unsecured wireless networks in airports or other public places.**

## Need help with managing your records?



Resource  
Options

Resource Options can assist you to review and improve your records section. Our services include:

- Planning and implementation
- Business classification schemes
- Staffing
- Special projects
- Software
- Training

Contact us on 07 3847 6499  
info@resource-options.com.au

Successfully delivering quality information management

www.resource-options.com.au

PTOTECT YOUR ID ONLINE: Continued from page 23

sends you an email which appears to come from your bank or credit union or an online retailer. The email will usually indicate that your account has been compromised in some way or that it needs updating, and invite you to click a link to go online and fix the problem.

Phishers use a variety of techniques to disguise where the email comes from and where the link leads to; if you click the link, you'll end up at a spoofed site – one that's been dummed up to look like the real thing. If you visit the spoofed site and type in your user ID, password, account number or other details, you've handed the phisher the key to your account – and, if you use the same ID/password combination repeatedly – possibly the key to many other sites and accounts, too.

**Key logging.** A keylogger is a program, installed surreptitiously, which monitors every keystroke you make and sends that information back to the person who deployed the key logger. A keylogger will record user IDs, passwords, account numbers, web site addresses, instant messages, chat room dialogue, email content and everything else you type. Some sophisticated keyloggers even take screenshots of your screen in order to defeat sites which use visual cues and mouse input as an anti-keylogger security measure.

How does an identity thief's keylogger get onto your computer? In most instances, you install it yourself. Keyloggers are distributed via attachments in infected emails or via programming scripts on web sites. By opening an infected attachment or clicking a booby-trapped link, you install the keylogger and it then goes to work in the background.

**Malware.** As well as keyloggers, identity thieves use a variety of techniques such as spyware, port probes, spam and viruses to infiltrate your computer or secretly take over its operation.

In addition to using purely digital methods for snaring your personal information, identity thieves may also gain access to your online accounts through physical means:

**Over the shoulder.** Some ID thieves know their victim. They may be housemates, colleagues or family members and much of the information they gain is by looking over your shoulder as you type your user IDs and passwords, or by checking around your desk for the same information stuck somewhere on a Post-It Note.

**Retrieving dumped computers.** Many people toss out their old computer when they buy a new one. If you do so, even if you've deleted all the files from your hard drive, there are ways to retrieve the information on it.

## Prevention is the Watchword

If you are the victim of identity theft, recovering from the loss is often a long, frustrating and complicated process. By obtaining a couple of crucial pieces of information about you, an identity thief can proceed to uncover more and more information, then use that information to make purchases and apply for loans in your name or as the basis for creating an entire ID based on your stolen one.

The sooner you discover the theft, the easier it is to rectify the problem. Unfortunately, most people don't realise their personal information has been stolen until well after the event. By that stage, as well as cancelling your credit cards and closing bank accounts, you may also need to correct your credit rating and, in the worst case, clear criminal records where your name has been used in the commission of crimes by the identity thief.

So it's important you take steps to protect your identity before the thieves strike and be on the watch for early warning signs if you are a victim. Those signs include:

- Unknown charges appearing on your credit card statements or in your bank accounts.
- No longer receiving bank or credit card statements.
- Receiving bills for a credit card you do not possess.
- Being denied credit when you haven't applied for it; or receiving credit for which you haven't applied.

In order to prevent your ID from being stolen, there are three key areas to monitor: your operating system security, your email and your online activities.

## Steps to Protect Your System

Install security patches for your operating system and for your applications. Use Windows Update to keep Windows patched, and

make sure you check regularly for updates to your software. It's particularly important to keep your browser up to date, as well as any other software which connects to the Internet.

These days, that includes almost everything, from MP3 players, VoIP programs (like Skype), instant messaging apps and email to graphics and accounting programs which check for downloadable content.

If you use Windows, upgrade to Windows XP or Vista. Microsoft no longer issues security patches for older versions of Windows, and that makes you particularly vulnerable, especially as identity thieves are well aware of the porous nature of these older systems.

Install anti-virus software, keep it turned on, and update it regularly.

Install several anti-spyware applications (no single one catches all spyware), use them regularly and keep them up to date. Spy Sweeper, from

**Beginner tip 1: Google yourself**  
Type your own name into Google and see what turns up. Whatever information you can find about yourself is public currency. If you uncover details you'd rather not share, see whether you can repair the damage by changing your posts or profiles or by contacting the site's owner.

**Beginner tip 2: Find out more**  
The Attorney General's Department puts out an excellent Identity Theft Kit. It's available online from <http://tinyurl.com/yp3hkq>.

**Beginner tip 3: A better firewall**  
Windows XP comes with its own firewall, but you shouldn't depend on it for protection as it only monitors incoming transmissions. Get yourself a third-party firewall, or buy a security suite which includes a firewall.



www.webroot.com, is particularly good. Use it in conjunction with the freeware Ad Aware Free (www.lavasoftusa.com/products/ad\_aware\_free) and Windows Defender (www.microsoft.com/athome/security/spyware/software).

Install a firewall and keep it active. It will warn you when any unauthorised program tries to download or transmit information.

Before you toss out an old system or send it for recycling, use a software shredder to scrape all the data off the hard drives. Deleting files, even formatting a drive, isn't sufficient to eliminate your data completely. Use a tool such as the freeware File Shredder from www.fileshredder.org.

### Steps to Protect Your Email

Use a spam filter. Spam (junk email) is often used as a delivery method for other malware or to entice you to unsafe web sites.

Don't open attachments from any unknown sources, and don't open any attachment without first checking it with your anti-virus and anti-spyware software. When you receive an attachment from someone you know, save it to your desktop, then right-click it and choose 'Scan for spyware/viruses' from the pop-up menu. Most anti-virus and anti-spyware programs add such an option to the right-click menu.

Only access online banks and financial sites by typing the address in your browser (or using a shortcut you have created); don't use links in email.

If you're unsure about an email's authenticity, phone the bank or company involved.

Turn off the preview pane in your email client. Some types of malware can be activated simply by previewing an email.

### Steps to Take Online

Be careful about the information you share online. When filling in forms, provide the minimum necessary information. Take care when creating profiles on social networking and other sites and, if possible, limit access only to those you know. Don't share identifying information on public message boards and remember that seemingly private conversations, such as instant messaging chats, are vulnerable to snooping.

Use strong passwords, especially on sites where you share financial information. Use a different password for each site, if possible. At a minimum, use different passwords for social and financial sites. A password manager, such as RoboForm (www.roboform.com) makes it much easier to create and use multiple, strong passwords. With RoboForm, all you do is to remember a single password; it takes care of all the rest.

Don't let web-based retailers save your credit card details. Instead, type them in each time they're required. Once again, a program such as RoboForm can automate this process for you: it will store your account details secured by encryption and a password, and then fill in those details in online forms when needed.

### Useful Websites

**Each state's Consumer Affairs or Fair Trading department offers information about dealing with identity theft. Here are their web sites: ACT - [www.fairtrading.act.gov.au](http://www.fairtrading.act.gov.au); NSW - [www.fairtrading.nsw.gov.au](http://www.fairtrading.nsw.gov.au); NT - [www.nt.gov.au/caft](http://www.nt.gov.au/caft); QLD - [www.fairtrading.qld.gov.au](http://www.fairtrading.qld.gov.au); SA - [www.ocba.sa.gov.au](http://www.ocba.sa.gov.au); TAS - [www.tas.gov.au](http://www.tas.gov.au); VIC - [www.consumer.vic.gov.au](http://www.consumer.vic.gov.au); WA - [www.docep.wa.gov.au](http://www.docep.wa.gov.au)**

Don't send credit card numbers by email, and don't conduct business online unless the site uses encryption (designated by https – instead of http – in the web address and a padlock icon in your browser's status bar).

Don't click any link or button in a pop-up window, especially those warning that your computer is infected or at risk. Use the close button in the top right corner, or right-click the browser button on your taskbar and choose Close from the pop-up menu.

Don't use Internet Explorer 6 or

any out of date browser.


If you use Internet Explorer 7, consider switching to Opera or Firefox. They are both more secure.

Don't engage in dodgy activity online, such as visiting porn sites, engaging in online gambling, visiting warez sites or using peer-to-peer file sharing software. All these activities make you more vulnerable.

If your bank or credit cards offer online access, take advantage of this. By checking your accounts daily, you'll have a chance to spot unauthorised transactions almost immediately. By the time your paper-based statement arrives in the mail, the damage may have already been done.

### Real and Virtual Threats

Identity thieves work offline as well as online. In addition to taking online precautions you should take care in the real world, too: shred important personal documents before you put them in the garbage; don't let your credit card out of sight when paying for a meal at a restaurant; don't let a stranger fill in your details in an official document; check all account statements carefully and as soon as possible; don't write down PINs; and keep records of all your important documents somewhere safe.

Finally, get a copy of your credit report every year. You can obtain one from Veda (www.mycreditfile.com.au) or Dun & Bradstreet (www.dnb.com.au). In Tasmania, you should also contact the Tasmanian Collection Service (www.tascol.com.au). 

### The Author

Currently based in New Orleans in the US, **Rose Vines** is one of the world's leading freelance technology writers. She has been writing for computer publications in Australia, the United States, and the United Kingdom since 1982, and is a regular contributor to *Australian PC User* and *Australian NetGuide*.



You can read more of Rose's work on her website, *Geekgirl's Plain English Computing* (www.geekgirls.com), and her blog, *Before Hours* (www.rosevines.org).

This article first appeared in the March 2008 issue of *Australian NetGuide*, and is reprinted in *IQ* with permission.

# Public & Private Sunshine & Reign

Something is amiss in the world of records and information: Too many public records are being kept in the dark, while too much private, personal data is being aired in sunlight.

**F**irst of all, too many US politicians are deleting electronic records, depriving the public of information they may be entitled to see.

Missouri Governor Matt Blunt and his administration are currently under investigation by the state attorney general for possibly destroying public records in the form of e-mails.

Last September, the Blunt administration fired a staff attorney, Scott Eckersley, saying he was let go 'for cause.' Eckersley contends that he was fired because he challenged Blunt's position on email retention and warned the governor's staff that state law requires them to save emails.

Blunt's staff said Eckersley never told them to retain emails. When pressed, Blunt told an Associated Press reporter, "Our policy is to follow

the Sunshine Law. That's it."

Secondly, too many marketers and retailers are exposing too many citizens' private information to sunlight – letting both hackers and legitimate marketers steal a glance and maybe more.

For instance, in late November, Facebook, the social networking website, said it would rein in parts of a new advertising program that send messages to users' friends about what they're buying online. However, the website relented only after more than 50,000 members signed a petition objecting to the advertising program.

Of course, any type of personal electronic information has the potential to suddenly turn back and bite an individual. As a November 25, 2007 US "60 Minutes" TV segment reveals, even using a credit card



while shopping at the mall can make you vulnerable to ID theft.

"Do you think twice when typing in your credit-card number online, but have no problem handing over your plastic card at a store?" "60 Minutes" correspondent Lesley Stahl asks. "Well, actually, you may have it backward," Stahl said. "Your personal information may be more secure in cyberspace than at the mall down the road."

That's because, the segment explained, earlier in 2007, TJX, the parent company of T.J. Maxx and Marshalls, disclosed it had suffered the worst high-tech heist in shopping history. Hackers raided the company's computer system, taking off with tens of millions of records – a theft that could have been prevented.

This and similar occurrences frequently stem from retailers using an outdated encryption code called WEP, which was developed in 1999, but has since has been cracked by hackers and made obsolete. A much-better encryption code called WPA has been developed, and credit-card companies urge retailers to upgrade to WPA, but many retailers resists WPA technology because of its cost.

Meanwhile, across the pond, in another type of security breach, UK government workers in November 2007 lost two computer disks containing the names, addresses, dates of birth, national insurance numbers and in some cases, banking details, of approximately 25 million U.K. residents.


The two disks were sent through the government's interoffice-mail system with no special tracking number. The breach was Britain's worst personal data security blunder and second only to the U.S. government losing data on 26.5 million former servicemen in 2006.

Finally, just to show that all security breaches shouldn't be blamed

on computers, here's another recent story: After two incidents within two months, in which personal records of its 28,000 students were stolen, lost, or left unsecured, the University of Cincinnati (UC) in Cincinnati, Ohio, said it would install encryption software on more than 8,000 UC computers to protect sensitive records.

However, a Cincinnati newspaper, *The New Record*, discovered a room at the McMicken College of Arts and Sciences containing multiple, unlocked filing cabinets filled with student information.

The newspaper reported that staff members were able to enter the unlocked room, open file cabinets, and access inactive student documents easily and without being questioned.

At least this problem has a simple solution. "Lock your file cabinets," Kevin McLaughlin, director of UC information security, told *The New Record*. "Lock your desks and don't keep sensitive data that you really don't need." 

### The Authors

This article first appeared as an editorial in the 'In Focus' section of the January/February issue of *The Information Management Journal* in the US, written by the journal's editors, and is reprinted in *IQ* with the permission of ARMA International.

## SYDNEY INSTITUTE



# Records Management is in Australia!

To meet the professional requirements of Records Management in Australia, we have put together a ground-breaking opportunity to recognise your existing skills and gain two highly respected qualifications in a single program of study.

They are:

1. Certificate IV in Recordkeeping, and
2. Certificate IV in Frontline Management

By completing a small number of additional units you can extend your Certificate IV in Recordkeeping into a Certificate IV in Frontline Management.

You can undertake this in a number of ways:

- ▲ A two (2) year part time distance education (online, anytime) program
- ▲ A two (2) year part time traineeship program

A tailored corporate group training program – your choice of 'workplace bundles' – in our commercial training rooms, on site in the Sydney metropolitan area and or by individual negotiation.

As usual, all your study, whether Recordkeeping or Recordkeeping / Frontline Management, is supported by:

- ▲ Return to study workshops
- ▲ Full course materials
- ▲ Email/telephone support
- ▲ Teaching by qualified, industry specialists and practitioners

Call or email Esther Aarons for full details on (02) 9217 3442 / [esther.aarons@tafensw.edu.au](mailto:esther.aarons@tafensw.edu.au).







# WHEN RECORDKEEPERS ARE PEACEKEEPERS

## Managing the Records and Information of a UN Peacekeeping Mission in War-torn Africa

By Tom A. Adami

The United Nations is in Sudan for several reasons, the most obvious of which is an attempt to alleviate suffering on a mass scale in the three western states of the country scarred by civil war. In this article, the author, who is chief of records and archives management with the UN Mission to Sudan, discusses the role of recordkeeping in peacekeeping missions, and wonders whether the keeping of recorded information can assist in the eradication of arbitrarily inflicted suffering from Darfur and elsewhere.

**M**ore than 19,000 heavily armed UN blue helmets will try to end the suffering in Sudan, but how can my work as an information manager assist the process? Why am I here? Peacekeeping is a complex and global undertaking with a long history going back to June 1948, but the management of its information legacy is only now being addressed in a systematic and holistic way.

Let me set the scene with a little bit more information about Darfur, Sudan and peacekeeping. Very few people outside Sudan would ever have heard of Darfur five years ago. Since 2003, the word 'Darfur' has taken on new and mythical meaning to many around the world. It probably generates instant but nonetheless valid mental images of burning villages and displaced persons.

However, Darfur is generally a wondrous and beautiful place populated by a warm and friendly people. The rains bring a shimmering green cover that make the vast Jebel Marra Plateau a sight to behold from the air.

What was largely a harmonious but ecologically fragile rural existence for most of the Darfurians before 2003 has become a terribly wretched and blighted life in a 'temporary' camp. From an international perspective the region has become an occasional sound byte and a diminishing cause célèbre. A recent delegation<sup>1</sup> to Sudan of eminent retired persons known as 'the Elders' achieved a measure of public recommitment on the side of the parties to the conflict.

Celebrities and elder statespersons aside, the situation in

Darfur is a complex and ever changing one. Sudan's people, at the beginning of the 21st century, had been subjected to decades' long conflict during the low-level but nonetheless vicious Second Sudanese Civil War and they could ill afford another conflict developing within their borders.

The signing of the Comprehensive Peace Agreement [CPA] in January 2005, which ended the civil war between the north and south, overlapped with the beginnings of the Darfur conflict. It is generally accepted that the Darfur conflict began in 2003 even though low levels of conflict had been traced back to 2001.

The United Nations involvement with Sudan began with the establishment of the UN Advance Mission in Sudan [UNAMIS] in June 2004. UNAMIS became UNMIS in March 2005 and subsequently in October 2007 the Security Council established UNAMID to deal with the Darfur conflict.

UNMIS is mandated to ensure that the CPA is not negated by a backsliding into conflict and this mandate is vital to the stability of the country and region. UNAMID was created because the Darfur conflict needed to be addressed fully and in a comprehensive manner without jeopardising the implementation of the CPA between the north and south.

Hence, we have for the first time ever, two UN missions in one country. Simmering conflicts in neighbouring Chad, Central African Republic, Uganda, and Eritrea / Ethiopia, make the resolution of conflict in Sudan a major priority of the international community to avoid a possible escalation or spread of hostilities.

*WHEN RECORDKEEPERS ARE PEACEKEEPERS:*

Continued from page 29

Given the extraordinarily complex nature of Sudan politics and the additional complications presented by other regional conflicts, the administrative structure of UNMIS reflects the nature of the mandate and its location. The UNMIS HQ is based in Khartoum with 2 major regional offices in Juba [capital of Central Equatoria state] and El Fasher [capital of Northern Darfur state].

The UNMIS Juba office is at the centre of CPA implementation oversight in the south of Sudan and is the seat of the Government of Southern Sudan [GoSS is a semi-autonomous entity with a president who is also first vice-president of the national government in Khartoum] and El Fasher deals with Darfur related issues.

UNAMID has its HQ at El Fasher and simply inherited the existing administrative structure but with over 15,000 extra troops and police to take over the role performed by African Union [AU] troops. Juba is the southern region HQ with smaller offices organised within six sectors.

The air operations section of UNMIS organises enough daily flights to move staff around these offices to rival any small airline. In terms of logistics, the maintenance of the mission is astounding. Feeding, housing, moving, providing for, training, recruiting, rotating thousands of troops, police and civilians requires lots of funding and of course it generates lots of paperwork. This is where I come into the picture.

The former ANC anti-apartheid freedom fighter and now Justice Albie Sachs of South Africa is a very powerful example of what the human spirit and the written word can achieve. His hand written note smuggled out of prison in 1963, 'Mummy, I'm being tortured', has become a classic piece of evidence of resistance to injustice. Sachs has called it 'the most powerful legal document I've ever written in my life.'

Such an impact from a 'scrap of paper' is not commonplace, but the principle is plainly evident – words are indeed powerful in their potential impact. However, there are still conflicting views on the effect of the usage of archives of atrocities.

The numbing effect generated by graphic images of atrocities has been discussed by people like of Susan Sontag but it is nevertheless an important method of getting the 'message' across to a wider global audience.

There is debate about the efficacy of using graphic images to stir concern, anger and hopefully action to alleviate human suffering. Some commentators state that it helps the overall call to action in any given cause but others say it does not.

Whatever the reality, it is true to state that archives should be made available so that viewers can decide for themselves what they will do when confronted with these images and words. It will remain a personal decision as to whether to become engaged with the archive and thereby confront reality or to reject it and also reject what is real, tangible and provable.

So in the context of justice, reconciliation and forgiveness, how could archival pursuits ever be relevant in Sudan? Our fellow human beings in the camps couldn't care less about recorded information when they have concerns relating to food, shelter, health and security.

Other human beings in power and in the conflicting parties probably couldn't care less about archives of atrocities - or maybe they wished to see such collections rendered useless. But on the other hand they would build up large collections of information of surveillance and gather intelligence to fight their battles.

Still other human beings in humanitarian efforts on the ground probably don't have the time or resources to document what they see and encounter as their imperative is to save lives above all else. Then more human beings remotely overseeing aid efforts document their relief work to satisfy auditors and wary donors.

Finally, those human beings who are called activists risk personal safety to publicise the situation and require information of the atrocities to stop what is happening and we have therefore gone full circle – back to the humanity in the camps.

Archival work is relevant in Sudan because it can help to put an end to the appalling humanitarian situation in conjunction with other measures such as the will of the international community to bring about change. In reality, the keeping of – and also making use thereof – recorded information is actually crucial to those in the camps.

The equation is simple: no recorded information means there is no response which leads to no outside intervention and therefore no hope of peace. There is an Ashanti saying from Ghana that says 'grief that is unspoken does not exist', so we need to speak about and record what is happening in places such as Sudan.

An archive can not in or of itself do anything. It is the human element in everything that makes the difference. It is this human element that makes all things we do complex and sometimes unfathomable for no real reason except that we can make it so. Complexity is a byword for some of the UN's operations in Sudan.

An example of what situations can occasionally add a layer of complexity to the function of keeping recorded information in this Sudan peacekeeping setting is the fact that the UN and AU have performed a joint operation in Darfur which has changed as of 1 January 2008 when UNAMID took over fully.

There are administrative structures in place with the ominous word 'joint' attached to them. Joint normally meant that there was lots of duplication and no real control over certain aspects of what was done administratively. The UN-AU Joint Mediation Support Team [JMST] is a prime example of the ad-hoc groups of recorded information that have developed.

The JMST was established to support the series of mediation talks held in Libya to bring together some of the factions from the Darfur region. There was no real precedence for the JMST so any subsequent archiving of these records will be a new experience. 'Joint' means joint ownership, and therefore there are two sets of all archival recorded information.

So what is the way ahead in this case? The only way forward is to apply our function based appraisal and taxonomy to the records. At the time of writing there was a decision to make the JMST a part of UNAMID, but some staff will still be part of UNMIS [or not]. Such complicated structures are not exactly new - they are just different - but the institutional memory is not sufficiently captured in the short or long term to deal with them when they occur.

The UN's corporate memory is not as sharp as it could be. A comprehensive study undertaken at the UN Mission in the



**Heavily armed young rebel  
at UN-brokered peace  
negotiations, Zam Zam,  
Darfur, January 2008.**

**Photograph by Stuart Pierce,  
Albany Associates**





Sudanese displaced from Darfur are forced to live in conditions such as these in a refugee camp in northern Sudan



*WHEN RECORDKEEPERS ARE PEACEKEEPERS:*

Continued from page 30

Democratic Republic of the Congo [MONUC] in 2007 found that creating a knowledge management environment and culture was possible and that explicit knowledge could be captured into appropriate electronic systems.

It didn't identify the knowledge management systems but stated: 'Consequently, there is a need for a knowledge management system that captures explicit knowledge in an easily accessible and efficient manner and facilitates the transfer of tacit knowledge within the Mission.'

The study identified that the obstacles to achieving a knowledge management culture within the mission were, 'The lack of staff with mid-range experience, the transfer of knowledge and the mentoring and coaching between very experienced staff and those less experienced, the consistent sharing of information, the provision of training opportunities, the use of staff knowledge and expertise in general and the appropriate filing and backup of Mission documents and information.'

'Further, it was apparent that these knowledge problems mirrored and confirmed issues raised in the literature review particularly with regard to knowledge transfer, organizational climate, leadership style, contextual information, framed experience and expert insight.'

The study's results and findings can be applied to most of the other UN DPKO missions worldwide. The administrative, technological and personnel structures are the result of events on the ground. Then to try to fit a technological solution around the structures in place becomes a difficult prospect in retrospect.

Thought should be given to the whole issue as a new mission is being created. Issues that would hamper the attempt at implementation of a 'knowledge management' solution at UNMIS would include the dispersed nature of the staff and offices and the accompanying lack of connectivity and bandwidth to make a remote access system viable. The use of Wi-Fi in many offices severely limits the amount of data one can access or upload to a central data store or recordkeeping system.

During a recent recordkeeping workshop in Brindisi, Italy organised by the Department of Peacekeeping Operations [DPKO] and Archives and Records Management Section [UN ARMS], it was highlighted and reinforced that the DPKO recordkeeping taxonomy advocates a uniform approach to managing recorded information based on what is a functional appraisal system of peacekeeping mission functions.

This does not rule out the fact that missions are not uniform, despite the main functions being the same, missions have different mandates and hence expected results and outcomes, which affects how the main functions are implemented for activities such as political affairs, civil affairs, human rights, etc., here is where we draw the line between taxonomy and mission specific file classification schemes [FCS].

The taxonomy summarises and/or defines DPKO mission functions, so it's a useful tool just like any of the many background publications on UN peacekeeping to understand how DPKO addresses its broad mandate of peacekeeping and building and forms a basis of developing recordkeeping systems.

While the taxonomy defines the main two levels and sometimes goes to a third of each main function; the Peacekeeping Operations Retention Schedules [PORS] goes further by providing records series of these functions.

The UNMIS FCS is a functions based tool for managing the recorded information of this mission. It is a mission tool that defines recordkeeping requirements specific to the mission based on their mandates, work plans and/or goals at the same time applying PORS.

Overall, a functions-based FCS development has bridged the gap between UN HQ developed recordkeeping tools with mission recordkeeping tools and hence a better DPKO recordkeeping system. What recorded information becomes archival is determined by the application of these function based appraisal and retention tools.

The UNMIS FCS is entirely dependant upon and closely linked to the DPKO and ARMS issued taxonomy and PORS and is therefore a logical extension of those two endorsed guidelines making the UNMIS FCS a vital component in recordkeeping in this mission.

As a way of mapping the relationships between the three recordkeeping tools of FCS, taxonomy and PORS, we examined the humanitarian assistance function from the UNMIS FCS and were able to confirm that we had a practical way of applying the high level taxonomy in a way that staff would be comfortable with.

I believe that is critical to the adoption and success of such systems in any organisation. If the filing structure is clear and precise, then administrative staff will understand it more readily and apply it as it should be applied. It also makes training easier if one is attempting to explain functional classification systems to non-recordkeepers.

The records and archives of peacekeeping missions have the potential to make many important contributions to world history and memory. In order to live up to this potential, however, it is essential that administrative and financial support is provided for various long-term information management and archival programmes.

Funding must be made available for the resources and staff needed to implement and run compliant record-keeping systems, ensure the intellectual and technical control of audio-visual materials, provide public access to the records, and develop outreach and capacity building policies.

Administrative support is required to develop plans for the deposition of copies of the archives in affected communities, and the long-term preservation of the materials. Support for these activities must be made available from the earliest days of the institution's existence through the completion of its mandate to ensure the successful completion of these programmes.

The maintenance of reliable, accurate records of an institution's operations is a crucial component in ensuring its transparency and accountability. The accessibility of records to internal users provides for efficient and effective work practices, and the accessibility of the records to the general public is necessary for educational and outreach purposes. The long-term viability of the records will ensure that the information is accessible to future researchers and historians and will provide a roadmap for the development of future institutions with similar mandates.

# WHEN RECORDKEEPERS ARE PEACEKEEPERS:

Continued from page 33

And finally, the availability of the records in communities affected by armed conflict can aid in the process of reconciliation in those communities.

A cynical observer once said that 'reconciliation doesn't come cheap', and there is some truth to that. It is because of the amount of resources devoted to peace-keeping, the provable veracity and integrity of the records generated in the completion of a mission's mandate are essential for the purposes of accountability and transparency. Around five billion US dollars are spent on peacekeeping every year.

Also, the security of all public and confidential documents is an important concern because of the volatile nature of the political climate in which peacekeeping missions are established.

It is a bleak reflection on the nature of human kind that there will undoubtedly be a need for the establishment of future peacekeeping missions; the records of past and present missions will provide insights into lessons learned, enhancing the efficiency of the operations of future missions.

The DPKO Best Practices Section plays an important role in enhancing the already established procedures for all aspects of a mission's administration, including information management. There is a large pool of knowledge and personal experience within DPKO and it is continuously growing and built upon through discussions forums, meetings and staff mobility.

The Best Practice Section of the United Nations has established several communities of practice [COP] and one of them is for recordkeeping professionals working in peacekeeping missions. It was started in June 2007 and has about 40 members representing all current peacekeeping missions as well as other United Nations offices such as UNON in Kenya, UN Habitat and the international ad-hoc criminal courts.

The recordkeeping COP has been widely used by its members to develop new approaches to issues such as training, outreach and taxonomy application. COP's are a knowledge sharing initiative to link colleagues working in similar job functions across peacekeeping missions. The COP is an email based online forum where members can pose questions, exchange information, build up a shared library of useful documents, and find counterparts in other field missions.

In a sense, it is like a standard listserv that maintains a history of previous discussions. It becomes the first avenue for members to ask for help on issues and avoids reinventing the wheel. There is a lot of literature around that equates communities of practice, lessons learnt databases, thematic and knowledge networks and general information management with the overall concept

of knowledge management when all these elements can be successfully brought together.

Broadly speaking, the application of the concept of 'best practice' principles in the field of records management and archiving has four main benefits to an organisation's effectiveness. Firstly, in the area operational efficiency there is increased productivity, improved service delivery, decreased storage and supplies cost and efficient deployment of staff.

Secondly, there is advancement of the nebulous concept of knowledge management with more effective information sharing, business continuity and cultural and historical memory being aided. Thirdly, in the area of evidence and accountability requirements

one can expect improvement in the retention of records of activity and decisions, increased transparency and openness and decreased risk of litigation.

Finally, in the area of protection of individual rights there would be tangible enhancements of the individual's rights to entitlements and the application of any privacy regulations. In tandem with the best practice principles the United Nations attempts to apply the concept of 'lessons learnt' to its peacekeeping operations.

Lessons learnt, when shared, can be a useful tool for passing on knowledge from one staff

member to another. The Best Practice Section of the United Nations is responsible for centralising and disseminating all the 'end of assignment' and similar evaluation documents from staff when they move onto new assignments.

These documents form a valuable resource for all staff to access. Some of these documents are confidential so the distribution can at times be restricted especially when they report on sensitive military aspects of a mission.

Overall, the idea of best practice and lessons learnt means that information should be more widely shared and made accessible and that standardisation of work practices is a goal to be aimed for. Records management in the peacekeeping field has become a prime candidate for such centralisation.

Prior to 2006, there was little standardisation among the various missions operated by DPKO regarding records management but in particular electronic records management. In most cases, the recordkeeping responsibilities belonged to the mail and diplomatic pouch registry staff of the mission, with different missions making use of a variety of electronic record-keeping systems.

Since 2006, UN missions have begun employing archival and information management professionals to enhance their recordkeeping practices, and an enterprise wide content management system is being developed that will be implemented in all DPKO-operated missions throughout the world in the very near future.



The treacherous condition of roads in southern Sudan make helicopters the preferred travel option for UN personnel

It is hoped that these developments will lead to a more harmonised approach to the information management practices organisation-wide, aiding the missions in completing their mandates through enhanced efficiency and accountability. While developing an enterprise-wide content management policy, lessons can and should be learned from both the failures and success of the information management practices of the UN sponsored organisations devoted to the field of international criminal law.

There is a strong connection between peacekeeping missions and the international courts that are historically linked by events dealt with by both organisations.

The International Criminal Tribunal for the former Yugoslavia [ICTY] was created after the Balkan Wars of the 1990's which saw peacekeeping efforts led by the United Nations [UNPROFOR, UNMIBH, UNCRO, UNTAES, & UNPSG]; the Sierra Leone Special Court [SCSL] operated while the United Nations Mission in Sierra Leone [UNAMSIL] was still active.

Many staff from the United Nations mission in Rwanda [UNAMIR] moved into a role with the International Criminal Tribunal for Rwanda [ICTR] in 1995; and, the United Nations missions in Timor Leste [UNMISET & UNTAET] supported the work of the Serious Crimes Unit. In a sense the administration of international justice becomes a mechanism for peacebuilding in the post-conflict phase and the international community is trying to address issues of justice and reconciliation.

Although the concept of reconciliation is somewhat vague and difficult to quantify, it is a key factor in determining the success or otherwise of the UN organisations devoted to international peace-keeping. It is a complex matter, involving the search for truth,

justice, healing and forgiveness. The level of success in attaining reconciliation can only be properly evaluated after many years.

The establishment of self-sustaining peace is an indicator of whether or not true reconciliation has been attained in a community affected by violent conflict. The aim of all peace-keeping missions is not simply to end conflict, but the establishment of peace.

The successful implementation of self-sustaining peace in a post-conflict region can be determined by evaluating such criteria as disarmament, government policies, donor demands, internal or external armed interference, and outside political manipulation.

But lasting peace can never truly be established without reconciliation. Justice is also a key component in the process of reconciliation. The legal process gives survivors and victims the forum in which to speak, and the opportunity to attempt to forgive the perpetrators of the atrocities they suffered.

The accountability of peacekeeping missions is a crucial component in the process of reconciliation. There appears to be little doubt in the professional literature or in practical experience that recordkeeping does aid the reconciliation process. As can be seen in the example of the Armenian genocide, lack of verifiable documentary evidence can seriously undermine international and local efforts to attain the goal of reconciliation.

Because accountability leads to a trust in the rule of law, the archives of international courts and peace-keeping missions can benefit the process of reconciliation, assisting in the return to normalcy for the affected communities and nations.

Although it is ultimately the courts that determine whether records are telling the truth, in my view archivists should, in conjunction with the courts, be part of the process, neither



## Beat the Email Challenge



www.maxus.net.au/cvaultBE  
maxus@maxus.net.au  
(03) 9646 1988

### Can you:

- ✓ Find any email in seconds?
- ✓ Capture all emails automatically?
- ✓ Comply with legal requirements for records retention?



Find out how to beat the Email Challenge with  **ComplianceVault** from Maxus

# WHEN RECORDKEEPERS ARE PEACEKEEPERS:

Continued from page 35

conceding nor abrogating their role in this regard.

There is a gradual but nevertheless perceptible change, almost on a daily basis, of the collective archival fond of the UN peace-keeping missions and judicial bodies.

The record, as described in the records continuum model developed by Frank Upward and Sue McKemmish of Monash University, is constantly ebbing and flowing, and is perhaps also transfigured, according to the various influences and uses attributed to it.

The archives of a peace-keeping mission may have future use as documentary evidence in the legal process. For example, documents created or received by the UN Assistance Mission for Rwanda [UNAMIR] in 1994 are often tendered as evidence in court at the ICTR.


In fact, the archives of a single organisation may contain many copies of the same document serving different, sometimes conflicting, purposes. Records are used, re-used, interpreted and re-interpreted according to a complex set of requirements of the users. The records can exist within the different vectors and dimensions of the continuum model, thereby serving multiple purposes and attaining different values.

The concept of burden of proof and evidential value of the record should be the fundamental *raison d'être* of any recordkeeping program in the legal field. As was proven by the looting of the archives of SCU in East Timor, the documentary evidence of crimes against humanity is greatly feared by the perpetrators of these crimes, and is therefore susceptible to destruction or alteration by individuals who fear they have something to hide.

The security of the archival holdings of peacekeeping missions and international judicial bodies must be vigorously maintained, especially when they are housed in regions of unrest.

Historical revisionism is a great threat to the establishment of peace and justice, and is more damaging to the process of reconciliation than the complete lack of recordkeeping that, to this day, has allowed the denial of the Armenian genocide.

The recorded information of peacekeeping missions needs to be preserved overtime as a testament to the survivors of the worst possible crimes. The five main responsibilities of human rights archives are to ensure historical accountability, retain memory of the victims and survivors, support prosecution, document the extremes of repression, and chronicle the individual's power against the state.

In our small way, I hope that my colleagues and I are contributing to a more humane life for those in Darfur and in the south of Sudan. 

**Do you have an interesting  
RIM AROUND THE WORLD  
story to tell?  
email [editor.iq@rmaa.com.au](mailto:editor.iq@rmaa.com.au)**

## The Author



**Tom A. Adami** is Chief, Records Management and Archives Unit, of the United Nations Mission in Sudan. Tom has been an information manager since 1990 when he started with the Australian civil service and worked for the Department of Defence [Navy] in Sydney, Australia.

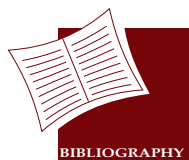
After several other appointments he was engaged in 1997 by the National Archives of Australia in Canberra to work on electronic recordkeeping projects including the DIRKS manual. In 1999 he joined the United Nations International Criminal Tribunal for Rwanda [UN-ICTR] as Chief Archivist. Notable achievements of his time with ICTR were to digitise the archive, establish the audiovisual collection and provide web access to the public records.

In May 2007, Tom took up an appointment with the UN's Department of Peacekeeping Operations [DPKO] with the Mission in Sudan [UNMIS]. Based in Khartoum, he is responsible for the management of all the recorded information assets of the mission throughout Sudan including the Darfur region until such time that the UNAMID hybrid mission can manages its own records and archives program.

He has taken an active interest in the African archival scene and presented at ESARBICA 2003 in Maputo, Mozambique and at a human rights colloquium in Dakar, Senegal in 2003. He has presented at several conferences notably at Society of American Archivist in Alabama, USA 2001, ICA CITRA in Cape Town South Africa 2003 and the Assoc. of Canadian Archivists conference in St. John's, Newfoundland, Canada, 2006.

Tom can be contacted at UNMIS HQ, 5A01. Obeid Khatim St., PO Box 69, Khartoum 11111 Sudan, or via [adami@un.org](mailto:adami@un.org).

All views expressed in this article are the personal views of the author and not of the United Nations.



See the transcript <http://www.abc.net.au/tv/enoughrope/transcripts/s837300.htm> of Albie Sachs being interviewed by ABC journalist Andrew Denton. Last accessed 23 November 2007.

H. Landon 'Developing a Knowledge Management Culture within MONUC', p.6 June 07.

Ibid, page 7.

VerneHarris, "Law, Evidence and Electronic Records: A Strategic Perspective from the Global Periphery" (National Archives of South Africa, 2000)

Frank Upward, Sue McKemmish, "In Search of the Lost Tiger, by Way of Sainte-Beuve: Re-constructing the Possibilities in 'Evidence of Me...'" (2001)

Bruce P. Montgomery, Fact-Finding by Human Rights Non-Governmental Organizations: Challenges, Strategies, and the Shaping of Archival Evidence; *Archivaria* 58 (The Association of Canadian Archivists, 2004)





# You Can't Buy COLLABORATION

By Joe Sweeney

Large-scale, monolithic collaborative initiatives run exclusively by IT will, says this author, prove difficult to justify over time and likely turn out to be white elephants. Instead, collaboration should be driven first and foremost by a change in company culture fully backed by management, with IT supplying a supportive network and software service architecture.

Over the past two years, my colleagues and I at IBRS have written a great deal about collaboration. We are constantly being asked about how to plan, procure and deploy collaboration. The interest in collaboration is being driven by the usual mix of vendor hype, media headlines and management looking for ways to gain competitive advantage.

The problem is, collaboration is not something you can buy. It's not even something you can install. Collaboration is an approach to business, not a solution.

OK, those may be fighting words, but let's look at the issues. First

of all, the definition of collaboration is 'the act of working jointly'. If people work together to a common goal then we have collaboration.

In a business sense, this means that collaboration is simply about getting people to work more effectively and efficiently together. In the dark-distant past, (pre-1990s), organisations attempted to achieve greater collaboration through training, management methodologies and, yes, IT systems.

So why do we have all of the excitement about collaboration now? There are two interrelated factors: the first techno-economical and the second techno-sociological.

### Pre-information age

Deep, narrow hierarchies



### Mainframe / minicomputer age

Organisational hierarchy begins to flatten. Rise of departmental computing



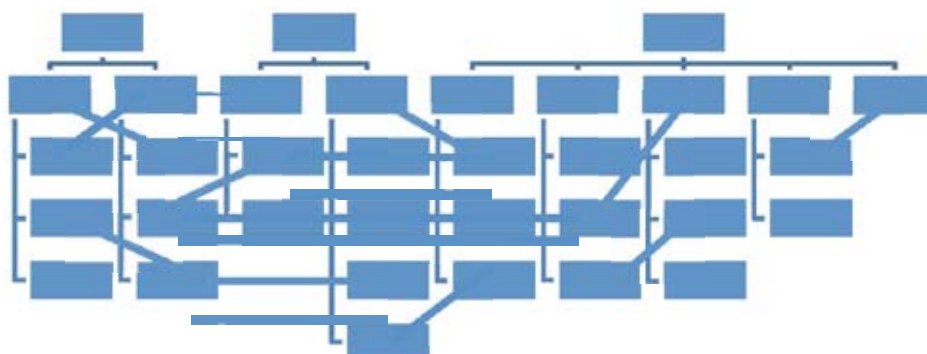
### PC / LAN age

Organisational hierarchy considerably flattened. Cross organisational and department-to-department communication



### Internet age

Organisational hierarchies become not only flat, but fluid. Communication crosses departments and organisation borders.



YOU CAN'T BUY COLLABORATION: Continued from page 37

## 1. Techno-economical - Collaboration's Reach

The definition of collaboration does not limit us to staff within a single organisation, but allows us to include people outside of our organisation: vendors, suppliers, utility and service providers and, importantly, customers and clients.

This ability to reach outside of the organisation in this manner is not new – EDI systems of the 1980's were certainly an attempt at this. However, it has only been with the increased interconnection of people and businesses due to the rise of the Internet that it has become feasible to get collaboration outside of organisational boundaries in an economical manner.

## 2. Techno-sociological - Familiarity with Collaboration

In the past, IT projects budgeted significant amounts of time and money on training. However, the advent of the first generation of Digital Natives (or Gen Y) workers and the familiarity these people have with web-based systems has changed the metrics.

If staff are familiar and very accepting of technologies that bring people together, then IT projects can be more open, more prevalent and, as an interesting side-effect, less rigidly defined.

## Collaboration as an Evolution in Organisation Structure

Neither of the above trends suggest that collaboration is anything more than getting people working together. However, they do suggest that we can begin to move to the next evolutionary stage of organisational structure (see figure 1, A history of organisational structure).

During the pre-computer era, organisations were exceedingly hierarchical, with deep and narrow management layers. Such management layers were required so that organisational directives would filter down through the organisation effectively - although not always efficiently. In many ways, the organisations reflected the class-based structures of the societies they served.

The dawn of the centralised mainframe and later the minicomputer saw the initial flattening of organisational structures as core processes within the organisation could be automated. At the same time, society in the Western world was also losing its rigid class-structure.

The advent of the PCs and local area networks further flattened the organisation, creating the concept of departmental and cross-departmental systems. It is at this point that concepts of supply chain management (SCM) become prevalent, as organisations looked for ways to extend communication to external partners on a department-by-department basis - eg. Sales department of company X to procurement department of company Y.

As our network infrastructure has begun to reach all layers of society and business due to the internet, we are seeing continued flattening of organisational structures. This flattening will result in not only the removal of additional 'vertical' management layers, but also breakdown 'horizontal' departmental barriers. The end result will be organisations with very fluid internal structures. Departments are likely to be superseded by flexible and agile teams.

When viewed this way, collaboration in the modern work place is more about how to strategise, manage, and guide people towards organisational goals both internally and with external partners, yet with less - or at least a different style of - internal management structure.

## Next Steps

IT management should avoid promising the delivery of a 'collaboration solution' for the business. Instead, they should talk in terms of deployment of an architecture, or framework, that will allow

new types of collaborative applications to be deployed on an as-needed basis.

IT managers must take on the task of educating non-IT management into the realities of collaboration – that it is primarily focused on changing how the business is structured and how work gets done. Such an understanding will no doubt raise political issues.

IT managers must gain not only the non-IT management support for business transformation, but also provide a role for all levels management in scoping specific collaborative work processes, which will then result in specific collaborative applications. Only with cross-department - even cross-organisation - input can specifications for discrete collaborative applications be developed.


IT departments must be prepared to offer 'user-defined' applications, allowing non-IT staff to deploy, update and destroy team-based applications on a common architecture.

IT managers will also need to ask non-IT management some hard questions about proposed collaborative applications, such as:

- Will this collaborative application increase productivity and how will we measure it?
- Does this collaborative application impact security, privacy, compliance and corporate governance?

IT managers should also consider how traditional IT systems (such as ERP and CRM solutions) will fit into the collaborative environment. Rather than looking for single 'collaboration suites', IT management should seek a unified set of architectural components than are interoperable.

- Key architectural components include:
- Network infrastructure
- Web application servers
- Mobile application servers
- Unified messaging
- Directory service
- Document / knowledge management
- Enterprise search
- Workflow
- Business intelligence
- Application Integration Middleware (AIM) services (preferably in the form of a Enterprise Service Bus)
- Basic team collaboration services (email, shared calendar, wiki, forum and message board, portal, dash-board, mash-up tools, social networking tool, and so on.)
- Development tools that cross all of the above.

In the final analysis, if they are to succeed, collaboration initiatives must be viewed more as a transformative whole of business project - with IT support. 

## The Author

**Joe Sweeney** is a business strategist and technology marketing expert with IBRS in Sydney.

Joe was founder and Vice Present of Asia Online, where he assisted the start-up into one of Asia's leading Internet and online services.

Most recently, Joe worked for a number of government and private sector organisations including Fortune 500 telecommunications firms.









# First Aid for Records

By Allen Hancock, ARMA

What exactly is a record? In the first few seconds of an emergency, First Aiders use 'DRABC' to remember the immediate steps to be followed - Danger, Response, Airway, Breathing, Circulation. The author argues that RIMs need something just as easy to remember as a tool to help colleagues overcome a lack of sensitivity to what recordkeeping is all about. Something, he suggests, as simple as ABC. Or, to be more exact, ABCDE.

Jack Welch once said about managing records... Actually, Jack Welch never said anything about managing records. Richard Branson? Nothing. Stephen Merchant never said anything either although I do recall an episode of 'The Office' where Dawn, the receptionist was doing some filing, but that was about it.

Sun Tzu did describe an information policy in the 'Art of War'. Something about whoever provides you with incorrect information should be summarily executed. As a policy though, I think it might be hard to get sign off.

So why do we make such a fuss about managing records if the gurus of modern management don't give them a second thought if they even think about them at all? Generally speaking, with the exception of records people, nobody else is really that interested.

A few years ago when I was working for the Australian Department of Defence I wrote a report that identified the biggest risk to records management in these terms

'Defence is an environment where most activities involve things that will eventually go to war. With that preoccupation, it's easy for something as unexciting as managing records to lose importance in the grand scheme of things. The greatest risk to records management is that the subject is simply not stimulating enough to anyone who isn't a records manager when compared to the core business of making things that go bang.'

Let's face it; records are just not that interesting so why then should anybody care about managing them? For years records managers have been pushing compliance, which is great when it comes to us dealing with senior management and getting them to invest in systems to manage records. But now we have to get that same senior management to put stuff into the systems.

Managing records is not rocket science. We've been doing it since the days of black and white, as my kids used to call them, back when more than just television was black and white, when we had registries to look after the records. In fact we didn't even call them records back then.

The mail would come into the registry, it would be opened - carefully slit on three sides to make sure nothing was left inside the envelope - and

it would be registered in the inwards correspondence register according to the date of origin. The registration clerk would make a decision about what file to put it on and send the correspondence off to the action officer attached to the file.

The action officer would draft a reply and send it to the 'girls in the typing pool' who would type it with 2 carbon copies and send it back for signature. Then back to the registry, register the reply in the outwards register, send off the original, put a copy on the file and another for the float file.

When the file got full it was replaced with a new one and eventually the old one was sent off to archives. After all that we'd grab a cup of tea from the tea lady's trolley.

The procedure I just described was the same in 1998 as it was in 1978, with the exception that the registers were in TRIM 3.1, the tea lady had been replaced by the rapid boil machine and the girls in the typing pool had been replaced by the desktop PC. In 2008 most of our records are electronic, the tea lady is an instant cappuccino machine with fair trade coffee, and the girls in the typing pool are running the company.

Keeping records is not the problem. We keep stuff now. We've always kept stuff. Everybody keeps stuff. The problem is that we keep too much stuff and it has no real structure. We can overcome the structure by implementing systems to manage it but how do we educate people to use the systems properly?

It's been said that 25% of the average working day can be spent searching for information and then less than half of the information found is of any use.

Dr Susan Marchant, Australia's own management guru, says that putting things on file is about organisation. Of course she was speaking about personal organisation and self-management, but it still holds true.

We need to keep the information we use regularly nearby while keeping information we need less frequently out of the way. Managing records is about keeping track of today's information for tomorrow; this week's information for next week; this year's for next year.

You say you're too busy and your job's too important, so why should

*FIRST AID FOR RECORDS: Continued from page 41*

you care about managing records? What's in it for you?

I can make you 25% more efficient in your day-to-day work. I can make the information you work with 50% more valuable. I can take a big chunk of the stress away from your already stressful day. I can help you do your job, that's what's in it for you.

The 2007 Victorian Auditor General's report into Records Management in the Victorian Public Service recommends the adoption of a "strategic approach" to records management.

In fact the report uses the words strategy or strategic 23 times in the executive summary alone and only one of those is in reference to the Victorian Electronic Records Strategy (VERS). But what does strategy really mean? Is it just the latest in a long-running series of buzz-words?

Strategy derives from the Greek words, stratos, multitude, army, expedition – literally, that which is spread out – plus agos, leader. From a military perspective strategy means to place your forces in a position from which they can fight the battle.

This not only involves their physical location but the provision of the right weapons and supplies as well. So in terms of applying a strategic

What are we accountable for? We're accountable for the decisions we make, the advice we give and anything we do in the course of our work. Anything that affects our accountability should be a record.

## **B – Business Activity**

Every business transaction we conduct is a record.

This can be something as simple as paying an invoice to something as complicated as a criminal investigation. Even the development of new legislation is a business activity. Records track what we and our work units do.

## **C – Communication**

All forms of communication sent by our work units or received by our work units that actually relate to the work our work units do should be recorded.

That means mail, email, newsletters, media releases, speeches, promulgation of policy, phone calls, conversations and meetings where decisions are made and even SMS messages and Post-it notes if they relate to our work and we're required to act on them.

**The problem is that we keep too much stuff, and it has no real structure**

approach it means that we have to provide not only the right environment but the right tools to get the job done. It also means that we need to plan for the management of records and to provide leadership.

OK, so what exactly is a record? How do we reduce the volume of stuff we keep by only keeping the stuff we need to keep?

For most of us in the records business we follow a fairly complicated process of defining evidence, documentation, responsibilities, exclusions, systems, obligations, schedules and so on. It's not easy to explain to people who have only the vaguest concept of records yet are expected to take responsibility for records as we move into an electronic environment.

We can give them fact sheets and guidelines to follow but when it comes to the crunch it is still going to be up to an individual sitting at a computer asking, is this email/word document/PDF a record, or is it not? Our aim is to make that decision as instinctive and as instantaneous as we can make it without ever having to resort to external aids.

## **Opening the First Aid Kit**

In the first few seconds of an emergency, First Aiders use DRABC to remember the immediate steps to be followed. Danger, Response, Airway, Breathing, Circulation. We RIMs need something as easy to remember as that. A tool for aiding our colleagues comprehend the importance of good recordkeeping to the life of their organisation. Something as simple as ABC.

I call it First Aid for Records – ABCDE

## **A – Accountability**

As employees, we are all accountable. For public servants it's written in stone in the Code of Conduct and to quote the Victorian Auditor General, "Accountability is underpinned by good recordkeeping". But the same can be said for people working in the private sector as well.

## **D – Decisions, Decisions, Decisions**

Decision-making 1.01 tells us to document important decisions. Particularly decisions that affect other people and agencies. This of course includes any relevant documentation or information that was used to base our decisions on.

In years to come when we're asked why that decision was made, we can honestly say, "Well, your Honour, it was like this..."

## **E – Expectation**

No list is ever going to be complete and you are the person who best knows your business.

If you're presented with a particular decision, meeting, transaction or occurrence, and you feel that it would reasonably be expected by an ordinary person to create a record of that occurrence then you should create a record.

If you expect that something should be a record then make it a record.

It's your decision. I won't stop you and you'll never be questioned about why you decided to make a record, only why you didn't bother to make one.

ABCDE. Hard isn't it?

A – Accountability

B – Business Activity

C – Communication

D – Decision Making

E – Expectation

A few years ago, Mike Steemson made a presentation to the RMAA -ASA convention in Hobart on ISO15489. What was truly memorable about it was that he sang his presentation to the tune of 'Frosty the Snowman'.

Believe it or not, by adding a couple of dooh dahs to this you can actually sing it to the tune of 'Camptown Races':

A – Accountability, dooh dah, dooh dah,


B – Business Activity, o dooh dah day,

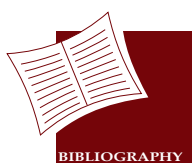
C – Communication

D – Decision Makin'

And E – if you are still confused

What's your Expectation?

Scary isn't it? Start singing the praises of the ABCDE approach to records awareness. And the next time someone in your organisation shows a lack of sensitivity to good recordkeeping practice, give them RIM first aid, the ABCDE way. 



Victorian Auditor Generals Office (2008), Records Management in the Victorian Public Service strategy. Dictionary.com. Online Etymology Dictionary. Douglas Harper, Historian. <http://dictionary.reference.com/browse/strategy> (accessed: March 11, 2008).

## The Author

**Allen Hancock** is the Manager Records Standards and Consultancy with the Victorian Department of Human Services. In this role his main task is to ensure that every staff member and business area within the department understands their recordkeeping responsibilities, are afforded the necessary tools, have access to standards and support to satisfy those responsibilities, and are held accountable to do so.



Allen has more than 30 years association with the records industry working as a member of the Australian Regular Army, Monash University, Department of Defence as the manager Defence Archives Victoria and as the manager Army Health Records Office, and most recently BHP Billiton Archives.

# E-Discovery *what's your best defence?*

Get the facts from TOWER Software with Gartner® Research

**Hurry!**  
Available for a  
limited time only

Start your journey to E-Discovery with  
**Information in Context: The E-Discovery Journey**  
To receive your copy of this informative publication  
visit our website: [www.towersoft.com/ap](http://www.towersoft.com/ap)

**TRIM Context 6 Release 2®** delivers proven productivity gains and compliance policy management, helping your organisation prepare for E-Discovery.

TOWER Software is a global leader in the delivery and successful implementation of industrial strength ECM solutions.

 **TOWER**  
SOFTWARE  
[www.towersoft.com](http://www.towersoft.com)

# KEYWORD AAA:

## Providing Potential Opportunities for its Application in a Financial Reporting Framework

By Rosetta Romano

Development of the Keyword AAA by the ACT's Territory Records Office has resulted in the discovery that Keyword AAA no longer needs to be constrained in a records management silo, but can venture into the taxonomy of other business applications. This report explores the possibilities.

**T**he Director of Territory Records is the regulator for records management in the ACT Government Service (ACTGS). The position, and its supporting administration, the Territory Records Office (TRO) were created under the Territory Records Act 2002.

This legislation was enacted to address specific concerns raised in a number of audit reports by the ACT Auditor-General, and in other controversies including the Canberra Hospital Implosion. These reports identified a series of failures by the Government to adequately account for its decisions in the absence of a regulated records management regime.

Records management in the ACTGS covers the administrative and the regulatory arrangements. Administratively, file creation, storage and file/mail movement is the business of a newly created Shared Services arrangement. The regulatory role is undertaken by the TRO, a small office of four whose responsibilities include:

- Developing recordkeeping policy, standards, guidelines and advices;
- Processing records disposal/authority with agencies;
- Providing administrative support to the Territory Records Advisory Council for public consultation; and
- Coordinating whole of government contract arrangements to engage recordkeeping services.

Whilst implementing its records regime, the TRO has realised many benefits through the process of developing the specific records management tools that are used by many organizations. With relatively simple changes to the use of the tools that support the principles of the Standard for Records Management ISO 15489 2001, the TRO has achieved particular improvements that are explained in this article for consideration by other jurisdictions.

Explicitly, the developments in the use of the Keyword AAA thesaurus for application in the creation of records disposal schedules has simplified the process used to: manage consistency in records management across the ACTGS; and more recently to identify opportunities for integration of records management elements in other business systems such as a Financial Management System.

### Keyword AAA

Keyword AAA is the general common administrative thesaurus developed by the State Records Authority of New South Wales (NSW) for the consistent classification and titling of records.

The Keyword AAA thesaurus is used in the Commonwealth Administrative Functions Disposal Authority (AFDA), developed by the National Archives of Australia.

AFDA provides the retention periods for records belonging to a common set of 17 functions. These are functions assessed as 'common' to all governments undertaking the business of delivering 'public service'. They include the functions required to engage, maintain and account for the staff, facilities, tools and funding provided to the Commonwealth, State, Territory and Local Governments.

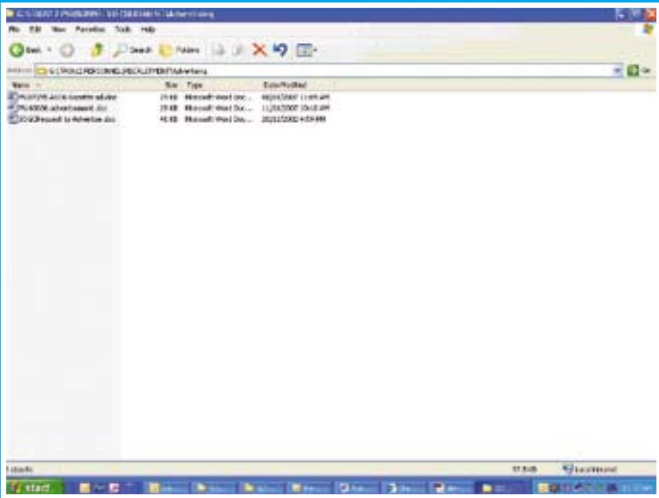
The NSW Authority's Keyword AAA thesaurus was assessed for implementation and was considered to be a suitable match to the ACTGS functional structure.

The ACTGS has adopted the classification under a whole-of-government licence agreement with State Records Authority of NSW. Slight global changes to the classification were required to remove redundant function/activity terms that did not apply to the Territory. The customised version is known as the Territory Version of Keyword AAA (TVKAAA).

The AFDA was also assessed and found to provide a suitable match for implementation in the ACTGS. Slight global changes to the Authority were made, including the retention term 'Retain as Territory Archives'. The resulting customized version is called the Territory's Administrative Records Disposal Schedule (TARDiS). TARDiS is based on the set of 17 common administrative functions in TVKAAA.

The recordkeeping taxonomy of function/activity may be applied in other business applications. For example it appears to be directly applicable to the current Australian Accounting Standard AAS 29 Financial Reporting by Government Departments that will be replaced on 1 July 2008 by Australian Accounting Standards Board Accounting Standard AASB 1052.





### Figure 1: Shared drive based on TVKAAA

Record Services Request for Creation of New File

and nominate role of officers allowed access to the file (limits to be authorised by supervisor or above)

Times from the TESSIS Thesaurus last modified on: Thursday, 7 October 2004

Factor:

Activity:

Authority:

Free text may also be used, the additional information can be added in the free text field to help describe the file contents (eg date/year)

**Authority:**

Enter type first character for activity/detail from an on-line encoder wheel to select:

- ☐ **Related Terms:** ☐ Controlled and ☐ ESTABLISHED and ☐ Marking

Reserve: The process of resourcing which includes options for approval for all existing vacancies, advertising vacant positions and handling applications, interviews, selection, cutting and appointment, also includes recruiting volunteers.

Physical location:

If your area doesn't have Active Officer Cade, your Name self office or ring Record Services on TESSIS

ENTER:

**Records Disposed Class:**

## Figure 2: eFile Request Form

[illegible]

### Figure 3: a.k.a.® Disposal plan with unique numbering

KEYWORD AAA: Continued from page 45

The requirements of AASB 1052 will be identical to the requirement of AAS 29. Both standards require the identification of major activities of government departments that are to be presented as separate disclosures in a complete set of financial statements.

The main benefit of the records management regime is that its structure is organisationally independent. The requirement to adjust processes due to an organisational restructure does not occur as information is created, stored and managed in terms of functions and activities.

Use of the established records management taxonomy for Functions and Activities in other business systems provides:

- an established system of information management; and
- traditionally organisationally-based recording system the ability to be organisationally independent, and allow across-time comparison in organisations that are constantly changing in form.

The ACTGS uses Departmental /Territory Authority Outputs for the assessment of major activities defined by AAS 29 for financial reporting. Another application for the records management business classification analysis is the justification for the non/applicability of the accounting standard by a particular government department.

Other local governments and government departments may find the ACT experience useful as an example of how possibilities can emerge from the development of solid taxonomies or information naming/storing structures in records management.

### **Mandated Elements to Manage a Whole of Government Thesaurus**

The TRO mandated three important policies to maximize the success of its records management regime. These are:

1. The TVKAAA Thesaurus is used as the classification scheme for the ACT Government's shared/common drive structure creating the terminology consistency between electronic and paper records;
2. The TVKAAA scheme is presented as selections for users naming file titles using the electronic file request system eFile;
3. The Thesaurus Manager maintains a single whole of government thesaurus, and processes all specific agency records disposal schedules in conjunction with agency records managers to maximize integrity and consistency;
  - a) Each function and activity term, and its scope note can only be listed once in the whole of government thesaurus; and
  - b) The function/activity set in the thesaurus is displayed identically in its related records disposal authority.

Mirroring the thesaurus in the common drive assists agencies to identify gaps.

The gap analysis is undertaken by conducting a business classification exercise and identifying records created in the agency, under the Function/Activity sets of the 17 common functions of TVKAAA.

The records that cannot be mapped require the development of new terms in the thesaurus. Together the combined TVKAAA and specific thesaurus form an integral part of an agency's records management program for creating, maintaining, tracking, storing, retrieving, appraisal and destruction purposes. Incidentally it also provides meaningful records terminology to agency staff for recordkeeping training purposes.

Once an agency has worked with this combined thesaurus for some time, the agency records manager builds the confidence to justify the development of a specific records disposal schedule. Articulating the gaps builds an ability to develop scope notes for the new unique functions/activities to describe the records created within the agency.

As agencies began to develop business specific thesauri, the TRO became engaged in complex thesaurus management. Negotiating specific activity titles that were unique, stand-alone and clearly distinguished from

other terms was vital in building confidence in the thesaurus.

It became apparent that to manage over 51 separate schedules a whole of government view in a single database was required. The TRO uses a.k.a.® as its thesaurus management tool since 2002, and this was used to create the new database.

### **TRO Modifications to Keyword AAA**

The development of a whole of government database required some changes to the NSW Keyword AAA. In summary this included:

- applying a unique three digit code for each function (to remove requirement for adding prefix codes to distinguish between databases e.g. Advocacy A. or Attorney General's A.G.);
- including the code at the end of scope title (to maintain alphabetical integrity in the thesaurus);
- applying a unique three digit code for each activity;
- including the activity code at the end of the scope title (to maintain alphabetical integrity in the thesaurus); and
- applying a three digit code for each disposal class (to ensure sequential numbering in excel and access database display).

The application of unique numbering for functions and activities also provides a visual guide for the database developer. See figure 4 where the unique number that results e.g. 174.158.001 is partially represented as a label in the Path field. It is representing Function number 174 and the Activity number 158. For the a.k.a.® package the record number is manually entered by the operator. The display in the Path field provides a visual prompt for record number construction.

Unique numbering also presented an opportunity for discrete activity and disposal class sets. Over and over again it was seen that in the development of disposal schedules, similar activities were being requested by agencies. For example all specific schedules contained the activities of advice, procedures, policies, tendering, etc.

As the pattern of standard activities emerged, it also became obvious that the disposal classes associated with these specific activities could also be predicted. In fact to manage the whole of government database, a set of disposal activities associated with specific functions could be recommended. Of course, business rules could justify variances, but on review the instances of deviation have been rare.

With a set of Activity/Disposal classes, came an opportunity to develop transparency. This is particularly evident when the Territory Records Advisory Council, made up of representatives from the ACT community, is able to anticipate the numbering applied to disposal classes, and also the retention period related to the Activity/Disposal class set.

### **Opportunities Provided by Regular Reviews**

The ACT Government records regime requires 5-yearly reviews of all elements including agency management programs. Both TARDiS and TVKAAA are due for review this year (2008). This provides an opportunity to introduce the concept of other business applications leveraging on the records management structure/taxonomy.

The lessons learned in applying a records management regime can be useful in other disciplines. Consideration of applying the function/activity coding in a chart of accounts could potentially expand the application of the information drawn from financial reporting.

### **Application of Keyword AAA in the Financial System Chart of Accounts**

A financial system chart of accounts is the classification system used to capture financial spending information for reporting purposes. In the ACTGS the Chart of Accounts captures agency (organizational) expenditure information answering:

- Who spent? (Business unit code);
- How much was spent? (\$);
- What category was it spent on? (Account code); and
- When was it spent? (Period).

By extending the inputs in a chart of accounts to capture the records management information relating to function/activity, then in addition to the above, reporting could easily include information that is not organisationally-focused. This is the type of information that is required to produce an annual report i.e. through the outputs and outcomes.

In the ACTGS the outputs are reported by Agency. The same outputs may already have been defined in the records management system, albeit at the detailed level of function/activity.

By mapping the functions/activities required to undertake an output, a broader whole of government view can emerge. Thereby removing the organisational constraint and viewing whole of government outputs.

This exercise may already have been undertaken by the records management personnel of an organisation in developing a business classification scheme.

If the information from a mapped Output in terms of function/activity is expressed in the chart of accounts, the resulting information can take on extra dimensions. Not only could the output be reported as a summary level, the details related to the lower level of Function, and at the lower level of Activity may also be reported.

The benefit of this is essentially that the entity can report on function/activity expenditure irrespective of the changes within the organization by capturing:

- What function was the expenditure used for? (Records Management -Function code); and
- What activity of the function was conducted? (Records Management - Activity code).

Further extension to an existing code that capture supplier and item codes such as the United Nations Standard Products & Services Code (UNSPSC) results in additional scope to reporting on:

- What service/product was purchased? (UNSPSC).

Other particular extensions to the codes used in a chart of accounts may support the capturing of specific data that is useful to an organisation for financial/other reporting purposes. For example, it may be interesting to cultivate an understanding of which suppliers the organisation used:

- Who received the money? (Contract/Procurement supplier information).

## ACT May be Unique But its Lessons are Widely Applicable


In the ACTGS the opportunity to embrace records management concepts in the financial systems coincides with the merger of multiple instances of Oracle Government Financial in the development of a single instance Chart of Accounts.

It is rare indeed to have development of a single chart of accounts, particularly in whole of government reporting for state or commonwealth across-agency initiatives.

In organisations using disparate financial systems, or different instances of chart of accounts an investigation of other technologies to achieve the same result may be required. For instance the use of Extensible Business Reporting Language (XBRL) may provide a solution.

However, the long-term benefit of reusing the records management taxonomy in the financial management taxonomy appears to provide multiple reporting benefits.

By making some minor adjustments to introduce unique numbering in Keyword AAA, and considering its coding within a Chart of Accounts, Records Management principles and data will begin to emerge in other business information and reporting. Imagine a Public Service where records management is reflected in its financial reporting.

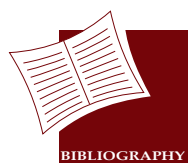
Recognising the available opportunities to leverage on the intellectual property existing in the records management regime for use in other business management systems may play an important role in raising the profile of records management. 

## The Author

**Rosetta Romano** has over 26 years experience in the Public Service. She has a BA in Accounting, a Graduate Certificate in Public Sector Management, a Graduate Certificate in Business Informatics, is a fellow member of the CPA. For the last 3 years she has been working in records management area as the Information Quality Manager in the Territory Records Office of ACT Government.



She is currently undertaking a Masters in Information Sciences (Research) with the University of Canberra and her topic considers ways of using existing business taxonomies in government organisations for better reporting. She may be contacted at [rosetta.romano@act.gov.au](mailto:rosetta.romano@act.gov.au) or alternatively at [r.romano@student.canberra.edu.au](mailto:r.romano@student.canberra.edu.au).



For example : Auditor General's Office - Bruce Stadium Performance Audit 2000 <http://www.audit.act.gov.au/auditreports/reports2000/bruce/report01.pdf>.

Bennett, Scott, 2000. The End of the Carnell Government in the ACT. Parliament of Australia, Parliamentary Library Research Note

13 2001-01 31 October 2000. <http://www.aph.gov.au/Library/pubs/rn/2000-01/01RN13.htm>, 17 March 08

Standards Association of Australia, Australian Standard – Records Management (AS/ISO 15489 2001. Sydney, Standards Association of Australia 2001.

Thesaurus : An alphabetical presentation of a controlled list of terms, linked together by semantic, hierarchical, associative or equivalence relationships. Such a tool acts as a guide to allocating classification terms to individual records. (Standards Association of Australia, Australian Standard AS ISO 15489, Part 2, Clause 4.2.3.2)

In a thesaurus, the meaning of the term is specified and hierarchical relationships to other terms are shown. A thesaurus should provide sufficient entry points to allow users to navigate from terms that are not to be used to the preferred terminology adopted by the organisation. <http://www.naa.gov.au/recordkeeping/control/tools/appendixB.html>

Records Disposal Schedules are documents approved by the Director of Territory Records, which sets out the types of records an agency should make and how long they must be kept. For examples see <http://www.territoryrecords.act.gov.au/recordsdisposal> 26 March 08

Classification : Systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods, and procedural rules represented in a classification system. ISO 15489-1:2001 (E) 3.5

a.k.a.® is software designed to support the development of records taxonomies and retention schedules for Australian government agencies in accordance with the framework outlined in ISO15489.

a.k.a.® is electronic records and document management system neutral. Records Advice Number 19, What is a.k.a. & why do we use it? [http://www.territoryrecords.act.gov.au/\\_data/assets/pdf\\_file/0008/55880/Records\\_advice\\_No.19\\_-\\_What\\_is\\_aka\\_14\\_Feb\\_08.pdf](http://www.territoryrecords.act.gov.au/_data/assets/pdf_file/0008/55880/Records_advice_No.19_-_What_is_aka_14_Feb_08.pdf) 26 March 08

As the TRO presents the disposal classes from highest to lowest retention period order, the sequential numbering is not maintained where a subsequent amendment affecting order is notified.

Business Classification Scheme – where categories in the classification equal the function/activity set. See the definition of Classification vi

# Information Seeking Behaviour of Electronic Document and Records Management Systems (EDRMS) Users: Implications for Records Management Practices, Part 3

By Pauline Singh, ARMA, Professor Jane E. Klobas and Professor Karen Anderson

This series has studied whether the way RM professionals manage records in accordance with the ISO 15489 standard is consistent with the information seeking behaviour (ISB) of Electronic Document and Records Management Systems (EDRMS) users. In this the final article in the series, the authors report their research findings.

All four organisations studied have implemented functional classification schemes and thesauruses based on the Keyword AAA (Accuracy, Accessibility, and Accountability; KAAA) or the Keyword for Councils (KFC) schemes.

## Classification Scheme/Thesaurus

Three of the four organisations have implemented the KAAA thesaurus developed in 1995 by the State Records Office of New South Wales (NSW). The KAAA is a keyword thesaurus of general EDRMS based on the keyword classification method. It covers administrative terminology common to most government organisations and 'is constructed to reflect an organisation's business functions and activities as they are documented by records', (Robinson and Knight n.d.).

KAAA and KFC use a structured hierarchy of keywords, activity, and subject descriptions: keywords are allocated to describe broad business functions; activity descriptors describe business activities; and subject descriptors are used to describe subjects or topics that connect related business transactions (State Records New South Wales, n.d.).

One organisation implemented the KFC, an adaptation from KAAA for local government councils. Similar to the KAAA, the KFC is a thesaurus designed for use in classifying, titling and indexing all council records in all technological environments (State Records New South Wales, n.d.).

The functional KAAA thesaurus is uploaded using the thesaurus modules of the EDRMS in two of these organisations. In the remaining two organisations, the thesaurus is uploaded using a third party software. In one instance the thesaurus is integrated with the

EDRMS, and in the other it is not.

None of the RM professionals in the four organisations consider the training of users on the use of the classification scheme as an information retrieval tool to be a requirement, as they had the following perceptions:

- 1) the classification scheme is a RM tool to group records for destruction, something that users are not interested in knowing about,
- 2) users only want to know the file number into which they should be filing their information and are not interested in gaining an understanding of the classification scheme,
- 3) users only search using the metadata fields, not the classification scheme, and
- 4) users are aware of the Free Text part of the classification scheme, and these are the terms they are likely to use when searching.

Figure 4 explains the search tools users have at their disposal for information seeking in the EDRMS and how the RM professionals use these tools for their RM tasks. It shows how users only have one search and retrieval tool made available to them, namely me-ta-data. In comparison, RM professionals have both metadata and the classification scheme as search and retrieval tools.

The classification scheme is not perceived as a tool which, as stated in section 4.2.2 of ISO 15489-2 (International Organisation for Standardisation, 2002) organises and groups like information, links interdisciplinary records so as to enable sharing of information within the organisation, and provides improved access, retrieval, and use of records in the organisation.

Exon, in her RMAA conference paper and article from 1997, points out that the 'major purpose of thesaurus has always been as an aid to efficient retrieval' (Exon 1997).

Hence, although the thesaurus and classification scheme are





## INFORMATION SEEKING BEHAVIOUR PART 3:

Continued from page 48

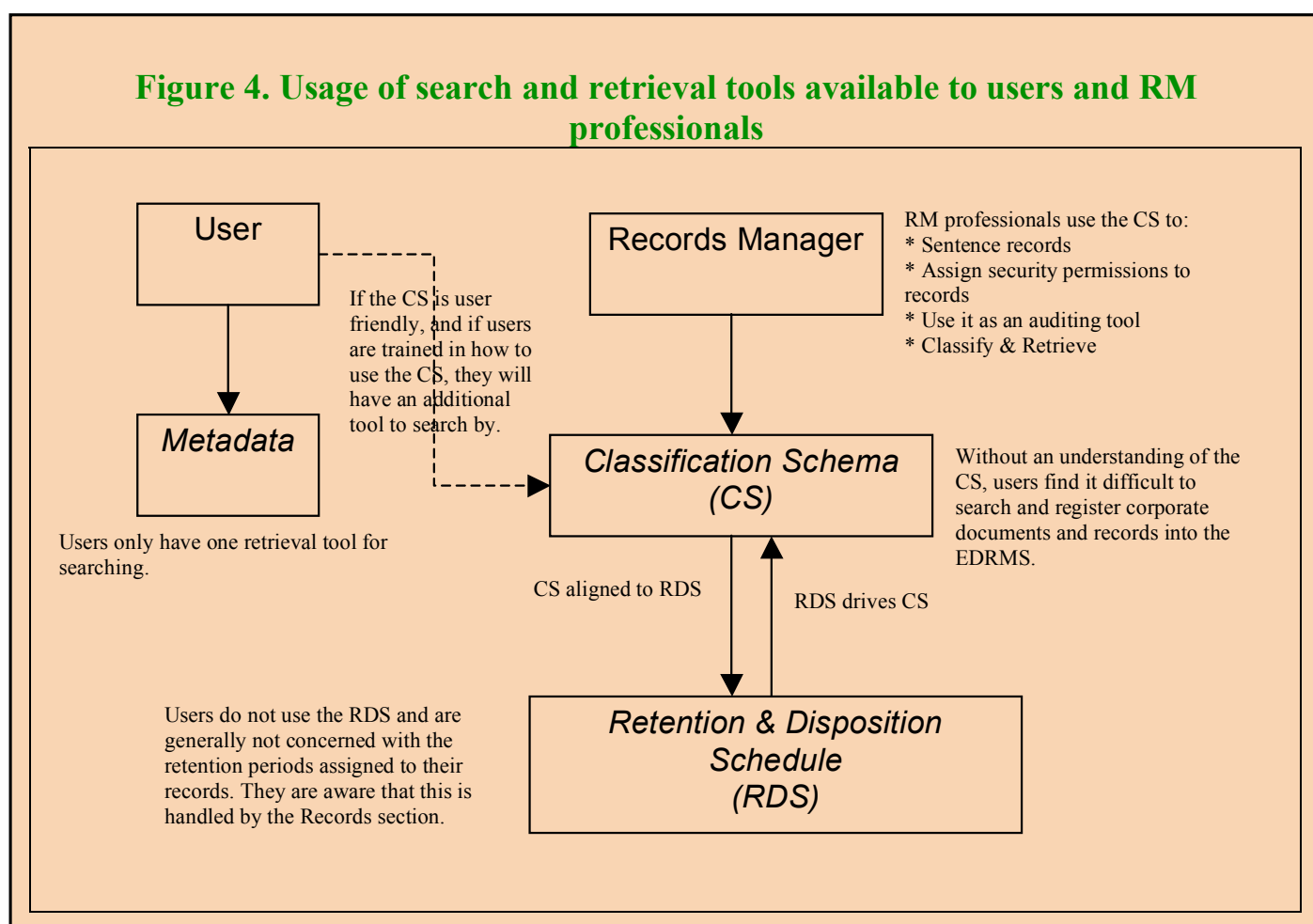
implemented in the EDRMS in compliance with RM principles and practices, training on how to use it is not provided to users in three of the four organisations. Thus, users did not know how to work with and use these retrieval tools for their information search and retrieval in the EDRMS.

Organisation C provided training on the classification scheme to users, but users still found it hard to comprehend the logic used to classify information. The following quotes from users in Organisation C verify their views and work experience using the KAAA

we used to file things, and there are occasions where putting stuff on particular files doesn't seem logical in EDRMS of how the structure's been arrived at. And also there are situations where stuff doesn't quite fit and you're almost, you try and find terms that are close to what you think is the right term, and you put stuff there, and again, you know, there is the concern that you know, it's fine today probably fine in a week, but in 12 months time if you had to find the same document, you may struggle. Look, again, you can always search on the document title if you can remember a particular term that related to the document, but if you knew not a lot, and you know, sometimes you might, I think you might struggle to find particular things."

Director Information Manager.

**Figure 4. Usage of search and retrieval tools available to users and RM professionals**



classification scheme in the EDRMS:

"Cumbersome, unclear to the novice, complex when it could be much simpler." Secretary & Records Focal Point.

"I kind of, I don't know, I neither like it nor dislike it in the sense of it's a Classification system [...] I don't find it intuitive but I guess I've grown to accept that it must have some sort of logic." Director Human Resources.

"I mean it's Keyword AAA, which I don't know if it's one of the great classification schemes that are around, but it makes sense I think to the person that put it together. Sometimes it doesn't really make sense to me." Director Information Manager.

"Look, I can understand the logic, I guess it's different to how

"I know there might be an article in the Western Australian about the prices of land increasing, this sort of thing, do you put it under 'valuer general'?, do you put it under 'land tax'?, do you put it under 'advice'?, do you put it under 'media'? [...] And you know, depending on what perspective you're approaching it from I might look at it from a different perspective as someone else but we could possibly both be right, you know what I mean." Team Leader, Land Tax.

The thesaurus module is integrated in the EDRMS for three of these organisations. However, these organisations did not make users aware of either the thesaurus or the classification scheme, and none of the organisations promoted the classification scheme as a search and retrieval tool.

Thus, users relied heavily on using metadata for searching, but this is not always the most effective or efficient search method. It explains why 68% of users relied on searching by the document or record title metadata field. It also explains users' frustration when documents and records are not titled meaningfully, as verified by their quotes:

"Probably searching for other people's documents. [...] Because they don't Title them correctly. [...] So brief Titles, abbreviations, just Titles that I wouldn't call something, so I find it hard to find others." Training Consultant.

"That people haven't put the right information in the Title Word. That they've used acronyms, or they've used their interpretation of what it is. They haven't, they've omitted information. A good example of that is that I've just recently been given access to search for some of these electronic, the scanning of bills that I get, but they haven't put the account number in the search, so I can't search on the account number. So it's usually the information in which it was recorded was poorly, inconsistent." Manager Communications, Systems & Technology.

"People aren't consistent in their titling, nor are they thoughtful in their titling. I don't believe that they give it enough thought and don't use the principle that in ten years time when this is no longer current nor relevant in the workplace will somebody be able to find this by the Title that I've described." Admin Officer, Risk & Compliance.

As Figure 4 indicates, classification schemes are aligned to the RDS and thus the retention periods of records actually drives how records are classified and thus drives the classification scheme.

This results in classification schemes that fragment the grouping of records by retention periods using the activity descriptors in KAAA and KFC, instead of grouping like records together. This, in turn, makes the classification scheme less intuitive in relation to how users work and think of retrieval using the EDRMS, thus making the classification scheme the least preferred information seeking characteristic of EDRMS users:

"The classification structure is probably one of the last ways I'd use of finding things. As I said before you know, going to that File Plan, tree structure to find things, I'd use that after I've tried a couple of other different ways of finding things." Director Human Resources.

We observed that users need to be made aware of the classification scheme not only for searching information in the EDRMS but also for registering information into the EDRMS. During the registration process, users need to decide where they are going to file their records, and if they lack an understanding of the classification scheme, they may misclassify records.

This leads to difficulties or failures when seeking information in the EDRMS, not to mention premature destruction of records. About 28% of the users commented that the most difficult metadata field for them to complete is the 'File Number' field.

These users asked if this metadata field could be removed from the registration screen. Three users admitted to taking the easy option of registering records into the EDRMS by classifying their records into the recently used folders displayed in the pick list of their registration window.

This again indicates the ambiguity and lack of understanding of how the classification scheme in the organisation works. The quotes from users verify their difficulty in identifying where to file the record:

"I don't (search for containers) any more, I just use the ones that I use all the time." Manager Communications, Systems & Technology.

A participant highlighted that his colleagues do not file information pertaining to a particular government agency by what business function had been performed for the agency. Instead, they picked one business function and filed all information regarding the agency into the one single folder in the EDRMS:

"Analysts are not, if they do work for a particular agency, they are not filing it by whether it's ADVICE agency, whether it's BUDGET agency, whether it's CAPITAL WORKS, OPERATING EXPENSES agency? They tend to just pick one area, maybe ADVICE and put even the BUDGET there?" Secretary & Records Focal Point.

"Look, the most difficult is not so much searching for information, it's again going back to just trying to find the right file to put it on. Sometimes it's relatively easy, other times, as I say, it can be painful and difficult, and again there has been more than one occasion where there's just, it just doesn't quite fit the File Plan, and you say, oh, no, this is, you've got to add something or something, or you'll put it somewhere where it looks like it will fit, knowing full well if you don't find this thing in the future, you're going to struggle, but you just sort of hope it's never, you never have to come back to it." Director Information Management.

## Retention and Disposition Schedule

All the organisations have a corporate RDS developed, approved and implemented in the EDRMS to sentence records stored in the EDRMS. The retention periods are assigned at a folder level when new folders are created and this retention period is cascaded to all the contents filed within the electronic folder.

Thirty-eight users stated that they are not interested in the retention periods for records when seeking information in the EDRMS. They have been informed, and are satisfied with that knowledge, that retention periods are applied to records and they will be consulted prior to the destruction of a record by the records section.

Two of the 40 users stated that the retention period is important to them as they handle sensitive information that needs to be retained for a longer period of time, and also because they usually search for historical information and need assurance that the information will be retained for a long time. These two users stated that they checked the retention periods assigned to some records whilst seeking information in the EDRMS.

## Security

All the organisations have comprehensive security models implemented in the EDRMS that ensure that only authorised personnel access information. Information can only be deleted by the Records Section and not by general personnel. Apart from organisation B, the rest of the organisations do not have their EDRMS security model documented.

The users are aware that there are security settings implemented in the EDRMS to ensure that access is provided only to authorised personnel in the organisation and within business units. They have a general understanding that they have access to information stored in the EDRMS that belongs to their immediate business units and projects or committees with which they are involved.

We observed that users have little understanding of the details of security settings using 'caveats', record or document types implemented in the EDRMS.

## Training

All the organisations provided RM and EDRMS training to their users during the implementation of the EDRMS or employee induction programs. All the EDRMS training provided to the participants was face-to-face hands-on training sessions in classroom style settings, with users having access to individual PCs. The training lasted two to five hours.

The training programmes covered a range of topics: configuring the EDRMS, registering documents via check-in/check-out functions, work flow processes, searching, and working generally with the EDRMS. None of the four organisations provided training on the use of the classification scheme implemented in the EDRMS for searching and retrieving information from the EDRMS.

See Figure 3 (February 2008 *IQ*, page 54) on the types of EDRMS training provided to users and the section titled 'The Effect of Training on ISB'.

## Monitoring and Auditing

The organisations have monitoring and auditing processes in place to check on the quality of the data being entered into the EDRMS. The Records Section performs these tasks. Any misclassification or inappropriate document titling is followed up with users for remediation. If users do not adhere to the remediation actions, it is escalated to the line managers for action. If this fails, in organisation D, the issue is flagged to the Audit Department for follow-up.

## Discussion

We observed that all four organisations have implemented the pillar RM principles listed in Table 1 (November 2007 *IQ*, page 39) and that their information management practices in the EDRMS does adhere to records management principles and practices.

The only variations of the RM principles between the organisations are in the implementation method in the types of policies, procedures, classification schemes, retention schedules, and training materials the organisations have developed.

The organisations have implemented RM policies and procedures that are endorsed by senior management in their organisations. The RM documentation outlines that records created and received by the organisation are to be managed according to records management practices and the legislative requirements to which the organisation needs to adhere.

The policies and procedures have been implemented in the organisation by communication to relevant staff, through campaigns during the launch or as part of the RM induction programs to new staff. The documentation is also published on the corporate intranets and in the EDRMSs.

Overall, the RM professionals perceived the EDRMS implementation in their organisations to be successful. However, as could be expected, there is resistance to the EDRMS from some user groups.

Our assessment of how the RM principles and practices used to manage records in the EDRMS interfaces with the ISB of EDRMS users is presented next.

## Stage 1: Starting Search

The RM policies set precedence in mandating the role and use of the EDRMS in the organisation. If there are policies in place that state that the EDRMS is the corporate repository for records, then users will use the EDRMS to register their records and will know that the EDRMS is the tool to use for seeking records. Thus, they start their information seeking in the EDRMS.

A number of users stated that they use the EDRMS in their organisations because it is the mandated corporate repository for records. Likewise, the RM procedures, standards, and guidelines, provide the guiding principles for users on how to use the EDRMS and what to expect from the RM infrastructure in the organisation.

The training materials for RM and use of the EDRMS form part of the RM procedures. This documentation also establishes the framework for the ISB of EDRMS users.

## Stage 2: Formulating Search Strategy

Three key RM principles affect this stage of the ISB pattern: 1) metadata standards, 2) classification scheme, and 3) training. Findings indicate that the most common and preferred ISB for EDRMS users is searching using metadata elements.

However, none of the four organisations studied have prepared a formal metadata standard documenting adherence to metadata standards such as the NWS Recordkeeping Metadata Standard (State Records New South Wales 2001), Recordkeeping Metadata Standard for Commonwealth Agencies (National Archives of Australia 1999), or the Dublin Core Metadata Element Set (International Organisation for Standardisation 2003).

However, all four organisations have implemented metadata elements in the design of the EDRMS, and they use different record type attributes to capture relevant metadata for the specific record type.

Findings also indicate that users are not using the classification scheme to conduct their information seeking in the EDRMS. All four organisations have developed and implemented the KAAA or the KFC thesauri.

It is interesting to discover that although records managers place importance on this tool when classifying information, its usefulness for searching and retrieving information is not passed on to users.

None of the four organisations promoted or trained users to use their respective classification schemes to seek information in the EDRMS in the way that they have done concerning the use of metadata fields.

Only a couple of the 40 participants displayed any understanding of the classification scheme or used it when searching the EDRMS. On the contrary, they preferred to use metadata elements to search. This could be because of lack of training and promotion on using the classification scheme to search.

## Stage 3: Executing Search

This stage is not applicable to RM practices for the management of records.

## Stage 4: Processing and Evaluating Search Results

The RM principles of metadata standards, classification schemes, and training impact this ISB pattern. Training on using the EDRMS functionalities, such as filtering, sorting, and refining the search



results, will enable users to process and evaluate their search results.

Awareness training on the different record types and their associated metadata fields and classification schemes will enable users to perform better at this stage of their information seeking.

### Stage 5: Accessing Search Results

Apart from the RM principles of training and security permissions, none of the other RM principles influence this ISB pattern.

Security permissions are important as they determine what records users are authorised to view and/or make changes to.

Having access to a record will enable users to launch it and then finalise decisions on the search results by scanning and verifying it. The lack of access will prevent the user from launching the record and thus render impossible the next stage, 'Making Decisions about Search Results'.

Users were not asked about how they handled the information once they found it in the EDRMS, but it is theorised that users will either VIEW or PRINT the item, TAKE A COPY of it, or CHECK-OUT the item for editing.

### Stage 6: Making Decisions about Search Results

The RM principles influencing this ISB pattern are: 1) training, 2) security permissions, and 3) monitoring and auditing. Training provides the skills to scan and verify the contents of the records and decide if it matches the information being sought. Security permissions enable users to access the documents and make decisions on search results.

Without the right security permissions, users will not be able to access the information they are authorised to view, and consequently they will make poor decisions given their limited access to all the information that should be available to them.

Monitoring and auditing RM practices ensure good content integrity in the EDRMS, and thus enable users to make efficient decisions about their search results.

### Stage 7: Ending Search

This ISB pattern is influenced by the following RM principles: 1) procedures and standards, 2) training, 3) security permissions, and 4) monitoring and auditing. RM policies and/or procedure documentation will provide an indication of what information should or should not be stored in the EDRMS.

If information that should be stored in the EDRMS is in fact registered in the EDRMS, it will be possible to retrieve it and close the search rather than ending the search. The delivery of training programs, implementation of security permissions, and regular monitoring and auditing by RM professionals will influence users' decision to either STOP or CLOSE their search.

### Conclusion

Is the ISB of EDRMS users consistent with the way information is managed according to RM principles and practices in ISO 15489?

EDRMS systems in these organisations have been designed to adhere to records management principles as stated in ISO 15489 in order to meet regulatory compliance and for evidentiary purposes. In theory, the RM best practices advocated in ISO 15489 are consistent with the ISB of EDRMS users.

EDRMSs designed using this standard will provide users with the option to search and retrieve information using both the metadata

elements and the classification scheme.

Having studied the ISB of EDRMS users and having compared it to how records are managed in the EDRMSs in our case study, we conclude that there is a partial match between the ISB of EDRMS users and how the organisations have implemented the standard to manage records in the EDRMSs. The RM tools that assist with search and retrieval are the metadata elements and the classification scheme.

In our case study, we found that EDRMS users preferred to seek information using the metadata elements to retrieve records from the EDRMSs. However, the metadata elements pertaining to 'classification' terms is not used, nor preferred as a search option.

Participants do not use the terms in the classification scheme, such as the keywords or activity descriptor metadata elements, when they conduct a metadata search to seek information from the EDRMS.

A handful of users (30%) reported navigating the tree-view folder structure using the classification scheme to seek information. The classification scheme presented in a thesaurus form via the thesaurus module is not being used as a retrieval tool in the EDRMS either.

In view of how classification schemes are currently being used, which does not include an implementation as retrieval tools, we recommend that RM professionals consider, and perhaps implement, the strategies presented in the following paragraphs so as to overcome this potential limitation.

Firstly, conduct in-depth training on how to use the current classification schemes, whether it is the KAAA or the KFC. This is achievable by devoting a segment in the RM induction programme to this topic. The training needs to ensure that users have a working understanding of the classification scheme and know how to use it successfully to register information in the EDRMS.

Promote the use of the classification scheme as a retrieval mechanism in the EDRMS and train users how to conduct searches using the classification scheme.

We suggest that training includes an explanation of the structure behind the classification scheme; the scheme works by classification from the broader to the more specific topic, and the classification is structured to classify by business function, then by business activity and then by the subject matter or topic, etc.

Given our finding that task drives users' ISB, we recommend highlighting to the users the specific keywords in the classification scheme that their business unit will be working with often.

This will provide users with familiarity of the classification terms relevant to their tasks, thereby providing them with the confidence to search for information at broad subject levels by using terms in the classification scheme.

Our findings also indicate that training modifies the IISS (Individual Information Seeking Style) of EDRMS users. Hence, incorporating training on the classification scheme would lead to users making use of the scheme as an information retrieval tool.

Secondly, modify the classification schemes used in the organisation, such as the KAAA or the KFC, so that they become "user friendly". We believe that this can be achieved by making the classification schemes intuitive to the users' way of thinking by removing any ambiguity from the classification scheme and aligning it to meet the users' work processes so that it is meaningful for them to work with in the EDRMS.

RM professionals may want to consider Exon's comment regarding the use of 'activity descriptors' in these classification

## INFORMATION SEEKING BEHAVIOUR PART 3:

Continued from page 53

schemes: 'The use of activity descriptors as the second level in all file titles places in an important position in the file title terms which are often not helpful for retrieval purposes and which add very little to the total effective meaning of the file title as a description of the content of the file', (Exon 1997, 20).

In her article, Exon comments that the way classification schemes are structured with an 'emphasis on functional analysis has been to the detriment of efficient retrieval', (Exon 1997, 19).

We agree with Exon's comment on the need 'to bring back into records management a commitment to precise retrieval at the level of the document', (Exon 1997, 21).

She continues, 'and begin to emphasise post-coordinate retrieval' (Exon 1997, 21), but given that it has been ten years since Exon's article was published, the new design and search technologies available today in EDRMSs makes it irrelevant whether post-coordinate or pre-coordinate indexing is used in the EDRMS. It is now possible to type in terms in the classification scheme, regardless of the citation order, by using Boolean logic search options and retrieve all records with the same classification.

It is not the aim of this research to focus on the effectiveness of the KAAA or the KFC, but the findings reveal that users in the studied organisations have difficulties working with these tools. Hence, we recommend that future research be conducted on how users retrieve records using these tools (see the section on 'Future Research').

Thirdly, develop a separate 'user friendly classification scheme' to be implemented in the EDRMS that is intuitive and aligned to the users' work processes and thinking patterns. Then, RM professionals

can align the 'user friendly classification scheme' to the underlying RM classification schemes, such as the KAAA or the KFC, in order to work out the retention periods for records in the background.

Alternatively, bypass the KAAA and the KFC and just use the RDS to sentence records. If the latter approach is taken, then the 'user friendly classification scheme' has to be aligned to the RDS.

Either way, the less user-friendly version of the RM classification scheme will be hidden from the users' view in the same way the RDS is. In this way, the users will have a classification scheme that they can relate to and work with in order to register and retrieve information successfully in the EDRMS.

Our observations of how users search and retrieve information from the EDRMS also suggest that users would like to browse by navigating down a tree view folder structure if they already know where the record is filed or if they have filed the record themselves.

Hence, when designing the EDRMS it is important to provide users with the option to browse visually to retrieve records via the tree view folder structure as well as to search by using the metadata search in a 'virtual database' design.

### Future Research

Many of the findings of this research indicate that training is a key issue in improving the effectiveness of EDRMSs for users.

We suggest that future research examine training in more detail. Research that identifies users' IISS prior to training and compares post-training search strategies with the preferences expressed as the IISS would help to confirm the role of training in the ISB of EDRMS users. In particular, it would be interesting to understand if training on using classification schemes for searching the EDRMS has any effect and, if not, why.

## The Authors

**Pauline Singh**, ARMA is a PhD Candidate at the University of Western Australia, completing her program in 2008.

For fuller details of her background and experience see the first part of this article, in the November 2007 issue of *IQ*. Pauline may be contacted at paulines@iinet.net.au.

**Jane E Klobas** is a Professorial Fellow at the University of Western Australia and Senior Research Fellow at Dondena Centre for Research on Social Dynamics, Bocconi University, Milan, Italy.

For fuller details of her background and experience see the first part of this article in the November 2007 issue of *IQ*. She may be contacted at jane.klobas@uwa.edu.au

**Karen Anderson**, PhD, was until late last year, a Senior Lecturer in the School of Computer and Information Science at Edith Cowan University, Perth, WA where she developed the Archives and Records program in 1994. From January 2008, Dr Anderson commenced duties at Mid Sweden University, at Harnosand, Sweden, as Professor of Archives and Information Science.

For fuller details of her background and experience, see the first part of this article in the November 2007 issue of *IQ*. She may be contacted at karen.anderson@miun.se.

This article first appeared in *Human IT Journal* and appears in *IQ* with permission.




In general, further research on the value of the classification schemes and thesauri seems warranted, particularly given the predominance of metadata searching among EDRMS users.

Focused research on organisations that have implemented the KAAA and the KFC and the users' experience of working with these RM tools is required to ascertain the value of these tools for classification and retrieval.

Research on whether RM professionals are expecting too much from the classification scheme/thesaurus tool is worth embarking on as well. The KAAA and the KFC tools enable RM professionals to sentence, classify, assign accountability and security, and conduct audits of the RM program. Are these RM tasks preventing these tools from being good mechanisms for information search and retrieval for users?

A number of other user studies could be pursued. For example, why do some users fail to use EDRMSs or use them only in the most cursory way, even when the RM principles, training plans, senior management support, qualified resources, and other factors believed to encourage system use are in place?

Finally, our research did not directly study user satisfaction with EDRMS, but such research – particularly where it compares different EDRMS – could provide interesting insights into the quality of EDRMSs and their acceptance among their users. 



Exon, Maggie (1997). "Contemporary Recordkeeping: The Records Management Thesaurus." *Informaa Quarterly* 13.4: 14-22.

International Organization for Standardization (2002). ISO 15489-1 and 2: Information and Documentation – Records Management. Geneva:

International Organization for Standardization.

International Organization for Standardization (2003). ISO 15836:2003(E) – Information and documentation – The Dublin Core Metadata Element Set. Geneva: International Organization for Standardization.

National Archives of Australia (1999). Recordkeeping Metadata Standard for Commonwealth Agencies. <<http://www.naa.gov.au/recordkeeping/control/rkms/summary.htm>> [2007-05-22]

Robinson, Catherine and Janet Knight (n.d.). Contemporary Recordkeeping - The Records Management Thesaurus - Response. <[http://www.records.nsw.gov.au/recordkeeping/contemporary\\_recordkeeping\\_the\\_records\\_management\\_thesaurus\\_response\\_10470.asp](http://www.records.nsw.gov.au/recordkeeping/contemporary_recordkeeping_the_records_management_thesaurus_response_10470.asp)> [2007-05-20]

State Records New South Wales (2001). NSW Recordkeeping Metadata Standard. <<http://www.records.nsw.gov.au/publicsector/erk/metadata/metadata-std/nrkmsstyle.htm>> [2007-05-20]

State Records New South Wales (n.d.). Keyword for Councils Overview. <[http://www.records.nsw.gov.au/recordkeeping/keyword\\_for\\_councils\\_430.asp](http://www.records.nsw.gov.au/recordkeeping/keyword_for_councils_430.asp)> [2007-05-20]

## Why names you know rely on Codaprint...



**TRIM®  
Interface  
now  
available**

Freecall 1800 263 234 today to order your free demonstration CD and be amazed by the benefits of Codaprint.

## Codaprint - Proven to maximise your records management efficiency...

Save time, money and resources by eliminating the need to apply individual labels to your files with Codaprint, the all-in-one labeling system.

In just four easy steps you can complete your files in minutes – not hours.

Design your own templates or choose from Codaprint's range of template designs.

### Recommended System Requirements:

Minimum Pentium 200MHz PC with 32MB RAM, 20MB Hard Disc Space (10MB for programs and 10MB for database and templates). Windows 95, Windows 98, Windows NT4, Windows 2000, XP and Vista

\*TRIM is a registered trademark of TOWER Software \*TRIM Context Interface is purchased separately from Codafile. Australian & New Zealand designed specially for Australian & New Zealand filing needs.

Freecall Australia 1800 263 234

Email [sales@codafile.com](mailto:sales@codafile.com)

Fax 61 2 9460 7838

[www.codafile.com](http://www.codafile.com)

Dealer enquiries welcome





# Who Are You, And What Can You Do?

Identity in the digital world is no simple thing to verify. Just think of the famous cartoon caption, 'On the Internet nobody knows you're a dog', or far more seriously think of the much discussed case of the loss of two CDs by Her Majesty's Customs and Revenue Department containing the personal details (bank details, addresses and phone numbers) of every UK family receiving child benefits.

The potential cost to the banking sector and UK government of this loss has been estimated at greater than £244 million.

Managing identity is far from simple. We, as individuals, are inundated with requirements to manage ever increasing numbers of authentication mechanisms. Judicious weeding can be applied – for example, I refuse to actively manage and remember the password to my video shop membership, or the code my infrequently used membership to an airline alliance programme has assigned me.

At the very minimum, I can count more than thirty individual combinations of user name and passwords that I rely on regularly. How many combinations of nifty identifying passwords and reminder questions can we come up with (and remember) before we have to write them down, thus immediately compromising the security of the details and systems they were designed to protect?

It is this two sided issue of identity management and access restriction that is the focus of one of the Butler Group's Technology Evaluation and Comparison Reports, Identity and Access Management: Laying the Foundations for a Trusted Business Environment.

For business, the management of identity is now a critical and complex issue. The growth of e-commerce, Web-enabled customer service systems (for the public sector, read e-government or citizen centric services), networked partnerships, remote workers and almost every aspect of business dependent on a software application of some kind makes this a crucial issue for all business.

In the physical world a physical person could be viewed and interrogated for identity purposes. In the virtual world, assertions of identity need to be proven by different methods – often by giving a person a token, a password, or a means of sharing a code that is (theoretically) only known by the possessor of the code.

The awkwardness of authentication protocols for individuals needing to sign on to multiple business systems with different levels of access and permissions for each raises this issue high on the agenda of business problems.

This Butler Report takes us through the business issues and multiple mechanisms available and being explored to overcome

## At a Glance

**Title:** Identity and Access Management: Laying the Foundations for a Trusted Business Environment.

**Authors:** Sue Clarke, Maxine Holt, Andrew Kellett, Alan Rodger

**Published by:** © Copyright the Butler Group, 2006

**Reviewer's view at a glance:** 'Of great interest to recordkeepers... But probably too detailed for our general purpose.'

**Availability:** Butler Direct Limited, [www.bhutlergroup.com](http://www.bhutlergroup.com)

this issue. It details the well known technologies and the more sophisticated – such as federated identity management, within the organisation, and beyond.

Federated identity management is technology supporting the somewhat elusive notion of 'single sign on' whereby a user signs on once, at a central hub and the technology then feeds this single sign on to multiple connected applications, thus relieving the individual of authenticating themselves at every individual system.

Within the organisation, technologies such as Microsoft's Active Directory or products using the Lightweight Directory Access Protocol have been widely adopted. Outside the organisation, a number of attempts at providing similar services, such as Microsoft's controversial Passport technology, have run aground amidst privacy concerns.

Coming down the track are service oriented offerings which can be invoked from a trusted source, and these will no doubt become ubiquitous with time.

The Butler Group's Technology Evaluation and Comparison Reports aim at providing a high-level, strategic overview of a technology followed by a rigorous and detailed analysis and comparison of the leading technology vendors and their supported features, culminating in technology ranking and market position tables.

This Report defines Identity and Access Management functionality as:

- User identification.
- Authentication requirements.
- Access control capabilities.
- The ability to effectively manage passwords and associated credentials.
- The efficient provisioning and de-provisioning of users.
- The availability of strong and efficient administration services.

Providing support for

- Information accessibility needs, whilst addressing associated protection issues. Individual and group-based access and movement requirements.

- Business risk assessments and corporate operating requirements.
- People, Policy, and Protection requirements.

In addition to reviewing business issues and functionality required for the combined notion of Identity and Access Management, the Report outlines challenges, some of which sound familiar.

The report identifies increasing uptake of this type of technology over the preceding 2 years (2004-2006) and predicts strong market growth in the technology.

However, it also identifies this as an emerging market, yet to be consolidated and therefore rife with multiple vendors often advocating proprietary rather than standards based approaches, a volatile market mixture beginning to reach maturity with acquisitions and consolidation of individual applications causing a significant risk to organisations backing the wrong technology.

The Report provides technology audits of 14 products representing some big names such as IBM, Sun, Novell and Oracle and then profiles a further 23 vendors/products.

So, what has this all got to do with records management? Well, a lot actually. In conceptualising recordkeeping, the notion of 'agent' is one of our key information entities. We need to manage information about individuals, roles, positions, workgroups and organisations as a critical part of managing the authenticity of the records created and received over time.

We organise records according to the concept of provenance, which is critically linked to who created/did something and who they were. At present, as is acknowledged by the Butler Group Report, enterprise content management (where recordkeeping sits) has one of the most complex requirements to manage access controls – requiring a granularity or detailed level of access roles more complex than most applications.

The management of access control and identity is, for that reason, often bundled within document and records management applications. But at the same time, this is a duplicated effort, with other parts of the organisation being functionally responsible for 'provisioning' and 'de-provisioning' (the Report's words) of human resources.

In theory, there is no reason for recordkeeping to assume responsibility for this functionality. We can inherit the required data from other, perhaps more suited, organisational systems managing who belongs to what group.

Centralising the administration of permissions and people would be a good thing for recordkeeping - BUT the problem is that the technologies used in other areas of the organisation are not recordkeeping systems.

As we know, protocols like LDAP do not maintain records of who was in what position at what time – they are information systems to support the authentication protocols which do not require over time information, but rather depend on accuracy of up to date information. Recordkeeping requires this information to be maintained over time. We need to know that Joe Bloggs was the cleaner in 1996, not the CEO as he later became.


The interpretation of the record depends on such time bound information, not maintained within the other organisational systems. So, there is a threat to records authenticity, integrity, reliability and usability if organisations, and the broad community of ECM, adopt these enterprise wide identity and access management systems without appreciation of the specific functional requirements for recordkeeping.

And there is absolutely no indication in this Report that the Butler Group has even realised this, and therefore it is obviously not on the radar of the technology vendors.

So, should records managers rush out and buy this technology report? No, I don't think so – but on the other hand, these reports are available for limited free evaluation download from [butlergroup.com](http://butlergroup.com), and it is well worth browsing and dipping.

This specific Report is aimed at senior management and IT managers seeking to identify and weave through a shifting marketplace. For that audience it provides positioning of specific products, a great statement of functionality required and a way of identifying potential winners in a volatile market.

For records managers, it is sufficient to raise some red flags and alert us to issues we should know about this area of technology at a general level, and enable us to position our arguments for problems likely to be encountered if the technology does not address recordkeeping (and there is no indication that it will!).

This Report is an in-depth discussion of an area of great interest to recordkeepers, but it is probably too detailed for our general purpose. However, the red flags should indicate that this is an area to keep a weather eye out for, and prepare our strategies for when this technology comes to our organisation. 

### The Reviewer

**Barbara Reed**, BA (hons), MA (hons), Diploma of Archives Administration, is a Fellow of the Australian Society of Archivists, and won the RMAA's J.Eddis Linton Award for Most Outstanding Individual in 2007.

Barbara is a Director and principal consultant of Recordkeeping Innovation Pty Ltd. She spent 5 years as a senior lecturer at Monash University's School of Information Management and Systems teaching both undergraduate and postgraduate programmes, specialising in recordkeeping and information management, and has written extensively on archives and records issues for a variety of professional journals.

The Head of the Australian Delegation to TC 46 SC11 responsible for the development of the ISO 15489 in records management and a member of IT21, Standards Australia's Committee on Records Management, Barbara is also involved in delivering recordkeeping education and training through The Recordkeeping Institute.



Originating from the cartoon of Peter Steiner, published in The New Yorker, 5 July 1993

Computing.co.uk 'HMRC Blunder Set to Cost at least £500m' 22 November 2007 <http://www.computing.co.uk/vnnet/news/2204125/hmrc-blunder-set-cost-least> (accessed December 2007)

<https://www.butlergroup.com/research/reportHomePages/reportsHomepage.asp>

Butler Group, Identity and Access Management: Laying the Foundations for a Trusted Business Environment, June 2006, p 83  
Ibid p65

# J Eddis Linton Awards: Entries Close August 1

**The achievements of individuals within the profession  
become the achievements of the profession itself.**

**T**he J Eddis Linton Awards for excellence in records and information management (RIM) in Australia and New Zealand, are the RMAA's pinnacle awards, and are presented annually in three categories.

## Outstanding Individual Contribution

This award is aimed at those RMAA members who have achieved excellence in RIM & contributed highly to the profession. It can be self-nominated or nominated by an independent person or group.

If you feel you have - or know an RMAA member who has - contributed significantly in the workplace or to the profession as a whole, you are urged to send in a nomination.

The nominator is required to provide a summary in no more than 1000 words of why they are nominating. The nominator may be required to meet with the Awards judging panel in regard to the nomination and may be asked to provide documentary evidence.

The outstanding contribution should demonstrate one or more of the following:

- An example of RM best practice or innovation that extends the boundaries of common practice.
- Evidence of a commitment to records and information management issues leading to increased motivation, involvement and improved business performance. Key internal personnel will need to verify that initiatives made a significant strategic and practical contribution to the organisation.
- A significant innovation or development in the field that increases the awareness of the profession to those outside the RMAA.
- Display of an outstanding degree of dedication and commitment to the profession.

## Outstanding Group Contribution

Aimed at RMAA members who as a group have achieved RIM excellence and contributed highly to the profession, this award is open to groups, committees (other than RMAA Committees), vendors, business units or consultants (whose work has not been performed for personal gain).

This award can be self-nominated or nominated by another party, with the following criteria.


1. Groups/committees must comprise at least 3 people.
2. The Company to which the group belongs must be a financial member (ie Corporate member) of the RMAA.
3. The nomination form must include the name of a representative who will accept the award if successful.
4. The nominator should provide a summary in no more than 1000 words of the outstanding achievement of the nominee (ie, why they are being nominated).
5. The nominator may be required to discuss the nomination with the Awards judging panel and may be asked to provide documentary evidence.
6. The outstanding contribution should demonstrate one or more of the following:
  - Innovation or best practice within the records management field that extends the boundaries of common practice.
  - Evidence of an increased commitment to RIM issues leading to increased motivation, involvement and improved business performance. Key internal personnel will need to verify that initiatives have made a significant strategic and practical contribution to the organisation.
  - A significant innovation or development in the field that increases the awareness of the profession to those outside the RMAA.
  - A level of achievement that results in an increase of RMAA members or displays an outstanding degree of dedication and commitment to the profession.

- Evidence of an increased commitment to RIM issues leading to increased motivation, involvement and improved business performance. Key internal personnel will need to verify that initiatives have made a significant strategic and practical contribution to the organisation.
- A significant innovation or development in the field that increases the awareness of the profession to those outside the RMAA.
- A level of achievement that results in an increase of RMAA members or displays an outstanding degree of dedication and commitment to the profession.

## Student of the Year

This category is awarded to a student who has achieved excellence in educational studies in records and information management, and is open to both fulltime and part-time students who have completed a dedicated records and information management course in the previous 12 months (July to June).

1. Study may be undertaken at any level, including tertiary and VET.
2. High level achievement is defined as attaining no less than a Credit (or its equivalent) for the entire course.
3. The educational institution/provider must be accredited by the RMAA.
4. A certified copy of academic record must be provided with the application.
5. The nominee must indicate his/her personal vision of the future direction of records management (1000 words).
6. The award is not limited by age.


For more information and an application form, see the RMAA website: <http://www.rmaa.com.au/docs/awards/fed/linton/index.cfm> 

## Jim Shepherd Award Also Closes August 1

The RMAA's Jim Shepherd Award is awarded to vendors in recognition of vendor/trade support of the Records Management Association of Australasia and in recognition of services to the records management industry. Previous winners include Tower Software, Objective Corporation and Recall.

A nominee must demonstrate:

1. A minimum of five (5) years continuous sponsorship of the RMAA at both Branch and National level (sponsorship can be financial or 'in kind').
2. Active involvement in advancing the records management industry.
3. Their product or service must be specific to the records/information management industry.
4. Must be a Corporate Member of the RMAA
5. Applications covering these criteria and demonstrating the company's suitability must be submitted by either an individual RMAA member (who does not work for the company) or by a Branch Council, Chapter or SIG of the RMAA.
6. Self-nominations will be accepted, but must be endorsed by a professional RMAA member who does not work for the company.
7. The nominator is required to provide details of the nominee, incorporating the award criteria, in no less than 1,000 words.

For more Jim Shepherd Award information see the RMAA website: <http://www.rmaa.com.au/docs/awards/fed/shepherd/index.cfm> 



# Win the Prestigious Objective RMAA Award, Earn Valuable Points

Have an article published in *IQ*, and, as an RMAA member, you automatically become eligible for the Objective RMAA Article of the Year Award and earn valuable CPD points.

**T**his year sees the Objective Corporation sponsoring the RMAA Article of the Year for the fourth year in a row.

"As the leading ECM solution provider, Objective is proud to support the leading publication for records management professionals and a quality Association like RMAA," Objective Corporation Chief Executive Officer Tony Walls told *IQ*.

"By supporting the RMAA Article of the Year we aim to encourage members to contribute editorial articles which foster professionalism in the Association and the industry," said Mr Walls.

All articles by RMAA members which appear in either *InfoRMAA Quarterly (IQ)* or the yearly RMAA online publication the *Information & Records Management Annual (iRMA)* between November 2007 and August 2008) automatically become eligible for the award – no entry forms or separate applications are necessary.

"Selecting a winner hinges on the value an article brings to the body of knowledge in the profession and whether it pushes the boundaries, asking new questions," says Tony Walls.

The winning article will be one which makes a contribution to the understanding or discussion of its subject matter and will be pertinent to the records and information



**Tony Walls**, Objective Corporation's CEO

## Objective

RMAA Article of the Year  
AWARD

management industry. Contents can be technical, academic or light, as long as the work is original, written in an involving, readable style, and shows the author's thorough grasp of the subject.

The judging panel is made up of the Editor of *IQ*, an Objective Corporation representative, and a member of the RMAA National Board. Eligible articles can be technical or opinion based, can be case studies or calls for action, can be long or short.

Last year's winning article was a disposal authority case study from New Zealand authors Amanda Cossham and Kerry Siatiras.

In addition, every article appearing in the Association's publications wins RMAA members CPD points, and, now that *IQ* is formally recognised as a peer reviewed journal, authors engaged in tertiary studies can claim maximum points for material published in the journal.

"This award gives Objective Corporation the opportunity to help reward Association members who put many hours of their own time into researching and writing often very complex papers which help records and information professionals discuss, dissect and develop this increasingly challenging industry of ours," Tony Walls remarked.

This year's awardee wins a Canon Ixy 1000 Digital Camera valued at \$699 (RRP), courtesy of Objective. The winner will be announced at the RMAA International Convention in Sydney in September.

To discuss an idea for article submission to *IQ* and so be in the running for the current award, email [editor.iq@rmaa.com.au](mailto:editor.iq@rmaa.com.au).



## WANTED!

### Editorial Submissions on Education & Training

The August issue of *IQ* will contain a feature on records and information industry education and training, and we are looking for editorial submissions on any related aspect.

Whether you are an educator with a story to tell about your institution's RIM training offerings, a trainer within industry, or a RIM practitioner with a story to tell or a view to express about education and training in the industry, contact the Editor of *IQ* today to discuss your submission, by emailing:

[editor.iq@rmaa.com.au](mailto:editor.iq@rmaa.com.au)

# RMAA Snapshot 1:

The People Who Help Make Us Tick.

## Susan Henshaw

**Our new Membership & Events Coordinator**

Recently joining the RMAA team, and working out of Launceston, Tasmania, Susan has an extensive background in events organising.



**S**he has worked in 5-star hotels in Sydney as part of their sales and marketing teams, and spent 5 years at a major publishing company in their learning & development department.

"It's been a particular pleasure to deal with many of RMAA members in the short time I've been in this role – everyone has been a delight. I'm looking forward to meeting you all in person at the RMAA International Convention in Sydney in September.

"My mission is for the Association to be recognised as having the most outstanding customer service."

### TRUE CONFESSIONS

**IQ asked Susan some personal questions:**

**A little known fact about you?**

I'm a kinesiologist....

**Marital status/children?**

I'm single, but a very proud Auntie Suse to my beautiful nieces and nephews.

**What sport have you played?**

Used to play A grade netball. (I think that's why I now have bad knees!) At the moment I'm into Boot Camp – and my knees are holding up pretty well.

**Word that best describes you?**

Can I use an acronym? LIFE – Laugh; Inspire; Fun; Eat!

**The most important lesson you've learned?**

You get what you focus on.

**Your motto for life?**

Dream big dreams, go after what you want, and be of service along the way.

**The award/honor you're most proud of?**

I'm really quite proud of the Award for Excellence for my Cert III in Applied Colour

and Design.

**The book that has influenced you most?**

There have been so many. The most recent one I've read is Eat Pray Love by Elizabeth Gilbert – a refreshingly honest account of her path to discovering just what's important to her – a very amusing, entertaining and meaningful read.

**Your favourite movie/s?**

I love Speed, with Keanu Reeves and Sandra Bullock. Having watched it a zillion times, should the need arise I feel I could take the wheel of a bus with confidence. On the more sedate side, Love Actually, and Holiday.

**Your favourite singing artist/s?**

Elton John is my singer of the moment, having been to his Rocket Man Solo Concert – what an amazing talent he is.

**Your favourite restaurant?**

The Quay Restaurant in Sydney – a stunning spot overlooking the harbour. I was very fortunate to be taken there for dinner by overseas friends – the chocolate pudding was heavenly! I must also mention Daniel Alps at Strathlyn in Tasmania's Tamar Valley wine region – he is a superb chef, and everyone should experience his talent for creating the most amazing food.

**Your favourite holiday spot?**

Since moving back to Launceston after living in Sydney for 15 years, Sydney is the holiday spot of the moment where lots of my friends and some of my family are – I go back as often as I can.

**Your favourite way to spend free time?**

Free time in this role?! Are you kidding?!! No, really, I love spending time with friends, discovering new restaurants, seeing a movie or just lazing with a good book.

**The vehicle you drive?**

Ford Laser sedan

**The vehicle you would like to drive?**

Being a Top Gear fan, this is a tough question – there are so many great cars out there. I've always had a soft spot for the SAAB 93 Cabriolet.

**Your personal measurement of success?**

It's all about enjoying what I'm doing, spending time with people who are important to me, and making the most of the opportunities and experiences that come along.

**The most memorable moment in your working career.**

Being part of the re-opening of Sydney's Luna Park - an historic occasion, and one I'm really grateful to have been involved in. It was quite a sight watching the new 'face' coming down the harbor on a barge with all the Sydney icons in the background.

**Where would like to see the RMAA in 5 years time?**

I'd like to see the RMAA widely recognized across all business industries as the association to belong to for cutting edge, pioneering records and information management.

**How would you like to be remembered by family, friends & colleagues?**

Having lived life to the fullest, made a difference to people I've come in contact with, and made sure everyone knew where to find the best food and wine!

**Your secret dream/ambition?**

To live between France and Italy for 6 months of the year, to learn to fly a plane, to make the perfect chocolate soufflé, to be in two places at once...there's more but I don't think they'll give me more room! ☺

# RMAA Snapshot 2:

The People Who Help Make Us Tick.

## Debbie Prout

**Victoria Branch President & RMAA Board Director**

Debbie Prout has been in the Records Management Industry for 21 years, receiving her initial training while working for the Australian Security Intelligence Organisation (ASIO) before moving into the local government sector.

**S**he has worked for six Victorian councils over the last 18 years and has also done consulting work for the private sector. During this time she has had two terms on the RMAA's Victoria Branch Council and is currently Victorian Branch President and an RMAA Board Director of the Association.

Debbie has been involved in the implementation of three EDRM systems for Local Government, and is currently the Coordinator Corporate Information at the City of Whitehorse, where she is the project leader for the implementation of TRIM.

### TRUE CONFESSIONS

**IQ asked Debbie some personal questions:**

**A little known fact about you?**

I used to do square dancing and ballroom dancing when I was younger.

**Marital status/children?**

Married to my wonderful husband Andrew for nearly 25 years, and have a daughter Katharine aged 14 who still likes to spend time with mum.

**What sport do you play or used to play?**

I used to play netball. Now I try to get to the gym 2-3 times a week.

**How did you get started in the RIM industry?**

I applied for a job that was advertised as an admin officer, not realising that it was for ASIO as a records officer.

**Words that best describes you?**

Outgoing, talkative, very family orientated

**The thing you like best about your job?**

The people I work with. Local government

is an exciting area to work in. We deal with information that covers all spectrums from planning and building to aged care & children's services. You definitely don't get bored. I also enjoy mentoring younger people.

**The thing you least like about your job?**

The constant battle to get users to understand how important good recordkeeping is.

**The most important lesson you've learned?**

Making time for family & friends is more important than being dedicated to work.

**Your motto for life?**

Enjoy every moment.

**The award/honor you're most proud of?**

Winning the Hamer Award in 2006.

**The book that has influenced you most?**

To Kill a Mockingbird. I first read it when I was about twelve. It made me realise that life isn't always fair.

**Your favourite movie/s?**

I don't see many movies, but did enjoy the Lord of the Rings series.

**Your favourite singing artist/s?**

Believe it or not, I loved John Denver. I also love to listen to my daughter - she sings with the Australian Youth choir.

**Your favourite restaurant, or favourite dining experience?**

Breezes at the Casino (Melbourne).

**Your favourite holiday spot?**

Winter at Lake Louise in Canada

**Your favourite way to spend free time?**

Curling up with a good book in front of an open fire with a glass of red wine and a box of chocolates.

**The vehicle you drive?**



I drive a Mazda 6 wagon (work vehicle)

**The vehicle you would like to drive?**

Not fussed as long as it's reliable. Wouldn't mind having a convertible.

**Your business philosophy?**

Always treat the customer with respect, and go the extra mile.

**Your personal measurement of success?**

Satisfied customers who keep coming back.


**Your plans for the RMAA in Victoria?**

To provide good quality workshops and information sessions and to continue to build on the success of our annual State Seminar. I am also keen to build an enthusiastic Victorian Branch Council that is responsive to members needs.

**How would you like to be remembered by family, friends & colleagues?**

Someone who was supportive, friendly and honest.

**Your secret dream or ambition?**

To have four months at home, four months up at our place at Falls Creek skiing, and four months traveling each year. 



The 2008 version of iRMA containing articles and case studies is due for release in October 2008

RMAA are currently negotiating strategic alliances with 11 organisations.

If you are looking for a response from RMAA on a query you will get it quicker via email than telephone, as RMAA currently utilise a third party service provider for their general query telephone numbers.

In addition to Branches running events, RMAA National runs events. Branches use their event profits to subsidise future Branch events. But what does National Office do with their profits? They are used to assist pay for professional development activities undertaken by the RMAA to provide members with additional or improved services and to promote records and information management to the wider community.

Current initiatives in development include:

- 2008 Industry Poster series release (known to you as the Pirate poster)
- New updated Membership Brochure promoting the Association
- RIM @ Work brochure series
- Disaster Recovery Wheel
- Updating the RMAA website to make it more user friendly and to improve functionality such as offering podcasts and ordering and paying online.

More than 44 hours per month are spent by RMAA staff answering email queries where answers are readily available on the RMAA website. The RMAA website is a wealth of information.

RMAA is represented on many different advisory committees, including IT21 (Standards Setting, both local and international), State Records Councils, Education Committees, Archives Councils, SNIA just to name a few.

Some statistics from the RMAA National staff. Collectively the 3.5 current 'full time' RMAA staff:

- Receive more than 2,000 emails a day
- Are managing an average of 15 events at any time
- Work more than 900 hours per month

## Coming Up

### In The August 2008 issue of *IQ*...

• Education & Training • RMAA Sydney International Convention Preview

The final deadline for accepted copy for August's *IQ* is July 1. Peer review submissions should be forwarded at least 6 weeks prior to each issue's copy deadline. Send all submissions to [editor.iq@rmaa.com.au](mailto:editor.iq@rmaa.com.au)



Rated 'the major journal for the dissemination of practical aspects of information management:' Pamber & Cowan Australasian Survey, 2007





# Are you compliant?

## De-stress with a secure, efficient document management solution

Recall are document management specialists with the experience, resources and know-how to take the worry out of your critical compliance and document management processes. Our nation-wide network, leading edge technology, dedicated customer managers and tailor-made products give you all the control, flexibility and assured quality you demand. Efficiency and security you can rely on to add value for your clients. Too easy!

**Comply today: call 13RECALL 13 732 255**  
**or visit [www.recall.com.au](http://www.recall.com.au)**  
**or email: [moreinfo@recall.com](mailto:moreinfo@recall.com)**

***recall***<sup>TM</sup>  
Your Information. Securely Managed.

DOCUMENT MANAGEMENT SOLUTIONS | DATA PROTECTION SERVICES | SECURE DESTRUCTION SERVICES

## MANAGING AND PROTECTING THE WORLD'S INFORMATION



### IRON MOUNTAIN SERVICES

- RECORDS MANAGEMENT
- SECURE SHREDDING
- DIGITAL ARCHIVING
- DATA PROTECTION
- VITAL BUSINESS RECORDS
- CONSULTING

With more than 50 years of experience, Iron Mountain continues to be the leading provider of records management and data protection services for companies around the world. Use our global network to archive, back up, and access your hard copy and electronic records in a secure, cost-effective environment.

Iron Mountain offers the most complete suite of services for managing all of your business records. We have the knowledge, expertise, global resources, and technology to help you achieve your business goals.

# 1800 IRON MTN

Iron Mountain operates in major markets worldwide, serving thousands of customers throughout the U.S., Europe, Canada, Latin America and Asia Pacific. For more information, visit our website at [www.ironmtn.com.au](http://www.ironmtn.com.au)

 **IRON MOUNTAIN™**

Level 1, 785 Toorak Road  
Hawthorn East VIC 3123

**1800 476 668**

|           |              |
|-----------|--------------|
| Sydney    | Auckland     |
| Melbourne | Wellington   |
| Brisbane  | Christchurch |
| Perth     | Hamilton     |
| Canberra  | Adelaide     |
| Darwin    | Hobart       |

