INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

MAY/JUNE 2013

Managing and Collecting Social Media for E-Discovery

Page 22

5 Steps for Managing an Offsite Storage Vendor Consolidation

Page 27

Exploring the Principles for Increasing Integrity, Objectivity in External Audits

Page 32

rsd THE OFFICIAL SPONSOR OF INFORMATION GOVERNANCE

twitter

IGaaS

RIM Manager (Records Manager)
Help! @RSDig We have 2 much information to manage

RSDig (RSD InfoGov)
Are u SURE u aren't over-retaining information?

LegalMgr (General Counsel)
I hope not, I have to reduce business #risk and #eDiscovery costs

RSDig (RSD InfoGov)
Have u considered implementing #IG (information governance)?

RIM Manager (Records Manager)
What is #IG?

RSDig (RSD InfoGov)
#IG enforces desirable behavior in the creation, use, archiving, and deletion of ALL corporate information

IT Manager (VP of IT Infrastructure)
Hey, but I have way too many #ECM and #RIM systems to manage. And what about content in the #Cloud and on #SharedDrives?

RSDig (RSD InfoGov)
Use **RSD GLASS** 2 ensure policy is enforced across information silos and regulatory jurisdictions

RIM Manager (Records Manager)
Finally!! +1 RT @RSDig: Use **RSD GLASS** 2 ensure policy is enforced **across** information silos and regulatory jurisdictions

RSDig (RSD InfoGov)
This is why we are the official sponsor of **information governance** :-)

Trending topics:

#InformationGovernance
#IGaaS™
#CentralizedPolicy
#PolicyEnforcement
#eDiscoveryReadiness
#RepositoryAgnostic
#MultipleJurisdiction
#LifecycleManagement
#RecordsManagementIsNotEnough

THE OFFICIAL SPONSOR
IG
of Information Governance

For more information, please visit **www.rsd.com** or scan the QR code.

INFORMATION MANAGEMENT

MAY/JUNE 2013 **VOLUME 47 NUMBER 3**

DEPARTMENTS

4 **IN FOCUS** A Message from the Editor

6 **UP FRONT** News, Trends & Analysis

FEATURES

22 **Managing and Collecting Social Media for E-Discovery**
Lauren A. Allen, J.D., PMP; and Michael C. Wylie, J.D.

27 **5 Steps for Managing an Offsite Storage Vendor Consolidation**
Julie Fleming, CRM

32 **Exploring the Principles for Increasing Integrity, Objectivity in External Audits**
Robert J. Dosch, Ph.D., CPA; James P. Haskins, Ph.D.; and Timothy P. O'Keefe, Ph.D.

SPOTLIGHTS

38 **GENERALLY ACCEPTED RECORDKEEPING PRINCIPLES® SERIES**
The Principles at Work in a Canadian Regional Government
Julie Gable, CRM, CDIA, FAI

42 **RIM FUNDAMENTALS SERIES**
Digital Dusting: Spring Cleaning for Network Drives
Blake E. Richardson, CRM, CIP

CREDITS

47 **AUTHOR INFO**

48 **ADVERTISING INDEX**

INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

Publisher Marilyn Bier

Editor in Chief Vicki Wiler

Contributing Editor Cyndy Launchbaugh

Art Director Brett Dietrich

Advertising Sales Manager Elizabeth Zlitni

Information Management (ISSN 1535-2897) is published bimonthly by ARMA International. Executive, editorial, and advertising offices are located at 11880 College Blvd., Suite 450, Overland Park, KS 66210.

An annual subscription is included as a benefit of membership in ARMA International. Nonmember individual and institutional subscriptions are $140/year (plus $25 shipping to destinations outside the United States and Canada).

ARMA International (*www.arma.org*) is a not-for-profit professional association and the authority on managing records and information. Formed in 1955, ARMA International is the oldest and largest association for the records and information management profession, with a current international membership of more than 10,000. It provides education, publications, and information on the efficient maintenance, retrieval, and preservation of vital information created in public and private organizations in all sectors of the economy.

Information Management welcomes submissions of editorial material. We reserve the right to edit submissions for grammar, length, and clarity. For submission procedures, please see the "Author Guidelines" at *http://content.arma.org/IMM*.

Editorial Inquiries: Contact Vicki Wiler at 913.217.6014 or by e-mail at *editor@armaintl.org*.

Advertising Inquiries: Contact Karen Lind Russell or Krista Markley at 888.277.5838 (US/Canada), +1 913.217.6022 (International), +1 913.341.3742, or e-mail *Karen.Krista@armaintl.org*.

Periodical postage paid at Shawnee Mission, KS 66202 and additional mailing office.

Canada Post Corp. Agreement No. 40035771

Postmaster: Send address changes to *Information Management*, 11880 College Blvd., Suite 450, Overland Park, KS 66210.

“How do I **expand** our U.S. domestic retention rules to our **international offices**?”

Zasio can help you.

ZASIO

RECORDS & DOCUMENT MANAGEMENT EXPERTS

Zasio's Records Management Consulting and Versatile Retention International™ Software is your complete global retention schedule management, legal research, and international consulting solution. It combines the powerful Versatile Retention International software with Zasio consultants' expertise and experience in international research. Whether you are doing business in one country or all over the world, Zasio can help.

Call the experts at Zasio to discuss your Records Information Management questions and challenges today.

800 513 1000, Opt. 1
www.zasio.com

Conquering the Chaos of "Too Much Information"

Although each of the articles in this issue is on a different topic, the common theme among them is the challenges that come from having too much information. This problem is only going to get worse, according to the International Data Corporation (IDC), a global IT market intelligence provider.

In "The Digital Universe in 2020," IDC predicted that between now and 2020, the total amount of data created, replicated, and consumed globally is expected to double every two years and reach 40 trillion gigabytes!

Because of its ubiquity, social media use is a major contributor to information growth, and it presents unique challenges, particularly with e-discovery. In their cover article, attorneys Lauren Allen and Michael Wylie share four keys to managing social media for e-discovery. Readers will get a better understanding of the types of information generated by social media applications, where and how to access it, and how to monitor and collect it for discovery.

Too much inadequately managed information also complicates information audits. As a trio of authors from the University of North Dakota writes in "Exploring the Principles for Increasing Integrity, Objectivity in External Audits," implementing an information governance program based on the Generally Accepted Recordkeeping Principles® (Principles) will tame information chaos, ensuring the integrity and objectivity of the organization's information, which is vital to the quality of audit outcomes.

The Principles are already hard at work in the Regional Municipality of Niagara (Ontario, Canada), according to its information management coordinator, Clare Cameron, CIP. "They provide a structure, a framework for ensuring that ideals can be met," she told Julie Gable, who authored this Principles Series article. Cameron explains how each of the Principles influences her work. The Principle of Protection, for example, is the impetus for her trying to work more closely with IT to ensure that security and protection are addressed when new systems are created.

A good relationship with IT will also help RIM professionals working to clean up network drives, which are common dumping grounds for extraneous information and where information chaos often reigns. Blake Richardson, CRM, CIP, tells how a thorough "digital dusting" of these drives begins with implementing folder structures and file naming conventions that will ensure files can be located easily by anyone who should have access. It continues with a manual or computer-assisted review that identifies files that can be deleted and those that need to be renamed. Just like other housework, digital dusting never ends. Regular monitoring, dusting, and an annual deep cleaning are necessary to maintain a network drive, Richardson writes.

Like digital information, paper also continues to proliferate and challenge organizations. In "5 Steps for Managing an Offsite Storage Vendor Consolidation," author Julie Fleming, CRM, describes how to consolidate physical records under one vendor to get better control of information, enabling compliance and improving operations.

The problem of having too much information can be solved, and RIM professionals can play a pivotal role if they are willing to accept the challenge. E-mail *editor@armaintl.org* to tell us how we can help. **END**

Vicki Wiler
Editor in Chief

"All I did was suggest we NAID the old records."

See what happened at www.naid-em.com.

NAID®

GOVERNMENT RECORDS

Feds' Budgets Out-Paced by Volume of Information to Manage

U.S. federal agencies – and their budgets – are being overwhelmed by the amount of information they must manage, according to a recent study of federal records managers and finance professionals from MeriTalk and Iron Mountain.

Published in March, the results of the online survey of 100 federal records managers and 100 federal finance professionals conducted in September 2012, "Federal Records Management: Navigating the Storm," showed that each federal agency spends an average of $34.4 million a year on records management, $5 million – or about 17% – more than budgeted.

According to the survey report, records management spending will likely more than double to $84.1 million by 2015 because of a projected 144% increase in records per agency.

Some of the main reasons for the overspending are:

- Too many records – a single federal agency currently manages about 209 million records, which totals 8.4 billion records government-wide.
- Runaway information growth – the number of records per agency is expected to grow to 511 million by 2015.
- Multiple information types – records are increasingly being created in more varied formats and sources.

Add to this the race to comply with the Presidential Directive on Managing Government Records, which instructs agencies to modernize their records management policies, predominantly by digitizing records and establishing a new infrastructure to minimize costs and promote openness and accountability.

The survey respondents said additional training, more funding, and greater support for records management from their agencies' leadership would enable them to meet the objectives of the directive. The federal finance professionals estimated that focusing on these three factors would allow them to save an estimated 24% of their records management budgets; the records management professionals estimated savings of up to 36%.

CYBERSECURITY

Reuters Social Media Editor Charged with Hacking

Federal charges were filed in March against Matthew Keys, a deputy social media editor for Reuters, for allegedly conspiring to hack the *Los Angeles Times* website in 2010.

Keys is accused of giving the website's password to the notorious hacker group "Anonymous" through its chat room, encouraging the group to breach the newspaper's website. One of the hackers followed up and altered an archived article. The *Los Angeles Times* is owned by the Tribune Co., which also owns a Sacramento television station at which Keys used to work as a web producer.

The U.S. Justice Department charged Keys with one count each of transmitting information to damage a protected computer, attempted transmission, and conspiracy. If convicted, Keys could face up to 10 years in prison on two of the counts, five years on a third, and a fine of $250,000 for each count.

As of press time, Keys had not yet been arraigned.

BIG DATA

With Big Data Comes Big Privacy Concerns

The potential of big data is huge. It opens the door to smarter decision making and greater advances in every field – provided it is effectively managed and mined, of course.

That potential in turn raises serious concerns around protecting privacy.

Last year, the World Economic Forum conducted a series of workshops attended by government officials, privacy advocates, and business executives from the United States, Europe, Asia, and the Middle East. The discussions centered on three major areas:

- Protection and security
- Accountability
- Rights and responsibilities for using personal data

Out of those workshops came the recently published report "Unlocking the Value of Personal Data: From Collection to Usage." The report, which was prepared in collaboration with The Boston Consulting Group, recommends an approach that shifts focus away from governing the usage of data to governing the data itself; recognizes the importance of context because there is no black and white, only shades of gray; offers new ways to engage individuals and help them understand how their information is to be used; and provides them with the tools to make real choices based on "clear value exchange."

For such an approach to be successful, the participants agreed there is a need 1) for principles to be updated and enforceable in a hyperconnected world; 2) to include technology as part of the solution – allowing permissions to flow with the data and ensuring accountability at scale; and 3) to demonstrate how a usage, contextual model can work in specific, real-world application.

EIM

Enterprise Info Management Critical, But Not Priority

Although business executives are generally well aware that information is an asset and that poorly managed information can be a potential legal and competitive liability, making enterprise information management (EIM) a reality is another story.

According to the OpenText white paper "Unleashing the Power of Information," a recent IDG Research survey of nearly 140 chief information officers (CIOs) and other IT and business executives showed that the majority believe in the benefits EIM can deliver, such as better data access and analysis, reduced costs, and better alignment of IT with business objectives. Yet only 67% of the organizations represented said they treat EIM as a strategic priority.

Part of the challenge is the overwhelming volume of unstructured data organizations are generating. According to the white paper, it is estimated that up to 80% of the information produced in organizations today is found in documents, e-mails, social media, slide presentations, videos, and other unstructured data formats. This information is often mission-critical and resides in a number of different locations and devices.

"Given the variability and complexity of today's information landscape," IDG wrote, "many companies find themselves dealing with distinct and nonintegrated information silos. Information in these silos is often disorganized, dated or duplicated, and data that could identify key trends or deliver critical insight is often buried under mountains of insignificant information."

That's why 80% of the survey respondents said a comprehensive EIM strategy is critical or, at least, very important to their organizations. Unfortunately, this recognition of the value of that information has not translated into policy. Organizations are not making EIM an institutional priority – even though it directly affects their ability to meet their top business objective: increasing business productivity, according to the IDG report.

BIG DATA

Report Examines Trends in Big Data

It's been talked about and written about at great length, but to what extent are companies actually addressing big data today?

A Tata Consultancy Services (TCS) survey of 1,217 companies in nine countries in the United States, Europe, Asia-Pacific, and Latin America that was completed in January 2013 found that more than half (53%) had undertaken big data initiatives in 2012. The countries with the highest percentage of companies with initiatives were India, Mexico, the United States, and the United Kingdom. Japan, The Netherlands, and Australia had the fewest percentage reporting initiatives in place.

The level of investment in big data initiatives varied greatly, the report found: 15% of the companies with initiatives spent at least $100 million per company on those initiatives last year; 7% invested at least $500 million. On the other hand, nearly one-quarter (24%) spent less than $2.5 million apiece. The industries that spent the most on the initiatives were telecommunications, travel-related, high tech, and banking. Life sciences, retail, and energy/resources companies spent the least.

More than half (55%) of the investments in big data initiatives went toward four business functions that generate and maintain revenue: sales (15%), marketing (15%), customer service (13%), and research and development/product development (11%). Only about a quarter (24%) of the investment went to IT (11%), finance (8%), and human resources (5%).

Forty-three percent of the companies that have invested in initiatives anticipated a return on investment (ROI) of more than 25% in 2015. The business functions expecting the greatest ROI were not sales and marketing, as might be expected, given that they received 30% of the funding, but rather logistics and finance, which received only 14% of the funding.

Companies reported that the biggest obstacles to getting business value from big data were as much cultural as they were technological. More specifically, it was the challenge of getting business units to share information across organizational silos. A close second was a technological issue: dealing with the volume, velocity, and variety of data. The third was determining which data to use for different business decisions.

"By applying Big Data in the right places in the organization, centralizing and nurturing talent, and building bridges to functional managers who need data-driven insights to make superior decisions, companies will greatly raise the odds of keeping up in a world in which digital data-driven decisions become the norm, not the exception," the TCS report concluded.

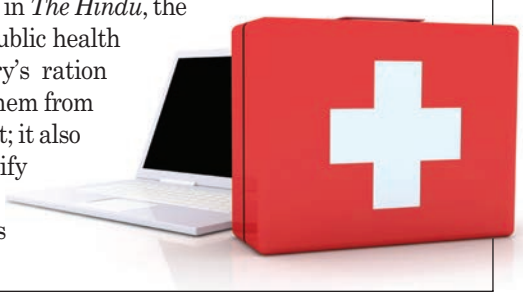
EHR

India Launches Electronic Health Records Program

The Jawaharla Institute of Postgraduate Medical Education and Research (JIPMER) rolled out the "Partners in Prevention Programme" for the police department in Puducherry (India) in mid-March as the first step in the country's move toward electronic health records.

Medical records of the policemen who are screened at JIPMER will be maintained online in a database accessible from anywhere in the world. The patients are issued a "Meddrecords Online Card" with a unique identification number and barcode, which will enable them to update daily blood pressure, blood sugar level, family history, and other details that their doctors could access as needed.

According to an article in *The Hindu*, the plan is to integrate the public health records with the country's ration card, which would help them from a public health standpoint; it also would help them identify those who had completed their immunization cycles and various screenings.




TOTAL RECALL™
PHYSICAL RECORDS
MANAGEMENT SOFTWARE
Manage and Protect Your Information
• Manage Onsite and Offsite Records
• Retention and Hold Management
• Organization-Wide Charge-Backs
• SCAN ON DEMAND™
and High-Speed Digital Imaging
• RIM Consulting Services
DHS WORLDWIDE℠
SOFTWARE SOLUTIONS
Call 1-800-377-8406 • www.dhsworldwide.com

PRIVACY

U.S. Electronic Communications Privacy Act Amendments Proposed

When the U.S. Electronic Communications Privacy Act was introduced in 1986, no one could have foreseen how the Internet and mobile communications technology would transform the world. To bring the law up to date, senators Tom Leahy (D-Vt.) and Mike Lee (R-Utah) introduced a bill in mid-March that they believe will strengthen the privacy protections for e-mail and other electronic communications.

Leahy explained that the bill strives "to improve Americans' digital privacy rights, while also promoting new technologies – like cloud computing – and accommodating the legitimate needs of law enforcement."

The bill requires law enforcement to obtain a search warrant based on probable cause to access e-mail and other electronic communications' content requested from a third-party provider. There are "balanced exceptions" to this requirement in emergency circumstances and to protect national security under current law.

The bill would further require law enforcement to "promptly notify" any individual whose e-mail content has been accessed. The government can ask the court for a temporary delay in notifying the individual, however.

The bill would not affect the government's ability to use administrative, civil discovery, and grand jury subpoena to access corporate e-mail and other electronic communications directly from a company.

EHR

DoD, VA Pullback on EHRs Draws Fire

Early this year the U.S. departments of Defense (DoD) and the Veterans Affairs (VA) announced they were scaling back their plans to create a single shared electronic health records (EHRs) system that would manage service members' and veterans' medical records from recruitment to grave. They decided, instead, to build their system on existing IT architecture and programs, pointing out that it would be more cost- and time-efficient.

The decision drew fire from the top lawmakers on the Senate and House Veterans' Affairs committees, which had charged the agencies in 2008 with creating and deploying an integrated health records system by 2017 at a cost of about $4 billion.

Unfortunately, the project has reportedly met technology challenges and delays. The new approach will enable the departments to exchange real-time data by the end of the year and allow patients online access to their medical records by summer. It is also expected to save hundreds of millions of dollars, according to DoD Deputy Chief Management Officer Elizabeth McGrath, according to an article in *Federal Times*. The endeavor has already cost an estimated $1 billion.

House Veterans' Affairs Committee Chairman Rep. Jeff Miller (R-Fla.) was less optimistic. "Previous attempts by DoD and VA to use disparate computer systems to produce universal electronic health records have failed and unfortunately it appears they are repeating past mistakes," the *Federal Times* reported.

The new system is being built with the VA's VistA EHR as its core system and a more current core EHR system. VistA system has generally been considered a strong EHR platform, but there is concern over its age and its ability to keep pace with newer systems.

CLOUD

The Best Countries for Cloud Computing

Japan, Australia, the United States, Germany, and Singapore are the top five countries for cloud computing based on their policy environment, according to the BSA|The Software Alliance (BSA) 2013 Global Cloud Computing Scorecard.

The study rated 24 countries (which together account for 80% of the global information and communications technology market) based on their policies in seven areas:

- Privacy
- Security
- Cybercrime
- Intellectual property rights
- Data portability across borders
- Free trade promotion
- IT infrastructure

Singapore showed the most improvement (up five places from last year) due largely to its introduction of a modern, balanced privacy regime. A late-comer to privacy regulation, Singapore passed its Personal Data Protection Act in October 2012.

"That timing has helped the country develop a regulatory framework that picks and chooses from the best parts of the European Union and Asia-Pacific Economic Cooperation approaches to privacy regulation and avoids much of the excessive legalese and administrative complexity found in other country's laws," observed BSA in its report.

Singapore took a broad, principles-based approach to privacy protection. It contains short sections on notice, consent, security, access, correction, and data retention, all of which are based on international standards.

Brazil improved its ranking by finally passing cybercrime legislation last November. That change alone moved it up two spaces and out of last place. That distinction now belongs to Vietnam.

Malaysia moved out of the group of countries still striving toward cloud-readiness by making a range of changes in cybercrime and intellectual property laws and improvements in efforts to improve digital trade.

The United States moved up one spot, not through major policy improvements, but through advances in standards development for cloud computing and infrastructure improvements.

Less positively, there continued to be efforts to keep data within national borders. Germany was cited in last year's report for some overly restrictive legal interpretations that would keep some data within its borders.

This year, Indonesia undermined any advantages it may have made from improving its privacy law by introducing regulations that would force some providers to establish local data centers and hire local staff.

In general, Indonesia, Korea, and Vietnam are taking steps to actually unplug from the global cloud. This works against the goal of making data more accessible globally.

CLOUD

Thailand Takes First Step Toward G-Cloud Computing

Thailand's Information and Communication Technology (ICT) Ministry and Electronic Government Agency (EGA) and Cloud Security Alliance (CSA) recently signed a memorandum of intent (MOI) to establish the official CSA office in Thailand. *The Nation* reported that EGA will handle the human resources budget issues to support CSA's activities.

"This effort aims to promote security system[s] for cloud computing among users. CSA will support all activities and provide know-hows," said Nattapong Seetavorarat, advisor to the ICT minister. The cloud computing system, especially G-Cloud, will build upon the GIN system currently in place. The system "can be scalable to Super GIN for more network expansion to other areas, availability of government data with accessibility for related agencies and bodies."

The MOI was signed during the ASEAN CSA Summit 2013. Topics discussed during the two-day event included cloud security, challenges to cloud adoption, public cloud, cloud for education, cloud businesses, and applications of cloud for national crisis management.

DATA SECURITY

Retailer Sues Visa over Data Breach

The Payment Card Industry's Data Security Standards (PCI DSS) are being put to the test in a suit filed in early March by specialty sports apparel retailer Genesco against Visa. Genesco is seeking nearly $13.3 million in fines that Visa assessed following a breach of Genesco's systems that may have resulted in fraudulent transactions.

According to *Wired* magazine, this is the first known case challenging the PCI DSS. The regulations require merchants that handle credit and debit card data to follow certain security practices or face fines from the credit card industry. Visa fined Genesco $13.3 million for noncompliance to the PCI standards after Genesco announced it had been hacked back in 2010.

In the filing, Genesco states that although it found packet-sniffing software on its network at that time, there was no forensic evidence of any card data having been stolen. Genesco alleges it was never out of compliance with PCI DSS regulations and, therefore, should not have been fined.

The PCI standards state that merchants are not to store card data, but may store some parts of the data, if necessary, as long as it's encrypted.

"Visa is not the only card company to go after Genesco and its banks. MasterCard did as well," reported *Wired* senior reporter Kim Zetter. "The two companies combined imposed $15.6 million in fines and assessments, but Genesco has so far only sued Visa."

Genesco is not the first company to be fined, but it is the first to fight back against the credit card companies. In Utah, a restaurant reportedly has sued its bank for wrongfully seizing money from its merchant bank account to pay credit card fines. Visa and MasterCard levied the fines after alleging the restaurant had failed to secure its network, leading to a data breach that resulted in fraudulent charges on customers' credit cards. That case is ongoing.

EHR

Electronic Health Records: How Transparent Should They Be?

How much access should patients have to their electronic health records? According to an Accenture study completed in December 2012, most (49%) physicians favor transparency, but only 21% allow online access.

"Many physicians believe that patients should take an active role in managing their own health information, because it fosters personal responsibility and ownership and enables both the patient and doctor to track progress outside scheduled appointments," said Mark Knickrehm, global managing director of Accenture Health. "Several U.S. health systems have proven that the benefits outweigh the risks in allowing patients open access to their health records."

The Accenture study surveyed 3,700 physicians in the United States, England, Spain, France, Germany, and Singapore. U.S. doctors were marginally more open to allowing patients to update their records online. There was a clear consensus among the respondents that, generally, patients should be allowed to update all or some of their information, from demographic details to lab test results. More than half of the responding physicians favored providing update privileges.

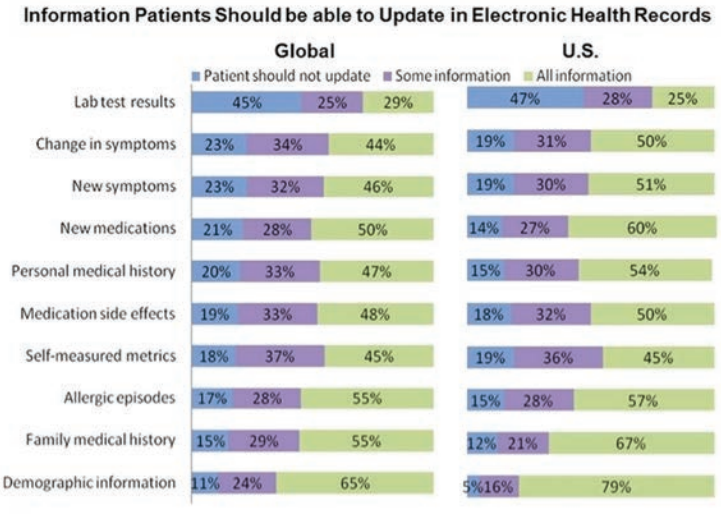


Figure 2: U.S. doctors were the most open toward patients updating the information in their electronic health records, according to Accenture's eight country survey of 3,700 doctors

Source: Accenture Doctors Survey

CYBERSECURITY

European Commission Launches Cybersecurity Strategy

The European Commission (EC) and the High Representative of the European Union for Foreign Affairs and Security Policy recently introduced a cybersecurity strategy for the European Union (EU). Part of the strategy included a directive on network and information security, a draft of which was released in conjunction with the strategy.

The strategy aims to clarify the principles the EC believes should guide the cybersecurity policy in the EU and internationally. Those principles are:

- The EU's core values apply in the digital world the same as in the physical.
- Protection of fundamental rights, freedom of expression, personal data, and privacy
- Access for all
- Democratic and efficient multistakeholder governance
- A shared responsibility to ensure security

It is predominantly the task of member states to deal with cybersecurity challenges; however, the EC strategy established five strategic priorities with both short- and long-term activities for the government, industry, and member states. Those priorities are:

1. Achieving cyber resilience
2. Reducing cybercime drastically
3. Developing cyberdefense policy and capabilities related to the Common Security and Defense Policy
4. Developing the industrial and technological resources for cybersecurity
5. Establishing a coherent international cyberspace policy for the EU and promoting the core EU values

On a related note, proposed changes to the European Data Protection Directive introduced about the same time the EC launched the cybersecurity strategy have come under heavy fire. *Wired.co.uk* reported that UK Information Commissioners past and present denounced the changes as being bad for business, and they said they should be thrown out.

Among other things, the EU directive is being described as "too prescriptive in terms of its administrative detail."

E-DISCOVERY

ISO Starts Committee on E-Discovery

The International Organization for Standardization (ISO) recently established a committee to develop standards for e-discovery processes. Its goal is to define procedures for technology companies, discovery providers, and their clients to follow when handling electronically stored information.

"We're not trying to impose requirements on lawyers or judges. That's not the intention of the activity," Hitachi Data Systems' Eric Hibbard, co-editor of the project and international representative on a U.S. contingent to ISO, told *Law.com*. "It's really intended to help them sort through some of the technology issues that are really nebulous."

The standards will refer to product auditing and will describe how discovery services and software should operate. They will also cite ISO 9001 quality control procedures, which means e-discovery companies could then achieve ISO 9001 certification and promote their products as being ISO 9001-compliant.

Other organizations, such as the American Bankers Association, are also working on legal technology standards. Reactions to plans to develop standards in this area have been mixed. While many fully support it, others think it premature.

"A lot of us think that standard-setting for an area in which the technology has not yet matured is a little bit premature," Steven Teppler, an attorney and data security expert, told *Law.com*.

DATA SECURITY

Keep Your Data from Walking Out the Door

The consensus in the industry is that regardless of how you feel about the bring your own device (BYOD) trend, you can't afford to ignore it.

A 2012 Nielsen study found that almost half (49.7%) of U.S. mobile subscribers own smartphones. According to Nielsen, this is an increase of 38% over 2011. It's a safe bet to expect a large percentage will want to connect to their company's wireless network. They'll forward documents to their personal accounts to read at home or while traveling.

With this increased access come increased security risks. Potentially sensitive corporate data is being sent to less-secure sites.

In a recent *BizTech* article, IBE.net co-founder Richard Minney suggested an alternate BYOD strategy in which the company actively allows BYOD, specifies what data can and cannot be transferred to and stored on those devices, and installs an app or two to provide some level of protection.

He added that the company may also want to insist that all devices used for work purposes be registered with the company's mobile device management (MDM) solution, which applies policy and security management capabilities across many operating systems or platforms. These applications are typically modeled after the client server architecture where software is centralized on a back-end server and a client component resides on the end system device.

Another option is for the company to allow employees to choose the devices they want, but the company supplies and owns them.

CLOUD

Cloud Adoption in India Grows

A recent report by ARC Advisory Group shows that the cloud market growth rate in India is outpacing the global market by a wide margin. Almost all the IT vendors in India have cloud offerings, as do many global players.

The report cites the country's growing IT industry, currently valued at $100 billion. The industry's rapid growth is due largely to the demand from global companies. But even micro, small, and medium businesses are turning to the cloud to reduce the cost of ownership.

CYBERSECURITY

Report Finds Data Breaches Mainly Involve Outsourced IT

A recent report published by Trustwave revealed that 64% of security breaches it analyzed last year involved IT outsourcing providers. The findings drive home the need for enterprises to be more aware of the security measures outsourcing providers have in place before contracting with them.

"We are not saying outsourcing is bad," explained John Yeo, director of Trustwave's SpiderLabs unit in Europe, the Middle East, and Africa, "but what we are saying is that there may have been a lack of due diligence in the selecting of outsourcing providers."

The UK's Data Protection Act requires data controllers to take "appropriate technical and organizational measures" to avoid "unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

Some feel more clarity is needed from regulators as to what sort of security standards can be considered as compliant with the Data Protection Act. Also, too many senior business executives lack sufficient knowledge or understanding of cybersecurity risks.

Other trends revealed in the Trustwave report include:

- Businesses are getting slower at containing cyber breach incidents, taking an average 210 days in 2012 compared to 175 days in 2011.
- Businesses tend to rely on third parties to tell them they've been hacked: 24% detected the breach themselves, while 48% were discovered by regulatory bodies and 25% by law enforcement.
- There were 400% more samples of mobile malware affecting the Android operating system last year than in 2011. Yeo said the company had not found a case where a smartphone was being used to hack a corporate network, although it could happen and may already have happened.

ELECTRONIC RECORDS

CIOs' Top Priorities for 2013

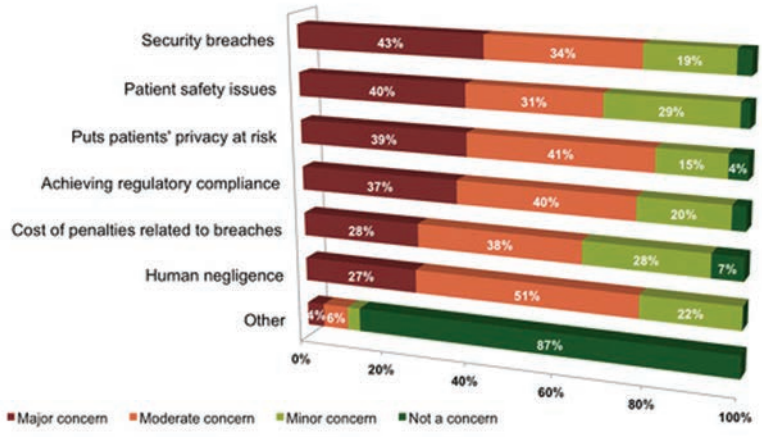
Ask 100 healthcare CIOs and senior IT executives what their top priorities are in 2013 and you'll hear network security issues, IT infrastructure upgrades, and electronic health records (EHRs) implementation. Those were the findings of an independent research study by Level 3 Communications.

Those surveyed were less inclined to focus on mobile-enabled healthcare (mHealth) and slow to adopt cloud computing.

Other findings include:

- 56% were only "somewhat confident" in their ability to prevent a privacy or security breach on their network.
- 80% agree the EHR-based systems will improve patient care.
- More than 60% think EHR and "meaningful use" mandates are a "good idea" to support better quality patient care.
- 76% plan to upgrade their network infrastructure in the next two years.

EXHIBIT 3:
Possible Security and Compliance Concerns EHRs



Source: Level 3 Communications

HIPAA

HIPAA Final Rule Tightens Data Security Requirements

On March 26, the final rule to the Health Insurance Portability and Accountability Act (HIPAA) went into effect, ending the more than three-year effort to overhaul the provisions of the 1996 law. Most of the changes were required by the 2009 HI TECH Act, which incentivized the implementation and use of electronic health records and prompted the development of standards, implementation specifications, and certification criteria for the exchange and use of electronic health information.

The new rule expanded the definition of "business associates," requiring more entities to take a more proactive role in complying with HIPAA. Previously, the law required healthcare providers and other "covered entities" to contractually require that any organization that handles protected heath information (PHI) on behalf of the covered entity (business associate) also to comply with HIPAA.

Under the new rule, the business associate must take full responsibility for ensuring it complies with HIPAA's data security and privacy rules. This means that business associates will also be subject to annual civil penalties for each HIPAA violation, which could be as much as $1.5 million per violation.

Breach notification requirements were also addressed in the new rule. The proposed rule defined a data security breach as the "acquisition, access, use, or disclosure of [PHI] in a manner not permitted [by the Privacy Rule] which compromises the security or privacy of the [PHI]." It went on to say the standard should be whether there was a "significant risk of financial, reputational, or other harm to the individual."

The final rule, however, requires that the entity trying to avoid breach notification obligations conduct a risk assessment that considers the following:

1. The nature and extent of the PHI involved and how easily it is or could become identifiable
2. The unauthorized person who accessed the PHI
3. Whether the PHI was actually acquired or viewed
4. Whether and to what extent the risk to the PHI has been mitigated

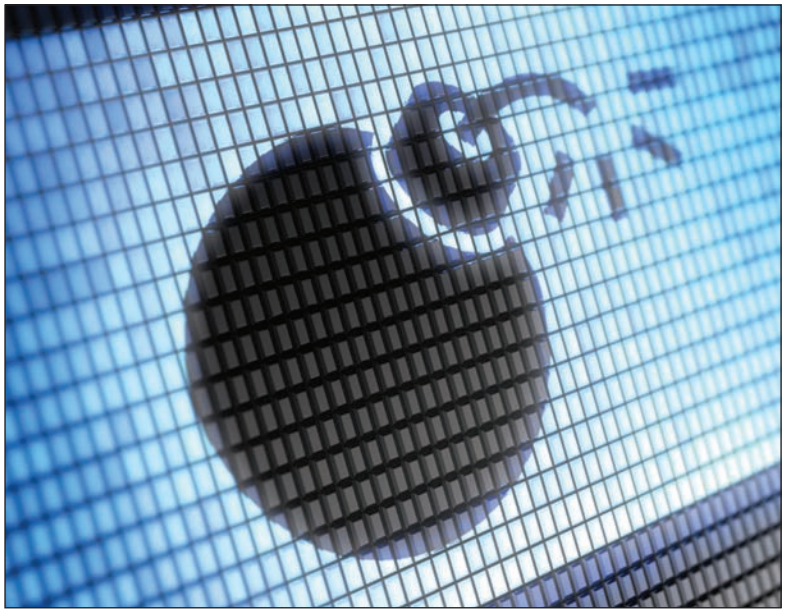
If it can be shown that there was a low probability that the protected information was compromised, it would not be considered a breach. If that can't be proved, the breach notification requirements must be met.

The other area addressed by the final rule limits the sale of PHI for marketing purposes. Bottom line is that protected information may not be sold or used without the individual's consent. Additionally, the covered entity or business associate must disclose the nature and extent of its relationship with the third party.

The compliance deadline for the final rule is September 23. Contracts entered into before January 25, 2013, that complied with the previous HIPAA Data Security and Privacy Rules will be considered compliant until September 22, 2014, as long as the contracts have not been renewed or modified during the grandfathering period.

CYBERSECURITY

Preventing 9/11 in the Cyber World



The evidence that cyber threats are very real and growing is ubiquitous. Earlier this year, U.S. Department of Homeland Security (DHS) Secretary Janet Napolitano warned Congress that a "cyber 9/11" could be imminent and strongly urged lawmakers to pass legislation governing cybersecurity, which it failed to do last year.

President Obama made it clear that cybersecurity is an issue to be taken seriously by signing an executive order that directs the National Institute of Standards and Technology to develop cybersecurity performance standards and methods to reduce risks to the country's critical infrastructure (CI). Among other things, it also directs DHS and agencies to proactively encourage CI owners and operators to voluntarily adopt the standards.

Given the increased volume and strategic nature of cyberattacks, many are convinced they are state-sponsored, and many are pointing fingers at China as the origin of the most sophisticated hackers. It's becoming a potentially lethal weapon of modern warfare.

For example, Team Cymru, a Florida-based Internet security firm, recently revealed to *The Verge* that its analysts have uncovered a massive overseas hacking operation in which one terabyte of data is being stolen on a daily basis.

A study released by the American computer security firm Mandiant detailed that company's efforts to track down a group of "cyber commandos" responsible for hacking the networks of hundreds of American companies over several years to steal trade secrets. Mandiant traced members of the group back to a Shanghai-based military unit. The claim is supported by reports from other security firms and all 16 of the U.S. intelligence agencies, according to the *New York Times*.

The group in question, dubbed "Comment Crew" by some of its U.S. victims, has allegedly stolen terabytes of data from companies such as Coca-Cola and reportedly is focusing increasingly on companies involved in the U.S.'s CI, its electrical power grid, gas lines, and waterworks.

China's government has repeatedly denied that it has engaged in computer hacking, stating that it has been the victim of such attacks, as well. Chinese officials claimed that they experienced, on average, 144,000 cyberattacks per month against its military sites in 2012. They blame the United States for almost two-thirds (63%) of them, saying that there are many hacking groups inside the United States as well.

The war of words between the two countries escalated when the White House warned China to end its campaign of cyberespionage against the United States or risk derailing efforts to build stronger ties between the two countries. China responded by agreeing to enter into dialogue with the United States about cybersecurity.

In the meantime, tension continues to build around the issue. In late March, attention shifted to Korea when South Korean banks and top television broadcasters were simultaneously paralyzed by a cyberattack. Speculation at the time was that North Korea was involved in the attack. The network paralysis took place a few days after North Korea accused South Korea and the United States of a cyberattack that shut down the country's websites for two days.

"This needs to be a wake-up call. This can happen anywhere," James Barnett, former chief of public safety and homeland security for the U.S. Federal Communications Commission, told Fox News following the attack on South Korean networks.

Studying for the CRM?

ARMA International's CRM Study Packs

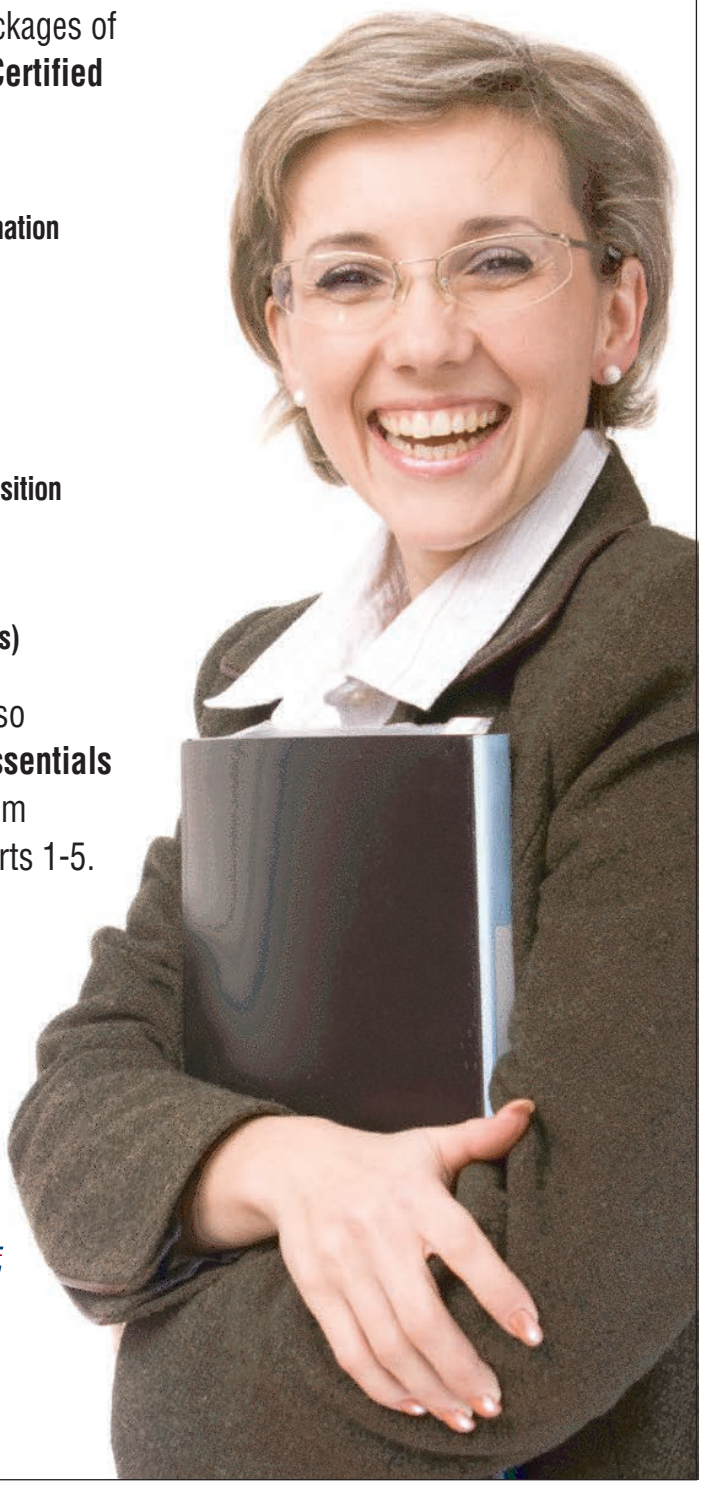
ARMA International has created specially priced packages of recommended resources to help you study for the **Certified Records Manager** (CRM) exam.

Available Study Packs:

- **Part 1: Management Principles and the Records and Information Management Program**
- **Part 2: Records and Information: Creation and Use**
- **Part 3: Records Systems, Storage, and Retrieval**
- **Part 4: Records Appraisal, Retention, Protection, and Disposition**
- **Part 5: Technology**
- **CRM Mega-Pack (combined version of all CRM Study Packs)**

CRM candidates (or potential candidates) should also consider enrolling in ARMA International's online **Essentials of RIM Certificate Program**; completing this program will help establish a great foundation for passing parts 1-5.

Get details at ***www.arma.org/learningcenter.***



Available online in the ARMA Bookstore!

ARMA INTERNATIONAL BOOKSTORE

www.arma.org

E-DISCOVERY

Information Governance Key to Containing E-Discovery Costs

As the volume of information generated by enterprises today continues to grow exponentially, so do the potential costs of e-discovery.

"One of the best ways to avoid excess costs of discovery is a reasonable dialogue with the other side," Magistrate Judge Andrew Peck, of the Southern District of New York, recently told a LegalTech New York audience.

Senior Judge Michael Baylson, of the U.S. District Court for the Eastern District of Pennsylvania, agreed, pointing out that "'I don't want to cooperate' may be a legitimate strategy, but it's going to cost them money in the long run."

Peck added that IT is usually the best source of reliable information when it comes to estimating what it will require to generate the necessary information.

Document review is the largest expense associated with e-discovery, at 73% of the total, according to a 2012 study by RAND Corp. Thus, finding ways to reduce the volume of documents that must be reviewed is vital.

Many are looking to *predictive coding*, which is a type of computer-categorized review application that classifies documents based on how well they match the concepts and terms in sample documents, as a solution for reducing information volume. RAND reported that studies have found that the reduced man-hours required to search fewer documents can cut document review costs by as much as 80%.

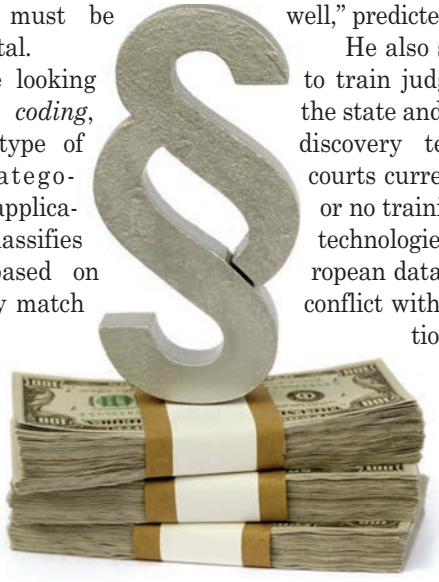
Peck encouraged federal judges to learn from the *Global Aerospace Inc. v. Landow Aviation L.P.* case, in which predictive coding was ordered despite plaintiff's objections. "That was a very, very successful use" of predictive coding, Peck said.

Perhaps more importantly, though, Peck foresees a much-needed shift toward information governance. "If 2012 was the year of predictive coding or technology-assisted review, 2013 or '14 seems to be information governance," he said.

"Despite the economy, companies are going to realize that it's important to get their information retention, their information governance, under control; get rid of the data that has no business need and mine the data that has business need…in ways that will improve the company's bottom line on the business side and reduce costs on the e-discovery side as a benefit as well," predicted Peck.

He also stressed the need to train judges, especially at the state and local levels, on e-discovery technologies. The courts currently receive little or no training on e-discovery technologies and on how European data privacy laws can conflict with discovery obligations here.

"I would advise lawyers to assume that they need to educate the judge," he said. **END**



The Only 3 Letters That Matter

If you're ready to take your career in records management to the next level, there are only 3 letters that matter. Becoming a **Certfied Records Manager** shows that you're ready for today's complex and changing information environment.

Stand Out The CRM designation shows a solid mastery of records management

Confidence You'll prove your ability to apply records and information management knowledge

Career Opportunities It's the well-known competitive advantage you need in business today

For more information, call **877.244.3128**
or visit **www.ICRM.org**

ICRM®
Institute of Certified Records Managers

MANAGING AND COLLECTING SOCIAL MEDIA FOR

Understanding the fundamentals of social networking services, the tools for managing, collecting, and authenticating information they contain, and the way to scope collection efforts can help organizations avoid evidentiary and authentication pitfalls.

Lauren A. Allen, J.D., PMP; and Michael C. Wylie, J.D.

Social networking services (SNS) are now an entrenched form of business and personal communication that requires the attention of records and information management (RIM) professionals and attorneys.

As described by U.S. Magistrate Judge Kristin Mix (District of Colorado) in "Discovery of Social Media" in *The Federal Courts Law Review,* Vol. 5, Issue 2, *social media* includes [internal citations omitted] "'web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.'"

This description includes the current array of *SNS types*: blogs, micro-blogs, wikis, web, video sites, and other new and evolving methods, as well as the most commonly used SNS: Twitter, Facebook, Google+, LinkedIn, Pinterest, YouTube, and Foursquare.

Ubiquity of Social Media

Organizations, both public and private, are embracing SNS.

In the private sector, a benchmark report from social media management company Spredfast, *Q2 2012 Social Engagement Index,* indicates that companies average 29 internal users of 51 accounts across an average of three SNS.

In an example from the public sector, as listed on the U.S. Navy's *Social Media Directory*, some 672 organizations within the Navy alone have one or more SNS presence.

Numbers for SNS use by individuals are no less staggering. For example, in the October 4, 2012, online *Newsroom,* Facebook founder and CEO Mark Zuckerberg headlined a posting with "One Billion People on Facebook."

Similarly, according to Nielsen's *State of the Media: The Social Media Report 2012*, the total number of minutes spent on SNS by users on mobile and PC devices increased 21% between July 2011 and July 2012.

Legal Implications of Social Media

With the rise in personal and professional use of SNS, RIM professionals and attorneys are increasingly required to address social media in both compliance and litigation. But, because social media evolved quickly – and to a large extent is still evolving – and because it is hosted in the amorphous cloud, these professionals are often unaware which properties of social media information are valuable as evidence.

As a result, organizations, attorneys, courts, and regulators are all grappling with the legal and practical implications of retaining, collecting, managing, and presenting social media information in a litigation context.

U.S. Courts, Agency Provide Guidance

According to a blog and lists published on the website of X1 Discovery, an e-discovery and enterprise search solutions provider, more than 900 court cases in the past two years addressed evidence from SNS. Cumulatively, these cases leave little doubt that the standard discovery framework – and resulting records management requirements – apply to social media in the same way they apply to myriad other electronic evidence.

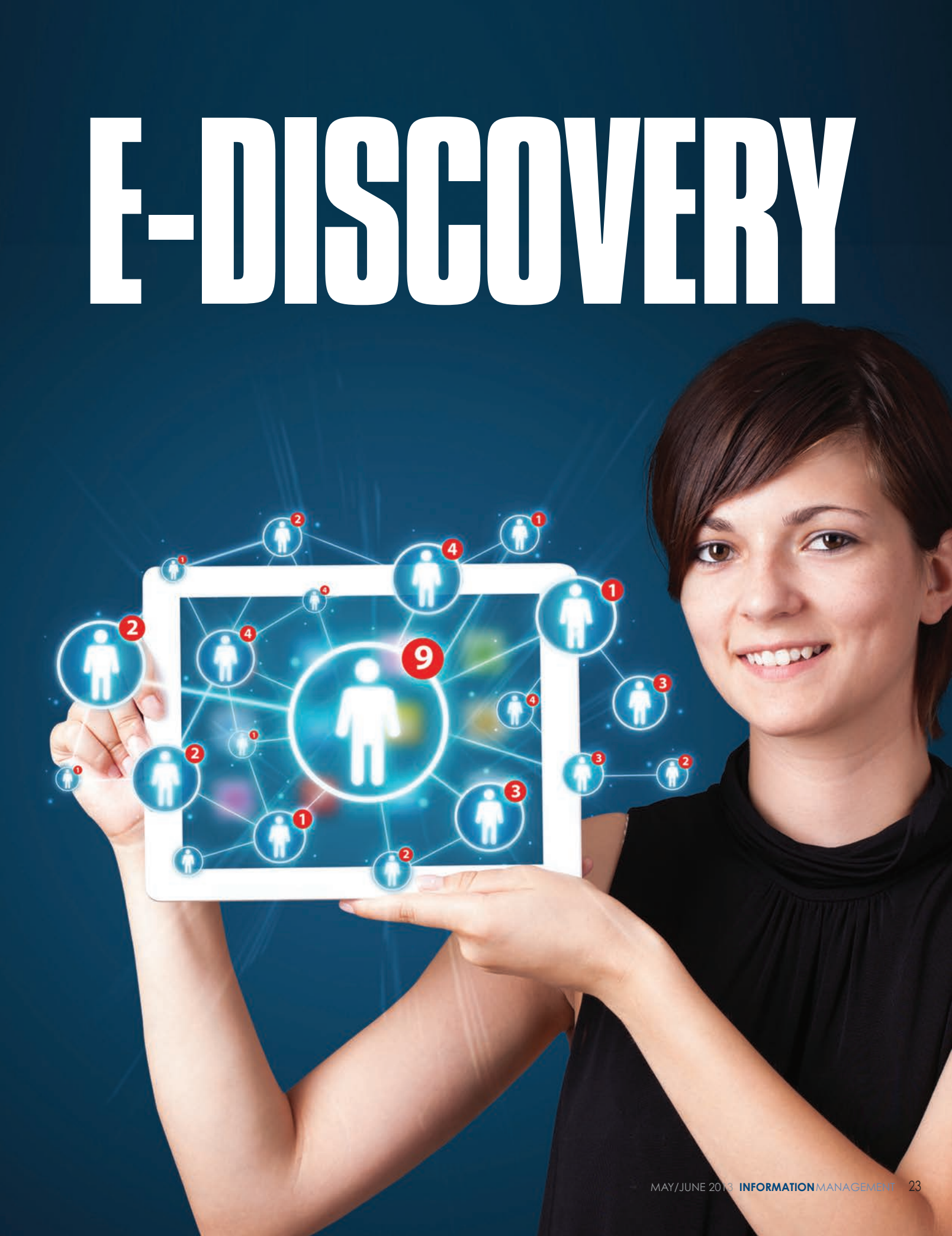
Similarly, *The Sedona Conference® Primer on Social Media,* published in December 2012, notes that the U.S. Financial Industry Regulatory Authority, Securities and Exchange Commission, Federal Trade Commission, and Food and Drug Administration have all issued guidance on social media use in their respective regulated industries.

Keys for Managing Social Media

Social media, like cloud-based e-mail and network infrastructure solutions, presents unique challenges in terms of monitoring, collecting, and managing the information as it resides on third-party network infrastructure and outside an end user's or organization's control.

To effectively manage social media information and ensure that organizations remain in compliance with their obligations during dis-

E-DISCOVERY



covery, attorneys and RIM professionals need to:

1. Understand the types of information available from social media sources and determine what information is possibly relevant for monitoring and collecting
2. Identify where to get the relevant information when it is necessary
3. Determine how secure the relevant social media is
4. Select an appropriate collection or monitoring tool based on the return on investment – i.e., balance the value of retrieving or maintaining the information with the cost of collecting or maintaining it in a particular manner

1. Understand Types of SNS Information

The most basic requirements of RIM professionals and attorneys are to understand the information available via social media and how such information can be relevant.

The potentially discoverable data types on SNS are the same as on other web pages. Social media's evidentiary value stems from the facts that the data originates with users, and it is arranged based on interactions between users.

User activity on general purpose SNS, such as Facebook and Google+, falls within four categories: profile pages, posts, tags, and private messages. While many of the services use varying nomenclature for features, they have substantially similar functionality.

In her article "Understanding and Authenticating Evidence from Social Networking Sites" in the Winter 2012 issue of *Washington Journal of Law, Technology & Arts*, Heather Griffith provides a short but straightforward description of social media interaction on Facebook and MySpace. More detailed descriptions can be found in Mix's article and in detailed help information written by individual SNS providers.

2. Identify Where to Collect Social Media

In a civil context, the level of information any monitoring or collection tool can reach is constrained by the type or level of access an attorney or records manager has to a target account. Therefore, the second requirement in collecting social media is determining the pathway that allows the collection of the greatest amount of information.

Because social media is hosted on geographically diverse servers and often uses cloud technology, there are effectively four potential sources for social media: the social media provider, the account holder, third-party access, and indirect access.

Most SNS providers claim they are prohibited under U.S. federal law, specifically the Stored Communications Act, from disclosing user content in response to a civil subpoena. (See sidebar "The U.S. Legal Framework for Social Media in Court.") While providers are not prohibited from providing basic user information in civil litigation, the SNS providers' claim means that options for lawyers and RIM professionals to access social media content are limited to access as an account holder, third-party access, or indirect access.

Account Holder Access: *Access as an account holder* requires that a user, adverse party, or agent accesses a social media site via the user's profile username and password or other means of identity verification. With respect to discovery of a non-business account, there are only two ways to get direct access through the account holder in a civil

The U.S. Legal Framework for Social Media in Court

Social media information is useful evidence in many types of legal claims, including employment law claims, Federal Trade Commission violations, intellectual property infringement matters, breach of contract cases, and insurance fraud. Use of social media did not change the applicable U.S. Federal Rules of Evidence (FRE) or the U.S. Federal Rules of Civil Procedure (FRCP).

Discovery

According to FRCP 26(b)(1), parties may obtain discovery over any "non-privileged," "relevant" information, and discovery requests must only be "reasonably calculated to lead to the discovery of admissible evidence." Relevance and privilege are defined by the FRE.

Admissibility

In federal court, admissibility of social media evidence usually hinges on the outcome of FRE Rule 403, balancing the probative value of evidence against the danger of unfair prejudice, usually the right to privacy. Note that many state courts, including those in Pennsylvania and New York, have expressly stated that there is no expectation of privacy on SNS.

Authentication

The most litigated aspect of social media is authentication. FRE Rule 901(a) governs authentication of social media evidence. The ease with which social media information can be manipulated, the manner in which social media information is created, and the way in which it is stored raise novel issues concerning its veracity.

Stored Communication Act

As interpreted by several SNS, the Stored Communications Act has been deemed to prohibit SNS providers from releasing anything more than basic user information pursuant to civil subpoena. However, the act does not prohibit users from providing the information themselves, and users can still be subpoenaed and compelled to release social media information in a civil suit.

case – through an agreement with an opposing party or by court order.

Barring evidence of spoliation, a court is unlikely to order a user to hand over access information to an entire profile or account. However, by limiting the scope of the information requested and by using appropriate software or methods, attorneys may be able to convince the court or opposing counsel that the request is relevant and reasonable.

An employment relationship may create additional methods of account holder access to an account. For instance, an account may be a business account to which the employer has access through a second employee or to which an employer has direct access under terms of an employment contract.

In some states, an employer may also require social media access information as a prerequisite to employment. However, according to the National Conference of State Legislatures online posting "Employer Access to Social Media Usernames and Passwords," six states (California, Delaware, Illinois, Maryland, Michigan, and New Jersey) have banned this practice. Note also that, as illustrated in the case of *PhoneDog v. Kravitz*, 2011 U.S. Dist. LEXIS 129229 (N.D. Cal. Nov. 8, 2011), the line between employer-owned and employee-owned accounts can be extremely fine.

Third-Party, Indirect Access: Third-party access and indirect access are less preferred methods of access because, regardless of the collection or monitoring tool used, a target user may restrict information from view through the use of security or privacy settings. *Third-party access* is using a third-party account to view and collect data from a target user's profile. Note that this method raises a number of ethical concerns not addressed here.

Indirect access consists of access via a web search.

3. Determine Security of Social Media

Security issues related to SNS encompass a number of factors that courts have discussed in deciding the authentication issue. Foremost among these are the availability of user-level security or privacy settings and user's application of such settings.

Other issues discussed by courts include account password protection, multiple users' access of a single account, past hacking events, and the security of the computer and network used to access the information.

Obviously, these factors vary by SNS and in many cases will also vary by user, but generally, the more secure the information, the easier to authenticate.

4. Select Collection or Monitoring Tool

Once the extent of availability of social media data is understood, RIM professionals and attorneys must assess the benefits and limitations of approaches to collecting it. Perhaps the most pressing issue in making such a decision is weighing the return on investment in terms of evidence quality and ease of authentication of using more expensive means.

When it comes to monitoring and collecting social media, organizations have multiple tools at their disposal. These solutions range from simple to complex, and costs tend to rise proportionally with the level of information the tool can deliver. Options for monitoring and collecting fall into the categories of screen capture, archiving solutions, and forensic software.

Screen Capture. The lowest-tech solution for addressing social media is simple screen capture. As it sounds, this method captures text and images on a SNS and saves them in a static hard copy or electronic image format. This is an extremely low-cost method of saving information, which maintains the visual relationships between data but not hyperlinks or relational references between pages.

As indicated by *The Sedona Conference® Social Media Primer*, simply printing out social media site data could result in an incomplete and inaccurate data capture that is hard to authenticate, except on the basis of the personal knowledge of a witness.

Archiving Solutions. Archiving solutions are software designed to target primarily text and image data from an SNS profile. Several social media network providers offer archive functionality, which preserves some user data.

Due to terms of use restrictions, these often provide minimal data, such as a user's posts to his or her own profile, shared photos, private messages, and other information. It does not include metadata or any comments users make on other users' posts or profiles.

To paraphrase Wikipedia, *metadata* can be briefly defined as data about data, data about containers of data, and data about data content. In the social media context, metadata often includes author, recipient, date, time, and location information.

Forensic Software. Currently available forensic software can be used either as a tracking tool to actively monitor a user's activities on the site or as a forensic tool to gather a snapshot of current and past usage. In either case, forensic software is currently the only way to collect metadata on a social media site.

Forensic software can include both static collection tools – useful for collecting a snapshot of all of the material related to a social network profile at a given point of time – and dynamic tracking tools – used to actively monitor a target user account.

Excluding law enforcement situations, these solutions are usually dependent on having an agreement with or court order involving the target account user. Note that compliance archiving tools are a sub-

Read More About It

Facebook, 2013. Facebook for Business. Available at *www.facebook.com/business*.

Payne, Andrew C. Twitigation: Old Rules in a New World, 49 WASHBURN L.J. 841, 845-46 (Spring 2010). Available at *www.washburnlaw.edu/wlj/49-3/articles/payne-andrew.pdf*.

Twitter, 2013. Types of Tweets and Where they Appear, Copyright Twitter 2013. Available at *http://support.twitter.com/groups/31-twitter-basics/topics/109-tweets-messages/articles/119138-types-of-tweets-and-where-they-appear*.

set of forensic software and are used extensively inside and outside regulated industries. Compliance archiving tends to be more costly than other methods typically used in litigation.

Avoiding Evidentiary, Authentication Issues

With smart approaches, attorneys and RIM professionals can tackle the challenges that monitoring and collecting social media present. "The best strategy for handling difficult preservation and collection issues is to confer with opposing counsel and agree on reasonable steps," according to *The Sedona Conference® Primer on Social Media*.

Narrow the Scope

During litigation, the elements of a claim, public web searches, available sources of information, and the types of information available on SNS should all be used to narrow the scope of information requested in discovering social media to avoid requests being found irrelevant or overbroad.

Authenticate Information

While social media information is not self-authenticating, under Federal Rule of Evidence (FRE) 901, the SNS matrix, comprising all the information making up a profile (e.g., HTML text, images, metadata, hash tags, posted information, online relationships), provide fodder for authenticating evidence in conjunction with deposition testimony, forensic investigation of software or hardware, or subpoena to a SNS provider to confirm user identity.

In other instances, enough matrix information can also allow for authentication by distinctive characteristics. In fact, the court in *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007) applied FRE Rule 901(b)(4) by ruling that metadata-level hash values were sufficient circumstantial evidence to authenticate.

For this reason, once the scope of a collection has been set, attorneys and RIM professionals should collect broadly. Acting within the confines of any litigation agreements, the more data collected, the easier it will be to find circumstantial evidence allowing authentication of social media evidence.

Similarly, preserving metadata and maintaining a clear chain of custody can be critical to authenticating social media and other electronic evidence. If metadata – especially dates, times, GPS stamps, and computers from which posts were made – are potentially relevant, use of a forensic software tool is necessary, as forensic software is currently the only method of preserving metadata from social media sites.

Monitor Compliance

In compliance monitoring, use careful scoping and technology to effectively manage social media information on an enterprise level and avoid creating over-monitoring.

Selling management on more software tools and increased staffing is never easy. However, RIM professionals can point to numerous court cases where social media has come into play as one reason to proactively tackle the issue of monitoring and collecting it.

Prepare, Don't Pry

With changes in the way that organizations are using social media, RIM professionals should expect SNS content to be relevant in litigation or a regulatory event. Failure to consider the legal and technical considerations of social media may leave organizations scrambling to comply with e-discovery demands or facing court sanctions.

On the other hand, RIM professionals need to be careful that monitoring social media is undertaken only with respect to organizational accounts. Employer monitoring of employee social media is restricted in several states, may run afoul of anti-discrimination laws and the National Labor Relations Act, and, as noted in *The Sedona Conference® Primer on Social Media*, it may open employers up to liability for actions of their employees. **END**

Lauren A. Allen, J.D., can be contacted at laurenallen@deloitte.com. *Michael C. Wylie, J.D., can be contacted at* miwylie@deloitte.com. *Their bios can be found on page 47.*

5 Steps for Managing an Offsite Storage Vendor Consolidation

For organizations using multiple offsite records storage vendors, consolidating records under one vendor can create economies of scale and improve operations – if they are properly prepared to make the move.

Julie Fleming, CRM

Although the world has reportedly "gone digital," organizations continue to struggle with managing large volumes of paper records. Using separate offsite storage solutions by geographically dispersed locations is quite common. Often, though, these locations have few controls to enable compliance with records management requirements.

Following the steps below for consolidating records from multiple locations under one vendor can enhance records management processes, providing a good solution for this challenge.

Editor's note: Because selecting a new vendor is too complex to cover in this space, this article points readers looking for guidance on that step to *Guideline for Evaluating Offsite Records Storage Facilities*, available at *www.arma.org/bookstore*.

Step 1: Gather Information

The first step in organizing a vendor consolidation project – before selecting a new vendor – is to create a database or spreadsheet to track the locations, volumes, and types of the organization's records, as well as the account numbers and contact information for each storage location. This information will be critical to developing a request for proposal (RFP) for vendor selection.

Identifying Storage Locations

Frequently, the accounting department can generate a list of vendors to whom storage fees are being paid to provide a starting point for a database.

However, it is possible that records are also being stored in internal onsite storage rooms, employee homes, and self-storage facilities. Payments to these locations may not have been coded as "records storage" in the accounting system, so identifying them

Date Prepared	Contact Name	Contact Address	Contact Phone	Contact E-mail
Account Number	Record Owner	Current Storage Location		

Box Number	Box Code Label #	Record Series Code/Name (from retention schedule)	Record Series Description	
Records Date From- To	Records Date (Aplha) From- To	Trigger Date	Destruction Review Date	Litigation Hold Codes

Figure 1: Sample Box Inventory

will likely require additional investigation.

Determining Transition Requirements

Each business unit will have unique requirements for transitioning its records to a new vendor, so begin by surveying each one to gather the following basic information:

- Name of business unit
- Address
- Authorized users and contact information
- Names of users requiring destruction authority
- A list of services needed (e.g., storage, shredding, on-demand imaging)
- Whether box-level or individual file listings are needed
- Whether online box submission will be required or if paper transmittals will be allowed
- Who will perform the data entry (internal personnel or the vendor)

Requesting Record Inventories

Provide a template for business units to use so data submitted from all locations can be merged into a uniform list. Determine the metadata to be captured, and use these fields to create the template. The template might include data fields as shown in Figure 1.

Some business units may not have an inventory and/or may not be tracking all required information. In self-storage type situations, only an estimate of the number of boxes may be available. For these locations, an inventory will be needed prior to sending the boxes to the new vendor.

Alternatively, the new vendor may be able to perform an inventory (for an additional charge) when it picks up the boxes.

Conducting Box Reviews

If a box review needs to occur, the following questions will need to be answered prior to scheduling the review:

- Who will conduct the review?
- Which boxes will need to be reviewed (all or just a sampling)? This will depend upon the types of records the location has and what metadata is available. Assumptions may be made if the volume of boxes is great. For example, if a business unit location submits only one type of record, it may be possible to assign dates based upon receipt dates. While destruction dates may not be entirely accurate using this method, depending upon the risk associated with the particular record type and the manpower available to conduct the review, this course of action may be feasible. Work with the legal department to develop a defensible process for destruction of large volumes of records for which adequate metadata is unavailable.
- How many boxes need to be reviewed and how long will the review take?
- Where will the review take place? Vendors will likely charge a fee to use their review rooms, so evaluate whether the cost to deliver the boxes to a company location for review is less than the cost to use the vendor's review room. Consider unpredictability of scheduling for employees who are conducting the review so any delays do not have an impact on the cost of the review.
- Determine what will be done with boxes that are eligible for destruction. Depending upon the vendor's fee schedule, returning the boxes to storage for destruction may be less expensive than destroying boxes onsite and paying permanent removal fees. In some cases, transitioning boxes to the new vendor and having destruction performed there may be less expensive than destroying boxes before the move.

Step 2: Issue Request for Proposal and Select New Vendor

Selecting a new vendor is a lengthy process, requiring much more explanation than can be provided here. *Guideline for Evaluating Offsite Records Storage Facilities* helps users assess the ability of vendors to meet their storage requirements.

This publication (available at *www.arma.org/bookstore*) includes checklists for records security and protection, service levels, contract terms, and cost comparisons, as well as free online access to a form-enabled, editable Microsoft Word version of the checklists that can be customized and distributed as a request for proposal.

Step 3: Set up New Account

When setting up the account with the new vendor, determine how to differentiate between each business unit's records. Sub-accounts can be established for each business unit location and further sub-divided, dependent upon the organization's structure.

Differentiation could be made by such characteristics as country, region, state, address, department, and accounting codes – or potentially all of the above, depending upon the organization's size and complexity and the vendor's system capabilities.

Once the account organizational structure has been developed, the vendor will need a complete, accurate list of all the business unit locations requiring a storage and/or shredding account and where each account should go within the predetermined structure.

After the vendor has set up and populated the account, ask for a spreadsheet that outlines each account/sub-account, the authorized users for each business unit location, and account mapping information for any accounts that were in existence prior to the conversion. This spreadsheet can be used to track changes to account users and sort out account mix-ups that may arise later.

Designating Required Metadata

Be cautious when designating metadata fields as "required." All inventory from existing locations will need to conform to required fields, or the system may preclude box information from being saved.

Consider generating "dummy" information (e.g., a record series code such as UNK001) for boxes that have unknown contents to get around this requirement until boxes can be reviewed.

Uploading the Retention Schedule

Loading the retention schedule into the vendor's system can assist with destruction processes if adequate metadata exists for records. Although, determining what format the vendor requires for the retention schedule upload would have been part of the RFP process, double-check to ensure this has not changed.

There will likely be character limitations requiring abbreviations of record series titles. Retention periods may also need to be converted into periods that a computer system can understand.

Although some organizations may choose to upload the entire retention schedule to the vendor's system, not all record series need to be included. For example, record types that exist only in electronic form or those with retention periods of less than one year should never end up in a storage box, so these record types can be excluded.

Whenever the retention schedule is modified, changes in the vendor system will also be required. Check with the vendor to determine its process for updating the retention schedule. Be sure to include this step in retention amendment processes so the retention schedule doesn't become out-of-date, resulting in the potential for non-compliance.

Records located at dedicated records storage vendors may require contract terminations and extraction timelines, which will require scheduling and management.

Step 4: Transition to New Vendor

Varying strategies may be needed to transition records. For example, records located at dedicated records storage vendors may require contract terminations and extraction timelines, which will require scheduling and management.

Records located at self-storage facilities may need to be inventoried. Accounts that already exist with the new vendor will require mapping to the new account and applying metadata fields.

Discuss all scenarios with the vendor and develop a timeline and processes for managing each type of situation.

Reviewing Contracts with Current Vendors

If this was not done during the RFP process, obtain copies of contracts for current storage vendors. Determine authorized users for each account, as typically, only authorized users have authority to terminate the contract.

Review early termination provisions for each contract and determine whether to extract the company from the contract prior to the termination date, or wait until the contract ends before moving the records.

This determination will vary depending upon contract terms, volumes of records in storage at each location, and extraction costs with each vendor. Calendar contract termination dates for vendors to be transitioned later so timely written notice can be provided.

Terms of the extraction from the current vendors can also be negotiated. The following steps are candidates for that discussion.

Obtaining Inventory Lists

Obtain an electronic copy of the inventory in a format that can be manipulated (such as Excel) for each storage location so a smooth matching process from old box numbers to new bar code numbers can occur on boxes being transitioned. It may be advantageous to obtain inventory lists prior to giving notice of contract termination, as charges may be assessed for electronic inventories later.

Alternatively, obtain a PDF version of inventories to enable verifica-

tion of information that locations may not have in their inventory. The disadvantage of obtaining the inventory at this stage is that sites will continue to inbound boxes up until the actual transition date, so inventory records may not be complete at the transition date.

Be sure to note the date each inventory list is obtained, so the gap in the inventory can be closed just before moving the boxes.

Also, note which boxes have been checked out from inventory and either have them returned to inventory to maintain the chain of custody or permanently remove them from inventory and resubmit them as new inventory at a later time.

Determining Removal Costs

Determine the costs associated with removing inventory from the current vendors. These costs can include fees for retrieval, delivery, handling, data entry, and dock use if boxes will be picked up by the new vendor.

Typically costs are charged by the cubic foot rather than by the box, so make sure all the costs involved are clearly understood in order to obtain an accurate picture of exit charges.

Find out when invoices will be received and how charges will be billed (e.g., weekly or monthly). Determine in advance how the number of boxes received will correlate to the charges on the invoice (e.g., whether weekly shipments will have a separate work order number referenced on each invoice so box totals can be verified).

Verify when payment is expected for boxes being delivered. This may be a factor in planning transition schedules if budgeting is a concern.

Setting Box Removal Schedule

Find out from current vendors the volume of boxes that can be extracted each week. Vendors sometimes do not have the manpower to deliver large volumes in a short time frame, so an extraction schedule may need to be developed.

Also, determine how many boxes the new vendor can comfortably accept each week and how long it will be before box information is available in the vendor's system. Discuss the process for locating boxes in transition in case some urgently need to be retrieved.

Good customer service during the transition will go a long way toward improving organization-wide acceptance of the records management program.

Developing Extraction Process

Work with current vendors to develop an extraction process ahead of time. Items to consider include:

- The name and contact information for the onsite manager who will be handling the transition
- When and in what format the boxes shipped will be reported. For example, will the shipping vendor provide a list of boxes being delivered? Or, will the vendor provide a pick list, which may or may not be accurate if all boxes are not located?
- How will boxes be extracted (e.g., by sub-account, location within the warehouse, or some other criteria)?
- How will boxes be transported to the new vendor (i.e., will the current vendor deliver the boxes or will the new vendor pick them up)?
- Is it necessary for the boxes to be delivered or picked up on a specific day or time?
- If the new vendor is picking up the boxes, what size truck will the current vendor's dock accommodate?
- Verify the warehouse addresses where boxes are to be picked up if the vendor has more than one warehouse location.
- Define the process for documenting missing boxes, as documentation will be needed if information contained in those boxes comes into question later (e.g., for litigation or audit).

Step 5: Provide Training

Users will need training on accessing the new vendor's system. Determine when and how the training will be conducted (e.g., web seminar, conference call, or in-person) to accommodate all locations, work shifts, and time zones so all users may attend.

While training should consist primarily of transition issues, the time can also be used to reiterate program information across the organization. Preparing and distributing cheat sheets (including translations in other languages, if applicable) to assist users with utilizing the vendor's system will reduce the volume of questions later.

Keys to a Successful Conclusion

The transition to a new storage vendor can be a lengthy process with many moving parts. To make the transition as smooth as possible, plan ahead and be understanding when mistakes occur. Realize that your vendor has other accounts, and be patient.

Communicate frequently to those affected by the transition. Know that no matter how many communications are issued, some users may remain unaware of the transition.

When the actual consolidation occurs, remain available to trouble shoot as people experience transition issues. Stay calm and help users work through issues that arise.

Good customer service during the transition will go a long way toward improving organization-wide acceptance of the records management program. **END**

Julie Fleming, CRM, can be reached at judgejulie33@aol.com. *Her bio is on page 47.*

Gartner Summits

Gartner Security & Risk Management Summit 2013

June 10 – 13
National Harbor, MD
gartner.com/us/securityrisk

Don't miss the premier IT security and risk event of the year

Save $300 on the standard price with priority code GARTMP4.

Discover five complete programs targeted to your specific security and risk needs

- Chief Information Security Officer (CISO) Program
- IT Security Program
- Business Continuity Management (BCM) Program
- Risk Management and Compliance Program
- The Business of IT Security Program

Scan to save!

GUEST KEYNOTES

Mastermind Interview keynote with Steve Bennett
CEO and Chairman of the Board, Symantec

Admiral Mike Mullen
Chairman of the Joint Chiefs of Staff 2007-2011

Keith Ferrazzi
CEO, Ferrazzi Greenlight; Author, "Who's Got Your Back" and "Never Eat Alone"

EXPLORING

THE PRINCIPLES FOR INCREASING INTEGRITY, OBJECTIVITY IN EXTERNAL AUDITS

Robert J. Dosch, Ph.D., CPA; James P. Haskins, Ph.D.; and Timothy P. O'Keefe, Ph.D.

Because the integrity and objectivity of information are vital to the quality of audit outcomes, records and information management professionals have an important role to play in the audit process.

This article proposes that incorporating the records and information management (RIM) function and Generally Accepted Recordkeeping Principles® (the Principles) into the financial statement audit process will enhance audit integrity and objectivity, increasing the quality of audit outcomes. Therefore, as RIM professionals define and refine the business case for RIM, their potential role in the external audit process should be included.

Internal vs. External Audits

In their November/December 2011 *Information Management* article, "Dodd-Frank Act Puts Focus on Information Governance," Fred Pulzello and Sonali Bhavsar described the Principles as "an important consideration in today's volatile financial market because they help organizations evaluate their current risk state specific to records, disclosures, compliance, and supervision rules,

as well as provide a roadmap to mitigate the risk." They also note that the Principles can be used to satisfy the requirements of the Dodd-Frank Act (Pub. L. 111-203), the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission, and the Federal Reserve, as well as other organizations.

Joanne Frampton, in her March/April 2012 *Information Management* article, "GARP®: A Tool to Drive Internal Auditing," reported, "When RIM is incorporated into the corporate governance and risk management framework and integrated into the internal audit regime, the [Principles] methodology can underpin and drive the entire audit process." She commented that the Principles have "provided the necessary framework and vocabulary to communicate to executives the importance of RIM."

Although Frampton addressed RIM and the Principles in the *internal* audit regime, to date the role that RIM and the Principles can fulfill in the *external* audit process has not been posited.

1. Purpose of an audit and premise upon which an audit is conducted
2. Responsibilities
3. Performance
4. Reporting

The order of the principles highlights the sequence in which an audit is conducted. Each stage of an audit builds upon the work of the prior stages. If specification of the purpose and premise of the audit lacks quality, the remainder of the audit, at a minimum, will lack the same quality.

The first auditing principle, purpose of an audit and premise upon which an audit is conducted, specifically addresses the responsibilities of organizational management and governance. In a financial statement audit, as specified in SAS 122, AU-C 200, paragraph A2, management is responsible:

a. For the preparation and fair presentation of the financial statements in accordance with the applicable financial reporting framework;
b. For the design implementation and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement whether due to fraud or error; and
c. To provide the auditor with
   i. Access to all information of which management and, when appropriate, those charged with governance are aware that is relevant to the preparation and fair presentation of the financial statements, such as records, documentation, and other matters;
   ii. Additional information that the auditor may request from management and, when appropriate, those charged with governance for the purpose of the audit; and
   iii. Unrestricted access to persons within the entity from whom the auditor determines it necessary to obtain audit evidence.

To the extent that RIM, based on the Principles, improves satisfaction of management's financial statement audit responsibilities, the integrity of the foundation upon which the audit is conducted will improve.

To the extent that RIM improves satisfaction of management's financial statement audit responsibilities, the integrity of the foundation upon which the audit is conducted will improve.

The External Audit Framework

External audits of financial statements prepared in the United States are performed according to Generally Accepted Auditing Standards (GAAS).

For companies not registered with the SEC, GAAS are established by the Audit Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). For companies registered with the SEC, GAAS are established by the Public Company Accounting Oversight Board.

The ASB began working on a redrafting and recodification of its U.S. GAAS in 2004, in what is called the Clarity Project. According to the "Clarity Project: Questions and Answers" on the AICPA website, only AU section 322, "The Auditor's Consideration of the Internal Audit Function," remains to be addressed, and it is expected to be released in late 2013 or early 2014.

Audit Principles

One result of the ASB's Clarity Project is Statement on Auditing Standards (SAS) No. 122, "Clarification and Recodification," which is effective for audits of financial statements for periods ending on or after December 15, 2012.

The preface of SAS 122 identifies principles that underlie an audit conducted in accordance with GAAS. These principles fall into four categories:

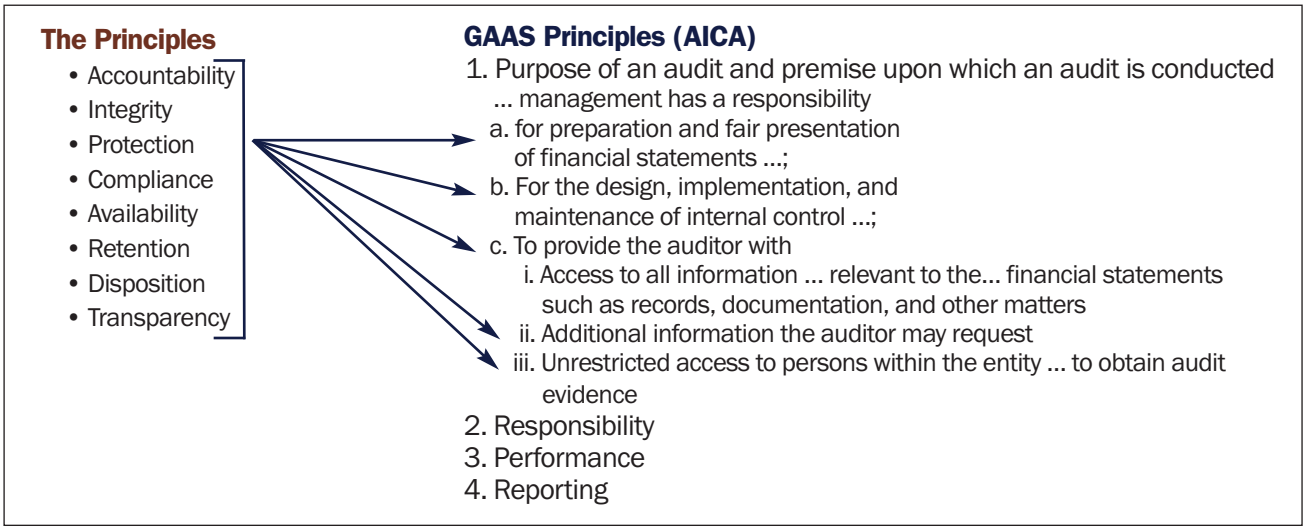


Figure 1: The GAAS Elements Directly Affected by the Principles

Business entities generate a voluminous amount of information. This information must be adequately maintained because it is utilized for key internal and external decisions. According to ARMA International's Principles' website (*www.arma.org/principles*), the Principles were established to assist organizations as they build and improve their RIM systems.

Each of the eight Principles can positively affect elements of organizational management's audit responsibilities.

Principle of Accountability

The Principle of Accountability ensures that the organization has identified an individual with the responsibility and – more importantly, the authority – to design and implement a documented, auditable RIM program. Further, this principle mandates the establishment of a governance structure which will, ideally, incorporate RIM into the organizational culture.

Financial statement auditors note that information products produced by the audited organization are the sole responsibility of the organization.

For example, according to the AICPA's AU 508, "Reports on Audited Financial Statements," the auditor's standard unqualified report for a public company includes the statement "These financial statements are the responsibility of the company's management."

According to SAS No. 122, similar language is used in the auditor's standard unmodified report for a non-public company.

Principle of Integrity

The Principle of Integrity demands that organizational records and information can be reasonably guaranteed to be authentic and unaltered.

Information that exhibits integrity is absolutely foundational and vital to the integrity of the audit process and audit results. The auditor, according to AU 110, "Responsibilities and Functions of the Independent Auditor," is responsible for providing reasonable assurance that there are no material misstatements, whether due to error or fraud.

However, financial statement auditors are rarely responsible for document authentication, according to AU 316, "Consideration of Fraud in a Financial Statement Audit."

The Principle of Integrity is critical to the audit process, and it is the responsibility of management to ensure the integrity of organizational records and information. To the degree an organization has implemented a RIM function based on the Principles, overall confidence in the integrity of records and information should increase.

Principle of Protection

The Principle of Protection dictates that records and information are afforded a reasonable level of protection to ensure the preservation of privacy and confidentiality. This principle is extremely broad, but from the perspective of an audit, it relates to internal controls that protect the integrity of an entity's documented information.

Essentially, the Principle of Protection, correctly implemented, attempts to ensure that only those authorized to create, modify, and/or delete organizational information can do so and that such activity is adequately documented to ensure accountability.

It is management's responsibility to implement internal controls that ensure adequate record and information protection. A Principles-based RIM program will help management incorporate adequate protection to ensure records and information exhibit integrity and that organizational processes and procedures preserve privacy and confidentiality.

Principle of Compliance

The Principle of Compliance requires that a RIM program manages organizational records and information in a manner that satisfies legislative and industry requirements. It is ultimately management's responsibility, but RIM is a vital component in achieving compliance.

The Principle of Compliance is possibly the best example of the interrelatedness of various principles. In order for an organization to be compliant, the Principles of Accountability, Integrity, and Protection must be adequately operationalized.

At a minimum, according to AU 314, "Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement," GAAS require the auditor to obtain an understanding of the design of a company's internal control system and whether the system is implemented.

In certain instances, the financial statement auditor will test the effectiveness of components of the internal control system, according to AU 314 and AS 5, "An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements." Adequate satisfaction of the Principle of Compliance is necessary to meet even minimum expectations in an external audit.

Principle of Availability

The Principle of Availability requires that records are maintained "in a manner that ensures timely, efficient, and accurate retrieval of needed information." The comprehensive scope of the Principles, almost by definition, includes objectives and characteristics that are in conflict.

For example, in order for records to be useful, they must be available, yet the ultimate implementation of the Principles of Integrity and Protection would so limit access that information would be of limited analytical value. The key is to strike an organizationally appropriate balance among the Principles.

A well-designed and implemented RIM program based on the Principles ensures that auditors not only have access to information, but that through the RIM function they potentially have a single resource for the identification, extraction, aggregation, and delivery of the information.

The RIM function is, in all likelihood, the only resource in an organization where knowledge of the organization, definition, format, and location of most, if not all, organizational records and information exists.

Were the RIM function tasked as the primary auditor resource for information in the audit process, fewer financial resources would be expended to retrieve the necessary information and to identify the people with adequate access rights to that information.

Further, since the RIM function does not have custodial responsibility for information, i.e., its creation and modification, the information extracted for the audit exhibits higher credibility.

Principle of Retention

The Principle of Retention requires that records and information are retained through their useful and/or legal life. Adequate implementation of the Principle of Retention ensures that records are available to auditors for the timespan encompassed by the audit. The Principle of Retention cannot be adequately discussed without simultaneous consideration of the Principle of Disposition since retention is bounded by disposition.

Were the RIM function tasked as the primary auditor resource for information in the audit process, fewer financial resources would be expended to retrieve the necessary information.

Principle of Disposition

The Principle of Disposition requires that once retention requirements have been satisfied, records and information will be securely and appropriately deleted. Secure and appropriate disposition preserves the privacy and confidentiality afforded retained records by the Principle of Protection.

While the Principles of Disposition and Retention would seem to embody opposite objectives, they form an integrated, mutually supportive whole. The Principles of Retention and Disposition collectively define the timespan over which organizational records and information are available.

Only through the RIM function can retention and disposition be organizationally implemented and controlled – a Principles-based RIM program will help to ensure that management has met its retention and disposition responsibilities.

Further, by systematically disposing of records once retention requirements have been satisfied, the organization will minimize the resources required to maintain, retrieve, and analyze information.

Regarding the audit function, an intelligent and comprehensive retention and disposition process greatly improves the efficiency of an audit.

	GAAS Purpose and Premise Elements				
The Principles	**a**	**b**	**c.i**	**c.ii**	**c.iii**
Accountability	X	X		X	X
Integrity	X	X	X		
Protection	X	X	X	X	
Compliance	X	X	X	X	
Availability	X	X	X	X	X
Retention	X	X	X	X	
Disposition	X	X	X	X	
Transparency	X	X	X	X	X

Table 1: The Principles/GAAS Purpose and Premise Cross Reference

Principle of Transparency

The Principle of Transparency dictates that an organization's RIM policies and procedures must be understandably documented and that said documentation will be available to appropriate parties.

Transparency in the RIM program is vital to ensuring a successful audit because RIM policy and practices are part of an organization's internal controls – controls which must be understood as part of the audit, according to AU 314.

Further, transparency of RIM policy and procedures will increase auditor confidence in the integrity of the information upon which the audit is conducted. This increased confidence may:

1. Increase the speed with which the audit is conducted
2. Decrease the amount of investigation the auditor feels is necessary to ensure integrity
3. As a result of benefits 1 and 2, potentially decrease the overall cost of the audit

The Principles and Audit Independence

Table 1 cross references the Principles and GAAS elements and highlights the extensive effect the incorporation of RIM, built upon a foundation of the Principles, will have on the financial statement audit process.

Just as proper utilization of the Principles can support and strengthen the internal audit process, a Principles-compliant RIM program can increase the level of integrity and objectivity in an external audit.

The AICPA Code of Professional Conduct ET 101, "Independence," requires auditors be independent of their audit clients, and ET 102, "Integrity and Objectivity," requires them to conduct their audit with integrity and objectivity.

All too often, however, the auditor must request information from individuals who are directly responsible for the information's creation and maintenance. The level of integrity and objectivity in the audit process could be increased if the auditor was able to request information directly from the RIM function independent of the individuals with custodial responsibility.

Further, auditors spend time simply locating information and those who have access to information. The RIM function is potentially a single organizational source of information, of knowledge regarding who has access to information, and of organizational policies associated with information usage and internal controls. The resources required to gather audit information could be greatly reduced if the RIM function served as the primary contact for external auditors.

Conclusion

Financial statement audits are a statutory requirement for publicly traded organizations. Financial statement audits are often required by financial institutions or other stakeholders for privately held organizations. This article cross-references Generally Accepted Recordkeeping Principles® and Generally Accepted Auditing Standards to show how the Principles positively affect the financial statement audit process and outcomes.

Organizational management has several responsibilities in the audit process, the satisfaction of which is the bedrock upon which audit quality is founded. Each of the Principles directly and positively affects management's satisfaction of its audit responsibilities. Consequently, a RIM program built on a foundation of the Principles has business benefits that include, but are not limited to, improvements in the efficiency and, quite possibly, the effectiveness of the external audit function. Records managers should include external audit process benefits in the business case for incorporating the Principles into their organization's RIM program. **END**

Editor's Note: Authors are listed in alphabetical order. Individual contributions to this article are approximately equal. Robert J. Dosch, Ph.D., CPA, can be reached at *rdosch@business.und.edu*. James P. Haskins, Ph.D., can be reached at *jhaskins@business.und.edu*. Timothy P. O'Keefe, Ph.D., can be reached at *tim.okeefe@business.und.edu*. See authors' bios on page 47.

Vendors, Products & People

BULLETIN BOARD

NAID

NAID is the non-profit trade association for the secure destruction industry, which currently represents more than 1,900 member locations globally. NAID's mission is to promote the proper destruction of discarded information through education, the NAID 'em initiative, and encouraging the outsourcing of destruction needs to qualified contractors, including those that are NAID-certified. ***www.bitly.com/NAID2013***.

Downstream Data Coverage

Downstream Data Coverage offers professional liability coverage that specifically addresses the risks associated with NAID-certified companies that provide data-related services. Call 877.710.2498 to learn more.

RSD recently announced IGaaS™, or Information Governance as a Service. Whether governing information stored on premise or within the cloud, IGaaS™ provides all services for in-place information governance including: policy definition, information classification, policy enforcement, information access, life-cycle management, audit, and compliance. RSD GLASS® deployed as a service mitigates the risks and lowers the costs associated with storing information in the cloud. For more information, download our complimentary white paper at ***www.rsd.com/wp-igaas.***

ZASIO

Records Management Consulting + Software

There are many challenges to globalizing records retention in a multinational company. Zasio's team of records retention specialists is highly skilled at globally harmonizing retention policies, typically from a U.S. baseline, and for recommending country exceptions where required. To solve any records retention challenge, it takes two other key components – a software tool and a solid strategy for implementation. Zasio Enterprises Inc. has such a solution – called Versatile Retention International™ – and it is unique in the records management industry.

For Zasio's FREE WHITE PAPER "Globalizing Records Retention in a Multinational Company," visit: ***www.zasio.com/consulting_whitePapers.asp.***

EDUCATE!

For more information, visit *www.arma.org/conference.*

VIVA! ARMALAS VEGAS2013
Conference & Expo, October 28-30
The Venetian Congress Center

The Principles at Work in a Canadian Regional Government

Julie Gable, CRM, CDIA, FAI

Recordkeeping may look the same in government as it does in business, but there are important differences in both how and why records are kept. (See Figure 1 on page 39.) To their credit, the Generally Accepted Recordkeeping Principles® (Principles) can provide as much practical value in the public sector as they do in business.

Just ask Clare Cameron, CIP, information management coordinator for the Regional Municipality of Niagara, which serves 12 communities in Ontario, Canada. The Niagara region nestles between Lake Erie and Lake Ontario, with the Niagara River as its eastern boundary with the United States. It covers 1,852 kilometers and has a population of more than 427,000. One of its best-known features is Niagara Falls.

Regional municipalities in Canada are something like U.S. counties. They are formed in populated areas to realize cost efficiencies in providing centralized services to an entire area rather than having each town provide its own.

Impetus for Records Management

At its inception in 1969, the Niagara regional government was primarily a vehicle for capital improvements, such as roads and water treatment projects that required significant funding. The early impetus for records management came from the Financial Services Department as it focused on the need to keep track of capital, debt, and tax collection records associated with these public works projects.

The Region's services now include water, waste collection, public transit, police, emergency services, public health, and social services, and it creates an estimated 1.2 million paper and electronic records annually.

Steps Toward IM Services

Niagara Region's first steps toward a formal information management services (IMS) function began in 1991, driven in part by the passage of the Ontario Municipal Freedom of Information and Protection of Privacy Act. This legislation gives citizens access to municipal information and mandates the privacy of personal information that governments maintain about individuals.

In terms of the Principles, the law requires government organiza-

Entity	Business	Government
Reason for existence	• Make a profit for shareholders	• Serve the public
Reason for records	• Develop new products • Market products successfully • Account for revenues and costs	• Document democratic processes, citizen rights, and obligations • Operate services for the public good
Major concern about records	• Protect intellectual property	• Assure openness and accessibility as part of public accountability
Emphasis on	• Predicting the future	• Preserving history

Figure 1: Comparison of Public- and Private-Sector Need for Records

tions to demonstrate the Principles of Protection and Availability as integral aspects of compliance.

Records Retention, Storage

As part of its efforts to meet the law's requirements, Niagara initiated its first records retention bylaw and retention schedule based on the Ontario Municipal Records Management Standard (TOMRMS), a methodology for organizing municipal documents that was itself developed by the Association of Municipal Clerks, Managers and Treasurers of Ontario, a professional organization for government leaders.

TOMRMS includes a classification scheme, records descriptions, generic codes to track and inventory records, and retention periods. By 2000, Niagara Region had a records retention schedule, an in-house records storage facility, and an Access database to track record locations.

"There was and continues to be an increased focus on accountability, risk management, privacy, and access," says Cameron, who has held her current position since 2008. "We must assure that the public can access required records but also assure that there are no privacy breaches."

Principles in Play

Cameron first became aware of the Principles by attending ARMA International events. When reviewing them in more detail, she noticed parallels with the Canadian Standards Association's Privacy Code, which Niagara had used for its corporate access policy.

"The Principles sum up values and best practices that we were already aiming to achieve," says Cameron, "But they provide a structure, a framework for ensuring that ideals can be met."

Applying the Principles

Some of the opportunities and challenges in applying the Principles at Niagara Region are a direct result of the unique situations governments face.

Accountability

While the Principle of Accountability recommends that a senior executive be involved in the records program with responsibility distributed throughout the organization, this is not always possible in regional government.

In U.S. counties, for example, leadership is a combination of elected, appointed, and hired positions, and departments exist in peer relationship rather than in any strict hierarchy. Departments have their own budgets and the freedom to choose their own information management methods. In these situations, records and information management staff can provide advice and guidance in the hope of influencing department decision makers, but there is no top-down mandate.

The same is true for Niagara Region, where IMS reports to the Office of the Regional Clerk, which is part of the Integrated Community Planning Department reporting to the chief administrative officer.

Cameron has dealt with the accountability challenge in several ways. She has developed a network of super users and administrative staff within the divisions and departments. She also turns to Legal Services and Information Technology on questions of legality and security.

In the near future, "The Principles will be formally incorporated to drive discussion at a newly reworked Information Governance Committee composed of staff with a particular interest or concern in information management across the organization," notes Cameron. Niagara is also trying to recruit Information Governance Committee members who report directly to senior management.

Another challenge has been to translate the Principles so senior management can grasp the concepts and see their practical application at Niagara.

"Offering the entire Principles

framework would potentially be overwhelming," says Cameron, "so we have to find ways to communicate the Principles to managers in a way that is specifically meaningful to their areas." She has found that using scenarios works well in this regard, as they can paint a picture of what needs to happen if a given event occurs and the crucial role that good recordkeeping practices can play.

Cameron has discovered that there is also great diversity in the understanding of information management within departments. Departments that handle a high volume of private information, such as Public Health, tend to have a better understanding than those that don't, she says.

periods shorter, where possible – a move that may result in cost savings for contracted records storage services. Work on the new bylaw also includes identifying the Office of Record for each records series as a way to reduce the amount of duplicate information being retained and stored.

Another change is an attempt to separate record series from filing needs. Cameron explains, "We are trying to make a distinction between the goals of the retention bylaws and the day-to-day filing needs of the business units."

Previously, there were attempts to use the retention bylaws as departmental filing standards. Now the hope is to reduce the complexity of the records bylaw and make it easier to use, working in partnership with departmental filing needs instead of competing with them.

"We want RIM policies, as well as information access and privacy policies, to be perceived as fresh, current, and easy to understand in order to improve compliance across the organization."

Compliance

Under the Principle of Compliance, Cameron is working to improve legislative research, which she sees as an important part of the retention program. IMS has revised its records bylaw every 18 months to two years. According to Cameron, "The latest revision has been very significant. We are reducing the number of overall codes to choose from when classifying records for retention purposes and improving the level of detail in descriptions."

Because physical records storage was outsourced in 2012, Cameron is revisiting legal requirements as a potential way to make retention pe-

Transparency

The Principles were incorporated into a new 2012 Records and Information Corporate Policy and will be listed as a reference to the upcoming 2013 Records Retention By-law. By documenting policies and making processes easy to understand, Cameron hopes to support the Principle of Transparency as well as the Principle of Compliance.

"We want RIM policies, as well as information access and privacy policies, to be perceived as fresh, current, and easy to understand in order to improve compliance across the organization," she states.

Integrity

The Principle of Integrity presents a challenge for paper records stored offsite. While boxes are coded and an audit trail of box movement is possible, the same isn't true for folders. There is no way to know whether anything has been removed from a paper file that has been retrieved. Cameron's efforts to ensure integrity of paper files are chiefly through training and informational sessions.

She is currently working on an online model for teaching privacy and information protection. IMS also does custom training that is flexible and designed to connect with the Region's staff in meaningful ways.

Cameron is also striving to raise awareness that records policy and bylaws apply to both paper and electronic records, and she is currently working with Niagara's Information Technology (IT) Solutions staff on this. For electronic records, the potential overlap of tasks between IMS and IT is perhaps the greatest challenge.

"IT may have initiatives under way that have governance implications for IMS, but because we operate in different departments, we may not always be aware of these efforts," Cameron says.

Protection

She has used the Principle of Protection to try to work more closely with IT and security staff to ensure that questions of security and protection are being addressed when new systems are created. The Principles have been useful in these conversations and provide a reference for the right questions to ask. "It is part of our IMS goal to present ourselves as open, easy to contact,

and eager to collaborate," notes Cameron.

Disposition

The Principle of Disposition is an example of the need for such close cooperation. Cameron is in the process of developing procedures for disposing of expired electronic records on shared drives, "but for structured data the issue is more delicate, as many database entries are cross-referenced, so deleting expired entries may compromise the quality of associated data. Disposition tools are seldom built into electronic systems from the beginning and are difficult to add later."

Increased collaboration and enhanced partnership with IT are at the top of her list for the future.

Next Steps

This year, Niagara Region's IMS plans to use the Information Governance Maturity Model (IGMM) and perform an assessment of the information management program, its effectiveness, strengths, and weaknesses. The results will be used as input to the IMS strategic plan and as a way to prioritize a work plan for the six-member IMS team.

"We're aiming for a [maturity level] three in most categories of the IGMM, realizing that it will take time to close any gaps identified through the model, but our group culture is to take a proactive stance on issues," says Cameron, "and we know that processes in information management are always evolving. Our immediate plan is to increase the emphasis on compliance, performance monitoring, and measurement for the relative success and status of the corporate-wide information management program."

It's safe to say that the Principles will be ready to help. **END**

Julie Gable, CRM, CDIA, FAI, can be contacted at juliegable@verizon.net.
See her bio on page 47.

Digital Dusting

Spring Cleaning for Network Drives

Blake E. Richardson, CRM, CIP

Spring is the traditional time to clear out clutter and deep clean. For organizations, that should include a thorough clean-up of network drives, where they are sure to find a lot of "digital dust" – which might be thought of as invisible electronic matter that shrouds digital files stored on those drives. Digital dust results in electronic clutter, employee frustration, the need to purchase additional storage space, and increased organizational risks.

Obviously, digital dust does not actually exist. However, the effects of improper management of electronic files on network drives are all too real. Over the past decade, the volume of digital content has exploded. According to EMC's 2011 electronic growth study, it is estimated that the world's electronic information is doubling every two years.

The majority of the volume is *unstructured information* – such as spreadsheets, word processing documents, e-mail, and image formats like PDFs and tiff files – which in many cases finds its way onto company network drives where it collects the figurative digital dust.

Regardless of the size or nature of an organization, its employees receive and create electronic information, and in many cases they store it on network drives. The absence of organizational guidance and controls in this area results in network and hard drives becoming digital graveyards that impede risk management efforts, corporate decision making, e-discovery, and operational efficiency.

The reality is that most organizations – even companies that have implemented enterprise content management or document management applications – still continue to rely heavily on the use of network drives. For many organizations, the use of network drives is a necessity; it represents the only logical choice of repository for the storage of large amounts of unstructured data.

Understanding Network Drives

Since the use of network drives remains prevalent, it is important to understand their characteristics and limitations in order to properly manage their use, maximize their potential, and avoid the digital dust effect.

Folder Structure

Network drives contain folders created to segregate organizational departments or operations located on the same network drive. In most cases, additional subfolders are created under the primary folder to group content of a similar nature. Security settings can be configured to grant or deny access to certain folders or prevent employees from creating new primary or subfolders.

Naming Conventions

If an employee has authorization privileges to create new subfolders, the network drive does not place any restrictions on the naming convention used to label the folder.

Duplication

Network drives have limited ability to prevent the storing of duplicate files. Network drives can detect duplication only if an employee is attempting to save a file using a file name that already exists in the same folder.

However, network drives do not prevent files with the same name from being stored in different subfolders.

Versioning

Network drives do not facilitate the automated versioning of files. If a stored file is modified, the employee has to reflect the new version by manually renaming the file with a new version number or combination of new version number and date of modification. However, by assigning a new name to the file, the former file still exists unless the employee deletes the former file.

Metadata

Unlike enterprise content management or document management software applications that allow users to create and assign metadata such as multiple keyword values to content, the only metadata an employee can assign to a file in a network drive environment is the file name.

Searching

The absence of additional assigned metadata limits network drive searching capabilities. Network drives allow searching by folder, all or part of the file name, date of file, size of file, phrase or words contained in the file, and modification date.

Retention Management

Network drives do not have automated retention management capabilities. Files stored on network drives have to be manually deleted if they no longer need to be retained.

One Solution for Limitations

Most enterprise content management and document management software applications contain functionality that resolves the aforementioned limitations of network drives.

Bringing Structure to Network Drives

One of the primary causes of digital dust is the lack of adequate network drive folder structures. Saving files to network drives is convenient – a few clicks of the mouse, some typing, and a file is stored. However, without structure, that convenience can be a detriment.

Imagine the equivalent scenario for a physical document that needs to be filed if there is only a single file cabinet drawer and one large hanging folder to receive it. Filing the document is very convenient because there is only one filing option.

But imagine that after several months, when hundreds or thousands of documents have been added to that single hanging folder, that specific document needs to be retrieved. Convenience no longer exists. Attempting to locate that document amongst all of those stored in that one hanging folder will take a lot of time and effort. The convenience of filing that document, then, will result in diminished efficiency, customer service, and decision making.

Without the creation of a proper folder and subfolder structure, employees attempting to locate a specific file will be searching for a needle in an electronic haystack.

The same scenario holds true for electronic files stored on network drives. Without the creation of a proper folder and subfolder structure, employees attempting to locate a specific file will be searching for a needle in an electronic haystack.

Folders

Since network drive primary folders are typically established and configured for each department sharing the drive, the following information will address how to develop an effective folder structure at the departmental level.

The first step in creating a network drive folder structure is to appoint departmental representatives who have a proficient knowledge of the department's business processes to determine what types of unstructured content are created and received in support of the functions. This step excludes *structured content,* which resides in database-oriented applications such as enterprise resource planning systems.

Once the unstructured content has been identified, the department representatives should determine the types of information that will be stored on the network drive. In most cases, the folder structure will comprise the primary folder (department name) plus several subfolders that represent the major categories of departmental functions.

Within each subfolder, it is common to add additional subfolders that allow for further filing and searching refinement. Figure 1 on page 44 illustrates an inefficient network drive folder structure. In this example, the primary folder is HR. However, rather than having additional subfolders pertaining to major department functions, all files are saved to the primary folder, making filing easy, but impeding subsequent searching.

Figure 2 on page 46 illustrates an enhanced and efficient folder structure. Though it takes an initial investment of time and resources to create an effective folder structure, the return on the investment can be measured in quicker retrieval times and reductions in misfiled and un-locatable information.

Once an effective departmental folder structure has been created, it is important to establish controls. It is recommended that an employee (and a backup) be designated to monitor and control the establishment of new folders in the directory. If feasible, only a limited number of employees should be able to create new folders. This approach helps ensure that the integrity of the folder structure is maintained. If a new folder needs to be created, it is advisable to have the request approved by department management or its designee.

Naming Conventions

To complement and increase the effectiveness of folder structures, it is important to establish naming conventions for folders and files. A good folder structure will fail to serve its purpose if the employees using it do not understand what the folders represent. Therefore, as part of the folder structure development process, there should be a consensus among employees as to folder naming.

Folders should be labeled in a manner that represents the logical name of a departmental process or function. Folder names should not be cryptic, include acronyms, or be named in a fashion recognizable only to department employees.

In some cases, it may be appropriate to include as part of the folder name the retention period of the files located within the folder. For example, a folder that contains invoices may be labeled "Invoices - 7 Years." This will assist employees in the proper deletion of content and prevent the accumulation of information that is no longer needed.

Folder names can also be subsequently modified to facilitate legal holds. If the contents of a folder need to be held, the folder name can be modified to include the words "Legal Hold (Do Not Delete)" until the hold is rescinded. It is important to remember that in the event of e-discovery, audits, or inquiries, other departments may need access to the folders and files. Therefore, the naming conventions used should be recognizable by other employees.

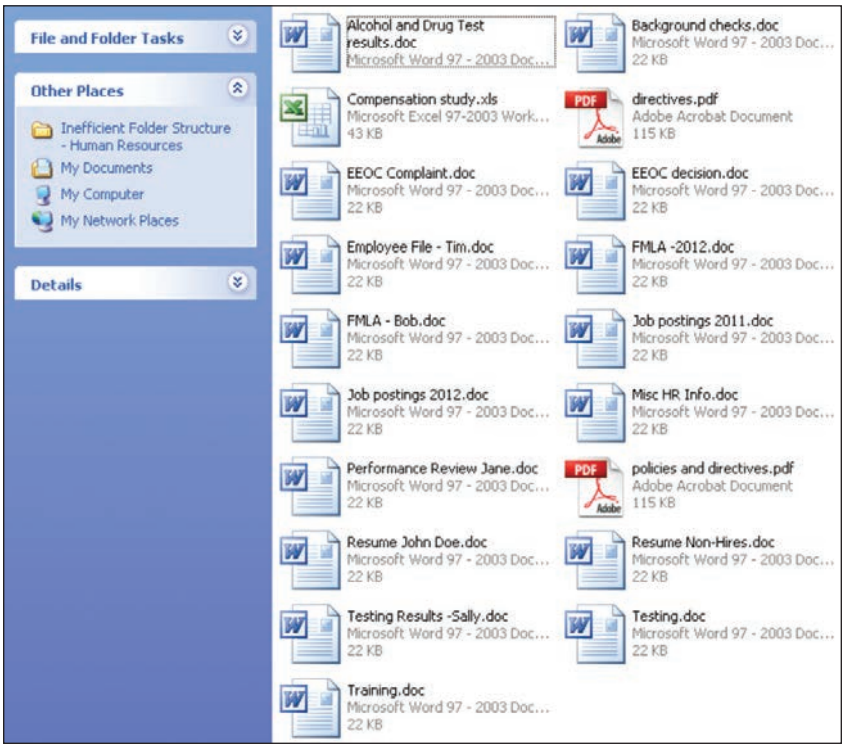


Figure 1: Inefficent Folder Structure – Human Resources

In addition to establishing standards for properly naming folders, there should be standards developed for naming files. The best folder structures will meet their demise if the files contained in the folders are not properly named. Files should also be named in a logical manner, avoiding acronyms and abbreviations.

The litmus test for naming files should be that any company employee could read the file name and understand the nature of the file without having to open it. If an employee has to open several files before he or she finds the one needed, there is a good chance that files are not being properly named.

Naming standards may include a consistent file prefix or suffix such as the date the file is stored, employee last name, or vendor company name.

Regardless of the standard implemented, it is important that it be followed. Employees who have been designated to monitor and control the creation of new folders can also periodically review file names to determine if the standards are being followed.

Dusting Your Drives

Most organizations have been using network drives for an extended period of time – meaning the digital dust storm most likely has already occurred. Tens or hundreds of thousands of files that no longer need to be retained are cluttering the folders, the employees who saved the files may no longer be with the organization, and the digital dust is continuing to collect.

The review should serve two purposes: deleting information that is no longer needed and – just as important – restructuring and renaming folders and renaming files, if needed.

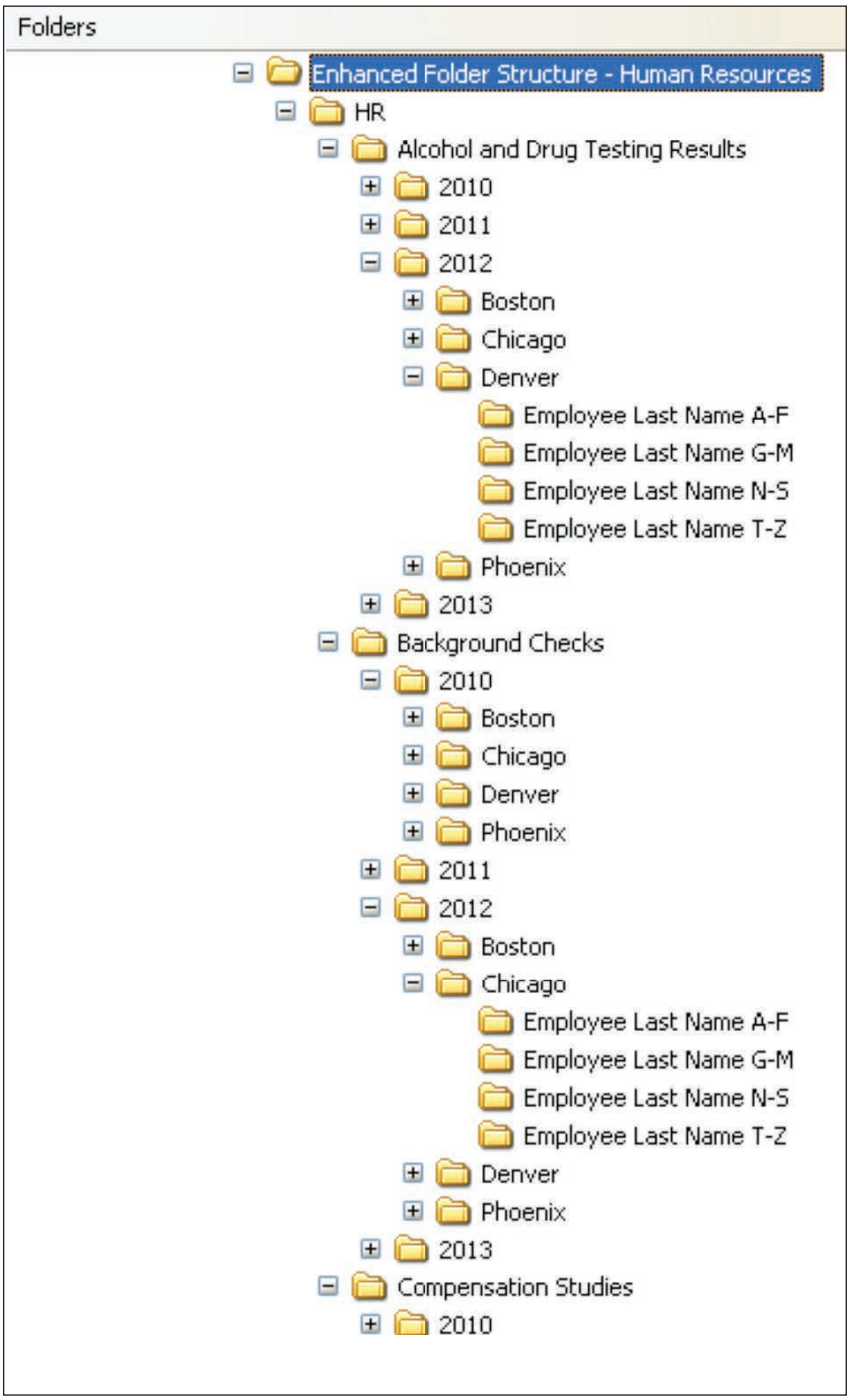


Figure 2: Enhanced Folder Structure – Human Resources

Understanding how to create an effective folder structure and naming convention is a great start. However, most organizations are affected by years of improper network drive management. To dust your drives requires a manual file review, which can be very labor-intensive, or it may require acquiring and implementing software targeted for this purpose.

Manual Review

The file review involves departmental employees manually reviewing all files and determining whether they need to be retained or deleted. However, it is vital that before and during this process that all employees review the department's retention schedule and applicable legal and tax holds. This will help ensure that files that still need to be retained and content relevant to holds are not deleted.

Computer operating systems can assist during the review process. Most systems allow users to view the date a file was created, last modified, and accessed. For non-record content, an organization may decide that files that have not been modified or accessed in the past three years should be deleted. If the file constitutes an official company record, then the record retention schedule will dictate whether the file can be deleted.

Computer-Assisted Review

Software applications can be used in lieu of a manual review. Software referred to as "index and classification management" can be installed that collects information about network drive files and presents back to the user what content may be eligible to be deleted. These systems can detect duplicate or near-duplicate files, allowing the employee to decide what files should be deleted.

Keeping Drives Clean

Regardless of the dusting method employed, it will take time to clean up years of improper network drive use. Once the organization's drives have been cleaned and controls have been established, employees will be able to more efficiently file and retrieve content. Keeping the digital dust under control with subsequent annual reviews and cleanings will be light housework by comparison! **END**

Blake Richardson, CRM, CIP, can be contacted at titansfan100@gmail.com.
See his bio on page 47.

Introducing the official

GENERALLY ACCEPTED RECORDKEEPING PRINCIPLES®

ASSESSMENT

ARMA International's new assessment evaluates more than **100 information governance attributes.** It can be deployed across the enterprise to determine how a department, division, location, or your entire organization measures up against the **Generally Accepted Recordkeeping Principles®.** Take advantage of this set of **organization-improving attributes** today!

Now Available! *www.arma.org/assessment*

Special thanks to our
Generally Accepted Recordkeeping
Principles® outreach sponsors:

Autonomy
an HP company

EMC²

Contact Information

AUTHOR INFO


Allen


Dosch

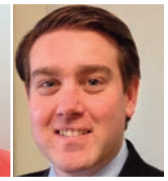

Fleming


Gable


Haskins


O'Keefe


Richardson


Wylie

Managing and Collecting Social Media for E-Discovery page 22

Lauren A. Allen, J.D., PMP, is a program manager for Deloitte Financial Advisory Services. In her role, she serves federal government agency clients on electronic discovery engagements. With more than 11 years of electronic discovery experience, Allen also holds Project Management Professional certification from the Project Management Institute and earned her legal degree at Hofstra University School of Law. She can be contacted at *laurenallen@deloitte.com*.

Michael C. Wylie, J.D., is a project management specialist with Deloitte Financial Advisory Services, focusing on discovery and federal litigation involving environmental claims. He has more than five years of experience serving federal government agency clients. Wylie earned his law degree at the University of Richmond School of Law. He can be contacted at *miwylie@deloitte.com*.

5 Steps for Managing an Offsite Storage Vendor Consolidation page 27

Julie Fleming, CRM, has been active in the RIM profession in the automotive, energy, pharmaceuticals, and healthcare fields since 2001. In 2011, she managed a multiple vendor consolidation of approximately15,000 boxes for the largest physicians management company in the United States. Fleming earned her bachelor's degree in business administration from Walden University and obtained her CRM in 2008. She can be contacted at *judgejulie33@aol.com*.

Exploring the Principles for Increasing Integrity, Objectivity in External Audits page 32

Editor's Note: Authors are listed in alphabetical order. Individual contributions to this article are approximately equal.

Robert J. Dosch, Ph.D., CPA, is an associate professor of accounting at the University of North Dakota. He earned his Ph.D. in accounting from the University of Iowa. His teaching and research primarily focus on auditing and fraud examination topics. He can be contacted at *rdosch@business.und.edu*.

James P. Haskins, Ph.D., is an assistant professor of finance at the University of North Dakota and a Certified Risk Manager. He earned his Ph.D. at Colorado State University. Haskins has conducted interdisciplinary research in several areas, including corporate finance, investment finance, private equity decisions, ethics, and banking. He can be contacted at *jhaskins@business.und.edu*.

Timothy P. O'Keefe, Ph.D., is chair of information systems and business education at the University of North Dakota. A university professor for 30 years, he earned his Ph.D. at the University of Arkansas. O'Keefe's primary research focus has been the improvement of the records management and information technology interface. He can be contacted at *tim.okeefe@business.und.edu*.

The Generally Accepted Recordkeeping Principles® Series: The Principles at Work in a Canadian Regional Government page 38

Julie Gable, CRM, CDIA, FAI, is president and founder of Gable Consulting LLC. She has more than 25 years of experience specializing in strategic planning for electronic records management, including business case development, cost-benefit analysis, requirements definition, and work plan prioritization. In 2003, she was named a Fellow of ARMA International. Gable has authored numerous articles and frequently speaks at national and international conferences. She holds a master's degree in finance from St. Joseph's University and a bachelor's degree in management from Drexel University. Gable can be contacted at *juliegable@ verizon.net*.

RIM Fundamentals Series: Digital Dusting: Spring Cleaning for Network Drives page 42

Blake Richardson, CRM, CIP, is a Certified Records Management and Certified Information Professional with more than 16 years of records and information management experience with several *Fortune* 500 countries. The corporate records manager for a national grocery retailer, Richardson is also author of *Records Management for Dummies*, published late last year by Wiley. He can be contacted at *titansfan100 @gmail.com*.

AD INDEX Contact Information

15, 17 **Access Sciences**
800.242.2005 – Intl. 904.213.0448 –
www.accessciences.com/contactus

9 **DHS Worldwide Software**
800.377.8406 – Intl. 904.213.0448 –
www.dhsworldwide.com

IBC **Downstream Data Coverage**
www.downstreamdata.com

31 **Gartner Security and Risk Management Summit**
www.gartner.com/us/securityrisk

21 **Institute of Certified Records Managers**
877.244.3128 – *www.ICRM.org*

BC **Iron Mountain**
www.ironmountain.com/advantage

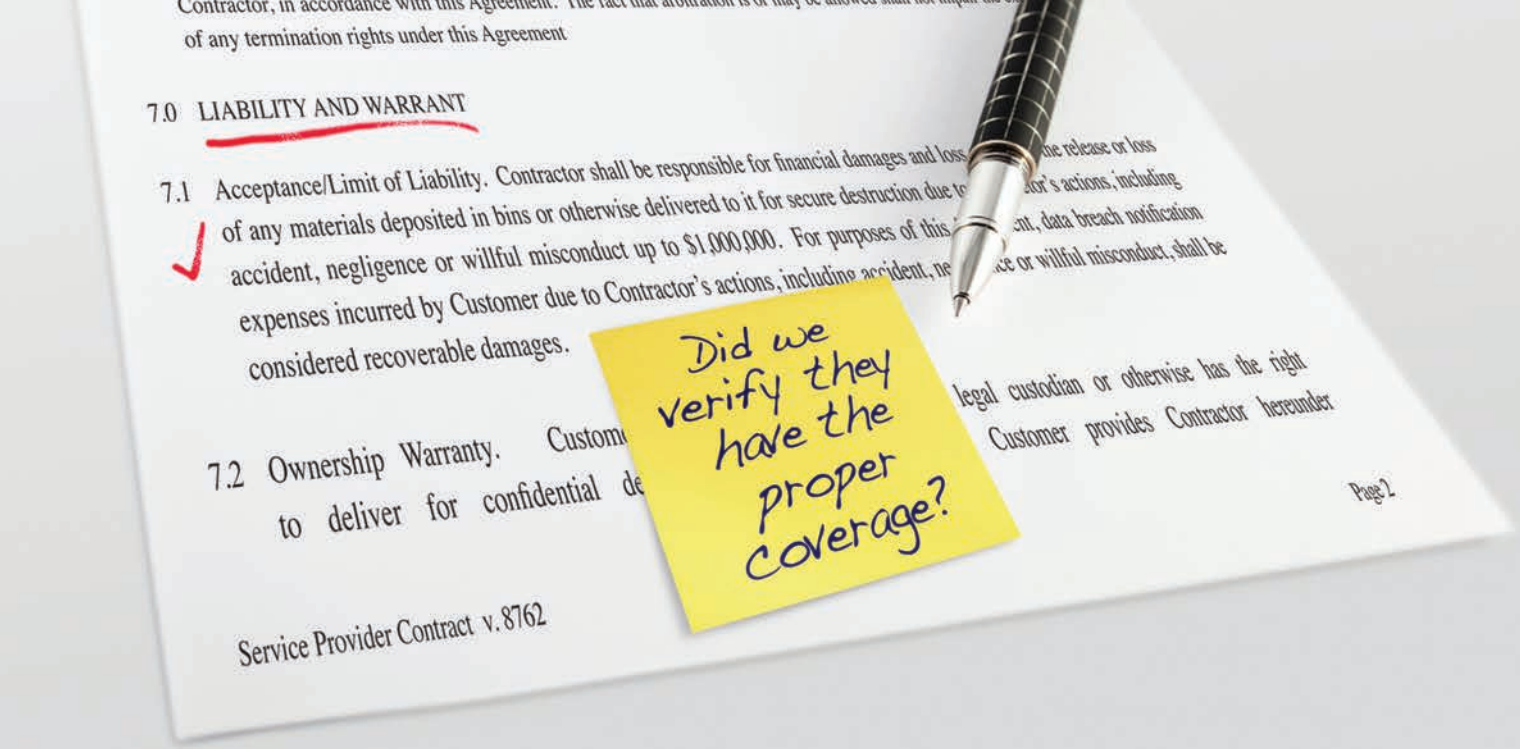
20 **iScan**
410.800.8332 – *www.iscan.com*

5 **NAID**
www.naid-em.org

IFC **RSD**
www.rsd.com

13 **Xact Data Discovery**
877.545.XACT – *www.xactdatadiscovery.com*

3 **Zasio Enterprises Inc.**
800.513.1000 Opt. 1 – *www.zasio.com*



Some customers assume their service providers have the proper liability insurance to cover their mistakes.

Unfortunately, that is not always true.

The National Association for Information Destruction (NAID), the non-profit watchdog for the secure destruction industry, discovered that most professional liability products do not offer adequate protection. So NAID created Downstream Data Coverage, a policy that better protects providers and customers.

- Includes data breach notification coverage to the full limit of the policy
- Requires periodic, unannounced audits of service providers
- Covers liability for electronic media destruction to the full limit of the policy
- Eliminates exclusions that make other policies useless

To protect your organization, encourage your service provider to look into Downstream Data Coverage today.

Downstream® Data Coverage

www.downstreamdata.com

EMPLOYEES WASTE VALUABLE HOURS EACH WEEK CHASING HARDCOPY DOCUMENTS.

(SOMETIMES, THEY EVEN FIND THEM.)

Companies today are trying to find new ways to cut costs. Chances are, yours is too. And yet, you may well be missing out on a major opportunity. Simply by making your records management more efficient, you can dramatically cut operational costs. Eliminating the time employees waste searching for documents is just one way to potentially put money back on your bottom line.

Learn more about how Iron Mountain® can help you cut costs and turn records management into a source of opportunity at: **ironmountain.com/advantage**

IRON MOUNTAIN®