INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

JULY/AUGUST 2014

Imagine the possibilities

with Information Management in the Cloud from ECM to eDiscovery

HP Autonomy's Cloud Solutions provide industry leading document management, search, process automation, secure collaboration, records management, and eDiscovery on a private cloud basis, hosted in HP's secure cloud centers.

Let us show you the possibilities with information management in the cloud at ILTA 2014, **Booth 606/608**

INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

JULY/AUGUST 2014

Top IG Tech Trends: Auto-Classification & Big Data

Page 20

Leveraging the Principle of Availability to Show ROI

Page 26

Cut Costs, Risks with Proactive Litigation Plan

Page 34

rsd Your Information. Governed.

Enforce desirable behavior

in the creation, use, archiving, and deletion of all corporate-related information.

RSD is the leading provider of information governance (IG) solutions for the enterprise. RSD GLASS® is the first patent-pending IG platform built from the ground up; making it easy for companies to solve the complex problem of what information they should keep and what they are allowed to get rid of with our policy management and enforcement engine for electronic and physical records. Using RSD GLASS, companies create corporate policies that are actively enforced across organizational and jurisdictional boundaries, IT systems, content repositories, content inthe cloud, and paper archives.

With RSD GLASS, you keep the information you need to grow your business, safely disposing the information you are allowed to – reducing storage and operating costs, risk exposure, and legal fees; all in the convenience of one system.

www.rsd.com

RSD GLASS® has 7 Benefits to help ensure your Information Governance goals are met.

INFORMATION MANAGEMENT

JULY/AUGUST 2014 **VOLUME 48 NUMBER 4**

INFORMATION
MANAGEMENT
AN ARMA INTERNATIONAL PUBLICATION

Publisher: Marilyn Bier

Editor in Chief: Vicki Wiler

Contributing Editors: Cyndy Launchbaugh, Jeff Whited

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 professional 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 editorial submissions. 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 +1 888.277.5838 (US/Canada), +1 913.217.6022 (International), +1 913.341.3742, or e-mail *Karen.Krista@ armaintl.org*.

Opinions and suggestions of the writers and authors of articles in *Information Management* do not necessarily reflect the opinion or policy of ARMA International. Acceptance of advertising is for the benefit and information of the membership and readers, but it does not constitute official endorsement by ARMA International of the product or service advertised.

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.

XACT DATA DISCOVERY

Fact: The world is digital.

Fact: Paper hasn't disappeared.

Xact Data Discovery is both

IN-HOUSE FORENSICS	ELECTRONIC DISCOVERY	NO-FEE PROJECT MANAGEMENT	DATA HOSTING & MANAGED REVIEW	PAPER DISCOVERY

XDD delivers EVERYTHING you need to tackle today's complex discovery challenges.

xactdatadiscovery.com
1.877.545.XACT

XACT DATA DISCOVERY
Because you need to know

Proving the ROI for an Effective IG Program

Despite the diversity of topics covered in this issue of *Information Management*, an underlying theme begins to emerge as you make your way through the feature articles: the return on investment (ROI) for effective information governance (IG). For many, the prospect of being able to add to your organization's bottom line, rather than being part of a cost center, should be a welcome one.

For example, if your organization is aggregating "big data" - which is one of the top two IG technology trends Gordon E.G. Hoke, IGP, CRM, discusses in his cover article - you can help ensure the high quality and accessibility needed to leverage it for such revenue-producing purposes as planning, customer service, research and development, and marketing.

This will require you to be knowledgeable about other functional areas and to develop collaborative relationships with and among IG stakeholders, who often work in silos. "Indeed," Hoke writes, "the task for the IG professional is to facilitate and enable cooperation."

A strong relationship with the information technology (IT) group is especially critical to governing big data. Hoke writes, "…unless technology plays a robust role, only limited IG progress will accrue from policies, procedures, and practices."

A University of Texas and Indian School of Business study of more than 150 Fortune 1000 firms underscores that point. The results of *Impacts of Effective Data on Operational Efficiency*, which studied the business implications of an organization's data quality, the ability for that data to be accessed wherever and whenever it's needed, and the relevance of that data in addressing a specific problem, "definitely demonstrate the often dramatic impacts that even marginal investments in information technology can have when that technology addresses data quality, usability, and intelligence…"

One technology investment organizations are making is for auto-classification tools that will help them better govern their data. These and related tools used for predictive coding, computer-assisted review, and content analytics represent the other top IG trend identified at the ARMA/Sedona Conference IG executive conference this spring. These technologies use algorithms to identify and classify records or even derive the meaning of content more quickly and accurately than humans can, Hoke writes.

Predictive coding and content analytic tools, which are primarily used to help identify information that is relevant to electronic discovery, can also be used to identify information that can be eliminated. "Reducing the universe of immaterial documents decreases risks associated with errors in large-scale document review and production,"

Michael C. Wylie, J.D., PMP, and Kelli Layton, J.D. write in "Cut Costs, Risks, with Proactive Litigation Plan." Cutting storage and litigation expenses is another way to show IG ROI.

In our Principles Series article, Julie Gable, CRM, CDIA, FAI, writes about how to leverage the Generally Accepted Recordkeeping Principles® Principle of Availability to show ROI. In one case study scenario, she shows how destroying thousands of boxes of eligible records not only enhanced the availability of the remaining information but saved more than $300,000 annually in storage and retrieval costs.

We'd like to hear how you are proving your IG program's ROI. E-mail us at *editor@armaintl.org.*

Vicki Wiler
Editor in Chief

Compliance monitoring is just a click away

Data protection regulations require organizations to monitor the qualifications and compliance of service providers that process sensitive information.

NAID just made this a lot easier!

Select the "**NAID AAA Notification**" link in NAID's member directory to receive emails announcing status changes to that member's certification and compliance qualifications.

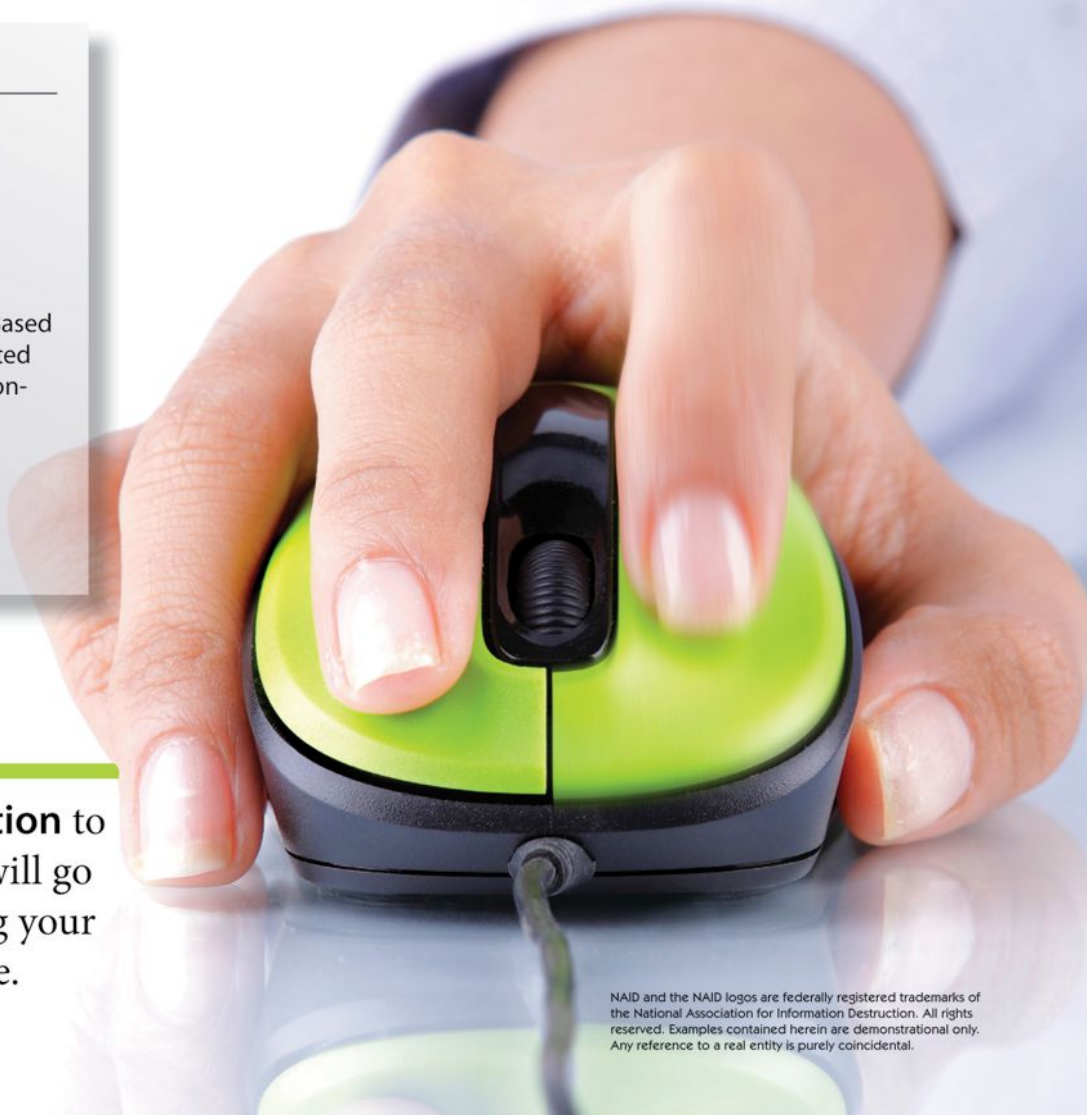
Data Destruction Co.

John Smith
123 S. 1st Ave.
Smalltown, AZ 85011
234-567-8901
www.123destruction.com

NAID CERTIFIED: Mobile and Plant-Based Operations Endorsed for Paper/Printed Media, Computer Hard Drive and Non-Paper Media Destruction

Original Date: January 16, 2008
Expiration Date: August 31, 2014

NAID AAA Notification



Visit **bit.ly/AAAnotification** to sign up. This simple act will go a long way in establishing your organization's compliance.

CYBERSECURITY

China Halts Cybersecurity Cooperation

China recently suspended its participation in the U.S.-China cybersecurity working group established last summer. The decision was in response to the announcement that the United States had indicted five Chinese military officials on charges of stealing trade secrets.

There have been hundreds of instances of Chinese military hackers breaching U.S. entities over the last several years, but the U.S. Justice department focused on five companies specializing in solar panels, metals, and next-generation nuclear plants, reported *Bloomberg*.

Predictably, there are some who are concerned that China will retaliate against U.S. companies. Kerry Brown, director of the China Studies Center and professor of Chinese politics at the University of Sydney, said it is unlikely that China will do so "explicitly." He added that the working group effectively established a mechanism for dialog on cybersecurity that may resume once things have calmed down.

EHR

Review: Australia's E-Health Records Program Should Be Opt-Out

When Australia rolled out its Personally Controlled Electronic Health Records system (PCEHR) in July 2012, citizens needed to voluntarily enroll to participate. Given the lack-luster enrollment to date – 1.4 million users by February 2014 – the government is now considering changing the system to an opt-out model.

Late last year Parliament tasked a panel of healthcare and IT experts to review the PCEHR in terms of implementation and uptake. The panel focused primarily on elements that would support realizing the benefits sooner, improve the value proposition for users, encourage stakeholders in the private sector to also "invest and embrace" the system, improve governance so the functions better align with target users' needs, and help minimize ongoing costs to develop and maintain the system.

The panel's report identified such key concerns as the "challenges associated with the registration process linked to the opt-in nature of PCEHR, the limited amount of clinically usable information, inadequate governance arrangements, and the usability of the system," according to Minister of Health Peter Dutton. The report included 38 recommendations, the most notable of which included:

- Transitioning to an opt-out model beginning January 1, 2015
- Renaming the system to My Health Record (MyHR)
- Ensuring compliance with e-health standards and privacy laws
- Conducting a campaign to educate users

There was no mention of incentives in the report; however, Australian Medical Association Vice President Geoff Dobbs told the Melbourne *Herald Sun* that the government must provide a monetary incentive if it wants doctors to spend the time putting patient clinical summaries into the system.

PRIVACY

Google Must Honor "Right to Be Forgotten" in EU

If you live in the European Union, you may be able to rewrite history after all.

The European Court of Justice, the highest court in the European Union, ruled in June that European users should have the right to be forgotten on the Internet. It decided there are certain cases in which Google and other Internet entities should help online users to be "forgotten" after a certain time by erasing links to web pages referencing them "unless there are particular reasons, such as the role played by the data subject in public life, justifying a preponderant interest of the public." Thus, Google and other Internet companies could be "obliged to remove web pages" even if the original "publication in itself on those pages is lawful" should a European user so petition.

If the provider doesn't grant a user's direct request to remove the link to the offending information, the user can take the matter to the appropriate authorities to force the removal, under certain conditions, at the Internet company's expense. The officials will determine how the removal of links could affect the "legitimate interest of Internet users potentially interested in having access to that information" and the individual's fundamental rights to privacy and to protection of personal data. The decision depends on the "nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life," observed the court.

That means, ultimately, that Google and other companies will need to become more actively involved in refereeing complaints from users about information carried online, reported the *New York Times*; they will no longer operate as a single, worldwide forum for people's information.

"This sounds like a landmark judgment," said Peter Hustinx, a top European Union official for data protection. "The court is saying that Google isn't just selling adverts in Europe, but is providing content along with those services. If you are a regular citizen, it gives you a remedy anywhere in Europe for you to ask companies to take down content connected to you."

The court's judgment came as a surprise to Google and many others because it differed so dramatically from a preliminary ruling by the court last June that seemed to let Google off the hook for removing links. Google stated that the court's final decision was "a disappointing ruling for search engines and online publishers in general," and that it would take time to analyze the implications.

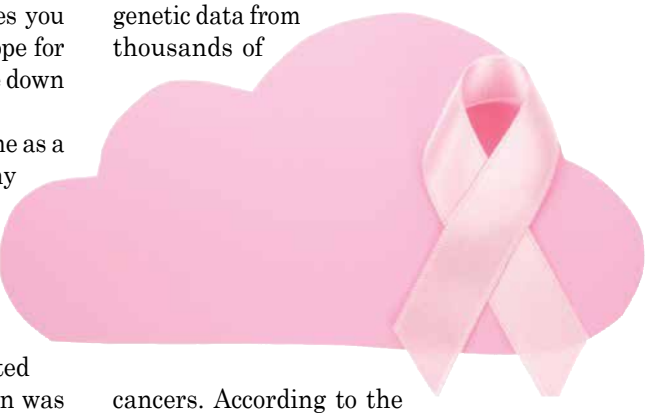
In the meantime, we are left to ponder some of the wider implications of this ruling. For instance, how will it affect efforts to create a global privacy policy, particularly since such a requirement would clash with the First Amendment in the United States?

CLOUD

Cloud Facility Created for Cancer Research

The Natural Sciences and Engineering Research Council (NSERC) of Canada recently announced that it is banding together with Genome Canada, the Canada Foundation for Innovation, and the Canadian Institutes of Health Research to build a cloud-computing facility for processing vast amounts of data to help find cures for cancer. The Canadian government will provide $7.3 million ($6.7 million U.S.) to fund the project through the NSERC's Discovery Frontiers program, and the University of Chicago is committing an additional $500,000 (about $460,000 U.S.).

The cloud facility is at the heart of the new project, which will develop powerful new computing tools so researchers can analyze genetic data from thousands of cancers. According to the NSERC, the new data mining tools are expected to be ready for beta testing in 2015 and opened to the broader research community in 2016.



"The ability to manage and analyze large volumes of data is transforming how we do research and opening new opportunities across a broad range of fields," noted Janet Walden, chief operating officer of NSERC.

INFO SECURITY

Security: The Next Frontier for Outsourcing?

Look for this year to mark the start of a new era in information security – the era of outsourcing security. So advises CounterTack's CTO Michael Davis in *InformationWeek Reports* summary of the 2014 Strategic Security Survey.

Managing the complexity of security remains the top challenge facing the 536 respondents (all from companies with 100 or more employees) to the annual survey. The main culprit is the personal device. According to the survey report, 58% of the respondents see an infected personal device connecting to the corporate network as a top security concern, even more so than phishing and lost devices. Almost as many (56%) say cyber-criminals pose the greatest threat to their organizations this year, followed by authorized users and employees (49%).

Perhaps most discouraging is the fact that 75% of the responding organizations are as vulnerable or more so to malicious code attacks and security breaches than they were a year ago. The reasons: the threats are more sophisticated (77%), there are more ways than ever to attack a corporate network (66%), and there are budget constraints (40%). Despite the increasing complexity and avenues for threats, companies are spending only 1% to 5% on security – the same amount as Gartner reported in 2010, Davis pointed out.

"Look behind the numbers and it becomes clear the issue isn't just, or even mostly, about technology," Davis said. "It's about a lack of people to execute." He added that most business executives realize they must do something about security, but that awareness doesn't necessarily translate into a bigger budget for the chief information security officer. It still comes down to measuring the value of security investments. Even with record-setting breaches, most organizations still measure the value of their security investments by whether they pass a third-party audit, the report revealed.

These increasing security challenges combined with a shortage of skilled security professionals make it understandable why outsourcing to multiple security services providers (MSSPs) is gaining the attention of business executives. The 2014 IT Budget Outlook Survey found that half of the respondents outsource 20% or more of their IT operations, and 28% outsource 40% or more. "And plenty of large trusted technology vendors are in the MSSP business, so get used to the idea being on the table," advised Davis.

PRIVACY

Getting Tough on Health Records Privacy

The Saskatchewan government is taking steps to protect patient health information when files are abandoned and from snooping in general. The steps, according to *GlobalPost*, include making it a specific offense when a worker unnecessarily accesses a person's health records and requiring providers to show they are trying to prevent records from being abandoned.

Explained Health Minister Dustin Duncan: "Prosecutors have not been able to pursue charges because the way the legislation currently stands, we have to prove that there was an intent and that's very difficult to prove....This will require that the trustees ... demonstrate the steps that they took to prevent the documents from being released."

The changes reportedly come at the urging of former Privacy Commissioner Gary Dickson, who called for tougher laws in 2010 following a case in which a pharmacist used his home computer to access a former patient's drug record out of personal interest. An additional influence, perhaps, was the discovery of thousands of medical records in the garbage behind a shopping mall in 2011.

"Our focus isn't just about charging people. This is obviously about protecting records," said Duncan. "But when there is a clear violation of the legislation, I think that this will provide us the ability to take the appropriate steps."

He said the changes could go into effect this fall.

New!

Gain the Competitive Edge Your Business Needs

Managing Active Business Records

This book (and PDF) explores records management concepts, principles, processes, and considerations for developing, implementing, and maintaining effective active file systems for paper- and electronic-based records. Equal treatment of all records, regardless of format, strengthens a company's legal position and allows ends users to make sound business decisions based on complete, accurate, timely, and up-to-date information. A well-designed and maintained file system (classification / taxonomy) contributes significantly to a company, sustaining a competitive edge.

Softcover **$60.00** Professional Members: **$40.00**
PDF **$55.00** Professional Members: **$35.00**

Order your copy online today!

ARMA INTERNATIONAL BOOKSTORE

www.arma.org/bookstore

MOBILE DEVICES

NARA Explores Effect of Mobile Devices on Records Management

The National Archives and Records Administration (NARA) is warning agencies about the implications of mobile devices for records management. Beth Cron, a policy analyst at NARA, opened discussion about the mobile challenge on NARA's blog, *Records Express*.

"When employees use devices without following agency policies or lack mobile device management tools, they open themselves and their agencies up to information, transmission, and operational security risks," wrote Cron. Those risks include lost or stolen devices containing federal records and legal issues related to e-discovery. From a records management perspective, the challenges include:

- Identification of records when content may be located in multiple places
- Capture of complete records in a manner that ensures their authenticity and availability when records frequently change and are located in many places
- Data being stored or replicated on the device or in an application instead of only being accessible from a central repository
- Development and implementation of records schedules, including the ability to transfer and permanently delete records, apply legal holds, or perform other records management functions when it is unclear where records reside
- Sources and formats of records will continue to change and it may be difficult for agency records management policies, processes, and technology to keep up

One of the first things agencies can do, Cron said, is recognize that employees have records management responsibilities when working on a mobile device. Second, they can look for best practices emerging in the federal community regarding mobile devices; some may be useful to records management as well. Third, agencies may consider establishing mobility policies.

CYBERSECURITY

SEC Tackles Cybersecurity

The Securities and Exchange Commission (SEC) is making cybersecurity a priority in 2014. It recently announced it will examine more than 50 registered broker-dealers and registered investment advisers to determine their cybersecurity preparedness. The agency will focus on cybersecurity governance, identification and assessment of cybersecurity risks, protection of networks and information, risks associated with remote customer access and funds transfer requests, risks associated with vendors and other third parties, detection of unauthorized activity, and experiences with certain cybersecurity threats.

Firms will be asked to provide copies of various policies and plans, including written information security policies, business continuity of operations plans, cybersecurity incident response policies, procedures for verifying authenticity of e-mail requests seeking transfer of customer funds, policies for addressing responsibility for losses associated with attacks or intrusions, cybersecurity risk assessment questionnaires, and sensitive data segregation policies. The SEC will also be checking that firms have established reasonable retention periods and have a comprehensive data destruction policy.

A sample cybersecurity document request is available on the SEC's website.

COPYRIGHT

U.S. Supreme Court Wrestles with Outdated Copyright Laws

A copyright case in front of the U.S. Supreme Court illustrates just how out of date some copyright laws are, especially given the advent of the cloud. Broadcasters contend that Aereo, a 2-year-old company that retransmits over-the-air-broadcast television to its paying customers using thousands of dime-sized antennas, is violating U.S. copyright law because it doesn't have the broadcasters' permission to do that.

According to an *Ars Technica* article, companies such as Microsoft, Google, Mozilla, Yahoo, and others, fear a decision in favor of the broadcasters "would threaten one of the most important and emerging industries in the U.S. economy: cloud computing."

Under current law, Aereo is free to retransmit broadcast signals without paying licensing fees, something cable companies can't even do. A federal appeals court likened the company's approach to providing three devices: a standard TV antenna, a DVR, and a Slingbox. The broadcasters counter that it's a copyright breach because Aereo hasn't paid fees to retransmit their content. They say it amounts to a "public performance," which would require the broadcasters' consent. As for endangering cloud services, the broadcasters think that likening Aereo to services like Dropbox and Google Drive is far-fetched.

"There is an obvious difference between a service that merely stores and provides an individual user access to copies of copyrighted content that the user already has legally obtained, and a service that offers the copyrighted content itself to the public at large," the broadcasters said in their brief.

The justices heard oral arguments on April 22. It's hard to predict what the final decision will be, but it does appear that the justices are leaning toward a decision that would not damage other companies.

INFO SECURITY

EU Makes Headway on E-signatures

It has taken more than 13 years to do it, but the European Union has finally introduced a cohesive electronic signature law that its 28 member states can support. The EU hopes to have an e-signature regulation in place by July, according to *Law Technology News*. The new law would be comparable to the U.S. e-signature law.

The legal groundwork for a cross-border e-signature law was established by a directive issued in 1999. Member countries were required to adopt the directive by 2001. However, each country adopted its own interpretation of the directive and there was a lack of interest from the commercial sector in adopting the model, according to Hugh Logue, a senior analyst at Outsell Inc., in an interview with *Law Technology News*. The new European regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, which was adopted in April and is now awaiting the final endorsement of the Council of Ministers in June, will remedy that situation.

Part of the reason the U.S. was able to more easily adapt to the e-signature landscape is because of its shared legal system, said Logue.

E-DISCOVERY

Comments Prompt More Changes to FRCP

The Committee on Rules and Practice and Procedure (the Standing Committee) has approved the changes to the Federal Rules of Civil Procedure (FRCP) proposed by the Advisory Committee on Civil Rules (Rules Committee).

The Rules Committee approved the proposed changes to FRCP during a public hearing in April. According to *Bloomberg BNA's* report on the meeting, the final changes were heavily influenced by the public hearings and more than 2,000 written comments it received regarding proposed changes to the rules governing electronic discovery.

One of the sections that drew the most fire was 37(e), which concerns the failure to preserve electronically stored information (ESI). Rules Committee member Judge Paul Grimm, of the District of Maryland, said commenters raised serious questions about whether the framework and approach of Rule 37 adequately addressed issues of duty to preserve and remedial and punitive measures. According to U.S. Judge David Campbell, chairman of the Rules Committee, the new phrasing is intended to reject the concept of strict liability because the most you can ask of people is reasonable conduct.

Members of the Standing Committee closely scrutinized this section, according to *Law Technology News (LTN)*, because the proposed changes differed so much from the original proposal. Campbell led the in-depth discussion, which included fielding several difficult hypothetical situations testing the application of the rule.

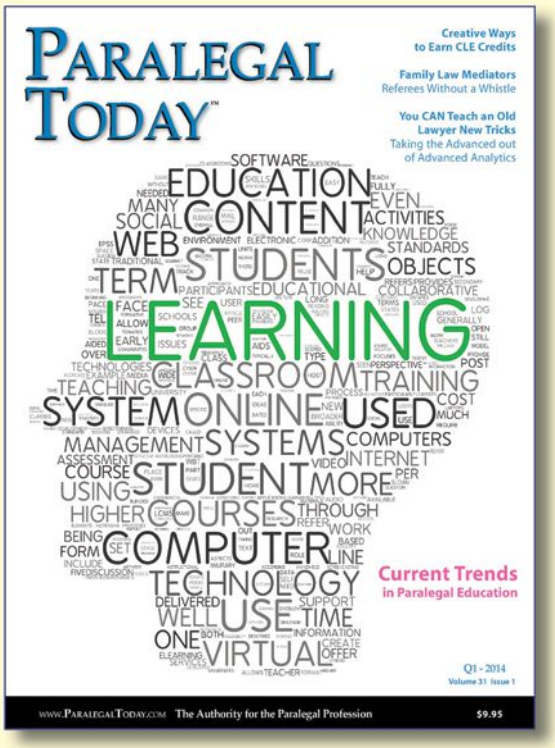
Another area of controversy was Rule 26, dealing with proportionality and discovery scope. After extensive discussion, the Rules Committee amended the rule to require that discovery be proportional to the needs of the case. Specifically, "Unless otherwise limited by court order the scope of discovery is as follows (italics denote revision):

> *Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.*

LTN also noted that the Standing Committee approved the explicit acknowledgement of the courts' and parties' responsibility to ensure a "just, speedy, and inexpensive determination of every action" by the proposed changes to this text. The committee also acknowledged in its Committee Note the role of cooperation in the effort and the need to clarify that there is no intention to create a right to sanctions for failures to cooperate.

The next step will be a review by the Judiciary Conference. From there, the amendments would proceed to the Supreme Court, which will be asked to review and vote on whether to send them to Congress. If all goes smoothly and Congress stamps its approval before May 2015, the new rules will go into effect December 1, 2015.

Members of ARMA get a special discount on subscriptions to Paralegal Today magazine!



For over 30 years ***Paralegal Today*** has been providing paralegals and legal assistants with the information they need to perform their jobs better. The ideas, techniques and insights you get from every issue will improve your skills, enhance your performance and help to make you an essential member of your firm or organization. This well-rounded, leading independent magazine brings you useful, pertinent information, including best practices, special reports, surveys, technology tips, association updates and much more to help you stay sharp and advance in your career.

Your subscription to ***Paralegal Today*** includes **BOTH** the **print** edition and the **digital online edition** that you can read on you iPad, iPhone or other digital device. You also enjoy a robust Web Site with a helpful "Listserv" group, a job bank, and other great features.

Save 27% or 38% off the newsstand price!

Member Discount Rates (USA Only)

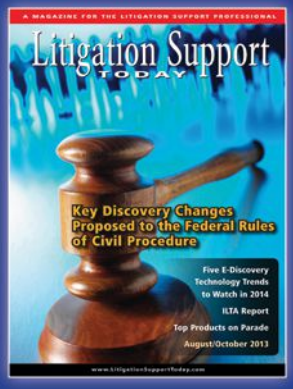
Order Code: X4ARMA2	Newsstand Rate	Your Discount	Your Net Cost
1 Year, 4 Issues	$39.80	27%	$29
2 Years, 8 Issues	$79.60	38%	$49

TO GET YOUR ARMA DISCOUNT USE THIS ORDER CODE: X4ARMA2

Your subscription to Paralegal Today includes BOTH the print edition and the digital edition!

Get a FREE digital subscription to *Litigation Support Today!*

As a Records Management Professional you qualify for a FREE digital subscription to our sister publication, *Litigation Support Today*, the No. 1 magazine serving the information needs of the litigation support profession. Simply go to www.litigationsupporttoday.com and complete the subscription request form.



IT'S EASY TO ORDER

- **ONLINE.** Go to www.paralegaltoday.com. Click Subscribe, **Enter your special Order Code.** Click "Order Subscription."
- **CALL TOLL FREE: 877 202-5196** and mention your special Order Code.

SUBSCRIBE OR RENEW TODAY!

PARALEGAL TODAY™

The Authority for the Paralegal Profession

A Publication of Conexion International Media, Inc.

E-DISCOVERY

When Is Social Media Discoverable?

If you want access to a party's social media accounts, you must show good reason. The fact that a plaintiff has a social media account doesn't automatically mean it's discoverable, according to a New York appellate court's recent ruling. In the case *Pecile v. Titan Capital Group*, the defendants requested access to the plaintiff's social media because the information could contradict the plaintiff's claim of emotional distress. The court denied the request, stating the defendants had not offered a proper basis for the disclosure. In other words, the existence of the social media account wasn't enough to order production.

That doesn't mean a plaintiff's social networking site is not discoverable, though. "Courts will order production of information on social networking sites, even information that is not publicly accessible, so long as there is a factual basis for requesting such information," clarified attorney Michael A. Frankel in a recent posting on Jackson Lewis's *E-Discovery Law Today* site. "For example, a court may require production of relevant information on social networking sites if the defendant, through written discovery or depositions, has identified information that contradicts the plaintiff's alleged claims or damages."

Even if no relevant information appears on the public portion of a plaintiff's social networking sites, Frankel advises defendants to at least request confirmation that the other party's counsel has reviewed and produced all relevant information on the sites. A New York District Court supported that approach in *Giacchetto v. Patchogue-Medford Union Free Sch. Dist.*

CYBERSECURITY

Shareholders Sue Corporate Boards over Cybersecurity Breach

Corporate board members take heed: you could be held accountable by your shareholders for cybersecurity breaches. Just ask the boards of Wyndham Worldwide and Target.

In May it became public that a shareholder is suing Wyndham Worldwide board directors and officers for failing "to take reasonable steps to maintain their customers' personal and financial information in a secure manner" after the company experienced three data breaches between April 2008 and January 10. The company is already under fire from the Federal Trade Commission regarding the incidents. (See "Wyndham Stands Up to the FTC," in the Up Front section of the November/December 2013 issue of *Information Management*.)

In his filing, the shareholder called out the board for failing to ensure that Wyndham had "implemented adequate information security policies and procedures (such as by employing firewalls)" prior to connecting networks. He also chastised the board for allowing the company to use an operating system so woefully out of date that the vendor stopped providing security updates three years prior to the breaches. Further, there was the lack of timely notification to those customers potentially affected by the intrusions; the stockholder cited the board for waiting two and a half years after the third incident to disclose the breaches in the company's financial filings.

Target's board has also been named in lawsuits filed by shareholders for the massive data breach the company experienced last year. Attorney Kevin LaCroix, publisher of *The D&O Diary* blog, reported that two shareholder claims filed in January accused the board of shirking its fiduciary duty and wasting corporate assets, among other things. Both suits allege the company "failed to take reasonable steps to maintain its customers' personal and financial information" and to "implement any internal controls at Target designed to detect and prevent such a data breach." They also raise the issue of the lack of timely notification.

"These allegations highlight the fact that shareholders may seek to hold company officials responsible for the failure to prevent the breach but also for the way that the company conducts itself as it responds to the breach," LaCroix noted.

These lawsuits aren't the first of their kind, but they may have drawn the most public attention. They are significant, said LaCroix, if for no other reason than that they show how a data breach can lead directly to a [directors and officers insurance] claim."

Survey: Information Governance Not Being Embraced

Most businesses have not yet seen the light regarding the importance of information governance (IG) despite increasing public attention to data breaches and information leaks. A recent study from AIIM determined that only 8% of organizations have IG programs in place and working. One-third of organizations reported they have undertaken or are planning to undertake IG projects, but the policies are not being referenced or enforced.

IG best practice ensures that the policy addresses *all* content, whether it is being stored, accessed, or transferred among servers, websites, users, or mobile devices. In reality, few if any IG programs in place today meet that standard.

"It seems that many organizations are more prepared to accept the consequences of non-compliance with information governance rules than to implement and mandate improved policies," observed Doug Miles, head of AIIM's Market Intelligence Division and the author of the survey report "Automating Information Governance – Assuring Compliance." He noted that 52% of the respondents reported they have had issues of non-compliance during the last two years. Nearly one-quarter (24%) overall – 31% of larger organizations – have had external litigation and discovery issues.

There is a variety of reasons for this state of affairs, to be sure. Creating a comprehensive IG program is not an easy undertaking. The biggest obstacles typically reported are getting executive support and getting the right people at the table (40%). Once a program is in place, adherence becomes an issue largely due to a lack of training. Only 40% of organizations allocate any time at all to IG training, and only 12% regularly train staff. A scant 4% hold specific update sessions for senior management.

Information Governance in Healthcare

A new study by the American Health Information Management Association (AHIMA) reported similar findings specifically within the healthcare industry. Given ongoing reports of personal health records being found in dumpsters and such, it comes as no surprise to learn that only 11% of healthcare organizations have mature IG programs in place. Further, only 17% said their organizations have mature policies and procedures. More than one-third (35%) said they didn't know if their organization had IG efforts underway or if they even see the need for it. Another 22% see the need for IG but haven't initiated a program.

"In healthcare for a while now we've been focusing on health data mostly, and what we're trying to share with you is our perspective on how information governance is really the umbrella over all information within the healthcare organization, not just the data that are captured in the electronic or paper record," AHIMA Vice President for Public Policy Meryl Bloomrosen said while speaking at the eHealth Summit, hosted by the Centers for Medicare and Medicaid in May. "If you think through the types of information that are collected – personnel files, HR files, health record files, purchasing data, employment data, suppliers, providers, financing – all of this needs to be governed."

AHIMA conducted the survey in partnership with Cohasset Associates as part of the association's efforts to help professionals in the health industry better understand what IG is and why it is critical.

INFO SECURITY

FTC Must Disclose Its Data Security Standards

The Federal Trade Commission's (FTC) chief administrative law judge ruled earlier this month that the agency can be compelled to disclose the data security standards it uses "to pursue enforcement action against companies that suffer data breaches."

The decision was issued in response to a motion filed by LabMD, a medical laboratory the FTC charged with unfair trade practices for exposing sensitive information belonging to 10,000 patients in 2010, reported *Computerworld*.

LabMD, which is now defunct, accused the FTC of holding it to security standards that didn't officially exist at the federal level – hence, the motion to require the FTC to disclose the standards it uses to determine if a company has reasonable security measures in place. The judge agreed, ruling that the FTC's Bureau of Consumer Protection "shall provide deposition testimony as to what data security standards, if any, have been published by the FTC or the Bureau upon which [it] intends to rely on at trial."

Several business groups, including the Chamber of Commerce, TechFreedom, and the National Federation of Independent Businesses, filed motions in support of LabMD. They have accused the FTC of overstepping its authority by forcing costly fines and settlements on companies that have suffered data breaches. LabMD is the second company to challenge the FTC's authority in court. Wyndham Hotels is the other.

INFO SECURITY

'Security by Design' Time Has Come

The ramifications of a security breach can be significant and far-reaching. First, there's the financial impact. According to the "2014 Cost of Data Breach Study: Global Analysis" conducted by Ponemon Research Institute, the average cost paid for each lost or stolen record containing sensitive and confidential information is $145 ($195 and $201, respectively, in German and U.S. organizations).

Then, there's the hit to the breached company's public image as thousands and even millions of consumers lose their confidence in the company as they deal with the aftermath of having their personal information stolen. It may even cost high-level executives their jobs, as in the case of Target's CEO.

Adam Levin, a frequent *Forbes* contributor, recently suggested that companies change the way they do security, using the "Privacy by Design" approach originally pitched in the 1990s by Ontario's information and privacy commissioner at that time, Ann Cavoukian. Central to this approach is that it makes good business sense for consumer privacy to be sewn into the fabric of everything a company does and builds. Now it's time for "Security by Design," an idea that Levin believes Target recently started marketing.

The basic tenets of "Privacy by Design" become the foundational principles of "Security by Design," such as:

- Be proactive not reactive. The focus would be on eliminating the risks associated with storing third-party information.
- Security should be the default setting. Consumers should not have to worry about whether their information is secure when they do business with an organization.
- Security should be part of IT design and architecture and business practices.
- Privacy and security can and should co-exist.
- End-to-end security is "embedded into the system prior to the first element of information being collected and extends throughout the entire lifecycle of the data involved, from start to finish."
- Unlike "Privacy by Design," "Security by Design" requires invisibility and opacity.
- Show respect for the customer. Architects and operators must "keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options."

SOCIAL MEDIA

Social Media Misconduct in the Office Is Rising

The misuse of social media among employees is skyrocketing, according to the 2014 global survey on social media in the workplace conducted by the international legal group Proskauer Rose LLP. In fact, 70% of businesses reported taking disciplinary action against social media misuse in the office. That's not so surprising given that 90% of companies now use social media for business purposes. After all, the more that people use social media for business, the more likely the fine line between personal use and business use will blur, noted the researchers.

The good news is that nearly 80% of companies today have social media policies in place, a significant increase over 60% reported last year. More than half of those businesses have also updated their policies within the last year. In addition, most of these organizations are now taking precautions to protect against specific risks associated with the misuse of social media, such as:

- Misuse of confidential information (80%)
- Misrepresenting the company's views (71%)
- Inappropriate non-business use (67%)
- Disparaging remarks about the business or employees (64%)
- Harassment (64%)

In many cases, the policy is to restrict employees' use of social media in the office. More than a third (36%) of employers actively block access to such sites, compared to 29% last year; 43% allow all employees to access social media sites today, a 10% decrease from last year. An area that still isn't getting enough attention, however, is employee training. Only about 38% of businesses train their employees on the appropriate use of social media, a slight increase from last year's 33%.

Proskauer noted that there are no actual laws specifically addressing the issue of monitoring social media usage, although the National Labor Relations Act plays a pivotal role in this issue in the United States. Consequently, the common approach to this issue is to apply general legal principles, especially drawing analogies from case law pertaining to other technologies (such as e-mail).

"In most [countries], the approach of the courts is to seek to balance, often on a case-by-case basis, an employer's right to demand that employees attend to their work with the employee's right to maintain personal privacy. Where data protection laws exist, such regulations limit the scope and methodology of collection and the eventual usage of information gathered by an employer's social media surveillance," the group stated in the survey report.

Proskauer offered the following tips to businesses based on its research and experience:

- Conduct annual audits to ensure your practices and policies comply with the developing legal requirements.
- Make training a priority.
- Identify specific risks, such as those mentioned earlier and ensure that other policies dealing with these matters expressly refer to social media.
- Implement clear guidelines so those individuals who use social media for work purposes know the boundaries.
- Don't forget ex-employees; implement explicit provisions that prevent the misuse of social media by ex-employees.

This is the third yearly release of the survey, which included responses from a broad range of businesses, many with a global presence. The countries represented were Argentina, Brazil, Canada, China, Denmark, France, Germany, Hong Kong, India, Ireland, Italy, Japan, Spain, The Netherlands, the United Kingdom, and the United States.

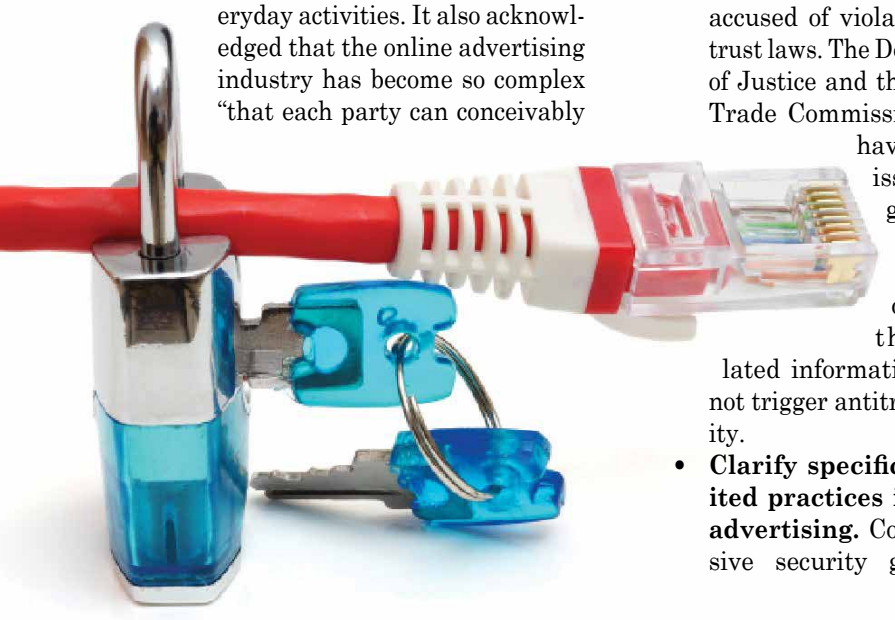
INFO SECURITY

U.S. Congress Expected to Move on Data Protection

Thanks to high-profile data breaches such as that experienced by Target last year, the U.S. legislature may finally be ready to address data protection. Department of Homeland Security Secretary Jeh Johnson recently told attendees at the Reuters Cybersecurity Summit that members of Congress are expected to move forward on bipartisan cybersecurity legislation this summer, according to *SecurityInfoWatch.com* (SIW).

About the same time, the Senate Permanent Subcommittee on Investigations released the report "Online Advertising and Hidden Hazards to Consumer Security and Data Privacy," in which it urged some leading high-tech companies to do more to protect consumers from hackers who use online advertisements to infect computers. It cited examples in which Google, Yahoo, and YouTube were exploited to infect visitors' computers without the companies' knowledge.

The subcommittee observed in its report that consumers risk being exposed to malware in their everyday activities. It also acknowledged that the online advertising industry has become so complex "that each party can conceivably claim it is not responsible when malware is delivered to a user's computer through an advertisement."



Ultimately, the subcommittee stated four basic recommendations:

- **Establish better practices and clearer rules.** Consumers need to keep their operating systems updated and carriers need to do more on their end. "If sophisticated commercial entities do not take steps to further protect consumers, regulatory or legislative change may be needed so that such entities are incentivized to increase security for advertisements run though their systems."
- **Strengthen security information exchanges within the online advertising industry.** According to the report, some online advertising companies claim they don't share information about security hazards with their competitors for fear they would be accused of violating antitrust laws. The Department of Justice and the Federal Trade Commission (FTC) have already issued joint guidance that the sharing of cyber threat-related information would not trigger antitrust liability.
- **Clarify specific prohibited practices in online advertising.** Comprehensive security guidelines should be developed by self-regulatory bodies or, if necessary, the FTC. "Greater specificity in prohibited or discouraged practices is needed before the overall security situation in the online advertising industry can improve."
- **Develop additional "circuit breakers" to protect consumers.** Online advertising systems should introduce "check points" that will help stop malicious advertisements earlier. The subcommittee also urged online advertisers to thoroughly vet new advertisers and periodically check to ensure that advertisements are legitimate.

There are advantages to a uniform federal law on data security, noted Maureen Ohlhausen, an FTC commissioner, during a recent conference on "The Future of Privacy and Data Security Regulation" at George Mason University's School of Law. Among other things, it would supersede varying state laws on the issue, providing a single, uniform statute.

Even if Congress provides guidance on how to protect consumers and their privacy, it falls to the companies to carry through.

"The reality is that all compliance (frameworks), whether they are industry compliance requirements, federal, or even international requirements, all of these are baseline standards and you have to think of compliance as the basement of where your security starts," said Randall Gamby, information security officer at the Medicaid Information Service Center of New York, in an earlier SIW interview.

COPYRIGHT

Copyright Alert System in Full Swing

Internet service providers (ISPs) sent out more than 1.3 million copyright infringement alerts during the first 10 months of the new U.S. Copyright Alert System (CAS), which launched in February 2013. AT&T, Comcast, Time Warner Cable, and Verizon sent the notices as part of the new "six strikes" alert system. The alerts graduate from a warning to "final mitigation," which could include bandwidth throttling, site restriction, or educational classes, depending on the ISP, reported *Forbes*.

The Center for Copyright Information (CCI) administers the program, which was a voluntary initiative launched by CCI and its member ISPs, entertainment community representatives, and the Consumer Advisory Board. It aims to reduce copyright infringement over peer-to-peer (P2P) networks.

"It is built simultaneously to encourage consumers to embrace the growing number of affordable licensed sources of films, music, and television programming content available online from a variety of different services and in many different formats," the CCI stated in its phase one report released in May.

During this first phase, CCI sent more than 2 million notices of alleged copyright infringement to the ISPs, which then sent 1.3 million alerts over the course of the next 10 months to 722,820 account holders. More than 70% of the alerts fell into the educational category, and 8% were mitigation alerts, only 3% of which were at the final mitigation level.

ISPs have a certain degree of discretion in how they execute the program, but all must:

- Maintain user privacy by not including personally identifiable information back to the content owners or vendors
- Include in the alert information about the alleged infringement and where to find legal sources of the content
- Offer to help consumers avoid future allegations of infringement by securing their wireless routers and home networks and removing unwanted P2P software
- Provide links to the CCI and other sites that help users find authorized copyrighted content
- Offer a streamlined linkable process for customers to request a review of the allegations by the American Arbitration Association if they believe the alerts were sent in error

"The CAS is still in its early stages, especially given that it is a first-of-its-kind program in the U.S. – however, the data that we have been able to review from the first ten months of 'ramp up' activity is encouraging, " concluded the CCI. **END**

Top IG Tech Trends: Auto-

Gordon E.J. Hoke, IGP, CRM

Classification & Big Data

Information governance (IG) is an emerging practice in several disciplines. Law, records and information management (RIM), information technology (IT), and others define it from their own perspectives. For example, some attorneys equate IG with defensible disposal, while some technologists see it as a storage or architecture issue.

April's Executive Conference on Information Governance, co-presented by ARMA International and The Sedona Conference® (TSC) and attended by more than 100 people from at least a half-dozen disciplines, did not seek or achieve a consensus definition, but the shared perspectives did encourage a cross-fertilization of ideas.

ARMA International defines IG as:

> A strategic framework composed of standards, processes, roles, and metrics that hold organizations and individuals accountable to create, organize, secure, maintain, use, and dispose of information in ways that align and contribute to the organization's goals.

This definition suggests IG is actionable – a strategy for accomplishing goals. In contrast, TSC's definition takes a descriptive approach:

> An organization's coordinated, inter-disciplinary approach to satisfying information compliance requirements and managing information risks while optimizing information value. As such, Information Governance encompasses and reconciles the various legal and compliance requirements and risks addressed by different information-focused disciplines, such as RIM, privacy, information security, and e-discovery.

The differences need to be acknowledged. Full benefit from IG requires an appreciation of both the descriptive qualities and the functional contributions. For example, TSC emphasizes risks twice while risk is only implicit in ARMA's definition. In contrast to TSC, ARMA emphasizes comprehensive precision. Until consensus emerges, practitioners will benefit from applying both definitions and keeping in mind the perspectives of others.

IG Stakeholders

The varied definitions notwithstanding, consensus was alive and well at the executive conference. For example, no voice contested the supposition that success in any IG initiative requires a strong executive champion. Further consensus ascribed IG success to overcoming the separation or isolation of such departmental stakeholders as IT, finance, RIM, legal, research and development, accounting, sales, human resources, procurement, and others. In many organizations, these departments function as what conference presenters termed "silos."

IG offers value: each functional area stands to benefit from harvesting synergies. Better coordination leads to less redundancy with better operations and compliance. Leaders from these areas (siloed or integrated) are stakeholders in IG. They stand to benefit from ending departmental insulation. Indeed, the task of the IG professional is to facilitate and enable cooperation. According to one session leader, the silo effect may be emotional as well as operational; another conference presenter invoked "organizational psychology" as a useful tool for IG.

IG Technology Challenges

For successful IG, participants must be able to share information. Their information systems need interoperability or, minimally, communication links. Further, technology should enhance operational efficiencies and

The first **Executive Conference on Information Governance** convened in April on Amelia Island, Florida. Presented jointly by ARMA International and The Sedona Conference® (TSC), the event featured plenary sessions with multiple presenters.

Guidelines for presenters and responders required "dialogue, not debate," a motif common to TSC meetings. Leaders encouraged attendees to comment on the conference in social media and more traditional forums, and many posted on Twitter. In the interest of free expression and exchange, however, conference guidelines required that no direct quotes appear and ideas not be attributed to an identifiable individual.

This report respects those requests and focuses on technological facets of information governance that surfaced at the conference. Definitions and parameters are presented for context.

The adoption of auto-classification appears to be more a matter of timing, cost, and tools rather than whether it will become a norm.

facilitate synergies. Clearly, an executive champion, council of stakeholders, and departmental implementers are essential, but unless technology plays a robust role, only limited IG progress will accrue from policies, procedures, and practices.

An information architecture can either help or frustrate IG efforts, but no single information model is ideal. Centralized or distributed servers may suffice, although the derivative issues vary. IG can thrive inside a tight firewall or by employing a public cloud; these are questions of style, not adequacy. In any situation, an enabling architecture facilitates IG stakeholders' collaboration.

There are hardware considerations as well. Some vendors' IG tools require a huge number of information processing cycles. Many require increased network bandwidth. Distributed architectures require high-speed communication. Organizations considering IG-enabling software may find themselves looking at estimable hardware purchases. Hosted solutions may mitigate this need.

Similarly, systems and applications play a key role. Legacy databases may resist IG. Migrating old systems to archives or newer, full-featured systems is costly and may risk the integrity of data and metadata.

E-mail used as a records repository is problematic for many organizations. SharePoint is another common conundrum: relatively few organizations govern it comprehensively, and records management is not the platform's forte.

IG Technology Trends

A half-dozen vendors and consultants at the executive conference offered professional solutions that are on the market and need evaluation for individual organizational needs.

Perhaps the good news for the technical side of IG is that the field is immature, meaning that the vendors have varied approaches. This lack of standardization suggests that any inquiring IT group may well find an approach that is compatible with its unique needs.

Within this context, two technology trends dominated presentations and conversation at the event. One, auto-classification, comes under many names – some related to its use. The other major trend, appearing under the umbrella of big data, depends on the efficacy of auto-classification.

Auto-classification

Synonyms or near-synonyms of auto-classification include automated e-discovery, predictive coding, content analysis (or analytics), and computer-assisted review. The software products sold with these names are tuned to somewhat different functions. Their approaches differ and certainly their underlying algorithms are distinct. Their commonality: they use machines to make valuable information more accessible and useful, and under most conditions they do it more quickly and accurately than humans.

In RIM, auto-classification arose in the last decade. Practitioners knew that some human record owners were neither quick nor accurate in declaring information as records and assigning them to records series with disposal dates. Some (at the time) brazen software developers suggested that their algorithms could declare records better than human workers could.

As early as 2007, software developers pointed out that a human that could assign 90% of appropriate records to the right record series 90% of the time had roughly the same success rate as a computer that could consider and assign the right series to *all* records 80% of the time. Because the machine was faster, though, they gave the advantage to the computer.

Over the intervening years, algorithms improved, processing speeds rose, and developers touted computer classification accuracy in the 90% range. Commensurately, the amount of captured information and records rose precipitously, to the point where humans could not expect to keep up without automation. This same phenomenon led to big data, which is discussed below.

In the legal arena, emerging case law and amendments to the Federal Rules of Civil Procedure gave parameters for court-admissible electronic information. This admissibility expanded the scope and the significance of electronically stored information. Manual inspection of large numbers of electronic records by high-priced law firm staffs raised the stakes. The software that could quickly analyze digital records – which previously was too expensive – became cost-effective. A new industry arose around legal search, e-discovery, and computer-assisted review.

A related technology that developed simultaneously was content analytics. This technology moved beyond using metadata and keyword search tools to identify and classify records; content analytics can actually recognize the *meaning* contained in text.

Language is highly complex, and for machines to rec-

ognize and flag relevant text based on its meaning, there must be sophistication in software and power in hardware. Consider two e-mail messages. The first says:

> *Dear Bill,*
> *You and Sue are invited to a barbecue on our new patio Saturday. The contractor did a great job.*

The second says:

> *Dear contractor:*
> *The work you did was terrible and your bill is invalid. I may sue you for damage you did.*

Some of the words are the same, but the meanings are very different. For a machine to recognize the difference, it needs profound algorithms that go beyond the dictionary definitions of the words, extracting meaning from the context and syntax – that is, the way the words are used.

Auto-classification and its variations have improved significantly in the last several years, and forthcoming versions should be even better.

Regarding auto-classification, executive conference participants fell into these general categories:

- *True believers*, who see the new tools as the only realistic way to bring the risks of undeclared records, misapplied records series codes, and unfound records down to an acceptable level at an acceptable cost
- *Skeptics*, who fear the consequences of relying on immature technology
- *Practitioners,* who appreciate the capabilities of auto-classification but do not see a practical way to implement it due to such things as limited budgets, technical expertise, user acceptance, and staff resources

In any case, a clear trend is the continued evolution of auto-classification. In the face of ever-increasing quantities of electronic records, the adoption of auto-classification appears to be more a matter of timing, cost, and tools rather than whether it will become a norm.

Big Data

The aforementioned rapid growth of electronic information and increase in the volume of records and court-acceptable information lead to big data.

Executive conference presenters vehemently contested the common misconception that big data is just "more of the same." The amount of data available for recordkeeping has grown exponentially over the last few years, and indications are that the rate of growth will continue. Not all organizations create or use big data, but those that do soon realize that techniques for processing the onslaught of information are discontinuous with earlier ways. The management tools are different as well.

Although big data was described as early as 2001, the executive conference offered a 2013 definition from the nonprofit association ISACA: "Data sets that are too large or too fast-changing to be analyzed using traditional relational or multidimensional database techniques or conventional software tools to capture, manage, and process the data at a reasonable elapsed time."

Where does big data originate? Why is there so much of it? Despite the many potential answers, two illustrations suggest some sources:

1. *The World Wide Web and mobile applications.* Any number of website owners are intensely interested in the behavior of their site visitors. They record every mouse or keyboard click and

every screen touch. The number of data points occurring at a popular website can be enormous. Similarly, mobile applications' owners record the activity of their users. While the reasons owners collect this information vary, the volume of data amounts to exabytes.

2. *"The Internet of Things."* Tens of billions of devices have sensors or signal relays that connect to the Internet. These range from radio frequency identification (RFID) chips reporting locations or inventories to sensors along railroad tracks that recognize and report boxcar wheels with hotboxes. In a home example, refrigerators may have sensors that report to the owner's mobile device if the internal temperature rises above a set level.

Big data is significant for more than its tremendous volume. Algorithms can organize this information into meaningful, predictive patterns. For example, Amazon knows that a specific percentage of its website visitors that looks at a book will later buy it.

Amazon also knows the geographical location of the viewers. With this information, the retailer ships an appropriate number of copies of a particular title to warehouses near its viewers, even before a viewer turns into a buyer. This facilitates the quick delivery that engenders customer satisfaction.

In another example cited at the executive conference, a father learned his teenage daughter was pregnant because a retailer – predicting behavior based on web views and/or store movement – began sending direct mail advertising for baby products.

Similarly, analysis of big data can affect momentous events such as natural disasters and terrorist activity. Big data analysis enables severe weather alerts, and the U.S. National Security Administration uses big data to predict enemy strikes.

Applying ethics to big data use is only beginning. While identifying and anticipating equipment failure are straightforward, collecting and acting upon information about people present moral and legal dilemmas. The questions may fall into three categories:

1. Personal information that individuals knowingly and freely provide to data collectors (for example, during registration at a website) for a known and approved use
2. Personal information collected about individuals without their knowledge or specific permission, such as location and movements obtained through cell phones
3. Personal information individuals knowingly and freely provide to data collectors that is analyzed for additional meaning (sometimes paired with external data) and used for purposes beyond the intent of the original permissions

Each of these uses of big data carries ethical implications. The ethical codes of attorneys and records managers certainly do not extend to all big data users, and the right path may not always be clear.

The Twain Shall Meet

The Generally Accepted Recordkeeping Principles® (Principles) apply to big data. The Principles rise above volume, source, medium, speed, and other variations. Just as they provide a comprehensive governing framework for both paper records and digital images, they guide the management of information in databases and big data repositories.

While the Principles apply universally, the methods and techniques for applying them vary by the nature of the information's attributes. This is where auto-classification, predictive coding, and content analytics meet big data. Since the quantity of big data is, by definition, too large for conventional database entry and processing, powerful computers running advanced algorithms are the tools of choice for big data governance. These algorithms and related policies can apply the Principles, especially retention, availability, protection, and disposition.

In the evolution of technology, capabilities typically come first, while governance, controls, and ethics arrive later. This is the case with big data. Years ago, users began exploiting big data, but attorneys at the executive conference reported that litigation based on big data has come to courts only recently. To prosecute, defend, and argue these cases, traditional discovery methods are impractical. Effective research requires computer-assisted review and other automated tools.

Records managers will similarly find these tools indispensable. They provide more than automatic records declaration. They can apply and release legal holds. They can protect records from unauthorized access. And of similarly vital importance, they can auto-delete records when retention periods are completed.

Looking Ahead

The executive conference received many positive evaluations, and plans are in motion for a 2015 edition. Undoubtedly IG technology and its rate of use will continue to evolve in the coming year. The functional and ethical challenges will grow as well.

Facing burgeoning volumes of information, practitioners will be hard-pressed to maintain current rates of success. Progress may well depend on leaders' ability to harvest synergies from inter-disciplinary collaboration. **END**

Gordon E.J. Hoke, IGP, CRM can be contacted at ghoke@mindspring.com. *His bio is on page 47.*

It is your life. It is your career. It is your certification.

CRM

In a business world of doing "more with less," your designation as a Certified Records Manager shows that you understand the many facets of the RIM profession.

In a business world that is rapidly changing, your designation as a Certified Records Manager shows you are up to date on the latest technology, the latest rules and regulations, and the techniques of the RIM profession.

In a business world in which new jobs are increasingly competitive, your designation as a Certified Records Manager shows that you have the experience and expertise that others may lack, and skills to show that you are a leader in the RIM profession.

For more information about becoming a Certified Records Manager, contact (518) 463-8644 or visit www.icrm.org

ICRM®
Institute of Certified Records Managers

Leveraging the Principle of AVAILABILITY to Show ROI

Can you still get funding for your initiatives when budgets are tight and senior management has decided it's more costly to mitigate risk than it is to suffer the consequences of poor recordkeeping? This article uses case studies to illustrate how you can sidestep the issue of risk and use the Principle of Availability to demonstrate positive return on investment for recordkeeping initiatives.

Julie Gable, CRM, CDIA, FAI

Much recordkeeping rationale is based on "what if?" What if there is a lawsuit requiring e-discovery? What if there is a regulatory audit and we need to produce records? What if our customers' personal information is compromised?

These are serious concerns, to be sure, and the basis of many articles, presentations, and product proposals that rely on the assumption that every organization wants to lower the risk of an information governance failure and its consequences.

But what if, in a tight economy with smaller revenues, an organization is willing to assume all of these risks, gambling that the probability of their occurrence is very small? If the perception among senior management is that the cost to mitigate such risks is greater than the chance of their occurring or the cost of their consequences, there may be no motivation to take action.

So what if the only way to get funding for any information management initiative is to show hard-dollar return on investment (ROI)? While all of the Generally Accepted Recordkeeping Principles® (Principles) are worthy of consideration in building and sustaining a high-quality program, most are based on the premise of reducing risk. Are there any Principles that offer the opportunity to recoup savings for the business?

The answer is yes. The Principle of Availability, working in concert with its partners Retention and Disposition, does have the potential to provide cost savings in productivity and storage and, in some instances, to actually generate revenue. Level 5 of the Information Governance Maturity Model (IGMM) for Availability specifically mentions measurable ROI as a result of excellence in information availability.

The trade-off is that achieving an acceptable level of maturity for the Principle of Availability is complex, requiring attention to such issues as inventory, finding aids, search methods, retention schedules, disposition policies, appraisal practices, and preservation needs. Once developed, however, availability continues to pay dividends year after year.

Regardless of industry, the ability

to find, retrieve, and use information is critical to business operations. Two case studies – one for a water utility and the other for a county government – will illustrate how availability provides ROI in different environments.

The Acadia Water Company Scenario

Over the last several years, Acadia Water has acquired more than 40 small, regional water service providers. The contracts, deeds, easements, insurance policies, litigation matters, permits, and construction documents have gone to Acadia's law department. The collection is mixed media, with some early items in paper only, some later items in electronic formats only, and some in both media.

Search Challenges

No one in the law department has specific responsibility for managing the records, and all search and retrieval are self-service. The records are arranged by year so that, for example, 1998 contains the records for Bismarck, Cedar Grove, and Innes Creek water companies, all of which were acquired in that year.

A searcher would have to know that Bismarck Water was acquired in 1998 to be able to navigate to the correct location in the records room, then scan the shelves to find where Bismarck records begin. There is a similar arrangement on the department file server. Company history and acquisition dates reside in the memories of long-term employees, some of whom are ready to retire.

Within each acquired company, files are divided into categories, but acquired companies had their own categories and there is no consistency among them. For example, street opening bonds can be found under four possible categories depending on which company is searched.

Navigating to the correct file does not always yield the desired document because in some cases a physical file's contents have been removed, leaving an empty folder. Checking for an electronic version of the desired document is hit or miss as well. Within the electronic folder hierarchy for any given company, there may be different documents, the same documents, or no documents at all compared to the paper files. With more than 25,000 paper files and at least as many electronic files, browsing is not an option.

Availability also dictates that "information must be described during the capture, maintenance, and storage processes in such a way as to make retrieval effective and efficient."

Cost of Poor Availability

There are 10 attorneys who use the collection on a regular basis to resolve contract, permit, and claim matters and as a reference in developing business proposals for expanding Acadia's services. Many attorneys report spending anywhere from 10% to 25% of their time trying to locate the information they need.

In cases where land records cannot be located, someone from Acadia may be dispatched to a county seat to get the document from a recorder of deeds, an all-day trip. The average salary and benefits for an attorney at Acadia is $250,000 per year.

Everyone acknowledges there is a lot of useless information in the paper and electronic files, but as lawyers they are reluctant to dispose of anything, particularly when there are no company policies governing disposition. There has been some discussion about imaging everything in the paper files and putting all of the electronic files into a document management system so they would be full text searchable and more easily available, but all projects at Acadia must demonstrate a strong ROI to get budget approval.

Keys to Improving Availability

The Principle of Availability states that "an organization shall maintain records in a manner that ensures timely, efficient, and accurate retrieval of needed information." Availability also dictates that "information must be described during the capture, maintenance, and storage processes in such a way as to make retrieval effective and efficient."

Acadia's law department is at Level 1 on the IGMM for Availability. One major problem is that Acadia's records collection is not arranged in a way that matches what the users know about the records they're seeking. For example, conversations with the attorneys show that they generally know the kind of document they're trying to find, an approximate date, the municipality or township involved, and the names of parties involved. In some instances, such as permits, a permit number is known. This is a directed search, one that is easily accommodated if standard metadata are available and searchable for records.

The law department also has no clear idea of what the collection contains, how much is really relevant to its work, and how much is without continuing value. In short, it doesn't know what it has or how long it needs to be kept. The Principle of Availability clearly notes the role that retention and disposition can play in enhancing availability at a reasonable cost, but Acadia has no mechanism for identifying and getting rid of what is useless. Without this, the records chaos will only worsen with each acquisition.

Regardless of Acadia's technology decisions, it is going to need an inventory of what it has, some research into the retention periods for the categories of records identified, a policy of disposition for things no longer needed, and a consistent file plan and standard metadata to assist in searching regardless of whether the records are paper or electronic.

Determining the ROI

Acadia's payroll for attorneys is $2.5 million annually. Cleaning up the files and making them searchable would save, at a minimum, 10% of its attorneys' time, for an annual savings of $250,000.

Acadia submits a proposal to hire a consulting firm that will provide the needed inventory and analysis, a set of standard metadata by document type, a retention schedule based on legal research, and a disposition policy. It is estimated the work will take six months and cost $150,000. The proposal is approved, based on the expected reduction of search time.

At the end of the project, Acadia hopes to reduce the collection by about half, thereby also reducing the cost of scanning and indexing for paper files and the cost to transfer electronic files into a document management system. In addition, paring the collection before converting it to electronic will reduce the future cost of storage, storage administration, back-up tapes, and back-up tape storage.

The Willett County Scenario

Like all organizations, Willett County must keep records for operational, fiscal, and legal purposes, but as a government entity, it has a duty to make records available to the public and to preserve history.

County departments include the district attorney, magistrate courts, tax assessment, recorder of deeds, sheriff, and others that are under the jurisdiction of elected officials who may or may not understand the importance of records beyond their day-to-day purpose.

Other departments include vital statistics, public works, and services for children, youth, veterans, and the aged. Each department has its own budget to spend as it deems necessary. Most departments have some records automation in the form of databases, but these have existed only for the last five to 10 years. Many records are still on paper because they are part of business processes that require signatures.

… as a government entity, it has a duty to make records available to the public and to preserve history.

Records Arrangement

Active records reside within each department, but space in the county building is very tight. Records from previous years, sometimes as recent as last year, are boxed and sent to a former elementary school that is now empty and unstaffed.

Each department has its own rooms for records storage at the school. Some departments have installed rack shelving in their store rooms and use standard cubic foot boxes, each of which is logged into a departmental spreadsheet or database as a finding aid. Other departments have simply piled boxes of all sizes into whatever spaces they could find at the school.

The county had a records manager who attempted to enforce retention schedules, but he resigned more than 18 months ago and has not been replaced. There are about 30,000 boxes stored at the school.

Search Challenges

Retrieval from the school requires driving from the county's offices to the outskirts of town, a drive of about 30 minutes each way. Those who have useful inventories and neat shelving arrangements can find their boxes easily; those who don't can't. No one relishes the task of retrieving from the old school, which is not heated or air conditioned. Cell phone reception at the school is nil. Departments insist on sending two people on each retrieval trip as a safety precaution.

The school is scheduled for demolition and the county will sell the parcel of land. All boxes must be moved. The county's facilities department has been assigned to explore storage solutions. Alternatives are using a commercial storage vendor, developing a county-run records center, implementing some form of automation, or a combination of all three. The county wants to serve its residents as efficiently as possible. Budgets are limited, and the county is determined to find a solution acceptable to all departments rather than having each one make its own arrangements.

Keys to Improving Availability

The first consideration was to develop a uniform understanding of "availability." Some departments believed they had to keep everything, no matter how mundane, because someone might ask for it. Others had a more savvy understanding of retention and disposition based on legal requirements, while still others believed that what to keep and what to dispose of depended on the desire of the elected official currently in power.

Here, the Principle of Availability and its corollaries of Retention and Disposition were helpful in creating a county-wide concept that records are governed by retention schedules and purging is possible if no litigation or investigation is underway or imminent.

Next was to determine what needed to be available for running the county's business and serving its citizens. Discussions with departments revealed which records were most frequently requested and by whom.

The recorder's office reported a high rate of retrieval for land records, mostly by title search companies, but some by large corporations, such as utilities, and by private citizens. Vital Statistics reported that people doing ancestry research were particularly interested in finding birth, death, and marriage records.

Quantifying the number of records that would require new storage space

or an electronic alternative was a priority. The Principle of Availability states that complete and accurate information depends on having "an efficient and intuitive set of methods and tools to organize the records" and "providing employees and agents with sufficient training to utilize these tools successfully."

To help inventory the stored boxes, each department received a pre-configured Excel spreadsheet, bar code labels, and bar code readers, plus instruction in using these tools. In addition, all participants were given department-specific retention schedules from the state's records commission or from the state's judiciary office. Emphasis was on the need to know how many boxes must move and how they would be accounted for before, during, and after the move. There was also discussion of what records would be considered historic.

The inventory results astonished those who never realized how many of their stored records were well past their required retention. For others, it was the first reckoning of exactly what they had at the school. Sadly, many bound books of very old records were deteriorating from the poor storage conditions. One happy find was a trove of photographs dating to the late 1800s, some documenting businesses and manufacturing companies, others showing the development of bridges, water lines, and power lines for farms and homes. Several important items, previously thought to be lost, were found.

Determining the ROI

Following the inventory and comparison with retention schedules, 11,000 boxes were eligible for destruction, and departments assigned personnel to make sure that no litigation or other action was pending for the records they contained. Destruction forms were completed and approved.

The county compared the cost of offsite storage and commercial storage but opted to set up its own records center in rented space within walking distance to the county building. Much of the old rack shelving from the school was recycled for stacks in the new space. The spreadsheet inventories that had been completed for the move were expanded to include box storage locations in the new site.

The inventory results astonished those who never realized how many of their stored records were well past their required retention.

The records center would be staffed by a records manager and one warehouse person to provide assistance and maintain order. Their labor cost was easily offset, as the average burdened cost of a county employee was $50 per hour, and each of 15 departments had averaged sending two employees on two, two-hour trips per week to the old school, for an annual productivity cost of $312,000:

2 staff x 2 trips x 2 hrs. per wk. =
8 hrs. per wk., per dept.

8 hrs. per wk. x 52 wks. =
416 hrs. per year, per dept.

416 hrs. per year x $50 hr. =
$20,800 annual savings per dept.

$20, 800 per dept. x 15 depts. =
$312,000 annual savings

Working with the county recorder, the facilities department proposed to make imaged land records electronically available. It was determined that fees could be charged for convenient access, particularly to land title companies and other bulk users who would be given protected electronic access for an annual fee that would be less than their costs to travel into town and pay for parking, gas, and meals.

The old photographs were found carefully labelled with locations or intersection names on the back. Working with the county historical society, these would also be scanned and reproductions made available for sale online. The sale of the school property, preservation grants, budget contributions from each department, plus revenues from the ventures would fund the cost of scanning and setting up the county records center.

The Bottom Line

Acadia's situation shows the effort involved in applying the Principle of Availability to a collection that had grown without oversight, and it illustrates the savings that can be realized in making the right information available to the right people at the right time. Applied carefully and well, the Principles of Availability, Retention, and Disposition can yield savings in productivity and reduce costs associated with potential automated solutions.

Willet County's experience underscores how capitalizing on availability has implications for employees and for citizens. By purging what is truly no longer needed, Willet saved more than one-third of the amount of cubic feet it needed and realized cost savings in productivity. By taking a big-picture view, Willet was able to turn availability into a potential revenue stream.

Availability, Retention, and Disposition may be the most universally applicable Principles when it comes to finding an ROI from information governance activities, although the savings may not be obvious at first. Improving availability takes time and effort, regardless of whether manual or automated methods are used. Inventories, analyses, retention schedules, and disposition activities will incur a cost in the initial year, but the savings from productivity and from opportunities to generate revenue will continue for years into the future. **END**

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

ARMA INTERNATIONAL

LIVE!

hands-on education

california, here we come!

Join us for ARMA Live! Conference and Expo 2014 in San Diego on October 26-28

ARMA Live! offers the most comprehensive educational and networking experience in the profession. From inspiring keynotes to cutting-edge best practices and technology, your takeaways from this conference are worth far more to you and your organization than the price to attend.

In addition to the warmth of California in late October – which those of you hailing from cooler areas will consider a perk – this conference will offer SO MANY NEW experiences. Look inside to learn about our new:

- **Opening Keynote by a *New York Times* Best-Selling Author**
- **Designation Academy**
- **Opening Reception**
- **AIEF Uncorked**
- **IGenius Bar**
- **(Unofficial) Monday Night Party Spots**
- **Education Tracks**
- **Pricing Discounts**
- **Roundtable Times**


Smolan

Opening Session: Does Big Data Have a Human Face?

Rick Smolan is a former *Time, Life*, and *National Geographic* photographer best known as the creator of the "Day in the Life" book series. His most recent project, *The Human Face of Big Data*, came after immersing himself in the world of big data scientists, engineers, and entrepreneurs – and coming away convinced that big data is going to have 1,000 times more impact on our lives than the Internet. The book's premise is that our electronic devices are creating a planetary nervous system and that the massive, real-time capture and analyses of the resulting data will allow us to address some of humanity's greatest challenges, including pollution, world hunger, and illness. During his keynote address, Smolan will seek to connect and visualize big data into meaningful ways that have very human implications.


Isaza


Montaña


Cunningham


Phillips


Bradley


Stephens


Shade


Colgan

Closing Session: ARMA International Company of Fellows

Join a panel of Fellows of ARMA International (FAI) at the closing session, "Embracing Change: Provocative Perspectives." In the highly regarded format of the Fellows Forum, industry thought leaders will engage in fast-paced dialogue to share their provocative perspectives on change in our information governance world. Reflect on your conference experience with a meaningful and memorable closing session that embraces change in your important and evolving role!


Dmytrenko

April Dmytrenko, CRM, FAI, will facilitate and be joined by the following panelists representing these unique perspectives:

- **Legal:** John J. Isaza, Esq., FAI; John Montaña, J.D., FAI
- **Technology:** Patrick Cunningham, FAI; John Phillips, CRM, FAI
- **International:** Alexandra Bradley, CRM, FAI; David O. Stephens, CRM, CMC, FAI
- **Past Presidents:** Wendy Shade, FAI; Julie Colgan, IGP, CRM

ARMA sandiego 2014

register online at *www.arma.org/conference*

ARMA INTERNATIONAL LIVE!

oceans of opportunities

strategic education

NEW! Education Tracks

We are extending our conference education sessions to include all information governance (IG) stakeholders. You can choose the track that most interests you and follow the sessions in the appropriate skill level.

Because collaboration with other stakeholders is so important to IG success, you may find sessions from other tracks are also relevant for you.

B/A Business & Audit	This education centers on how proper IG reduces risk and brings value to the organization. Learn how appropriate IG practices can help your organization become more competitive and compliant in the face of 21st century information management challenges.
IT Information Technology	This education extends beyond the traditional scope of electronic records management to address challenges of emerging technologies. Learn about tools and resources that can position your organization to meet IG requirements using legally defensible technology.
L Legal & Compliance	This education focuses on the most pressing legal and compliance aspects of IG. Learn about best practices and the laws and regulations that affect activities such as litigation, discovery, and organizational compliance. Some content provided by ILTA.
P Privacy	This education revolves around the principles and practices within the rapidly evolving field of privacy and data protection. Learn how privacy laws, regulations, and the protection of information within and across products, services, and borders demonstrate effective IG.
RIM Records & Information Management	This education pertains to the knowledge and skills required to systematically manage information as the foundation of sound IG. Learn how standards, best practices, and the Generally Accepted Recordkeeping Principles® can help move your organization forward.

Skill Level Tracks:

Core: Education suggested for those who are new to the profession; are in entry-level positions; or are practitioners from other disciplines and domains, such as IT, legal, compliance, and risk.

Management: Education suggested for seasoned practitioners who have some level of hands-on, prior experience; possess significant knowledge of information management practices and information governance concepts; manage or develop projects and staff; or possess extensive knowledge in other business domains.

Strategic: Education suggested for high-level experts with a strategic focus, such as executives, senior business managers, legal counsel, technology architects, and compliance officers.

For a complete list of sessions, visit *www.arma.org/conference*.

NEW! Pre-Conference Designation Academy

We're pleased to introduce ARMA International's **Designation Academy**, which offers certificate programs and certification exam prep courses to help you take your next steps toward a professional designation.

The 2014 Designation Academy will feature education from ARMA International, the International Association of Privacy Professionals (IAPP), the Institute of Certified Records Managers (ICRM), and the Information Systems Audit and Control Association (ISACA).

Designation Academy Programs*

Two-Day Seminars

Friday & Saturday, October 24-25

- Certification Foundation and CIPP/US Privacy Training (IAPP)
- CRM Exam Prep: Introduction and Parts 1-6 (ICRM)
- Fundamentals of IS Audit and Assurance (ISACA)

One-Day Seminars

Friday, October 24

- Certification Foundation Privacy Training (IAPP)
- Essentials of the Generally Accepted Recordkeeping Principles® Certificate (ARMA)
- Introduction and CRM Exam Parts 1-5 (ICRM)

Saturday, October 25

- Becoming a Certified Information Governance Professional (IGP) (ARMA)
- CIPP U.S. Private-Sector Privacy Training (IAPP)
- CRM Exam Prep Part 6: The Business Case (ICRM)

Other Pre-Conference Programs*

Half-Day Seminars

Saturday, October 25

- A Roadmap to Records Retention Schedule Development
- How to Develop a Litigation Readiness Plan

*Registration and additional fees are required to attend these programs.

ARMA sandiego 2014

register online at *www.arma.org/conference*

LIVE!

sky's the limit

social expo days/networking nights

Expo 2014: Talk, Trends, and Technology

Come early and stay late – the exhibit hall is open the first two days of conference – Sunday and Monday only. Don't miss out on the education, technology, and excitement.

Emerging trends and technologies abound at the ARMA Expo, which will host more than 150 exhibitors. Check out featured solutions for content management, e-discovery, cloud computing, e-mail management, and much, much more!

The EXPO is **FREE (a $150 value)** to registered attendees. It includes:

- Admission to the opening general session featuring *New York Times* best-selling author Rick Smolan
- Education sessions in three Expo Hall rooms
- Guidance at the Consultant's Corner
- Product demos
- Beverage breaks
- Relaxation station
- Pub Crawl Finale in the Expo Hall 3:30 p.m. - 5:30 p.m. on Monday
- Eligibility to win cash and prizes in the Big Money Giveaway. (Check your conference bag for your game card.)

NEW! IGenius Bar

On tap at the **IGenius Bar** is all the knowledge you can drink in. Served by an expert facilitator, these lively, interactive, sessions will quench your thirst for solutions to your industry-specific challenges. Come ready to collaborate!

California Knows How to Party!

ICRM Business Meeting and Cocktail Reception

Saturday, October 25, 7:00 p.m.

The ICRM will host a business meeting at 6:00 p.m. followed by a cocktail reception at the Hilton Bayfront. The business meeting is free and open for all interested parties. Registration is not required. To attend the cocktail reception, purchase your $30 ticket during online conference registration.

2014 Opening Reception

Sunday, October 26, 5:00-6:30 p.m.

Join us for a cash bar and light appetizers (immediately following the Sunday education sessions) at the San Diego Convention Center's outdoor "Center Terrace." No ticket will be required, but you will need your name badge!

San Diego Tour

Monday, October 27, 5:30-7:30 p.m.

Looking to take in the highlights of San Diego? Come aboard ARMA's private San Diego Trolley for a 1 1/2 hour guided tour. Highlights will include Coronado, Balboa Park, Little Italy, Old Town, and the Embarcadero area along San Diego's waterfront. Cost is $35 per person.

AIEF Uncorked

Monday, October 27, 6:00-8:00 p.m.

Spend the evening with the ARMA International Educational Foundation (AIEF) at JSix Restaurant & Lounge for a four-course wine tasting menu with hors d'oeuvres. The cost is $150 per person or $250 per couple, with net proceeds benefiting the AIEF. Availability is extremely limited, so be prepared to register during your online conference registration.

Unofficial Monday Night Party Spots

Monday, October 27

ARMA is partnering with a collection of nightlife venues in the famous Gaslamp District as unofficial party spots for conference attendees to gather and continue networking. Receive a 10% discount on adult beverages when you show your conference badge to the server at any of the venues listed in the conference guide. (The guide will be available when you check in at conference.)

ARMA sandiego 2014

register online at *www.arma.org/conference*

LIVE!

escape to extraordinary

join us in america's finest city

"San Diego. Drink it in; it always goes down smooth."

– Ron Burgundy

You don't have to be a fan of the "Anchorman" movies to love this beautiful coastal city. Bordered by the Pacific Ocean to the west and the Laguna Mountains to the east, the diverse neighborhoods of San Diego are spread out over 4,200 square miles, offering endless opportunities for exploration and activities. ARMA 2014 will be taking place in San Diego's downtown, in the heart of the iconic Gaslamp District, where eating, drinking, shopping, and fun will literally be footsteps away.

Hotel(s) California

ARMA International has arranged for rooms at the Hilton Bayfront, Marriott Marina, and the Omni at a discounted rate. **And, if you book your room when registering online for the ARMA 2014 Conference, you will save $100 off your full conference registration.**

Please note that the hotel deadline is 5 p.m. (CDT) on September 30. Hotel reservations made after this time will be based on availability, with no guarantee that conference rates will apply.

Hilton San Diego Bayfront

Conference headquarters to the Designation Academy, pre-conference seminars, and evening functions. **$285 night, plus tax**

Marriott Marquis & Marina San Diego

Features four restaurants and a Starbucks, located near the West end of the Convention Center. **$269/$249 night, plus tax**

Omni San Diego

Located next to Petco Park and features an outdoor fireplace and heated pool. **$259 night, plus tax**

Don't Wait, Register Today!

Be sure to register by September 15, 2014, and receive a $100 discount with the early registration rate on FULL conference registration!

Want to save an ADDITIONAL $100 off your FULL conference registration? Book your hotel room when you register for FULL conference at *www.arma.org/conference* by September 15 for the best deal of the year!

Please note: phone registrations are not eligible for this additional discount.

Early Registration Discount (BY September 15)

Full Conference	**PRO $1,149/REG $1,399**
One-Day	**PRO $475/REG $475**
EXPO Only	**Complimentary**

Pricing AFTER September 15:

Full Conference	**PRO $1,249/REG $1,499**
One-Day	**PRO $500/REG $500**
EXPO Only	**Complimentary**

Questions? E-mail us at ***conference@armaintl.org***, or visit ***www.arma.org/conference*** to register today!

Cancellation Policy

Written cancellations postmarked, e-mailed, or faxed by **September 26, 2014,** will incur a cancellation penalty of 15% of all registration fees.

Cancellations postmarked, e-mailed, or faxed after **September 26, 2014,** and by **noon (CDT) October 10, 2014,** will be subject to a penalty of 50% of all registration fees. There will be no refunds to registrants who do not cancel by October 10, 2014. Substitutions are encouraged.

Start the ARMA Conference conversation now by following us on Facebook, Twitter, and LinkedIn. Be sure to use #ARMA2014.

ARMA sandiego 2014

register online at *www.arma.org/conference*

Cut Costs, Risks with Proactive Litigation Plan

Michael C. Wylie, J.D., PMP, and Kelli A. Layton, J.D.

In the last few years, production of electronically stored information (ESI) for business and other purposes has increased exponentially. As the amount of information that organizations maintain grows, so do the costs and risks associated with effectively managing that data.

To counter these effects, it is essential that organizations prepare themselves for potential litigation by creating a litigation readiness plan. By mapping their data types, locations, and custodians and establishing plans to respond to discovery, organizations can save money and reduce risk in litigation.

As a result of this complexity, discovery obligations necessarily involve not only legal counsel, but also records and information management (RIM) and information technology (IT) personnel. Operationally, these groups work independently. As such, solutions created solely to solve RIM or IT problems may create inefficiencies when applied to litigation.

However, as recognized by the EDRM in the 2011 publication "How the Information Governance Reference Model Complements ARMA International's Generally Accepted Recordkeeping Principles" (EDRM 2011), organizations can identify and mitigate these inefficiencies through careful planning.

Identify Proactive Solution Elements

Legal, RIM, and IT professionals have the ability to incrementally improve discovery response processes and save significant time and money

This article explains how to develop a litigation readiness plan that will help reduce costs and mitigate risks associated with e-discovery when the plan is implemented and adhered to by employees who deal with electronically stored information.

by taking proactive steps to understand their organization and the litigation risks it faces. By focusing on the nexus between RIM, IT, and legal requirements, organizations can identify hurdles presented by existing processes and create a litigation response methodology that successfully uses existing infrastructure.

To identify the processes and systems required for an organization's litigation readiness plan, three factors should be considered: 1) litigation portfolio, 2) organizational structure, and 3) current discovery and records retention processes.

Litigation Portfolio

Perhaps the most important element of an effective, proactive litigation strategy is an understanding of past litigation. This generally may be achieved by studying three categories of information:

1. Information concerning cases with ongoing discovery or retention requirements per Rule 26 of the Federal Rules of Civil Procedure (FRCP)
2. General metrics for an organization's litigation portfolio, including the total number of cases and number of cases by practice area. This information is gathered for both active and historical litigation, usually for a period of five or 10 years.
3. Litigation budgets, including annual budget information for each practice area and average case expenditures overall and by practice area.

Such an analysis would bring to the organization's attention any responses that are immediately necessary and help predict future litigation. Additionally, each of the above plays a key role in performing cost/benefit analyses for changes to litigation response processes.

Organizational Structure

Organizational data required for litigation planning includes organizational charts, data maps, and basic information concerning organizational structure. In broad terms, this information is necessary to identify the types and locations of paper documents, ESI, and potential witnesses relevant to litigation.

Organizational charts plot business structure and, ideally, the individuals working within defined groups. *Data maps* outline the physical or virtual location of information. Ideally, a data map will include locations of hard copy documents, e-mail documents, locally stored files, root information and access requirements for network drives, web-based storage such as SharePoint®, and any other storage location. Locating information and access points is particularly important for geographically distributed organizations.

In most instances, individual-level organizational charts and data maps must be supplemented through consultation with document custodians to mitigate obsolescence. Input from document custodians may also be necessary where organizational charts or data maps cannot accurately predict interactions between individuals or interactions between individuals and data.

This issue is particularly likely to arise in "matrix" or "lattice"-type organizations. Note, however, that even in these types of organizations, organizational charts or similar diagrams will identify levels of decision-making authority.

Depending on the organization's size, structure, and budget constraints, consultation usually takes the form of interviews with key points of contact within the organization or surveys of a broader cross-section of employees. The level and method of consultation with custodians may vary by litigation type.

Discovery Processes

When approaching litigation proactively, it is imperative not only to recognize risks associated with organizational structure and future litigation, but also to identify the current methodologies used to reply to discovery requests.

While many organizations do not have formalized processes for meeting discovery obligations, legal departments and RIM professionals have experience executing litigation holds and collecting and tracking documents responsive to discovery requests.

Legal, RIM, and IT professionals may determine the effectiveness and scope of discovery processes by analyzing preservation notices, questionnaires for document identification, collection instructions, sample chain-of-custody logs, and sample documents.

Records Retention Processes

As illustrated by the existence of the Generally Accepted Recordkeeping Principles® Principle of Disposition, as referenced in EDRM 2011, proactive efforts to reduce risk and save costs in a discovery context cannot ignore records retention.

While the incremental cost of electronic storage is decreasing, the cost of managing that additional data is increasing. It is well recognized that the true cost of storage greatly exceeds the incremental cost of storage space. As noted in 2012 by the American Institute of Certified Public Accountants'

Information Technology Section in "A Practice Aid for Records Retention," this figure includes costs associated with complying with litigation discovery requests for that data.

In 2005's *Arthur Andersen LLP v. United States*, the U.S. Supreme Court held that a records retention policy must consider not only how long an organization *wants* to keep information, but also how long the organization is *required* to keep information. The court further indicated that retention policies are valid even where "created in part to keep certain information from getting into the hands of others, including the government."

The limits of records retention expressly set out by the court in *Arthur Andersen* have, when applied to electronic records, come to be known as "defensible deletion." *Defensible deletion* is what it purports to be – a policy that maximizes *reasonable* document preservation, i.e. keeping materials that have a business use or as required by law, while also allowing an organization to eliminate data that lacks business value and is not required to be retained.

By decreasing the volume of electronic records being retained, companies may reduce the amount of data retained and thereby limit the corresponding management costs. More importantly, reducing the universe of immaterial documents decreases risks associated with errors in large-scale document review and production.

In 2010, the Southern District of Texas concluded in *Rimkus Consulting Group, Inc. v. Cammarata* that what constitutes a "reasonable" document preservation policy is industry- and company-dependent and depends on the proportionality of the policy to the needs of the case and generally applicable standards.

Whatever the terms, adopting a defensible deletion strategy will decrease costs and risks associated with over-retention of ESI. As noted by Gibson Dunn's "2013 Year-End Electronic Discovery and Information Law Update," retaining "large volumes of uncontrolled and unorganized data can make e-discovery *extremely* costly . . . controlling and organizing a company's data allows [the] company to decrease its risk of spoliation, simply by having less data that could be overlooked when instituting a litigation hold or collecting documents to disclose."

. . . reducing the universe of immaterial documents decreases risks associated with errors in large-scale document review and production

Evaluate Risk Factors

Once an organization's litigation portfolio, organizational structure, and current discovery and records retention processes have been sufficiently outlined, an analysis of strengths, weaknesses, opportunities, and threats (SWOT analysis) should be performed on any plan seeking to address these factors.

The SWOT analysis will compare the actions with respect to selected risk factors. The risk factors evaluated and the weight assigned to each risk factor may vary from organization to organization. However, litigation readiness plans can generally be evaluated based on four key factors: 1) extent of business disruption; 2) level of control over information; 3) effectiveness of operational processes and technology used during litigation; and 4) avoidance of discovery sanctions.

Extent of Business Disruption

Discovery obligations can have a profound effect on business operations, particularly when employees are required to search large quantities of data. Further, Charles Ragan noted in a 2013 *Richmond Journal of Law and Technology* article "Information Governance: It's a Duty and It's Smart Business" that absent investment in costly search technologies, large volumes of data create inefficiencies in data retrieval to the extent that strategic opportunities may be lost. The Principle of Availability, as discussed in EDRM 2011, anticipates processes that will reduce the employee search time and increase employee effectiveness when confronted by big data and discovery obligations.

Level of Control

E-discovery expert and attorney Ralph Losey indicates that there are good reasons to outsource litigation support in "Five Reasons to Outsource Litigation Support." However, releasing data to a third party always bears potential risks, including inadvertent release – particularly with respect to proprietary and controlled information.

As noted in EDRM 2011's overview of the Principle of Protection, organizations routinely maintain sensitive or classified information, information containing personally identifiable information or protected health information, and business confidential information which cannot or should not be released. Accordingly, organizations would be wise to consider the threat of inadvertent dissemination, waiver of privilege, and other risks of release when evaluating their litigation readiness policies.

Effectiveness of Technology and Processes

Gibson Dunn's "2013 Year-End Electronic Discovery and Information Law Update" makes clear that despite cost control efforts, the cost of e-discovery continues to rise due to inconsistently applied requirements and expanding volumes of data.

Per Microsoft's "Global Enterprise Big Data Trends: 2013," approximately 89% of responding companies had a budget for a big data solution, and 72% indicated that they are actively

planning a solution. As more organizations implement big data or information governance programs, pressure to piggyback e- discovery processes onto such solutions is expected to increase.

While not primarily intended for e-discovery, if repurposed correctly, big data solutions can be used to effectuate document retention, defensible deletion, and discovery collection efforts. If concerns of discovery can be met by repurposing big data or other RIM or IT strategies (such as off-the-shelf e-mail storage solutions), significant cost savings may be achieved. This approach is also supportive of the Principles of Integrity and Compliance.

Avoidance of Sanctions

The Advisory Committee to the FRCP accounted for emerging technologies in discovery as early as 1970. Fed. R. Civ. P. 34(a) (*Notes of Advisory Committee on Rules – 1970 Amendment*). In 2006, the committee formally codified in Rule 34(a)(1) the generally accepted interpretation that discoverable information includes both tangible information and ESI. The amendments specifically cautioned against limiting the definition of ESI, thereby creating uncertainties regarding proper preservation of large volumes of data.

As indicated by Barbara Rothstein's 2007 *Managing Discovery of Electronic Information: A Pocket Guide for Judges*, both courts and judges have recognized hurdles inherent in ESI discovery, and courts have made clear their view that retention policies do not have to be perfect to be defensible.

As an example, Rothstein cited 2012's *Monique Da Silva Moore, et al. v. Publicis Groupe & MSL Group*, in which the court held that ESI computer-assisted review need not be perfect, but it must instead produce accurate and complete results at a proportional cost.

Further, as discussed by U.S. Magistrate Judge Craig B. Shaffer (District of Colorado) in his article "Defensible' By What Standard?," published by The Sedona Conference® in 2012, "a technology-assisted e-discovery process should not be held to a standard of perfection, but it should produce discovery results that are defensible in terms of the producing party's discovery obligations and reasonable from the standpoint of cost and efficiency."

Recent proposals will increase organizations' ability to proactively prepare for litigation by reducing uncertainty in e-discovery

Nevertheless, as indicated by Rothstein, electronic data that is difficult to access and/or produce often falls within the normal discovery parameters. Per *The Sedona Principles* editor Thomas Allman in his analysis of *West v. Goodyear Tire & Rubber Co.* in 2010's "Preservation and Spoliation Revisited: Is it Time for Additional Rulemaking?" and Fed. R. Civ. P. 37(e), parties must have the capability to comply with procedural rules governing production of ESI or risk sanctions for non-compliance or "spoliation." Because of this, it is advisable for companies to adopt litigation readiness measures well before litigation.

Both The Sedona Conference's® 2010 *Commentary on Legal Holds: The Trigger & The Process* and the 2010 opinion of U.S. District Court Judge Shira Scheindlin (Southern District of New York) in *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities*, Federal Rule 37(e) provide that an organization's duty to preserve potentially relevant documents and ESI is triggered once litigation is reasonably anticipated.

Moreover, in the 2011 report to the Judicial Conference Advisory Committee on Civil Rules entitled "Motions for Sanctions Based on Spoliation of Evidence in Civil Cases," Emery G. Lee III reported that, per a study of spoliation motions in 19 test districts, 15% of civil cases filed in 2007–2008 involved spoliation issues, and ESI was among the evidence at issue in 93% of those cases. Motions for sanctions were granted in 23% of cases.

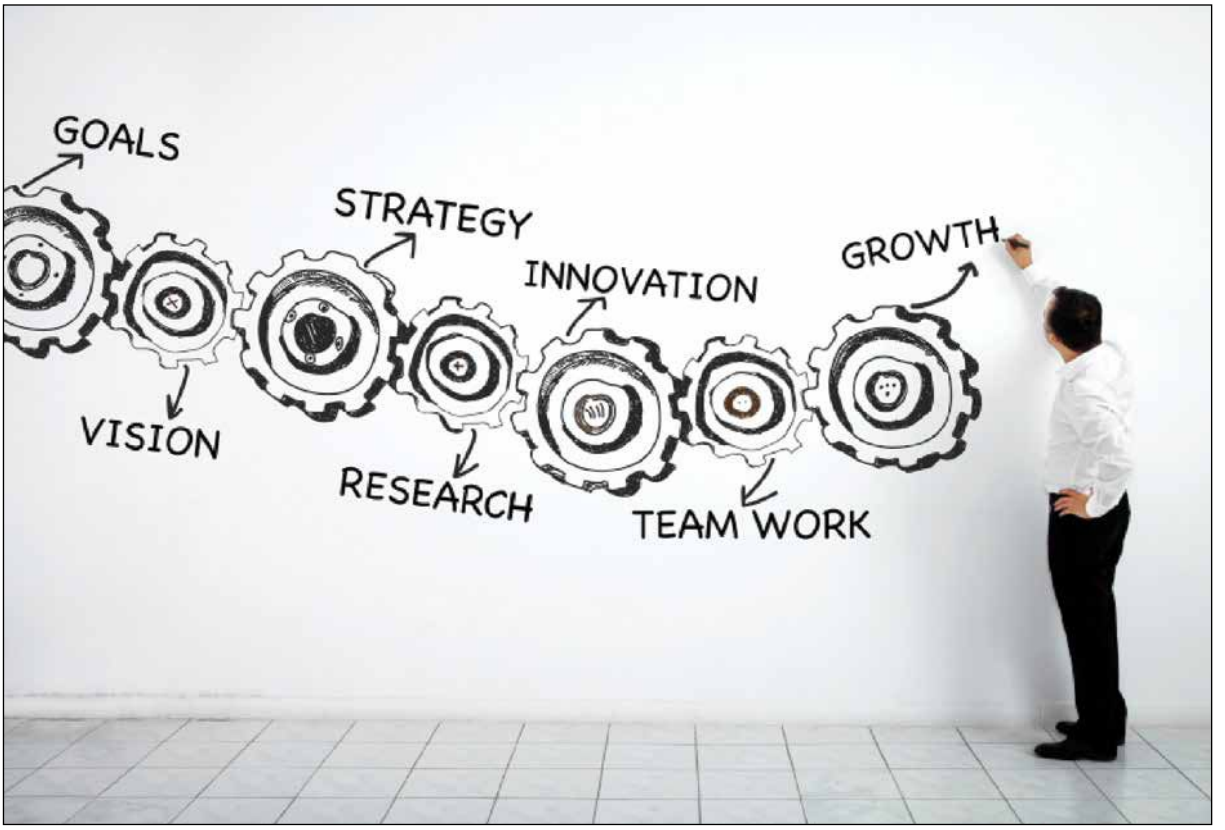
Recent proposals will increase organizations' ability to proactively prepare for litigation by reducing uncertainty in e-discovery. In his presentation at Duke Law School, Allman, suggested that the FRCP address the issue of spoliation by codifying preservation obligations and sanctions for preservation violations.

Proposed amendments to Rules 26 and 37 would further reduce sanctions related to ESI. Although the 2006 addition of the "Safe Harbor Clause" in Rule 37(e) partially addressed problems with preservation of ESI by limiting the extent to which parties may be liable for unintended destruction of ESI, the rule did not eliminate sanctions for routine or inadvertent non-compliance.

The proposed amendments to Rule 37(e) offer additional curative measures to allow organizations to avoid sanctions. By further identifying curative measures, the proposed rules would ensure that organizations have more leeway to develop reasonable, focused litigation readiness policies.

END

Michael Wylie, J.D., PMP, can be contacted at miwylie@deloitte.com. *Kelli Layton, J.D., be contacted at* klayton@deloitte.com. *See their bios on page 47.*



How to Develop and Implement an Effective RIM Policy

Blake E. Richardson, CRM, CIP

Business policies provide an organizational framework in which employees are expected to operate. Effective policies provide clear directions and expectations, enhancing consistency and eliminating employee "guess-work" factor. Policies should cover a multitude of topics, from business ethics to sexual harassment to travel and entertainment and, yes, records and information management (RIM).

Of course, not all policies are created equally. While some policies leave the employee with a clear understanding of what to do, others are ambiguous, leading to misinterpretation and inconsistent behavior. It is difficult to govern behavior with policies employees cannot understand. So, keep the language simple. Avoid verbosity, acronyms, and complex sentences. Policy writers must also keep in mind that they know the subject matter much better than most readers do.

It is important to note that a policy should communicate to employees *what* to do, not *how* to do it. The policy message can quickly become lost when individual procedural steps are incorporated. Employees are left to separate *what* they should do from *how* to do it. However, it is appropriate in a policy document to say that procedures related to a policy exist and where they are.

Policies communicate specific guidance and expectations that they will be complied with – both internally and externally. But, employees must have the necessary resources to comply; a policy must not set up employees for failure.

Basic Policy Components

The following sections describe basic policy components that should be included.

Purpose

A policy should begin by stating its purpose and what it addresses. Here is one example of describing the purpose of a RIM policy:

This policy is intended to assist all employees in effectively managing the organization's records and information. It will help ensure that all records and information necessary for fulfilling operational, legal, regulatory, and tax responsibilities are readily accessible and retained for the appropriate period and properly disposed of when their retention period has expired and they have been approved for destruction or deletion.

Scope

A policy scope summarizes the policy and identifies whom it applies to. For example, "This policy applies to all company and temporary employees as well as contractors, and it governs the management of physical and electronic information."

Glossary

Because a policy often includes terminology that some employees might not know, always include a glossary. Electronically posted policies often contain hyperlinks to each definition.

Audits

Inform all parties included in the scope that policy compliance is subject to internal and external audit.

Basic RIM Components

After establishing basic policy components, focus on RIM-specific topics that will help ensure that organizational content is managed in an efficient and compliant manner. Following are common RIM policy components.

Vital Records

Include a section on identifying and protecting vital records. For example, the policy might state, "It is the responsibility of the department heads to identify their operation's vital records." In addition, the glossary should define the term to educate employees on what constitutes a vital record.

Because a policy often includes terminology that some employees might not know, always include a glossary. Electronically posted policies often contain hyperlinks to each definition.

Retention Schedule

The RIM policy should address the purpose of the retention schedule, how to read it, and the need to comply with it. The policy should provide guidance on how to update the schedule.

Legal Holds

This section of the policy must provide specific direction on employees' responsibilities for handling legal holds. Policy language might say, "Any information on hold because of an active or anticipated lawsuit, audit, or regulatory inquiry must be retained even if its retention period, according to the organization's retention schedule, has expired."

Record Storage

The policy should say that company records are to be stored only with RIM-approved vendors and that individual departments cannot enter into contractual relationships with storage vendors.

Hard Drives and File Shares

A RIM policy should guide employees on the appropriate use and maintenance of hard drives and file shares. For example, "Local hard (C: drives) are not to be used for the storage of company records or content of business value. This type of information must be stored in a repository accessible by employees with appropriate authorization." The policy should also communicate that employees must maintain the content they save to hard drives and file shares.

E-mail

How an organization manages e-mail is primarily dependent on available technology. Therefore, it is important to understand what capabilities exist, such as e-mail management and archiving applications, Outlook personal storage table (more commonly referred to as .pst) folders, and enterprise content management software. The RIM policy should provide direction to employees in accordance with available technology.

Regardless of existing technology, basic e-mail policy components need to address such topics as forwarding business e-mails to personal e-mail accounts, minimizing the distribution of attachments, and evaluating e-mail content for retention purposes.

Information Destruction/ Deletion

Include a section that addresses the proper methods for the de-

… it is imperative to collaborate with each department during the policy draft phase and to have those departments conduct a final review before the policy is distributed.

struction and deletion of physical and electronic information, advising employees that only vendors approved by the RIM department are to be used.

Additional Policy Considerations

As technology advances, RIM policies need to keep pace. The following topics are being incorporated in many RIM policies.

Social Media

Many organizations have issued general-use social media policies with a focus on limiting what an employee can post. Because organizations want to preserve their image and prevent the disclosure of proprietary information, their social media policies might state that employees are prohibited from posting disparaging comments about their employer. In the United States, though, a policy that prohibits employees from posting about their wages or working conditions might conflict with Section 7 of the National Labor Relations Act, which allows non-management personnel to do just that.

A RIM policy should approach social media based on content. If posts submitted by employees as part of their job function or posts received on the organization's social media sites from the public constitute an organizational record, then the content should be retained in accordance with the retention schedule. In addition, the organization must have the ability to preserve social media content (created and received) in the event of litigation or regulatory inquiry.

Cloud

Cloud storage and computing can reduce capital expenses related to data center hardware, software, storage, supplies, and maintenance. Before bouncing to the cloud, though, RIM professionals should ensure the RIM policy addresses the things that put the organization's records and information at risk. The policy should address requirements such as availability, security, data ownership, and retention.

Bring Your Own Device (BYOD)

The advent of personal "smart" technologies has required organizations to rethink their approach to company-only devices for accessing and processing information. Many employees question the need to carry company-issued phones and laptops when their personal devices can perform many of the same functions.

An organization should issue a BYOD policy that addresses such topics as types of devices allowed, connection protocols, and the need to sign a waiver. The RIM policy should address issues related to device security, to imaging data on the device for legal hold orders, and to separating personal from corporate information.

Getting Policy Approval

For a RIM policy to be successful, other departments must abide by it. Therefore, it is imperative to collaborate with each department during the policy draft phase and to have those departments conduct a final review before the policy is distributed. Listed below are departments and specific policy topics that require collaboration.

IT

RIM policies often require electronic records with long-term retention to be accessible for the duration of their assigned retention period. This requires IT to have a data migration strategy that ensures the operating systems and applications needed to access the information remain available.

During the draft phase, the RIM professional should confirm that IT can meet the migration requirement; together, RIM and IT can then work out the policy language. If IT does not have the capability to properly migrate data, the requirement should not be in the policy until it does have that capability.

Internal Audit

For a policy to be successful, employees must comply with it. Further, there must be ways to measure compliance. Thus, the RIM policy should tell employees that compliance will be audited.

Often the RIM department will not have the resources to audit the policy and therefore will rely on the internal audit department. In such cases, the RIM professional should collaborate with internal audit to determine what needs to be audited, what constitutes compliance, and if that group has the resources to do the auditing.

Legal

RIM policies should include language on legal hold orders that has been approved by the legal department. Often, legal departments will conduct a full review to ensure a policy does not violate labor practices or laws.

Distributing the RIM Policy

After the RIM policy has been approved, determine the most effective method for distribution.

Distributing hard copies is the least recommended option. Because policies are periodically updated, employees might keep several versions and are therefore more likely to refer to outdated versions.

E-mail attachments are preferable to a hard-copy release, but they include the same risk: employees might electronically file the soft copy and subsequently refer to it even after the policy has been updated. E-mail attachments can include a request for employees to respond to the message, acknowledging their receipt of the policy.

The best method is to send an e-mail containing an intranet link to the policy. Some organizations use a database to track which employees have accessed the policy. When using database tracking, design the policy form to include an e-acknowledgement – a box the employee clicks to acknowledge receipt and review of the policy.

Auditing for Compliance

For a policy to be successful and credible, it must be enforceable and its compliance measureable. Organizational policies are frequently the focus of lawsuits and regulatory inquiries. Therefore, organizations should be able to provide evidence of establishing relevant policies, training employees to follow them, and auditing for employee compliance with them.

Audits also can provide insight into a policy's effectiveness. The results might indicate negative trends that can be analyzed and resolved.

The following elements should be included in an audit plan:

Audit Areas

Determine what policy components need to audited. Include areas that create the greatest potential for risks from non-compliance.

Testing

After identifying elements of the policy that need to be audited, establish a process that allows the auditor to accurately test for compliance.

Communication

Distribute a communication plan to all operations subject to the audit. The plan should tell employees when the audit will occur, what will be audited, and how to prepare for it.

Audit Findings Report

After the audit, the auditor must send a report of the findings to management. The report should communicate areas of non-compliance, the degree of organizational risks, and recommendations for resolving the issues.

Conclusion

An effective policy is fundamental to the success and credibility of a RIM program. Therefore, it is important to develop a RIM policy that is easy to understand, encompasses key components of the program, and provides employees with the guidance they need to ensure organizational content is managed in an efficient and compliant manner. **END**

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

Case Studies in Managing Change

Andrew J. SanAgustin

I was once a part of a RIM department that provided a textbook example of how *not* to launch a new tool and a new paradigm to go with it. Years later, I took part in a very successful implementation of a strategy change that included an end-user behavior reset and adoption. In this article, I discuss why one change-oriented project failed and the other thrived.

A Failed Approach

The textbook failure – *mea culpa* – was in transitioning to a new document management system (DMS) in a politically driven government agency with about 600 staff. There was a newly elected mayor and a newly appointed agency president.

The Environment

The electronic records infrastructure was made up of rogue file shares on numerous onsite servers. The program deliverable required a transition from this unregulated, decentralized approach to a centralized DMS with unified taxonomies and retention that would manage records in place and provide robust searching capabilities to find and share documents.

RIM Objective

Our task was to deliver this solution enterprise-wide. I arrived as the last member of a newly established records and information management (RIM) team. This wasn't to be merely a transition or migration of electronic records into a new solution, it would also be a paradigm shift in how people saved their work, with greater rigor around managing agency assets.

Further, most of the agency's work force members were seasoned users who had become accustomed to the way they had stored electronic records over the years. And that's what it essentially was – mere data storage.

Project Issues

I noticed issues from the be-

ginning that led to the project's failure, including these:

We didn't prepare adequately. The RIM leads frequently met with the vendor development team and information technology (IT), but not with the users. They did not plan introduction meetings or quick announcements at an all-hands meeting to introduce this project, even though it affected everyone. There were no change roadmaps, no behavior studies or analytics, or even heat maps to promote the transition.

We did not promote the project. This seemed to be a highly confidential project with little publicity even though it was to be delivered to all internal users. Data was pulled from the back-end for strategizing, but there was no transparency with those outside the team.

We did not allow users enough input. We selected individuals from different departments to be part of a pilot group to help develop and embrace this business shift, but these sessions were sporadic and driven by the solution, which didn't leave much room for input from the users. The message they received was, "Here is what you are going to do." This eventually led to one user saying, "This is simply not going to work and I won't do it."

We tried to do too much, too fast – and it was too complicated. As we created process workflow maps, I immediately noticed that our re-engineering plan was going to create culture shock for anyone creating and saving a document. We were trying to "boil the ocean" instead of taking small steps, building confidences, and collaborating on successes.

Despite the concerns I voiced several times, C-level staff took the aggressive stance that we were going to take advantage of the solution's sophisticated services. This meant changing users' practice of saving documents any way and anywhere they wanted to forcing them to use a micro-managed, metadata-driven repository. This was a complete disruption to the ecosystem. Users questioned the necessity of the change and asked how the benefit of making it would outweigh the burden.

It was a large burden: The design included thousands of retention categories, including more than 231 document types within a single department. To save a document to the tool, end users were required to populate 14 fields. I didn't find one person who knew where to find the retention schedule needed to categorize properly.

We were trying to "boil the ocean" instead of taking small steps, building confidences, and collaborating on successes.

It was clearly unmanageable and unsustainable. There were policy, enforcement, and compliance issues – and too many loopholes that allowed users to opt-out of the system. It was like seeing a dangerous iceberg, but being unable to maneuver around it to avoid catastrophe.

We did not collaborate well. A battle for control between the heads of the IT and RIM departments created contentious interactions that were uncomfortable, softened participation, promoted indecision within the change team, and caused confusion for the vendor. Better collaboration would have produced more clarity, helping bridge the gaps among technology, governance, and policy/compliance personnel.

We did not communicate well. The greatest issue was the lack of communication all around – between department leads and C-Level administrators, between the change teams and the vendor, and within the agency as a whole.

Lessons Learned

I would like to say that the marketing of the tool failed, but the truth is that there was no real plan. And, of course, I failed. As the new project manager, I implemented strict process strategies. When they were not well received, I changed gears and moved forward with a different approach.

This was a mistake. I should have stayed the course and worked harder to help others understand the process better. Instead, I deferred, letting fear and my desire to "fit-in" drive my actions instead of relying on my experience and knowledge.

I worked on this project for more than a year before I moved on. I heard later that the project was shelved indefinitely. I learned from this experience and promised myself that I would do things differently. Little did I know the opportunity would come sooner, rather than later.

The Success Story

I soon moved to another organization, where I served as the records manager of a mid-sized firm with multiple locations and some growing pains.

The Problem

Immediately, I discovered the need for a change in the way the physical records were being managed. My manager agreed, so I knew this issue was on the firm's radar.

The physical structure in this quasi-decentralized environment needed a facelift. The labels on the files and the folders needed to be updated to better serve the attorneys and secretaries and to improve efficiencies.

The Solution

The following describes how we made this a successful project:

We prepared adequately. I immediately put into place an action plan. I examined the file folder structure and put together a strategy for the roll-out. The structure had been used for decades, and a change would require careful maneuvering and input from the RIM team, the users, and IT.

I first shared my ideas with my manager, who had more than 20 years with the firm and could provide accurate guidance about the firm's culture. The manager approved my plan.

Next, I went to my RIM team, gave suggestions, and asked for members' input. The discussions were productive, partly because the team members saw the need for the change, but also because as their new manager, I was seeking their insight. This showed that I was sensitive to their feelings and was working to build trust and effect a team effort. I listened and continued an open dialogue throughout the process.

Once I had their support, I began researching the tools that would work with our existing systems and streamline the file creation process.

We communicated and collaborated well with others. Next, I sought input from the IT team, which was responsible for the project budget and could address any technical and connectivity concerns. In the process, I built relationships with IT staff and continued seeking their ideas and approval before moving forward. I already had the solution in mind, but I wanted the IT manager and team's buy-in so the implementation would have their ongoing support. With IT's blessing, I moved forward.

I was able to share general RIM knowledge and methodologies so they had a better understanding of how things worked and what we could do for them.

The next step was the most complex. I was in the position of an outsider facilitating a significant behavior change, so I knew I would need the support of the secretaries. In reality, the attorneys only wanted what they wanted when they wanted it; the secretaries were on the hook to deliver. I knew it wasn't going to be easy to win them over, as many had been at the firm for 15 to 20 years and had partnered with associates who had gone on to become senior members.

We asked for end user input. I began attending all of the secretary meetings. At the end of each one, I asked for a few minutes to discuss my plan, answer their questions, and seek their input. As a RIM professional, I knew what the best solution was, so I wasn't actually looking for guidance – I was simply working to make the key users feel they were part of the decision making process and had a stake in its success. I also made sure to demonstrate how these improvements would make their jobs easier:

- The files would have more reference information on them, rather than the murky "miscellaneous" label.
- Abbreviations would be eliminated, improving accurate retrieval by eliminating the need to "decode."
- The client and matter number would be added to the file for easy, at-a-glance reference.
- Labels would be color coded for easier identification and to minimize misfiling.

By working so closely with the secretaries, I was able to share general RIM knowledge and methodologies so they had a better understanding of how things worked and what we could do for them. In fact, I was also able to provide many of them access to the records management system so they could see their existing files for each matter, which helped them determine how to best categorize their new files.

The End Result

In the end, the results were impressive. There was a 48% increase in file creation time from the previous system, with 50% more real estate on the file labels. Most important, we had **100**% compliance and user acceptance for all offices. One secretary said, "It makes so much sense now. I am able to change the way I create files for my different attorneys and there's no confusion!"

In short, this project succeeded because we did the opposite of what had caused the earlier one to fail. The end users were included in the process from start to finish. Small steps were taken so as not to overwhelm anyone. And, of course, careful communication was a priority from day one to the roll-out. **END**

Andrew J. SanAgustin can be contacted at asanagustin@hotmail.com. *See his bio on page 47.*

Vendors, Products & People

BULLETIN BOARD

Global information governance (IG) leader **RSD** understands that IG is critical as businesses generate an increasing amount of sensitive data that requires policy management and compliance. Here are five IG items to remember:

1. **Initiate an IG steering committee and make sure IT is part of it.** All key organizational stakeholders must be represented, from records management (RM) to legal, compliance, security, AND IT.
2. **Get your corporate IG policies in order.** Create data policies that include retention, disposition, lifecycle, ownership, data loss prevention, security, privacy, classification, and metadata.
3. **Align people, processes, and technology.** RM solutions require support from IT, legal, compliance, and RM groups.
4. **Don't let IG take a vacation.** IG is an ongoing process; stay on top of policy maintenance and company information.
5. **Govern corporate records in the cloud.** Cloud-based repositories must be governed the same as on-premise records.

Learn more at ***www.rsd.com***.

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.naidonline.org***.

Recall Holdings Limited (ASX: REC), a global leader in information management, announced that it was awarded ISO/IEC 27001:2005 Management System certification by SRI Quality System Registrar on December 19, 2013. Recall is the first information management company to achieve ISO27001 Certification for all global operation centers. ISO/IEC 27001:2005 is a process-based certification recognizing organizations that can link business objectives with operating effectiveness. Recall's Global ISO27001 Certification demonstrates excellence in Information Security Management System (ISMS) planning, deployment, and provisioning services that support IT infrastructure to protect information and enable the associated secure service delivery processes to Recall employees and customers.

XACT DATA DISCOVERY (XDD) is an international discovery and data management company providing streamlined forensics, processing, hosting, document review, project management, and paper discovery services for corporations, law firms, and government agencies. XDD has offices throughout the U.S. and two locations in India, and recently added a domestic review option to its managed document review services. Visit ***www.xactdatadiscovery.com*** for more information.

NEW!
ARMA LIVE! 2014 Designation Academy offers certificate programs and certification exam prep courses to help you take your next steps toward a professional designation.

The 2014 Designation Academy will feature education from ARMA International, the International Association of Privacy Professionals (IAPP), the Institute of Certified Records Managers (ICRM), and the Information Systems Audit and Control Association (ISACA). Course listing at ***www.arma.org/Conference/2014/Education/DesignationAcademy.aspx.***

ARMA INTERNATIONAL®

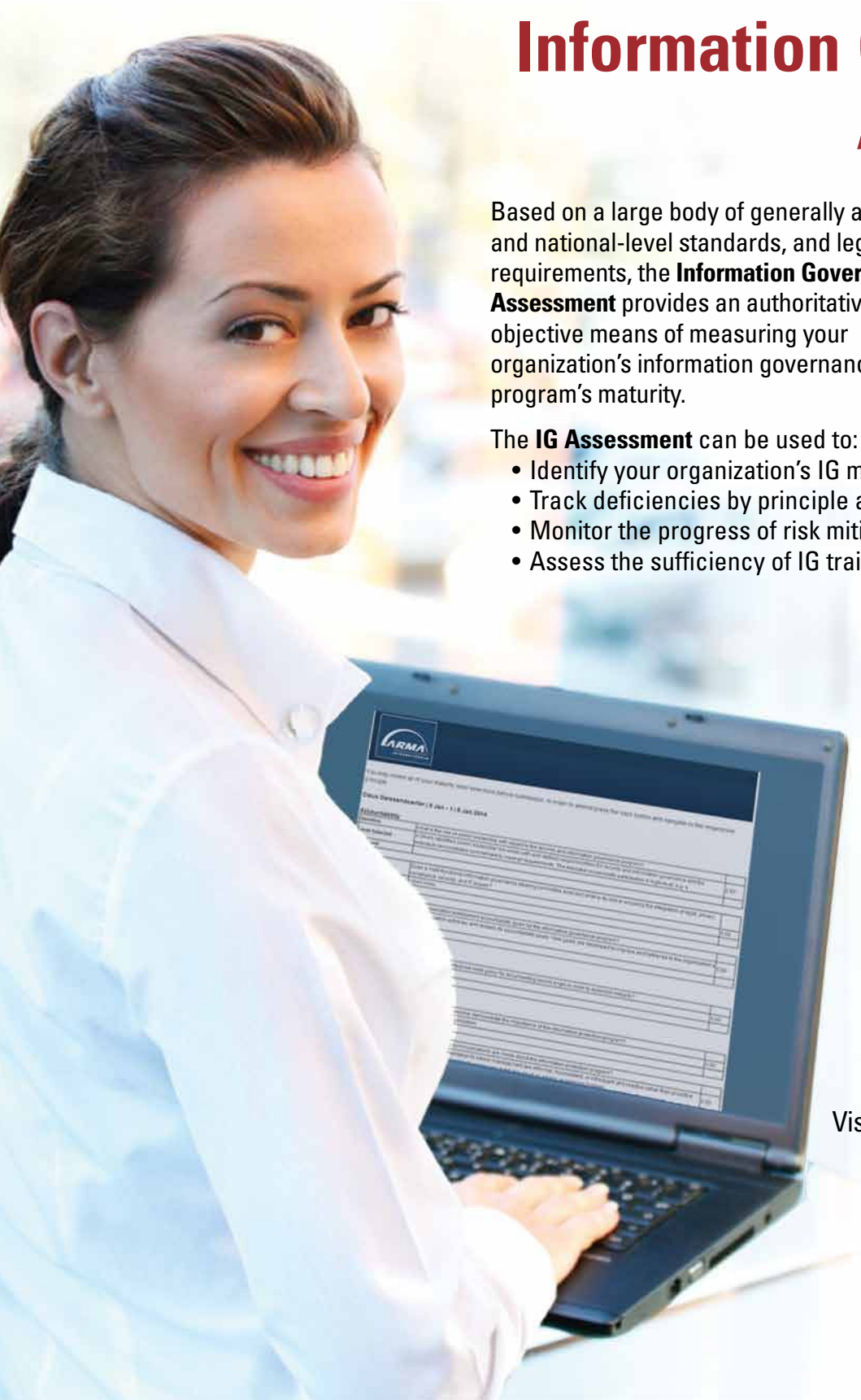
Introducing the official

Information Governance Assessment

Based on a large body of generally accepted practices, international- and national-level standards, and legal and regulatory requirements, the **Information Governance Assessment** provides an authoritative and objective means of measuring your organization's information governance (IG) program's maturity.

The **IG Assessment** can be used to:

- Identify your organization's IG maturity
- Track deficiencies by principle and overall score
- Monitor the progress of risk mitigation efforts
- Assess the sufficiency of IG training and documentation



Find out how the **IG Assessment** can work for you!

Visit ***www.arma.org/assessment***

Contact: **Elizabeth Zlitni**

+1 888.279.7378 (U.S., Canada)

+1 913.217.6015 (international)

Contact Information

AUTHOR INFO

GABLE HOKE LAYTON RICHARDSON SANAGUSTIN WYLIE

Top IG Tech Trends: Auto-Classification, Big Data Page 20

Gordon E.J. Hoke, IGP, CRM, is an independent consultant, speaker, and author whose focus is on information governance (IG). Evolving from content management and records management to IG, he proffers a business point of view and a risk-based approach. Some of his 300 articles, white papers, case studies, and other work has appeared in *Information Management, Healthcare Informatics*, and *Metropolitan Corporate Counsel*. Hoke has been a guest lecturer at universities and spoken at regional, national, and international conferences on subjects like persistent records, the synergy of ECM and RIM, and the Generally Accepted Recordkeeping Principles®. As a recent practitioner, he was manager of electronic records for Abbott Labs. Hoke can be contacted at *ghoke@mindspring.com*.

The Generally Accepted Recordkeeping Principles® Leveraging the Principle of Availability to Show ROI Page 26

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. 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*.

Cut Costs, Risks with Proactive Litigation Plan Page 34

Michael Wylie, J.D., PMP, is a Senior Project Management Specialist with Deloitte Transactions and Business Analytics LLP. He is a Project Management Institute-certified Project Management Professional with more than six years of experience in litigation consulting and e-discovery. He focuses on supporting federal agencies involved in environmental litigation. He attended the University of Delaware and the University of Richmond School of Law. He can be reached at *miwylie@deloitte.com*.

Kelli Layton, J.D., is a Discovery Senior Specialist with Deloitte Transactions and Business Analytics LLP. She is a litigation support and e-discovery professional focusing specifically on federal environmental claims. Layton attended the College of William & Mary and Washington and Lee University School of Law. She can be reached at *kelayton@deloitte.com*.

RIM Fundamentals How to Develop and Implement an Effective RIM Policy Page 38

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 in 2012 by Wiley. He can be contacted at *titansfan100@gmail.com*.

Case Studies in Managing Change Page 42

Andrew J. SanAgustin is a project manager at Microsoft LCA (Legal and Corporate Affairs) where he is working to implement global RIM strategies in line with professional business partners. An information governance professional for more than 20 years, he began his career in Washington, DC, where he attended the University of Maryland. His experience spans various industries with expertise in back-end system development and front-end user interaction, global policy and compliance, solution delivery, process/operations, standardization, change management, and electronic data management. San Agustin has authored several articles and been a speaker on records management topics. He can be contacted at *asanagustin@hotmail.com*.

AD INDEX

	Contact Information
Cover Tip	**HP/Autonomy** *www.autonomy.com/infogovcloud*
25	**Institute of Certified Records Managers** 518.463.8644 – *www.ICRM.org*
BC	**Iron Mountain** *www.ironmountain.com*
5	**NAID** *bit.ly/AAAnotification*
13	**Paralegal Today** **877.202.5196** - *www.paralegaltoday.com*
IBC	**Recall** 888.RECALL6 – *www.recall.com*
IFC	**RSD** *www.rsd.com*
3	**XACT Data Discovery** **877.545.XACT** - *xactdatadiscovery.com*

recall™
Your Information. Securely Managed.

"Your Passport to Information Management Freedom"

As organizations face increasing complexity with managing the expanding volume of physical and digital information and complying with industry and government regulations, they need a trusted partner that can help them. At Recall, we can help your business gain a competitive edge through the strategic, compliant, and economic use of information. Now that is Information Management Freedom!

Contact us at 1.888.RECALL6 (732.2556) or info@recall.com