INFORMATION MANAGEMENT

Embrace the Cloud, Big Data to Take Control of the Digital Deluge

More Than Paper: How RIM Can Influence IT and Shape IG

Five Essential Project Management Skills for RM and IG Professionals

INFORMATION MANAGEMENT

18

24

28

KEEP CALM AND DUE DILIGENCE

Data protection laws require due diligence when selecting service providers.

NAID's Services Selection Dashboard helps you achieve compliance.

http://directory.naidonline.org

Collaboration Ensures
RIM Career Success and Growth
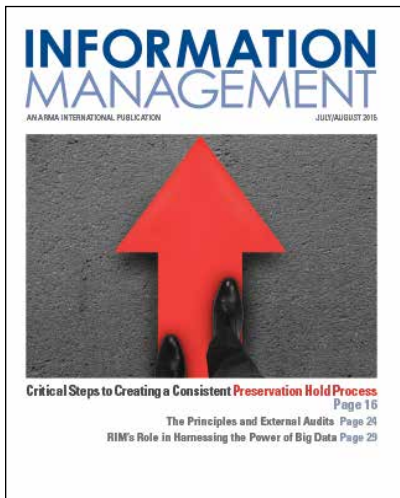
Wherever you are along the records and information management (RIM) career ladder, good collaboration skills are among the most critical to your being effective in your current role and to climbing to a higher rung. This issue's articles describe the valuable collaborative roles you can play in several business functions, including legal and technology initiatives.

Richard Vestuto, J.D., and Bill Piwonka write in the cover article that because legal holds "intersect with business units across the organization, including legal, IT, records management, HR, and compliance, among others," a steering committee comprising these stakeholders is essential to ensuring that the organization's preservation protocols are applied consistently.

In "RIMS's Role in Harnessing the Power of Big Data," author Kevin L. Dale, CRM, says RIM professionals can help solve the big data problems that come with disorganized, duplicative, poor quality data. "Big data can partner with RIM to reduce the costs of identifying, preparing, and analyzing data," Dale writes. Further, he says, "By creating synergies between RIM and the big data program staff and integrating RIM principles into all processes that 'touch' data, organizations can forge and maintain a sustainable path to the information governance (IG) needed to ensure high-value data."

As the foundation of IG, RIM must be effective to ensure positive outcomes from audits, Julie Gable, CRM, CDIA, FAI, writes in the Principles Series article. "An IG program based on the Generally Accepted Recordkeeping Principles® (Principles) and the Information Governance Maturity Model (IGMM) goes a long way to show that the organization takes its information management responsibilities seriously," she says. "Used well, these comprehensive tools guide in developing and sustaining an IG program that delivers reliably during even the pickiest inspections."

It also delivers in disaster scenarios. In "Planning for and Managing During a Paper Document Disaster," William R. Gulley, Jr. writes that RIM best practices are not only fundamental to an organization being prepared for a disaster, but also to it responding efficiently and getting a favorable insurance settlement.

To close the issue, an excerpt from the upcoming third edition of *Records and Information Management: Fundamentals of Professional Practice* by William Saffady, Ph.D., FAI, emphasizes that "Information is a collaborative initiative that requires the involvement and expertise of multiple stakeholders." In addition to records management, Saffady identifies IG stakeholders as IT, information security, risk management, legal, compliance, and business units that have or supervise control of information.

To be sure, RIM professionals who collaborate regularly with other IG stakeholders will broaden their skill sets, be sought out for their expertise, and find themselves in a good position for advancement.

How else can we help you excel in your career? Let us know at *editor@armaintl.org*.

Correction: In the print edition of the May/June 2015 *Information Management*, we should have included this disclaimer for "Avoiding the Hammer: Defensible Strategies for FRCP Proposed Rule 37(e)" by Katherine Aversano, J.D., and Joe Starnes, J.D.: "The views and opinions expressed in this article do not necessarily represent the position of the Department of Justice, the United States, or any agency thereof." We apologize for this error.

Vicki Wiler
Editor in Chief

GOVERNMENT RECORDS

Court Says State Workers Can Delete E-mails

State employees can delete their e-mails at their discretion, a Pennsylvania Commonwealth Court panel has ruled.

PG Publishing, the legal name of the *Pittsburgh Post-Gazette,* and other news organizations had sued the state in an attempt to require e-mails to be stored for up to two years. The paper filed suit after requesting information about a former education secretary's work as a special advisor and receiving only five e-mails in response.

If a state employee deletes an e-mail from an inbox, it is permanently deleted from the state server in five days, according to *Philadelphia* magazine. The *Gazette* argued that the policy allowing state workers to delete e-mails violated the spirit of the state's 2008 "right to know" law.

A three-person panel threw out the case and determined that the right to know law does not establish any records retention policy for state agencies.

"Simply, the RTKL (Right to Know Law) governs whether records currently in existence must be disclosed," the panel wrote in its decision. "Because (the law) provides that nothing in the RTKL affects that policy, PG Publishing has failed to allege facts demonstrating a violation of the RTKL."

PRIVACY

Data Collection Policy Prompts Privacy Concerns

On July 15, Uber's new policy overhauling its customer data collection practice took effect, prompting a complaint from the Electronic Privacy Information Center (EPIC).

Uber's new policy allows it to collect detailed information about its users and their contacts and to approximate customer locations based on nearby networks, even if users opt out of location sharing. The changes also allow Uber to store user data long-term and to send ads to customers' contacts without notification.

According to *Legaltech News*, one of the risks associated with the updated policies includes Uber's ability to collect information about when a customer's home will be unoccupied. This information also could be used to triangulate the details of users' private lives, making them possible targets of social engineering attempts.

The San Francisco-based company is no stranger to criticism over its collection of customer data, and EPIC has asked the Federal Trade Commission to bar certain provisions of Uber's updated policy. But, *Legaltech News* said, "the proverbial genie of private information collection has long been out of the bottle and new efforts from Uber are more a sign of things to come than an onerous harbinger of privacy abuse."

Consumers are paying attention. In a survey released in May by Pew Research, 93% of adults said they consider it important to be in control of who can get information about them. And companies are not shying away from collecting as much personal information as they can, experts warn.

Robert Neivert, chief operating officer of *Private.me*, told *Legaltech News* that he expects "companies to continue to push the boundaries of what they can get in terms of personal data, and only when there is backlash will this stop."

As for Uber, in a blog related to the policy changes, Managing Counsel Katherine Tassi said, "We care deeply about the privacy of our riders and drivers. It's why we're always looking at ways to improve our practices. In the last few months we have doubled the size of our privacy team, overhauled our data protection training for employees, published an external review of our privacy program and hired Joe Sullivan, a former cybercrime prosecutor, as our chief security officer."

Study Spotlights Business, Records Manager Gap

The gap between those who manage data and those who use it still exists, according to a survey released by Iron Mountain. "The Records Management Study," conducted by Coleman Parkes Research in January and February 2015, highlighted the gap between business leaders and records managers.

As reported at *www.baselinemag.com*, the study found that the role of records managers has shifted from organizing paper records to managing digital records, and they have had to evolve and apply new skills to effectively manage large amounts of digital data. Forty-eight percent of North American records managers said their role and responsibilities have changed significantly over the past five years, according to the survey.

The survey also found:

- The most important skill set for records managers is the ability to add value, insight, and analysis to the information they manage, according to 37% of business decision-makers and 25% of records managers.

- Only 20% of U.S. business leaders and 10% in Europe expressed total confidence in their organization's ability to extract value from information. However, 80% of records managers said they believe they are successful at this.
- Records managers aren't entirely sure what's expected of them. Only about 20% said they are clear on what they're expected to deliver to business divisions, including marketing, manufacturing, and finance. About 30% of business leaders in the United States and 20% in Europe said they have "complete understanding" of a records manager's function.

According to Sue Trombley, Iron Mountain's managing director of thought leadership, businesses must adopt a paradigm that allows each department to have direct access to the information it requires in order to extract value to meet its goals.

Information governance (IG) can help institute a new model in which instead of just dumping data on records managers, it will be assigned to the business groups that want to extract value from it. Both sides must work together "developing the skills demanded to navigate a shifting information landscape," she said.

Records managers and IG professionals who hope to prove their value to their organizations have a great opportunity to do that by becoming more involved in their big data, data mining, and/or knowledge management initiatives. Extracting value from information requires examining its actual content, learning how it is used, determining which parts of the organization could become more effective with a different kind of access to it, and then working with business units and IT to implement solutions to enhance its use.

IRS Used IM System to Conceal Communications

Documents released by the U.S. House Committee on Oversight and Government Reform reveal that Internal Revenue Service (IRS) officials used an instant messaging (IM) system, seemingly to prevent their communications from being archived, according to a July 28 article in the *Washington Free Beacon*.

The committee's documents show that IRS officials used an IM system called the "Office Communication Server" (OCS) that was not set up to archive messages.

Lois Lerner, former director of exempt organizations, had warned her colleagues to be cautious about what they said in e-mails; the agency had been asked several times by Congress to provide select e-mails. She asked IRS employees whether the OCS e-mails were saved, and when she was told they were not, she replied, "perfect."

The IM revelations come as several members of the House committee have called on President Obama to fire IRS Commissioner John Koskinen for obstructing the congressional investigation into the agency's targeting of conservative groups.

DoD Awards Contract for EHR System

Accenture, Leidos, and Cerner have won the Defense Department's behemoth electronic health records (EHRs) system contract, estimated to cost $11 billion through 2030. The award for the Defense Healthcare Management System Modernization (DHMSM) was for a fraction of that amount, however – just over $4.3 billion over 10 years if the options are exercised – according to an *FCW.com* report.

The winners have no easy task: DHMSM's goal is a single, commercial product featuring full interoperability with the Veterans Affairs' VistA health records system as well as private sector systems, while serving some 9.6 million service members, retirees, and dependents, *FCW.com* reported.

In addition, the system has to be deployable from the front lines of combat all the way home, and accessible to more than 150,000 professional providers at 55 hospitals and more than 600 clinics, said Jonathan Woodson, assistant secretary of defense for health affairs. The DoD continues to consolidate military health services, so the system must be compatible with about 50 legacy systems, gradually

Canada Passes New PIPEDA Provisions

Canadian officials are warning organizations that handle personal information to review their privacy policies and security safeguards to ensure compliance with the recently passed Digital Privacy Act.

The new provisions, which took effect June 18, are part of the Personal Information Protection and Electronic Documents Act (PIPEDA). They allow for significant fines and require breach notifications.

The *Financial Post* reports, "The mandatory notification provisions require organizations to notify the privacy commissioner, as well as potentially affected individuals, of a privacy breach 'as soon as feasible,' but only if there is a 'real risk of significant harm.'"

The mandate defines significant harm as humiliation, reputational damage, loss of employment or business opportunities, financial loss, and identity theft, according to the *Financial Post*. Companies also may be required to notify other organizations if doing so might mitigate the harm.

Penalties for knowingly violating the notification requirements can reach $100,000 per violation. The new provisions also state that the privacy commissioner is no longer required to keep private the confidential information gathered from complaints or others.

"This is likely to make organizations much less willing to make a full and frank disclosure to the Commissioner," advised lawyers Daniel Glover, Charles Morgan, Barry Sookman, and Kirsten Thompson in McCarthy Tétrault's e-Lert. "In addition, organizations dealing with the Commissioner will now have to be concerned about ensuring their trade secrets and confidential information are adequately protected (potentially through sealing orders or similar mechanisms) as well as ensuring that, by providing information to the Commissioner, they are not in violation of their agreements with third parties or requests made by law enforcement."

Other notable features of the legislation include targeted exceptions to the need for consent, and expansion of the scope of "business contact information" that will not be treated as "personal information."

replacing some and working with others, Chris Miller, DHMSM's program executive officer, told *FCW.com*.

DHMSM will be tested at eight sites in the Pacific Northwest starting in late 2016, with a full rollout by 2022, *FCW.com* reported.

E-DISCOVERY

Cost-Shifting Denied Despite Discovery Errors

In a long-running battle over the production of electronically stored information (ESI) in *Malone v. Kantner Ingredients Inc.*, the U.S. District Court for the District of Nebraska issued a memorandum and order saying that although the defendants may have made mistakes in their 2012 manual review of their ESI, they did not have to pay for the forensic review of their servers and external hard drive the plaintiffs conducted in an attempt to prove information had been withheld.

This ruling came in response to the plaintiffs' motion to show cause alleging that the defendants had destroyed or tampered with evidence, lied to the court regarding its existence, and failed to comply with an earlier court order that they were to locate and determine if the server imaging they had performed at the outset of the case was full and complete; produce invoices located on the server, the names of those who had access to the server, and all metadata related to the server; and produce sent e-mail recovered from their servers that was responsive. The plaintiffs also requested an order requiring the defendants to reimburse them for the forensic analysis.

The court's analysis said the defendants' legal counsel had confirmed that the data image from the shared server was full and complete. But, the legal counsel could not access the exchange server data because he did not have the needed connector. So, the defendants sent the servers to their forensic expert, who fully imaged the servers and provided a full copy of it to the plaintiffs.

The order said that by providing this image, the defendants complied with the court's order.

The court said that, at most, the plaintiffs had provided evidence of defendants' mistakes during their 2012 manual review, but this did not warrant imposing sanctions – "particularly where the plaintiffs now have full access to the server imaging."

In denying the plaintiffs' motion, the court stated that "human error is common when attorneys are tasked with personally reviewing voluminous electronically stored information."

INFO SECURITY

Do CISOs Belong on the Leadership Team?

Cybersecurity solutions company ThreatTrack Security reveals in its "CISO Role Still in Flux" whitepaper that chief information security officers (CISOs) have made modest gains in commanding corporate respect, but hurdles still exist.

The survey of 200 C-level executives shows that although 79% of respondents believe their board of directors already has or should have a cybersecurity expert, 75% said that the CISO did not "deserve a seat at the table" nor should it "be part of an organization's leadership team. In 2014, 74% viewed CISOs the same way.

The survey also shows that organizations have not given CISOs full authority over strategy and purchasing. Just 38% of the respondents answered that CISOs should be responsible and accountable for all information security strategies and cybersecurity technology purchasing decisions, down from 44% in 2014.

ThreatTrack Security points out that CISOs are still often viewed as scapegoats for data breaches; 47% of the respondents said CISOs "should be held accountable for any organizational data breaches," compared with 44% in 2014.

The whitepaper notes that these attitudes likely stem from executive views on what a CISO's primary function should be. More than half of respondents (51%) said the CISO position should be advisory and "provide valuable guidance to senior leadership related to cybersecurity," while just 27% said CISOs "typically possess broad awareness of organizational objectives and business needs outside of information security."

There is a silver lining, however, as more executives are open to the idea of CISOs taking roles outside of the position's normal purview. According to the whitepaper, 62% of executives said they believe their CISO "would be successful in taking another leadership role, outside of information security." That's up 23% over 2014.

UK High Court Rules Data Collection Legislation Unlawful

The UK High Court has ruled that the government's Data Retention and Investigatory Powers Act (DRIPA) is "inconsistent with EU law."

The legislation, which was rushed through by the coalition government last year, requires Internet and phone companies to keep their communications data for a year and governs how police and intelligence agencies can access it.

Parliament members Tom Watson (Labour) and David Davis (Conservative) challenged the law, arguing that its data collection methods are too expansive and not limited to cases involving serious crime as the law required.

The Guardian reported that judges found two big problems with the law:

1. It does not provide for independent court or judicial scrutiny to ensure that only data deemed "strictly necessary" is examined.

2. There is no definition of what constitutes "serious offenses" in relation to which material can be investigated.

However, despite ruling that the act should be "disapplied," the judges decided to suspend that order until March 31, 2016, "to allow time for the government to legislate properly." This means DRIPA will end only nine months earlier than it may have anyway, as the initial act contained a sunset clause for the end of the 2016 calendar year.

The government will now have to pass a new law that must become effective before the end of March. Government officials had already been working on a DRIPA follow-up, with the newest version coming in the soon-to-be-introduced Investigatory Powers Bill (IPB), according to *The Guardian*. While DRIPA was criticized as ambiguous, IPB is expected to provide a clearer standard.
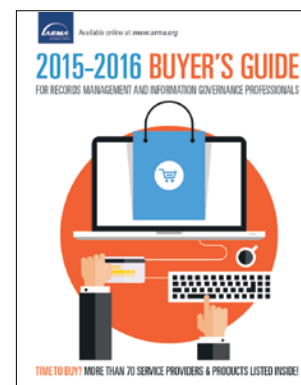
Court: Data Breach Harmful Even Without Identity Theft

The U.S. Seventh Circuit Court of Appeals ruled in July that customers affected by a data breach are likely to be injured even if they don't experience identity theft or other fraud.

In *Hilary Remijas, et al v Neiman Marcus Group LLC*, the court ruled against Neiman Marcus after a large data breach spurred a class-action lawsuit, which the court has allowed to proceed.

"Customers should not have to wait until hackers commit identity theft or credit card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur," Judge Diane Wood wrote in the ruling.

In 2013, hackers attacked Neiman Marcus and stole customers' credit card numbers. In December 2013, the retailer learned that some of its customers had discovered fraudulent charges on their cards. Between July 16, 2013, and October 30, 2013, about 350,000 cards had been exposed to the hackers' malware. But Neiman Marcus didn't announce the cyberattack until January 2014.

Karen Katz, Neiman Marcus Group CEO, said that of the 350,000 cards that may have been breached, only about 9,200 were subsequently used fraudulently.

The class-action complaints were consolidated in a First Amended Complaint filed in June 2014 by four customers.

Invoking Federal Rules of Civil Procedure, Neiman Marcus moved to dismiss the complaint for lack of standing and failure to state a claim. In September 2014, the district judge granted the motion because a litigant must "prove that he has suffered a concrete and particularized injury that is fairly traceable to the challenged conduct, and is likely to be redressed by a favorable judicial decision."

Neiman Marcus tried to argue that the plaintiffs' injuries cannot be redressed by a judicial decision because they were reimbursed for the fraudulent charges.

"That may be true for the fraudulent charges … but it is not true for the mitigation expenses or the future injuries," Wood said in the court of appeals decision.

Gretchen Freeman Cappio, an attorney at Keller Rohrback, called the Neiman Marcus opinion the new "high-water mark" in privacy protection for consumers and employees.

Judge Orders Sacramento to Save 15M E-mails

A Superior Court judge has ordered the city of Sacramento, California, to preserve 15 million of more than 80 million e-mails on its server, according to the *Sacramento Bee*.

Judge Shelleyanne W.L. Chang expressed concern that the petitioners' request for records represented "a moving target," and levied an $80,000 undertaking – an $8,000 bond that plaintiffs must pay the city to review the records. In June, Chang had granted a temporary restraining order stopping the city from deleting the e-mails, giving both sides time to work out an agreement.

Two Sacramento residents had filed separate public records requests in June for e-mails the city had planned to delete as irrelevant to the public record. One requested city e-mails from January 1, 2008, to the present, while the other requested e-mails that were to be deleted July 1 as part of the city's planned move to another e-mail system.

City attorneys argued that the requests were an effort to dictate how the city retains its information and that the plaintiffs' requests were overly broad and too heavy a burden for city staff to meet.

The attorney for the plaintiffs said the records request was not an attack on city policy, but an assertion of his plaintiffs' right to review the e-mails.

"There is no greater denial of a record than destroying it before someone can see it," he told the judge. "Public records are the public's property. We want access to as many records as possible."

Access to Information Requests Often Censored

Critics who have long complained that Canada's Access to Information program is ineffective and sluggish have new reason to criticize after an analysis revealed that requests for government records are often censored by federal agencies.

According to information from the government's open information portal, of 28,000 requests sent between June 2013 and July 2104, only 21% came back without redacted information. Fifty-seven percent were censored in some way, while the government said it could not find records in 18% of cases.

The data show that CSIS was by far the most secretive agency. During the one-year period, the intelligence service did not fully release a single government file. The Privy Council Office was a close second, with staff completely fulfilling only 3% of requests.

Canadian critics say U.S federal agencies grant full access to government records at a much higher rate.

For example, while only 26% of requests sent to Environment Canada were not censored, the full disclosure rate last year for its U.S counterpart, the Environmental Protection Agency, was 88%, according to the Center for Effective Government.

Of the 15 U.S departments profiled by the Washington-based think tank, 10 fully disclosed more than half of all documents requested. No major federal agency in Canada topped the 50% mark, according to *The Toronto Star*.

"The United States Freedom of Information system is far, far superior to our Access to Information system," Tom Henheffer, the executive director of Canadian Journalists for Free Expression, told the *Star*. "A lot of reporters, if there's some kind of international trade thing or something going cross-border between Canada and the United States, they'll try and file (a request) in Canada and they won't get anything back. They file in the United States and they'll have all the information they requested within a couple of weeks."

Henheffer admitted some information should be withheld to protect trade secrets and national security. But he called such widespread redactions by government agencies evidence of a "widespread clampdown on information in Canada."

Only 2% of the 28,000 requests were outright denied, the *Star* reported. But the rate was much higher among law enforcement and national security agencies, with the Royal Canadian Mounted Police refusing to disclose any information 9% of the time and CSIS 8%.

Conversely, 40% of the requests filed to Library and Archives Canada were completely fulfilled, the highest of all major federal agencies.

Canada's Access to Information Requests (%)
June 2013 – July 2014

57 Partial Disclosure

21 Full Disclosure

18 No Records Found

2 Records Excluded

2 Records Exemptes
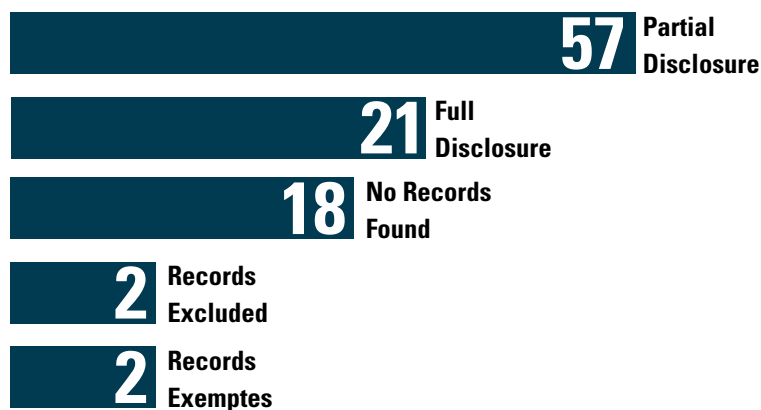
Note: Out of 28,000 requests, only 21% were returned free of redactions.
Source: *Toronto Star*

Senators Introduce Measure to Secure Connected Cars

Cars connected to the Internet may be creating new opportunities for cybercriminals.

Senators Richard Blumenthal (D-Conn.) and Edward J. Markey (D-Mass.) along with members of the Commerce, Science, and Transportation Committee, recently introduced a bill that would help protect connected vehicles. The Security and Privacy in Your Car (SPY Car) bill offers guidelines for the National Highway and Traffic Safety Administration (NHTSA) to regulate the private information collection and cybersecurity of networked vehicles, with the goal of making them safer for American drivers. The bill would also establish controls for car owners to enable them to manage their privacy and data-sharing options.

According to *Legaltech News,* connected cars are increasingly common on U.S. roadways. Research conducted by *Business Insider* shows that by 2020, 75% of the cars shipped globally will be connected to the Internet.

Hackers accessing owners' location data and other personally identifiable information is of primary concern right now, but as connected cars become more sophisticated, hackers could cause even more trouble. For example, a *Wired* article recently showed that persistent hackers can use internal computing systems to hijack a connected vehicle, a new form of vehicular sabotage that could become common without any security measures to prevent it. Clever criminals could theoretically ransom access to the vehicles by requiring wire payments to unlock them, or in extreme cases. take control from drivers.

DHS Officials Used Private E-mail

Despite the department banning private e-mail on its computers in April 2014, top U.S. Department of Homeland Security (DHS) officials have been using private e-mail from their work computers for more than a year, according to a top DHS official. Those top officials include Jeh Johnson, DHS secretary, and 28 of his senior staff.

The official also said that, despite the ban, top DHS officials were informally granted exceptions. When questioned, DHS's press secretary, Marsha Catron, confirmed it but said future exceptions are to be given by the chief of staff only. "Going forward," she said, "all access to personal webmail accounts has been suspended."

Johnson and the 28 other senior officials asked for and were granted informal waivers several times over the past year, the official said. Catron said exceptions were determined on a case-by-case basis by the chief information officer, Luke McCormack. DHS employees are permitted to use their government e-mail accounts for limited personal use.

It is uncertain whether any of the officials conducted DHS business on their private webmail accounts, but even if one work-related e-mail was sent or received, they could be in violation of regulations and laws governing the preservation of federal records, said Jason R. Baron, Esq., a former director of litigation at the National Archives and Records Administration.

Anne Weismann, executive director of the Campaign for Accountability and a former Justice Department official who worked on FOIA litigation, told Bloomberg that even by requesting the waivers at DHS, Johnson and the other officials created at least an appearance and opportunity for impropriety.

"How could they possibly justify exempting the secretary and the most senior people from the policy? You are allowing the people who are most likely to create e-mails that are most worthy of preservation to bypass the system that would ensure their preservation," she said.

Court Affirms Machine-Generated Evidence

A U.S. appeals court has ruled that machine-generated evidence is not hearsay in a ruling that allowed Google's satellite images to be used as evidence in a criminal case.

United States of America v. Paciano Lizarraga-Tirado concerns the January 2013 arrest by U.S. border patrol agents of Paciano Lizarraga-Tirado in Arizona near the U.S.-Mexico border. He was charged with re-entering the country illegally after being removed in 2012. Lizarraga-Tirado argued that the agents had crossed into Mexico to arrest him.

During the 2014 trial, the U.S. government introduced a Google Earth satellite image to prove the location of the arrest was in Arizona based on the coordinates recorded by the agent on a handheld GPS device at the time of the arrest. According to *Cronkite News*, the image included a digital "tack" of the coordinates that was automatically generated by the Google Earth program. Lizarraga-Tirado was convicted in July 2014.

Roger H. Sigal, lawyer for the defendant, claimed that both the satellite image on its own and the digitally added tack and coordinates were impermissible hearsay.

"Because a satellite image, like a photograph, makes no assertion, it isn't hearsay," Judge Alex Kozinski wrote in the June 18 Ninth Circuit ruling. "A tack placed by the Google Earth program and automatically labeled with GPS coordinates isn't hearsay. The hearsay rule applies only to out-of-court statements, and it defines a statement as 'a person's oral assertion, written assertion, or nonverbal conduct.'"

Kozinski also noted that the ruling does not convey that machine statements don't present evidentiary concerns given that a machine might malfunction, produce inconsistent results, or have been tampered with. "But such concerns are addressed by the rules of authentication, not hearsay," he said.

Library of Congress' Twitter Archive Project in Limbo

It was something to tweet about: In the spring of 2010, the U.S. Library of Congress (LOC) announced it had acquired Twitter's entire archive of tweets and was planning to make it all available to researchers.

But more than five years in, the project is in limbo, *Politico* reported. The library is struggling with how to manage an archive of half a trillion tweets, and no date has been set for it to be available.

LOC spokeswoman Gayle Osterberg said in an e-mail to *Politico* that the library is still making progress on the Twitter Research Access project.

"The Library has been working to index the collection and develop use policies," while having to balance "the size and dynamic nature of the Twitter platform" and "the resource realities of a public institution," she said.

The library also has created the Twitter Access Group, which includes technology, research, legal, and library science experts, and is charged with opening up the archive sooner rather than later.

But the project is a huge challenge. For example, the LOC must collect and store a static archive of tweets from Twitter's beginning in 2006 up to the signing of the agreement – about 20 billion tweets. It must also collect regular updates that number around 400 million tweets a day, determine how to index the tweets, and make them searchable to researchers allowed to access them in the library's reading rooms. The library, not Twitter, is responsible for figuring out how to manage the archive, as well.

Federal inspectors have complained about the lack of information on how the project is going, and the LOC missed its own unofficial public deadline for launching the project in June 2014.

E-DISCOVERY

Deloitte Survey Reveals Government Officials Confident About E-Discovery Skills

Deloitte's ninth annual survey of e-discovery in government agencies has found that government professionals are becoming more comfortable with discovery of mobile devices and more confident about their e-discovery skills.

For example, the 2015 survey found that 54% of the 149 respondents had collected and preserved mobile data. Last year, only 26% said they had done so. Twenty-eight percent of government officials, meanwhile, said that they had requested mobile data from opposing counsel in a case.

Deloitte's "Benchmarking Study of Electronic Discovery Practices for Government Agencies" also analyzed the growing trend of predictive coding and mobile device discovery in government cases and found that it isn't going to stop anytime soon.

The survey revealed that 27% of respondents used predictive coding in at least one case in 2015, up from 23% in 2014 and just 6% in 2012.

Chris May, the leader of Deloitte's government discovery sector, told *Legaltech News* that the increase in mobile discovery is related to the awareness of the amount of data stored on mobile devices, as well as the rise of BYOD in the workplace.

While the survey found a rise in the prevalence of e-discovery concepts, it also discovered a decrease in confidence in discussing e-discovery with opposing counsel. Just 42% of respondents felt that they were adequately prepared to discuss matters regarding e-discovery with opposing counsel, down from 56% in 2014. Still, government professionals reported feeling confident in their e-discovery skills, as 85% said they feel either more or as confident in their e-discovery skills as in the previous year.

It appears that agencies are making progress with e-discovery. While a large 78% of respondents reported that their agency is either somewhat or not at all effective in dealing with the challenges of e-discovery today, that number is down from 95% in 2012. In the survey, government officials identified the three biggest challenges they face today: insufficient manpower, insufficient time, and increasing volumes of data.

PRIVACY

Google Defies French 'Right to Be Forgotten'

Google has refused to follow an order from the French protection authority, the CNIL, to delete search results globally when users invoke their "right to be forgotten" online, risking fines from European countries.

In May 2014, the European Court of Justice ruled that European residents can request that search engines delete links about them from search engine results. Google complied and has since received more than 250,000 removal requests, according to its transparency report. It has accepted about 41% of them. In France, more than 60,000 requests have been made, more than from any other country, according to the *New York Times*. About half of those links were removed, according to Google.

However, it has limited removals to its European websites, such as *Google.de* in Germany and *Google.fr* in France, arguing that more than 95% of searches made from Europe are done through local versions of Google, Reuters reported.

Google warned that applying the right to be forgotten globally would trigger a "race to the bottom" where "the Internet would only be as free as the world's least free place." It is expected to fight the case in local courts – a process that could take several years, the *Times* reported. **END**

Embrace the Cloud, Big Data
to Take Control of the Digital Deluge

Highlights of the Forrester Research and ARMA International RM Survey, 2015

Cheryl McKinnon, IGP

2015 marks the seventh year that ARMA International and Forrester Research have surveyed records and information management (RIM) decision-makers in an effort to track the profession's key trends and challenges. In June, more than 500 respondents from around the world shared their perspectives through their survey answers. Here are some quick results of particular interest:

- North American representation was once again dominant: 69% of the respondents are from the United States and 24% are from Canada.
- 33% of the respondents work in government, topping all vertical industries.
- 31% of the respondents work in large enterprises that have more than a billion dollars in annual revenue.
- 20% of RIM programs report to IT, compared to 15% from last year's survey; 16% report to legal, 16% to a corporate services group, 11% to compliance, 9% to a line of business, and 24% to "other."
- The most frequently used vendors were Microsoft (for electronic records solutions) and Iron Mountain (for offsite storage of physical records).

The Pivot to IG Has Begun

RIM professionals are instigating change inside their organizations, as shown by their response to this new question in the 2015 survey: "Have you restructured or re-organized your RIM and/or IT programs to support an information governance [IG] strategy?" Nearly a third of survey respondents (32%) said they have (see Figure 1), and 34% said they plan to make this change over the next 12 months.

But there is still work to be done, particularly in the following three critical areas for IG success.

Stakeholder Alignment

Forrester notes a slight rise in the number of RIM programs aligned to IT – an indication that an alignment of policies and priorities may be on the horizon. This needs to continue, as evidenced by what respondents noted as two of their top three challenges: 29% said it is the lack of stakeholder alignment among IT, legal, compliance, and business decision-makers, and 29% identified it as lack of staffing or in-house expertise development (see Figure 2).

According to the survey, 59% of surveyed RIM professionals are included in their company's IT strategic planning, which involves such activities as requirements definition and vendor selection. This figure has remained relatively consistent over the seven years of the Forrester-ARMA survey, regardless of where RIM reports.

Governance Structure

Governance structures for RIM programs also remain in flux. While 28% of respondents said they have "a steering committee of senior stakeholders" to guide decisions, 24% said they have no formal governance at all. Other responses include "multiple, coordinated, cross-role committees" (11%), "a center of excellence or dedicated program team" (11%), and "multiple, disjointed cross-role committees" (9%). Just 4% rely on

legal to make decisions, while 3% let IT run the show.

Executive Sponsorship

Executive sponsorship for RIM programs continues to be influenced by legal: 41% report that the general counsel or the senior legal decision-maker is the key executive sponsor, particularly in the private sector. Of government respondents, 42% identify the CIO or the most senior technical decision-maker as the executive sponsor.

Digital Content Is Top IG Challenge

Respondents identified a new top challenge in this year's survey. Given a list and the opportunity to choose more than one challenge, 43% said their greatest challenge is "the volume of unmanaged digital documents outside of RIM control" (see Figure 2).

"Have you restructured or re-organized your RIM and/or IT programs to support an Information Governance Strategy?"

Yes — 32%
No, but plan to in the next 12 months — 34%
No — 27%
Don't know/ not applicable — 6%
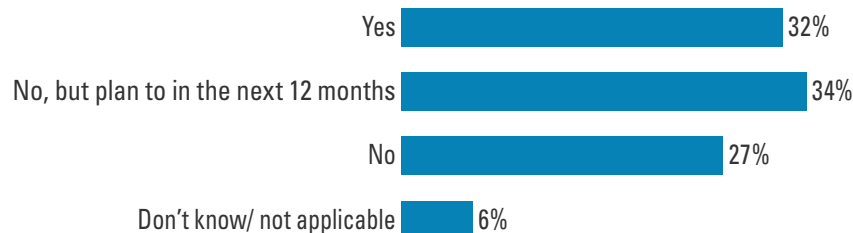
Base: 467 records management professionals

Figure 1.
Source: Forrester Research and ARMA International Records Management Online Survey, Q2 2015

Growing Volume

The unabated growth of electronic information provides enterprises with a wealth of opportunities to use data and captured knowledge to make better decisions, but it also presents an ever-greater burden to the information professionals who must organize and manage it.

Only 6% of respondents expect the volume of "non-record" documents to decrease over the next year, and only 1% expect the volume of electronic re-

"Which of the following represent the top records management challenges for your organization?"

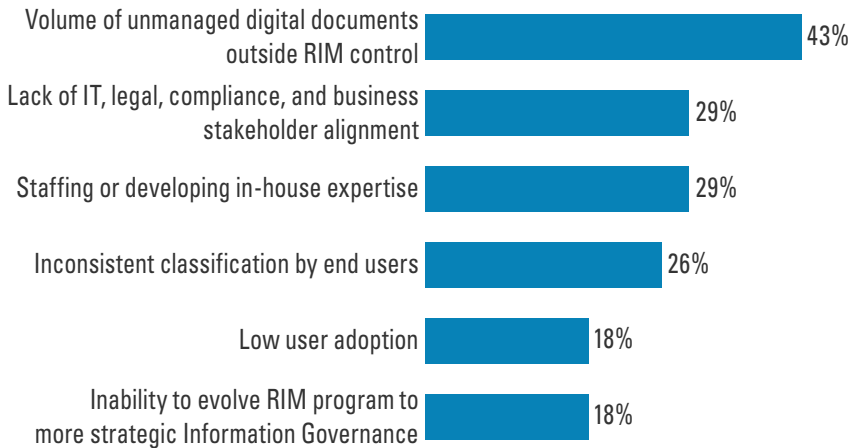| Challenge	Percentage
Volume of unmanaged digital documents outside RIM control	43%
Lack of IT, legal, compliance, and business stakeholder alignment	29%
Staffing or developing in-house expertise	29%
Inconsistent classification by end users	26%
Low user adoption	18%
Inability to evolve RIM program to more strategic Information Governance	18%

Base: 453 records management professionals

Figure 2.
Source: Forrester Research and ARMA International Records Management Online Survey, Q2 2015

cords to decrease. In comparison, 43% expect the volume of onsite physical records to decrease, and 34% project a decrease in physical records held in third-party storage facilities.

Emerging Sources

RIM professionals still are not adequately controlling the emerging sources of business records in their enterprise. An IG strategy must look beyond traditional sources of records and know where the organization's client-facing peers are communicating and creating content.

Enterprises largely have a handle on physical records, e-mail, and office documents but are failing with new content. Big data sources, social and collaboration sites, cloud-based file sharing tools, and mobile messaging apps are least likely to have any retention management implemented. For example, more than three-fourths (82%) of enterprises say they are applying retention policies to paper files, but only 18% claim to do so with their collaboration sites.

IG programs need to consider the "non-records" generated inside their organizations. Forrester sees a delib-

erate shift in technology investments as enterprises increasingly focus budgets on priorities like revenue growth and improved customer experience.

The apps and platforms that generate and hold data and documents – potential business records – will continue to change. External engagement with customers, citizens, or partners is driving new content management use cases, and governance now needs to extend to repositories beyond the firewall.

Big Data Presents Challenges and Opportunities

Big data is not just about size and volume; it is about new-generation analytic technologies that help organizations get more value from their information assets. Big data programs help shed light on customer behavior and reveal patterns that can be used to improve operations or detect problems. As shown at *https://solutions.forrester.com/big-data-ban*, Forrester has defined big data as "the practices and technology that close the gap between the data available and the ability to turn that data into business insight."

RIM's Current Role

Forrester included several new questions to understand what role, if any, RIM professionals already are playing in their organizations' big data projects. One-third of survey respondents reported that their organizations are pursuing a big data project, at least at a pilot level. A further 17% expect a big data program to be kicked off over the next year. A surprisingly high 75% of those who know about a big data program indicate that the RIM team is indeed part of the big data planning or governance discussions.

The primary roles RIM professionals play in a big data initiative are to:

- Advise on deletion or disposition policies (84%)
- Assess big data technologies as part of automated categorization projects (52%)
- Advise on security or privacy risks (48%)
- Consult with big data teams on sources of historical data to be included in analysis (34%).

Yet despite this apparent activity, only 6% have retention policies for big data, and just 7% have them in early implementation stages.

RIM's Evolving Role

RIM professionals must position themselves to be a key resource for their business and technical peers who want to understand what data is, in fact, available. A decade's worth of customer communications could be a tremendous asset to a customer experience program, yet in most enterprises it likely will lie untouched in an e-mail archive.

As big data initiatives begin to extract insights to inspire better, smarter actions, RIM professionals also must be prepared to rethink some of their retention policies. Disposal policies for data are often established based on diminished "business value."

But the promise of new-generation analytic technologies from the world

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.

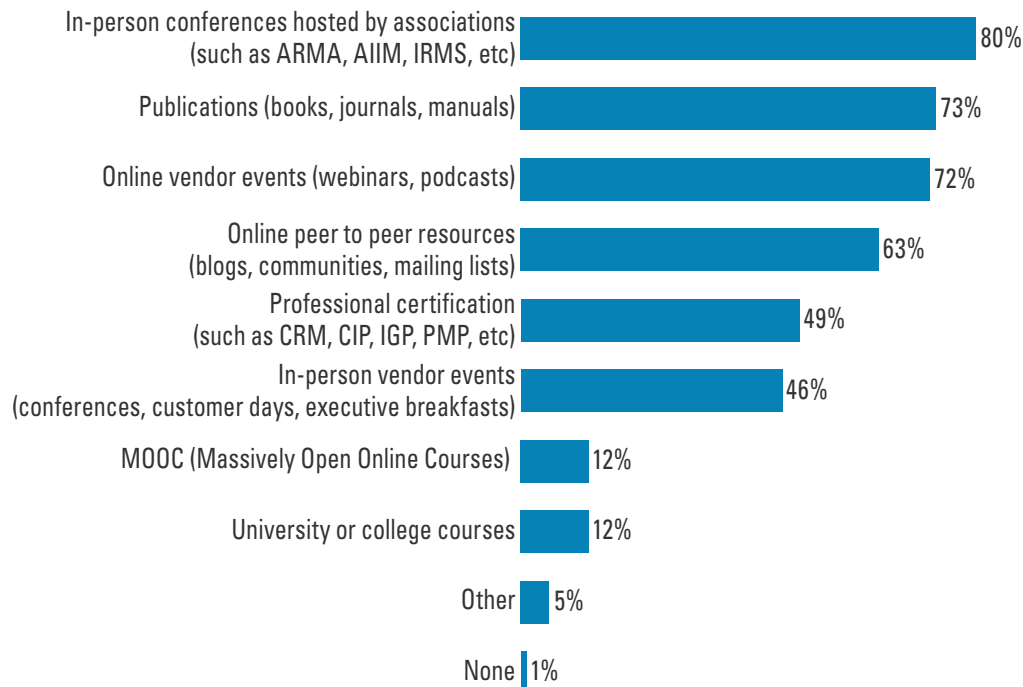**In a business world in which new jobs are increasingly competitive,** your designation as a Certified Records Manager (CRM) demonstrates that you have the experience and expertise to lead change and deploy best practices as they evolve in the RIM profession.

For more information about becoming a Certified Records Manager, contact (518) 694-5362 or visit www.icrm.org

ICRM®
Institute of Certified
Records Managers

"In which continuing education activities do you plan to engage to stay current on records and information management trends?"(Select all that apply)

In-person conferences hosted by associations (such as ARMA, AIIM, IRMS, etc)	80%
Publications (books, journals, manuals)	73%
Online vendor events (webinars, podcasts)	72%
Online peer to peer resources (blogs, communities, mailing lists)	63%
Professional certification (such as CRM, CIP, IGP, PMP, etc)	49%
In-person vendor events (conferences, customer days, executive breakfasts)	46%
MOOC (Massively Open Online Courses)	12%
University or college courses	12%
Other	5%
None	1%

Base: 357 records management professionals

Figure 3.
Source: Forrester Research and ARMA International Records Management Online Survey, Q2 2015

of big data has the potential to shake up how business value is defined. Individual documents or e-mail messages may have little or no business value over time, but when they are combined with other data sets or in large volume, their business value can be extracted in new ways.

Forrester advises RIM professionals to understand where these new analytic projects are in place and the data sources being mined, and to be prepared to adjust traditional assumptions about retention rules.

Keys to the IG Evolution

Enterprises that fail to invest in their employees' skills will find it difficult to shift to a more digital business. While 48% of respondents expect their RIM budgets to increase over the next year, a larger share of the budget is expected to go into technology investment than into people:

- 43% expect to increase their spending to upgrade RIM technologies.
- 30% will spend more on new technologies.
- Only 27% expect to spend more for in-house staffing.

Many organizations do not plan to hire additional full-time RIM resources.

Continuing Education

With limited budget and plans to expand internal teams, continuing education will be essential if IG programs are to be started, be rebooted, or reach the next level of maturity.

Attending in-person conferences hosted by professional associations such as ARMA, AIIM, or the International Records Management Society is considered the top continuing education activity (see Figure 3). Most (80%) respondents plan to engage in some

form of in-person event.

Other highly valued activities for continuing education include publications (73%), online vendor events (72%), and peer-to-peer forums such as blogs or mailing lists (63%).

Professional Certifications

Nearly half (49%) of respondents plan to pursue such professional certifications as the Certified Records Manager (CRM) designation, the Information Governance Professional (IGP), or the Project Management Professional (PMP).

The CRM designation is considered the most valuable by survey respondents, with 44% of participants describing it as "very valuable." Only 13% described the CRM as having "no value." Second on the list is the relatively new IGP designation, with 29% describing it as "very valuable." The third most-valued certification

is the PMP, with 21% of respondents rating it highly.

The key motivations for professional certification are quite personal. Nearly half (41%) of respondents chose "personal interest and self-improvement" as their top driver for pursuing a designation. Finishing second, at 19%, was the benefit of differentiation during a job or contract search, and finishing third, at 15%, was getting a direct benefit such as a promotion or pay increase. Only 9% of respondents indicated they would not pursue a professional certification.

Advice for RIM and IG Professionals

With seven years of joint research with ARMA now completed, Forrester sees several constants in the results that suggest actions RIM and IG professionals should take.

Embrace the Cloud

Cloud adoption remains in a nascent stage, with security, privacy, and other compliance risks holding back adoption. This worry over cloud services lingers despite the increasing adoption of the cloud for other content-rich use cases, such as archiving and e-discovery review.

RIM professionals may have to look at the cloud through a fresh lens; many of the leading enterprise content management – and thus records management – vendors are aggressively moving to a cloud-first roadmap.

Extend IG to All Content

Optimism about ongoing technology deployments is still high, although budgets remain tight, and there's not much hope of expanding teams. Confidence in retrieving today's records some 15 years from now is rising, which demonstrates hope on the digital preservation frontier.

The gap in applying retention policies to emerging sources of business content, however, puts a question mark on the future retrieval and preservation of these data types. Regard-

ing risk, Forrester continues to see that RIM professionals are not extending consistent governance practices to the social, cloud, and collaboration tools that their client-facing colleagues have embraced.

With the top RIM challenge described as "the volume of unmanaged documents outside of RIM controls," the gap between governance and chaos is at risk of widening.

RIM professionals need to home in on where communication and content creation patterns are shifting inside their enterprise, and they must be prepared to extend their purview to the collaborative, social, and mobile world of today's digital business.

This is the promise of IG as a "holistic strategy for using and managing information to meet business objectives." It's not just about documents vs. records anymore. **END**

Cheryl McKinnon, IGP, can be contacted at cmckinnon@forrester.com. *See her bio on page 47.*

More Than Paper:
How RIM Can Influence IT and Shape IG

Phyllis Elin

Records and information management (RIM) professionals are perfectly positioned and have the requisite expertise to play an advisory role that will help ensure that their organizations are governing all information in all formats in ways that will reduce costs and risks. To step into that role, though, they must forge a collaborative relationship with IT. This article describes how professionals can do that by demonstrating that they understand IT's perspective and can help them meet their unique challenges and goals.

The rapid, dramatic shift from physical records to digital documents is evident in nearly every industry, leading many records managers to question the viability of a career based on managing a format that is decreasing in volume. Although organizations continue to produce volumes of paper that require expert management, job descriptions in records and information management (RIM) are evolving. This is good news because RIM professionals are perfectly positioned to serve in an expanded role – that of information governance (IG) advisor.

In a 2010 blog posting, Gartner analyst Debra Logan writes that Gartner defines IG as "the specification of decision rights and an accountability framework to encourage desirable behavior in the valuation, creation, storage, use, archival, and deletion of information. It includes the processes, roles, standards, and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals." A RIM professional lives and breathes every word of that definition as it applies to physical documents, but the same knowledge and expertise are typically not inherent to IT managers, who are responsible for managing the ever-expanding ocean of digital data.

Because compliance regulation and privacy laws – and associated penalties for violating them – apply equally to both paper and digital formats, classifying information based on format is an outdated practice. Forward-thinking organizations see their information as either managed or unmanaged, and RIM professionals are well-versed in this distinction.

They can ensure that information is properly managed through its life cycle and troubleshoot IG gaps that IT managers probably would not recognize. The key to un-locking this insight is making sure a relationship between RIM and IT is created and maintained; nurturing such a collaboration, though, requires more than RIM simply sending IT a list of suggestions to follow.

Bridging Technology-Created IG Gaps

Technology facilitates vast amounts of digital data, which has spawned an industry aimed at creating solutions to help manage it. As a result, organizations have a variety of management options, including cloud storage, software as a service (SaaS), digital imaging, data dictionaries, SharePoint®, e-discovery retrieval, and more. Unfortunately, an abundance of options often obscures the unique needs every company has and subsequently creates gaps in IG implementation. As IG advisors, RIM professionals can help organizations understand such lapses and offer corrective advice in any of the following areas.

Decentralized Documents

It is common for organizations to have dozens of siloed data repositories across their networks. Only certain departments have access to this data, making it difficult for IT to locate it during a regulatory audit or when a legal matter requires discovery.

RIM Expertise: RIM professionals know all too well the risks associated with decentralized records and are experts at creating infrastructure to maintain access for appropriate parties. They can offer real-life examples of the risk reduction associated with data centralization.

Gluttony for Data

Cloud storage is convenient and relatively inexpensive, which, theoretically, sounds like a win-win. However, when faced with limited storage for the growing moun-

tain of data that IT managers own, many will opt to buy more storage instead of managing or reducing their data footprint. Having too much data increases risk and is a speedbump to attaining IG health.

RIM Expertise: Retention schedules are typically not IT's forte, as evidenced by the "throwing storage at the problem" solution. Records managers can offer guidance in creating full lifecycle data management strategies that reduce the risks associated with excess data. In turn, organizations are less likely to fall out of compliance, and if a breach occurs, there is much less data for cyber criminals to compromise.

Non-Uniform Classification

Digital documents are often created and saved with classification methods that differ from solution to solution, department to department, and person to person. Such a wide variance leads to data retrieval inefficiency and expands risk because there is no intuitive path to pinpointing what data exists.

RIM Expertise: Given their deep-rooted familiarity with IG implementation, RIM professionals can quickly identify whether sensitive data exists in a physical record based on the method by which it has been named and filed. Their expertise in crafting intuitive, uniform classification policies

can translate into helping IT understand the type of data in a digital document and where to find it. Additionally, very important documents are no longer "floating" around on the network, waiting to be accessed by unauthorized personnel or, worse, a cyber criminal.

Stagnant Policies

Technology becomes obsolete at a rapid pace, requiring frequent updates and replacements to information management systems. However, many organizations fail to update the policies that dictate how data should be handled in the new systems, leading to gaps in IG standards.

RIM Expertise: RIM professionals are well-versed in developing and updating policies and can share examples of how to lessen data risk by simply revising guidelines. Additionally, rules and regulations that dictate information management – and, in turn, IG strategies – also evolve. The knowledge that records managers possess in updating policies can help promote greater compliance.

Forging the Relationship with IT

IG implementation would be easy if trust between records managers and IT could be initiated by a records manager saying, "I have a wealth of experience, and these are really great ideas." But the reality is that records and IT managers often have two very different points of view with differing objectives and simply do not interact on a regular basis. In short, relationships – and the trust that accompanies them – take time. Given IT's growing importance in driving business, building the relationship is more important than ever to ensure IG health. Records managers should consider the following strategies for creating and sustaining a successful RIM-IT partnership.

Speak the Language

To initiate a conversation – and to adapt to the records manager's evolving role – it is critical to have a continually expanding knowledge of technology and its impact on digital data. While IG theories may translate from physical to digital information because regulations apply equally to both, RIM professionals may need to adjust the ways they implement best practices to better relate with IT. Understanding where idea transference may hit a snag and having a greater appreciation for IT-specific challenges and obstacles will give records managers more credence when they make suggestions.

Collaborate

Participate in projects and committees where interaction and problem-solving with IT can occur. While such projects may be peripheral in nature to IG, getting face time and working with IT managers will help facilitate relationship-building. More organizations are creating IG steering committees; this is a perfect example of a collaborative effort that empowers records managers to share their knowledge with IT managers. Records managers can also reach out directly to seek ways to work together.

Present Ideas to Decision-Makers

Present IG best practices to influencers, even if IT isn't included. If a case can be made to C-level executives, then records managers' influence and ideas can migrate to other departments. Raising visibility through internal thought leadership is key to getting important ideas taken more seriously and put into action.

Leverage Legal Knowledge

RIM professionals have been trained to be keenly aware of legislation and industry regulations that impact information management at all times. Sharing news of new regulations or trends with appropriate stakeholders not only positions the records manager as an expert but could serve as the proverbial "foot in the door" for dialogue with IT. To that same end, RIM professionals often have a more direct relationship with legal and can serve as a liaison among all three departments.

Becoming Trusted Advisors

RIM professionals are – and will continue to be – doing more than utilizing their expertise to manage physical documents. To maintain visibility and remain a business-critical component of an organization's strategy, they must identify synergies that exist between their wealth of information and the ways information is and will be managed.

The role's evolution will require them to be trusted advisors in trouble-shooting IG challenges and creating policy that helps organizations avert risk and maintain compliance. By developing meaningful relationships with IT and other decision-making departments, RIM professionals have the power to help implement IG best practices in the largely undefined realm of digital data management.

Phyllis Elin can be contacted at recall@mslgroup.com. See her bio on page 47.

> Raising visibility through internal thought leadership is key to getting important ideas taken more seriously and put into action.

174 Strong. And Growing.

Congratulations to these
Certified Information Governance Professionals

Elizabeth Adkins
Pey-Jia Angell
Christine Ardern
Deborah Armentrout
DeAnna Asscherick
Randy Aust
Christie Baird
Salvador Barragan
Christopher Beahn
Richard Berlin
Margaret Boeringer
Isabel Bracamontes
Susan Burd
Doug Caddell
Stacie Capshaw
Melissa Carlis
Diane Carlisle
Laurie Carpenter
Alexander Carte
Mark Carter
Anita Castora
Elizabeth Castro
Tod Chernikoff
Carol Choksy
Vicki Clewes
Julie Colgan
Bud Conner
Dani Cook
Marvin Cross
Kristen Crupi
Becky Darsch
Lisa Marie Daulby
Nicholas De Laurentis
Melissa Dederer
G. Derk
Deborah Dotson
Christina Doyle
Sandra Dunkin
Priscilla Emery
Sofia Empel
Tony Epler
Debra Farries
Elizabeth Farthing
Carol Ann Feuerriegel
Glenn Fischer

Matt Fisher
David Fleming
Patricia Franks
Rhonda Galaske
Caroline Gallego
Stephen Garner
Charles Garrett
Irene Gelyk
Sue Gerrity
Kimberly Giertz
Susan Goodman
Joshua Grisi
Komal Gulich
Jocelyn Gunter
Allen Gurney
Michael Haley
Grace Hammar
Joshua Hargrafen
Paula Harris
Charles Herbek
Margaret
  Hermesmeyer
Caroline Higgins
Gordon Hoke
Patricia Huff
Janice Hulme
Bethany Hynes
Leigh Isaacs
Mary Frances Janicik
C'Les Jensema
Chris Johnson
Todd Johnson
Deborah Jostes
Deborah Juhnke
Soo Kang
Andrew Keller
James Kennedy
Anju Khurana
Ellie Kim
Michelle Kirk
Tamara Koepsel
Greta Krapac
Peter Kurilecz
Tera Ladner
Ronald Layel

Anna Lebedeva
Gilles Legare
Donnell Long
John Loveland
Eric Lynn
Cindy MacBean
Rudolph Mayer
Brian McCauley
Stephanie
  McCutcheon
Cheryl McKinnon
James Merrifield
Sandy Miller
Dana Moore
Dermot Moore
Rafael Moscatel
Linda Muller
Jen Murray
Stephen Murray
Joe Nadzam
Lindy Naj
Peggy Neal
Lee Nemchek
Sheri Nystedt
Carolyn Offutt
James Owens
Eleanor Ozaeta
Lewis Palmer
Jadranka Paskvalin
Alan Pelz-Sharpe
Graham Pescod
Denise Pickett
Debra Power
James Presley
Cindy Pryor
Fred Pulzello
Tony Ratcliffe
Joshua Rattan
Jessica Rickenbach
Deborah Rifenbark
Carol Rittereiser-
  Coritt
David Rohde
Donna Rose
Kathryn Scanlan

Danna Schacter
Teresa Schoch
Terry Schrader
Karen Schuler
Mary Sherwin
William Silvio
David Skweres
Michael Smith
Natalie Spano
Brian Starck
Jason Stearns
David Steward
Melissa Suek
Paula Sutton
Marjorie Swain
Sheila Taylor
Robin Thompson
Brian Tretick
Susan Trombley
Nathan Troup
Brian Tuemmler
Martin Tuip
Amy Van Artsdalen
James Vardon
Jennifer Watters Farley
Bridgett Weldner
Erik Werfel
Steven Whitaker
Kristi Whitmore
Jesse Wilkins
Marc Willemse
Dylan Williams
Steven Williams
Rick Wilson
Terri Wilson
Brett Wise
Jennifer Witt
Kristin Wood
Robin Woolen
Jeffrey Yawman
Andrew Ysasi
Ryan Zilm

Application deadlines: Nov. 14, 2015 and March 28, 2016.

Register today at *www.arma.org/igp.*

Five Essential Project Management Skills
for RM and IG Professionals

Anna Lebedeva, IGP, PMP

The just-released results of the Forrester Research/ARMA International RM Survey conducted during the second quarter of 2015 show the Project Management Professional (PMP) certification is considered one of the most valuable credentials for records and information professionals to earn. Whether you're pursuing the PMP or not, this article identifies and tells you how you can develop and use several project management skills that will help you be more successful in your career.

The success of an organization's information governance (IG) program depends on the contributions and collaboration of people in many functional areas, including records management (RM), legal, compliance, information technology (IT), and information security. As the conductor who often will lead this orchestra of cross-functional staff, an IG professional must have many skills to ensure that the members play in tune, rather than create a cacophony.

Having project management (PM) skills is one key for leading the orchestra to deliver a great performance in implementing complex IG initiatives. This is because whether they are building an IG program, developing a retention schedule, implementing a legal hold process, or developing strategies for defensible disposition, IG professionals are probably running multiple projects, or initiatives, concurrently.

Among the PM discipline's knowledge areas that can directly benefit IG professionals in their daily work are these five:
1. Gathering business requirements and defining scope
2. Building and managing a project plan
3. Managing stakeholders and communications
4. Managing timelines, risks, and issues
5. Managing change

This article examines each to show how they can help IG professionals drive IG initiatives to successful completion.

Gathering Business Requirements, Defining Scope

Gathering business requirements is the first activity to undertake once an IG initiative is approved, although it might sometimes be necessary even before approval. Without well-defined requirements, the IG professional cannot plan the project, the IT team will not know what to build, customers will not know what to expect, and there will be no way to validate that the end result will satisfy all stakeholders' needs. In fact, one of the most common reasons projects fail is because business requirements were not defined or were poorly defined.

The business requirements lay the foundation for:
1. Defining scope
2. Testing deliverables
3. Measuring success

Without well-defined requirements, the IG professional cannot plan the project, [and] the IT team will not know what to build…

Defining Scope

Business requirements define the scope of a project and enable everyone involved to agree on what will be delivered and what the end result will be. Requirements always need to be documented clearly, in great detail, and in understandable and unambiguous language to allow better estimates of the timeline, budget, and resources, and to provide a method for controlling requirements changes.

An essential part of defining the scope of an IG initiative is identifying deliverables that are out of scope. Thus, if the project, for example, is about implementing an enterprise content management system, but the web content management module is not part of the initial implementation, it needs to be clearly stated in the scope statement. All stakeholders should formally accept the scope statement before the project progresses.

Testing Deliverables

Business requirements are also used to build a test plan, with each requirement becoming a testable item. If IG professionals do not reconcile re-quirements against deliverables, they most likely will end up with a system or a process that is useless. The consequences of that will be severe, resulting in wasted company resources, lost time, unmitigated risks, and missed opportunities, to name a few.

Not every IG initiative will have a formal testing phase, but there will always be some form of validation. In either case, it is important to test or validate as early as possible in the project's life cycle in order to identify gaps in requirements and take corrective actions without impacting the timeline, cost, and scope.

Measuring Success

The dependency among timeline, cost, and scope is one of the most fundamental PM concepts. Called the "triple constraint," it is a way to monitor the project and measure its success.

Project success and failure also depend on how the project is perceived. If the wrong business requirements were addressed and the project was set up to deliver the "wrong thing," it may be considered a failure even if everything is delivered on time and within budget and scope.

Gathering the appropriate business requirements ensures that the project delivers business value, leads to happy customers, and increases the adoption rate for the IG program – which is what IG is all about.

Building and Managing a Project Plan

The project plan is one of the most important tools in managing the IG

initiative. Created during the planning phase and constantly updated, the project plan contains the tasks needed to accomplish the scope of the IG initiative, the time allotted to complete the tasks, and the resources required to perform the tasks. The project plan content and format will vary based on the type and complexity of the IG initiative.

Before a project plan can be created it is important to gather the prerequisites; business requirements and scope statement are vital inputs because they enable the creation of tasks.

Identifying Tasks, Resources

In order to derive tasks from the business requirements, IG professionals will need help from those who will do the work. First, learn what the roles and responsibilities of the initiative's stakeholders are. Next, obtain resources and commitments, including black-out periods, such as holidays, vacations, conflicting project timelines, and other events that may divert resources from working on the IG initiative.

After defining tasks, identify the dependencies between the tasks because these drive the project timeline. The more tasks that can be scheduled in parallel, the faster the project will be completed.

Creating a Timeline

Create a preliminary timeline when building a project plan; this can be as simple as a breakdown of project phases. The most common phases are planning, designing, building, testing, implementation, and post-implementation support; however, not every initiative will have all of these phases. Give each phase a high-level estimate of completion in months or weeks.

It is ideal when the timeline can be based on the project scope and available resources, but this may not be possible, such as when the project end date is imposed by senior management.

There also can be a hard date for implementation, such as the contract expiration date for software, which will drive the implementation date for a new solution. In that case, project planning starts from the end date and the project phases are planned in reverse order.

Sometimes tasks must be rescheduled to run in parallel until they fit within the fixed timeframe. Or, it may be concluded that the timeline is too aggressive and cannot be met. Beware of unrealistic deadlines: working under constant and excessive timeline pressure will lead to project failure.

Finally, it is important to build some contingency into the baseline project plan before it gets published. Things do not always go as planned, and buffers need to be added to critical tasks to allow for the unknowns.

Responding to Changes

Completing a project plan is a big accomplishment, but the job does not end there. Be prepared to constantly adjust the plan because of changes and issues that arise. To be a valuable tool in managing the IG initiative, the project plan needs to be current and responsive to changes.

Managing Stakeholders and Communications

Stakeholders are people or organizations that are positively or negatively affected by the IG initiative; they may include customers, project sponsor(s), project team members, vendors, and others. Key stakeholders are identified in the project planning phase, and their needs and expectations are analyzed and converted into business requirements. It is important to document communication needs for each stakeholder group, including communication format, content and level of detail, method, frequency, escalation, and feedback process.

Following Up

Just because tasks were assigned to resources weeks or months ago does not mean they will remember what

> Following up enables the project manager to perform his or her most important duties, which are to communicate, coordinate, and motivate the project team.

they were asked to do and when they were supposed to do it. Following up is one of the most critical communication skills IG professionals should have. It is both a science and an art.

Following up is a science because there needs to be a system for keeping track of task status (e.g., checking in at mid-point in task duration and two days before it is due). Insufficient follow up will result in issues not being surfaced and addressed early. It is an art because it takes interpersonal and organizational skills to bring stakeholders together and make things happen. Following up enables the project manager to perform his or her most important duties, which are to communicate, coordinate, and motivate the project team.
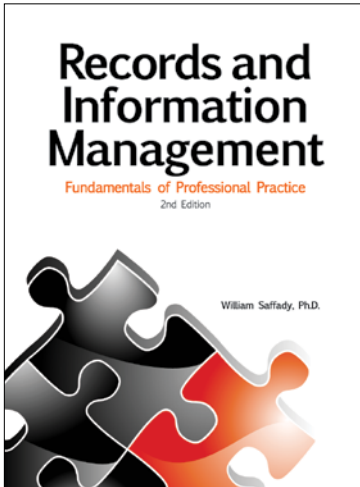
Escalating Issues

Escalating issues to management is another important element of communications. It is always advisable

to privately inform the manager in charge of the area with issues about the plans to escalate first. It is never a good idea to surprise the manager with the "bad news" in front of a wider audience that might include his or her superiors. When done properly, escalations will help the IG professional by engaging the management team to do its jobs, which are to make tough decisions, remove roadblocks, and provide organizational resources.

Reporting Project Status

Truthful project status reporting is a key to successful communications. Beware of *green shifting*, or reporting project status positively when there are obvious indications of serious problems. For example, it is better to report that the e-mail retention implementation initiative is trending from green to yellow status because of anticipated business resource availability issues than it is not to say anything and suddenly report red status later.

If IG professionals choose to do the latter, not only could they be questioned as to why they did not see this issue arising, they also could lose an opportunity to either set the right expectations or get management's support to mitigate the situation, preventing the red status.

Continuing LEssons Learned

It is recommended to formally conductt lessons learned sessions after each project phase in order to realize process improvements while the project is still ongoing.

Finally, it is important to talk to stakeholders informally and be open to feedback any time during the life of the IG initiative, as that is the only way to know what is really going on.

Following up, escalating, reporting status, and sharing lessons learned can be difficult skills to master, but they are necessary to being effective as a project manager, as they can make or break the project

Managing Timelines, Risks, Issues

The key to managing the project timeline is being proactive; always be on alert for things that can go wrong and act on them as soon as they become known.

Keeping the Timeline

When delays happen and time buffers built into the project plan are used up, there are only three things IG professionals can do to stay within the original timeline, provided they have management's approval:
1. Reschedule some tasks to run in parallel.

2. Reduce scope by removing some requirements.
3. Add more resources, although this does not always work and may result in lower team performance.

As desirable as it is to keep the original timeline, do not make the timeline the driving force. Compromising the quality of deliverables to meet the timeline will result in a failed project.

Extending the Timeline

If none of the above measures is workable, the last resort is to *re-baseline*, or officially extend the timeline. Extension may be the only solution warranted by significant issues or scope changes. For example, an organization implementing a cloud-based records management system may discover during testing that – due to a missed or ambiguous requirement – it cannot apply new retention rules on existing data in the event of retention schedule changes. The new system cannot go live until this issue is resolved, so there is no choice but to extend the timeline in this situation.

Managing Risks

Risk management is an important activity that starts during scope definition by engaging stakeholders to identify risks and creating a risk log. The next steps are to analyze risks, document their probability and impact on the project, and create a risk response plan.

Among the risk response strategies that can be utilized are to:
1. Mitigate – Take measures to reduce the probability and/or impact of a risk.
2. Transfer – Shift the negative impact of a risk to a third party, such as the vendor. This does not elimi-

Compromising the quality of deliverables to meet the timeline will result in a failed project.

nate the risk; it just transfers the ownership for risk management.
3. Accept – Take no action, leaving the project to deal with the consequences if risk occurs. The most common acceptance strategy is to use a contingency reserve built into the project budget.

Risks management, like many PM activities, should continue throughout the life of the IG initiative. Existing risks can be changed to a higher or lower probability and impact as the project progresses, new risks may surface and have to be added to the risk log, and risk response strategies may need to be updated.

Managing Issues

The difference between a project "risk" and a project "issue" is that a risk is an uncertain event that may or may not happen, and an issue is an event that has already happened and made some measurable impact on the project. Issues are tracked in an issues log.

It is critical for IG professionals to communicate about issues candidly.

Beware of *confirmation bias*, which is dismissing information that might show the project has issues. This may make the IG professional look good in the short run, but it will set the project up for failure in the long run.

Issues should not be seen as a "bad thing"; they happen on every project and are sometimes outside of anybody's control. Stay in constant communication with stakeholders, look out for early signs of potential issues, promptly engage the right resources to work on issue resolution, and keep management and customers informed. Don't be defined by the issue, but how you handle it.

Managing Change

Managing change is a critical activity because projects rarely run according to their original project plans. Rather, the project plan, scope statement, and other deliverables must be maintained by continuously managing the changes.

Many organizations create a change management board consisting of the project sponsor(s), customers, and other stakeholders. Change requests must be documented and include impacts to timeline, cost, risk, and staffing. To maintain the integrity of the project plan and timeline, it is vital to ensure that resources work only on approved change requests. It is recommended to have a formal change management process that outlines the steps for how changes will be requested, reviewed, and approved/rejected.

Monitoring Scope

The most notable and impactful type of change that should be monitored closely is scope change. Uncontrolled scope changes, often referred to as "scope creep," can make a significant negative impact on the project.

Be very careful if customers or other stakeholders try to "squeeze in" additional requirements after the project scope has been approved.

For example, if the IG initiative is to implement a social media archiving solution and somebody states that it should integrate with the e-discovery application, verify if such integration was included in the scope statement. If it was not, document this requirement as a change request, and go through the change management process for approval.

Preparing Stakeholders

Change management includes preparing stakeholders for the changes that the project will bring. Stakeholders can be divided into three categories:

1. Active supporters – individuals who will accept the change and actively support it
2. Fence sitters – stakeholders who will take a "wait and see" approach
3. Active blockers – people who will be uncomfortable with or critical of the change

The change management goal is to convert active blockers and fence sitters into active supporters. Try these tactics:

- Ask active supporters to coach their peers and their direct reports on the change.
- Recognize and thank active supporters publicly.

- Surround active blockers with active supporters.
- Have active blockers meet with their direct supervisors to review the case for change.

Everyone responds to change differently, and sometimes all it takes is clearer communications. Incorporate training, create an open door policy, avoid jargon and management speak, be transparent about what is known and unknown about the change, be empathetic, and let all know that their voices are heard and that everyone needs to get through the change together.

.
Reaping the Rewards

Managing project requirements, scope, plan, timeline, risks, issues, stakeholders, communications, and changes requires important PM skills every IG professional should work to develop. Be patient; it certainly takes experience and maybe a few failures to build PM strong skills. It is worth the effort, though, paying rewards in terms of the IG program's return on investment, satisfied customers, and personal fulfillment. **END**

Anna Lebedeva, IGP, PMP, can be contacted at anna.lebedeva@peoples.com. See her bio on page 47.

Making a Business Case for the **Principles**

Julie Gable, CRM, FAI

The purpose of developing a business case is to outline the difficulties of a current situation, tell how these will be overcome if certain actions are taken, and illustrate how the future will be better because of a commitment of resources in the present. An important part of the business case is the justification for expending resources, usually showing an expected return on investment (ROI) over a given time period, such as three to five years.

Most records and information management (RIM) professionals are adept at describing the difficulties caused by unmanaged and ungoverned information, as well as the actions that need to be taken to resolve the difficulties and how implementing an information governance (IG) program will benefit the organization. The piece of the business case that may be difficult for them is justifying the resource investment and quantifying the ROI.

The Principles, IGMM as Basis for IG

Integrating the use of the Generally Accepted Recordkeeping Principles® (Principles) and the Information Governance Maturity Model (IGMM) into specific information-related efforts can be done on an *ad hoc* basis with little financial expenditure since both are available for free from the ARMA website (*www.arma.org/ principles*). The Principles Series of articles presented in each issue of *Information Management* magazine over the past four years provides a wide variety of guidance about how that can be done.

The Principles and the IGMM are methodologies based on international standards and broadly accepted best practices, providing a unified underpinning and common understanding of what things need to be done and how. Standardized methods like these point the way forward; they don't usually require an elaborate business case.

While there are optional RIM and IG resources an organization may wish to invest in, such as the Next Level assessment tool and the Information Governance Professional (IGP) and Certified Records Manager (CRM) certifications for staff, the costs for these are generally within the range of departmental budgets and hardly require cost justification measures. However, using the Principles to develop and implement an IG program across the enterprise *will* call for a business case to be presented, as this will require collaboration among RIM, IT, legal, and business units; involve a contribution of brain power from levels above, below, and including middle management; and demand executive endorsement.

One of the strongest arguments for the Principles is that they underpin and contribute to other efforts that are designed to deliver tangible and intangible results. Nowhere is this more evident than in IG, where the Principles provide the unifying thread in what may look like piecemeal projects proposed from narrow viewpoints.

Because the Principles are the foundation of IG, implementing them is closely interwoven with business cases for IG. In turn, IG's justification is based on risk reduction, cost reduction, or increased productivity. More recently, business cases based on asset value are emerging as well.

IG: Risk Reduction

The perceived importance of IG varies from one organization to another. IG has greater weight where external challenges such as liability lawsuits and regulatory examinations have a high probability of occurring and can have serious consequences when they do. Yet risk reduction is not limited to billion-dollar corporations. The risk of scandal, amplified by news organizations and social media, and the damage to reputation, haunt non-profits and government alike.

Information Cost Statistics

Up to 80% of IT infrastructure is used to support duplicate data.

(Source: "Big data: The next frontier for innovation, competition, and productivity." McKinsey Global Institute, 2011.)

70%-75% of IT budget is spent on infrastructure maintenance (to maintain and operate the organization, systems, and equipment).

(Source: "Debunking Two Myths About Tech Budgets," Forrester Research, 2014)

Storage cost per GB is down, but investment in infrastructure to support storage has doubled from $2.5 trillion to $5 trillion in the last seven years.

(Source: "IDC Digital Universe Study," IDC, 2011)

Cost to perform e-discovery on 1 TB of data is approximately $18,000.

(Source: "Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery," Rand Corp., 2012)

The average information worker spends 48 to 72 minutes per day locating information. The opportunity cost of wasted time, based on $75,000 in annual salary and benefits per employee, is $19,372 per employee per year.

(Source: "Bridging the Information Worker Productivity Gap," IDC, 2012)

The IG business case based on risk reduction and mitigation is easiest after the worst has already happened, and the resulting fines, discovery failures, or loss of public trust are keenly felt. The Principles then become a guideline for remedial action rather than for proactive prevention.

Where catastrophe has not occurred, efforts aimed at reducing the risk of compliance, discovery, or public relations disasters may be regarded simply as an insurance policy, an unavoidable overhead expense that should be limited. After all, no organization wants to buy more insurance than it needs.

However, if the probability of occurrence is low, or if the potential consequences are not considered significant, the organization may choose to accept the risk, and a business case for IG based on risk reduction alone will not succeed. In this culture, the promise of avoiding costs that may or may not occur is not a strong enough impetus for an outlay of time and resources today.

IG: Cost Savings, Productivity

The stronger driver for IG, and the more quantifiable contribution of the Principles, may be an approach that bases the business case on productivity gains and cost savings. Here, the business case is less about occasional outside risks than it is about day-to-day operations. Eliminating duplication of effort, information silos, and widely varying metadata within business processes can have an impact on costs and productivity.

Efficiencies, gains, and savings are best showcased against a backdrop of overall business strategy. If the company intends to grow through acquisition, then a business case showing the cost impact of acquired systems on administrative and backup costs makes sense because acquisitions will be ongoing.

The trade-off is that, while this kind of business case is likely to merit management attention, it is much more difficult to produce. Success or failure depends on whether the organization insists on *hard-dollar*

savings, that is, the demonstrable elimination or reduction of out-of-pocket costs, versus *soft-dollar savings*, namely cost avoidance or the reduction of time spent on recurring tasks.

Underlying all of this is the ability to gather accurate information about current costs, no easy feat for information management-related tasks. Industry statistics may be helpful in general (see sidebar "Information Cost Statistics"), but management is better convinced by the organization's actual cost data and realistic, conservative savings estimates.

IG Business Case Examples

In reality, IG business cases don't fit neatly into one category or another. This is because work on one aspect of IG has implications for all the others. Information has a life cycle – creation, use, storage, retention, and disposition or preservation – and the Principles reflect this. While all of the Principles make important contributions, some come to the fore more than others depending on what objectives

the business case hopes to achieve.

At a minimum, the typical business case requires a cohesive narrative covering a current situation, its cost impact on the organization, the proposed solution and its expected benefits. What's usually missing is a discussion of whether the organization is in a position to implement the proposed solution successfully. In short, whether there is a sufficient level of foundational maturity, a fact sometimes lost in the rush to fix a problem and the enthusiasm for new technology.

The Business Case for Risk Reduction, Cost Savings

It's common that a business case based on risk reduction may have implications for cost reduction as well, as shown in the table "The Business Case for Risk Reduction and Cost Savings."

The level of IG maturity needed to realize true benefit from defensible destruction is significant. The business case for risk reduction and cost savings relies on the Principles of

Retention and Disposition, the yin and yang of IG policy. Retention and Disposition, in turn, must be based on a careful understanding of laws and regulations (Principle of Compliance). To have credibility and legal weight, the retention schedules must have organizational approval, which implies that there is a governing body in place to do so (Principle of Accountability). Retention and disposition policies must be documented and their existence and purpose widely made known to employees through training (Principle of Transparency). Without any one of these, "deletion" isn't defensible at all.

Note that in one real-world case, a company that could not destroy anything spent more than $1.75 million annually in various tiers of cloud storage and backup fees. Even a modest reduction of 20% would have saved $350,000 annually.

Opponents of destruction on the grounds of possible spoliation would do well to read the federal court decision *In re Pradaxa Products Liability Litigation*. Although Pradaxa's manu-

The Business Case for Risk Reduction and Cost Savings

Issue	Current Situation	Cost/Risk Impact	Proposed Solution	Expected Benefit	Foundational Maturity Required
E-discovery	Search for requested information returns voluminous results. Can't place reliable legal hold on information needed for litigation, so must suspend destruction of all records company-wide	Cost: Expense of contract legal assistance with relevance review. Cost: Expense for IT to administer storage and backup of all information, while lawsuit progresses Risk: Finding a "smoking gun" that could have – and should have – been destroyed. Risk: Spoliation of evidence through inadvertent destruction.	Defensible deletion – the automatic deletion of records no longer needed for compliance, legal, fiscal, or operational purposes, tempered with strong legal hold capabilities.	Reduced discovery costs Reduced ongoing storage and backup costs	Retention schedules and disposition processes are defined, approved, documented, disseminated, and enforced. Legal hold process is in place and integrated into critical systems. Communication of legal holds are routine. (Principle of Compliance)

The Business Case for Productivity

Issue	Current Situation	Cost/ Risk Impact	Proposed Solution	Expected Benefit	Foundational Maturity Required
Decentralized systems hamper information capture, retrieval, and use.	Product codes change as business processes progress. Duplicates of essential documentation are in various systems throughout process. There is inconsistent indexing. Staff must know who knows (use personal network) to retrieve needed document.	Cost: Engineers, manufacturing, quality control, and others spend hours looking for and validating documents. Risk: Potential quality issues if superseded specifications are given to contract manufacturers, fillers, or packers. Risk: There are potential issues with regulatory auditors, where applicable.	With a consolidated document management system, all product-related documentation is accessible via the web. Limited self-service access can be granted to suppliers and contractors on a need-to-know basis.	Less time is spent searching for information. Time spent administering multiple systems is eliminated. "Silos" of information are eradicated. Risks of providing wrong information are reduced.	There must be consistency of metadata used for indexing and for chain of custody. (Principle of Integrity) Users must be able to distinguish among copies, duplicates, and official records. (Principle of Availability) The organization must be able to control and limit access to proprietary information. (Principle of Protection)

facturer was sanctioned for several issues related to its legal hold process, the court found that it did not willfully destroy evidence because it heeded its own well-documented retention and disposition policies. (See *www.technologylawsource.com/2013/10/articles/privacy-1/defensible-deletion-no-spoliation-where-defendant-destroyed-emails-and-documents-pursuant-to-its-records-retention-policies/*

The Business Case for Productivity

In the business case for increased productivity, the Principles of Availability and Integrity underlie successful implementation of the proposed solution. A single document management system makes sense, but better findability and retrieval speed won't be realized until metadata discrepancies are reconciled and obsolete or redundant document versions are removed. Just as important is a way to protect proprietary information stored in the cloud, particularly if suppliers and contracts will be granted access to it.

Organizations that insist on hard-dollar savings may expect to see elimination of jobs as the result of productivity gains. Where cost avoidance is acceptable, the ability to demonstrate reduced time in information capture, search, retrieval, use, and maintenance will be sufficient. One real-world company was able to demonstrate savings in excess of $2 million over a five-year period through the elimination of duplicative efforts among the 25 people charged with capturing, finding, retrieving, and maintaining these records.

The Future Business Case for IG

Regardless of whether an IG business case emphasizes risk reduction or cost savings, the underlying Principles of good governance remain unchanged. They assist in identifying problematic issues and facilitate the underlying structure that enables solutions to be put in place.

Work on the Principles paves the way for intelligent application of time, money, and human resources and amplifies the benefits expected from any proposed solution. They broaden horizons by considering all aspects of governance, beyond the immediacy of technology acquisition.

The greatest justification for IG may be yet to come, however. New areas of opportunity based on the value of information assets are emerging. Content analytics make it possible to identify patterns of purchase, use, satisfaction, and other knowledge from document-based, unstructured information.

Some firms see this as a way to increase revenues by producing new products or inducing others to joint ventures on companion products. Yet, early adopters of analytics technology are finding that one major obstacle to success is the inability to trust their own documents because they are inaccurate, incomplete, and often not timely, which are all matters of Integrity. It seems the role of IG based on the Principles will continue to expand for some time to come. **END**

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

Best Practices for
Governing Social Media Content

John T. Phillips, CRM, CDIA, FAI

The personal and professional use of social media is continuing to proliferate in homes and enterprises including across international boundaries. According to the Statista website, Facebook alone was estimated to have about 1.94 billion monthly active users as of the second quarter 2015, and many online social networks, such as Google+, Twitter, and Instagram, had several hundred million users each as of August 2015.

A recent study by the Pew Research Center, according to its July 14 online article "The Evolving Role of News on Twitter and Facebook," found that 63% of both Twitter and Facebook users get a major portion of their news from these sources.

Social Media Challenges

As these online communications environments slowly replace e-mail as the preferred electronic communications medium, they are creating a variety of digital records types – YouTube and Pinterest, for example, are specifically designed to share video and image format data – and they are storing records for information-sharing and collaborating.

The impact of this change in communications mode and information-

sharing architecture creates unique challenges for ensuring that personal and workplace-originated electronic records are created, stored, and retained in a responsible manner.

These challenges can be met with an effective information governance (IG) program, the enterprise-level strategic information management perspective that most thoroughly encompasses records retention guidelines, regulatory compliance mandates, information privacy concerns, intellectual property protection, and litigation document production requirements.

IG for Social Media

IG – which ARMA International defines as "A strategic framework

Because IG is an evolving arena, it currently has few examples of extensive enterprise-wide implementation, so there is a need for sharing new perspectives and lessons learned, especially with regard to incorporating social media records into IG plans. This article provides technical information about social media platforms and suggestions for governing their use that should be of value to organizations that are struggling to extend IG controls over their social media-based information assets.

Social Media Technologies

Social media applications like Facebook and Twitter usually reside on multiple servers hosted by third parties in the Internet "cloud." They

agreements (EULAs) and service level agreements (SLAs) are designed or modified to be in compliance with their IG program plans.

EULAs and SLAs

EULAs and SLAs form legally binding contractual relationships between software users and vendors of the software. The EULAs that organizations must sign with cloud vendors rarely address data management; vendors make their own design decisions to maximize their software platform's responsiveness, ease of maintenance, and robustness of security.

Typically, software vendors employ EULAs to limit the use of their software by prescribing the software

[EULAs and SLAs] present opportunities for proactively addressing issues that will arise during IG initiatives, especially with respect to the ownership and management of electronic records.

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 with and contribute to the organization's goals" – is rapidly developing. Its concepts are embedded into the Generally Accepted Recordkeeping Principles® (Principles), which are available at *www.arma. org/principles*.

The implementation of the Principles and IG practices depends on the state of an organization's information management policies, IT systems architecture, and business environment. This means that the best way to approach IG will vary based on the organization's recordkeeping mandates, litigation profile, risk management priorities, and social media systems architectures.

also can be hosted and maintained internally by organizations wanting to reap the rewards of browser-based collaboration functionality while maintaining access control and security themselves. But, most organizations today want to benefit from lowering their IT systems infrastructure maintenance costs through taking advantage of cloud-based applications that intrinsically offer worldwide access, minimal IT infrastructure installation costs, and little or no internally required help desk or training challenges.

This approach to outsourcing IT support and maintenance infrastructure means that organizations do not directly control the recording and retrieval of their electronic records that are being stored on third-party systems. This means they must ensure that their end user license

buyers' rights with respect to operation, archiving, sale, and backup. SLAs are arranged by both software buyers and software vendors to specify mutual expectations for system performance, data ownership, and service support levels.

EULAs are generally created by software vendors, whereas end users often initiate and negotiate SLAs. Although both are contractually binding, they may need to be enforced through legal system actions, thus creating business cost and operational hazards for those organizations trying to exert their rights under these agreements.

These types of agreements present opportunities for proactively addressing issues that will arise during IG initiatives, especially with respect to the ownership and management of electronic records.
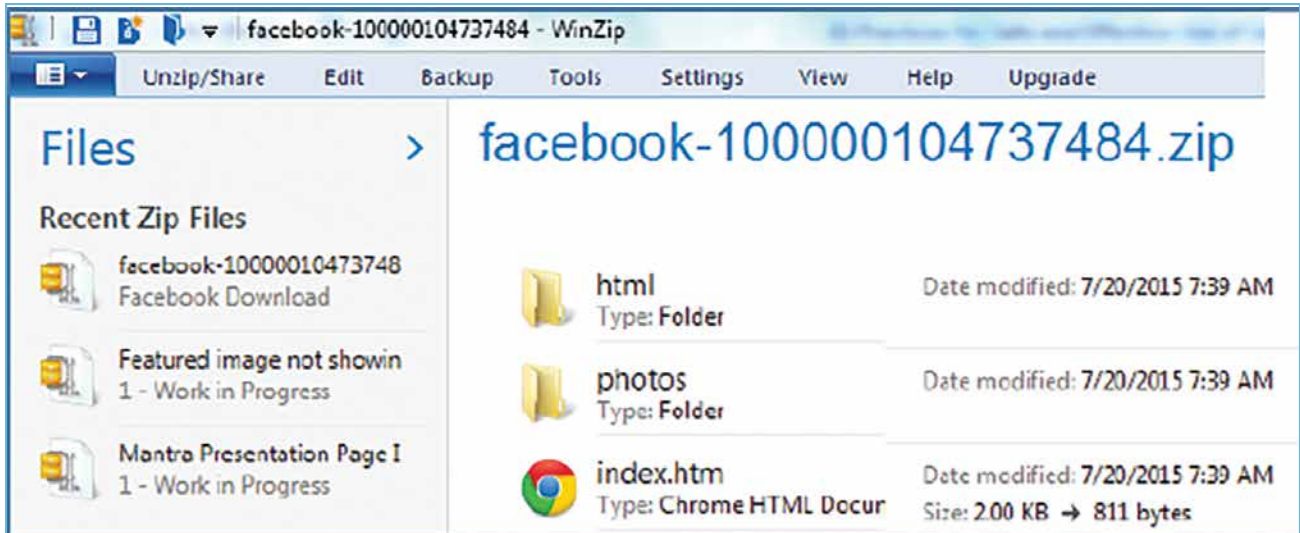
Figure 1 - WinZip software view of downloaded Facebook files

Use of Software

EULAs will often contain clauses that limit the use of the software, potentially causing problems with retaining multiple copies of the software for business continuity or data archiving reasons.

Liability Limitations

EULAs also contain clauses that limit the liability of the software vendor if the customer experiences loss of data while using the software. SLAs focus more on a characterization of services, expectations of performance, problem resolution, customer responsibilities, and limitations of the scope of the agreement.

Although historically, SLAs were mostly process- and services-focused, the need to deliver potentially vast quantities of data to customers for electronic discovery exercises during litigation has become a feature of some proactively designed SLAs.

Ability to Negotiate

Unfortunately, most EULAs are agreed to during the standard processes for installation of software by end users or information technology (IT) systems personnel, thus they are vendor-prescribed and largely non-negotiable. When logging into many social media systems to create a user account, the new system users simply click acceptance to the EULA with their mouse or the software does not install. Unless IT and IG personnel intervene in this process by prior arrangement with the software vendor, there will be no opportunity to decline and negotiate this agreement.

In contrast, SLAs are often subjected to contractual negotiations, especially during procurement business processes, and present more opportunities to insert IG policy that will support an organization's IG program.

Data Delivery

SLA deliberations allow specification in advance of a need for data deliveries, data formats, and database system reports with metadata and data content expected during litigation or audits. Having these parameters designed in advance into an SLA with a vendor can preclude them from telling a customer to just "log into the system and print it yourself."

Access and Preservation

For IG policies to work in an organization, advanced planning will be required to ensure that the organization can access and preserve any information stored on social media by an employee or contractor when that action is taken during a "normal course of business."

For instance, Facebook does not agree to share all information on all parties with whom an individual may have communicated or shared data. As a best practice for any IG program, the data map that describes the information repositories to be subject to organizational retention policy must include a description of the information an individual may store on Facebook or other social media, as well as the means and methods of preserving it.

Social Media Records Capture

Capturing records outside of the organization's control has unique challenges that will need to be addressed. Some social media vendors allow users to obtain their own data in limited formats, and they make the process straightforward, but obtaining data from others sometimes requires special expertise.

Following is information about two of the most prevalent social media platforms, Facebook and Twitter. It makes it clear that even though information can be obtained from both fairly easily, interpreting and analyzing the results can be challenging.

IS INFORMATION YOUR ALLY OR YOUR ENEMY?

NEXT LEVEL™
information governance assessment

Your business data is doubling by the year. And all this new data can either help you or hurt you. Find out what it's doing for your company with the Next Level Information Governance Assessment. You'll discover areas of strength and opportunities for improvement. In the end, you will be empowered to increase organizational transparency and data integrity while decreasing risk.

Start turning information into an asset by visiting **arma.org/nextlevel**.

Cloud Database Management Systems Architecture

There are different considerations for storing data in social media applications than for single server content management applications. Due to geographically dispersed users, social media application data must be distributed across many geographically dispersed servers to maximize data retrieval speed and promote data redundancy. Following are examples from three broadly used database management systems.

Amazon's Dynamo

Amazon's Dynamo is a database system used to store large data volumes that span many servers for data-intensive applications requiring fast read/write activities. Based on NoSQL, it is a non-relational database management system that does not need fixed table schemas and can scale without complex join operations. According to Amazon's web services documentation website, it uses consistent hashing to partition data across multiple servers. Data replication is supported for increased data availability, and data versioning is used to ensure consistency in data recall.

Google's Bigtable

Another example of a database system used to store social media data is Google's Bigtable. By using proprietary technology, such as Google File System (GFS), Chubby Lock Service, and Stored String Table (SSTable), Google has created its own schema-free database system built for high performance with respect to the special requirements of storing social media data.

In Bigtable, data and log files are stored on top of the GFS in SSTable format. Additional software technology constructs that empower Bigtable are the use of a master server, tablet servers, and a client library. This type of database management system architecture is much more complex than simple relational database architectures.

Apache's Cassandra™

Similar to both Dynamo and Bigtable, Apache's Cassandra™ database management system uses elements of both, including a Bigtable data model and a Dynamo-like architecture for servers. Cassandra is used by Facebook, Twitter, and other social media applications for large scale data storage on distributed systems.

Instead of using a set of relational tables, Cassandra uses a keyspace – a container for application data – where a table column family consisting of different rows and columns does not have to share the same columns. This provides an ability to store frequently accessed columns in separate files located closely together to enhance speed of information recall. For this reason, information about a Facebook user's friends, for instance, can be more easily collocated, speeding up retrieval of frequently accessed information.

System Performance Benefits

These specialized database architectures improve overall system performance and maintenance activities by providing increased capabilities with respect to information replication, partitioning, and querying. They also allow managing the "social locality" of data by enabling the storage of a user's data closer to its neighbor user's data store, thus increasing system performance.

Unfortunately, this means that data stores for social media applications are sufficiently complex that simple data dumps or backups to ASCII text, comma delimited text, spreadsheets, or simple database formats are unlikely to provide meaningful data for recordkeeping purposes.

Facebook

Facebook has specific informational pages, such as "Accessing Your Facebook Data" (*www.facebook.com/help/405183566203254*), that direct users regarding downloading information about shared posts, pictures, and videos, as well as information on messages, conversations, and profiles.

Specific information is available for requests from law enforcement agencies and parties to civil litigation. But where an individual has agreed to share his or her information with those entities, Facebook prefers that users authenticate the appropriateness of this third-party access, including by signing an authorization for access.

Using Facebook's download option can provide an extensive variety of data, including logs of activities such as posts, administrative settings, messages sent/received, login histories, and personal information posted. This information does not replicate the Facebook application interface most users are familiar with, though, so it will take some interpretive analysis to make use of it as a record of Facebook content or interactions.

It also is not immediately available online and must be collected by Facebook and sent to the user through an e-mail interaction, unlike many corporate computer system reports that are available online. The data comes as a compressed "zipped" file with HTML and JPG data format components in different directories that must be viewed separately. (See Figure 1.)

Twitter

Unlike Facebook, Twitter does not offer a directly available download for users to obtain information about their accounts' records and prefers that users make requests for information through help desk queries.

Twitter specifically warns that it does not validate the authenticity

of users' identities or metadata and does not validate the information they post online. Twitter also states that retention of the information varies depending on its perception of the information's value to users or for varying system administration purposes.

Twitter information will be produced as text files in word processor compatible format, and users are cautioned that some images seen on Twitter may be hosted on third-party systems. The company also cautions that cost reimbursement may be requested for some types of information.

Twitter, like Facebook, has a well-developed policy for law enforcement

al complexities involved in capturing, storing, and retaining social media records, many organizations prefer to enlist the aid of third-party organizations with experience and expertise in the arena.

As discussed in the ARMA International *Newswire* article "Scheindlin Issues Landmark Opinion on Custodian Self-Collection," there is considerable professional debate and discussion as to how advisable it is to employ "custodian self-collection" in e-discovery activities during litigation. While records custodians may be the best informed about the nature, content, and locations of electronic records, they

tion's employees must be subject to the same policies as for the use of internally hosted systems. However, as mentioned earlier, information stored on externally hosted and administered computer systems will be managed based on the dictates of the social media system owner unless there are specifically negotiated EULAs and SLAs that ensure compliance with expected IG policies.

The best practice for any organization today is to take initiative in arranging for technology solutions to preserve social media online records. This will ensure that the records' content, metadata, and formats to be

Due to geographically dispersed users, social media application data must be distributed across many geographically dispersed servers to maximize data retrieval speed and promote data redundancy.

organizations to request information. Users who are the subject of a law enforcement request for information will be notified.

Decision to Outsource

There are different considerations for storing data in social media applications than for single server content management applications. Due to geographically dispersed users, social media application data must be distributed across many geographically dispersed servers to maximize data retrieval speed and promote data redundancy.

There also are no universally accepted data formats or processes for social media records retention due to the tremendous variety and scale of the technologies and data stores used to operate social media applications. (See the sidebar "Cloud Database Management System Architecture" for technical information about three of the prevalent database management systems.)

Due to the technical and procedur-

are often only marginally prepared to accurately collect records and could have inherent conflicts of interest in doing so.

The challenges of capturing social media records may indicate the best solution in many cases is to retain third-party vendors of software, hardware, and data collection services. Vendors of such services can operate on behalf of users to make requests for records, capture records, and store them in a dedicated repository for archiving and retention.

This can be performed occasionally or through a social media application style interface so users' data can be accessed in a manner that creates the look and feel of the original social media system. Though these services come at a price, the costs of collection, storage, and retrieval may be more easily managed than the costs of self-collection and local data storage.

Best Practices for Using Social Media

Social media use by an organiza-

preserved are designed in advance to meet the needs of specific records for the IG program.

It is best for most organizations to employ these practices:
1. Enforce IG policies that distinguish employees' personal and work-related use of social media.
2. Ensure that IG issues are encompassed by contracts with vendors of cloud-based services. Design or modify EULAs and SLAs to be in compliance with IG program plans.
3. Create data maps for e-discovery initiatives to incorporate social media applications.
4. Consider outsourcing the collection, storage, and production of social media records for e-discovery.

Above all of these, the best practice for effective IG of social media is to do comprehensive advanced planning for its governance before the organization begins using it. **END**

John T. Phillips, CRM, CDIA, FAI, can be contacted at john@infotechdecisions.com. *See his bio on page 47.*

'The Devil Is in the Detail': Simplify Processing to Reduce Backlog, Provide Access to More Information

Sara Janes

Daniel A. Santamaria's *Extensible Processing for Archives and Special Collections* is a highly practical and method-oriented guide to making archival processing more efficient and effective. Santamaria starts with a few basic precepts:

Most traditional archival processing is done in greater detail and takes more time than necessary.

Providing access to records is the end goal of processing and description work.

From there he establishes that archivists could and should change their processing practices to get more done at lower cost.

Speed up to Reduce Backlogs

Santamaria's book expands on "More Product, Less Process" (MPLP), a methodology advocated by Mark Greene and Dennis Meissner in a 2005 *American Archivist* article "More Product, Less Process: Revamping Traditional Archival Processing" that has been discussed widely and frequently in the archival community to the present.

He applies MPLP principles to an extensible processing program, which he defines as an iterative system for surveying and providing baseline access to all archival collections and for eliminating processing backlogs.

Top-level descriptions and basic inventories for all collections, he argues, can be done quickly and provide better access for researchers than careful arrangement, detailed preservation work, and extensive description for just a fraction of the records.

Learn 'How,' Not 'Why'

This book is procedure-oriented and includes examples, templates, and thorough instructions for running processing projects in the way suggested. It's written in plain, detailed language and doesn't leave anything out: this book tells you exactly what you need to know to start using extensible processing methods in your work.

The appendices make up a quarter of the text: the first four are case studies showing the application of the techniques to a variety of situations, which I found to be a useful complement to the less concrete discussion elsewhere in the book.

Santamaria's focus is entirely on *how*, not on *what* or *why*. The volume does not make any attempt to address the theoretical challenges of appraisal or selection of records, instead treating appraisal as one step of many that must be done.

It's Not So Simple

Likewise, the text assumes that review for privacy or confidentiality is a simple process and one that could be performed more efficiently. This may be frustrating to archivists where complicated appraisal questions or access decisions have contributed to backlog problems: an improved process is not always enough.

However, not weighing in on any discussion of which records should be kept could also be considered a strength of this book: the methods can be applied regardless of any other policies or practices of the institution.

I was somewhat skeptical of some of the recommended applications of researcher statistics to decision making. For example, Santamaria recommends keeping track of which collections are used most frequently and prioritizing for more detailed description. This may create a feedback loop where well-used collections are made even more accessible, and the "hidden collections" stay inaccessible and undiscovered. Improving description on unused collections will improve their discoverability and use.

Modify As Needed

Readers should note that much of this book is written for archivists working in a collecting institution, like a college or university archives or a historical society, and is much less directed at institutional or government archives. Institutional archives are more likely to be dealing with fewer but larger and more complex individual collections and would thus need to modify some of the recommended practices for surveying and accessioning records.

Government archives also may be more directly responsible for privacy and confidentiality issues and may not be able to follow the advice to primarily rely on information from donors in identifying access restrictions.

Records managers and those in combined RM/archives roles should take note of the recommendation that archivists make more use of inventories and identification of privacy or confidentiality concerns provided by the records creators. This is a more efficient technique from the archivist's perspective, but it takes for granted that the records have passed through an RM program or that lists provided by the records creators are accurate and complete.

Stay Informed

As extensible processing becomes a more common practice, records managers should stay informed and be aware of how their work is being used by archival institutions.

With the caveat that not all advice applies to all situations, readers can draw from this book good ideas that will help in their work. Nearly all archives are coping with large processing and description backlogs, so adopting some, if not all, of Santamaria's recommended techniques will make a difference in speeding up the work and making more records accessible to more researchers sooner. **END**

Sara Janes can be contacted at SJanes@thunderbay.ca. *See her bio on page 47.*

BULLETINBOARD **Vendors, Products & People**
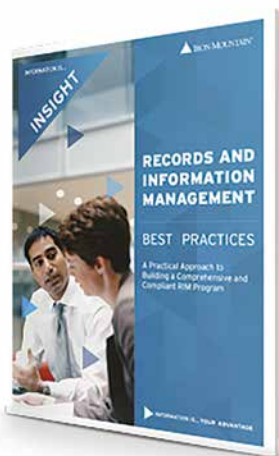
IRON MOUNTIAN
Protecting your information is key to the success of your business, so why take the risk of not protecting it properly? Check out the RIM Best Practices Guide and discover the practical approach to building a comprehensive and compliant RIM program. Download the RIM Best Practices Guide today at *ironmountain.com/BestPractices.*

OPEX CORPORATION
From document conversion services to mobile scanning to digital mail centers, Falcon™ is the only prep-reducing scanner on the market to combine all your scanning needs into one universal document scanning workstation. Falcon allows operators to prep and scan documents at a faster rate than most current prep-only processes. For more information, visit *www.opex.com.*

NAID
NAID is the non-profit, watchdog association for the information destruction industry. To learn more about the mission or how to join, visit *www.naidonline.org.*

SHERPA
Records and information management professionals are faced with the monumental challenge of locating, organizing, and managing electronic data. How do you manage something that large and complex? Where do you start? With a mountain of data to scale, you need a guide with the right tools. You need a Sherpa. Contact Sherpa Software to reach new heights in managing your data. *www.sherpasoftware.com*

ELIN   **GABLE**   **JANES**   **LEBEDEVA**   **MCKINNON**   **PHILLIPS**

Embrace the Cloud, Big Data to Take Control of the Digital Deluge Page 18

Cheryl McKinnon, IGP, is a principal analyst for Forrester Research. She covers the trends, challenges, and recommended practices for managing enterprise content. Her focus is delivering research and advisory services into areas including enterprise content management (ECM), content archiving, enterprise file-sync and file-share, document-centric collaboration, lifecycle management, information governance, and e-discovery. She can be contacted at *cmckinnon@forrester.com*.

More Than Paper: How RIM Can Influence IT and Shape IG Page 24

Phyllis Elin is director of information governance for Recall Holdings. An expert in records management and information governance, her experience encompasses consulting work and project management for most major industries and contributing to the Recall blog. She can be contacted at *recall@mslgroup.com*.

Five Essential Project Management Skills for RM and IG Professionals Page 28

Anna Lebedeva, IGP, PMP, is a director of records management at a large regional financial services company. Her RIM accomplishments include establishing RIM programs, developing retention schedules, standing up legal hold processes, and working on electronic records strategies. Lebedeva has a master's of science degree in software engineering from Fairfield University and spent nine years as a software developer before spending more than eight years managing large enterprise projects. She can be contacted at *anna.lebedeva@peoples.com*.

The Principles: Making a Business Case for the Principles Page 26

Julie Gable, CRM, CDIA, FAI, is the retired president and founder of Gable Consulting LLC, a firm that served clients' information governance needs for 25 years. The author of numerous articles on information-related topics, she has 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*.

Best Practices for Governing Social Media Content Page 38

John T. Phillips, CRM, CDIA, FAI, is a management consultant with Information Technology Decisions. With more than 30 years of experience in many varied information and technology management professional positions – including a recent six-year term on the National Archives and Record Administration's Advisory Committee for the Electronic Records Archive – he assists clients in developing comprehensive records management programs, especially with electronic records management issues and technology systems selection. Phillips can be contacted at *john@infotechdecisions.com*.

'The Devil Is in the Detail': Simplify Processing to Reduce Backlog, Provide Access to More Information Page 45

Sara Janes is records analyst/archivist at the city of Thunder Bay and an instructor with the Lakehead University Department of History. She received her master's degree in library and information science from McGill University. Her work has focused on access, privacy, and legal issues, and outreach and public engagement. She is a member of the Northwestern Ontario Archivists' Association and the board of directors of the Thunder Bay Historical Museum Society. She can be contacted at *SJanes@thunderbay.ca*.

INFORMATION MANAGEMENT.
DON'T JUST SURVIVE IT.
THRIVE IN IT.

Information Managers, you are not alone.
See how we can help you manage and leverage
data in powerful, new ways. **arma.ironmountain.com**

Find out how at ARMA Live! 2015
Booth #400 and the Mountain Ca Fe

IRON MOUNTAIN®