INFORMATION MANAGEMENT

50TH YEAR

AN ARMA INTERNATIONAL PUBLICATION

NOVEMBER/DECEMBER 2016

Data Privacy Meets a World of Risk:

A Landscape in Turmoil

Page 20

Documents decoded.

Optimize business-critical data while minimizing costs and improving productivity with PaperStream Solutions suite of document capture software.

- High-quality capture
- User-friendly applications
- Scalable for any size project or any size organization
- Backed by Fujitsu Computer Products of America's US-based industry leading maintenance and support

PaperStream Solutions complements Fujitsu's highly productive document scanners.

Visit us.fujitsu.com/fcpasolutions to learn more!

FUJITSU | PaperStream

INFORMATION MANAGEMENT

50TH YEAR

NOVEMBER/DECEMBER 2016 **VOLUME 50 NUMBER 6**

INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

Publisher: Robert Baird, IGP, CRM, PMP

Editor in Chief: Vicki Wiler

Contributing Editors: Nikki Swartz, Jeff Whited, April Dmytrenko, CRM, FAI

Art Director: Brett Dietrich

Advertising Account Manager: Jennifer Millett

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

An annual subscription is included as a benefit of professional membership in ARMA International. Nonmember individual and institutional subscriptions are $150/year (plus $20 shipping to destinations outside the United States and Canada).

ARMA International *(www.arma.org)* is a not-for-profit professional association and the authority on governing information as a strategic asset. Established in 1955, the association's approximately 27,000+ members include records and information managers, information governance professionals, archivists, corporate librarians, imaging specialists, legal professionals, IT managers, consultants, and educators, all of whom work in a wide variety of industries, including government, legal, healthcare, financial services, and petroleum, in the United States, Canada, and more than 30 other countries around the globe.

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

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

Advertising Inquiries: Contact Jennifer Millett at +1 888.277.5838 (US/Canada), +1 913.217.6022 (International), +1 913.341.3742, or e-mail *jennifer.millett@armaintl.org*.

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

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

Canada Post Corp. Agreement No. 40035771

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

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

Magazine Changes in 2017 Promise to

Enhance Member Value

As we close this 50th volume year, we're looking ahead to an important change for *Information Management* in 2017. Beginning with our next issue, *Information Management* magazine will be published in a digital format only. Though some may not welcome this change at first, we are confident you will quickly see its value.

By eliminating the long and expensive print production and mailing processes, the magazine will be timelier, and we will be able to offer more content – even adding or updating content between issues. Over time, we also expect be able to increase the number of issues you will receive each year.

Even better, we will be able to redirect saved resources into other areas that will enhance the value of your membership.

For example, we will be able to move the magazine to a *responsive* design application that will enable you to read the digital version more easily on virtually any device, such as laptops, smartphones, and tablets. This means the magazine layout will "respond" to the size of the device you are using by reformatting itself, eliminating or minimizing the scrolling that often has been required to read the current digital version on many screens.

This application also will offer more interactivity, such as real-time commenting on content, participating in polls that will provide instant results, and viewing "how to" videos and other informational content.

If you "have to have" a physical magazine, there will be options for printing it to your own printer or ordering a commercially printed and bound version through an online print-on-demand service at a small cost. We will also offer an "at-cost" subscription for those who want a printed magazine sent automatically. Because these will be printed by a digital printing service, the look and feel may be a little different from the current magazine, which is offset printed on a web press, but it will still be perfect for those who prefer to read hard copy. Watch for more communications about this from us over the next few months.

Our research indicates that *Information Management* is highly valued as a membership benefit. Because of that, we will continue to work towards making the magazine even more robust, timely, accessible, and relevant for enhancing your knowledge and skills in 2017.

We welcome your questions, suggestions, and comments on the transition to a digital-only format – and on any matters related to *Information Management* magazine. Please contact us at *editor@armaintl.org*.

Vicki Wiler
Editor in Chief

MS *in* CYBERSECURITY MANAGEMENT

ENROLLING NOW!
For February & June 2017

Cybersecurity = *Job Security*

Our completely online **MS IN CYBERSECURITY MANAGEMENT** prepares graduates for both initial placement and mid-level positions in career track jobs in cybersecurity, information assurance management & analytics, digital forensics, and risk management fields. All students will be educated in the **LEADERSHIP OF CYBERSECURITY SYSTEMS AND PERSONNEL**, and will be prepared to assume immediate responsibility for the management and oversight of such systems. They will also acquire necessary and in-demand **LIFELONG LEARNING SKILLS**, including the confidence and positive attitude necessary to grow and sustain their careers for decades. We also offer a concentration in **DIGITAL FORENSICS** as part of the graduate program.

- **Classes begin every October, February, & June**
- **Completely Online**
- **Financial aid available**
- **No GMAT or GRE required**

For more information visit
GRADUATE.BAYPATH.EDU

BAY PATH UNIVERSITY
1897
FOR A CONSTANTLY CHANGING WORLD

CLOUD

Forrester: Cloud Technology in a 'Hypergrowth Phase'

Cloud service revenues will reach $236 billion in the private sector by 2020, predicts Forrester Research. That total exceeds Forrester's 2014 forecast by 23%.

According to the Forrester study, public cloud will become the dominant technology model by 2020. The growth won't come from a huge influx of new customers, but from portfolio expansion and new application scenarios, the study predicts.

Cloud technology, according to Forrester, is currently in a "hypergrowth phase" that will gain speed for the next four years for cloud platforms, cloud applications, and cloud business services.

The increasingly strong market for software-as-a-service (SaaS) and dramatic increases in infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) will continue, according to the study. By 2020, Forrester predicts SaaS will comprise more than two-thirds of spending on customer relationship management, human resource management, e-commerce, and e-purchasing.

Forrester says it has been "astonishing" how cloud service providers, including Amazon Web Services, Microsoft Azure, IBM, Google, and Salesforce, have already affected sales of on-premises servers and storage devices. By 2018, Forrester's research suggests, North American and European companies will run 18% of their custom-built application software on public cloud platforms.

INFO SECURITY

Pokémon Go Proves that Companies Need Strong BYOD Policies

The Pokémon Go game has become an insanely popular hit worldwide, enticing millions of players to find, catch, battle, and train virtual monsters that pop up at real-world landmarks. But it's also a huge security risk for organizations everywhere, underscoring their need for a strong "Bring Your Own Device" (BYOD) program.

According to *Legaltech News,* although many BYOD policies separate corporate data from personal activities, they cannot restrict employees from downloading to their personal devices games like Pokémon Go, which by default has full access to players' Google e-mail, files, and location data. According to Pokémon Go's privacy policy, the "data it collects – including personal information – is an asset of the developer."

This popularity of Pokémon Go likely means that such games will become the norm. Here's how to keep your organization safe, according to a *Legaltech News* report:

- Implement a written BYOD policy, enforce restrictions, and make sure you have the tools to do so. Train staff on cybersecurity and appropriate digital device usage.
- Verify that your employees' personal devices have not been "jail broken" before allowing them onto your network. According to *Legaltech News*, this means that a user has gained access to a device's operating system (usually in Apple devices) in order to run unauthorized applications.
- Encrypt all devices and data used for work purposes.
- Restrict network access for employees who don't want to install security tools on their personal devices.

INFO SECURITY

Data Breaches Cost More than Money

According to a recent *Journal of Accountancy* article, a new report by Deloitte & Touche LLP lists 14 impact factors of a cyberattack, including seven that might not be readily apparent:

1. Higher insurance premiums: Deloitte says companies may face premium increases of 200% for the same coverage, or they may be denied coverage until they prove to the insurer that they have shored up their cyber defenses. Insurers may tell a company what to fix before coverage will be continued.
2. Increased cost to raise debt: After a data breach, a company's credit rating can be lowered, which will affect its ability to raise debt or renegotiate its existing debt, Deloitte said. Deloitte's analysis said credit ratings agencies typically downgrade by one level companies that have experienced a cyber incident.
3. Business disruption: When normal business operations are disrupted, a company suffers financially. If a company's e-commerce site must be shut down temporarily, for example, the company will lose current and possibly future business when customers move to a competitor.
4. Lost customer relationships: Customers may not return to a business that suffers a breach. Deloitte's hypothetical analysis showed that customer attrition rate increases 30% after a cyber incident and doesn't return to normal for three years.
5. Lost contract revenue: Negotiating contracts with other entities is harder after a data breach, and contracts may be terminated as a result of a cyberattack.
6. Devaluation of trade name: If a company's business is offering services to other companies, those companies will be less likely to seek additional services from a company that has suffered a data breach. Most companies will need to rebuild brand loyalty after a breach.
7. Loss of intellectual property: This can be the most crippling effect of a data breach. The effects could be long-lasting or potentially fatal to the company's survival, depending on what type of intellectual property is lost. "If you lose plans, if you lose designs, or lose [research and development] that you've been working on for months or years, and that then is brought to market by another organization faster and cheaper than you can do it, that impact can be reverberating for decades," said Emily Mossburg, principal in Deloitte & Touche's cyber risk practice and a report author.

INFO SECURITY

Connecting Phones to Rental Cars May Expose Data, FTC Warns

Automotive IT systems that connect smartphones with onboard media players may put your private data at risk when you're driving a rental car, the Federal Trade Commission has warned.

Lisa Weintraub Schifferle, an attorney in the FTC's Division of Consumer and Business Education, said that when you return the car, those connected systems might reveal your private data to those who know where to find it, according to an article on *FCW.com*.

For example, the car's GPS device can store the locations you visited, which may include a rental car user's workplace and home. By connecting a smartphone to any of the systems in the vehicle, someone could find telephone numbers, call and message logs, contacts, and text messages, Schifferle wrote.

If you connect to any system in a rented vehicle, you must proactively delete the data to keep it from being accessed by the next driver or by hackers, she warned.

Schifferle said even charging a smartphone on a rental car's USB port could automatically transfer data to the onboard systems. She recommends charging a smartphone on an adapter instead; checking onboard screens for options to limit access to connected devices; and deleting your devices from the list when you return the vehicle.

GOVERNMENT RECORDS

OMB Updates Rules to Protect Government Data

After a spate of large breaches involving federal agencies, the Office of Management and Budget (OMB) has revised its rules to promote data protection in the federal government.

OMB released an 85-page update to Circular A-130 highlighting how the OMB "recognizes the need for strong data governance that encourages agencies to proactively identify risks, determine practical and implementable solutions to address said risks, and implement and continually test the solutions," according to a *Legaltech News* report.

The document, which was sent to the heads of all federal departments and agencies, is designed to establish general policy for the planning, budgeting, governance, acquisition, and management of federal information, personnel, equipment, funds, IT resources, and supporting infrastructure and services.

With its circular, the OMB is sending a message to government agencies – in the form of a framework – that they need to develop a culture of privacy and security protection.

Bart Lazar, attorney at Seyfarth Shaw, told *Legaltech News* that for years the private sector has been encouraged to establish a C-suite level champion within each company for data privacy and security. "Without support from the top, it is difficult, if not impossible, to get the budget and resources allocated in order to develop a culture of data privacy and security compliance. This circular, coming from OMB in the White House, in some ways is the U.S. government's C-suite support for developing, implementing, and maintaining that culture of compliance," he said.

In response to the document, federal agencies need to make changes, including creating a risk management framework, maintaining a continuous privacy monitoring program, implementing an overall privacy awareness program, and training staff and vendors on how to handle data breaches, *Legaltech News* said.

"It is hard for the U.S. government to expect businesses in the private sector to do something the government does not do itself, the whole 'talk the talk, walk the walk,'" Lazar said.

PRIVACY

Illinois Public Employees' Private Messages May Be Made Public

Illinois Attorney General Lisa Madigan recently issued a binding decision that the personal e-mail accounts of many types of public employees are subject to Freedom of Information Act (FOIA) requests if those e-mails contain public business, the Illinois News Network reported. The decision is the result of a CNN request to the Chicago Police Department to turn over any personal e-mails that officers may have made concerning the Laquan McDonald shooting.

Legal experts said the ruling will affect municipalities across the state. "Sometimes the easiest thing to do is to pull out a smartphone to text a colleague for a public works project or something similar," Mark Burkland, Holland & Knight senior counsel, said. "If a water main breaks at 2 a.m., is the public works director not supposed to use their personal device to call or to text someone to get out and fix it?"

An attorney for CNN argued that granting public employees' private e-mails immunity from FOIA requests would undermine current disclosure laws because it would give them reason to use those accounts to hide sensitive information.

The rule doesn't apply to elected officials and their private accounts.

Burkland said public bodies should make rules to establish a way to get to their employees' private accounts should they need to.

At time of publication, it was unclear whether the city of Chicago would appeal the decision.

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

PRIVACY

Facebook Cannot Collect Data on WhatsApp Users in Germany

WhatsApp angered some users when it announced in August that in an effort to provide better service, it would begin sharing users' phone numbers and analytics data with Facebook – which acquired WhatsApp in 2014.

The city of Hamburg, Germany's data protection commissioner, Johannes Caspar, has ordered Facebook to stop collecting and storing data on WhatsApp users in Germany and to delete all information on about 35 million German users that already had been forwarded from WhatsApp. The Hamburg regulator has authority over Facebook's activities in Germany because the company's German subsidiary is based in the city, according to the *New York Times*.

Caspar said that neither WhatsApp nor Facebook had received individuals' permission to share the information and had potentially misled people over how their data would be used in the future. He added that millions of people whose contact details had been uploaded to WhatsApp could now see that information shared with Facebook against their will, which would infringe German law.

"It has to be their decision, whether they want to connect their account with Facebook," Caspar said in a statement. "Therefore, Facebook has to ask for their permission in advance. This has not happened."

After the order was issued, Facebook said it had complied with Europe's privacy rules and was willing to work with the regulator to address its concerns.

"Facebook's answer, that this has merely not been done for the time being, is cause for concern that the gravity of the data protection breach" will have a more severe impact, Caspar said.

GOVERNMENT RECORDS

Federal CIOs Focused on Cybersecurity, Survey Shows

Cybersecurity is the top priority and challenge for U.S. federal chief information officers (CIOs) and chief information security officers (CISOs), according to the 26th annual Professional Services Council survey, conducted with Grant Thornton.

This year's survey, "Federal CIOs: Delivering Results While Preparing for Transition," highlights federal IT leaders' efforts to modernize outdated IT infrastructure, raise the bar on cybersecurity, reform IT acquisition processes, deliver on the promise of innovation, and address the ongoing war for top IT talent in both government and industry.

"Today's government IT leaders need to wear many hats as demands increase and budgets shrink," said George DelPrete, principal with Grant Thornton Public Sector and leader of its Information Technology Service line. "They face a number of daunting challenges, but it is reassuring to see how they are being creative in using technology and new strategies to keep their agencies agile and responsive."

While cyberattacks on government systems continue to make headlines, overall, survey respondents report that government is making progress coordinating on cyber issues. The cyber sprint conducted in the summer of 2015 was helpful for them to gain insights into their own cyber risks and improve communication within the CIO community on threats and mitigations to common cybersecurity risks.

CIOs and CISOs who responded to the survey also said:

- Cybersecurity challenges are exacerbated as federal legacy systems and infrastructure continue to age, and that additional investment is required to address this crucial issue.
- Hiring rules need to change to make it easier to recruit and offer competitive pay to new cybersecurity talent. Skills in greatest demand include cybersecurity, agile development, cloud expertise, and digital services skills.

There is a need to modernize federal IT legacy systems, reduce network footprints, rationalize and modernize applications, and migrate to the cloud. Modernizing the IT environment is needed to close security gaps, refresh infrastructure to improve IT performance, reduce spending on outdated equipment or software, take advantage of fast-changing technology improvements, and better manage, consolidate, and analyze the increasingly large volumes of government data.

PRIVACY

How to Prepare for the EU's General Data Protection Regulation

The European Union's (EU's) General Data Protection Regulation (GDPR) provides specific guidelines for how to classify, secure, and manage EU individuals' private data. They affect companies operating there, as well as any organization that does business there or that collects data on EU citizens.

The GDPR aims to give individuals more control over their personal information by clarifying the law relating to the clear and affirmative consent to data processing, how and where data can be stored, and individuals' right to be forgotten, according to *Legaltech News*.

GDPR mandates that organizations must proactively classify data and have tools in place to take action on this information, including applying governance policies, detecting and responding to data breaches, and optimizing backup and recovery. According to the new rules, organizations must understand their data and where it resides, as well as protect it in use, in transit, and in storage.

Organizations have a May 2018 deadline to comply with the GDPR or face significant fines, sanctions, and lawsuits.

Joe Garber, vice president of marketing at Hewlett Packard Enterprise, recently provided *Legaltech News* with the following tips to help organizations prepare for the GDPR:

Understand your data. If your organization is subject to GDPR, first assess your data:

- What and where is the information that falls under GDPR regulations?
- How do I identify information in accordance with "right to be forgotten?"
- How do I apply and enforce policies to manage information in use, in transit, and at rest?
- How can I quickly and cost-effectively respond to investigations or legal matters requiring information under management?
- How can I mitigate the risk of a data breach? What is my plan of action if one occurs?

Assess technology platforms to ensure compliance. The cloud hasn't been as widely adopted in the EU as in the United States because of data sovereignty issues, but many EU organizations are now re-thinking their cloud strategy, Garber says. Those companies need to ask:

- Is data stored and processed within the European Economic Area?
- What security measures does the cloud provider have to protect data as it relates specifically to GDPR?
- How can I access this information for investigations and litigation, if necessary?
- Will these cloud-based technologies provide broad enough tools to address the full scope of GDPR, or will I have to switch to other capabilities over time?

Break down the GDPR into simple use cases. The GDPR has more teeth and specificity than many requirements that have come before it, Garber said, so playing the "wait and see" game is not a good idea. If organizations wait until right before the May 2018 deadline to prepare, they may not be fully compliant when the requirements kick in, leaving them and their customers' information at risk.

Garber says the smart approach is to take GDPR compliance in a methodical, modular way. There are specific use cases mapped out by certain technology vendors that align directly to GDPR requirements.

E-DISCOVERY

Report: 2016 a Good Year for E-Discovery

2016 is shaping up to be an eventful year for e-discovery, according to a mid-year report.

With the U.S. Federal Rules of Civil Procedure (FRCP) amendments in effect and plenty of new technologies, Gibson, Dunn & Crutcher's "2016 Mid-Year Electronic Discovery Update" describes e-discovery as evolving, ripe for innovative technologies, struggling to keep pace with new sources of discoverable information, and watchful of post-FRCP changes.

E-discovery looks "much better" than in years past, in part because FRCP Rules 26(b)(1) (discovery must be relevant and proportional) and 37(e) (preservation responsibilities and sanctions for failure to preserve) have "for the most part" had "their intended effects," noted co-author Gareth Evans, litigation partner at Gibson Dunn. This is a stark change from the 2006 amendment to Rule 37(e), which was not applied as intended, he added.

According to the report, the positives include the following:

- In the first six months of 2016, Rule 37(e) was applied in 32 decisions, with 13 granting sanctions and 19 denying them. This is a "substantially slower" pace than in past years, the report says (150 sanctions in federal courts in 2011 and 120 in 2012). The report says the reduction is likely due to a growing awareness of preservation duties.
- A rational, easy-to-apply set of criteria in amended FRCP 37(e) for imposing sanctions for failure to preserve discoverable electronically stored information (ESI) seems to have resulted in shorter sanctions decisions that are faithful to the amended rule, as well as in substantially fewer sanctions motions and decisions.
- Courts also appear to be faithfully implementing the requirement of amended Rule 26(b)(1) that discovery must be both relevant and proportional, with courts repeatedly holding that merely establishing relevancy but not proportionality is not enough. Despite once implicitly allowing broad "fishing expeditions," courts are now explicitly prohibiting them.
- What appears to be a dramatic reduction in the number of sanctions decisions likely is due, in part, to greater awareness among litigants of preservation duties, as well as improved legal hold practices. But it is almost certainly also a result of a clearer, more consistent legal framework, which should discourage sanctions motions that do not satisfy each of the criteria set forth in the amended rule – particularly the elimination of the harshest sanctions where there was no intent to deprive other parties of the lost information.

The report also identified several challenges to consider:

- New sources of potentially discoverable ESI, such as text messaging and social media, have created new risks and difficulties for identification and for legal hold preservation and collection, and, further, have made it difficult to determine just what is discoverable. Indeed, many of the sanctions decisions so far in 2016 have involved failures to preserve text messages on mobile devices, the report found.
- The potential of predictive coding to greatly reduce costs and increase accuracy and review speeds remains largely unfulfilled, hampered by several factors, including a lack of awareness of the technology, lawyers' comfort with traditional keyword searches, obstacles raised by those opposing its use (such as demanding access to irrelevant documents in training sets), and the limited availability of the latest predictive coding software.
- Vendors have yet to put together a single, full suite of "best in breed" software for companies to handle e-discovery tasks internally from beginning to end (legal holds through production). It is likely only a matter of time before they do so, however, the authors noted.

FOIA

NJ May Deny Public Records Access, Court Says

Government agencies in New Jersey may deny access to public records by saying they can "neither confirm nor deny" their existence when they receive an information request under the state's Open Public Records Act (OPRA), New Jersey's state appeals court has ruled.

The decision makes New Jersey the second state to adopt as law what one media lawyer has called "a broad and damaging secrecy tool" first used by the U.S. government during the Cold War to protect its national security interests. The other state, Indiana, authorized "neither confirm nor deny" responses through a statute, not a court ruling.

The ruling was made against North Jersey Media Group, a division of Gannett that publishes several newspapers, including *The Record*. The New Jersey appeals court allowed what is known as a "Glomar" response, which some U.S. agencies have used since the 1970s to block requests for public records submitted under the U.S. Freedom of Information Act.

"Glomar responses are used under FOIA in two contexts: where confirming or denying raises national security issues or privacy issues," said Erwin Chemerisnky, a First Amendment expert and dean of the law school at the University of California, Irvine. "But even then, agencies must present as much as possible. It is essential that Glomar responses be limited or they could be used to undermine public records laws."

In 2013, a reporter for North Jersey Media Group filed a request under OPRA and the common law seeking from the Bergen County Prosecutor's Office recordings or transcripts of 911 calls, complaints, and other documents regarding a Catholic priest who has never been arrested or charged with a crime.

To protect the priest's privacy, the prosecutor's office neither confirmed nor denied the records existed. "Exposing information regarding individuals who have not been arrested or charged with any crime is an invasion of privacy and could have devastating repercussions," the office stated.

When the dispute went to trial, Superior Court Judge Peter Doyne ruled for the first time in New Jersey that a government agency could answer a request for public records by neither confirming nor denying the existence of relevant documents, according to media reports.

Doyne based his ruling on the state constitution's right to privacy. The appeals court upheld the response from the prosecutor but its decision was even more specific.

Judge Marianne Espinosa wrote for the appellate court that although "there is no language in OPRA that explicitly permits an agency to decline to confirm or deny the existence of responsive records," that law does allow agencies to respond to public records requests by stating that they are "unable to comply." Those agencies, however, should be prepared to show a court a "sufficient basis" for neither confirming nor denying the existence of relevant documents, Espinosa added.

"It is obvious that, in order to protect the confidentiality of persons who have been the subject of investigation but not charged with any offense, the prosecutor must respond to requests for such records uniformly," Espinosa wrote. "To deny records exist in some cases and to issue no denial in others would implicitly confirm the existence of records in a particular case, entirely defeating any effort to protect the confidentiality interest at stake."

E-DISCOVERY

Sedona Releases Draft E-Discovery Publication

The Sedona Conference® recently released the public comment version of *Commentary on Defense of Process: Principles and Guidelines for Developing and Implementing a Sound E-Discovery Process*. The publication addresses the tension between the principle of party-controlled discovery and the need for accountability in the discovery process. It establishes a series of reasonable expectations and provides practical guidance to meet these competing interests.

The overriding goal of the principles and guidelines set forth in this commentary is to reduce the cost and burden typically associated with modern discovery by helping litigants prepare for – or, better yet, avoid – challenges to their discovery processes, and by providing guidance to the courts in the (ideally) rare instances they are called upon to examine a party's discovery conduct.

The commentary may be downloaded free from The Sedona Conference® website. The public comment period closes November 15. Questions and comments may be sent to *comments@sedonaconference.org*.

PRIVACY

More Than 100 U.S. Companies Earn Privacy Shield Certification

The European Commission recently said that more than 100 U.S. companies have been certified by the U.S. Department of Commerce as having privacy policies that comply with the data protection standards required by the U.S.-EU Privacy Shield.

"I'm pleased that many companies have already signed up and brought their privacy policies in line with the Privacy Shield," Vera Jourová, the EU's commissioner for Justice, Consumers and Gender Equality, said in the announcement. "I encourage many others to continue to do so to ensure Europeans can have full confidence in the protection of their personal data when transferred to the U.S."

The European Commission announcement also notes that the U.S. Commerce Department is reviewing the privacy policies of another 190 companies that have signed up for the Privacy Shield and that another 250 companies are submitting applications. In contrast, more than 4,000 companies had been certified under the Safe Harbor that was invalidated by the European Court of Justice in 2015.

The Privacy Shield program, which became available to U.S. organizations on August 1, provides companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States.

E-DISCOVERY

ESI Infrastructure Still Frustrates E-Government

Government agencies have hired additional e-discovery experts to help manage their data volumes, but most still struggle with electronically stored information (ESI) infrastructure and processes, according to consulting firm Deloitte.

Deloitte's 10th annual benchmarking study on the use of e-discovery by government agencies found that internal systems and processes remain the most pressing challenge agencies face in their e-discovery practices.

In "Study of Electronic Discovery Practice for Government Agencies - 2016," 35% of 210 respondents reported that "internal systems and processes" created the biggest challenges in handling, processing, reviewing, or producing ESI. The category has been ranked the top challenge for respondents of the survey five years running.

Surprisingly, the report also found that government agencies rarely request social media data, with only 19% of legal experts polled saying they requested social media data from opposing counsel, down slightly from 23% last year.

"Social media data – while important on some matters – is not a source of information in most federal litigation matters," Patrick McColloch, managing director in the government sector discovery practice of Deloitte Transactions and Business Analytics, told *Legaltech News*.

McColloch said agency staff has taken some measures over the last decade to mitigate these concerns. For example, agencies have hired specific e-discovery counsel to specialize in technology and issues surrounding ESI within their general counsel offices.

McColloch noted that the Department of Justice has also added to its own e-discovery staff and resources in an attempt to better support agencies during litigation.

McColloch suggested that agencies start to invest more heavily in supporting ESI needs, despite budgetary constraints.

"Agencies need to view investments in internal systems and processes as they would any other investment," he said. "With the expanding volumes and complexities of data, and without investing in the systems in processes, government agencies are forced to tackle the issue with more manpower or potentially face litigation risks."

ScanPro i9300

Bring your Blipped Microfilm into the Digital Age with the **ScanPro i9300**!

The ScanPro® i9300 microfilm scanner is the product you've been waiting for to bring your blipped film into the digital age. We know that original blipped film scanners are aging and limited in their capabilities. That's where the i9300 comes in!

Find your blip the first time

Utilizing patent pending technology, the ScanPro i9300 finds your blip the first time with fast and exceptionally accurate searching. It works with one, two, and three level simplex and duplex film and is ALWAYS as easy as 1-2-3.

1 load your film | 2 enter your search address | 3 click search

Automatic scanning/printing

The i9300 automatically scans/prints a single image, a range of images, or the entire roll of microfilm easily and efficiently.

Universal microfilm scanner

Not only does the i9300 support blipped film, it also scans/prints your fiche, ultra-fiche, aperture cards, micro cards, and 35mm roll film microfilm, making it truly universal!

The ScanPro i9300 is the solution you've been waiting for. It is easy to use, reliable and backed by an unmatched 3-year warranty and a lifetime lamp warranty.

The ScanPro i9300.

Precise. Powerful. Universal.

e-ImageData microfilm scanners

www.e-imagedata.com • 800-251-2261 • www.facebook.com/eimage.data • @eImageData

E-DISCOVERY

Court Orders a $3 Million Fine for E-Discovery Misconduct

Legal experts have called the recent *GN Netcom v. Plantronics* decision a "teaching opinion" for how e-discovery should be conducted and one of the more significant opinions since the enactment of the U.S. Federal Rules of Civil Procedure (FRCP) amendments in December 2015.

In the antitrust case, the District of Delaware issued a scathing opinion relating to the scope of sanctions that may be applied for e-discovery misconduct. A senior manager for Plantronics Inc. instructed employees to delete e-mails and deleted messages from his own account. After the establishment of a litigation hold, the senior manager deleted as many as 90,000 unrecoverable e-mails, of which 6.5% were estimated to be responsive.

The court imposed sanctions on Plantronics, including the fees and costs incurred for bringing the motion, $3 million in punitive damages, possible evidentiary sanctions to be determined at a later date, and an adverse inference jury instruction, according to *Legaltech News*.

The court said that although Plantronics may have taken reasonable, and even extensive, steps to preserve documents, the organization was still responsible for the failure of one of its managers to follow preservation procedures. The court said the senior manager's actions were the opposite of reasonable and were inexcusable, even though he believed that IT personnel would continue to have access to his deleted e-mails.

Further, the court made a finding of bad faith on the part of the senior manager and Plantronics. The court also found that the deleted e-mails and deprivation of discovery caused prejudice to the plaintiff, a point which Plantronics failed to disprove in its argument.

Chief Judge Leonard Stark noted in his decision that the behavior of Plantronics' senior manager requires a "perverse interpretation" of Rule 37(e), a finding that might place a strict precedent for those who choose to participate in evidence spoliation.

INFO SECURITY

Canada's Police Chiefs Want Access to Encryption Keys, Passwords

At its annual conference in Ottawa, the Canadian Association of Chiefs of Police adopted a resolution seeking "a legislative means for public safety agencies inclusive of law enforcement, through judicial authorization, to compel the holder of an encryption key or password to reveal it to law enforcement."

According to the resolution, Internet and computer-related crime threatens the privacy and security interests of Canadian citizens, and law enforcement authorities have been unable to complete investigations of serious criminal activity as a result of their inability to execute judicially authorized services of electronic devices. The resolution contends that legislative authority to compel an individual to provide either law enforcement or public safety agencies with the password or encryption key for an electronic device is needed to support legitimate law enforcement interests.

"Canadian police are fighting an uphill battle," wrote cybersecurity analyst Eric Jacksch in an online column for IT in *Canadaonline*. "Their recent request for new legislation to compel people to disclose passwords and encryption keys demonstrates both desperation and lack of cybersecurity savvy."

Jacksch contends the authority could be rendered ineffective by technical controls, and it "could be used to bully those who cannot afford legal representation and appeals into allowing police to rifle through their digital lives at an unprecedented level."

He added that it "seems highly unlikely" that the Canadian government could draft a law to force people to disclose passwords and encryption keys without violating their constitutional rights.

REGULATORY ACTION

Utility Fined $25.6 Million for Recordkeeping Violations

California regulators hit PG&E with a $25.6 million fine for many recordkeeping violations that resulted in the San Bruno natural gas explosion that killed eight people in 2010.

The state Public Utilities Commission (PUC) voted unanimously to punish the utility for failing to keep accurate records on its aging natural gas pipeline system, the *East Bay Times* reported.

In June, PUC Administrative Law Judge Maribeth Bushey noted that PG&E was guilty of widespread deficiencies in its recordkeeping.

"These inaccurate records were relied on for locating and marking underground facilities in anticipation of excavation," Bushey wrote in the proposed ruling. "The inaccurately mapped and consequently inaccurately marked facilities led to excavators damaging the distribution system in several instances."

Six incidents, from September 2010 to March 2014, prompted regulators to open a formal probe into PG&E's recordkeeping. Most of the incidents resulted in leaks and service interruptions. In one incident, natural gas leaked into an empty home that eventually blew up.

A National Transportation Safety Board (NTSB) investigation concluded that PG&E's recordkeeping played a major role in the 2010 San Bruno explosion, in which eight people died and dozens of homes were destroyed. The NTSB determined that inadequate pipeline maintenance by PG&E and lazy oversight by the PUC were also key contributors to the explosion.

In April 2015, the PUC fined PG&E $1.6 billion for causing the San Bruno disaster, the largest financial punishment ever levied on an American utility. In August 2016, a federal jury found PG&E guilty of six felony charges, including five violations of U.S. pipeline safety rules before the San Bruno blast and one count of obstructing the government's investigation.

CLOUD

10 Tips for Effective Cloud Service Agreements

Legal experts in a *LegalTech News* article recommend 10 best practices for those who negotiate and write cloud service agreements:

1. Require service providers to comply with all applicable privacy and data security laws, regulations, and industry standards.
2. Identify a minimum standard of care for privacy and data security to meet the organization's particular needs, and require service providers to meet it.
3. Allow cloud providers to access the organization's IT systems and use its data only as required to perform the agreed-on services or as authorized for other purposes.
4. Restrict cloud providers from disclosing the organization's data to third parties except as specifically authorized. Address how the provider will handle any data requests from government authorities.
5. Require cloud providers to impose the same privacy and data security mandates on their subcontractors and to monitor them to ensure compliance.
6. Include privacy and data security performance expectations and measures in service level agreements, including timeframes for addressing risks and reporting security incidents.
7. Require cloud providers to return or destroy, at the organization's request, all copies of the organization's data when the service agreement ends.
8. Define specific security incident reporting and response requirements, including timeframes, cost allocation, and responsibilities for handling data breaches and any ensuing liabilities.
9. Obtain the right to audit or otherwise regularly assess and review the cloud provider's privacy and data security practices using common assessment methods, such as direct audits, vendor self-assessments, and independent third-party audits, assessments, or certifications.
10. Address risk allocation, especially if a security incident occurs. Service agreements should cover responsibility and cost allocation for regulatory penalties or other liabilities if service providers fail to meet privacy and data security requirements. Also consider requiring cloud providers to maintain cyber insurance coverage.

CYBERSECURITY

Yahoo Says Hackers Stole Data on 500 Million Users in 2014

Experts have called it the biggest data breach to date. At least 500 million Yahoo users' account information was stolen by hackers in 2014.

In a statement, Yahoo said user information – including names, e-mail addresses, telephone numbers, birth dates, encrypted passwords, and, in some cases, security questions – was compromised in 2014 by what it believes was a "state-sponsored actor."

According to the *New York Times*, Yahoo is one of the Internet's busiest sites, with one billion monthly users and one of the oldest free e-mail services. Many users have built their digital identities around it, from bank accounts to photo albums and even medical data.

"The stolen Yahoo data is critical because it not only leads to a single system but to users' connections to their banks, social media profiles, other financial services and users' friends and family," said Alex Holden, the founder of Hold Security, which has been tracking the flow of stolen Yahoo credentials on the underground web.

"This is one of the biggest breaches of people's privacy and very far-reaching."

Upon discovering the breach – two years after it occurred – Yahoo instructed users to change their passwords and stay vigilant over their other online accounts. Yahoo said it was working with law enforcement agencies in their investigations.

Yahoo said it learned of the data breach this summer after hackers posted to underground forums and online marketplaces what they claimed was stolen Yahoo data, the *Times* reported. A Yahoo security team eventually found the breach.

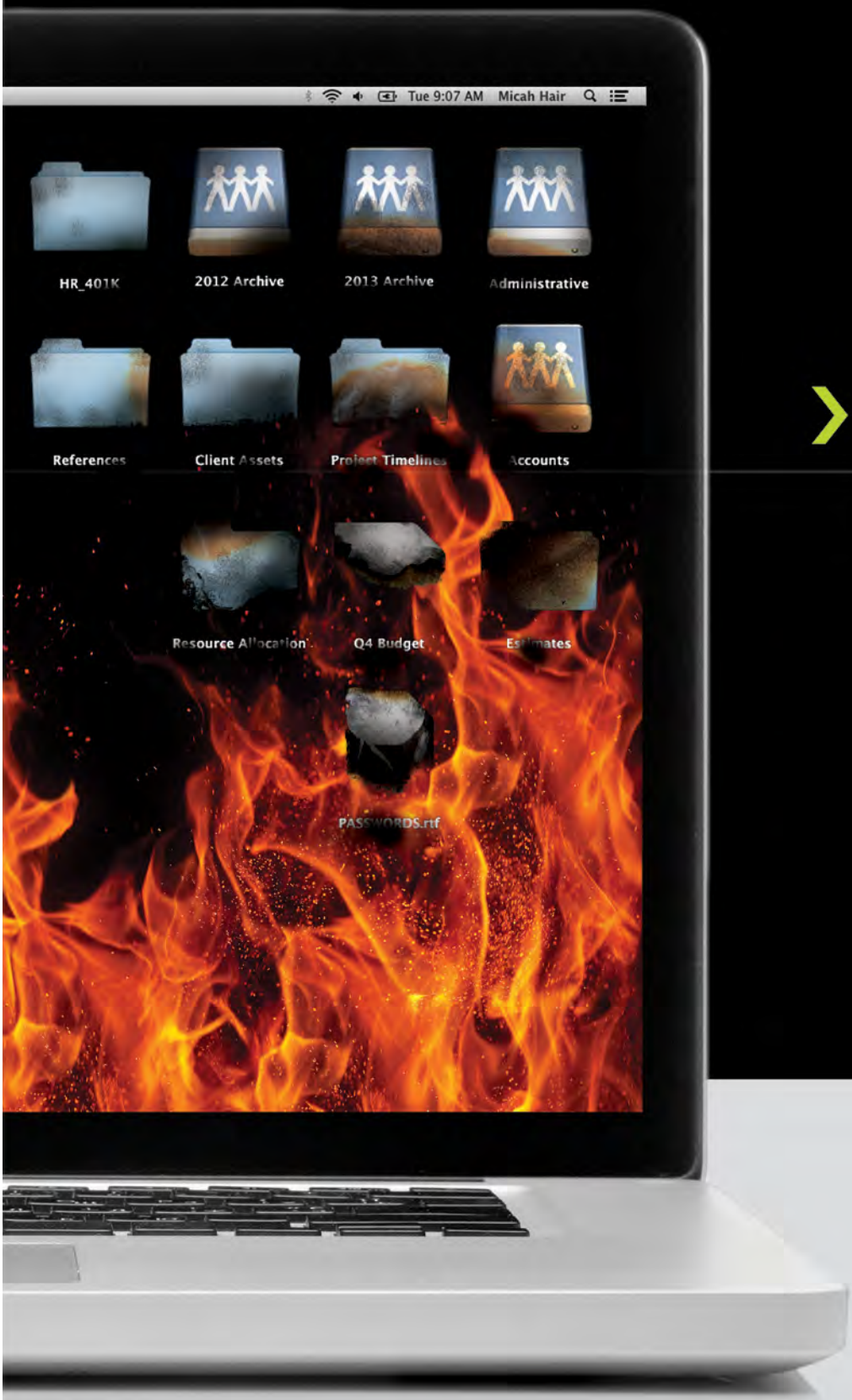
According to the Ponemon Institute, which tracks data breaches, the average time it takes organizations to identify such an attack is 191 days, and the average time to contain a breach is 58 days after discovery.

Security experts told the *Times* that the breach could result in class-action lawsuits on top of other costs. An annual report by the Ponemon Institute released in July found that remediating a data breach costs $221 per stolen record. In Yahoo's case, that would total more than $4.8 billion – the price Verizon Communications is purchasing Yahoo for. The *Times* said it was not clear how the breach would affect the acquisition.

Sen. Mark R. Warner, a Democrat from Virginia and former technology executive, issued a statement that said the "seriousness of this breach at Yahoo is huge."

He has called for a federal "breach notification standard" to replace data notification laws that vary by state. Warner added that he was "most troubled" that the public was only learning of the incident two years after it happened.

END



Don't get burned by MISMANAGED INFORMATION.

NEXT™ LEVEL

information governance assessment

Your amount of sensitive customer and business data is doubling by the year. And a little loss could have a big impact on your bottom line. Now more than ever, the way you manage your company's information matters. Find out where you stand with the Next Level Information Governance Assessment. Through this self-administered online assessment tool, you'll discover areas of strength. You'll also uncover opportunities for improvement. In the end, you will be empowered to increase your organizational transparency and data integrity.

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

Data Privacy Meets a World of Risk:

A Landscape in Turmoil

John C. Montaña, J.D., FAI

2016 continued a tumultuous string of years for privacy law and for those charged with implementing it and managing the records affected by it. Prior years saw an assortment of inter-governmental squabbles related to eavesdropping by U.S. intelligence agencies, disputes over intelligence sharing for counter-intelligence purposes, and ongoing concerns in Europe over the adequacy of the Safe Harbor arrangement between the European Union (EU) and the United States.

In each of these cases, there was tension between the purported need to make information transfers and the countervailing desire of governments or individuals to keep information private. The cases created issues for organizations outside of government, caught as they often were between conflicting demands and responsibilities on both sides of the Atlantic and their own needs to use personal information for business purposes.

Safe Harbor Gives Way to Privacy Shield

These issues were distilled in *Schrems v. Data Privacy Commissioner* (C-362/14 (Oct. 6, 2015)), in which law student Max Schrems sued in the European courts, alleging that Facebook's policies and practices violated EU data privacy law, and, thereby, so did the Safe Harbor Agreement, which permitted transfer of EU data from the EU to the United States under specified conditions.

Shield Cedes Power to DPAs

Late in 2015, after years of litigation, the European High Court of Justice in the *Schrems* case finally issued a ruling. The decision did not, strictly speaking, invalidate the Safe Harbor Agreement. Rather, the court ruled the agreement was nonbinding on national data privacy authorities (DPAs), throwing 20 years of practice and doctrine into a state of great uncertainty.

The *Schrems* decision had the effect of allowing a national DPA to find a violation for *any* data transfer to the United States. Given the extent and duration of data transfer that had occurred, and the scope of potential penalties – up to 4% of a company's worldwide revenue – this new DPA power was, and remains, a matter of considerable concern to all.

Data Privacy Regulation Brings Little Relief

2016 at first seemed to have brought relief from the court's decision. Early in the year, the European Union published the new General Data Privacy Regulation (GDPR), as well as the EU-U.S. Privacy Shield Agreement, which were intended to relieve the uncertainties arising from the Safe Harbor Agreement – and its demise in the courts – and from the ongoing problems organizations faced with the pre-existing privacy regime and its 28 country-specific privacy regimes.

Litigation Threatens Privacy Shield

The small relief from these developments may be short-lived, however. The successful plaintiff in the Safe Harbor litigation has already made it clear that he's dissatisfied with the terms of the Privacy Shield and intends to litigate it. Thus, even before it had been formally adopted by the parties, Privacy Shield faced an uncertain future that is not likely to be decided for several years.

Parties who relied on Safe Harbor, and who then looked to Privacy Shield to permit cross-border data to continue, are now faced with an extended period of uncertainty as Privacy Shield slowly works its way through the courts. Given the scope of those transfers, the underlying value of the business they represent, and the near impossibility of unwinding already-comingled data sets should Privacy Shield ultimately be invalidated, this is very high-value uncertainty indeed.

GDPR Fails to Unify Rules

The GDPR likewise offers far less certainty than it seems to at first glance. In theory, it replaces as many as 28 sets of rules that an organization might be subject to with a single set of rules. Except that it does no such thing.

Under the prior regime, national DPAs had complete autonomy – they answered to no one, and all promulgated such rules as they saw fit, applicable to organizations operating within their jurisdiction. This has not changed; each still has plenary and unchallengeable authority. And therein lies the rub.

Although the GDPR encourages DPAs to cooperate and to develop a single set of rules for any organization, they are not actually required to. So, maybe this will happen and maybe it will not. There is no mechanism to

Despite this year's passage of the EU-U.S. Privacy Shield agreement and the EU's General Data Privacy Regulation, the privacy landscape remains unstable, leaving organizations uncertain about their next steps. This article explores the causes of the instability and suggests how organizations might respond.

force such things, and, in fact, the GDPR reaffirms each DPA's absolute independence and authority. As a result, organizations must now play this hand and discover how it's really going to work – which will again take several years to shake itself out, even under the best of circumstances.

Even if it plays out as planned, there may well be very disparate results. The EU countries have taken different approaches to privacy, ranging from extremely prescriptive and detailed regulation in places such as France and Germany, to a relatively light hand in places like the United Kingdom – whose impending exit from the EU (i.e., "Brexit") ensures additional complication.

That means an organization based in France, whose DPA is supposed to manage the rules-rationalization process for it, could well find itself subject to a much more prescriptive and challenging set of rules than one fortunate enough to be based in, say, Ireland.

The GDPR likewise does not affect the current rules quagmire. Rules currently in effect remain in effect, and national DPAs are in no way inhibited from enacting new rules in line with their existing philosophies. The most that can be done is to delay a rule's implementation for a year if the authorities at the EU level disagree with it. And, again, those rules vary widely from country to country and are likely to continue to vary.

Organizations Must 'Wait and See'

At the end of the day, the GDPR's harmonized rulemaking process amounts to little more than a series of suggestions to the national DPAs that maybe they should consider changing some things. Maybe they will, but maybe they will not. So, again, organizations are forced into a waiting game to see if what amounts to wishful thinking by the EU authorities actually results in changes on the ground that will make the issues simpler.

At the end of the day, the GDPR's harmonized rulemaking process amounts to little more than a series of suggestions to the national DPAs that maybe they should consider changing some things.

All of this poses significant questions to trans-Atlantic organizations and to those operating only within the EU: "Should we gamble on the continuing viability of Data Shield, or should we plan a future with more restrictive transfers of data outside the European Union? Can we plan on a single rule set within Europe, or must we continue to deal with multiple regimes? And what about Brexit?"

Making a significant change in management practice based on an assumed future is likely to be expensive: vast data sets might somehow have to be parsed out; new systems designed, built, and configured; and long-standing business practices changed. It could all be bad enough if the guess is right, but possibly catastrophic if the guess is wrong.

Terrorism May Force Direction Change

An entirely countervailing influence arises from the issue of terrorism. Europe has been shaken in 2016 by deadly terrorist acts. And, as authorities investigate the incidents and seek to prevent future ones, they find themselves hampered by the restrictiveness of their own privacy laws. Two of the countries with the most restrictive laws, France and Germany, have been hit particularly hard by terrorism. According to two recent *Wall Street Journal* (*WSJ*) articles, both countries are taking a long look at whether the concept of data privacy has perhaps swung too far in one direction. This could play itself out in a couple ways.

Legislation May Loosen Restrictions

First, there might be legislative changes that relieve restrictions on such things as data transfer, short mandatory periods of retention, or data sharing. As the *WSJ* articles point out, such relief would significantly improve the capabilities of law enforcement, which has found itself hampered by aggressive, privacy-driven retention policies, or by the fact that existing data is subject to transfer and sharing restrictions. This is, in fact, what France and Germany, and no doubt other countries, are contemplating.

That, however, is a relatively long-term solution, if ever it comes, and it would result in changes only to those matters directly specified by the legislation.

Quicker and broader relief might come much sooner in the simple form of lax interpretation and enforcement.

Enforcement May Be Weak

This would be nothing new. Safe Harbor – and privacy compliance generally – have always been to some extent a sham. Organizations claimed compliance with a complex set of laws they barely understood and frequently violated; as long as the organizations stayed under the radar and did nothing egregious, the European authorities turned a blind eye towards what was happening. Enforcement has generally been directed at high-profile offenders with deep pockets, such as Facebook and Google.

Schrems and the lawsuit that ultimately brought down Safe Harbor put a spotlight on data management practices, but terrorism concerns could change it right back. DPAs, legislators, and judges in the EU face the question of how tightly they want to enforce whatever privacy law may be in effect, and the reality that zealous privacy enforcement may well – and sometimes clearly does – conflict with effective law enforcement and counterterrorism activities.

Given that reality, Schrems may well find a less receptive audience for his future arguments. The more terrorist attacks there are in Europe, the more likely this is to be true. And, ultimately, data privacy is what the DPAs and the courts say it is. If they choose to see it – and enforce it – less restrictively, legal theories to the contrary will not count.

In the Meantime…

So where does all of this leave organizations? That's a question whose answer has multiple parts.

Use the Privacy Shield

First, because Privacy Shield is for now the law of the land, organizations should avail themselves of its protections. It would take years to get a lawsuit through the courts, and in the meantime a lot can happen. Further, there's no guarantee the next ruling will be a winner. At worst, Privacy Shield buys an organization a few years; at best, it's all that's needed.

Lobby for Rules Unification

Organizations can ask the DPA in their jurisdiction to work with the other DPAs to develop a single regulatory framework. Their worst result would be a unified regime that's as bad as the worst one they're subject to now, which means there's little downside to such a move. More likely, nothing substantive would come of it. But there's always a chance that things could actually get better.

Build in Privacy Controls

If building or configuring new systems, build them to minimize data privacy problems in the first place. Much of the need for Safe Harbor and Privacy Shield arises from the fact that people built systems and moved data first and thought about data privacy laws second.

Wait for More Change

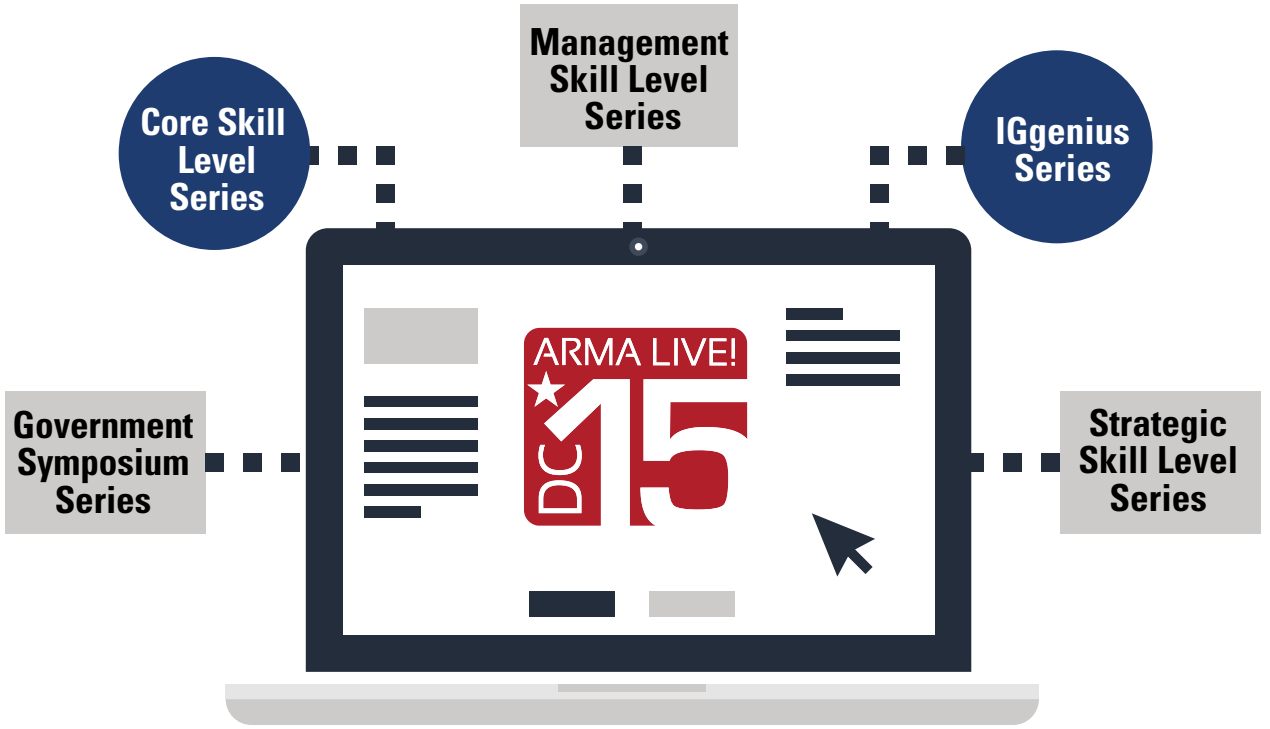
Beyond that, wait. It will take much time before the national DPAs, courts, and other relevant parties figure out how to operate in the new landscape. Until they give a clear indication of where they're going, it's much too early to reconfigure existing systems or rearrange complex business processes, with all the attendant costs and issues. To repeat, a wrong guess now could indeed be costly later.

On the other hand, it's not a good idea to assume nothing will ever change. Very likely, there will be substantive changes to the landscape that will require changes for organizations. Indeed, the best path is to wait and watch, while keeping all options open as long as possible. **END**

John C. Montaña, J.D., FAI, can be contacted at jcmontana@montana-associates.com. *See his bio on page 47.*

NOW SHOWING WEB SEMINARS

What's Your Type?



Regardless of how you define yourself, there's a web seminar series for you! Visit the ARMA Bookstore to catch up on what you missed at **ARMA Live! Conference 2015.**

Reg: $479 Pro: $349

View online now!

ARMA INTERNATIONAL BOOKSTORE

www.arma.org/bookstore

Click on "Web Seminars" or search for ARMA 2015

Tips for Globalizing a

U.S.-Based Records Retention Schedule

U.S-based organizations that try to globalize their U.S.-focused records retention schedules by simply extending them to include international requirements will fall short in meeting their compliance obligations. Discover the problems this approach creates and how to avoid them.

Tom Corey, Esq., CRM

For years the processes of creating, implementing, and maintaining records retention schedules for organizations with an international footprint were U.S-focused. The schedules addressed U.S. requirements and were designed to minimize the impact of the litigious U.S. business environment. Addressing the records created and maintained by international offices often was an afterthought or considered the responsibility of those offices.

But the increased use of electronic records management systems that cross borders and the passage of stricter data privacy and recordkeeping laws are forcing organizations to address international recordkeeping requirements when creating and maintaining a single, unified retention schedule.

Organizations often begin by trying to implement their U.S. schedule for their international operations. While at first this might seem like a cost-effective approach, it leads to problems the organization must address. What follows are examples of these problems with their potential solutions.

Problem 1: Meeting Widely Varying Requirements

International retention requirements vary greatly, with both minimum and maximum requirements for certain records.

Factors to Consider

Though picking the maximum retention requirement as a default is a common practice in the United States, this doesn't work for a global schedule. Variations in retention requirements for similar records are within years in the United States, but may vary by decades in other countries.

For example, U.S. state wage and hour records retention requirements range from one year in Georgia, Kentucky, Louisiana, and New Mexico to – at the other end of the spectrum – six years in Hawaii, New Jersey, and New York; the U.S. federal requirement is three years. So, choosing six years as the retention period for U.S. employee payroll and time card data is not overly burdensome.

However, international retention requirements for payroll and personnel records range from a maximum of two years after termination in countries with strict privacy policies, such as the Netherlands, to as many as 50 years in Bulgaria, Lithuania, Poland, and Romania. Therefore, choosing a 50-year retention period would not only be far more burdensome, but would present a conflict for organizations that operate in both Eastern Europe and the Netherlands.

> U.S. terms found on many U.S.-focused records retention schedules often have no meaning to international users and will only confuse them.

A Solution

Use a "base" retention period for each record category, specifying a *variance* for those categories where relevant countries require a different retention period.

1. Identify the records the organization creates.
2. Identify the jurisdictions to which the organization's retention schedule is subject.
3. Determine a reasonable base retention period for each record category that will meet the requirements of all or most relevant jurisdictions to minimize the need for variances.
4. Specify variances for those categories for which relevant jurisdictions have different requirements.

Avoid using U.S. retention requirements for base retention periods and then creating variances to comply with international requirements. Because U.S. requirements are comparatively low, especially as they relate to accounting and contract limitations, using them to establish base requirements will necessitate more variances than if the relevant jurisdictions' requirements are used.

Problem 2: Using U.S.-Centric Terms

When organizations first develop schedules for their U.S. operations, they often rely on U.S. concepts and terms.

Factor to Consider

U.S. terms found on many U.S.-focused records retention schedules often have no meaning to international users and will only confuse them. For example, a records category called "I-9 Forms" to describe the form required in the United States to verify the employment eligibility of workers is meaningless to international offices.

A Solution

Name records categories for their *functions,* rather than for the forms that might be captured in these categories. So, instead of naming a records category "I-9 Forms," call it "Employment Eligibility" with a description that includes "the citizenship and/or immigration status of an employee that demonstrates a legal right to work within the organization."

Use this same approach for describing the purpose of certain tax forms, such as ERISA 5500, IRS 1099, and financial control records like those required under Sarbanes-Oxley. Other countries that have an impact on a retention schedule may have similar forms that can be listed as examples.

Problem 3: Recognizing Unique, Non-U.S. Requirements

Many countries have unique traditions that must be identified and addressed.

Factors to Consider

Because other countries' unique traditions may be unfamiliar to U.S.-based companies, a U.S.-based records retention schedule may not include a records category that will accommodate them. For example, stamp taxes, which are levied on documents used to demonstrate the validity of certain transactions, are common in many countries. (The term originates from the concept of affixing stamps on a document to demonstrate the tax was paid.) This concept is foreign to most U.S. organizations, so there may not be an appropriate category for it on a U.S.-based retention schedule.

As another example, each employee in Vietnam has his or her own labor book. The employer holds the book, updates it with employee information, and returns it to the employee upon termination. This book is a part of recordkeeping in Vietnam, but it is not acknowledged in

most U.S.-based retention schedules, so it may not fit well into any records category on the schedule.

A Solution

When globalizing a schedule, an organization should consider the culture and unique requirements of each jurisdiction that impacts its recordkeeping obligations. In some situations, the schedule must include specific record categories to address these foreign concepts. In others, a records category description might be broad enough to encompass them. For instance, stamp taxes may be included under a category referred to as "other taxes," with stamp taxes listed as an example in the description.

Regarding the labor book example, an organization will need to maintain the physical employee labor book as required, but it could also maintain this information in its electronic recordkeeping system. However, while a requirement to retain information in a specific form does not necessarily preclude its retention in other forms more useful for global operations, the organization must be aware of restrictions associated with records media, location, and transfer before deciding to take this approach.

Taking on the World

No longer should international records and international recordkeeping obligations be afterthoughts. Instead, organizations should make sure to research their recordkeeping obligations based on the records they actually create and the records they should create. They should then create schedules, along with supporting systems, that accommodate these international variations. With this type of retention schedule, any organization should be able to "take on the world." **END**

Tom Corey, Esq., CRM, can be contacted at tcorey@hbrconsulting.com. *See his bio on page 47.*

Protecting Information Assets Using **ISO/IEC Security Standards**

The ISO/IEC 27000 *Information technology – Security techniques* series of standards takes a risk management approach that will enable information professionals to contribute to an information security management system featuring the controls needed to protect information assets against external and internal threats.

Lois Evans

Since 2005, an estimated 5,000 data breaches involving 675 million individual records have taken place worldwide, according to a November 7, 2015, article in *The Economist*, "Data Breaches in America: The Rise of the Hacker."

In the United States, data breaches have occurred across many industry sectors, including:

- Government defense (e.g., U.S. Army, U.S. State Department, National Security Agency)
- Finance (e.g., Morgan Stanley, JP Morgan Chase, Wells Fargo)
- Retail (e.g., Target, eBay, Home Depot, Staples)
- Communications and entertainment (e.g., Yahoo, Tumblr, Sony Pictures)
- Online service providers (e.g., Dropbox, Epsilon, Evernote)
- Medical services (e.g., Anthem,

Complete Health Systems, Advocate Health and Hospitals)

While the responsibility for information security has escalated to the executive level, many executives do not understand the threats their organizations face and find it difficult to keep up-to-date on the responses and products needed. As a result, some organizations lack sufficient protection while at the same time over-spend for it, paying $100 for every $50 of loss prevented, according to *The Economist* article "Cyber-Crime and Business: Think of a Number and Double It," published January 17, 2015.

ISO/IEC 27000 Is 'Family' of Standards

The ISO/IEC 27000 *Information technology – Security techniques* series of standards provides the information that executives and other stakeholders need to develop and operate a customized information security management system (ISMS) that is based on clearly communicated objectives and controls and incorporates features experts believe are essential for managing information as an asset.

The series, published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), includes nearly 20 standards. The first three, ISO/IEC 27000, ISO/IEC 27001, and ISO/IEC 27002, describe the vocabulary, requirements, and code of practice, while the balance provide general instructions for governance, security risk management, measurement, and auditing, as well as sector-specific instructions for finance, cloud services, energy utilities, and health. (See the "ISO/IEC 27000 *Information technology – Security techniques* Series" sidebar for the complete list of standards in this series.)

The series takes a risk management approach, enabling each or-

Information Technology –

Security Techniques

The ISO/IEC 27000 series is to information security what the ISO-9000 series is to quality assurance – a comprehensive set of standards that provides best practice recommendations for organizations of any type or size.

ISO/IEC 27000:2016	*Information security management systems – Overview and vocabulary*
ISO/IEC 27001:2013	*Information security management systems – Requirements*
ISO/IEC 27002:2013	*Code of practice for information security controls*
ISO/IEC 27003:2010	*Information security management system implementation guidance*
ISO/IEC 27004:2009	*Information security management – Measurement*
ISO/IEC 27005:2011	*Information security risk management*
ISO/IEC 27006:2015	*Requirements for bodies providing audit and certification of information security management systems*
ISO/IEC 27007:2011	*Guidelines for information security management systems auditing*
ISO/IEC 27008:2011	*Guidelines for auditors of information security controls*
ISO/IEC 27009:2016	*Sector-specific application of ISO/IEC 27001 – Requirements*
ISO/IEC 27010:2015	*Information security management for inter-sector and inter-organizational communications*
ISO/IEC 27011:2008	*Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*
ISO/IEC 27013:2015	*Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*
ISO/IEC 27014:2013	*Governance of information security*
ISO/IEC 27015:2012	*Information security management guidelines for financial services*
ISO/IEC 27016:2014	*Information security management – Organizational economics*
ISO/IEC 27017:2015	*Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
ISO/IEC 27018:2014	*Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*
ISO/IEC 27019:2013	*Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry*
ISO/IEC 27799:2016	*Health informatics – Information security management in health using ISO/IEC 27002*

ganization to tailor its ISMS to its own business environment to protect a range of information assets (e.g., financial, personally identifiable, confidential, and third-party) against specific threats and vulnerabilities.

In essence, the ISO/IEC 27000 series is to information security what the ISO 9000 series is to quality assurance – a comprehensive set of standards that provides best practice recommendations for organizations of any type or size. Importantly, the standards are battle tested: stemming from a 1995 British security standard (BS7799), they have been in place since 2005 and are reviewed and updated regularly.

In essence, the ISO/IEC 27000 series [of standards] is to information security what the ISO 9000 series is to quality assurance.

ISO/IEC 27001 Is Series' Foundation

The key to the ISO/IEC 27000 series is ISO/IEC 27001:2013 *Information security management systems – Requirements*. At 23 pages, ISO/IEC 27001 can be read through in one sitting, yet contains enough information to direct a months-long project. The first half consists of 10 narrative sections outlining the general requirements for an ISMS, while the second half consists of an annex listing the 14 key control objectives required for ISO/IEC 27001 compliance.

An easy way to approach the document is to skim through the narrative sections, read the annex to get a sense of the extent of an ISMS, and then return to the first section for a more in-depth read. Orienting to the controls listed in the annex provides a better sense of the effort required.

Narrative Sections Summarized

The ISO/IEC 27001 narrative sections include the following:

Scope: ISO/IEC 27001 specifies the requirements for an ISMS, based on assessing and treating information security risks specific to an organization.

Normative Reference: ISO/IEC 27000 *Information security management systems – Overview and vocabulary* is the normative reference for ISO/IEC 27001. ISO/IEC 27000 provides an overview of principles, processes, administration, and benefits of an ISMS, as well as an explanation of how the standards in the ISO/IEC 27000 "family" are related.

Terms and Definitions: The 80-plus security terms and definitions found in ISO/IEC 27000 apply to ISO/IEC 27001.

Context of the Organization: Each organization faces unique external and internal issues that affect its ability to achieve information security. Identifying these issues ensures that the needs and expectations of interested parties are met and that the scope of the ISMS is appropriate.

Leadership: Top management must ensure that information security objectives align with organizational objectives, that information security is integrated into business processes, that the appropriate level of resources is assigned, and that roles, responsibilities, and authorities are clear. Management must also establish an information security policy and ensure communication of and conformance with the policy.

Planning: Using a risk management approach, an organization must determine the risks and opportunities it faces, analyze and evaluate the risks, and define treatments.

Support: All persons working under an organization's control must be competent, aware of the security policy and their responsibilities, and understand what aspects of the ISMS may or may not be communicated. Documentation for the ISMS must be maintained, updated, and controlled.

Operations: Information security processes must be identified, implemented, and documented per the security objectives identified through risk assessment. Risk treatments must be implemented and documented.

Performance Evaluation: Organizations must determine what should be monitored and measured and when and how results should be analyzed and evaluated. Internal audits and management reviews are required at planned intervals.

Improvement: An ISMS must exist in an atmosphere of continual improvement. Non-conformity must be evaluated, corrected, and documented, with a focus on eliminating the cause so it does not recur.

ISMSs Require Collaboration

An ISMS depends on information governance (IG), which extends across both information security and records and information management (RIM). Importantly, the two disciplines share many priorities.

For example, the overall objectives of information security are most commonly expressed as preserving confidentiality, integrity, and availability (often referred to as CIA). According to ISO/IEC 27000, these objectives can extend to involve authenticity, accountability, non-repudiation, and reliability.

These objectives mirror the Generally Accepted Recordkeeping Principles® (Principles) of protection, integrity, and availability, and overlap

with the remaining Principles: transparency, compliance, accountability, retention, and disposition. In fact, RIM professionals and information security managers are partners in meeting IG objectives and can benefit the organization by fully understanding and supporting their colleagues' programs.

From this perspective, ISO/IEC 27001 provides RIM professionals with a starting point and vocabulary for considering and acting on areas of overlap between the organization's RIM system and the ISMS. Governance is an important issue in most collaborative efforts, where different teams often represent varying perspectives and priorities. ISO/IEC 27014:2013 *Information technology – Security techniques – Governance of information security* provides further guidance for those looking to collaborate across business units successfully.

ISMSs Focus on Risk Management

Another takeaway from the ISO/IEC 27000 series is the focus on risk. A RIM system typically includes elements of risk management, but not all RIM professionals have participated in the type of exercise required for defining or updating an ISMS. While ISO/IEC 27001 does list the basic elements of a risk management exercise, ISO/IEC 27005: 2011 *Information technology – Security techniques – Information security risk management* provides additional direction.

Risk management involves risk identification, analysis, evaluation, and treatment, based on a thorough consideration of an organization's context, the specific threats and vulnerabilities faced, the level of risk tolerance, and the availability and affordability of treatments. If properly conducted, these activities cannot be completed overnight. Risk identification alone takes significant effort, leveraging a range of activities such as brainstorming, interviews, checklists, scenario analysis, and/or business impact analysis.

In orienting to risk management processes, RIM professionals will appreciate the risk register approach typically used. In a *risk register*, each risk is entered as a line item in a spreadsheet, and data is entered as each item is analyzed, categorized, evaluated, prioritized, and considered for possible treatments. Risk registers can be used to create a risk table that visually depicts risk priorities and form the basis of the formal risk plan provided to top management to clarify and confirm security objectives, resourcing, responsibilities, timing, and prioritization.

Annex Provides Security Controls

The control objectives and controls listed in the ISO/IEC 27001 annex are aligned with those listed in the 90-page ISO/IEC 27002: 2013 *Information technology – Security techniques – Code of practice for information security management* and are numbered using the same schema.

According to ISO/IEC 27000, *controls* are the means of managing risk, such as organizational structures, policies, procedures, guidelines, and practices, while a *control objective* is a statement describing what is to be achieved as a result of implementing controls.

ISO/IEC 27001 and ISO/IEC 27002 examine 14 control categories, 35 control objectives, and 114 controls: ISO/IEC 27001 briefly introduces all items in tabular form, and ISO/IEC 27002 provides guidance for implementing each control.(See page 32).

As shown below, the ISO/IEC 27001 *control category* "8 Asset Management" lists three *control objectives:* Responsibility for Assets, Information Classification, and Media Handling.

Drilling down a level, the *control objective* for "Information Classification" is "To ensure that information receives an appropriate level of protection in accordance with its importance to the organization." This objective is achieved through three *controls*: Classification of Information, Labelling of Information, and Handling of Assets.

Drilling down another level, the *control* "Classification of Information" states: "Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification."

The complementary implementing guidance provided by ISO/IEC 27002 discusses the "Classification of Information" control in terms of the business needs and legal requirements for sharing and restricting information,

Control Category:
8 Asset Management
Control Objectives:
1. *Responsibility for Assets*
2. *Information Classification:* "To ensure that information receives an appropriate level of protection in accordance with its importance to the organization."
   Controls:
   1. *Classification of Information:* "Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification."
   2. *Labeling of Information*
   3. *Handling of Assets*
3. *Media Handling*

ISO/IEC 27000 Series Controls and Objectives

Control	Name	Objectives
5	Information security policies	Provide management direction and support in accordance with business requirements and relevant laws and regulations.
6	Organization of information security	Establish a management framework; ensure the security of teleworking and mobile devices.
7	Human resource security	Ensure that employees and contractors understand their responsibilities and are suitable for their roles prior to, during, and upon termination or change of employment.
8	Asset management	Identify organizational assets and assign protection responsibilities based on information classification and appropriate handling of media.
9	Access control	Limit access to information and information processing facilities, manage user access, and ensure users safeguard their authentication information, to prevent unauthorized access.
10	Cryptography	Ensure proper and effective use of cryptography to protect information.
11	Physical and environmental security	Prevent unauthorized physical access, damage and interference to information and information processing facilities and equipment.
12	Operations security	Ensure correct and secure operations, including: documenting operating procedures, protecting against malware and data loss; logging and monitoring to record events and generate evidence; preventing technical vulnerability; and minimizing the impact of audit activities.
13	Communications security	Ensure the protection of information in networks and in transfers.
14	Systems acquisition, development and maintenance	Ensure that security is integrated in all information systems, across their lifecycle.
15	Supplier relationships	Ensure protection of assets accessed by suppliers in line with supplier agreements.
16	Information security incident management	Ensure a consistent and effective approach is taken to incidents, including appropriate communication of events and weaknesses.
17	Information security aspects of business continuity management	Embed information security into the business continuity management system, including redundancy of information processing facilities.
18	Compliance	Avoid breaches of legal, statutory, regulatory, or contractual obligations and ensure information security reviews take place in accordance with organizational policies and procedures.

as well as the responsibilities of owners for classification of information assets in terms of confidentiality, integrity and availability. Importantly, with respect to the ISMS, information classification refers to the organization's access control policy rather than its retention and disposition policy.

While information security and records classification are not the same thing, there are potential overlaps that could be exploited. As an example, ISO/IEC 27002 states that classification "should be included in the organization's processes and be consistent and coherent across the organization," and, in particular, sensitive information must be protected from disclosure, but not to the extent that public information is not made available.

Many records schedules include details about records that contain personal or confidential information; optimally, an organization's record and security classifications could be combined within the same schedules, resulting in increased compliance and accessibility.

Series Can Help Build Partnerships

The ISO/IEC 27000 series represents an expansive body of knowledge designed to support information security professionals in their work. While RIM professionals do not require the same in-depth knowledge, they can benefit from knowing information security objectives and controls.

Identifying areas of overlap where collaboration can occur between the two business areas will encourage a culture of mutual support and understanding. To this end, ISO/IEC 27001 acts as a "CliffsNotes" / "Coles Notes" introduction to information security practice and a great way to orient to this challenging but increasingly important information domain. **END**

Lois Evans can be contacted at levans18@mail.ubc.ca. *See her bio on* page 47.

The New Waypoint Along the CRM Journey:

Certified Records Analyst

Jean Ciura, Ph.D., CRM

For some records and information management (RIM) professionals, the journey toward earning the Certified Records Manager (CRM) designation may appear to be or already has been too long. For others, the pursuit of the CRM may be hindered by limited time or financial resources. Still others may not need a certification as comprehensive as the CRM but need to demonstrate their professional competence. Anyone falling into one or more of these categories should consider a new certification offered by the Institute of Certified Records Managers (ICRM): Certified Records Analyst (CRA).

To earn the CRA certification, applicants must meet the same educational and professional experience that is required to sit for the CRM exam, but they need to pass only Parts 2, 3, and 4 of that six-part exam.

"We are excited to deliver the CRA certification to the RIM profession," said Brice Sample, president of the ICRM. "This new certification follows our time-tested approach and allows for more professionals to obtain a value-added RIM credential."

Earning the CRA designation demonstrates the individual has a

solid RIM foundation with knowledge and experience in the lifecycle management of active and inactive records and their systems, electronic records, regulatory compliance requirements, and more.

RIM professionals who attain the CRA will potentially be on the path to attaining the CRM designation. Sample, in fact, said the ICRM fully expects "many to use the CRA as a spring-board to achieving their CRM over a timeline that meets their individual needs."

Qualifying for the CRA

Potential candidates must submit an application form online (available at *icrm.org*) with supporting documentation of earning a four-year (bachelor's) degree from an accredited institution and having at least one year of professional RIM experience. Alternatively, one year of professional RIM experience can be substituted for each year of college education.

Applicants may not sit for the exams until their application has been approved.

According to the ICRM, CRM candidates that have already passed Parts 2, 3, and 4 of the examination are eligible for immediate CRA certification. Sample said the ICRM already has contacted those who are eligible under this criteria and will invite those who become eligible in the future to declare the CRA credential. He advises any candidates who believe they are eligible but have not been contacted to call the ICRM business office at 877.244.3128.

Preparing for the CRA Exam

The ICRM has resources to support CRA candidates, an annotated bibliography, sample questions, and guidance that is available online, and a licensed Examination Preparation product that offers comprehensive workshops for CRM exam Parts 1 through 6, including case studies.

RIM professionals who attain the CRA will potentially be on the path to attaining the CRM designation.

The product is delivered through ARMA chapters and industry-specific associations. Other materials relevant to RIM competencies and educational sessions are offered through ARMA International. For a comprehensive list of materials, resources, and prep workshops, go to *www.icrm.org/exam-preparation-resources*.

Taking the CRA Exam

The exam requirement consists of CRM Exam Part 2 (Records Creation and Use), Part 3 (Records Systems, Storage, and Retrieval), and Part 4 (Records Appraisal, Retention, Protection, and Disposition).

The exams, which are offered on a quarterly basis at Pearson VUE professional testing services around the world, can be taken together or in any order, but candidates must pass all three parts within five years of their acceptance as a candidate. Dates for each exam cycle are posted on the ICRM website at *www.icrm.org/public/exams/*.

Maintaining the Certification

The CRA maintenance process ensures that members maintain professional competencies, update their existing knowledge and skills, and continue to attain new knowledge and skills. Active CRAs must submit 100 certification maintenance points for approved educational activity during each five-year period following initial certification.

Going the Next Step

Once certified, CRAs who wish to pursue the CRM certification can elect to take the additional parts of the CRM exam (i.e., Parts 1, 5, and 6) at their own pace (not limited to the five-year exam cycle). Credit toward the CRM is awarded for having passed Parts of 2 through 4 during the CRA certification process.

Taking Advantage of Other CRA Benefits

Earning the CRA provides many benefits of ICRM membership. CRAs may:

- Vote in ICRM elections
- Serve as a member or chair of an ICRM commission, committee, or task force, although the CRA cannot hold office
- Attend the ICRM business meeting and the ICRM reception held annually at the ARMA International Annual Conference & Expo
- Access the ICRM website, the membership directory, and all publications and information provided as a benefit of ICRM membership

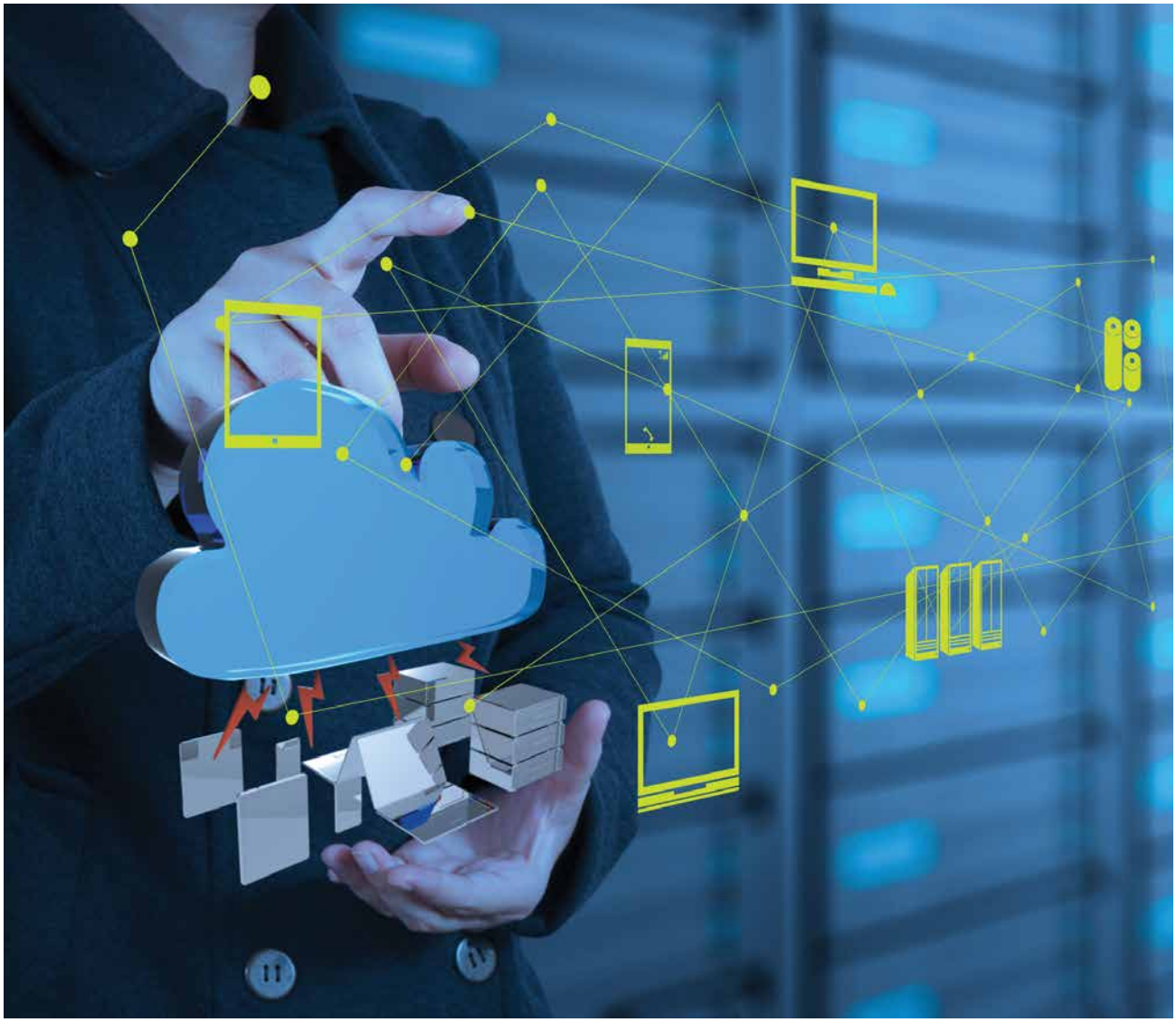
Learning About the ICRM

The ICRM is an international certifying organization of and for RIM professionals. It was incorporated in 1975 to establish a standard by which persons involved in RIM could be measured, accredited, and recognized according to criteria of experience and capability established by their peers. The primary mission of the ICRM is to develop and administer RIM certifications. It serves as the certifying body for the CRM, CRA, and the CRM-NS designations; the CRM-NS is the Nuclear Information and Records Specialist designation conferred to CRMs who meet NS qualifications. **END**

Jean Ciura, Ph.D., CRM, can be contacted at jean.ciura@yahoo.com. *See her bio on page 47.*

Establishing a Records Appraisal Workflow

Maik Schmerbauch, Ph.D.



Although many standards and other publications advise on the ways to properly manage physical records, theoretical knowledge from reading about it is no substitute for practical experience. This case study describes the workflow established for a records and information management (RIM) project to appraise and manage the inactive records of the procurement unit in a United Nations (UN) agency in Germany.

Setting the Stage

RIM as its own operating section was established in the middle 2000s as a result of the release of the UN's formal archive and records management program, which had been authorized by the secretary general. It declared: "Archives and Records Management Section shall be responsible for establishing policy and setting standards, including the design of record-keeping systems and procedures for the management of the records and archives of the United Nations, including their use, storage, retention and disposition and access rights."

Before the RIM unit became operational, each unit of the secretariat conducted records management with unique filing techniques according to its professional requirements and stored its records in a separate repository. Shortly after the secretary general's proclamation, RIM was staffed, minimally, and the department created its own policies and procedures based on the international recordkeeping standard ISO 15489-1:2001 *Information and documentation – Records management – Part 1: General*.

RIM therefore had to manage information to ensure that it was accurately documented, that business records were managed efficiently, and that they remained suitably accessible during their retention periods. In addition to performing its daily records and document management operations, the young RIM section functioned as the records center for inactive records with a retention requirement and as an archive for records classified for permanent preservation.

RIM conducted several records appraisal projects for such departments as human resources and the procurement unit as part of the general administrative program, which for two decades had secured inactive records in a single storage repository – a room with shelves but without archival order or any appraisal or classification procedures. Anyone who required access to the inactive records had to search for them manually.

In 2013, after RIM had conducted several smaller appraisal projects, the procurement unit requested professional help on its entire inactive physical records collection. Afterwards, RIM developed a qualified project proposal and delivered it to management, which acknowledged the need for the project and provided the resources.

Getting Started

After the project proposal was developed, RIM and the procurement unit negotiated the project workflow, time schedule, and resources. Project managers and temporary RIM professionals were added, as was a staffer from the general services department who helped with records transport and destruction.

Upfront, RIM developed the retention schedule and the records classification scheme (RCS) according to UN standards, but tailored for the organization's special requirements. The organization-based RCS for the procurement unit was numerical, and in addition to describing per position a special procurement records series, it described the series content and its confidentiality and security requirements.

The RCS covered 15 main records series with their related retention requirements. Retention for inactive records had been set by the retention schedule, with a special trigger – for example, 10 years after their expiration date. As shown in Figure 1 "Retention Schedule Excerpt," the retention schedule for the procurement department included the metadata schedule number, title, retention period, disposition, notes, trigger, and the related offices of creation of the records.

Developing the Workflow

The workflow developed by RIM contained these eight steps:

1. Locate all inactive procurement records in the storage repository and in the clerks' offices.
2. Conduct a complete first inventory for an overview.
3. Create storage according to records series classifications.
4. Set records retention with appraisal according to the series for preservation and destruction.
5. Transfer the records for preservation into RIM repositories and conduct physical disposal of the records whose retention periods had expired.
6. Clarify the future retrieval process in the archival database.
7. Train the procurement employees on the practical RIM processes.
8. Review the project and compose a justification report for all stakeholders.

FUNCTIONS (Level 1)	ABBR.	No	ACTIVITIES (Level 2)	No	SUB-ACTIVITIES (Level 3)	Scope Notes	Title instructions
Procurement	PRO					Records and non-record copies related to the office procurement activities.	
		01	Contract Management			File here: Case folders for non-record copies of contracts, leases and institutional or corporate agreements. Records related to the management of the contract, including correspondence with the vendor.	Title will consist of: Name of Contractor and/or Type of Contract [.] Year
		02	Purchase of Goods and Supplies	01	Files for the acquisition of good and supplies under $4,000	File here: Records relating to Requisitions and purchases including bids, proposals, quotations, invoices payment records, etc	Title will consist of: Name of contractor and/or PO number [.] Year
				02	Files for the acquisition of goods and supplies over $4,000	File here: Non-record copies relating to Requisitions and purchases including bids, proposals, quotations, invoices payment records, etc	Title will consist of: Name of contractor and / or PO number [.] Year

Figure 1: Retention Schedule Excerpt

The project can be viewed as a prototype for continued improvement and success at the UN and is applicable to other public and private organizations.

Step 1

The process of locating all functional procurement business records was conducted in close consultation with every procurement staff member in order to have a clear knowledge of the inactive records and their locations. The procurement records were located in the procurement storage repository and on shelves in staff offices. The records had been kept by procurement in containers, binders, hanging folders, boxes, and loose paper collections. The next step was to conduct a basic inventory of all these records.

Step 2

All inactive records from the offices were transferred into the inactive procurement repository and a written inventory was produced by the project manager. The inventory covered the running number of the folder range and the written text on the folder labels. Besides indexing, the project managers reviewed each folder for clarification – that is, they pulled out folders covering only non-records when it was absolutely clear or they denoted empty folders with no content. (These exceptions were collected for later disposal.) As a result, RIM got a first qualified impression of the kind of records with the inventory lists.

Step 3

The classification procedure was performed with the RCS. Eight main records series – 60 linear meters (approx. 197 linear feet) of physical records – were classified in periods from the early 1990s to 2013; of this, about seven linear meters (approx. 23 linear feet), or about 12%, consisted of non-records. The inactive records consisted of the series of procurement contracts, competitive bids, vendor files, procurement procedures, invoices, procurement committee files, procurement staff files, and several records classified as working and reference files.

Step 4

The retention scheduling and appraisal process had to be conducted separately for every records series. All records were appraised according to their retention into 1) records for permanent or temporary preservation or 2) records that were already due for destruction.

As an example, typical procurement records series are the contract files. These confidential classified files were the basis for the organization's mostly long-term procurement activities with vendors. The contract files contained the official signed contract with the special procurement terms, as well as the contract-related records such as the processed selection criteria, contract extensions, and additional explanations of vendor and clerk correspondence. The retention of the contract files records series was set at 10 years and the trigger matched the contract expiration and end date.

Step 5

After the appraisal procedure, the procurement records were transferred in blue, acid-free folders to RIM for permanent and temporary storage in blue-acid boxes; they were labelled with the special metadata of the records series requirements and with a single signature. The preserved records were stored professionally in a RIM repository. The non-records and expired records were professionally shredded.

Step 6

Next, RIM organized the future retrieval and request process for the procurement clerks. All metadata from the transfers were implemented in the RIM electronic archival database, where every request could be further processed.

Step 7

For the future professional management of active and semi-active records, the procurement clerks were trained to manage their records throughout their life cycle according to RIM requirements, relying largely on the retention schedule and RCS.

Step 8

Afterwards, the RIM project manager wrote a project report for all stakeholders. It covered all developments and had information about the project's progress and all important project-related metadata, such as statistics of records series.

Looking Back

The process and its steps were successful. The project was completed within its estimated time frame, and it raised the visibility and esteem of RIM and its stakeholders. Other organizational units contacted RIM for support with their active and inactive records. The project can be viewed as a prototype for continued improvement and success at the UN and is applicable to other public and private organizations. **END**

Maik Schmerbauch, Ph.D., can be contacted at schmeichi@web.de. *See his bio on page 47.*

A New Approach to Scanning

If you are looking to get rid of your paper more quickly, simply buying a faster scanner won't help you. You're going to have to dig a little deeper than that.

For years, OPEX has studied the document scanning process. Like you, we've realized the excessive amount of labor costs associated with scanning. We have not only identified the problem, but have also provided the solution to minimize or eliminate much of that document prep.

REALIZE YOU HAVE A PROBLEM

In most situations, document prep is lost labor. There is no value, just hours of work to get paper ready based on the needs of the scanning device, rather than the needs of the business. The first step to understanding your prep requirements is to realize that you have a problem!

In most cases, if you ask the scanning manager about prep, they will tell you there is no problem at all. Prepped work magically shows up at the front of their scanner and off they go. If you ask the operations manager, they will shrug and tell you it's just the cost of doing business, explaining that if you want to scan, you have to prep, nothing much to talk about. So to understand the issue of prep you have to go back further in the process to understand exactly what takes place with the paper.

AN UNMANAGABLE PROCESS

Take inventory:

How does the paper come to you?

Is it delivered by the post office? Inter-office mail? In banker boxes or just a stack of file folders?

How many people touch it before it is scanned?

Does it go from department to department? Desk to desk? Person to person?

What do you have to do to it?

Do you open it? Remove staples? Tape torn pages? Sort it into batches? Copy small items or tape them to larger pages? Stamp received dates? Stage it for scanning?

In fact at OPEX we have identified roughly 25 prep activities to date.

- Is there a different scanner that can help mitigate this prep?
- Why you do all of these tasks? Do you perform all these steps for the business? Or are you performing them to match the capabilities of the scanner?

We've heard directly from our customers time and again who verify industry reports that document prep labor accounts for upwards of 70% of the cost of document scanning.

SANITY. RESTORED.

FalconV™ combines the performance of a high capacity production scanner with OPEX's unique prep-reducing process. With two additional sort bins and enhanced multi-feed detection, FalconV increases the functionality and flexibility of its universal document scanning workstations. From forms processing, insurance & mortgage documents, invoice capture, backfile/archive scanning, to medical records, legal discovery, and digital mailroom, FalconV is designed to attack the most difficult workflow challenges.

FalconV allows operators to prep and scan documents at significantly faster rates than can be achieved using the traditional multi-step process of separating, prepping and then scanning the pages. By combining these steps into a single process, labor costs are dramatically reduced.

FalconV is engineered to process a variety of document types, from thick paper to onion skin and fragile or damaged pieces, to envelopes and file folders stuffed with receipts, odd-shaped pages, and business cards. FalconV can even take on difficult challenges other scanners will not touch, including X-rays and three-dimensional objects – nearly any style or type of "document" can be scanned.

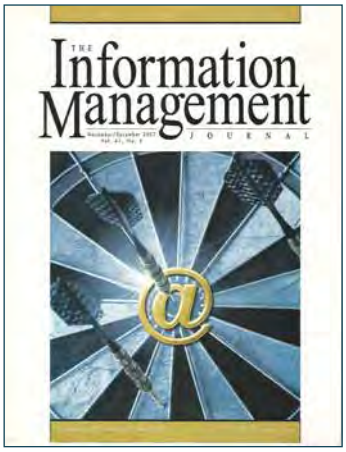
Designed with five sort bins, FalconV offers enhanced sorting capabilities. An additional pass-through bin allows large or delicate documents to be scanned. Seven strategically placed Ultrasonic Multi-Feed Detectors (MFDs) recognize the slightest paper overlap wherever it occurs, practically eliminating any chance of multiple pages being scanned simultaneously. This capability vastly improves the overall scanning process and helps to eliminate the problem of missing documents.

Now go tell the world!

For more information, visit opex.com

OPEX CORPORATION

10 Years
Looking Back...



Because this magazine was a quarterly until 1999, there are no November/December issues from 1967 or 1992 at which to look back. This issue's special section highlights the Nov/Dec 2007 issue.

November/December 2007
The Information Management Journal

Association News

- Hot Off the Press! *Procedures and Issues for Managing Electronic Messages as Records* (ANSI/ARMA TR 02-2007) and *Requirements for Managing Electronic Messages as Records* (ANSI/ARMA 9-2004)
- ARMA International is promoting its "Keeping Good Company" DVD-based staff training program produced by Kahn Consulting, Inc.
- ARMA International is promoting its Risk Profiler Self-Assessment suite of diagnostic tools, with content provided by NetDiligence and LeCG.

Articles

- Taking ECM from Concept to Reality," by Jeffrey D. Bridges, Esq.
- "Eight Steps to Successful Taxonomy Design," by Jim Connelly, CRM
- "The Sarbanes-Oxley Act: Five Years Later," by John Montaña, J.D.
- "How to Create and Facilitate Meetings That Matter," by Janice M. Francisco
- "Solving the Unmanaged Content Conundrum," by Addie Mattox
- "Putting Retention Management on the Right Track," by Nikki Swartz

Advertising

- 3M – "Automate file tracking and save time for…well, everything else you need to do today."
- Access Sciences – "[Perception] We have good archiving and search tools, so our discovery problems are solved. [Reality] Your company is keeping way more information today than needed – for compliance or for knowledge sharing."
- AIIM – "ready. aiim. learn. Learn How to Improve Your Business Processes."
- Allegheny Paper Shredders – "SelecShred Adjustable Screen. Double your security at the touch of a button!"
- Bankers Box – "STRONGER THAN YOUR BREAK ROOM COFFEE"
- BELFOR Property Restoration – "We listen. Clean and simple."
- DACS – "You're one in a 60 million."
- Dahle – "Shred It Yourself!"
- DHS Worldwide – "TOTAL RECALL Records Management Software. Experience the most flexible and comprehensive records management software in the world."
- FileTrail – "Stranded by your RIM vendor? Get on board with FileTrail and never be left behind again."
- Information Requirements Clearinghouse – "Are you taking the right steps to your retention schedule?"
- Iron Mountain – "Sally files it. Jack prints it. Jen downloads it. Tim PDFs it. Fortunately, you can trust one company to protect it."
- MBM Corporation – "Before a discarded document comes back to bite you… Shred it at the Source."
- NAID – "TOSS OR SHRED? Who Are You Relying On To Meet Your Information Destruction Compliance Requirements?"
- O'Neil Software – "Scan. Store, Manage. Deliver.™"
- OmniRIM – "Take Control of Your Records Management."
- Paige Company, The – "Ordinary boxes hold stuff. Ours are built to hold your future."
- Recall – "THEY SAY, 'Nobody's Perfect.' WE SAY, 'How Hard Are They Trying?'"
- Securit – "Now you need it. Now you don't. SECURE. Information management and destruction."
- Tower Software – "Information without the excess baggage. Find critical content fast with TRIM Context."
- Visioneer – Visioneer OneTouch with Kofax® VRS™ technology automatically enhances the quality of scanned images."
- Zasio – "Point. Click. Save. When it comes to managing your electronic records, you'd be happy if Point-Click-Save were all it took. With Zasio, it is!" **END**

229 Strong. And Growing.

Congratulations to these **Certified Information Governance Professionals**

Mitchell Abrams
Elizabeth Adkins
Angela Akpapunam
Xavier Alabart
Anthony Allen
Pey-Jia Angell
Christine Ardern
Deborah Armentrout
DeAnna Asscherick
Randy Aust
Wendy Austin
Christie Baird
Robert Baird
Patty Baldacchino
Salvador Barragan
Christopher Beahn
Shawn Belovich
Richard Berlin
Mike Biancaniello
Margaret Boeringer
Isabel Bracamontes
Aaron Bryant
Susan Burd
Kiji Burston
Doug Caddell
Stacie Capshaw
Melissa Carlis
Diane Carlisle
Laurie Carpenter
Elizabeth Carrera
Alexander Carte
Mark Carter
Peter Casey
Anita Castora
Elizabeth Castro
Tod Chernikoff
Carol Choksy
Vicki Clewes
Andrew Cogan
Julie Colgan
Bud Conner
Dani Cook
Russ Cottle
Marvin Cross
Kristen Crupi
Becky Darsch
Lisa Marie Daulby
Nicholas De Laurentis
Melissa Dederer
G. Derk
Deborah Dotson
Christina Doyle
Sandra Dunkin
Priscilla Emery
Sarah Emes
Sofia Empel
Tony Epler
Debra Farries
Elizabeth Farthing
Carol Ann Feuerriegel
Clinton Field
Glenn Fischer
Matt Fisher
David Fleming
Mariel Fox
Patricia Franks
Audrey Gaines
Rhonda Galaske
Caroline Gallego
Claire Galloway Jenkins
Stephen Garner
Charles Garrett
Irene Gelyk
Celine Gerin-Roze
Sue Gerrity
Kimberly Giertz
Susan Goodman
Joshua Grisi
Komal Gulich
Jocelyn Gunter
Allen Gurney
Michael Haley
Grace Hammar
Joshua Hargrafen
Paula Harris
Julie Harvey
Matthew Hebert
Charles Herbek
Margaret Hermesmeyer
Caroline Higgins
Gordon Hoke
Patricia Huff
Janice Hulme
Bethany Hynes
Nicolas Inglis
Leigh Isaacs
Mary Janicik
C'Les Jensema
Chris Johnson
Elizabeth Johnson
Kurt Johnson
Todd Johnson
Deborah Jostes
Deborah Juhnke
Soo Kang
Andrew Keller
James Kennedy
Anju Khurana
Ellie Kim
Michelle Kirk
Monica Kirsch
Tamara Koepsel
Greta Krapac
Peter Kurilecz
Tera Ladner
Richard Lang
Ronald Layel
Anna Lebedeva
Gilles Legare
Donnell Long
Howard Loos
John Loveland
Eric Lynn
Cindy MacBean
Mark MacFarlane
Rudolph Mayer
Brian McCauley
Stephanie McCutcheon
Cheryl McKinnon
Felecia McKnight
James Merrifield
Bruce Miller
Sandy Miller
Dana Moore
Dermot Moore
Rafael Moscatel
Linda Muller
Jen Murray
Stephen Murray
Deborah Naas
Joe Nadzam
Lindy Naj
Peggy Neal
Lee Nemchek
Kurt Neumann
Sheri Nystedt
Shanna O'Donnell
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
Angel Ramos
Tony Ratcliffe
Joshua Rattan
Scott Raynes
Jessica Rickenbach
Deborah Rifenbark
Carol Rittereiser-Coritt
David Rohde
Donna Rose
Shawn Ryan
Kathryn Scanlan
Danna Schacter
Tonia Schneider
Teresa Schoch
Terry Schrader
Karen Schuler
Jason Scott
Karen Shaw
Mary Sherwin
William Silvio
David Skweres
Doug Smith
Kathleen Smith
Michael Smith
Kirke Snyder
Natalie Spano
Brian Starck
Jason Stearns
David Steward
Courtney Stone
Melissa Suek
Lisa Summers
Paula Sutton
Marjorie Swain
Sheila Taylor
Robin Thompson
Kathleen Timothy
Louis Tirado
Brian Tretick
Susan Trombley
Nathan Troup
Brian Tuemmler
Martin Tuip
Amy Van Artsdalen
Paul Van Reed
James Vardon
Katharine Voldal
Jennifer Watters Farley
Alexander Webb
Katherine Weisenreder
Bridgett Weldner
Erik Werfel
Steven Whitaker
Kristi Whitmore
Jesse Wilkins
Marc Willemse
Dylan Williams
Steven Williams
Natausha Wilson
Rick Wilson
Terri Wilson
Brett Wise
Jennifer Witt
Kristin Wood
Robin Woolen
Jeffrey Yawman
Cheryl Young
Margo Young
Andrew Ysasi
Ryan Zilm

Application deadline: November 12, 2016.

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

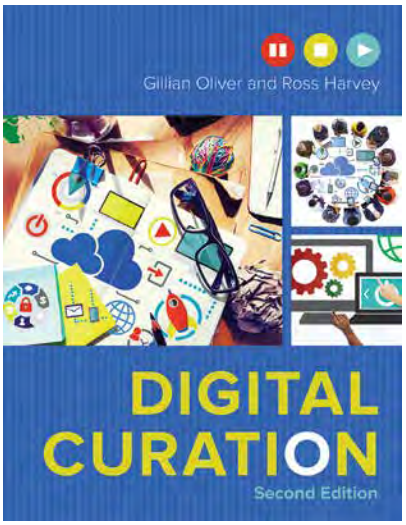
NEXT™ LEVEL
information governance assessment

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**.

Second Edition of *Digital Creation* Balances Theory and Practice

Ryan Speer



This extensive revision of Oliver and Harvey's *Digital Curation* presents comprehensive background information and expert guidance for managing and preserving digital material over the long term.

What's New in this Edition

Conceptual models of digital curation processes are central to the organization and tone of the book: The Digital Curation Centre (DCC) Curation Lifecycle Model lends structure to the discussion of curation requirements and actions in the latter portion of the book, and the authors present a new theoretical model, the Data Curation Continuum, as an alternative to the lifecycle model.

Other material new to this second edition of *Digital Curation* addresses the impact of cloud computing on the cost of data curation and associated storage solutions. This edition adroitly balances theory and practice and will be useful in both academic and professional settings.

Part I: Digital Curation Overview

Part I consists of four chapters intended to provide an overview of the digital curation field. The first two chapters explain the need and incentives for digital curation and describe the landscape of digital curation.

Two chapters introduce conceptual models (the DCC Curation Lifecycle Model, the Open Archival Information System [OAIS] Reference Model, and the Data Curation Continuum) and explore in-depth the term *data* and its implications for the practice of curation.

The chapter covering the curation landscape uses academia as an interpretive standpoint, but it includes insightful descriptions of digital curation and data management professional requirements with the potential for broader application. The discussion of data and its various meanings is also adequately generalized, emphasizing the scope of data management issues well beyond the e-science considerations which originally inspired the digital curation field.

Part II: Full Lifecycle Actions

Part II has four chapters, each of which covers one of four Full Lifecycle Actions specified by the DCC Curation Lifecycle Model, central actions which apply to every stage in the life cycle. These four actions are:

1. Description and Representation Information
2. Preservation Planning
3. Community Watch and Participation
4. Curate and Preserve

The longest and perhaps most valuable chapter is on metadata, with a brief, excellent introduction to the varieties of metadata (administrative, descriptive, technical, structural, and preservation), with an emphasis on preservation metadata. The chapter also covers other pertinent topics, such as persistent identifiers, metadata schemas and standards, and representation information. The chapter on preservation policy is brief but does include a useful discussion of the costs of curation.

Digital Curation, 2nd Ed.
Authors: Gillian Oliver and Ross Harvey
Publisher: Neal-Schuman
Publication Date: 2016
Length: 240 pages
Price: $85
ISBN: 978-0-8389-1385-7
Source: *www.alastore.org*

Part III: The DCC Curation Lifecycle in Action

The final section of *Digital Curation* is titled "The Digital Curation Lifecycle in Action." At seven chapters, it is the largest section. Where Part II covers the DCC Curation Lifecycle Model's Full Lifecycle Actions, Part III is concerned with the model's Sequential Actions and Occasional Actions: Conceptualise; Create or Receive; Appraise and Select; Ingest; Preservation Action; Store; Access, Use, and Reuse; and Transform.

These chapters largely take a long-term view of data curation, approaching the task from an archival standpoint. For instance, the chapter on "deciding what data to keep" conducts a lengthy examination of data appraisal largely without reference

to legal recordkeeping requirements – and "Dispose" itself is only an Occasional Action within the DCC Curation Lifecycle Model.

The discussion of technical topics such as ingest and migration is quite well done, and the chapter on storage contains useful commentary on repository software and related topics.

Good Addition to Bookshelf

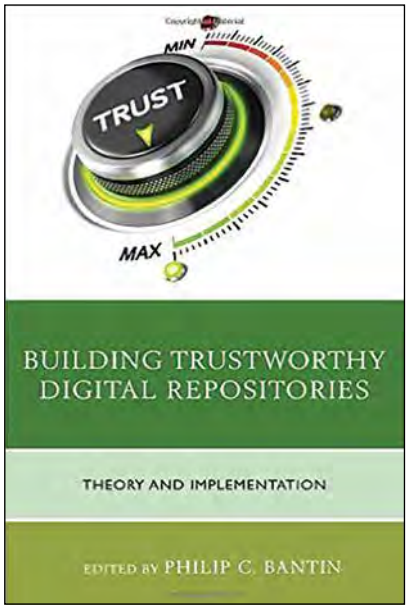
Digital Curation provides a concise and approachable overview of data management and preservation. The authors are professors of information management, and their approach is sympathetic to the needs of researchers and academic data managers, but much of the content should also be relevant for practitioners in other fields.

The use of data curation conceptual models as an arranging principle for the text ensures that, while some examples and discussions are specific to a particular occupational setting, the content as a whole addresses generic principles and situations. As such, the book should be a welcome addition to the reference shelves of records and information management practitioners and allied audiences. **END**

Ryan Speer can be contacted at rps@vt.edu. *See his bio on page 47.*

New Insights in **Building Digital Repositories** Benefit All Information Professionals

Norman Mooradian, Ph.D.



To my knowledge, this is the first text devoted to creating trustworthy digital repositories. Its target audience is professionals in the fields of archives, library science, and records management. As defined early in the text, quoting from the 2002 Online Computer Library Center report "Trusted Digital Repositories: Attributes and Responsibilities," a *trusted system* is "one whose mission is to provide reliable, long term access to managed digital resources to its designated community, now and in the future."

Structured by System Functions

The book is an anthology of articles written by 43 experts from across these fields, structured according to component functions that make up a trusted system:

- Policy/management
- Ingestion
- Metadata
- Audit capabilities
- Retention
- Access
- Security
- Preservation

It ends with a section on current trends and future directions.

Each section begins with a brief theoretical piece that provides the conceptual framework for the topic and is followed by implementation articles or case studies. This breakdown into functional areas that balance theory and practice makes the book comprehensive and readable.

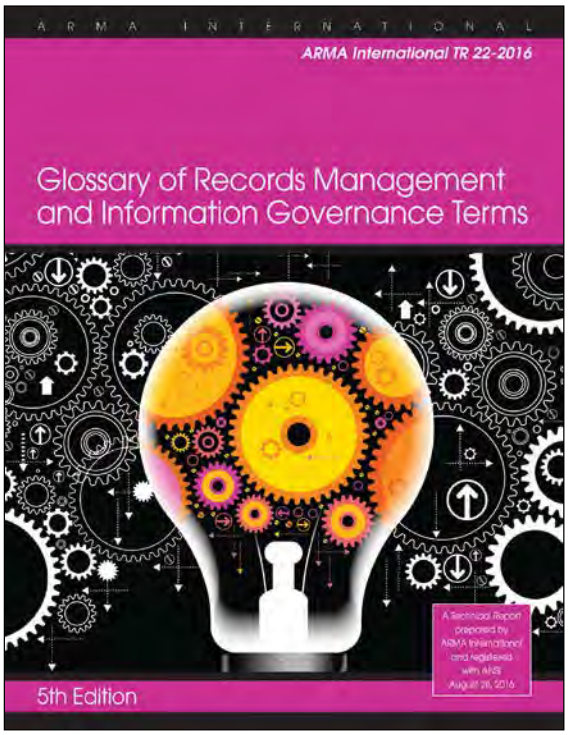
Distinction Between Systems

The type of system on which the book focuses is succinctly described in the theory piece in the chapter on access as one that holds archival or library materials for long periods of time by trusted bodies (libraries and archives) for the benefit of multiple, external constituencies. This is in contrast to enterprise content management solutions that manage active files (along with permanent records) in support of business objectives and compliance requirements for a limited set of internal users.

The goal of the book is to provide theoretical and practical guidance on creating digital repositories that satisfy the requirements of the Open Archival Information System model codified as ISO 14721: 2012 *Space data and information transfer systems — Open archival information system (OAIS) — Reference model.*

Building Trustworthy Digital Repositories: Theory and Implementation
Editor: Philip C. Bantin
Publisher: Rowman & Littlefield
Publication Date: 2016
Length: 388 pages
Price: $65
ISBN: 978-1-4422-6378-9
Source: *https://rowman.com*

NEW in the Bookstore



Glossary of Records Management and Information Governance Terms, 5th Ed. (ARMA International TR-22-2016)

ARMA International Standards Workgroup

With an expanded scope that encompasses more than 100 new entries from key information governance disciplines, this fifth edition of the glossary now defines more than 1,000 terms from disciplines that intersect with records and information management, including security, privacy, audit, legal, information technology, archives, and business management.

A5032 **$70.00** Professional members: **$50.00**
V5032 PDF **$65.00** Professional members: **$45.00**

Order online today!

ARMA INTERNATIONAL BOOKSTORE
www.arma.org/bookstore

Chapters 1-2: Policy, Management

The first two chapters (Chapter 1 – "Evaluating and Selecting a Trustworthy Repository" and Chapter 2 – "Resources, Policies and Management Structures") provide a general description of trusted digital repositories (TDRs) from procurement, management, and operational perspectives. The OAIS model/ISO 14721 and its associated audit standard ISO 16363: 2012 *Space data and information transfer systems – Audit and certification of trustworthy digital repositories* are reviewed in these chapters. Standards that apply to both archival and ECM repositories, such as ISO 15489:2016 *Information and documentation – Records Management – Part I – General* and *Model Requirements for the Management of Electronic Records* (better known as MoReq2) are also covered.

Chapters 3-4: Ingestion, Metadata, Audit

The chapters on ingestion, metadata, and audit trails (Chapter 3 – "Building a Trustworthy System: Ingest Process," Chapter 4 – "Creating and Capturing Metadata," and Chapter 5 – "Capturing Audit Trail Data") provide a detailed description of the steps required to capture digital files and metadata of bulk record sets from contributing systems in a way that their provenance, integrity, context, and internal structure are preserved and maintained on a long-term basis and can be disseminated to a broad community in a form that preserves the record sets as originally captured.

Chapters 6-7: Retention, Access

The chapters on retention and access (Chapter 6 – "Assigning Retention and Disposal Data" and Chapter 7 – "Creating an Access Strategy") do a good job describing the particular goals and challenges of long-term digital preservation undertaken for the benefit of broad and hard-to-define external, future stakeholders.

Chapters 8-9: Security, Preservation

The chapters on security and preservation (Chapter 8 – "Creating a Secure System" and Chapter 9 – "Creating a Preservation Strategy"), along with the chapters on metadata and audit trails, address what I view as the central functional areas of trusted systems in general. Chapter 8 covers basic security elements of any computer network, but it has an excellent case study on implementing a comprehensive architecture to manage access to sensitive behavior-scientific data. Chapter 9 also covers common preservation strategies and provides a case study on implementing a preservation system that includes a helpful discussion of (capture) workflows for different kinds of collections and materials.

A Different but Relevant Perspective

Because the focus of the book is on trusted digital repositories and long-term digital preservation, the implicit meaning of "trusted system" is not identical to that presupposed in records management. A central concern of records professionals managing digital records is that the records can be trusted to provide evidence of business activities when that evidence is produced by the organization itself and where there is an inherent conflict of interest to do just that. For this reason, other ISO, AIIM, and National Institute of Standards and Technology standards have focused on replication to write-once media, for example, as well as metadata, formats, and audit trails.

But while the themes and methods presented are not identical to the interests of records managers as regards to trusted systems, there is considerable overlap. This book provides new insights in managing trustworthy records in general, and especially for the long term, and therefore is a valuable resource for records professionals, archivists, and librarians. **END**

Norman Mooradian, Ph.D., can be contacted at nmooradian@kmbs.konicaminolta.us. See his bio on page 47.






COREY EVANS MONTAÑA MOORADIAN SCHMERBAUCH SPEER

Data Privacy Meets a World of Risk: A Landscape in Turmoil Page 20

John C. Montaña, J.D., FAI, is founder and a principal of Montaña and Associates, a full service records and information management and information governance consulting firm. In addition to writing *How to Develop a Retention Schedule*, Montaña has co-authored several other books and written dozens of articles. Montaña ia a Fellow of ARMA International and a member of the group that developed the Generally Accepted Recordkeeping Principles®. He holds a juris doctor degree from the University of Denver. Montaña can be contacted at *jcmontana@montana-associates.com.*

Tips for Globalizing a U.S.-Based Records Retention Schedule Page 25

Tom Corey, Esq., CRM, is a manager within the information governance practice of HBR Consulting LLC, working with law departments on information governance/records management policies, including reviewing compliance with domestic and international requirements. He earned his law degree from Charlotte School of Law, is a Certified Records Manager, and is an active member of the North Carolina State Bar, Mecklenburg County Bar, and the American Bar Association. Corey can be contacted at *tcorey@hbrconsulting.com.*

Protecting Information Assets Using ISO/IEC Security Standards Page 28

Lois Evans is an archive and records management specialist with more than 12 years of experience in local government in a research project on social media and trust in government, and is the working group chair for the Canadian General Standards Committee on Electronic Records as Documentary Evidence. She earned a master of information studies degree from the University of Toronto, has taught records management and information assurance and security for the University of British Columbia's School of Library, Archives, and Information Management, and recently contributed to *Building Trustworthy Digital Repositories*.Evans can be contacted at *levans18@mail.ubc.ca*.

The New Waypoint Along the CRM Journey: Certified Records Analyst Page 34

Jean Ciura, Ph.D., CRM, is president of JMCIMC LTD., an information management consulting firm in Chicago specializing in corporate information governance implementations. A records veteran of more than 35 years, she has published several articles, co-authored *The Retention Book: Retention and Preservation of Business Records*, and taught records management at the university level. Ciura, who earned a Ph.D. in history from the University of Rochester, can be contacted at *jean.ciura@yahoo.com.*

Establishing a Records Appraisal Workflow Page 36

Maik Schmerbauch, Ph.D., is permanent state archivist at a German archival department. Previously he worked for five years on temporary-based projects in archives, library and records management in Germany and Poland. He studied information, library, and archival science, theology, and history in Germany and universities abroad and received several post-graduate degrees. Schmerbauch can be contacted at *schmeichi@web.de.*

Establishing a Records Appraisal Workflow Page 43

Ryan Speer is manager, university records and information governance, at Virginia Tech. Previously he worked as an archivist at Georgia Tech and as an archivist and records management analyst at the Georgia Archives. He holds a master's degree in library and information science. Speer can be contacted at *rps@vt.edu.*

New Insights in Building Digital Repositories Benefit All Information Professionals Page 44

Norman Mooradian, Ph.D., is senior engagement manager at Konica Minolta in the enterprise content management group. He has technical and professional certifications, received a Ph.D. in philosophy from the Ohio State University, and has completed graduate courses in legal studies. He has published articles on information technology and business ethics and is the author of the forthcoming *RIM Ethics: Records and Information Management Ethics* from ALA Editions. He can be contacted *at nmooradian@kmbs.konicaminolta.us.*

ADVERTISE IN *IM* MAGAZINE

Information Management magazine is ***the*** resource for information governance professionals.

Talk to Jennifer about making a splash.

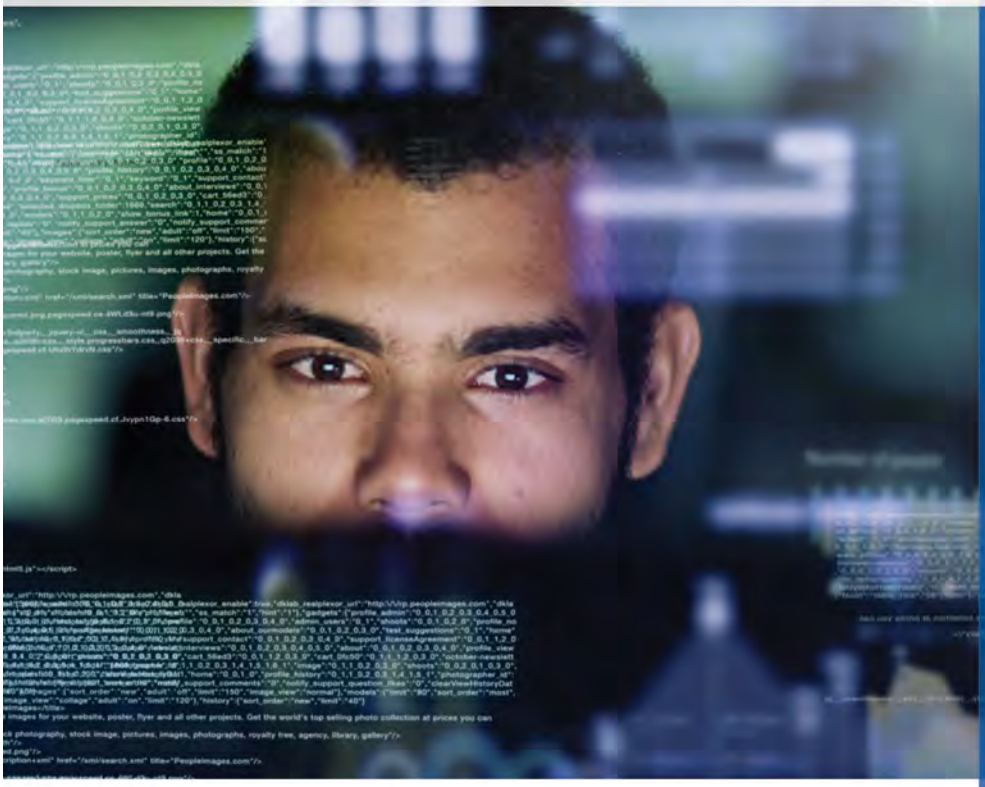
Advertise today!

Jennifer Millett
Sales Account Manager
+1 888.279.7378
+1 913.217.6022
Fax: +1 913.341.6823
jennifer.millett@armaintl.org

ADINDEX

	CONTACT INFORMATION
5	**Baypath** *graduate.baypath.edu*
15	**e-Image Data** *800.252.2261 – www.e-imagedata.com*
BC	**Feith** *www.feith.com/records*
IFC	**Fujitsu** *us.fujitsu.com/fcpasolutions*
9	**Institute of Certified Records Managers** 518.694.5362 – *www.ICRM.org*
3	**NAID** *http://directory.naidonline.org*
19, 42	**Next Level** *www.arma.org/nextlevel*
39	**OPEX Corp.** *www.opex.com*
IBC	**San José State University** *ischool.sjsu.edu/mara*

SAN JOSÉ STATE UNIVERSITY



Immerse Yourself in the World of Information

Study Information Governance at San José State University

Earn your Master of Archives and Records Administration degree from SJSU, where more Silicon Valley professionals earned their degrees than any other university.

As a MARA graduate student, you'll learn to use sophisticated technologies to organize, preserve, and provide access to a growing volume of records and digital assets.

And with a master's degree in hand, you'll be prepared to work in a rapidly expanding field that plays an important role in today's digital world.

Convenient, flexible, 100% online graduate program.

Accredited by WASC

WESTERN ASSOCIATION OF SCHOOLS AND COLLEGES
Accrediting Commission for Schools

SJSU | SCHOOL OF INFORMATION

ischool.sjsu.edu/mara

YouTube

Feith Systems & Software serves Records Managers across the Department of Defense, Civilian Agencies, & Intelligence Community, where risk matters most.

Trusted for :

- Comprehensive Electronic & Physical Records Management
- 30 Years of Experience
- DoD 5015.2 Certified
- Developed and Supported entirely in the USA
- Full Security and Classified Records Support

feith.com/records

FEITH