INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

MARCH/APRIL 2015

Designing a Records Audit: A Controls-Based Approach

Page 20

You're in Luck.
Find your labor savings with OPEX.

With OPEX prep-reducing scanners, we're taking the work out of document imaging. While many companies focus on faster scanners, we create smarter solutions that make it possible to scan even the most challenging documents with little or no document preparation. Our technology brings new simplicity to an otherwise complex process – helping you reduce labor requirements, save money and enhance productivity.

OPEX®
CORPORATION

WWW.OPEX.COM | **856.727.1100**

INFORMATION MANAGEMENT

MARCH/APRIL 2015 **VOLUME 49 NUMBER 2**

INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

Publisher: Jocelyn Gunter

Editor in Chief: Vicki Wiler

Contributing Editors: Cyndy Launchbaugh, Jeff Whited

Art Director: Brett Dietrich

Advertising Sales Manager: Elizabeth Zlitni

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

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

ARMA International *(www.arma.org)* is a not-for-profit professional association and the authority on 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 Karen Lind Russell or Krista Markley at +1 888.277.5838 (US/Canada), +1 913.217.6022 (International), +1 913.341.3742, or e-mail *Karen.Krista@ armaintl.org*.

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

Establishing and Monitoring the Right Metrics for RIM Program Success

Metrics," "benchmarks," "key performance indicators (KPIs)," "measurements," "standards" – whatever terms your organization uses, you're expected to establish and meet them. After all, according to the oft-quoted and variously attributed adage, "What gets measured gets done."

On the other hand, it's important to be sure you're measuring the right things; as Albert Einstein reportedly said, "Not everything that counts can be counted, and not everything that can be counted counts."

Echoing that idea, Paula J. Smith, practice lead, Information Management at Optimation, responded to a RIM Professionals LinkedIn Group question about what the best KPI for a records management department is: "…before we start looking at the KPI's – first what business outcomes are you trying to achieve?" She added, "…remember KPI's do drive a certain behaviour set so if you are focused on meeting KPI X, then that KPI must have value to the organisation – let's make sure we are measuring the right things for the right outcome."

The right KPIs, Smith said, provide "…a means of monitoring and demonstrating performance, ensure that we are tracking to our goals, highlight any areas that require further analysis or investigation and give us and senior managers often, the visibility that the programme(s) they are investing in has returned results."

Several articles in this issue of *Information Management* will help you in your quest to measure the right things in the right way to ensure your records and information management (RIM) program's success.

In the cover article Andrew Altepeter writes about an objective way of measuring compliance with RIM program policies and procedures, which can be critical to the program's legal defensibility. *Control standards*, Altepeter writes, are "binary, concise, numbered, unambiguous, easily referenced ways of stating and measuring compliance with policy."

So, for example, changing a narrative policy that says "The corporate records manager is responsible for developing employee training and ensuring training is taken by all employees" to a control standard that says "Training must be completed by all employees when hired and every three years thereafter" provides an objective measurement for determining compliance.

Mark Grysiuk, CIP, provides a primer on online tracking technologies, which RIM professionals must understand in order to ensure that their organizations are in compliance with privacy laws and regulations. He includes a checklist for developing transparent online tracking policies and secure web applications and mapped it to the Generally Accepted Recordkeeping Principles® (Principles), providing an objective metric for ensuring compliance with those Principles.

In her Principles Series article, Julie Gable, CRM, CDIA, FAI, provides tools for evaluating the recordkeeping practices of third parties to whom an organization outsources mission-critical business processes to ensure the providers' compliance with the organization's RIM policies and procedures.

Finally, the "Business Matters" sub-feature excerpts a checklist for evaluating a third-party provider's electronic records storage protection from the ARMA technical report *Understanding Electronic Records Storage Technologies* (ARMA International 26-2014).

Please let us know how you are able to use this information to strengthen your RIM program – or what other information you need – by e-mailing us at *editor@armaintl.org*.

Vicki Wiler
Editor in Chief

shaping tomorrow with you

FUJITSU

Take on bigger projects.

You'll find government compliant Fujitsu scanning solutions in some high places. From the world's fastest high-volume document scanners to versatile, easy-to-use scanners for desktops, Fujitsu has one you should consider. Include the ability to integrate with dozens of leading software providers and you have a strong and reliable solution that lasts. Get started today by visiting **ez.com/infomgmt**

See the New FUJITSU Document Scanner fi-7160

LEGAL

U.S. Supreme Court Moves Toward Electronic Filing

No one would ever call the U.S. Supreme Court an early adopter of technology. While the rest of the legal community has had to embrace new information technologies, the court has remained a paper-based system, but it is preparing to take some baby steps into the digital age.

On December 31, Chief Justice John Roberts released his "2014 Year-End Report on the Federal Judiciary" in which he announced that the court is developing its own electronic case filing and case management system, which may be operational as early as 2016.

The court's slowness to deploy new technology directly reflects its nature. Roberts described the court's role as "passive and circumscribed," making it only logical that it "focus on those innovations that, first and foremost, advance their primary goal of fairly and efficiently adjudicating cases through the application of law."

According to the report, "The federal courts, including the Supreme Court, must often introduce new technologies at a more measured pace than other institutions, especially those in private industry. They will sometimes seem more guarded in adopting cutting-edge innovations, and for good reason, considering some of the concerns that the judiciary must consider in deploying new technologies." Those concerns include security of information.

"The judiciary has a special duty to ensure, as a fundamental matter of equal access to justice, that its case filing process is readily accessible to the entire population, from the most tech-savvy to the most tech-intimidated," the report asserts.

Once the system is implemented, all filings at the court will be available free to the public and legal community on the Court's website. They also will be available on paper. The court expects that electronic filing eventually will be the official means for parties represented by counsel, but paper copies will also be required, particularly for those parties without counsel.

E-DISCOVERY

Internet of Things Brings Discovery Challenges

About this time last year, Wintergreen Research estimated there were 9 billion devices (consumer and enterprise) connected to the Internet. Depending on the source, that number will be anywhere between 26 billion and 100 billion by 2020. Either way, it is clear that the Internet of Things (IoT) is growing at a tremendous pace, making it an exciting new frontier for technology vendors but a source of considerable concern for many in the legal community.

As the IoT explodes, so will the amount of data subject to potential federal oversight, e-discovery, and data breaches, pointed out Erik Post, CEO of the litigation support company OmniVere, in a recent *Law Technology News* article. The situation is further complicated by the likelihood that "most IoT devices won't have adequate data storage capacity, making e-discovery of the devices especially time sensitive," according to Post.

"The universe of potentially relevant information will increase geometrically, complicating an already messy collection and review process," predicted Post. "As plaintiffs' attorneys (and government agencies) become educated on the discovery potential for the IoT, organizations will need to proactively plan for a more demanding, invasive EDD [electronic data discovery] environment."

CYBERSECURITY

DHS Cybersecurity Role Continues to Grow

In December President Obama signed a bill that, among other things, continues to establish the role and authority of the U.S. Department of Homeland Security (DHS) in the nation's efforts to protect its information systems.

The bill – Federal Information Security Modernization Act of 2014 (FISMA 2014) – updates and modernizes FISMA 2002. The purpose of FISMA 2002 was to provide a framework for developing and maintaining minimum security controls to protect federal information systems. It tasked the director of the Office of Management and Budget (OMB) with overseeing the development and implementation of agency information security policies and practices. FISMA 2014 authorizes the DHS to actively assist the OMB in that task.

According to *The National Law Review*, the DHS secretary will be responsible for coordinating information security efforts government-wide, providing operational and technical assistance to agencies, and consulting with the National Institute of Standards and Technology on related standards and guidelines. Furthermore, DHS will oversee agencies' implementation of "binding directives" developed by the OMB.

FISMA 2014 also modifies the scope of "reportable information" to include specific information about threats, security incidents, and compliance with security requirements. In addition, it directs the OMB to clarify what constitutes a "major incident" in the context of agency reporting requirements.

The new law also updates the cyber-breach notification requirements. The OMB director must ensure that agency policies and guidelines are periodically updated and that agencies notify Congress within 30 days of discovering a breach. That notification must include details such as the number of individuals affected, the likely risk of harm to those individuals, and the date by which the individuals would be notified.

BIG DATA

Will Big Data Tools Make Proportionality Irrelevant?

It may be hard to believe at first, but there's a real possibility that big data tools could make proportionality a non-issue – or at least less of an issue – in legal matters.

Proportionality has been a factor because the costs of searching for immense amounts of electronically stored information can be crippling. The courts instituted a formula to ensure production expenses didn't exceed a reasonable percentage of the settlement being sought.

The emergence of big data platforms, however, has "so drastically reduced the burden side of the proportionality analysis that it may no longer be credible to limit or preclude discovery in many cases," suggested James Shook, director of e-discovery and compliance legal practice at EMC Corp. in Atlanta, in an article he penned for *Law Technology News*.

"The same proportionality rule that protected us from technology may now be in danger of elimination by technology," he wrote.

Shook was referencing technologies such as the open source platform Hadoop, which allows organizations to store a large number of files and very large files. The software includes Map Reduce capabilities that enable it to quickly analyze huge volumes of data and create a search index. "The computer and network bandwidth requirements that create burdensome proportionality outcomes on normal data sets do not apply to Hadoop platforms," Shook explained.

Some may see these capabilities as a liability, while others will realize they now are able to more efficiently analyze large volumes of data that might be relevant to a matter. Either way, the tools are here today.

At the very least, counsel needs to be aware of when these capabilities are available before suggesting that accessing the data will be burdensome. The courts have made it clear that ignorance is not a defense when it comes to e-discovery-related technologies.

PRIVACY

Verizon Yields to Pressure

Verizon Wireless has succumbed to pressure regarding its use of a Unique Identifiable Header (UIDH) for tracking customers' web traffic. Although customers could opt out of having their information sold to third-party marketers, Verizon did not offer an opt out of the UIDH until the end of January.

The wireless company started inserting UIDH into the web traffic of its retail customers (not corporate or government contacts) in 2012, reported the *Washington Post*. It was quickly dubbed the "supercookie" as privacy groups and others protested its use, stating the concern that other companies (and even governments) could use the supercookie to track an individual's online activities.

In November, AT&T abandoned its plans to implement a similar program. But Verizon brushed off the critics until a privacy researcher revealed that a third-party advertising tracker company was using the UIDH to bring back its own cookies, even if consumers had tried to remove them. According to the *Washington Post*, the tracking company has since stated it was discontinuing the practice. Verizon announced it would allow customers to opt out of having supercookies inserted into their web traffic.

The privacy watchdog group Electronic Frontier Foundation has meanwhile petitioned the Federal Communications Commission and Federal Trade Commission to investigate Verizon for "unfair and deceptive" practices related to the UIDH. A few Congressional members are also looking into it.

Verizon's decision to allow customers to opt out is not enough for some critics. The Center for Digital Democracy reportedly has stated opting out should be the default – that users should have to choose to opt in.

GOVERNMENT RECORDS

New Coalition to Help NARA Meet E-Records Management Order

ARMA International has pulled together a group of related organizations to support the federal government's efforts to modernize its records management infrastructure and implement proven information governance practices. The group will provide training and resources to help the federal agencies' practitioners meet President Obama's 2011 Managing Government Records Memorandum and the implementation directives issued by the National Archives and Records Administration (NARA) and the Office of Management and Budget. It will also provide a forum for the practitioners to learn more about the private sector best practices from industry leaders.

In addition to ARMA International, the coalition includes the American Health Information Management Association; AIIM; the Information Governance Initiative; the National Association for Information Destruction; and PRISM International.

"Since the issuance of the Managing Government Records Directive in August of 2012, we have consistently reached out to the private sector for input and support. With the recent enactment of the Presidential and Federal Records Act Amendments of 2014 calling on all agencies to transfer permanent electronic records to NARA in electronic form to the greatest extent possible, we will need continued assistance from non-governmental organizations like those in this coalition," Paul Wester, NARA's chief records officer, told *Government Executive*.

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

CYBERSECURITY

China's New Cybersecurity Rules Rile Western Tech Companies

Regulations adopted by China at the end of last year have many Western businesses – particularly technology companies that sell in China – seriously concerned. One of the new rules states that companies that sell computer equipment to Chinese banks will be required to turn over their source code, submit to invasive audits, and build back doors into hardware and software, according to the *New York Times*.

Many foreign companies are concerned that this is a concerted effort by China to shut them out of one of the world's largest and fastest-growing markets. Indeed, as a related article by Reuters pointed out, China has long considered its reliance on foreign technology a national weakness.

The U.S. Chamber of Commerce in China and 17 other U.S. business lobbies have written to China's top cybersecurity policy group asking to postpone the implementation of the policies, stating the new rules would require "intrusive" security testing and the disclosure of sensitive intellectual property.

The new rules are the first in a series of policies Beijing says will strengthen cybersecurity in critical Chinese industries, the article stated.

MOBILE DEVICES

The Life-Changing Side of Mobile Communications

Most of us take the conveniences of mobile computing for granted, oblivious to how it has changed lives in developing countries.

"Twenty years ago connectivity was a rarity. Today Internet access is so central to how people interact with one another, create and share information, and conduct business that the United Nations has called broadband connectivity a basic human right on par with food, shelter, and education," noted Juniper Networks in its recent Global Bandwidth Index. The report was based on findings from a survey of how people in developed and developing countries use the mobile Internet in their daily lives and what they hope to achieve using their devices in the future.

Although researchers found commonalities, the differences they observed were most revealing. First and foremost, they found that consumers in emerging markets see mobile connectivity as a catalyst for progress and change, while those in developed countries tend to regard it as a tool for accomplishing daily tasks more easily.

According to the study, 97% of people in emerging markets believe that connectivity has transformed their lives by changing "how they complete a wide range of essential and everyday tasks."

Not surprising, almost twice as many users in developed countries use their mobile devices for business purposes than those in emerging markets (53% vs. 26%). Yet, 40% of respondents in emerging markets said that connectivity has improved their earning power, compared to only 17% in developed markets.

Education is another area where there is a dramatic difference. Nearly twice as many people in developing countries reported regularly using their mobile devices for educational purposes than in developed countries. Overall, 39% of people in the developing countries said they have experienced a significant transformation in their access to education.

Network speed, network capacity, mobile device quality, and the ability to find a connection were almost twice as likely to be cited as issues by respondents in developing countries. More specifically, 60% considered connection speed the greatest problem, and 30% said finding a connection remained an issue.

PRIVACY

Google and UK Call a Truce on Privacy Policy

The U.K.'s Information Commissioner's Office (ICO) and Google have signed an agreement that may finally begin to lay to rest the long battle over Google's privacy policy. By signing the agreement, Google has agreed to make numerous changes to its policy by June 30. In return, the ICO agreed to close its investigation.

The battle over Google's privacy policy gained momentum in 2012 when the Internet giant combined the 70 policies it had used for its individual products – such as You Tube and Gmail – into one. Privacy watchdogs contended the change led to confusion among users and ultimately eroded their privacy. The new agreement does not require Google to unbundle its privacy policies for different services, reported *ZDNet*. The company has implemented a "multi-layered approach" to its privacy policy, which it will continue to enhance.

Other changes that Google agreed to include:

- Making the privacy policy easier to find
- Disclosing in the policy its data processing activities, including the types and purposes for which it processes users' information and guidance on how users can exercise their rights
- Clarifying the entities that may collect anonymous identifiers through Google products and for what purposes

These changes should bring Google's privacy policy into compliance with not only U.K. laws but those of the European Union, thereby potentially settling similar investigations in Italy, Spain, France, the Netherlands, and Germany.

CLOUD COMPUTING

IBM Sets Its Eyes on the Cloud

IBM is in the midst of a massive structural reorganization to make it a serious player in the cloud. It has shifted its focus onto software, letting hardware take the back seat.

In December IBM announced it was partnering with Apple to launch 10 IBM Mobile First for iOS apps. The apps range in capabilities to benefit governments as well as businesses in the banking, retail, insurance, financial services, telecom, and airline industries.

In mid-January, it unveiled the z13 mainframe, which it calls the most powerful and secure system ever built. The new system's scalability and reliability make it "the ideal private or hybrid cloud architecture," IBM stated. In fact, it can run up to 8,000 virtual servers. IBM further estimated that a cloud system on the z13 could lower the total cost of ownership between 32% and 60% over three years.

The z13 is being heralded as the first system that can process 2.5 billion transactions a day, the "equivalent of 100 Cyber Mondays every day of the year." It's also the first system to make practical real-time encryption of all mobile transactions at any scale. Plus, it's the first mainframe system with embedded analytics.

At the same time it announced the new mainframe, IBM previewed its new z/OS software, which is supposed to help further extend mainframe enterprise applications to mobile users.

Restructuring clearly hasn't slowed down innovation at IBM. In 2014 it received 7,500 patents, more than any other company. Online publisher Seeking Alpha noted that 2014 was the 22nd consecutive year that IBM topped the patent list.

Despite these advancements, IBM does not appear to be growing sales in these new markets fast enough to offset the decline in traditional enterprise hardware and services, which still account for the bulk of its business, noted the *International Business Times*. This was borne out by the company's fourth quarter earnings report. Analysts such as Credit Suisse's Kulbinder Gulcha expect IBM stock will continue to underperform as it weathers a painful multi-year transition, reported *Investors.com*.

In the meantime, IBM continues to forge ahead in its plans to become a key player in the cloud. It has opened SoftLayer data centers in Paris, Mexico City, Tokyo, and Frankfurt.

PRIVACY

Proposed Customer Data Retention Sounds Alarm in Australia

Industry and privacy advocates are up in arms over legislation before the Australian Parliament that they say threatens all Australians' privacy.

The proposed legislation would require Australian telecommunications companies to retain a set of customer data – including, but not limited to, e-mail records, IP addresses, call records, and address information – for two years, reported *ZDNet*. Australian law enforcement agencies have voiced support for the bill and for the need to access that data without a warrant in criminal investigations.

AIMIA, the Digital Industry Association of Australia, whose members include Google, eBay, Twitter, Microsoft, and Facebook, has raised concerns that the legislation not only increases the risk of interference with fundamental rights, but also carries with it heightened security risks.

"The increased security risk of unnecessarily requiring businesses to retain data for two years should also not be underestimated, especially in light of the recent Sony hack. Businesses of all sizes that do not have a strong internal security engineering department will be particularly vulnerable to external threats when storing large volumes of data for long periods of time," the group said, according to the *ZDNet* article.

The Victorian Commissioner for Privacy and Data Protection has also spoken out against the proposed legislation, stating that "[B]y requiring retention of such sweeping categories of data, and by allowing potentially numerous agencies to have access, the scheme significantly interferes with the fundamental right to privacy in a manner that is not proportionate to the objectives of the Bill."

The Australian Human Rights Commission also stated that the legislation reaches "beyond what can be reasonably justified." It went on to suggest that the data set be defined in legislation and that a one-year retention period be tried first.

PRIVACY

Privacy, Data Security on M&A Radar Screens

Dykema's 10th annual M&A survey revealed that privacy and data security are showing up on the radar screen for a third of mergers and acquisitions (M&A) professionals.

It shouldn't be surprising given the increased attention from regulators and customers affected by data breaches in recent years. *Inside Counsel's* Ed Silverstein predicts there will be an even higher volume of M&A transactions this year than there were in 2014.

In a recent issue of *Inside Counsel*, Stephen Tupper, leader of Dykema's privacy, data security, and e-commerce practice, highlighted some issues that could become major problems if not addressed early and well. If the deal includes the transfer of personally identifiable information (PII), it matters what the parties have promised customers. If the acquisition target has promised its customers it will not transfer their PII to a third party, the Federal Trade Commission would likely hold up the deal.

Transferring PII across national borders becomes even more problematic. Foreign regulators, particularly those in the European Economic Area, strictly prohibit the movement of their citizens' PII across borders to countries where local law does not provide comparable data protection. This doesn't have to be a deal breaker, but it does require research and advance planning.

"Consumers and others are beginning to care more about who has their data," Tupper added. He pointed to Google's recent acquisition of Nest Labs as an example. The deal prompted discussion in public forums about what combinations of data mean for privacy.

The best strategy for now, advised Tupper, "is to make room in the due diligence process and deal planning to identify any PII involved in any transaction and be prepared to take into account the evolving regulatory environment and likely consumer reaction."

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**.

INFO GOVERNANCE

CIGO May Be Next Step in Information Governance

Big data is one thing, but what about the quality of that data? Information governance (IG) professionals voiced concern about such matters at the 2015 LegalTech held in early February in New York, according to a report in *Law Technology News*. In an attempt to leverage big data, many organizations are holding on to more information than they may need. According to one panel of IG experts, almost 70% of retained data is unnecessarily kept.

"We are living in a post-Sony, post-Snowden world. We are in 2015, the 'year of the data breach,'" said Jason Baron, Esq., of counsel at Drinker Biddle and Reath. "If you secure the borders, you are doing something that is necessary, but that is not sufficient."

Jordan Lawrence's Marty Provins suggested organizations start with their e-mail. "If an organization did nothing but get better control over e-mail, they would be starting on a path to success," he said. "They tend to make arbitrary decisions over time limits on saving e-mail; the secret to making something work is to understand how they are using it, not having a one-size-fits-all model."

According to the panelists, some organizations are beginning to wonder if a chief IG officer (CIGO) is a necessity or a luxury. Baron said he could envision a scenario in which there was a need for a CIGO.

"I think the moment has come for one of two things," Baron said. "A designated head of info governance as a subfunction of legal … or a fully mature model where you have a C-suite person who stands as a peer of the CIO of an organization."

This need could materialize soon if 2015 does indeed shape up to be "the year of the data breach," as some have predicted.

"I think the job got a lot easier with the Sony Pictures breach," said Gareth Evans, a partner at Gibson, Dunn, and Crutcher. He added that data security is increasingly being addressed at the board level.

INFO SECURITY

Finland Cracks Down on Social Media Companies

On January 1, Finland's new Information Society Code went into effect. The umbrella act simplifies the country's electronic communications legislation in an effort to improve consumer protection, boost information security, and strengthen competition among telecommunications markets.

The law fulfilled the first goal by consolidating 10 laws into one. Most notable is the new requirement that all electronic communication distributors – including social media companies – ensure the confidentiality of communications, reported *ZDNet*.

Olli-Pekka Rantala, director of the communications market at the Finnish Ministry of Transport and Communications, explained that this "is a small step towards a level playing field between traditional telecom operators and new internet players but it was a big change in principle."

In practice, the new law means that companies such as Apple, Facebook, and Twitter must ensure that users of their messaging services get the same standards of privacy and security as other already-regulated sectors such as telecoms, the article stated. The scope of the legislation also extends to companies based outside the EU but offering services in Finland.

The new code is in line with current EU legislation, but Finland is the first to extend its scope.

PRIVACY

EU Data Protection Rules Hit a Snag

Creating a data protection law for the European Union (EU) as a whole is proving to be a grand challenge. Hopes for a law being passed this year are already dwindling.

The EU published a legislative package in January 2012 that would replace the existing rules (passed in 1995 when the Internet was still fledgling) and provide more protection to personal data across the EU. It was voted in during its first reading at the European Parliament in March 2014, before the elections, at which point it contained one directive and one regulation. The scope of the reform expanded following the scandal surrounding the U.S. cyber-espionage program PRISM.

Now it contains "an arsenal of measures" to protect European citizens' personal data, reported *EurActiv.com*. Companies that send personal data outside the EU without permission could face stiff fines. On that there is consensus. What may keep the law from being passed this year is a debate between Parliament and EU member states on the issues of informed consent for the use of data, sanctions, and privacy by design, according to German Green Parliament Member Jan Philipp Albrecht, the vice-chairman of the Parliament's civil liberties committee.

One of the most contentious points is the provision that citizens could complain to their local data protection authority regarding a breach anywhere throughout the EU. Albrecht told *EurActiv.com* that Germany, France, and the United Kingdom were all holding up the negotiations. The Germans are concerned the data protection rule would erode the sovereignty of the country's powerful regions. Both Germany and France worry that data issues could be decided in smaller member states that have less-established data traditions. The United Kingdom, Albrecht said, opposes the data protection regulation altogether, preferring instead that the EU adopt a directive.

EHR

Feds to Ease EHR Certification Schedule

The medical community and electronic health records (EHR) vendors have been asking U.S. regulators for some time to slow down on the final implementation stages of EHR certification. A petition from a coalition of 35 medical societies, led by the American Medical Association, got a response.

"Among physicians there are documented challenges and growing frustration with the way EHRs are performing. Many physicians find these systems cumbersome, do not meet their workflow needs, decrease efficiency, and have limited, if any, interoperability. Most importantly, certified EHR technology (CEHRT) can present safety concerns for patients," the coalition stressed in its January 21 letter to the national coordinator for health information technology.

The group specifically asked that the regulators, among other things:

- Decouple EHR certification from the Meaningful Use program
- Consider alternative software testing methods
- Incorporate exception handling into EHR certification
- Develop guidance and tests to support exchange of data

On January 29, the Centers for Medicare and Medicaid Services (CMS) announced that it would be updating the EHR Incentive Program this year.

"The new rule, expected this spring, would respond to provider concerns about software implementation, information exchange readiness, and other related concerns in 2015," wrote Patrick Conway, M.D., the agency's deputy administrator of innovation and quality, in a CMS blog posting.

CMS is considering proposals to:

- Realign hospital EHR reporting periods to the calendar year to allow eligible hospitals more time to incorporate 2014 edition software into their workflows and to better align with other CMS quality programs
- Modify other aspects of the program to match long-term goals, reduce complexity, and lessen providers' reporting burdens
- Shorten the EHR reporting period in 2015 to 90 days to accommodate these changes

On January 30, the Office of the National Coordinator for Health IT (ONC) released for public comment a draft Interoperability Roadmap, which focuses on actions that will enable consumers and healthcare providers to send, receive, find, and use a core set of electronic health information nationwide by 2017. That core set of information would include standardized data such as demographics that would facilitate matching and linking the information across all systems and platforms, the ONC said in the draft.

The Roadmap identifies three "critical pathways" that need to be addressed to achieve this level of interoperability: 1) requiring standards; 2) incentivizing use of those standards; and 3) creating a "trusted environment" for collecting, sharing, and using electronic health information.

According to ONC, the four most important actions the public and private sectors need to take to make interoperability a reality in the near-term are:

1. Establish a coordinated governance framework and process for nationwide health IT interoperability.
2. Improve technical standards and implementation guidance for sharing and using a common clinical data set.
3. Enhance incentives for sharing electronic health information according to common technical standards, starting with a common clinical data set.
4. Clarify privacy and security requirements that enable interoperability.

ONC will accept public comments on the draft version of the Roadmap until 5 p.m. (ET) on April 3 via its website *www.healthit.gov/interoperability*. The draft is available at *www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf*.

What's your IG IQ?

Find out by earning your

Information Governance Professional Certification

- Showcases your information governance expertise
- Brings professional recognition within your organization, network, and industry
- Extends your professional network to include an elite group of other IGPs
- Increases your potential for career growth

"I highly recommend the pursuit of your IGP by those who either lead or significantly contribute to the management of your organization's information governance framework."

– Nick De Laurentis, CRM, IGP
Technical Analyst, State Farm Enterprise

For more information and to apply, go to ***www.arma.org/igp***.

INFO GOVERNANCE

Study: Content Management Needs More than Technology

A new study revealed that most companies are dropping the ball when it comes to managing content enterprise-wide. Less than one-quarter of the participants in a study conducted by the APQC rated their content management practices as effective; 43% said their programs were minimally or not at all effective. Interestingly, the culprit was not the lack of technology. The vast majority said the biggest challenges were change management, organizational structure, and accountability.

"In short, employees weren't following processes in place to manage content or the organizations had not defined sufficient ownership models for the tools and approaches," according to the study conducted by APQC, a member-based association and proponent of best practices and business research.

These results prompted the benchmarking association to launch its second comprehensive best practices study. It focused on content management practices at five best-practice organizations and found that the one unifying characteristic was how attuned the content teams were to the needs of content stakeholders and end users inside their organizations.

"The best-practice organizations thoroughly understand their target audiences for content, and the result is that their tools and processes align with how people want to contribute, access, share, and reuse organizational knowledge," the research team observed.

As part of the research, the study team identified 20 best practices within the following general topic areas:

- Developing a strategy to connect people to content
- Creating content people want
- Managing the end-to-end lifecycle
- Ensuring content is findable and accessible in the flow of work
- Integrating content and social challenges
- Managing change and evaluating success

E-DISCOVERY

IG, E-Discovery Pros to Win with FRCP Changes

There will be two big winners should the proposed amendments to the Federal Rules of Civil Procedure (FRCP) clear the U.S. Supreme Court as expected: information governance professionals and e-discovery consultants. That is a prediction made by Helen Geib, general counsel and practice support consultant for QDiscovery, in a recent article in *Law Technology News*.

The proposed changes emphasize the need to 1) know what electronically stored information (ESI) the client has; 2) know it early in the case; and 3) understand the technology for handling the data.

"The amendments' focus on preservation is a strong argument for better information governance," reasoned Geib. "In-house counsel must know the what, where, why, who, and how of their company's ESI to effectively implement and manage a litigation hold." Improved information governance, she noted, not only increases the company's ability to defend against preservation-compliance challenges, it helps in controlling costs.

That doesn't mean litigators will be off the hook. The pressure will continue to be on them to become more familiar with ESI and IT systems. "Even if the actual work of data mapping the client's ESI is delegated to others, lawyers must still be able to effectively communicate about ESI in the meet and confer, discovery plan, written discovery, and so on," said Geib.

CLOUD COMPUTING

The Power of the Cloud

They came to the cloud to save money; they stay because of its potential to change their business. More precisely, almost half (49%) of the enterprise executives who participated in the 2014 Cloud Computing Survey conducted by KPMG, "Elevating Business in the Cloud," said the biggest benefit of using the cloud is its cost efficiency. However, an increasing number are using it to enact large-scale change at the business-unit level as well as enterprise-wide.

The transformative effect of the cloud is being realized by using it to better enable a flexible and mobile workforce; improve alignment and interaction with customers, suppliers, and business partners; and better leverage data for more "insightful" decision-making.

"Cloud has become almost a business imperative because the benefits seem to outweigh the risks," said KPMG's Rick Wright, principal and global cloud enablement leader. The survey participants reported that the cloud has helped them improve business performance (73%), improve levels of service automation (72%), and reduce costs (70%). These enhancements come at a price, however. More than half (53%) cited data loss and privacy risks as the most significant challenges of doing business in the cloud, followed by intellectual property theft. The high costs of implementation and the challenge of integrating the cloud with existing architecture are also notable stressors.

KPMG's survey report included five tips to help companies succeed with their cloud transformations:

1. Make cloud transformation a continuous process.
2. Drive cloud transformation from the top.
3. Focus on strong leadership and engagement.
4. Avoid silos.
5. Measure success. **END**

Designing a Records Audit: A Controls-Based Approach

Andrew Altepeter

Using a controls-based approach to auditing for IG program compliance can help ensure a focused scope, collaborative effort among appropriate stakeholders, quantifiable findings, and trackable remediation progress.

Giving a deposition about an organization's information governance (IG) program in connection with litigation or a regulatory investigation can be a daunting experience. Opposing counsel may ask for evidence, such as policies and procedures documentation, retention schedules, and employee training, to show that the organization has an effective IG program.

More challenging, though, is if counsel also asks for proof that all members of the organization are being trained and that they are following the policies and procedures. Producing policies, procedures, and retention schedules is a great start, but their mere existence does not prove that they are being followed; the organization must have a way to show it is doing what it says it is doing.

Auditing as Evidence

Many organizations choose to audit their internal processes as a way to show that they are living up to the mandates set in their policies. But auditing IG – something that touches every member of the organization – can be challenging, and not all audits will satisfy a court.

For example, some organizations may "audit" by asking all employees to click an electronic check box or sign a statement to attest that they are in compliance with the organization's IG policies and procedures. This process is easy to set up and easy to get a majority of employees to respond to since it takes only a few seconds to check a box or sign a form.

This approach is useful for periodically reminding everyone in the organization about their need to comply with the policies and procedures. But, this is not an audit. And in all likelihood it will not satisfy opposing counsel or a judge.

The key to an effective audit is having the right controls, scope, and stakeholders. This article provides guidance for assembling these elements and building an audit that will enable an organization to show its IG program is legally defensible.

Narrative Policy

The company shall maintain records in accordance with all retention schedules, which are to list the retention periods for all major record categories of records across the organization. Employees are responsible for maintaining their own records in accordance with these retention schedules. When the records reach the end of their required retention period, and if they are not subject to legal hold, they must be disposed of in a secure manner.

The corporate records manager is responsible for the maintenance of the retention schedule and in assisting employees in its use. When changes to the retention schedule are required, the corporate records manager must undergo a formal change management process.
The corporate records manager is responsible for developing employee training and ensuring training is taken by all employees in the organization.

Control Standards

RM1001 – The corporate records manager is responsible for the maintenance of the RIM policy, training, and retention schedule.

RM1002 – All electronic and hardcopy records must be retained in accordance with the records retention schedule.

RM1003 – The records retention schedule must be updated to reflect current legal and regulatory requirements.

RM2001 – Training must be completed by all employees when hired and every three years thereafter.

RM3001 – A legal hold mechanism must be in place to notify users that their records are subject to legal hold.

RM3002 – All records subject to legal holds must be retained until the hold is lifted.

Figure 1: Narrative vs. Controls-Based Policy

Going Beyond the Maturity Model

ARMA International's Generally Accepted Recordkeeping Principles® (Principles) includes the Principle of Accountability, which stipulates that practitioners must ensure program auditability; specifically, it dictates "Review/auditing of information governance policies and processes to monitor success and failure and to improve and update them proactively."

There are multiple ways to accomplish this. For example, ARMA created the Information Governance Maturity Model (Maturity Model), among other instruments, for organizations to use to benchmark their growth in accordance with the Principles. This is well and good; the Maturity Model is a useful tool for measuring an organization's IG profile at a high level. But, that is different from conducting a true audit.

Audits require a scientific inventory of current practices across the organization, its repositories, and its office locations. It may involve interviews, questionnaires, observation, or the collection of other evidence. This is often where practitioners become overwhelmed trying to determine where to start, what questions to ask, and what aspects to audit.

Using Control Standards

The key to a successful audit begins with a policy against which com-

pliance can be measured. One way to make a policy auditable is to write it in the form of *control standards,* which, simply put, are binary, concise, numbered, unambiguous, easily referenced ways of stating and measuring compliance with policy. Controls are often used in the areas of IT, information security, or finance. One well-known example of this is the Sarbanes-Oxley Act, which requires certain internal controls for publicly traded companies.

Control standards should avoid ambiguity. Avoiding such qualifiers as "effectively," "timely," and "properly" will clarify the requirements and expectations, which will make the auditing process more straightforward. Often, policies are written in a narrative form instead, as shown in the left-hand box in Figure 1; it uses sentences and paragraphs to explain the roles and responsibilities of the organization's members. There is nothing inherently wrong with this approach, except it lacks the advantage of being auditable. Compare it to the right-hand box in Figure 1, which would be easier to audit.

Whether the organization is replacing a narrative-form policy with control standards or supplementing it with controls, the important thing is to have controls that can be referenced in an audit. There are several advantages to the controls-based approach, as discussed below.

Allows Prioritization, Focus

Policy requirements are not necessarily equally important. Numbered controls allow an organization to choose which ones are the most important or have the highest risks and prioritize them to be addressed first in an audit.

Numbered controls also can be gathered into intelligible groups, such as those dealing specifically with offsite storage of physical records, or electronic records, or legal holds, and so on. Some controls may fall into multiple groups. These control groupings allow an organization to focus an audit on a specific topic and keep the scope appropriately defined.

Compliance Matrix

	The Principles	ISO 15489	HIPAA	PCIDSS	Sarbanes-Oxley	COBIT
RM1001	X	X				
RM1002	X	X			X	
RM1003	X		X		X	
RM2001	X	X				X
RM3001	X	X		X		
RM3002	X	X	X		X	
RM3003	X	X				X

Figure 2: Compliance Matrix

Makes Results Quantifiable

Numbered controls also enable an organization to calculate risk based on the number of controls that are being met and to report that risk in a quantifiable way in the audit findings.

Maps to Other Standards

Control standards can be built from and mapped to other standards, such as ARMA's Principles, ISO 15489:2001 – *Information and documentation – Records Management – Part I – General*, the Health Insurance Portability and Accountability Act, the Payment Card Industry Data Security Standard, the Sarbanes-Oxley Act, and so on.

Mapping can be shown in a compliance matrix as illustrated in Figure 2; this is useful when responding to management or customer requests regarding the organization's compliance with specific standards.

Scoping the Audit

The beauty of IG control standards is that they allow the audit's scope to be defined precisely. The policy is no longer an "all or nothing" requirement in an audit. It can be defined based on any number of factors.

For example, if an organization has acquired another company in the past year and had a resulting large influx of employees, it may be wise for it to focus an audit on the controls related to new employee training or merger and acquisition activity. Or, if an organization's litigation profile has increased recently, perhaps an audit should focus on the controls relating to the effectiveness of the legal hold mechanism.

The bottom line is that it is unrealistic and a misuse of resources to attempt to audit an entire IG program. Control standards allow an audit's scope to be limited to the most relevant controls and the highest risks.

Identifying Stakeholders

An IG audit should be a multi-team effort. While the IG professional may be accountable for the audit outcome and remediation, there may be other resources in the organization that can be leveraged. For example, it may be unrealistic to audit all locations of a multi-national organization, but stakeholders throughout the business can act as "boots on the ground." Logical stakeholders to invite may be records champions embedded in the business, loss prevention and/or physical security, internal audit, and risk management.

Control standards allow accountability to be assigned to these stakeholders. While IG owns the policy and maintenance of the controls, responsibility may be assigned across the organization. For example, controls

Dashboard Reporting

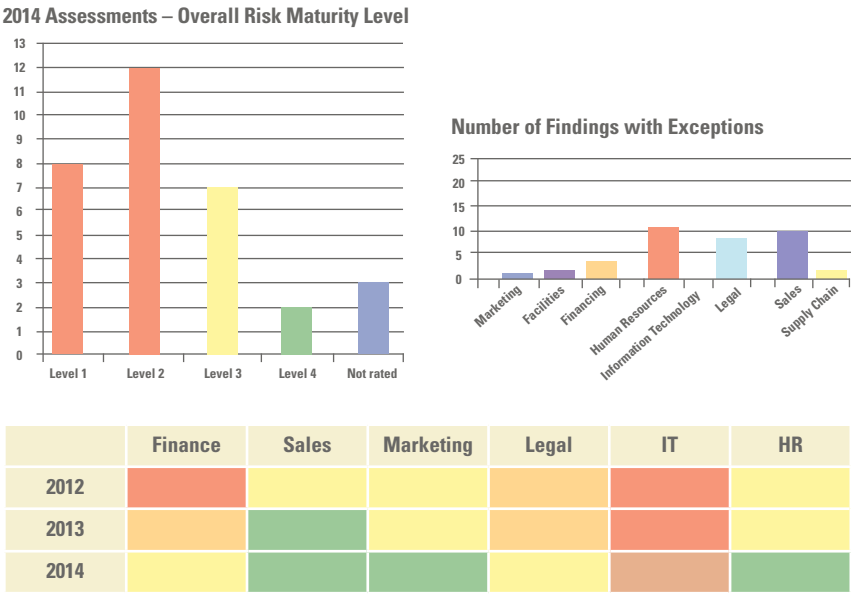


Figure 3: Dashboard Reporting

concerning paper records storage in an onsite records center may be the responsibility of facilities or physical security. Perhaps a member of the legal team is responsible for adherence to the controls of the legal hold mechanism. Internal audit may be responsible for controls requiring desk or inbox audits, and so on.

Obviously, it is very important to communicate and establish consensus on which teams are responsible for which controls. This approach allows the IG professional to focus on the organization's overall IG profile and not get caught in the weeds or be seen as simply the person responsible for pulling boxes.

Scoring Results

Score the results by audit category, but avoid becoming *too* granular. Take a risk-based approach that ranks results as 1-4 or as "critical," "high," "medium," and "low" risk. Senior management doesn't necessarily want to know all of the audit findings; it will want to know the highest risks. It is up to the IG professional to determine which audit findings are "high risk," and this will depend on the organization and the type of information it maintains. Use a dashboard like the one shown in Figure 3 to summarize the findings. A dashboard illustrates the cumulative risk across the enterprise and allows it to be tracked over time

Tracking Remediation, Exceptions

It is important to track remediation of high risk audit findings until they are corrected. A remediation plan is an important tool for this process and should be created with the business owner or functional lead.

On the remediation plan, record the organization and contact names, as well as the relevant control(s), cause of the deficiency, short-term remediation plan (to address high risks immediately), long-term remediation plan (to become in full compliance with the control), and potential impact analysis. Have the business owner agree to the plan and check the status of the finding every 90 days until it is closed.

Some findings may be impractical to remediate due to business or technical reasons. These must be documented under a formal exceptions process. Exceptions should be limited in number and valid for a finite period (typically three months to a year). Exceptions are temporary because the risk environment changes over time. It is expected that controls will be complied with as soon as possible. Exceptions should be revisited at expiration and go through an approval process if they are to be renewed. Compensating controls also must be put into place to mitigate the risk.

Finally, the risk must be accepted by someone in the organization with the appropriate level of authority – often a vice president or above. Using an exception management tool to track exceptions and map outstanding exceptions against control standards may be beneficial. When auditing again, focus on new controls or those with existing high risk findings.

Receiving the Payoff

Auditing an IG program does not have to be a daunting task when following these steps:

1. Adapt the IG policy using control standards.
2. Focus on high risk areas to limit the audit's scope.
3. Assign responsibility for specific controls to the appropriate stakeholders.
4. Communicate the findings using a dashboard to highlight high risk areas.
5. Track remediation progress and manage exceptions.

Following this plan will lead to manageable and effective audits, which will help the organization minimize its information risks, maximize its information value, and make its organization's IG practices legally defensible. **END**

Andrew Altepeter can be contacted at andrew.altepeter@gmail.com. *See his bio on page 47.*

The Cookie Trail: **Why IG Pros Must Follow the Crumbs**

Mark Grysiuk, CIP

Information governance (IG) professionals must understand evolving online tracking technologies and take a leading role in ensuring that their organizations are in compliance with privacy laws and regulations that apply to them. This article provides an overview of the technologies and suggests actions IG professionals should take.

Cookies, which Webopedia.com defines as "a message given to a Web browser by a Web server," have long been a hot topic, generating both positive and negative opinions. They are important to developers and companies for enhancing website functionality and providing valuable information about website visitors. But, they are considered threats to individual privacy when they're hidden and used inappropriately.

This article provides a high-level overview of the purposes and risks of cookies and other web-tracking technologies. It also offers a framework information governance (IG) practitioners can use to incorporate ARMA International's Generally Accepted Recordkeeping Principles® (Principles) into the development of secure web applications in partnership with developers. The article can also be used to educate the user community, who are often oblivious to how their information may be at risk.

What Are Cookies?

Cookies were developed by Netscape Communications Corporation in 1995. The word *cookie* (also known as *browser cookie* or *HTTP cookie*) is derived from *magic cookie*, a term used in programming languages to describe the information shared between "co-operating pieces of software." The Cookie Central website gets a little more technical, defining it as "a text only string that gets entered into the memory of your browser."

Cookies are actually text files, about 4 KB in size, that hold name-pair values that are used to maintain *state,* which is the "application's ability to work interactively with a web user." Without it, user adoption for the Internet might not have happened.

Types of Cookies

Session cookies are stored in temporary memory and deleted when users close the browser. They contain a session ID, which keeps users logged into a website as they navigate from page to page (that is, they maintain "state" on a website).

Persistent cookies, as the name implies, stick around a little longer and are not deleted when users close the browser. How long they survive depends on the expiry date that was set by the website or when the user deletes the cookies.

First-party cookies are cookies placed on a visitor's hard drive by the initial website a person visits.

Third-party cookies are cookies placed on a visitor's hard drive after clicking on an advertisement or other content that is hosted by the initial website that person visited. It is important to note that third-party cookies are not always covered in the privacy policies that govern the original website.

Flash cookies were developed in the early 2000s by Macromedia (later acquired by Adobe Corporation). Officially referred to as locally stored objects, flash cookies improve the operability of Adobe Flash. They can do everything standard cookies do and more:

- They are persistent. No expiry dates are required. This means information can be stored indefinitely unless the developer is mandated by business requirements to include expiry dates.
- Their default size is 100 KB, which is 25 times larger than a browser cookie.
- Where they are stored in a user's machine is system-specific and not controlled by the browser. Thus, a computer running a Windows operating system will store the file in a different location than where a computer running a Mac operating system will store it. For the average user, these locations are difficult to find.
- Since flash cookies are not controlled by the browser, other browsers on the same machine can access the same flash cookies.
- Information collected is dependent on the application. To put it another way: whatever the developer wants, the developer can get!

These characteristics are the reason flash cookies are often referred to as *super cookies*.

The Rise of the Evercookie

A new type of super cookie has emerged: the evercookie. For the average user, evercookies are nearly impossible to delete. Even someone with above-average technical skills may become frustrated by them.

Evercookies use a technology called Persistent Identification Element (PIE), developed by online tracking firm United Virtualities, to recreate or copy cookies to other locations on a user's machine. *Whatis.com* defines *PIE* as "a method of individually tagging users' browsers for the purposes of identification and tracking.... [It] uses a combination of Javascript and Flash to create this tracking substitute.... The method makes it possible for deleted HTTP cookies to be respawned from stored data associated with the unique identifier."

Sam Kamkar, developer of the evercookie, elaborates further: "Cookie data [are stored] in several types of storage mechanisms…available on the local browser. Additionally, if [an] evercookie has found the user has removed any of the types of cookies in question, it recreates them using each mechanism available."

There are at least 10 storage mechanisms, including HTML5 Session, Local Storage, and Silverlight Isolated storage. For a list of available storage mechanisms, check out *samy.pl/evercookie/*.

Other Tracking Mechanisms

Other tracking mechanisms fall into the same family as cookies.

Web beacons (sometimes called *web bugs* or *pixel tags*) are small GIF or PNG transparent images (1 pixel by 1 pixel) embedded in some web pages or HTML-formatted e-mail messages. When a user opens a web page or e-mail message containing a web beacon, regardless of whether it's from a computer or mobile device, a request is sent back to the server, where a record of that request will be stored.

Web beacons are used primarily by third-party advertisers to analyze website traffic and improve the quality of advertisements. When used in conjunction with cookies, they help advertisers build unique profiles about the user.

Device finger printing pertains to information collected

Method	Description
Session fixation	The perpetrator guesses what the user's session ID might be by using e-mail phishing or brute-force searching and induces the victim to log into the web application. To mitigate the risk of such an attack, developers should ensure randomly generated strings are used to create session IDs.
Session sidejacking (or man-in-the-middle attack)	Packet or network sniffing software is used to read network traffic between two people, usually on a public Wi-Fi network. In this vector, the thief steals the session cookies while in transit and uses the information to impersonate the victim. To help prevent such an attack, developers should ensure encryption is used for the entire life cycle of a cookie, not just while in transit.
Cross site scripting (XSS)	Here, attackers use methods such as e-mail phishing or entry points such as search fields, feedback forums, and messaging boards to inject client-side script. When successful, they compromise a web application and gain access to session cookies. To mitigate the risk, developers must ensure end-user input is validated and sanitized.

Table 1: Cookie Hijacking Methods and Mitigation Strategies

online in real time from smartphones, tablets, and other computing devices. Unique characteristics are collected, including operating system, screen resolution, mouse screen position, server domain, the type of cookies stored, a postal code within a four kilometer accuracy radius, and more.

That's just the tip of the iceberg! Like cookies, device finger printing can be used to identify those devices on subsequent visits and build unique user profiles. More information about device finger printing can found at *https://panopticlick.eff.org/*.

IG's Role in Privacy Protection

As the Principle of Protection states, "Information governance program shall be constructed to ensure a reasonable level of protection to information that is personal or that otherwise requires protection." This Principle applies to *all* information collected through any technology, regardless of medium or process. IG practitioners should take an active role in ensuring compliance with this Principle, including the following.

Collaborating with Developers

IG practitioners can point developers to the guidance provided in the proposed standard Internet Engineering Task Force (IETF) 6265 *HTTP State Management Mechanism*. (Although a request for comment about this proposed standard was published in 2011, it has not been finalized.) "[It] defines the HTTP Cookie and Set-Cookie header fields."

That header includes the following attributes that, when used in conjunction with the Principles, reduce liability exposure:

- The Expires Attribute
- The Max-Age Attribute
- The Domain Attribute
- The Path Attribute
- The Secure Attribute
- The HttpOnly Attribute

For newer technologies that utilize HTML5 storage and other collection mechanisms, it's equally important, if not more so, to ensure the Principle of Protection is incorporated early in the systems development lifecycle (SDLC). Though it is beyond the scope of this article to delve into security for HTML5 and other collection mechanisms, IG practitioners can point developers to *http://html5security.org/* and to the Table 2 "Checklist for Developing Transparent Policies and Building Secure Web Applications."

Mitigating Cookie-Related Risks

Vulnerabilities related to cookies *can* be exploited by what seems to be a growing number of attack vectors. Take, for instance, *cookie hijacking* (also called *session hijacking*), which takes place when an attacker intercepts a valid session token, exposing the end user's identity credentials for logging into a remote server.

Table 1 describes three methods for initiating such an attack and ways in which developers can mitigate their risks.

Getting Executive Support

C-level leaders must understand their responsibilities

for the security of information. Otherwise, the costs can be enormous.

Although the cost of the December 2014 cyberattack on Sony Pictures Entertainment is not yet known, Reuters News Agency projected it could be as much as $100 million. Robert Smallwood, executive director of the Information Governance Institute, said in a Dec. 30, 2014, LinkedIn blog posting that estimate is "way off." He speculated that the cost could be as high as $1 billion, factoring in lost revenue; cyber insurance; recruiting, onboarding, and training IT security personnel; reputational ill will; and areas yet to be identified.

Establishing Risk Programs

Thousands of laws around the world regulate privacy, which is why many organizations are establishing privacy risk mitigation programs.

In the European Union (EU), for instance, companies must comply with amendments to the 2002 EU E-Privacy Directive. Nicknamed the "Cookie Law," the new rules apply to any web-tracking technology.

In Spain, several investigations are under way, with fines having been levied against two companies in 2014 for non-compliance. *Computer Weekly* reported in late 2013 that six EU countries "are investigating Google Privacy policy because of concerns about personal data [collected] and stored in foreign jurisdictions."

Since 2010, many companies have faced legal action as a result of using flash cookies. *Wired* magazine reported in December 2010 that Quantcast, an online tracking firm, "agreed to pay $2.4 million to settle a class action lawsuit alleging it secretly used Adobe's…Flash plug-in to recreate tracking cookies." In 2012, Amazon settled a similar case, though the details were not disclosed.

Applying the Principles

In addition to the Principle of Protection, three other Principles are relevant to the use of cookies and web-tracking technologies:

- Principle of Integrity: If session cookies can be intercepted in transit, unauthorized users can assume someone's identity and alter the information on that system. By adhering to the Principle of Protection, an organization can protect the integrity of its information.
- Principle of Transparency: Being deceptive about the techniques used to collect information exposes a company to risks associated with consumer backlash. If fraud prevention and enhanced functionality are reasons for using web-tracking techniques, then make it clear in your privacy policy.
- Principle of Disposition: If multi-year expiry dates are set (for HTTP cookies), or if none is set at all (for flash cookies), then organizations are transferring the risk of unauthorized exposure to their customers, whose machines may contain information that is sensitive. If there isn't a well-defined business reason for storing information on a user's machine for a long period, then there is no reason to allow cookies or other tracking technologies to persist for several years.

Read More About It

- The Unofficial Cookie FAQ: *www.cookiecentral.com/faq/#3.3*
- Cookie Overview: *http://itlaw.wikia.com/wiki/Cookie*
- HTTP Cookie: *http://en.wikipedia.org/wiki/HTTP_cookie#Persistent_cookie*
- HTTP State Management Mechanism: *http://tools.ietf.org/html/rfc6265*
- "Flash Cookies and Privacy" Study Report: *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862*
- Session Hijacking Information: *http://en.wikipedia.org/wiki/Session_hijacking*
- White Hat Security Statistics Report 2013: *www.whitehatsec.com/statistics-report/2014/06/10/statsreport.html*
- "Cross-site scripting explained: How to prevent XSS Attacks": *www.computerweekly.com/tip/Cross-site-scripting-explained-How-to-prevent-XSS-attacks; HTML5 Security resources: http://html5security.org/*
- When do items in HTML5 local storage expire?: *http://stackoverflow.com/questions/2326943/when-do-items-in-html5-local-storage-expire*
- "How should application developers manage cookies?" article: *http://searchsecurity.techtarget.com/answer/How-should-application-developers-manage-cookies*
- Evercookie information: *http://en.wikipedia.org/wiki/Evercookie*
- About Device Fingerprint/Deviceprint: *http://www.darkwavetech.com/device_fingerprint.html*
- See your device fingerprint: *http://noc.to/#*

Developing Policies

In collaboration with the stakeholder community, IG practitioners can use the checklist below to develop transparent policies and build secure web applications.

The Future

From a technological perspective, a lot has happened in the last 20 years in the field of online data collection, now referred to as web analytics. Some readers may have drawn the conclusion that Http cookies' days may be numbered as HTML5 matures in the marketplace. That may be true, especially as more applications become interactive, though probably not any time soon.

There are many intranet and Internet sites that utilize cookies and web beacons and will continue to use them for a variety of well-defined business reasons. Heating up fast is the debate about whether respawning standard browser cookies after the user has deleted them is an acceptable business practice.

The world is changing fast. As such, IG governance and leadership are now a requirement for many organizations. IG practitioners must be ready to step into that role.

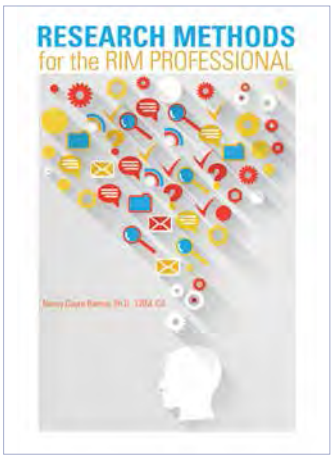
END

Mark Grysiuk, CIP, can be contacted at mgrysiuk@rogers.com.
See his bio on page 47.

Checklist for Developing Transparent Policies and Secure Web Applications

Question	The Principle	Accountability	Yes, No, N/A
Has a privacy impact assessment been conducted?	Protection	IG Team/ Senior Management	
Is the section about web-tracking technologies in the privacy policy easy to find?	Transparency	IG/Team Senior Management	
Is the policy written so it's easy to understand?	Transparency	IG Team/ Senior Management	
Does the policy explain what information is collected, why it's collected, and how long it is kept?	Transparency	IG Team/ Senior Management	
Are web beacons explained (if applicable)?	Transparency	IG Team/ Senior Management	
Is device finger printing explained (if applicable)?	Transparency	IG Team/ Senior Management	
Is the opt-out feature easily accessible?	Transparency	IG Team/Developer	
Is the application collecting the minimum amount of data that's required?	Transparency	IG Team/Developer	
Is the expires attribute set at the minimum period required?	Disposition	Developer	
Is the max-age attribute set?	Disposition	Developer	
Is the domain attribute properly set?	Protection	Developer	
Is the path attribute set?	Protection	Developer	
Is the secure attribute set?	Protection	Developer	
Is the HttpOnly attribute set?	Protection	Developer	
Are randomly generated strings used for session IDs?	Protection	Developer	
Are expiry dates coded for HTML5 local storage?	Disposition	Developer	
Are all available storage mechanisms being used? If so, are valid business reasons documented?	Disposition	Developer/IG Team	
Is user input validated and sanitized?	Integrity	Developer	
Are cookies encrypted for the entire life cycle of their existence?	Protection	Developer	

Resources for Advancing Your Career



Research Methods for the RIM Professional

Nancy Dupre Barnes, Ph.D., CRM, CA

In this era of "big data," records and information management (RIM) professionals that have a basic understanding of the foundational theories buttressing data analysis, such as research methods, have increased value to their organizations.

This book serves as an introduction to research methods, using examples that are specifically relevant to archives and RIM professionals, where possible. It will also help IGP candidates improve the knowledge and skills referenced in the DACUM chart domain of "Managing Information Risks and Compliance."

A4970 Soft cover **$60.00** Professional Members: **$40.00**

Managing Active Business Records

Ann Bennick, Ed.D., CRM & Judy Vasek Sitton, CRM

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

A4913 Soft cover **$60.00** Professional Members: **$40.00**

Order online today! **ARMA INTERNATIONAL BOOKSTORE**

www.arma.org/bookstore

Principles for Outsourcing Mission-Critical Business Processes

Julie Gable, CRM, CDIA, FAI

Organizations that outsource mission-critical business processes have a distinct challenge ensuring their information is properly managed, as service providers are not just storing the organization's information, they are using highly automated processes to create, process, and use it. This article discusses how it must also be governed.

Cloud-based services such as storage, software-as-a-service, and infrastructure-as-a-service have made it possible to outsource almost anything. Although it has been common to outsource paper and electronic records storage, as well as back-office business processes such as HR benefits administration or payroll processing, organizations now are also outsourcing mission-critical functions and services.

For example, a county government might decide to outsource turnkey social welfare, human services, and correctional functions, while a pharmaceutical company might decide to outsource a regulatory function such as adverse event reporting.

This so-called "second tier" outsourcing is in response to the more recent availability of large service providers offering sophisticated technology and tools, such as big data, business analytics, and industry-specific processing services.

While the traditional rationale for outsourcing has been cost savings, operational flexibility, off-loading non-core competencies, and the short-term tax advantages of outsourcing versus making capital investments in specialized systems, the rationale for outsourcing mission-critical functions is more about gaining access to providers' technology and expertise.

In outsourced customer-related processes, for example, organizations may glean competitive insights through using the service provider's data manipulation capabilities.

Shared IG Responsibility

What happens to information governance (IG) when mainstream

business processes are transferred to a service provider (SP)? Because IG is about how an organization handles information that arises from its business processes, regardless of where or how those processes are completed, IG principles must apply to how the organization's SPs handle its information, as well.

For this reason, mission-critical outsourcing is becoming a topic for discussion at the enterprise level by the legal, records, and IT members of the IG council or among senior management in consultation with an IG officer.

As the trend to outsource business operations continues – a trend IDC predicted in its "Worldwide and U.S. IS Outsourcing Services 2013–2017 Forecast" would grow 6% per year worldwide, reaching $209.4 billion – organizations need to be aware of how these third parties accomplish their tasks and how they treat the records that are created as part of outsourced business processes.

Tools for Evaluating Providers

The bottom line in this age of compliance, litigation, and operations concerns is that it is reasonable to expect that when SPs create and manage an organization's information, they will do so to the contracting organization's standards.

The Generally Accepted Recordkeeping Principles® (the Principles) are a good source of such standards. With a little tweaking, this highly adaptable tool can be used to:

- Highlight the trade-offs inherent in outsourcing and show areas where higher risks may justify requests for additional third-party IG services
- Evaluate a potential SP's information-handling methods before committing to a contract
- Establish a common understanding of governance at the outset of the relationship
- Help set expectations and evaluate an SP's performance over time

The Principles and the Information Governance Maturity Model (IGMM), which are both available free at *www.arma.org/principles*, are templates for conversations among all the stakeholders involved, providing the basis for arriving at an understanding of what is ideal and what is realistic. The truth is that contracting for extra IG services may incur extra costs. The point is to identify and prioritize those aspects of IG where the reduction of risk is worth the extra cost.

Here, then, are possible considerations for using the Principles to assess an SP's IG capabilities.

The point is to identify and prioritize those aspects of IG where the reduction of risk is worth the extra cost

Evaluating Service Provider Attitudes

The Principles of Accountability, Compliance, and Transparency are the cornerstones of an organization's entire IG program and are not necessarily associated with any one business process. The point in due diligence is to understand how the SP will help (or hinder) efforts at ensuring the outsourced process is performed with reasonable levels of all three Principles in mind.

It is important to realize that an outsourcing organization retains ultimate responsibility for accountability, compliance, and transparency and that the service provider should work as a partner to its goals. There are three primary questions to consider:

Who Is Accountable?

Who at the SP is accountable for the business process and the records it creates? If the answer is the account rep, run! There should be someone at a management and/or technical level who is directly accountable for process oversight, verifying the process gets done correctly and that all aspects of the process, including the information produced, are handled as they should be.

All too often, the real test of an SP's accountability occurs when something goes wrong. Recognize, too, that ultimate responsibility for the validity of the process remains with the outsourcing organization, not with the SP. This implies there is someone within the outsourcing organization who regularly monitors the outsourced business process to ensure it is going as expected.

How Is Compliance Defined?

Does the SP interpret compliance in the same way the outsourcing organization does? Where an outsourced process is regulated, it is important to make sure the SP, even one who specializes in the outsourcing organization's industry, interprets the relevant regulations in the same way.

For example, how does the SP maintain records that demonstrate the outsourcing organization's compliance? If there is a reporting deadline, for instance, how does the SP prove the deadline was met?

Another question to ask is how the SP participates in a regulatory audit. Note that due diligence in compliance capabilities implies the outsourcing organization already knows the compliance requirements for the business process. As noted above for accountability, someone within the outsourcing organization should

regularly monitor that compliance requirements are met.

Are There Policies and Procedures?

Does the SP have written policies and procedures for the process that go beyond simple programming documentation? Adherence to the Principle of Transparency should be demonstrable by the SP in the form of documented processing and information management rules. Ideally, these should be available to regulators or investigators as needed.

Other aspects to consider are how, and how often, the SP's employees are trained in these rules. Many large SPs have substantial employee turnover, so training should be frequent and documented.

Evaluating Recordkeeping Practices

The Principles of Integrity, Protection, Availability, Retention, and Disposition are directly associated with good recordkeeping practices and IG maturity. They prescribe the quality of services expected from the provider with respect to the records created, used, and stored as part of the business process.

One of the disconnects inherent in outsourcing is that *ownership* of the information remains with the outsourcing organization, but *responsibility* for the information's reliability, security, accessibility, maintenance, storage, and disposition rests with the service provider.

SPs may be unfamiliar with these Principles. Most are organized as information technology-enabled SPs, and their interest is in a business model that stresses automation to deliver process results for each client while leveraging systems and software across many clients. Providers sell their services touting benefits like flexibility, mobility, and accessibility, and they may not be familiar with the risk-related aspects of recordkeeping principles.

Consider including a contractual clause giving the outsourcing organization the right to audit the provider's protection process…

Here is where the biggest potential trade-offs are, and it is wise to go into the outsourcing agreement with an eye not just on present benefits, but also on future risks. Some considerations from the Principles include the following:

Demonstrating Integrity

How does the provider demonstrate that the records it makes and manages on the outsourcing organization's behalf are reliable and authentic? Possibilities include:

- Test results that show its hardware and software consistently produce the same result
- Strict controls on who may edit or change records
- Audit trails to record when and by whom changes are made
- Standards for process timeliness and backlog prevention
- Ongoing training that is refreshed as needed for old and new employees

Often overlooked is the importance of the integrity of record dates. If the provider will import a large batch of the organization's records, be sure the metadata field for record date does not change to the import date. The same is true for paper records that will be scanned by the provider for use in its processes.

Providing Protection

SPs typically have excellent antivirus, anti-hacking, and back-up capabilities, which are important for protecting *systems*. *Records* protection, however, includes generating automated access logs that are updated frequently to ensure that only authorized individuals can work with the process or view the information.

The SP must limit the number of people who may access personally identifiable information and health information. The need for protection extends to information the provider asks the cloud service providers to store.

Because SPs have high turnover rates, it is important that access is denied immediately to employees that leave the company and that functionality controls are in place to prevent unauthorized e-mailing, copying, tweeting, or posting of sensitive information to the Internet.

Consider including a contractual clause giving the outsourcing organization the right to audit the provider's protection processes at regular intervals.

Ensuring Availability

One key benefit of outsourcing is that people with access rights may view records anywhere, from almost any device, at any time. The risk connected to the Principle of Availability is subtle and long term.

For example, an organization has to know whether at the end of the contract its information will be viewable and usable if it no longer has access to the provider's system and software. Some SPs' contracts allow for organizations to continue to use their infrastructure for some time until new arrangements are made either to bring the process back in-house or transfer it to another provider.

Another consideration is for any paper records the SP has scanned. If the paper records require retention

along with their electronic counterparts, they need to be kept in order. Most scanning processes are throughput-driven, and documents are often simply put back into boxes without the benefit of file folders to separate them or keep them in order. When this happens, the result at the end of an outsource agreement is a truckload of boxed chaos delivered back to the outsourcing organization.

An additional concern related to the Principle of Availability is whether records can be transferred to an e-discovery process, which also may be an outsourced service. Many law firms outsource e-discovery for large cases, so it is important to know in advance exactly how records in the custody of SPs will be designated for legal hold and how they will be made available for discovery purposes.

Effecting Retention and Disposition

Most SPs keep everything forever, which can be a risk, depending on the category of the records. It is rare, though not impossible, for retention codes to be captured as part of the metadata for records as they are created. Adhering to retention rules, particularly when they are event-based, is much more difficult for electronic records and usually requires human intervention. Because the provider's process model relies on automation as much as possible, it may have neither the ability, nor the willingness, to assume responsibility for retention and disposition.

Most organizations would not want an SP to perform disposition, and certainly not without a pre-defined approval process that considers legal hold requirements. It is prudent to document that the records associated with the outsourced business process may be retained in excess of the outsourcing organization's normal policy and acknowledge that the organization is aware of this risk.

'Outsourced,' Not Out of 'Scope'

In the past, few standards for outsourced functions existed other than service level agreements that covered things like system availability, uptime, and security. In the old view, the SP was a "black box" with little or no oversight given to how it operated except to accomplish what was contractually required. Some organizations believed that when they transferred information to SPs, they transferred all responsibility and accountability to them as well.

In the current age of regulatory and legal scrutiny, more organizations realize that outsourced does not mean out of scope of their IG accountability. Luckily, the Principles' clear definitions and the IGMM's specific benchmarks provide guidance in assessing the providers' IG capabilities.

The key is to use these tools to determine what SPs can – and cannot – provide and determine the impact of that on the organization's IG goals. Identifying risks may not impede the decision to outsource, but it does provide the advantage of a long-term perspective and the avoidance of surprises in the future. **END**

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

An organization that has decided to outsource its electronic records storage must do its due diligence in selecting a service provider (xSP) to ensure that its information will be managed appropriately throughout its life cycle. A critical aspect of this is investigating how potential xSPs will protect the information it is hosting.

The three following checklists from the technical report *Understanding Electronic Storage Technologies* (ARMA International TR 26-2014) will be invaluable tools for evaluating xSPs – and most of the checklist items would also be relevant for organizations wanting to evaluate how well they are protecting the records they store in house.

Readers should note that not all items in these checklists may be applicable to their organizations; careful consideration of their unique needs, requirements, and resources (i.e., timelines, personnel, and budgets) is essential.

Checklists for Evaluating Electronic Records Storage Protection

Checklist for Evaluating the xSP

Financial Stability

What is the ownership structure of the xSP (e.g., family-owned, sole proprietorship, partnership, or corporation)?

How many years has the xSP been in business?

How many years has the xSP been providing electronic records storage services?

If the xSP encounters financial difficulties, what legal agreements control the operation of the facility?

- Does bankruptcy trigger evacuation of all stored electronic records?
- Would a third party be enlisted to operate the facility?

xSPs' Providers

What electronic records storage services does the xSP subcontract?

Who are the subcontractors and where are they located?

Does the xSP own or lease the business's facilities such as the physical structure or real estate?

Could the real estate owner's bankruptcy or lienholders create a disruption in the conduct of business?

Are protection agreements in place should a utility company (e.g., communications services provider) fail to deliver on a contractual agreement?

If an energy crisis occurs that disrupts power or fuel availability, is a contingency plan in place that provides an alternative energy supply?

Checklist for Evaluating Electronic Records Security

Access Controls

How does the xSP prevent commingling of electronic records from various contracting organizations?

- What procedures are used to ensure xSP employees cannot release electronic records to the wrong contracting organization?

Are processes in place to secure electronic records from corruption, theft/intrusion, unauthorized access, and/or viruses?

What encryption methods are available and how are encryption keys stored?

What access controls are available?

What procedures exist for detecting security breaches?

What notification processes are in place (to alert the xSP and contracting organization) of potential security breaches (e.g., unusual usage patterns or unapproved configuration changes)?

What services are provided from entities located outside the United States?

What subcontractors or third parties have access to the contracting organization's electronic records?

- Is access encrypted and is it granted over the public network, a virtual private network (VPN), or via physical tape transfer?

Are all electronic records transmissions between the xSP and contracting organization performed in a secure (e.g., encrypted) manner?

- If a VPN is used, what entity is responsible for its maintenance?

Does the xSP have a robust firewall to prevent unauthorized external access?

How are audit trails tracking security-related activities managed?

System Issues

What are the critical points of system failure and how is redundancy ensured?

How is equipment slated for de-commissioning and previously used to transmit/store electronic records dispositioned?

Breach Response

If a security breach occurs (or is thwarted) while a backup is in process, what procedures are in place to avoid compromising backup operations?

In sophisticated attacks, secure lines can be diverted and backup mimicked. How would this situation be handled?

In the event of sabotage, can a remote command purge electronic records stored at the facility?

> Readers should note that not all items in these checklists may be applicable to their organizations; careful consideration … is essential.

Checklist for Evaluating Facility and Personnel – Safety and Security

Environmental Issues

Has an "Unacceptable Threat Matrix Identification" been performed?

Has the site been evaluated as outside of the 100-year flood plain?

- Are there issues that could change the flood risk at the site?

Is there proximity to nuclear power plants, chemical plants, pipelines, refineries, or other facilities that could create the need for a facility evacuation?

- Are underground storage tanks adjacent to the site?
- Could tanks create a contamination that would necessitate evacuation?
- Has a Phase III Environmental Hazard Risk Assessment been done?

Is the site in an area prone to civil unrest or high crime? (Lack of a secure neighborhood can affect the xSP's ability to retain a highly-skilled staff and maintain effective operations; criminal activity in the area can diminish employee morale and increase the xSP's insurance costs.)

Who are the adjacent tenants and landowners?

- Are there adjacent tenants that limit control and integrity of the site's ingress/egress?
- Is the site in an airport glide path where a crash or radar signals could interfere with electronic systems operation?

Does the site have security fencing, closed circuit television, motion sensors, and manned patrol or security guard monitors?

- Is there a security gate at the entrance to the site?

If applicable, has the security of fuel storage tanks been verified?

- Is there control fencing or are there buried units?
- Given the risk exposure, are the tanks of sufficient size? (Hurricanes or earthquakes can limit power supply for several weeks.)

How is the communication grid attached to the building (e.g., underground)?

How is traffic controlled?

- Could traffic patterns make the site difficult to reach in a threat (e.g., narrow and/or one-way streets)?
- Are there motor traffic set backs or barriers to limit vehicles proximity to the building?
- Are visitor and service vehicles searched for contraband?
- Can vehicles be inspected 150 feet or more away from the building?

How are parking areas secured?

- Are parking spaces assigned?
- Is there proper security lighting?
- Are there areas where trespassers could conceal themselves?

Are there multiple entry requirements with access controls such as photo identification badges, key cards and/or biometric interfaces?

Building Security

How is the building secured?

- Does the building design incorporate tiered levels of security such that there is lower to higher security as the data production and media storage areas are approached?
- Are there window barriers (burglar bars), security screens, or polycarbonate barriers?
- Is there visual control of delivery bays and entry doors?
- Is there minimal signage to avoid publicizing the existence of the building and its assets?
- Are dumpsters located away from the building?

What digital surveillance cameras and systems are in place?

- Are all entry doors, passageways, docks, delivery bays, foyers, and the entire server and data center area covered by digital cameras or closed circuit television with continuously monitored feeds?
- Is the digital camera feed set up to record locally and feed to a secure browser for remote monitoring? Or, is there monitoring via a mobile device such as a smartphone? (Remote feed or mobile device access could serve to assist fire fighters in responding efficiently to a threat.)
- Are the digital cameras equipped with motion sensors to respond to movement in secure areas? (These motion sensors can help firefighters locate staff trapped in the building during a fire.)
- Is digital video sent offsite to a remote recorder with dual copies available?

How is building access controlled?

- Are there access control levels with increasing rings of security and anti-passback (i.e., "in" must be followed by "out" before another "in" can be used)?
- Are there multiple entry requirements with access controls such as photo identification badges, key cards, and/or biometric interfaces?
- Is access also controlled by shift scheduling so that work hours are defined?

What are the procedures for ensuring the security of visitors to the building?

- Are there sign-in logs or a digital photo log?
- Are appropriately designated identification badges (e.g., color-coded tags worn in an externally-identifiable manner) issued to visitors?
- Are visitors escorted at all times while on-site?

Building Stability

Have the building's design and structure been assessed?

- What are the ratings for snow load, wind, water runoff, and ice storms?
- Is the facility grounded for lightning?
- Are window designs consistent with threat levels?
- Is the building rated for the proper seismic zone (I thru IV)?
- Is there base isolation for the data processing area?
- Are there prints on file with the original stamp and approvals?
- If the building is older than 15 years, has there been a licensed, professional inspection by a structural engineer with a review of existing wiring and light fixtures, and a review for contaminants, polychlorinated biphenyls (PCBs), or asbestos?
- Has the roof been inspected? Is there a water leak report or drainage inspection?
- Are walls floor-to-ceiling to prevent movement over the walls or through the heating, ventilation, and air

conditioning (HVAC) ductwork?
- Is the overall structure four-hour rated per the National Fire Protection Association (NFPA) standards for ground-supported structures?

Has there been a fire sprinkler inspection to evaluate water supply and source pressure as well as actual pressure available at heads?

Fire Protection

Has the building been assessed for fire hazards?

- Has there been a fire sprinkler inspection to evaluate water supply and source pressure as well as actual pressure available at heads? Have the pump systems been maintained?
- Is electrical wiring in conduit? Are ground fault or arc breakers used for critical area breaker panels?
- Are firewalls a vital part of the building design? Are fire stops used in wall penetrations? Are fire dampers in place to stop spread of smoke and fire and explosive gases?
- Is a fire marshal's inspection report on hand?
- Are the fire marshal and fire fighters familiar with the facility?
- Are hose seats defined in a fire fighter's plan of action?
- Are high security areas defined for early action suppression?
- Is a fire drill procedure in hand, allowing the evacuation of the building's occupants and the identification of a meeting area at evacuation?
- Is the fire department aware of media vaults and server vaults?
- Is the fire department aware that firefighters should not penetrate vault doors or server vault doors as it voids fire suppression control?
- Has the fire and casualty insurance carrier audited the facility for acceptability?
- Are there adjacent undeveloped, wooded areas that could pose a fire risk?
- Are staff smoking areas located a sufficient distance away from the building or media storage area?

Communications

What are the procedures for communication security?

- Are alarm signals sent by dual technology (FM and hardwire)?
- Is satellite telecommunication available to maintain connectivity during a utility outage, e.g., mobile satellite radios and repeaters?
- Are the communication lines monitored to avoid security risks and what is the procedure if a security breach occurs?
- If Wi-Fi is utilized, are appropriate security precautions implemented to safeguard communications transmissions originating inside the facility from possible detection by external entities?
- Are the wiring logs and design plans protected, with access limited to only authorized personnel?
- Is there radio frequency shielding or protection for server vaults?
- Are there rated cable trays for all wire entry points?
- Is the communication infrastructure located within rigid conduit within the facility?
- Are laptops and other mobile devices controlled through a mobile device management plan?
- Is there a call tree for communicating a change of security status?
- Will a fire alarm or security event trigger a breakdown in security?
- Are wireless local area networks secured? Is the information encrypted? To what level?
- Is the communication program designed so that the contracting organization and the xSP can easily remain in contact?
- Are there documented procedures for contact with community fire or police services?

Vaults

How secure is the vault structure?

- Is the secure vault chamber rated as Class 125 (UL 72) to protect the computer hardware, servers, switches, routers, and media?
- Is a secure vault door with a Class 125 (UL 72) fire rating and listing in place? Is the door labeled as such for audit assurance and documentation?
- Is the vault door equipped with a smoke- and heat-activated hydraulic closer to seal the vault door in the event of a fire?
- Is the door closer equipped to communicate with the internal clean agent fire suppression alarm panel as well as the building alarm panel to close the vault chamber during either alert status?
- Is the location of the vault capable of providing the ultimate security for the data chamber?
  - If the vault is located above grade, is the vault rated as six-sided for protection (per GSA Federal Specification AA-V-2737) from a fire below the server or data processing area?
  - Is the vault located above the level where flooding

could occur?
- Are the batteries for the uninterruptable power supply (UPS) system located within the vault?
- Is the vault located sufficiently away from elevator shafts, transformer or switch gear, or other equipment that delivers high electromagnetic interference?
- Are restroom or other plumbing-related facilities located so that they cannot create water or flooding hazards to the chamber?
- Is the vault optimally located to avoid the outside entrapment of radio frequencies or other information that could disclose data to a saboteur?
- Is the vault chamber equipped with a water-shield roof deck to avoid contamination from external firefighting activities, sprinkler activation, and water main breaks?
- Is the vault rated for water-shielding (per NFPA 220) if the data center is in a hurricane or tornado-prone region?
- Is the vault rated for Zone IV seismic protection (per NFPA 220) if the data center is in a seismic activity area?
- Is the vault rated for regional threats, e.g., termites, snow loads, high humidity, etc. (per NFPA 909)?
- Can a fire alarm, security alarm, or general evacuation order pose a particular threat by opening egress doors or circumventing access control?
- Is the vault chamber designed to secure itself upon each ingress or evacuation?
- Are portable extinguishers available near the vault for first responders?

Is the vault rated for regional threats, e.g., termites, snow loads, high humidity, etc. (per NFPA 909)?

What is the electrical design for the vault?
- Are the wire penetrations and cable trays rated for fire protection to the level of the vault chamber?
- Are the wire systems earth-grounded and fitted with the proper breaker switches?
- Is the electrical load sufficient for the load capacity?
- If the computer or switch equipment has been changed lately, has the chamber's load capability been re-evaluated for proper voltage?
- Are the vault penetrations completed with Class 125 (UL 72) fire-rated cable trays?
- Are the wiring harnesses, power circuits, and communication cables located above the servers to avoid flood contamination?
- Are the wiring systems set at ceiling level for ease of change out and to avoid extended downtime?
- Are wire management systems sufficient for future growth?
- Are communication fibers compliant with current industry standards?
- Are communication fibers Class IV (ISO/IEC 11801) or higher?

What are the environmental controls for the vault?
- Is the air conditioning facility a split system requiring through-wall coolant piping? (If so, these penetrations should be designed to avoid heat transfer from a fire.)
- Is the air conditioning system external to the chamber? (If so, the fire dampers should be of the same rating as the vault and designed to seal the duct opening by activation of heat or smoke detection.)
- Is the supply and return capability sufficient for the hardware loading?
- If the server equipment has been retrofitted after the initial vault install, is this chamber sufficiently cooled for the new heat loads?
- Is there a mechanical engineer's stamped drawing attesting to the proper cooling loads?
- Is there an environmental monitor providing online, real-time and historical vault status?
- In the event of a failure or alarm detection, is the environmental monitor set to report to a manager (via mobile phone, for instance) at all times?
- Is the vault chamber equipped with vapor barriers to prevent smoke and environmental contamination of the area?
- Is the vault equipped with an air-lock foyer to prevent dust and other contaminants?
- Are the man-trap foyer and the vault chamber entrance doors equipped with card or biometric access control?
- Is there a procedure for maintaining the cleanliness of the vault that will not compromise the integrity of the vault's security?
- Is air filtration accomplished with high efficiency particle arrester filters? (Ozone air cleaning may affect computer equipment and is a health concern for employees.)
- Is the vault chamber set up with closed loop technology to avoid contaminants?
- Are air intake vents for the vault area secure from sabotage?
- Is the roof area over the data chamber routinely main-

tained and designed to direct water leaks away from the vault area?
- Is the heat level within the server vault monitored?
- Are temperature and humidity displayed online for management control?
- Are environmental control systems designed to routinely and automatically communicate with managers?
- Have pest control features been incorporated into the data center structure's design (e.g., rodent and/or termite infestation prevention)?
- Is pest control part of the data center's ongoing maintenance program?
- Are there sealed slab and moisture barriers, as well as sealed windows?

Is there a clean agent suppression system for the vault?
- Is the clean agent suppression system designed for use with fragile electronic/computer equipment?
- Is it a "zero residue" clean agent suppression system?
- Are smoke, heat, and ionization detectors integrated into the system design?
- Is the system inspected and "green tagged" as safe for use?
- Has a complete scenario been run on the alarm panel, door closer interface, door closer, strobes, horn or alerting device, connection to the main building alarm, and alert to the community fire station?
- Does the alarm set off alerting devices outside the building to notify neighbors, if applicable?
- Are systems in a protected wiring loop?
- Is the building alarm an Underwriter's Laboratory Class A Central Station reporting type?
- Has the backup power system to the alarm panel been tested for battery life?
- Does the system present a risk to the servers or personnel at activated delivery?
- Is the system of high dielectric strength to avoid damaging computer hardware?
- Is the system equipped with an abort switch as well as a remote annunciator? (The remote annunciator allows the staff to check on the vault with sensors and camera video without opening the door and possibly defeating the design concentration required.)
- Is a Very Early Smoke Detection Apparatus (VESDA) system in place for early detection?
- Are the light fixtures dust and vapor resistant?

Personnel

What are the policies and procedures for personnel screening?
- Are background checks done for all personnel, both employees and non-employees?
- Are biometric and/or fingerprint records maintained?
- Is there a lie detector procedure?
- Is drug testing randomly conducted?

Are there personnel safety and security policies and procedures for employees as well as non-employees (e.g., janitorial or cafeteria vendors) who provide on-site services?

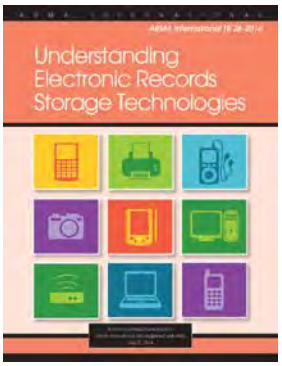
Outsourcing and Audits

Through an audit, the organization should determine the physical security, management capabilities, and processes available to protect the information within the xSP's electronic storage environment. The ongoing protection of the organization's information assets is a task that requires constant vigilance. Economic downturns can pressure xSPs to cut back on operations, especially back-office procedures that are not immediately visible or apparent.

As part of an audit, the organization may wish to review the xSP's history of responses to previous threats and security events or suggest conducting a mock drill. Ideally, the auditor should be able to review a "Threat-Risk Manual" developed by the xSP that indicates the response procedure for each type of event.

Well-developed, consistent response is the goal. The organization may need to change to a different xSP when audit findings reflect unacceptable performance levels or an unwillingness/inability to comply with industry standards benchmarked in the audit.

Read More About It



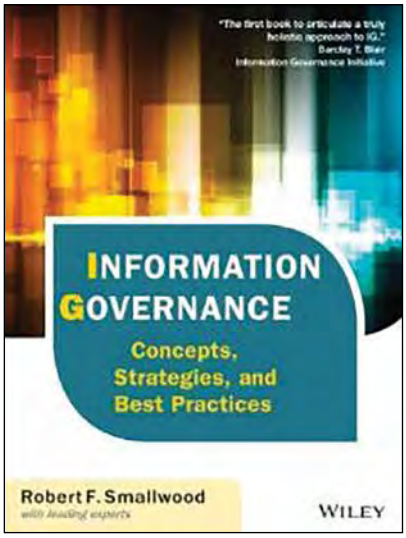
Understanding Electronic Storage Technologies (ARMA International TR 26-2014) is registered as a technical report with the American National Standards Institute. It includes a broad discussion of storage technologies and service offerings for electronic records, 10 checklists for evaluating service providers, and guidance for creating a request for proposal (RFP) document.

It may be purchased in hard copy or PDF format from the ARMA International online bookstore at *www.arma.org/bookstore*. **END**

This technical report was developed by an ARMA International Standards Development Program workgroup led by Kim Mayberry, CRM. She may be contacted via standards@armaintl.org. *See the complete list of team members on page 47.*

A Comprehensive Information Governance Resource

Robert Bailey, Ph.D., CRM



Information governance (IG) is a hot topic in records and information management (RIM) circles, creating a significant amount of interest and conversation online and dominating conference agendas. There are bits about IG here and there on blogs, listservs, web pages, and in magazines, but this book was the first effort to distill all this information to understandable and practical content.

How IG Evolved

Prior to reviewing this book, I would always wonder if IG was just some more of the ARMA and AIIM Kool-Aid or if it was the result of fewer paper records and most communication being electronic: as data generation exploded, regulations and compliance issues increased, and cybersecurity became a concern, traditional records management failed to keep pace.

Since technology changes can render digital resources inaccessible, issues like file formats, metadata, storage media, and compatible software and hardware became more important, and a more comprehensive platform for managing records and information became necessary to address all phases of the lifecycle. This led to the advent of IG and the need of this book.

What IG Is

IG is a developing and evolving field, emerging as a platform for organizations and governments to define policies at the enterprise level, across multiple jurisdictions. It goes beyond records retention and destruction to include privacy, access controls, and other compliance issues. IG includes processes and procedures that can be used to manage information as a business asset, enabling smart companies and information managers to leverage information's value while satisfying legal requirements and controlling risks related to it.

The Book's Structure

This book is extremely well put together. Its five major categories are broken down into 18 chapters, two large IG appendixes, and 442 pages of information. IG theory is backed up and documented with real world examples. The bulk of the work was developed by Robert Smallwood, and 10 other influential experts contributed to various topics with Smallwood co-authoring and editing much of their material.

The Book's Content

The longest chapter in the book is the one on RIM, which is the field most closely associated with IG, according to research contained in the Information Governance Initiative's 2014 Annual Report. Be aware, though, that this is not a deep dive into records management.

Information Governance: Concepts, Strategies and Best Practices
Author: Robert F. Smallwood
Publisher: Wiley
Publication Date: 2014
Length: 442 pages
Price: $75
ISBN: 978-1-118-21830-3
Source: *www.arma.org/bookstore* or *www.wiley.com*

As expected, compliance, e-discovery, privacy, and security also are covered, and the chapter on legal is quite extensive. Because Microsoft® SharePoint® recently has been added to the mix of the leading enterprise content management systems, I read the chapter titled "SharePoint Information Governance" several times.

I really appreciated the Key Point summary at the end of each chapter for quick reference and review. Because of my experience and interest in international records management, I found Appendix B & C's records management and privacy laws and regulations for non-U.S. countries very informative. This content is sadly missing from most other sources on IG and related topics.

Relevance for a Wide Audience

Smallwood presents IG in a high-level, clear, and concise way that is extremely helpful to RIM professionals like me and other readers; hardly a day goes by when he is not poached on the subject.

Information Governance: Concepts, Strategies and Best Practices is already being used as a text in several courses and programs, and it

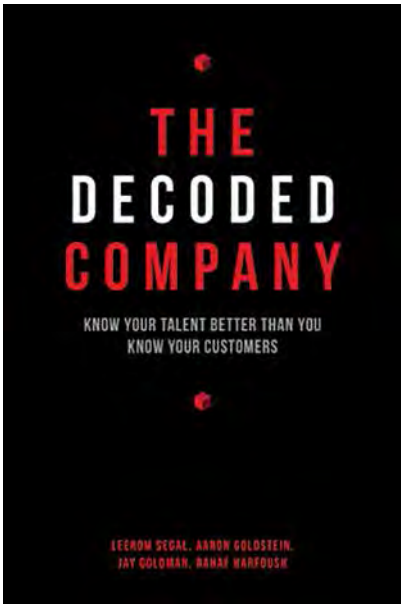
would be a good reference for those studying for the Information Governance Professional exam. It definitely should be included as an essential part of the RIM library and read by all RIM professionals.

It also should be read by CEOs, CIOs, CFOs, and various boards of directors. Without their understanding and stakeholder support to see that the IG program is functioning well and providing business benefits, there is little likelihood of its success. **END**

Robert Bailey, Ph.D., CRM, can be contacted at robertbai@mccarran.com. *See his bio on page 47.*

Following the **Data Trail** for Competitive Advantage

Mary Broughall



The Decoded Company: Know Your Talent Better Than You Know Your Customers by Leerom Segal, Aaron Goldstein, Jay Goldman, and Rahaf Harfoush examines and describes methods to utilize the pervasive trend of tracking data about everything around us. While this book is not intended specifically for records professionals, anyone working with people will be interested in the ideas advanced by the authors.

The Decoded Company

The key to "sustainable competitive advantage," according to the authors, is to become a *decoded company:* one that is "talent-centric, data-driven, flexible, and fast." The authors highlight companies like Google, Starbucks, and Whole Foods, who use big data for serving their customers – and have turned their algorithms inward to decode their own employees.

The authors write that decoding the "real story that is embedded in the data trail" that follows employees and their projects allows companies not to "get the better" of their talent, but to "get the best from them."

3 Transformative Ideas

The Decoded Company distills how this process works with what they call the following "three transformative ideas."

Technology as Coach

The first idea, "Technology Can be a Coach," posits that by personalizing processes to the individual based on experience, an organization can offer training interventions precisely at the teachable moment.

For example, the telecom Sprint was struggling with customer service issues in 2008. The authors' relate how Sprint was able to identify a troubling statistic in one call center:

> Thanks to their informed intuition, managers were able to track down and identify the problem: a group of recently hired agents were unfamiliar with certain features on a newly released device. Therein lies a teachable moment. Sprint was able to identify the agents who needed training at the precise moment when they really needed it. They were able to intervene with real-time training…

Data as Sixth Sense

The second idea proposes that "Data Can Be a Sixth Sense." By collating organizational insights using actual data, organizations can watch their blind spots and give their people enhanced decision-making ability. An example cited in this section is Google's "Did you mean…?" feature. In the authors' words:

> What you probably don't know is that it works entirely based on ambient data fed by Google users into a sophisticated, statistical, machine learning algorithm…

The Decoded Company: Know Your Talent Better Than You Know Your Customers
Authors: Leerom Segal, Aaron Goldstein, Jay Goldman, and Rahaf Harfoush
Publisher: Penguin Random House Company/ Portfolio
Publication Date: 2014
Length: 336 pages
Price: $27.95
ISBN: 978-1-59184-714-4
Source: *www.penguin.com*

> the algorithm looks for a repeated pattern of a search term entered followed very quickly by an almost identical term seconds later. That pattern indicates someone realized the mistake they made the first time and fixed it the second time, teaching the algorithm one way to misspell the correct term. With its steady diet of ambient data from hundreds of millions of users, Google was able to create a spelling correction system without teaching the system anything about spelling.

Engineered Ecosystems

The third idea is that "Engineered Ecosystems" that give employees flexibility and autonomy will prevail over hierarchies, reduce bureaucracy, increase transparency, and be wildly inspiring to teams. The premise is to deliberately engineer data-driven cultures guided by clearly outlined priorities and vision. An example cited here is from grocery chain Whole Foods:

> Whole Foods eschews traditional hierarchy in favor of an autonomous team approach. Each store is an autonomous profit center, broken down into an average of ten self-managed teams… each team operates autonomously, with its own performance metrics and an elected team leader… The company has engineered a program called gainsharing to reinforce the importance of the team as the central unit; it uses ambient data to measure productivity in the form of sales per hour each team is to make. This creates an easily measurable financial consequence to bad decision making.

Resources to Explore

The book wisely includes resources organizations can use to assess these ideas. Reading lists and recommendations are highlighted with one icon, and another icon indicates experiments to try.

In addition, an accompanying website, *decodedbook.com*, is full of further resources to explore.

The conclusions of chapters about the core ideas include a summary, a toolbox, experiments, and industry examples, among other things.

A Guide for Getting Started

The last chapter in the book, "Getting Started," is a step-by-step guide readers can use for decoding their own companies. The ideas within the book rely on processing data either through custom algorithms and surveys or by running ambient data through off-the-shelf software – some of which, coincidently, the author's company can supply. However, there are other things readers can investigate on their own.

For instance, one of the experiments at the end of the chapter "Data as A Sixth Sense" is called Project 360. It is a quick, cheap tool to implement with resources most companies already employ, like spreadsheets and surveys.

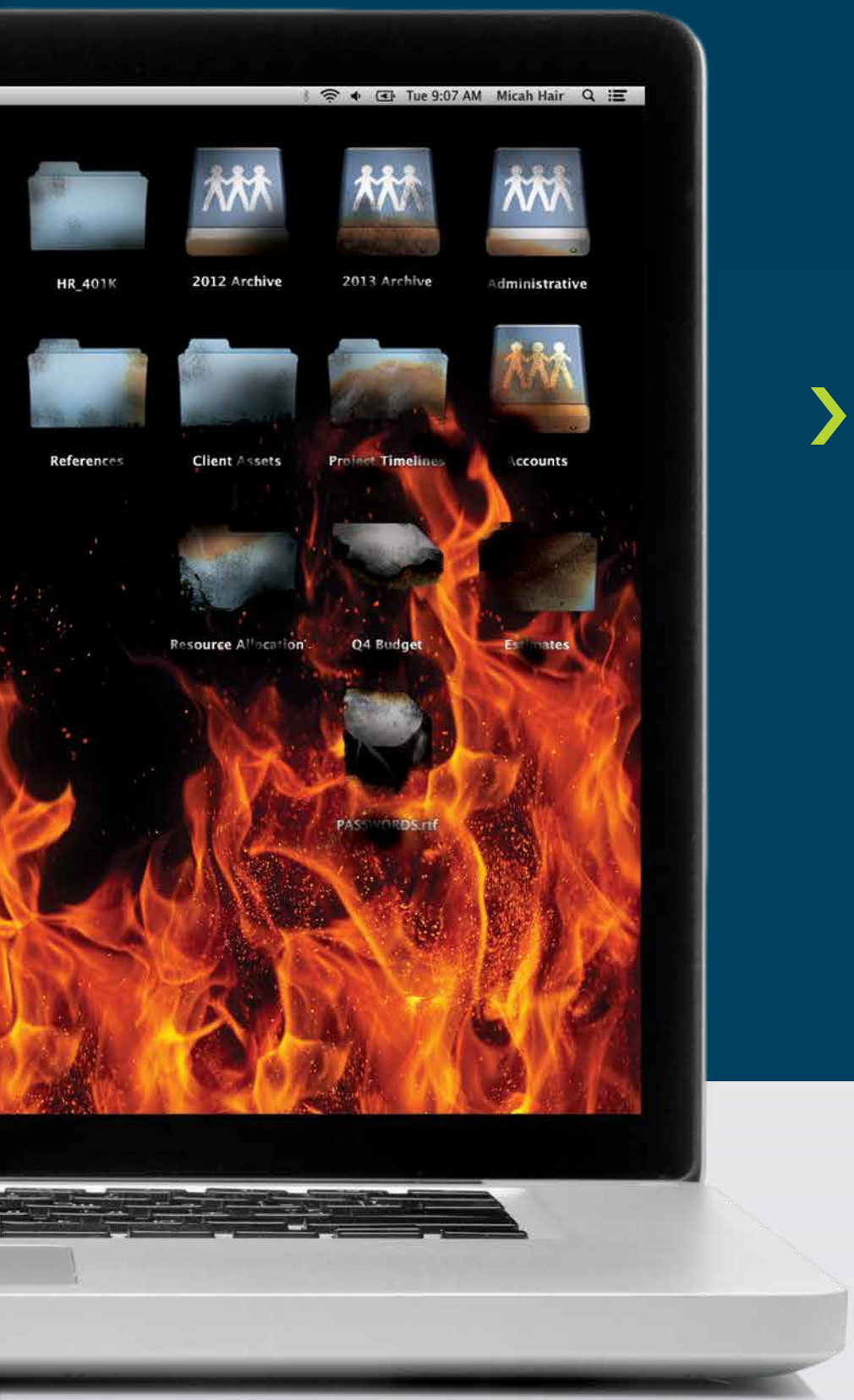
Old Idea with New Terms, Tools

The praise for the book, and the prose within, promotes decoding as the newest best thing. The authors call themselves quasi-evangelical about this "movement" of decoding the workplace. However, the idea of empowering people has been around in one form or another for a long time; the authors recycle this trend with updated tools and terminology. That's not to discount the philosophy; it seems worthwhile to try many of these ideas.

The drawback of a book like this is its general nature. It is not specifically records-related, although in a concession to the profession, the authors speak of transparency as the saving grace against a "big brother" reaction.

The Decoded Company is a constructive manual for understanding how empowering employees will evolve in the business world. All readers will be able to identify ways these processes can be put to use in their own organizations and can be adapted to policies and procedures already in place, moving their enterprises forward in the ever-changing business environment. **END**

Mary Broughall can be contacted at mbroughall@tristategt.org. *See her bio on page 47.*



Don't get burned by MISMANAGED INFORMATION.

NEXT™ LEVEL

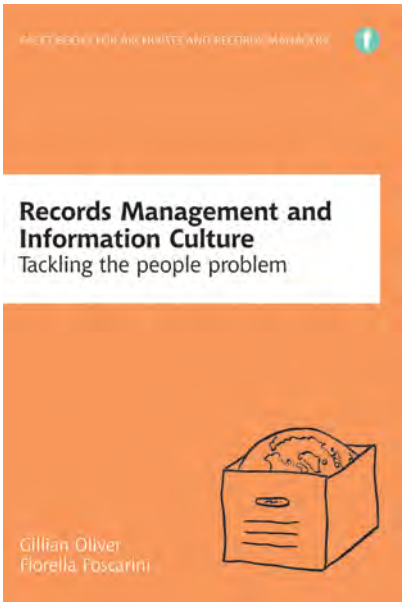
information governance assessment

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**.

Culture: The Key to Records Program Success

Meribeth Plenert



Records Management and Information Culture: Tackling the People Problem by Gillian Oliver and Fiorella Foscarini describes what information culture is, why it is important, how to analyze an organization's culture, and how to use the results of the analysis.

This book, which provides examples of information cultures from a variety of organizations around the world, could prove useful to others, but its heavy reliance on the reader to know information management theories makes it useful predominantly to trained information professionals.

Information Culture Framework

Although information professionals are charged with overall responsibility, employees have a role in the records management program's success through their records management practices. The authors use the Information Culture Framework to illustrate how employees' differing views of records can affect an organization's records management program.

The base of this pyramid-shaped graphic shows those areas the authors identify as ones records managers are required to know about – but cannot change. This includes the value employees give to records, their preferences when it comes to information, language requirements, and infrastructure.

The second layer of the pyramid encompasses employees' skills and knowledge, which records managers can change through training employees so they improve in and become accountable for their records practices.

The top layer of the pyramid represents IT governance and trust, which are the most influential for records management program success – and can easily change to the program's great detriment.

The information culture framework is a very useful tool, outlining small details in employees' lives that have huge effects on their information management practices. Drawing out sensitive topics, such as differences in language, information sharing outside social groups, and preferences for oral instead of written discussion, is important for those who are trying to manage change.

Providing a current example of each problem would have helpfully expanded each of these sections and heightened their importance better than does the authors referring readers to examples in other chapters.

Too Much vs. Too Little

A huge drawback of the book is its continual references to other parts of the book to remind the reader where topics have been or will be covered. Although specific references can be useful for a large volume or series of volumes, in such a slender book this becomes distracting, and it is made redundant by an exceptionally thorough index and detailed chapter titles.

Although the authors outline some basic methods for identifying various records problems within an information culture, they rely on the typical options of conducting an employee survey and watching employees work rather than provide new ideas.

The book also does not provide much guidance on how to delve into sensitive topics like discovering an employee's cultural background. Suggesting how to address survey questions to ascertain that information would have been more helpful than simply telling readers to consult their local human resources department.

Oliver and Foscarini tackled a very challenging problem in a way that will be valuable to trained records managers. Although they developed a useful framework for illustrating and ranking cultural problems according to their changeability, their book provides only limited help on identifying the problems; solutions will have to be found elsewhere. **END**

Records Management and Information Culture: Tackling the People Problem
Author: Gillian Oliver and Fiorella Foscarini
Publisher: Facet Publications
Publication Date: 2014
Length: 192 pages
Price: $95
ISBN: 978-1-85604-947-4
Source: *www.alastore.ala.org*

Meribeth Plenert can be contacted at mc.plenert@gmail.com. *See her bio on page 47.*

Privacy+ is an international certification program open to all companies providing outsourced storage and protection of hard-copy records and off-line removable computer media. Participation in Privacy+ is voluntary and allows companies to publicly demonstrate their commitment to protecting the privacy of information entrusted to them by their clients. Privacy+ certification is owned and administered by PRISM International (Professional Records & Information Services Management), the not-for-profit trade association for the commercial information management industry. Look for the Privacy+ logo, ask for it in your RFPs, and expect your records and information management partners to have it. For more information, please visit ***www.prismintl.org.***

Falcon™

OPEX

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

Recall Holdings Limited (ASX: REC), a global leader in document storage, digital document management, and data protection, announced its growth into new markets over the previous 12 months. Recall now services customers with records management needs in the following markets of San Diego CA, Ottawa QE, Kansas City KS, Cleveland OH, and Pittsburgh PA. This growth represents Recall's continuous efforts to provide service where our customers need us, adding innovative solutions that promote best practice, efficiency, and cost savings. ***www.recall.com***

recall™ Your Information. Securely Managed.

NAID®

NAID

The NAID 2015 Annual Conference and Expo will be held March 20-22, 2015, in Grapevine, Texas, just outside of Dallas. Sign up today at ***www.naidonline.org.***

FREE DEMO EVERY FRIDAY!

NEXT LEVEL is a software platform organizations can use to identify information-related compliance across the enterprise, drive improvements, and develop metrics for evaluating information governance (IG) program maturity. The assessment is based on the fundamental best practices of the Generally Accepted Recordkeeping Principles® and the Information Governance Maturity Model, whose concepts are widely acknowledged as critical to assessing information risk across an organization. In this 30-minute, live demo, you will learn how Next Level can help you identify key areas to proactively assess within your organization. Space is limited! Register at ***www.arma.org.***

NEXT LEVEL

ARMA INTERNATIONAL

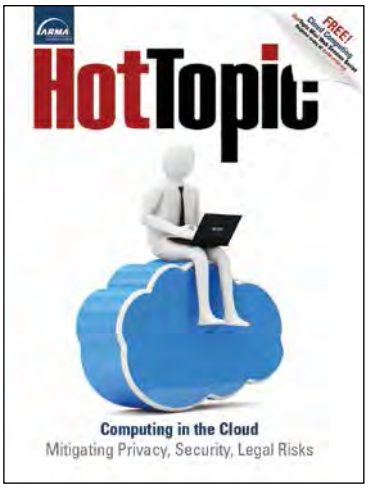
twice as hot

Double your professional development with ARMA International's

free mini web seminars

Our **hottopic series** is now available and includes three to five 20-minute web seminars brought to you by the industry's best and brightest. Sign up just once, and come back again and again to take advantage of this fantastic education.

www.arma.org/rl/professional-development



International Retention Requirements

These volumes survey and provide hyperlinks to national laws and regulations that specify retention requirements for commonly encountered records that are likely to be maintained in electronic form – corporate, accounting, tax, customs, legal, employment, workplace health and safety, intellectual property, and surveillance.

NEW!

Legal Requirements for Electronic Records Retention in Asia

William Saffady, Ph.D.

This volume includes Bangladesh, Brunei, Cambodia, China, Hong Kong, India, Indonesia, Japan, Macau, Malaysia, Mongolia, Pakistan, The Philippines, Singapore, South Korea, Sri Lanka, Taiwan, Thailand, and Vietnam.

Cat # V5021
PRO $295 **REG** $395

Legal Requirements for Electronic Records Retention in Western Europe

William Saffady, Ph.D.

This volume includes Austria, Belgium, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Liechtenstein, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, and United Kingdom.

Cat # V4980
PRO $295 **REG** $395

Legal Requirements for Electronic Records Retention in Eastern Europe

William Saffady, Ph.D.

This volume includes Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Estonia, Hungary, Latvia, Lithuani, Macedonia, Montenegro, Poland, Romania,Russian Federation. Serbia, Slovak Republic, Slovenia and Ukraine.

Cat #V5018
PRO $295 **REG** $395

Order online today! **ARMA INTERNATIONAL BOOKSTORE**


ALTEPETER


BAILEY


GABLE


GRYSIUK


PLENART

Designing a Records Audit: A Controls-Based Approach
Page 20

Andrew Altepeter is an information governance analyst at Motorola Solutions, Inc., where he is responsible for records management and IT audits for Sarbanes-Oxley and Payment Card Industry compliance He has previous experience in institutional archives and records management. Altepeter earned a bachelor of arts degree in history from Marquette University and a master of arts degree in public history from Loyola University Chicago. He can be contacted at *andrew.altepeter@gmail.com*.

The Cookie Trail: Why IG Pros Must Follow the Crumbs
Page 24

Mark Grysiuk, CIP, has been in information management for more than 12 years, working as a technical writer, documentation specialist, and records management practitioner in Toronto, Ontario, Canada. For the past eight years, he has provided leadership in building defensible disposition programs in both private and public sector organizations. Grysiuk can be contacted at *mgrysiuk@rogers.com*.

The Principles: Principles for Outsourcing Mission-Critical Business Processes Page 30

Julie Gable, CRM, CDIA, FAI, is the retired president and founder of Gable Consulting LLC, a firm that served clients' information governance needs for the past 25 years. The author of numerous articles on information-related topics, she has a master's degree in finance from St. Joseph's University and a bachelor's degree in management from Drexel University. Gable can be contacted at *juliegable@verizon.net*.

Checklists for Evaluating Electronic Records Storage Protection Page 34

The ARMA International Standards Development Program Workgroup for the technical report from which this article was excerpted, includes the members below. Employers listed are those that were on record with ARMA International at the time of publication in July 2014. The workgroup leader was Kim Mayberry, CRM, Turner Broadcasting System Inc. Workgroup members were: Darin Coté, CRM, National Archives and Records Administration; Ashleigh Faith, SAE International; Nicholas Fonseca, CIP, Alberta Motor Association; Mark Grysiuk, CIP; Shan Jin, CRM, CIP, Queen's University Archives; Zahn M. Krava, Vorys, Sater, Seymour & Pease LLP; Tera Ladner, J.D, IGP, CRM, SunTrust Banks Inc.; Dernea Michaux-Davis, CRM, CIPP/US, Kemper Corporation; Joao Penha-Lopes, Ph.D., CleverTime-Consulting LLC; Angel Ramos, CRM, Mylan Inc.; Douglas Schultz, CIP, Marathon Oil Corporation; Amelia Winstead, CRM, CA, Georgia-Pacific LLC; and Trudi Wright, District School Board of Niagara.

A Comprehensive Information Governance Resource
Page 40

Robert Bailey, Ph.D., CRM, is records program administrator and EMC project leader at McCarran International Airport in Las Vegas. Previously, he was records manager advisor in the Office of Chief Information Officer, St. Johns, Newfoundland and Labrador, Canada. He is an active consultant, speaker, and seminar leader at numerous national conventions. Bailey can be contacted at *Robertbail@mccarran.com*.

Following the Data Trail for Competitive Advantage
Page 41

Mary Broughall is a records specialist for Tri-State Generation & Transmission Association Inc. Previously, she did records and Freedom of Information Act work with the U.S. Department of Energy. She can be contacted at *mbroughall@tristategt.org*.

Culture: The Key to Records Program Successs
Page 44

Meribeth Plenert has been working in archives and records management for the past three years. She received her master's degree in archival studies from the University of British Columbia. Plenert can be contacted at *mc.plenert@gmail.com*.

AD INDEX CONTACT INFORMATION

5	**Fujitsu**	*ez.com/infomgmt*
9	**Institute of Certified Records Managers**	518.694.5362 – *www.ICRM.org*
FC, BC	**Iron Mountain**	800.899.4766 – *www.ironmountain.com/RMSeries*
3	**NAID**	*http://directory.naidonline.org*
13, 43	**Next Level**	*www.arma.org/nextlevel*
IFC	**OPEX Corp.**	856.727.1100 – *www.opex.com*
Insert	**PRISM**	*www.prismintl.com*
IBC	**Recall**	1.888.RECALL6 – *www.recall.com*

recall™

Information Management Simplified.

Recall Portal provides you with unprecedented visibility, access and control of your information. You can now manage your documents and digital information seamlessly and securely anywhere, anytime.

recall.com

To receive Recall Portal call

1.888.RECALL6 (732.2556) or visit us at www.recall.com

Inventory Governance Made Easier

The industry's first and only RFID-*ready* boxes set you up for your immediate or future auditing needs while protecting your information and staying green.

RFID-*READY*

PROVE COMPLIANCE WITH EASE

- Pre-applied RFID labels on most popular boxes
- Automatically set for auditing needs
- Faster location services

SECURE

PROTECT YOUR INFORMATION

- Built-in hole for zip ties
- Professional grade
- Durable in long-term storage
- pH buffered paper for preservation

GREEN

GO GREEN

- Made with 65% recycled material
- 100% recyclable
- Constructed with virgin and recycled materials

BUILT-IN HOLE FOR ZIP TIE

- Added level of security
- Zip ties sold separately

PROTECTIVE LID

- Additional durability during transportation and storage
- Won't warp or blow off

PRE-APPLIED RFID LABEL

- Easier path to inventory audit with no line of sight required
- All-in-one RFID chip and barcode label
- RFID label is open sourced and can be read at your location with an RFID reader
- RFID labels also sold separately for non-RFID-*ready* box types

Now available via Iron Mountain Connect™ or at 800 899 IRON (4766)

IRON MOUNTAIN®