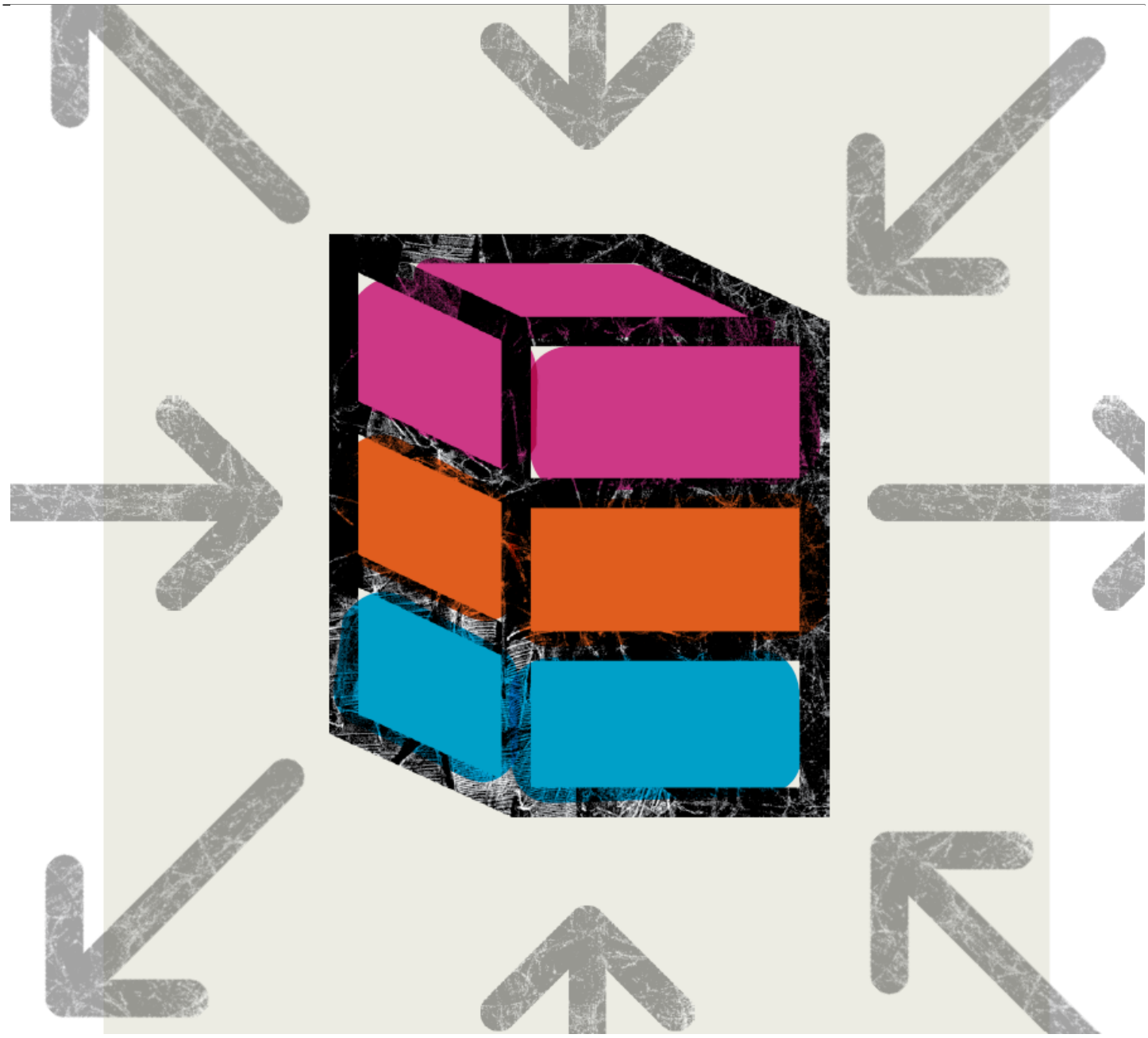
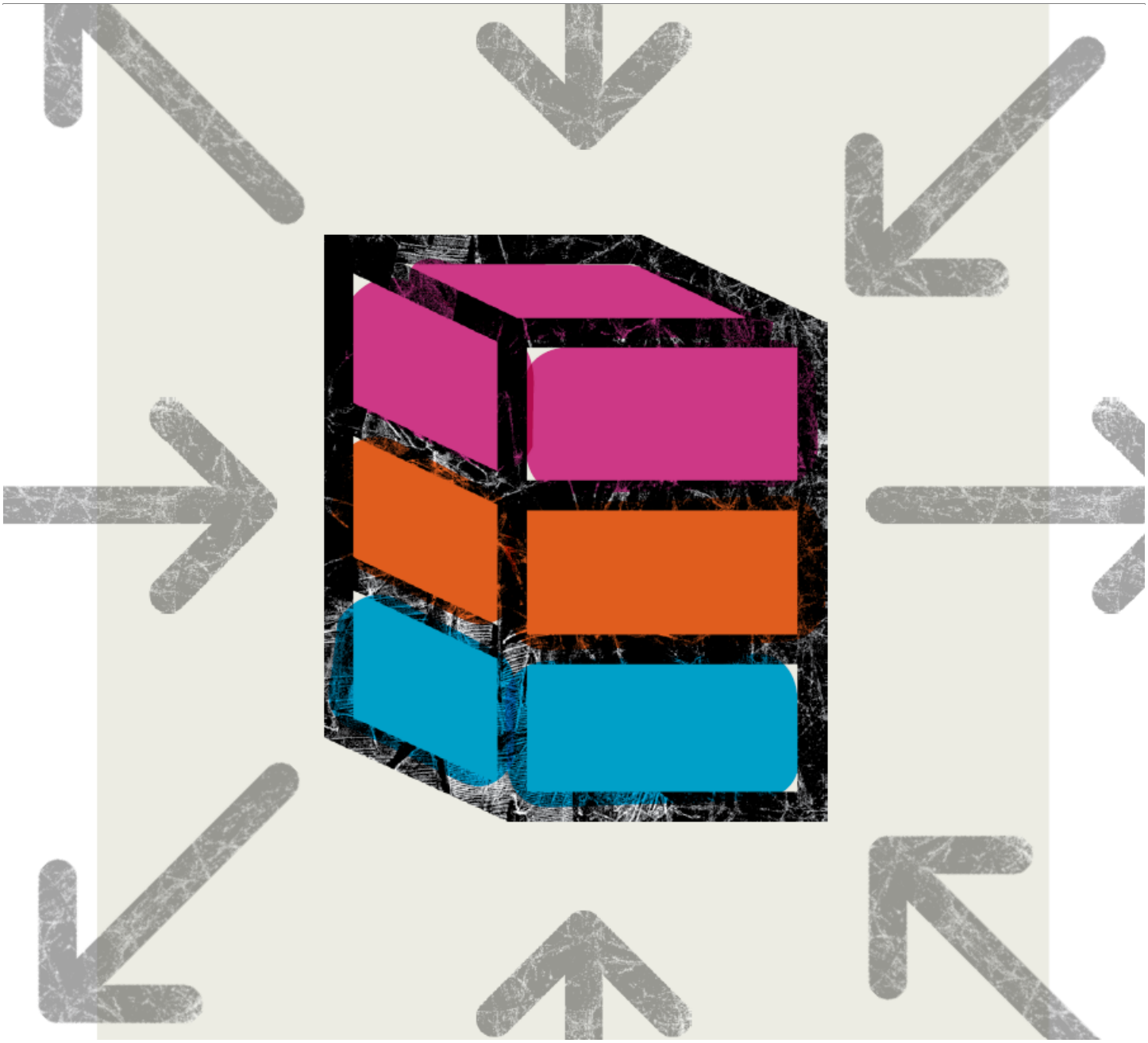


Save Smart: Records Management in the Digital Age

Technology, Privacy, and eCommerce





CHEAT SHEET

- ***Too much of a good thing.*** Experts predict a 4,300 percent increase in annual data production by 2020, but companies use only a fraction of the data they collect and store.
- ***Take inventory.*** Organizations need to identify and target data that is no longer useful or valuable, and that creates risks and costs by being stored.
- ***Resources.*** Provide significant training resources to ensure that there is across-the-board implementation and accountability.
- ***End goal.*** The goal should be to retain records needed to conduct business and meet legal requirements, and destroy all other records under a formal records retention policy.

In this ever-growing digital economy accompanied by escalating cyber risks, a company's need to properly manage and protect its universe of documents, data, and records has never been more imperative. As data grows at exponential rates and cyberattacks increase in frequency and severity, a comprehensive records management approach forms the very cornerstone of sound governance and organizational risk management. For organizations operating on a global basis, records retention for its overseas business is just as important as it is for its domestic operations.

Implementing an effective, company-wide records management policy is challenging and resource intensive. However, the benefits that an organization derives by expending the necessary effort in launching such an initiative are well worth the investment. Conversely, an organization that fails to develop and implement a records management policy to control the rising volume of data it amasses will undoubtedly face increasing burdens: difficulty in managing its information assets; inefficiencies in accessing needed information; and heightened business and legal risks in conducting daily operations.

Clear "wins"

There are some clear "wins" an organization realizes by instituting a records management policy including:

- Enables compliance: promotes compliance with pertinent legal and regulatory mandates by having clear records retention practices;
- Protects sensitive information: fosters a culture and understanding of what must be protected, such as personally identifiable information, trade secrets, and other types of confidential and proprietary information;
- Reduces storage and operational costs: avoids expenditures on unnecessary data and paper storage;
- Manages information growth: provides an approach for managing the explosive growth of information;
- Streamlines document requests: lessens burden of document production as part of the electronic discovery process[1] and reduces the risk of spoliation by adopting a consistent policy-driven approach to records management;[2]
- Meets expectations: aligns with expectations of clients, outside auditors, and third-party certification authorities; and,
- Mitigates risk: reduces the likelihood of unauthorized destruction of business records, data misappropriation, and other breaches.

1 The Policy, however, must be clear that all disposal and destruction practices are suspended for those records and emails subject to a litigation hold pursuant to a company's eDiscovery obligations. See T*he Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age*, available here.

2 See Arthur Andersen LLP v. United States, 544 U.S. 696 (2005); In re Prudential Ins. Co. of America sales Practices Litigation, 169 F.R.D. 598, 615, 36 Fed. R. Serv. 3d 767 (D.N.J. 1997).

Harnessing the data explosion

With the ever-rising tide of data being generated, organizations need to identify and target data that

no longer has value or that has outlived its usefulness, and the very fact that it is still being stored and maintained could present its own risks and costs to the organization.[3]

It's not just the sheer mass of information that is posing challenges to organizations, but also the changes taking place in the type of data being created and how organizations account for them. "More than 90 percent of new records being created are of the unstructured variety, coming from such sources as social media and email."[4] This data needs to be managed and accounted for according to sound and consistent records management practices.

The problem is compounded when predicted data growth is taken into account: Experts are predicting a 4,300 percent increase in annual data production by 2020.[5] But companies use only a fraction of the data they collect and store.[6] This will cause a flood of information to pile onto the data companies are already struggling to properly manage.[7] The message is clear: retaining all data does not make good business sense.[8]

The exponential increase in data creation also leaves companies vulnerable to spoliation of evidence, which carries great risks and penalties, including reputational, civil, and even criminal.[9] With so much at stake, it is critical that any implemented records management policy not only meet customer expectations and maintain organization-wide standardization, but also comply with all applicable jurisdictional regulations.

3, 4 The estimate of how much redundant, obsolete and trivial content is clogging up enterprise storage systems varies from 30 percent to 75 percent. AIIM 2014 www.aiim.org / Iron Mountain 2014, www.ironmountain.com.

5, 6, 7 Big Data Overload: Why Most Companies Can't Deal with the Data Explosion. April 28, 2016. Forbes. Marr, Bernard.

8, 9 "Hoarders Beware: Defensible Data Disposal is Good Business". May 2013. *ACC Docket*. Williams, Pamela & John Martin.

Combating cyber risks

The likelihood that an organization will suffer a data breach varies with its size. In 2016, "[w]hile fifty-one percent of organizations with 1,000 employees or less reported a breach, eighty-one percent of those with 100,000 or more employees had been breached."[10] The reported likelihood of having a breach also varied by organization type and industry. Only 41 percent of for profit, privately held companies reported a breach in the last year, whereas 65 percent of public companies and 68 percent of governmental institutions reported a breach.[11]

Moreover, the scale and sophistication of cyberattacks is also increasing, which includes phishing, ransomware, and a variety of security-related cyberattacks.[12] Regardless of the industry, all organizations are at risk.

10, 11 Data Breach Incidents, Causes, and Response. November 2016. Society of Corporate Compliance and Ethics and the Health Care Compliance Association.

12 www.fbi.gov/investigate/cyber.

Regulatory developments and international standards in data retention

Evolving regulatory requirements are imposing prescribed record retention policies, and overall cybersecurity safeguards for an organization vary by jurisdiction.

For instance, in April 2016, the European Union Parliament approved the EU General Data Protection Regulation (GDPR), which took effect on May 25, 2018, and applies to all companies that conduct business in the European Union.[13] GDPR, designed to harmonize data privacy laws across Europe, replaces the Data Protection Directive 95/46/EC and mandates that organizations cannot retain personal data longer than necessary.[14] Accordingly, organizations should treat the implementation of GDPR as an opportunity to revise and update their retention periods for certain types of personal data.

The Office of the Privacy Commission of Canada recommended that companies establish and implement their own records retention policies, including maximum and minimum retention periods, and retain personal information only for as long as needed to fulfill the business purpose, unless the data subject consents to a longer retention period or if required by law.[15]

On March 1, 2017, the New York State Department of Financial Services (DFS) promulgated cybersecurity requirements.[16] These requirements apply to all “covered entities,” companies, or persons authorized to operate under the Banking Law, the Insurance Law, or the Financial Services Law. All covered entities must adopt a cybersecurity program with minimum standards to ensure the safety, soundness, confidentiality, and integrity of the entity’s information systems and to protect customer’s private information.

Further, under New York’s new regulations, each covered entity must have policies or procedures on the timely destruction of non-public information when it is no longer necessary for business purposes, except where the information must be retained pursuant to law or regulation.[17] Moreover, covered entities must maintain certain records as required by DFS’ new cybersecurity regulations, including audit trails designed to detect and respond to cyber events, for a prescribed retention period.[18]

A recent Australian Encryption Trends Study[19] found the key barrier to encryption for 55 percent of Australian organizations is locating where data resides. It’s particularly problematic for companies that had not spent the time doing inventory and prioritizing their data, leaving critical vulnerabilities in the business. To address these weaknesses, a comprehensive records management approach would require a proper inventory and prioritization of company records and related information.

The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies. The work of preparing international standards is carried out through ISO technical committees, which include governmental and non-governmental participation. ISO 15489-1:2016 defines the principles for the creation, capture, and management of records relating to:

- Records, metadata for records, and records systems;
- Policies, assigned responsibilities, monitoring, and training supporting the effective management of records;
- The current analysis of business context and the identification of records requirements;
- Records controls; and,
- Processes for creating, capturing, and managing records.

In sum, ISO 15489-1:2016 creates international standards that apply to the creation, capture, and management of records, regardless of structure or form, in all types of business environments.

13 Regulation (EU) 2016/679 of the European Parliament and of the Council. Chapter 2. Article 5 (e). 26 April 2016.

14 *Id*. at Chapter 2, Article 5(e).

15 PIPEDA Report of Findings No. 2014-019, Re Office of the Privacy Commissioner of Canada.

16 New York State Department of Financial Services 23 NYCRR 500. Cybersecurity Requirements for Financial Services Companies.

17 *Id*. at 23 NYCRR 500.13. *Nonpublic Information* means all electronic information that is not Publicly Available Information and is: (1) Business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations, or security of the Covered Entity; (2) Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code, or password that would permit access to an individual's financial account, or (v) biometric records; (3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present, or future physical, mental, or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.

18 *Id*. at 23 NYCRR 500.06(b).

19 https://gets.thalesesecurity.com.au/.

Necessary steps to implement a records management policy

How do you create and implement an effective and successful records management policy in view of regulations that vary based on jurisdiction?

There are some basic records retention policy guidelines that will form the baseline for compliance with applicable laws and regulations:

1. Clearly define "record" in the policy (as distinguished from nonrecords): typically characterized as documents with business value and/or that must be retained for legal and regulatory requirements for a prescribed period.
2. Create a records inventory: a complete listing of locations and contents of company records that extends across business units and corporate information systems.
3. Devise a records retention schedule: retention periods by record type and discipline/department based on business needs and legal requirements.
4. Establish disposal practices: determine appropriate method of disposal by record classification or media type (in consultation with information technology personnel) and institute a consistent and secure system for disposal of records in accordance with the

records retention schedule.

5. Designate a records management team: identify company representatives responsible for enforcing the policy in their area or discipline (e.g., HR, finance, sales, etc.).
6. Address email: several options exist, including specific retention periods for emails in employee inboxes, a cap on the size of each employee's mailbox, creation of local shared folders for archival storage of critical emails, or unlimited email server storage (each option is dependent on cost, compliance issues, and the needs of the business).[20]
7. Ensure eDiscovery obligations are met by working with your information technology staff, make sure that retention/destruction periods do not apply and are suspended for any records or responsive documents subject to a litigation hold until such time that the underlying suit or matter is resolved and the hold is lifted by the legal department.
8. Create organization-wide accountability to achieve compliance with the policy, which should be integrated into your internal audit and business unit compliance process.

To be successful and set the appropriate direction, you will also need the support of your organization's executive management team, and you will also need to partner and collaborate with your IT department in the planning and execution of an effective records management policy.

As with any other compliance program, you will need to provide significant training resources, both online and in-person trainings, to ensure that there is across-the-board implementation and accountability.

The goal should be to retain those records needed to conduct your business, meet your legal requirements (including e-discovery obligations), and destroy all other records under a formal records retention policy.

20 The decision on retention periods for emails is also dependent on whether an email constitutes a "record" under a company's policy. Some emails may qualify as "records" dependent on content and the nature of the business. Whether any emails may be considered "records" should be clearly delineated in the records management policy.

In closing

An effective, organization-wide records management policy is essential for controlling data growth and mitigating the growing threat of cyber risks. It reduces risk and promotes compliance with legal and regulatory mandates, as well as addressing client and consumer expectations that their sensitive information is secure. A sound records management approach:

- Provides an effective means to manage and contain the proliferation of records and data;
- Addresses both the business and legal risk of data over-retention;
- Reduces risk and scope of unauthorized access or data breach; and,
- Presents viable means to mitigate the threat of cyber-attacks.

While leveraging big data and using predictive analytics has become mission-critical for companies to remain competitive, and as data continues to grow at its current exponential rate, behavior needs to change from "save everything" to "save smart." A comprehensive enterprise-wide records management policy will assist organizations in striking the delicate balance between the strengths and vulnerabilities that data presents in this complex and evolving area.

The author also acknowledges the valuable contribution of Quinterrion Waits, a law student at the

Roger Williams University School of Law, for help researching this article. The views and opinions expressed in this article are those of the author and do not necessarily reflect the policies or positions of FM Global.

Jonathan I. Mishara



Senior Vice President, General Counsel, and Secretary

FM Global

FM Global is a commercial property insurer headquartered in Johnston, Rhode Island.