Deloitte.

Records and information management comes full circle

Potential records management risks attract C-suite attention—again

Issue snapshot

Records and information management (RIM) became an imperative for businesses in the early 2000s in the wake of the Sarbanes-Oxley (SOX) Act. Heavy investments in RIM personnel, technology, processes, and governance were not uncommon to support compliance with SOX record retention requirements. However, the investments were often proportionally applied to areas of perceived external risk and not necessarily to broad-based, enterprise-wide programs.

The 2008 recession impacted these efforts as businesses scrambled to cut costs and survive the economic downturn. Many companies decentralized their RIM organizations and governance. RIM personnel were reassigned or let go, technology solutions and processes were relegated to lines of business, and control over RIM was diluted.

Today, new forces are elevating RIM back to the level of C-suite imperative:

- Emergence of strict security and privacy regulations in many countries (see "The expanding regulatory net")
- Continued expansion of businesses and e-commerce across international borders, adding to the complexity of RIM
- The exponential growth of enterprise data and challenges associated with managing both the data volumes and emerging information formats
- Re-energization of the M&A market in certain industries with related due diligence and regulatory compliance requirements
- The increasing discovery demands of litigation and regulatory investigations, including scope of discovery, deadline pressures, and high costs
- Expanding passage of anti-tax avoidance laws around the world and sharing of corporate information between countries' tax authorities

Decentralized and outdated RIM operations have largely been inadequate, often resulting in incomplete and inconsistent compliance with RIM policies. Fully centralized models haven't fared much better, often suffering from high costs and struggles with transparency across the enterprise.

Moreover, in the face of new and dynamic requirements, organizations are forming new functions and sub-functions outside of RIM that may take over operations normally administered by RIM. These functions may emerge in the areas of compliance, privacy, tax, IT, digital, or innovation—often supported by businesses that desperately need RIM governance to keep pace with their business demands and regulatory scrutiny. While this may meet organizational needs in the

Expanding regulatory net

Around the world, regulations are being imposed on companies to enforce record retention, promote data protection, and compel transparency when needed. Following are several of the most prominent developments:

US-EU Privacy Shield—"frameworks designed by the US Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce."[1]

EU General Data Protection Regulation—"designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy, and to reshape the way organizations across the region approach data privacy."[2]

Japan's amended Act on the Protection of Personal Information—Japan formed a Personal Information Protection Commission in January 2016 to enforce significant amendments to the original 2003 Act, which went into full effect on May 3, 2017.[3]

China's complex environment—China has either proposed or enacted numerous laws and regulations defining personal information and enforcing data privacy, including most recently the Cybersecurity Law (2017)[4] and related regulations.[5] The net effect is to create a labyrinth of rules to which companies with operations in China—and some that don't have a physical presence there—could be subject.

South Korea's Personal Information Protection Act—passed in late 2011, it has been amended in recent years along with stricter penalties for data protection or privacy violations.[6]

Russia's Federal Law on Personal Data—originally implemented in 2006, this law has been amended and updated several times in the years since, and other regulations have been passed to strengthen its provisions and introduce stricter penalties for noncompliance.[7]

BEPS-inspired tax laws—The Organisation for Economic Co-operation and Development's (OECD) Base Erosion and Profit Shifting (BEPS) initiative has inspired tax law changes in countries around the world, including increasing requirements for companies to provide visibility into financial, sales, supply chain, and other operational data and records for tax compliance purposes. (http://www.oecd.org/ctp/beps-actions.htm)

near term, such a model can also contribute to multiple, redundant information silos and inefficient information management.

Taking a step back, it's clear that there should be a function responsible for understanding and administering data in a compliant and consistent way across the enterprise, and that such administration could efficiently and actively fuel cost reduction, support business process improvement, and innovation. RIM, at least by definition, seems a function well-positioned to address this need. But historical models might not be relevant in the current information environment. Clearly, more linkages are required of a RIM program than ever before given technology, regulatory requirements, and geographic challenges.

What's an answer? What do you want your RIM program to be? In this paper, we discuss three opening issues:

- Defining a RIM program
- Determining a RIM operating model
- Deciding where the RIM program should reside in the organization

Then we describe a hybrid, federated model that can be considered to encourage RIM standardization across an enterprise, as well as optimization of processes to promote consistency and quality of RIM service delivery.

[1] https://www.privacyshield.gov/welcome

[2] https://www.eugdpr.org/

[3] https://www.ppc.go.jp/en/

[4] https://privacylaw.proskauer.com/2017/05/articles/international/a-primer-on-chinas-new-cybersecurity-law-privacy-cross-border-transfer-requirements-and-data-localization/

[5] https://www.huntonprivacyblog.com/2018/07/17/china-publishes-draft-regulations-classified-protection-cybersecurity/#more-16650

[6] https://datamatters.sidley.com/south-korea-enacts-stricter-penalties-for-data-protection-violations-by-telecommunications-and-online-services-providers/

[7] https://www.hldataprotection.com/2017/02/articles/international-eu-privacy/russia-increases-fines-for-violations-of-data-protection-laws/

Defining a RIM program

A key element of a sustainable enterprise RIM program is a well-defined governance structure that includes at least four functional components: policies and procedures, operations and delivery, oversight and reporting, and stakeholder engagement (Figure 1). Strong support from a company's C-suite and line-of-business (LOB) executives for these functional areas is an imperative for effective program design, implementation, and ongoing operation.

Policies and procedures. An organization needs guidance to understand how to create, maintain, and dispose of records. The tools generally used to establish this guidance are policies, such as a RIM policy and retention schedules, which include defining record types and associated required maintenance periods (sometimes including how records should be maintained) and procedures—the specifics of what end users should do to comply. The scope of policy typically extends beyond formal records and into more general information management (e.g., active business and transient data). Important issues associated with policies and procedures include:

- *The external and internal environments are dynamic.* The external regulatory environment has changed, and many new regulations have been implemented globally. New internal systems and technologies have emerged, while others have been de-commissioned. These changes can be disruptive, so policies and procedures need to be maintained and updated.
- *There is often overlap* between a company's RIM policy and other organization policies and procedures. For instance, privacy and information security often operate on the same records and information stores. Organizations may align these under a global information management policy umbrella or maintain such policies somewhat autonomously. Either way, policies help to avoid confusion and potentially reduce inadvertent business risk.

Figure 1. RIM program governance structure

Simply stated, building and maintaining policies and procedures is not a trivial matter. Effective maintenance requires linkages with the external regulatory environment and internal organizational environments. Moreover, maintaining such linkages requires resources. Often, managing this network with appropriate visibility can provide an effective balance of consistency and efficiency.

Oversight and reporting. Generally, RIM is an enterprise function. For the RIM program to be able to gather information and report on how RIM is operating, the RIM program should partner with other parts of the organization, such as LOBs and other functions, depending on the organization's structure. These linkages with other parts of the business can relate to compliance (Are we following the rules? How are we doing?) or understanding change (Are there new requirements or new systems?). Properly structured, the RIM program can provide a specialized view of the enterprise to help organize and identify both opportunities and risks. Important issues include:

- *What does oversight mean?* The range of scope can extend from policy publishing and maintenance to organization information inventory management. Most organizations choose to walk before they run, but well-organized RIM programs can potentially generate millions of dollars in savings, so fundamental scope issues are important to success.
- *Who to report to?* A later section of this paper discusses different operating models, steering committees, and ways to organize and manage to the organization.
- *Frequency and type of reports.* RIM is a business-as-usual function, and business-as-usual reporting is often associated with monthly, quarterly, or other periodic reporting cycles. However, RIM has a role to play in the context of M&A and divestiture or with investigations and litigation. While such events can be disruptive from a flow of work perspective, they also provide the opportunity for the RIM program to clearly demonstrate its value and to help avoid unnecessary costs to the event. The ability to provide relevant, ad-hoc reports—especially on inventory and practices—becomes a strategic and tactical accelerator for the M&A teams and attorney teams responsible for managing the event.
- *External reporting.* Depending on industry or sector, organizations sometimes have a compliance responsibility to report on a period or an ad-hoc basis (for example, response to audit). Such requirements help to determine who in the organization are the stakeholders and should have steering committee or other involvement.

Operations and delivery. Depending on the organization, the RIM program may be responsible for delivering technology capabilities, training, or advisory roles. From this perspective, LOBs and other functions are clients of the RIM program. Or, the RIM program may serve a compliance and enforcement function. Key issues associated with operations include:

- *Resource scarcity.* Supporting activities require resources, and many RIM programs are not sufficiently staffed to achieve program objectives.
- *RIM team composition.* In addition to sourcing centralized functions in management, physical records, and technology, organizations sometimes deploy networks of stakeholders across the organization and in different geographies, sometimes referred to as RIM coordinators or liaisons. These resources often have a part-time responsibility to support the RIM program. While such networks provide some level of visibility and organizational "touch," they can also be difficult to set up and maintain.

Stakeholder engagement. Stakeholders across the enterprise can be diverse. The RIM program needs to manage across the stakeholder set. Specific stakeholders may include:

- Leadership often in the form of a steering committee
- Adjacent enterprise functions such as legal, compliance, information security, and others
- LOB stakeholders who serve both as a client and a conduit for education and enforcement
- Employees who need to understand and implement against procedures and policy.

The well-structured program provides opportunities for stakeholders at all levels to offer input to the program and measure satisfaction on a recurring basis.

Determining an appropriate operating model

A well-defined, industry-leading operating model can help drive benefits of effective RIM out into the business. Three common models allocate responsibilities differently for the four RIM functional areas described previously (Figure 2).

The distributed model is often employed in organizations that emphasize LOB autonomy. Corporate establishes the RIM policies, while the other functions are performed at the LOB level.

Deploying a distributed model overtly drives costs out of the RIM cost center. However, just because the costs are pushed out doesn't mean that they are not realized elsewhere in the organization in different cost centers or through inefficiencies. Moreover, LOBs often treat RIM as a secondary priority to conducting business, except in cases where the LOB has strict external compliance reporting requirements. From this perspective, many distributed RIM operating models result in untended RIM practices and poor records and information maintenance. Of course, where there is waste there is often opportunity for tangible improvement.

In **the shared services model**, a central RIM organization enforces compliance and program consistency to pursue cost efficiencies, while corporate drives overall records management, including providing supporting resources.

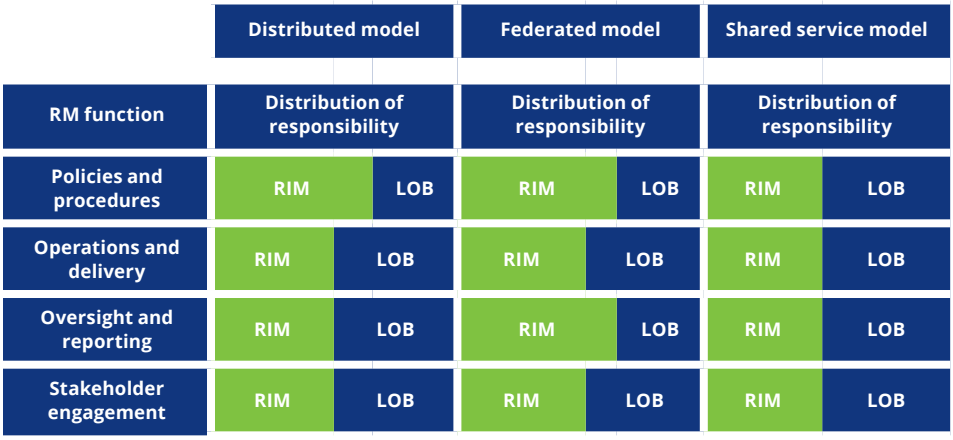
A centralized organization is often better resourced to provide visibility into practices and to sustain RIM efforts. However, cost is a high-profile issue for centralized records groups and such organizations need to pick and choose their places wisely. Thus, scope of the program is often limited to that which the RIM program effectively supports with its resource base. Moreover, the resource base needs to be trained to evolve with technology and advancements. Generally, centralized RIM programs erode in influence and scope of management.

What's managed is often managed well, but the RIM program may not be able to influence or address new and emerging opportunities, requirements, or activities that the business needs.

The federated model, which represents a hybrid of the distributed and shared services models, features a core organization—essentially a RIM center of excellence—that offers on-demand expertise and resources to the LOBs and measures overall RIM program compliance and performance. The LOBs provide operational capabilities and retain business decision making authority.

What can make the federated model effective is the application of process and technology to labor-intensive parts of the RIM process. For instance, LOBs may create massive amounts of data that is uncontrolled and unclassified relative to policy. Understanding this inventory, whether it is physical records, file server, or file-sharing applications, can be cost-prohibitive. By providing the tools to a LOB that help it organize its content on creation in a framework that is consistent with RIM program policy, the federated RIM program can be much more directed and effective in teaming with the business to comply with RIM and realize financial and strategic value. Yes, the LOB is still undertaking the effort, but the effort is integrated to the RIM purpose. In-place and emerging technologies, coupled with a trend toward information centralization via cloud and other channels, make such a strategy approachable.

Figure 2. RIM operating models



Deciding where the RIM program should reside

Organizational dynamics play a vital role in governing and operationalizing a RIM program. In addition to hierarchy and relative influence of different functions, the ability for RIM to have an interconnectedness with the enterprise is vital to its success. For that reason, where the RIM program is placed is often organization-specific. Four common functional areas that often "house" the RIM program (Figure 3) are discussed here, each having advantages and disadvantages.

Legal and compliance function. When a RIM program reports to the legal and compliance function, the focus is typically on operational oversight and regulatory and legal compliance. This approach gives RIM resources direct access to oversight functions provided by each LOB's compliance officer. However, this may result in "the business" viewing RIM as a "compliance issue" rather than a business imperative.

Risk management function. Reporting to the organization responsible for corporate risk and security can create a natural alignment between the RIM program and other risk-related activities at the corporate level. However, some organizations may find this approach difficult to deploy if their risk management resources are spread across multiple organizations within the corporate structure.

LOB operations. When a RIM program reports to the LOBs, with strong influence by the business, program leaders can benefit from direct access to the business and insights into compliance challenges there. Often found in organizations where records management grew out of a paper records function, this approach can be hampered by decisions that favor business operational needs over compliance.

IT function. Reporting to an IT department whose focus is on digital technology capabilities and cost containment, a RIM program may benefit by having a seat at the table when systems are configured and their records management capabilities are enabled. However, this approach may create a disconnect between the RIM program and the corporate risk and compliance functions.

Structuring an effective RIM organization

Whichever RIM operating model a company chooses, and whatever corporate function it is slated to report to, it is important to create a RIM team structure that can deliver leading practice RIM capabilities across the enterprise, including planning, quality, and support (Figure 4).

Key roles in such an organization are at executive, management, and operations levels:

Executive—an enterprise risk committee can help clarify and provide strategic direction for the RIM program, while leaders from corporate IT, each LOB, and the RIM program sponsor take responsibility for gaining buy-in for the RIM policies from key functional stakeholders. Those leaders also contribute to the day-to-day strategic direction for the RIM program provided by the enterprise risk committee.

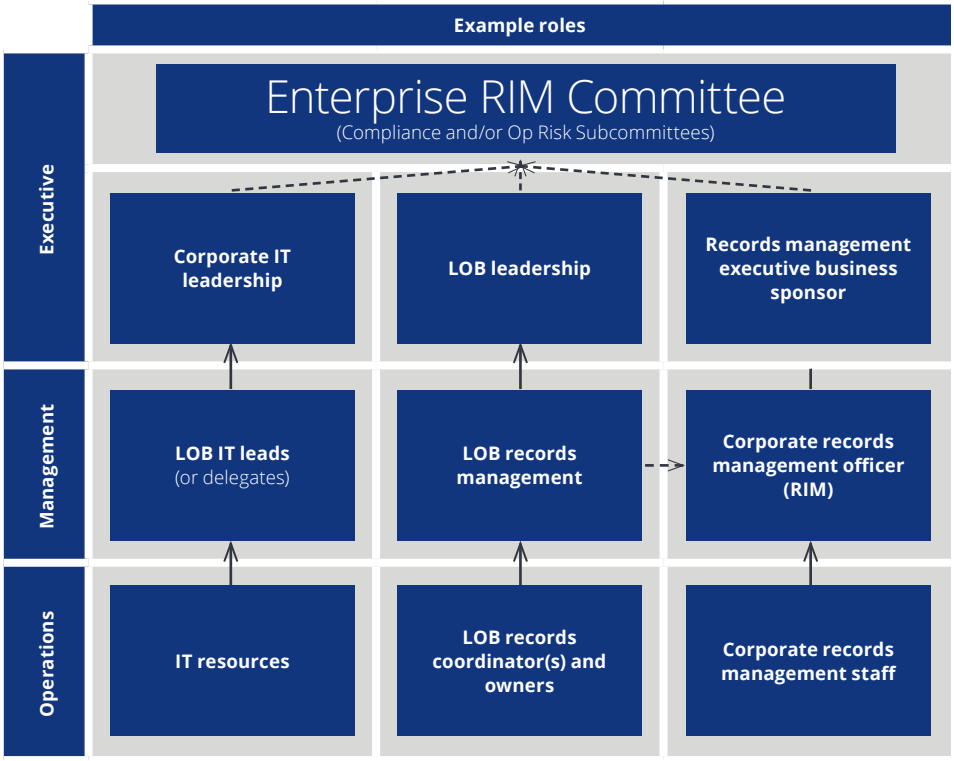
Management—LOB IT representatives or delegates, along with the LOB RIM program lead and a corporate RIM program officer, can be given responsibility for managing the activities of the RIM staff and corresponding LOB teams. This management team also works with the executive team to monitor RIM user acceptance and provides appropriate reporting on LOB team activities and metrics.

Operations—comprising IT resources, LOB records coordinators and owners, and the members of the corporate records management staff, this group is responsible for day-to-day records management, implementing and maintaining records management solutions, and assuring program security, authenticity, and safety, along with availability of the records.

With RIM demands growing, it's time to act

Many multinational organizations have a global RIM program, even one as barebones as a policy, a retention schedule, limited in-house counsel time, and outside counsel responsible to update the policy at intervals. Often, such programs focus on mission-critical records maintenance,

Figure 4. Illustrative example of a RIM organization



especially in companies and industries subject to a direct reporting requirement to a government or other external agency. Records management activities not deemed mission-critical often receive less attention and support, and may not be performed on par with established the global RIM policy.

Companies with an inadequate RIM program may face several risks, including:

Too much data. Often, more data is retained than necessary because records managers may not be enforcing records maintenance principles with the business and stakeholders. Not only can this create unnecessary day-to-day storage costs, but in the case of litigation or regulatory investigation too much data can cause delays in responding to discovery requirements, create a nightmare scenario for legal personnel tasked with discovery, and result in significant costs.

Retrieval challenges. Without a consistently defined RIM process, standard retrieval tools may not be used, making it difficult to find and retrieve relevant records in a cost-effective manner.

Non-compliant data disposition. Often, data and other records are disposed of without consideration of potential consequences, sometimes as a way to avoid maintenance costs. This can present create legal or regulatory exposure and the potential for significant fines and other penalties.

In the absence of a broad-based RIM program, these risks can materialize very quickly today. An important question for senior executives of multinational businesses is what level of investment might produce an effective RIM program that aligns with corporate objectives and risk appetite? Whether a centralized, decentralized, or hybrid federated model, an effective RIM program can support transparency and visibility that are vital in a world that increasingly values data protection, privacy, and security.

Contacts:

Jack Walker
Principal
Deloitte Discovery
Deloitte Transactions and Business Analytics LLP
+1 312 486 3149
johnwalker@deloitte.com

Paul Yackinous
Senior Manager
Deloitte Risk and Financial Advisory
Deloitte Transactions and Business Analytics LLP
+1 212 313 2931
pyackinous@deloitte.com

Deloitte.