IRON MOUNTAIN®

THE 12 RESPONSIBILITIES OF INFORMATION GOVERNANCE

5-MINUTE READ

THE 12 RESPONSIBILITIES OF INFORMATION GOVERNANCE

INFORMATION TOUCHES EVERY PART OF YOUR BUSINESS. RESPONSIBILITY FOR ITS GOVERNANCE BELONGS TO DEPARTMENTS AND LEADERS FROM A WIDE RANGE OF DISCIPLINES AND DEPARTMENTS.

1. LEGAL

2. DISCOVERY

3. RISK

4. COMPLIANCE

5. RECORDS AND INFORMATION MANAGEMENT

6. DATA OFFICE OR DATA GOVERNANCE

7. INFORMATION TECHNOLOGY

8. INFORMATION PRIVACY

9. INFORMATION SECURITY

10. INFORMATION ARCHITECTURE

11. BUSINESS
(LINES OF BUSINESS, BUSINESS UNITS AND/OR DEPARTMENTS)

12. INTERNATIONAL REPRESENTATION

1. LEGAL

- Determines the risk profile of an organisation based on litigation exposures, international privacy requirements, intellectual property protection, working environment and more.
- Develops and approves your organisation's Records Retention Schedule and Records and Information Management policy.
- Designates privacy classifications.
- Develops rules for management of email, social media, mobile, electronic and networking devices.
- Communicates organisational change through mergers, acquisitions and divestitures.
- Issues approvals for defensible disposition.
- Communicates rules and regulations changes to Risk and Information Management and IT teams.
- Collaborates with key Information Governance stakeholders.

2. DISCOVERY

- Communicates, instructs and coordinates with business units and/or individuals related to information that must be located, preserved and produced to satisfy litigation requirements.
- Manages Freedom of Information requests in countries like the UK. Includes updating custodians on the status of holds on information and when it can be released for normal lifecycle management.
- Updates Records and Information Management and IT teams on changes to discovery requirements.
- Establishes a repeatable process with guidelines to manage the spectrum of litigation that impacts the legal holds controls within the framework.

3. RISK

- Protects your organisation's brand, finances and operations by managing and mitigating risk exposure.
- Needs full understanding of your organisation's risk profile (litigation, investigations, regulatory requirements, protection of private information and intellectual property) and associated controls.
- Collaborates with Legal to create acceptable use policy.
- Collaborates with IT to develop acceptable disaster recovery and business continuity processes, selection of SaaS/Cloud providers.
- Educates employees about prevention of risk-related activities.
- Provides input to key risk indicators.

4. COMPLIANCE

- Ensures your organisation is aware of and meets requirements of the rules and regulations imposed by authorities (such as EU, regulatory agencies, data privacy authorities, industry groups)
- Determines internal metrics and controls; establishes an enterprise-wide audit programme; responds to and manages requests from regulators, auditors, investigators, customers and other third parties.

5. RECORDS AND INFORMATION MANAGEMENT

- Develops and publishes the RIM Programme policy for paper and electronic records.
- Provides implementation support through training and ongoing communications.
- Determines and measures compliance.
- Contains costs through information lifecycle awareness and storage options, as well as disposition.
- Participates on IT projects for software review and implementation.
- Establishes a support system for lines of business to include a records coordinator network.
- Stays abreast of trends in Records and Information Management (cloud, big data, and BYOD).
- Communicates/collaborates with key stakeholders to determine policy/approach.

As business-level self-governance becomes institutionalised, the RIM department must create a self-service environment from which businesses can pull the information they need to comply with RIM Information Governance requirements.

Information Governance will make it necessary for this function to evolve from providing records-centric guidance to being inclusive of all information – whether it's physical or electronic.

6. DATA OFFICE OR DATA GOVERNANCE

- Assists businesses and other functions in ensuring a consistent and controlled approach to the development and use of information assets and critical data elements across an organisation (role of Chief Data Office function, and specifically the role of the Chief Data Officer (Chief Health Information Officer in the Healthcare Industry).
- Guides the establishment of processes and systems that are able to create, maintain and share data in compliance with an organisation's data standards and external regulations/laws.
- Implements a framework of controls to support effective and efficient data management (in collaboration with members of Enterprise Data Governance Council).

The Chief Data Officer partners with Data Governance Officers assigned to the functions and businesses across the organisation. They conduct data governance/data management practice assessments through various tools such as the Data Maturity Model, Data Quality Platform and Data Standards implementation plans.

7. INFORMATION TECHNOLOGY

- Function is shifting to be more aligned with lines of business and their objectives.
- Increases ability to manage the high volume of data being created and received.
- Eliminates costs particularly around redundant technologies and storage.
- Provides input for Records and Information Management controls dealing with protection and authentication of data and its availability for use, preservation and disposition.
- Collaborates with Records and Information Management, Risk and Compliance to determine appropriate disaster recovery and business continuity plans.
- Collaborates with all other Information Governance roles to understand the technology selection and deployment requirements of each.

8. INFORMATION PRIVACY

- Manages risks and business impacts of privacy laws and policies.
- Responds to regulator and consumer concerns over use of personally identifiable information (PII), (including medical and financial data) and laws and regulations for use and safeguarding of consumer financial and banking transactions.
- Advises on proper protection and safeguards for specific high-risk information and its impact on the RIM Risk controls.

9. INFORMATION SECURITY

- Develops, implements and manages an organisation's security vision, strategy, policy and programmes.
- Creates policy, selects technology and implements policy, monitors and informs parties about malware, breaching, hacking and other related events.
- Communicates policies and procedures to the business.
- Enables security standards dictated by customers, such as the Government.
- Informs necessary parties of breach issues.
- Issues data classification codes (in conjunction with Legal).
- Remains compliant with International Organisation for Standardisation (ISO) and other regulatory bodies.

10. INFORMATION ARCHITECTURE

- Focuses on the organisation of information and database development to support your business needs.
- Designs complex, shared information systems.
- Gets involved in selection and management of cloud-based services.
- Support archive creation for email and social media content.
- Supports building efficient websites and intranet sites to support Records and Information Management.

11. BUSINESS

(LINES OF BUSINESS, BUSINESS UNITS AND/OR DEPARTMENTS)

› Ensures compliance with Information Governance policies.

The management of the information lifecycle is most efficient when it acquires the attributes, tags, indices or metadata necessary for compliance as close to its creation as possible, such as, flagging a piece of information as being confidential, or containing personally identifiable information, or that it belongs to a specific record class or group.

Lines of business often complain that records management gets in the way of doing business. To address this, IT and Records and Information Management should work closely with lines of business to work out how they can best take control of their information through technology and process in the least intrusive way.

Lines of business are in the best position to judge the value of the information they create, maintain or receive beyond that of its original use. Certain types of records may be used to determine marketing trends, track quality control issues, expand customer profiles and identify 'bad actors' in a regulated environment. Records and Information Management should work with the lines of business to determine valuable information and how it should be managed in a secure and compliant manner.

There's a strong move towards making lines of business responsible for self-governance for a variety of corporate requirements, including Records and Information Management. This is particularly the case in large, geographically dispersed organisations with diverse lines of business. The business expectation is to pull the information required to self-govern from sources such as Records and Information Management and Legal.

12. INTERNATIONAL REPRESENTATION

Because Information Governance should extend across an organisation's entire enterprise, there must be strong geographic representation on the Council. This could be a delegate from a region (i.e. Asia Pacific, EMEA and North America) that can speak to the concerns of the different jurisdictions within the region.

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organisations lower the costs, risks and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including back-up and archival data, electronic records, document imaging, business records, secure shredding and more, for organisations around the world.

Visit the company website at www.ironmountain.co.uk for more information.

Need more information, help or advice?

CONTACT US AT: 08445-60-70-80 or WWW.IRONMOUNTAIN.CO.UK/CONTACT-US

IRON MOUNTAIN®