Components of Information Governance (IG)

Overview

IG is a super-discipline that includes components of several key fields: law, records management, information technology (IT), risk management, privacy and security, and business operations.
Robert F. Smallwood, Information Governance: Concepts, Strategies, and Best Practices 2014.

IG is not a Project, but is an ongoing Program.

IG seeks to manage and control information assets to lower overall information risk, ensure compliance with regulations and improve information quality and accessibility while implementing information security measures to protect and preserve information that has business value.

IG is a subset of corporate governance and includes the following key concepts:

- Records Management
- Content Management
- IT Governance
- Data Governance
- Information Security
- Data Privacy
- Risk Management
- Litigation Readiness
- Regulatory Compliance
- Long-Term Digital Preservation
- Business Intelligence

Key Components Defined

Records Management (RM) & Records and Information Management (RIM)

- Foundational component of IG.
- Primarily concerned with the identification, classification, retention, use and eventual disposition of records and information.

Content Management

- Primarily concerned with the storage and access of electronic records and information.
- Incorporates security, access controls, retention and disposition, and legal holds for electronic information.

IT Governance

- Primarily concerned that stakeholders can ensure investments in IT create business value and contribute toward meeting business objectives.
- IT Governance seeks to align business objectives with IT strategy to deliver business value.
- The focus of IT Governance is on software development and maintenance activities for the lowest costs to achieve desired results.
- The Chief Information Officer (CIO) typically has line responsibility for implementing IT Governance and reports to the CEO and Board of Directors.

Data Governance

- Alias “Data Integrity” - processes and controls are in place to ensure data is true, accurate and unique.
- Often involves data cleansing (scrubbing) to remove corrupted, inaccurate or extraneous data and de-duplication to eliminate redundant data.
- Often referred to as Master Data Management (MDM) to ensure reports, analyses and conclusions are based on clean, reliable, trusted data, normally contained in databases.
- Biggest Risk is bad decisions based on inaccurate data.

Information Security

- Focus on controlling access to information (identify and access management) (IAM) and maintaining the security of confidential information and communications.
- Also addresses Digital Signatures, Document Encryption, Data Loss Prevention (DLP) also known as leak prevention, and Information Rights Management (IRM).

Data Privacy

- Is primarily concerned with the identification and protection of personally identifiable information (PII).
- PII is any information that can identify an individual, such as name, Social Security number, medical record number, credit card number, etc… (normally name + one more identifier).
- Involves the development of Data Breach Response Plans and responding to breaches.

Risk Management

- The identification, assessment and prioritization of organizational risks.
- Focus on risk identification, mitigation and cleanup activities.

Litigation Readiness

- Key legal processes include electronic discovery (e-discovery) readiness, records and information retention policies, legal hold notification, and legally defensible disposition practices.
- Federal Rules of Civil Procedure (FRCP) govern the preservation and discovery of records and information in the litigation process. (Amended in Dec 2006 – plans to revise in Dec 2015)

Regulatory Compliance

- Alias Legal and Regulatory Compliance.
- Key focus is to ensure the organization is conforming to relevant laws, regulations and internal policies.

Long-Term Digital Preservation (LTDP)

- LTDP methods, best practices and standards should be applied to preserve an organization’s historical and vital records, those without which it cannot operate or restart operations) and to maintain its corporate or organizational memory.
- Uploading permanent electronic records into your digital records center will not necessarily preserve records over long periods of time.
- Digital Preservation is a process and not a technology, addressing format, media, software and hardware obsolesce associated with digital information.

Business Intelligence

- Primarily concerned with data analytics to identify insights and emerging trends.
- Can provide solid information for decision makers to use in times of crisis or opportunities.
- Has a desire to retain all information to provide better analytics.