BYU

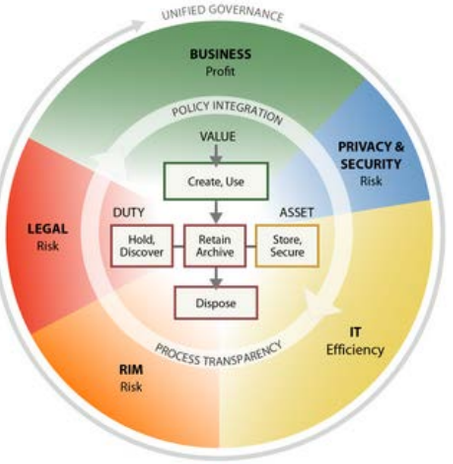
UNIVERSITY RECORDS &
INFORMATION MANAGEMENT

Components of Information Governance

September 17, 2015

Presented by: Howard Loos

IG

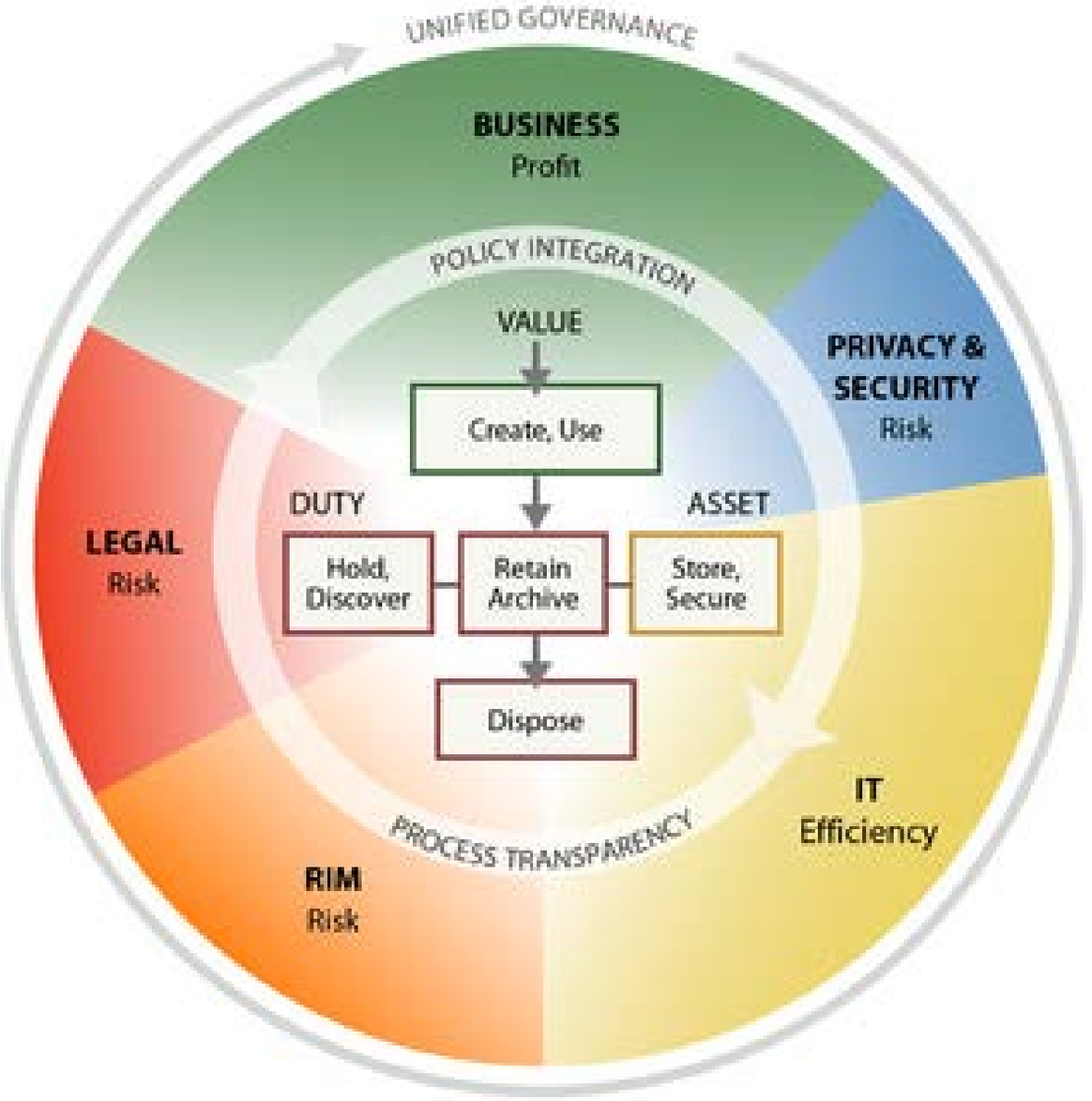


IG is a super-discipline that includes components of several key fields: law, records management, information technology (IT), risk management, privacy and security, and business operations

Robert F. Smallwood, Information Governance: Concepts, Strategies, and Best Practices 2014.

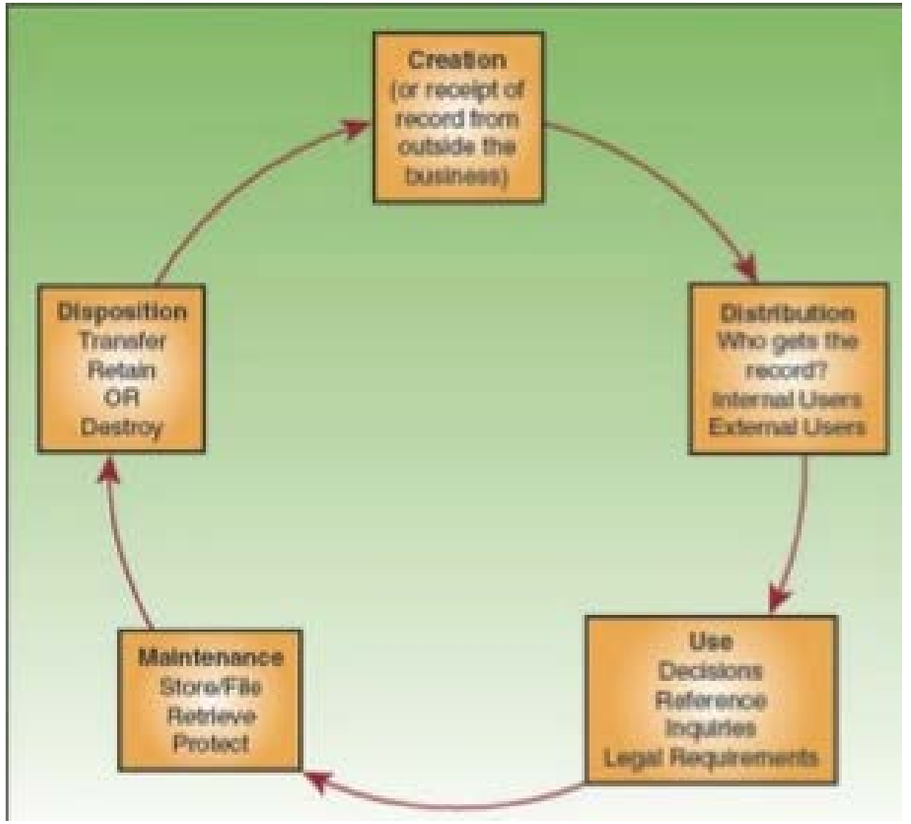
IG Components

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



Records Management

- Primarily concerned with Records:
  - Identification
  - Classification
  - Retention
  - Use
  - Disposition

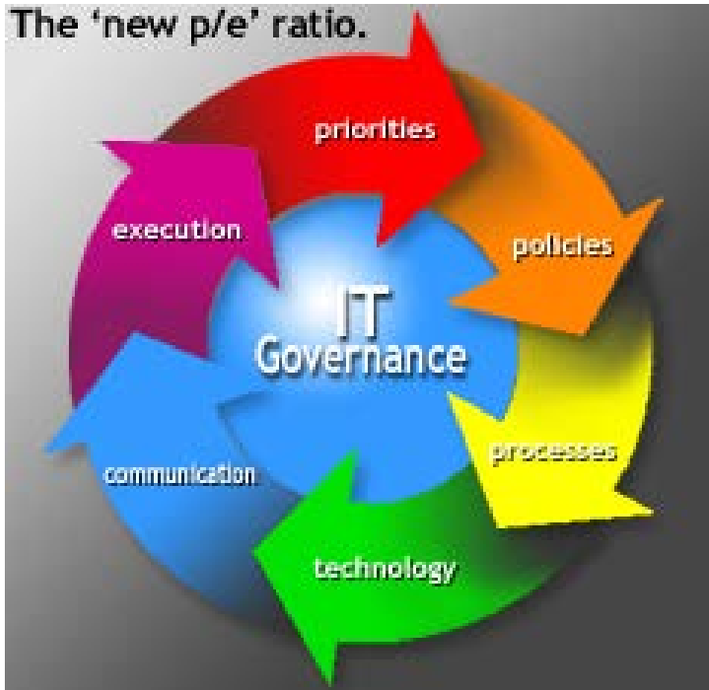


Content Management

- Primarily concerned with the storage and access of electronic records and information
- Often incorporates the following capabilities:
  - Security
  - Access Controls
  - Retention and Disposition
  - Legal Holds

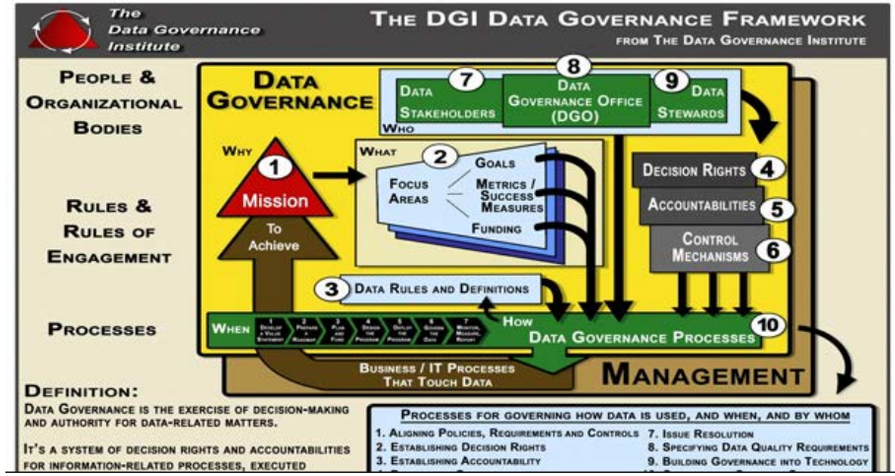
IT Governance

- Ensure IT investments create business value and contribute toward meeting business objectives
- Focus on software development and maintenance activities at the lowest cost 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, who provide oversight



Data Governance

- Focus on Data Integrity - processes and controls to ensure data is true, accurate and unique



- Often referred to as Master Data Management (MDM) to ensure reports, analyses and conclusions are based on clean, reliable, trusted data, normally contained in database rows and fields
- Biggest Risk is bad decisions based on inaccurate data

Information Security

- Focus on controlling access to information and maintaining the security of confidential information and communications
- Also addresses Digital Signatures, Document Encryption, Data Loss Prevention (DLP) also known as leak prevention, 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…
- Data Breach Response Plans

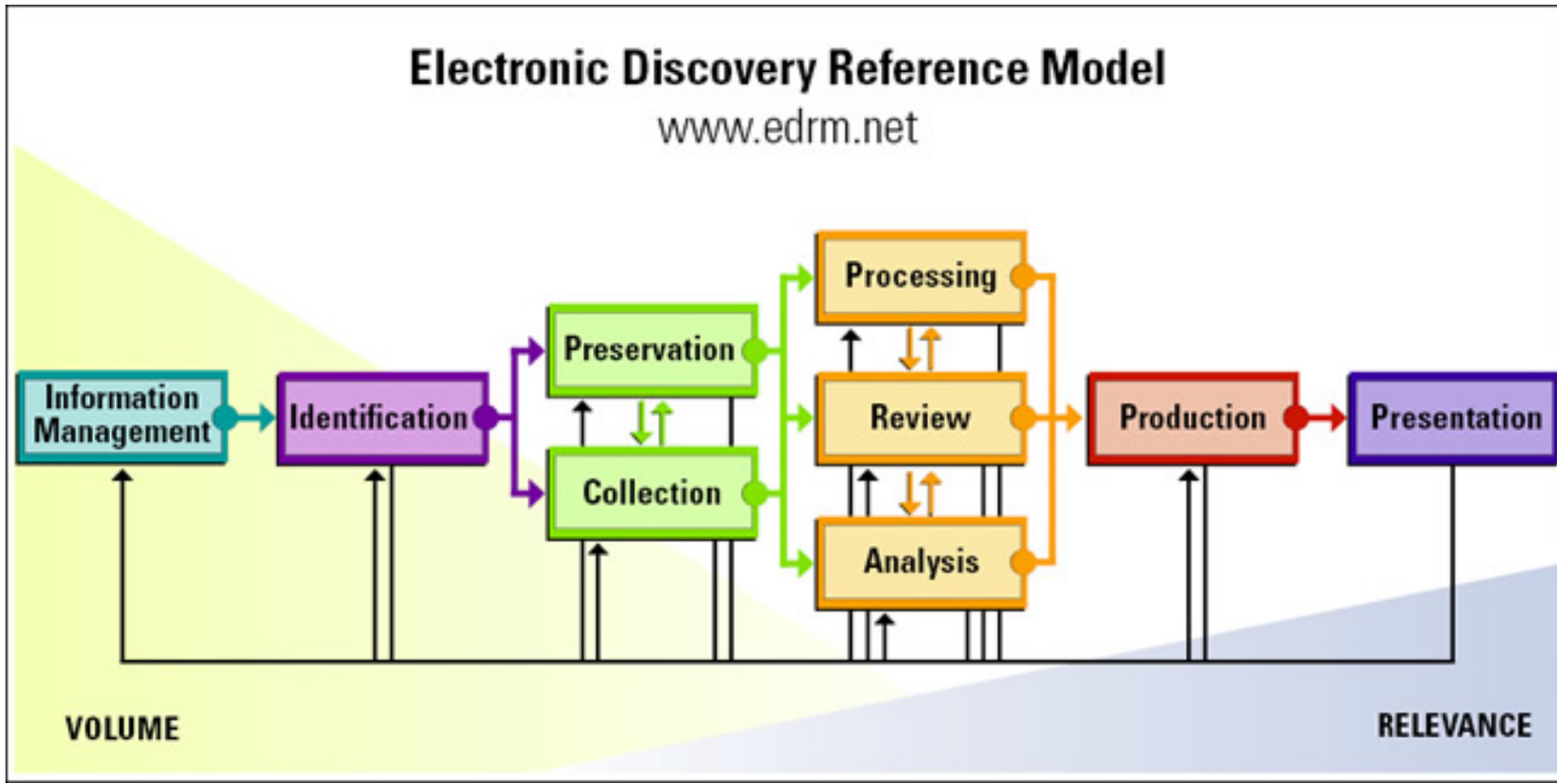
Risk Management

- The identification, assessment and prioritization of organizational risks
- Focused 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
  - Legally Defensible Disposition practices

- Federal Rules of Civil Procedure (FRCP) govern the preservation and discovery of records and information in the litigation process



Regulatory Compliance

- Often referred to as 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

- Uploading electronic records with permanent retention into your digital records center will not preserve records over time

Business Intelligence

- Primarily concerned with data analytics to identify insights and emerging trends
- Can also provide solid information for decision makers to use in times of crisis or opportunities