Information Governance: A Key Component of Your Compliance Strategy

Diane Carlisle, CRM
ARMA International
ABOUT ARMA INTERNATIONAL

• Not-for-profit professional association
• Worldwide membership - 10,000+
• Education and resources
  – Live & online education
  – Technology news & trends
  – Standards, best practices
  – Books, newsletters, magazine
  – Web seminars
The principles of information governance, known as the Generally Accepted Recordkeeping Principles® (the Principles), are well-developed and well-understood by information governance and information management practitioners. The Principles, which are grounded in practical experience and based on extensive consideration and analysis of legal doctrine and information theory, form the basis upon which every effective information governance program is built, measured, and – regardless of whether or not an organization or its personnel are aware of them – will one day be judged.
INFORMATION GOVERNANCE & RECORDS MANAGEMENT
Information governance is a strategic framework comprised of standards, processes, roles, and metrics that holds organizations and individuals accountable to create, organize, secure, maintain, use, and dispose of information in ways that align with and contribute to the organization’s goals.

ARMA, 2012
INFORMATION: ASSET? LIABILITY?

- Basis for sound business decisions
- Enables compliance with regulations, litigation obligations
- Evidence for claims made in court
A RIM program defines the rules and controls that allow a company to manage records and information from creation/receipt until no longer needed:

- Email management
- Retention policy/process
- Legal/regulatory compliance
- Risk assessment
- Litigation/ediscovery
BENEFITS OF GOOD IG

- Compliance with laws and regulations
- Legally defensible recordkeeping practices
- Ensure integrity of information
- Ensure availability of information for decisions
- Efficient and effective processes
- Reduced risk
- Reduced costs
Information Governance Reference Model (IGRM)

Linking duty + value to information asset = efficient, effective management

Duty: Legal obligation for specific information
Value: Utility or business purpose of specific information
Asset: Specific container of information
IG REQUIRES COLLABORATION

• Key Stakeholders
  – Business units
  – Legal
  – IT
  – Compliance

• IG professionals integrate these various needs into unified solutions
INTERNAL ALLIES

Lawyers and IT are Natural Allies

Lawyers priorities include:

- Risk
- ROI
- Preparing 30 (b)(6) expert witnesses
- Impact on overall litigation profile
- Comprehensive ECM and RM programs

IT priorities include:

- Understanding the current environment
- Documenting key systems and data stores
- How much legacy data?
- Restricting tapes to only DR
- Matching systems to ROI priorities
GENERALLY ACCEPTED RECORDKEEPING PRINCIPLES

• Framework for information governance
• Introduced in 2009
• Carefully vetted “best practices”
• Derived from international & national standards
• Industry independent
• Recognized by standards organizations and legal counsel
THE PRINCIPLES

- Accountability
- Transparency
- Integrity
- Protection
- Compliance
- Availability
- Retention
- Disposition

www.arma.org/principles
BAD PRACTICES, BAD RESULTS

• Evidence comes from the records & information

• BP rig explosion and oil spill litigation
  – $4.5 Billion to government
  – $7.8 Billion to businesses
  – Engineer charged for deleting 200 text messages
  – Claims against Halliburton - $20 Billion
  – Emails are the “smoking gun”
  – Contractors – who is at fault?
KEY CHARACTERISTICS

Taken together, the Principles provide the framework for effective Information Governance.

- Objective
- Reasonable
- Reality-based
- Scalable
- Standards-based
CONTEXT IS CRUCIAL

• Application will vary from organization to organization
• Contextual factors:
  – Mission
  – Compliance requirements
  – Laws and regulations
  – Jurisdictions
  – Constituency
  – Operations and workflows
  – Litigation profile
WHY STANDARDS ARE CRUCIAL

• Objective foundation for judging an IG program
• Represent best thinking & practices
• Standards evolve toward greater consistency
• They provide a body of guidance applicable to many
MEASURING INFORMATION
GOVERNANCE
WHY IG METRICS ARE IMPORTANT

• Transform strategy into action
  – Specific & quantifiable goals
  – Monitor progress toward goals
• Document improvements and “good faith efforts”
• Demonstrate impact of program
• Support compliance/litigation efforts
INFORMATION GOVERNANCE MATURITY MODEL

- 1st generation assessment tool
- Defines characteristics of IG at different levels
- Use to identify gaps between current state and desirable state
- Quantitative & qualitative measures
- Systematic process
  - Evaluate program & assess risks
  - Plan program improvements
### The Maturity Model

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Sub-Standard</td>
<td>RED</td>
</tr>
<tr>
<td>2 In Development</td>
<td>ORANGE</td>
</tr>
<tr>
<td>3 Essential</td>
<td>AMBER</td>
</tr>
<tr>
<td>4 Proactive</td>
<td>BLUE</td>
</tr>
<tr>
<td>5 Transformational</td>
<td>GREEN</td>
</tr>
</tbody>
</table>

- No need to stair step through levels
- Level may vary across principles
- Level 3 – minimum acceptable
- Less than 5 may be acceptable:
  - Risk tolerance
  - Level of regulation
# MATURITY MODEL - EXCERPT

<table>
<thead>
<tr>
<th>Principle</th>
<th>Level 1 (Sub-Standard)</th>
<th>Level 2 (In Development)</th>
<th>Level 3 (Essential)</th>
<th>Level 4 (Proactive)</th>
<th>Level 5 (Transformational)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountability</td>
<td>A senior executive (or person of comparable authority) shall oversee the information governance program and delegate responsibility for records and information management to appropriate individuals. The organization adopts policies and procedures to guide personnel and ensure that the program can be audited.</td>
<td>No senior executive (or person of comparable authority) is responsible for records or information. The records manager role is largely non-existent, or it is an administrative and/or clerical role distributed among general staff. Information assets are managed in a disparate fashion or not at all.</td>
<td>No senior executive (or person of comparable authority) is involved in or responsible for records or information. The records manager role is recognized, although the person in that role is responsible only for tactical operation of the existing records management program, which is concerned primarily with managing records.</td>
<td>The records manager role is recognized within the organization, and the person in that role is responsible for the tactical operation of the established records management program on an organization-wide basis. The organization includes electronic records as part of the records management program.</td>
<td>The organization’s senior management and its governing board place great emphasis on the importance of information governance. The records manager directs the records management program and reports to an individual in the senior level of management, (e.g., chief information governance officer). The chief information</td>
</tr>
</tbody>
</table>


USING THE MATURITY MODEL

• Target the optimum level for your organization for each principle
  – Different levels for different principles is ok
• Determine maturity of existing practices
• Identify gaps between current and optimum levels
Practical Applications
Prominent Security Threats

- Natural threats
- Cybercrimes
- Human error
- Technology failure
- Uneducated employees
- Malware
Security Measures

• Data encryption
• Firewalls
• VPN for remote access
• Passwords
• Physical security
• Updated policies
• System audits
PRIVACY CONSIDERATIONS

• Striking the balance
  – Trust vs. business intelligence
• Opt in vs. Opt out
• Data protection
• Data breach prevention
  – 46 states have notification laws
  – Cost per record: $194
  – Cost per organization: $5.5M
KEY FACTORS IN DATA BREACHES

Protections

• Security officer in the C-suite
• Quick notifications (<30 days)
• Get outside help in response plan

Potential Threats

• Third party providers (41%)
• But not too quick
• Lost / stolen devices (39%)

Ponemon Institute Cost of Data Breach study, 2012
# IG AND PRIVACY COMPLIANCE

<table>
<thead>
<tr>
<th>ITEM</th>
<th>Principle</th>
<th>IG Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security at the C-level</td>
<td>Accountability</td>
<td>Enterprise IG Program</td>
</tr>
<tr>
<td>Quick response process</td>
<td>Transparency; Compliance</td>
<td>Defined policies Data map Metadata index</td>
</tr>
<tr>
<td></td>
<td>Availability</td>
<td></td>
</tr>
<tr>
<td>Get outside help</td>
<td>Accountability</td>
<td>Proactive discussions</td>
</tr>
<tr>
<td>Identify confidential info</td>
<td>Transparency; Availability</td>
<td>Data map Business process analysis</td>
</tr>
<tr>
<td></td>
<td>Protection</td>
<td></td>
</tr>
<tr>
<td>Data loss prevention measures</td>
<td>Accountability</td>
<td>Defined policies Employee training Technology</td>
</tr>
<tr>
<td></td>
<td>Protection</td>
<td></td>
</tr>
<tr>
<td>Integrate protection practices into business process</td>
<td>Protection</td>
<td>Work process analysis Technology application</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Passwords; encryption</td>
</tr>
<tr>
<td>Measured response process</td>
<td>See above</td>
<td>Risk assessment</td>
</tr>
<tr>
<td>Third-party providers</td>
<td>Accountability</td>
<td>SLAs – negotiated</td>
</tr>
</tbody>
</table>
CLOSING THOUGHTS

• Mitigate risk and improve compliance with good Information Governance
• Use the Principles for IG framework and measurements
• Use Maturity Model for benchmarking
• Maximize resource use
• Collaborate with internal allies
Questions?

Diane Carlisle, CRM
Executive Director of Content
ARMA International
Diane.carlisle@armaintl.org

For more information:
www.arma.org/principles