Mitigating compliance and information security risk through records management

EY’s point of view

2018
# Key drivers for investment

Regulatory fines and legal sanctions for non-compliance with record retention regulations, discovery mishaps, and the inability to produce support for key financial, operational, supervisory and risk decisions can present significant business risk. Similarly, retaining records past their legal retention requirements can increase legal and regulatory exposure and costs.

## Regulatory enforcement actions

<table>
<thead>
<tr>
<th>Year</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>FINRA fines LPL Financial LLC $7.5 million</td>
<td>for significant email system failures</td>
</tr>
<tr>
<td>2013</td>
<td>FINRA fines Barclays $3.75 million</td>
<td>for failure to retain Bloomberg instant messages and email attachments</td>
</tr>
<tr>
<td>2016</td>
<td>In 2016, FINRA reported a 423% increase in books and records related fines from $4.3 million in 2015</td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td>FINRA fines 12 firms a total of $14.4 million</td>
<td>for failure to meet WORM requirements</td>
</tr>
<tr>
<td>2015</td>
<td>FINRA fines Scottrade $2.6 million</td>
<td>for significant failures in required electronic records and email retention</td>
</tr>
<tr>
<td>2017</td>
<td>FINRA fines 10 firms a total of $4.25 million</td>
<td>for deficiencies relating to the preservation of broker-dealer and customer records in WORM format</td>
</tr>
</tbody>
</table>

## Top enforcement reasons

- Failure to retain electronic records in Write Once Read Many (WORM) format
- Supervisory system is not reasonably designed
- Failure to implement an audit system regarding the inputting of records in electronic storage media
- Failure to obtain attestation from third-party vendors to confirm the ability to provide records to regulatory bodies

## Digital transformation

- As digital continues to transform businesses, a strategic and holistic approach to leverage technology to optimize RM is essential
- RM is part of the value chain in the big data trend, with analytics providing previously unseen levels of insight, resulting in significant competitor advantages

## Information security

- With rising costs and increased media coverage of data breaches and continued information security and data protection threats, there is opportunity to integrate records management (RM) principles with data protection standards
- Metadata utilized for RM will help identify strategic data sources and flows, including PII and sensitive information for data stored internally, on the cloud and at off-site locations

## Regulatory changes

- MiFID 2 requires firms to retain external and internal telephonic conversations and electronic communications for client order services – receipt, transmission and execution
- The EU General Data Protection Regulation (GDPR) is enforceable on May 25, 2018, with major implications for holding or processing personal data on EU-resident subjects
- CFTC Regulation 45.2 subjects swap dealers to onerous retrievability requirements, e.g. each record must be readily accessible via real time electronic access throughout the life of the swap
- NY DFS 23 NYCRR 500 proscribes limitations on data retention, and storage requirements for non-public information.
In light of recent regulatory scrutiny, firms tend to experience significant challenges in managing and governing an end-to-end RM program across all types of information and communication channels.

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Risks/impacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of end-to-end governance and dated supervision</td>
<td>Unclear roles and responsibilities</td>
</tr>
<tr>
<td></td>
<td>Inability to effect systemic changes</td>
</tr>
<tr>
<td></td>
<td>Unclear roles and responsibilities</td>
</tr>
<tr>
<td></td>
<td>Inability to effect systemic changes</td>
</tr>
<tr>
<td>Inconsistent and decentralized records definition</td>
<td>Inconsistent and decentralized records definition</td>
</tr>
<tr>
<td></td>
<td>Insufficient recordkeeping coverage</td>
</tr>
<tr>
<td></td>
<td>Heightened information security risk</td>
</tr>
<tr>
<td>Inaccurate record inventory and retention schedules</td>
<td>Non-compliance with regulations</td>
</tr>
<tr>
<td></td>
<td>Over-retention</td>
</tr>
<tr>
<td></td>
<td>Complicated event correlation</td>
</tr>
<tr>
<td></td>
<td>High eDiscovery costs</td>
</tr>
<tr>
<td>Non-standard and ineffective search technology</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To establish a sustainable RM program across the enterprise, guidelines listed below provide industry standards for each of the RM program components throughout the life cycle of a record.

Industry standards

1. **Policy**: Provides guidance and sets expectations around practice and execution of RM program activities across the enterprise and applicable lines of business.
2. **Governance**: Defines the ownership and associated roles and responsibilities for oversight functions and business as usual (BAU) activities.
3. **Procedures**: Documents key processes, practices and controls regarding the creation, classification, storage, retrieval and disposition of records.
4. **Regulatory mapping**: Documents the relevant regulatory requirements governing recordkeeping practices.
5. **Records inventory**: Identifies applicable record types created and stored and includes record metadata (classification, location, storage type).
6. **Records retention schedule**: Links to the record inventory and identifies retention periods for each of the record types based on regulatory requirements and enterprise or LOB guidelines.
7. **Information security**: Adhere to information security standards to protect the data, including data governance.
8. **Technology capabilities**: Technology tools leveraged to support various stages of records management including storage, retrieval and disposing of records.
9. **Training and awareness**: Collateral and tools to educate all users with access to records based on their roles and responsibilities.
10. **Monitoring and reporting**: Defined metrics (risk and performance indicators) and management reporting requirements to support oversight of the program.
Mitigating compliance and information security risk through records management

Leveraging principles to create a sustainable framework

Information classification standards and data protection controls can be leveraged with records management principles to optimize the RM framework.

► Information security standards such as data handling controls can be leveraged with records management principles to optimize the RM framework.

► RM processes such as electronic record disposal and record classification can benefit from alignment with the existing information security practices.

► Data protection is a common theme across RM and information security programs. The natural synergies and connections across the programs can reduce compliance and information security risk and promote cost efficiencies across an organization.
Integrated approach to RM and information security

Data protection is a common theme across sustainable RM programs and information security programs. There are many benefits of designing an operating model that aligns with both RM and information security objectives. By aligning objectives across data privacy, information security and records management, organizations can improve controls, promote efficiencies and reduce risk.

Benefits of aligning RM and information security programs

- Reduced risk by having better control of the information (e.g., improved security, protection and access to information)
- Implementation of consistent information classification standards and security controls based on criticality and sensitivity
- Streamlined information governance across the organization
- Cost efficiencies as a more streamlined program result in less unnecessary information to protect
- Increased awareness throughout the organization of the importance and interrelatedness of these risks

Data protection components

- Cyber threats require a set of preventative, detective and corrective measures
- Information classification and tagging is the basis for proper data management with appropriate protection
- Integrity and availability of information throughout the RM life cycle (including archived)
- Confidentiality of sensitive information throughout the RM life cycle
- Identity and access management based on “need to know/need to do”
- Security and privacy by design embedded in the development and support processes
- Employee awareness/training regarding information security requirements and regulations
- Compliance with regulations is an objective of relevant information security standards
Mitigating compliance and information security risk through records management

**Conceptual target state RM framework**

With increasing volumes of structured and unstructured data, organizations must establish a sustainable record management program that considers applicable laws/regulations, local policies, governance and relevant technology capabilities.

**RM target state framework**

- **Governance**
  - Steering committee
  - Roles and responsibilities
  - Interaction model

- **Policy**
  - Definition
  - Scope
  - Requirements

- **Monitoring and reporting**
  - Control Framework
  - MIS Reporting
  - Investigations

- **Training and awareness**

**Leading practice considerations**

1. List all systems that create, transmit and store records with the associated owners and contingency plans.

2. Classify records, systems and establish a “golden-source” of each record type with guidance from business, data governance and information security functions.

3. Implement a centralized retention schedule to support a consistent approach to maintaining the records inventory. Secure data at rest by adopting a robust data protection controls framework.

4. Assess system capabilities and establish procedures to support timely retrieval and e-discovery.

5. Adopt necessary technologies, policies and procedures for defensible disposition of expired or redundant data.

6. Leverage existing information security and data protection controls throughout the life cycle of a record to underpin the RM target state framework.

**Record life cycle**

1. Create
2. Classify
3. Store
4. Retrieve
5. Dispose

**Business analysis**

- Regulatory mapping
- Records inventory
- Detailed procedures

**Technology**

- Records capture
- Classification
- Storage
- User interface
- Purging
- Indexing
- Encryption
- Dashboard
eDiscovery

**Information security standards and data protection controls**
Mitigating compliance and information security risk through records management

EY’s integrated service offerings

EY leverages its electronic recordkeeping expertise and experience to offer a wide array of service offerings that enables our clients to adapt to a constantly changing regulatory environment, thereby seizing opportunities and managing risks at every stage of the value chain.

1. Build current-to-target state assessments, identify gaps, prioritize efforts, create business case for change, provide options and road map design

2. Define the optimal operating model, including capabilities, roles, skills, responsibilities, performance metrics and collaboration model across all groups involved in information management

3. Support all aspects of vendor selection including identifying vendor short list and defining evaluation criteria to be included as part of the RFP documentation; proof of concept selection and implementation support

4. Support all aspects of technology implementations including business and functional analysis; data preparation and migration; feasibility and impact analysis; testing; validation; and strategic architecture

1. Assist in enhancement of existing policies and procedures or development of new standardized policies and procedures to comply with requirements of record keeping regulations

2. Provide regulatory guidance and interpretation of specific information management requirements

1. Standardized policy and procedures
2. Initial program playbook
3. Retention schedules
4. Records inventory
5. Technology capabilities

1. Detailed vendor scorecard

2. Detailed program plan
3. Training plan and materials

Key deliverables:
- Prioritized list of gaps
- Key recommendations
- Detailed project plan
- Change management framework
- Target operating model

Key deliverables:
- Standardized policy and procedures
- Initial program playbook
- Retention schedules
- Records inventory
- Technology capabilities

Key deliverables:
- Detailed vendor scorecard

Key deliverables:
- Detailed program plan
- Training plan and materials

Objective
Policy and procedures development

Objective
Vendor selection and proof of concept (POC)

Objective
Solution implementation and training

Current state

Target state

Strategic roadmap design

Key deliverables:
- Standardized policy and procedures
- Initial program playbook
- Retention schedules
- Records inventory
- Technology capabilities

Policy and procedures development

Vendor selection and proof of concept (POC)

Solution implementation and training
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2018 Ernst & Young LLP.
All Rights Reserved.
1802-2590333
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com