Records Retention and Data Minimization

eBook

Table of Contents

ARCHIVE360

Section 1: Changes in the regulatory environment

Regulatory requirements are forcing organizations to more carefully consider Record Retention and Data Minimization, including the Defensible Disposition of records. Compliance with these obligations requires the coordination and collaboration of many parts of the organization, beyond the Privacy Office and Information Security.

Regulatory Compliance

Data privacy and cybersecurity rules are forcing organizations to rethink the protection of customer data – companies must assure the identification, appropriate retention and disposition, limited acquisition and use, and restricted sharing of data.

1. These rules implicate most, if not all, aspects of a company's interactions with its customers.
2. One consequence is that companies need to re-think their traditional posture of "keeping everything" - because the best protection against a data breach is not to retain sensitive information for longer than necessary.

Three Takeaways

1. These data privacy and security rules are about much more than just privacy and security controls.
2. Data Minimization and Defensible Disposition should now be part of your data management program – determining what information is needed to run your business and comply with the law, and when and how to defensibly dispose of that information.
3. This may take new policies and systems capabilities, including data-driven retention and disposition, guided by better Information Governance, to help manage the day-to-day task of compliance without losing valuable information or causing unnecessary risk.

Section 2: Updating your Information Governance policies

Here are four examples of these rules, which place renewed weight on a company's overall information governance – and the comprehensive infrastructure needed to collect and keep only the information needed, and then only for as long as necessary and no longer.

Example 1: California Consumer Privacy Act (CCPA)

In addition to addressing data privacy and security, the California Consumer Privacy Act (CCPA) regulates:

1. How companies use and share personal information;
2. How they inform customers about the collection, use, storage and sharing of their personal information;
3. How they address customer rights to data access, limited use, consent to sharing, portability and deletion.

Example 2: EU General Data Protection Regulation (GDPR)

Personal data should be kept for no longer than necessary for the purposes for which the data are processed.

Example 3: Section 500.13 NY DFS

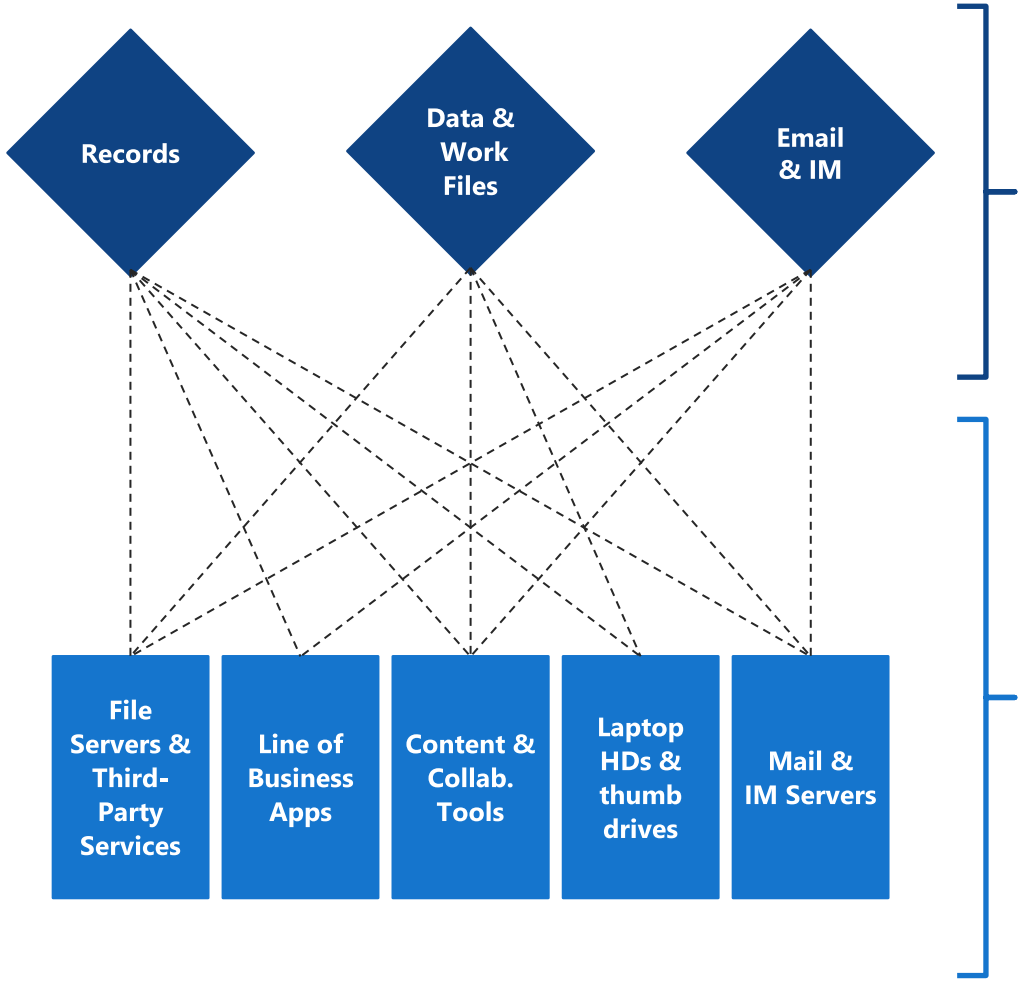
Section 500.13 of the NY DFS Cybersecurity Regulation tells companies that they:

Shall include policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information that is no longer required for business operations or other legitimate business purposes, except where such information is required to be retained by law or regulation.

Example 4 – the NAIC Data Security Model Act

Insurers must "define and periodically reevaluate a schedule for the retention of Nonpublic information and a mechanism for its destruction when no longer needed."

Section 3: Where is the data to discard?



Current Landscape

Information is acquired and stored in many places.

Little control is exercised over where and how information is copied and retained.

Volumes of email, files, applications and other data rise at 10% or more annually.

Vital records often are stored separately from the rest of corporate data and cataloged differently.

Data can be lost due to lack of controls.

Information lives in multiple systems:, including “unstructured” data systems:

- PC hard drives have unmanaged information.
- Email and IMs spread across mail servers, personal archives, hard drives, and file servers.
- End user content may be on multiple systems.

Information moves between silos:

- Drafts and data dumps are stored on hard drives.
- Information is placed on file sharing platforms to facilitate sharing and collaboration.
- Information is moved or copied to archives or other systems.

Lack of tools for legal holds, data collection, and risk analysis.

ARCHIVE360

Section 4: More is no longer better when it comes to records, for reasons beyond compliance with these regulations, including:

Costs

The more data you have, the more it costs to keep it.

Security

The more data you have, the harder it is to secure – and the greater the potential risk of a data breach.

Reduced Business Effectiveness

When you have too much data, finding what you need, when you need it, in a timely fashion, is more difficult.

Customers

The traditional "keep everything" approach now runs afoul of your obligations and commitments to customers.

Companies need to actively determine what information they have, whether to keep it and why, and how to dispose of it carefully and legally.

ARCHIVE360

Section 5: What does it take to comply?

Compliance will be difficult – finding the information, determining its retention period, assessing if there are any other business or legal reasons to keep it, and, most challenging, applying your retention or destruction decisions across the wide range of covered information. Dedicated resources, consideration of appropriate tools, and coordination across stakeholders will be needed.

Data map	1. Map the data you have, where it is, how and by whom it is used, and how it is retained. 2. Include structured and unstructured data – data in IT systems and data in email/eComm systems. 3. Look for data retained in your organization and data about your business that is retained by third parties. 4. Complete a comprehensive inventory of all information systems and applications, and the information they contain.
Deciding what to do with the data	1. Assess the applicable retention schedule, business value, and legal need to retain. 2. Develop retention/disposal decisions and justifications. 3. Create the road map for compliance. 4. Identify or design technology solutions to implement this road map.
Executing and documenting your decisions	1. Determine how best to retain or safely dispose of information. 2. Execute and document the decisions. 3. Continue to monitor changes in the business, operations, technology, and regulations. 4. Train and educate your staff to get their cooperation and participation in these decisions.

Section 6: Managing these Risks through Information Governance

Information Governance ("IG") can enable Data Minimization and Defensible Disposition, through the organized governance of information based on legal obligations, regulatory requirements, customer implications and business value.

Aims of Information Governance:

1. To know what information is needed to achieve business objectives and meet compliance requirements.
2. To know where information is stored and who owns/manages it.
3. To understand how information will be generated and used with new tools, technologies and data sources.
4. To know how long to keep information and why.
5. To properly dispose of information when not needed or required to be kept.

Outcomes of good Information Governance:

1. Risk reduction through increased information and record keeping compliance.
2. Controlled information costs.
3. Reduced legal discovery costs.
4. Reduction in the risk of improper access to, breach or use of personal and sensitive business information.
5. Ease of locating information for business needs and customer requests.
6. Availability of accurate and complete information to support business decisions and operations and be transparent and accurate with customers.

Information Governance "means an organization's coordinated, interdisciplinary approach to satisfying information compliance requirements and managing information risks while optimizing information value."

The Sedona Conference

ARCHIVE360

Section 7: The four objectives of effective Information Governance

An effective IG Operating Model can build, deliver and operate projects that will accomplish these four objectives, all necessary for minimizing data risk and exposure.

1. Classify

Understand what you have, where it lives, and its value to the organization:

- Classify all enterprise information and records and align with systems of record.

2. Store

Once you understand what you have, manage information based on business value:

- Tiered storage, with careful attention paid to keeping information and records in the right IT systems.

3. Manage

Monitor compliance, reduce risk of leakage, track and control retention:

- Measure risk across the enterprise, predict issues before they arise, and address issues quickly when they do arise.

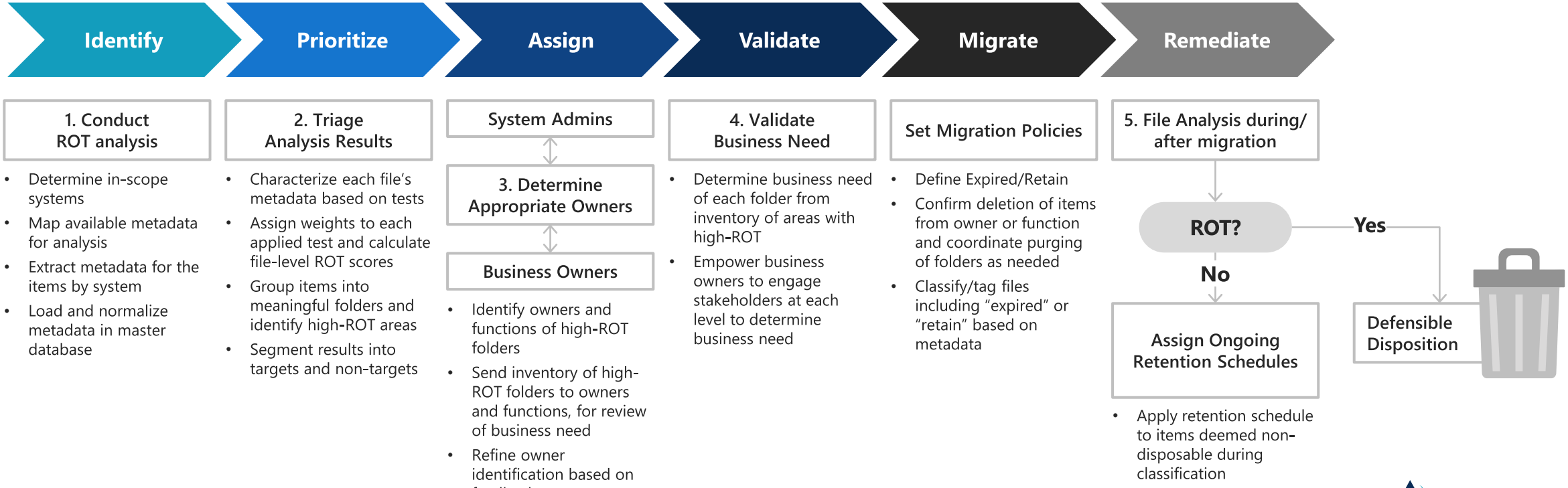
4. Dispose

Keep only what is needed to run the business, decommission old apps and data:

- Enable the identification and deletion of redundant, obsolete or trivial data (ROT) that can be defensibly discarded, thereby reducing risks and costs.

Section 8: ROT Analysis, Migration, and Defensible Disposition

An important component of your IG program should be the identification, classification and as appropriate, defensible disposition of Redundant, Obsolete and Trivial data (ROT). The easiest time to perform ROT/Defensible Disposition is during a migration utilizing programmatic automation. ROT analysis and defensible disposition will advance the protection of sensitive information, decrease exposure to breach risk, reduce eDiscovery costs, and reduce the complexity and costs associated with retaining records indefinitely.

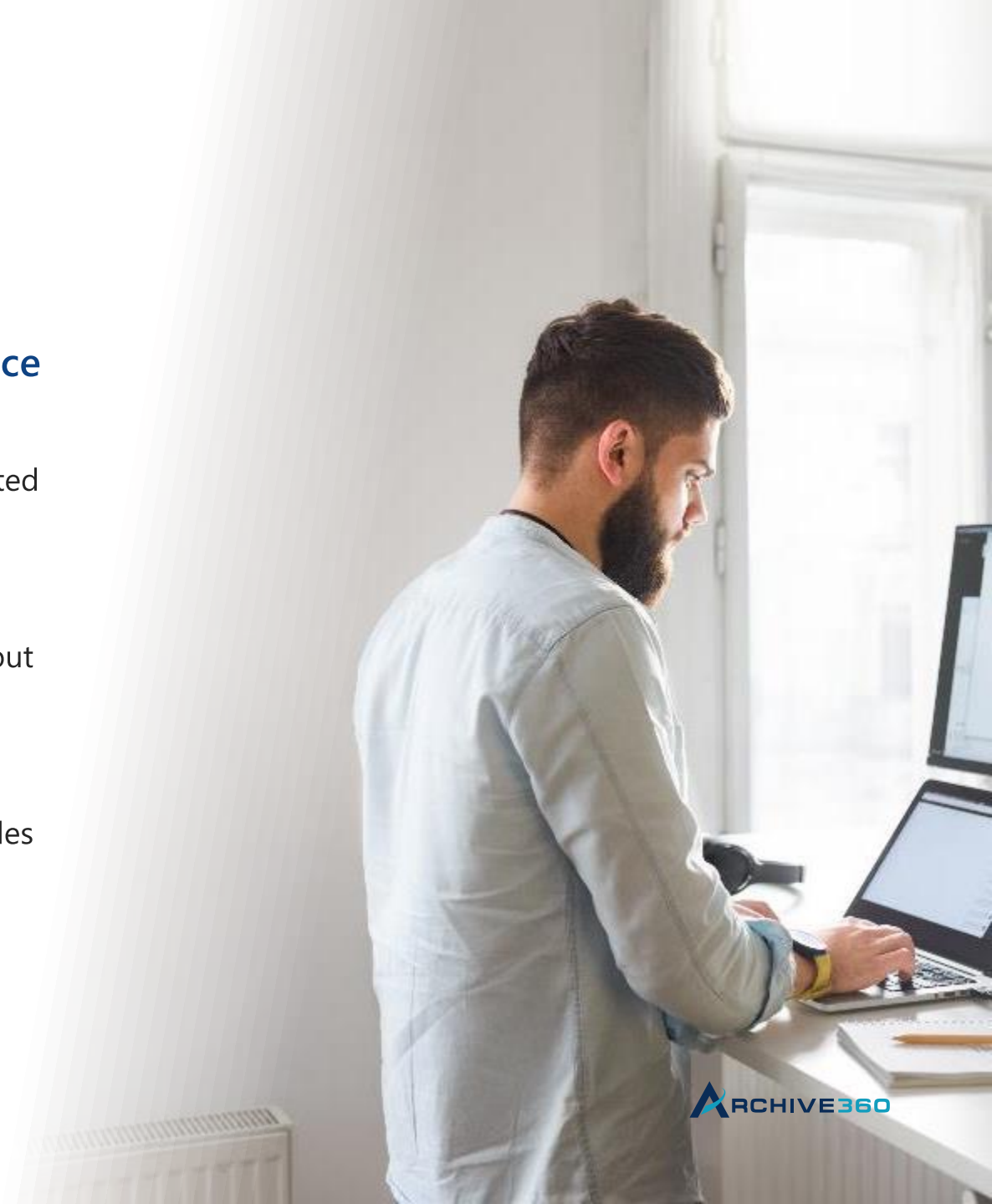


ARCHIVE360

Section 9: Achieving broader organizational goals

Companies can leverage enhanced Information Governance to accomplish business, operational and financial goals.

- Organizations require detailed, accurate data to drive analytics and targeted business activities.
- Accurate information is critical to facilitate timely and correct strategic decisions at an enterprise level.
- Customer touch points must provide high-quality, insightful service without increasing costs.
- Customers trust companies that protect their personal information and honor their choices about its use.
- Timely and accurate reporting for operational and financial analysis enables more informed decisions.
- Companies can build and execute plans for the current and future use of information technology.



Summary: A path forward

The journey to effective Record Retention and Data Minimization begins by prioritizing these objectives within your organization.

1. Assess the current state of relevant capabilities.
2. Develop a vision for Records Retention and Data Minimization that is tailored to the organization's specific risks, issues and requirements, as well as its business strategy and goals.
3. Craft a roadmap, with priority to high-impact initiatives including Defensible Disposition.
4. Develop, fund, staff and rollout the applicable organization and program.
5. Select and implement tools for implementing the program and managing the risks.

I help our enterprise and government customers translate compliance, privacy, and data sovereignty regulations into actionable solutions and I assist with modern eDiscovery best practices. I'm available to answer any questions about information management, data security, data privacy, orany emerging regulation impacting human-generated data in your business.

To schedule time with me, just send me an email:
bill.Tolson@archive360.com

Bill Tolson | Vice President, Compliance & eDiscovery

Learn more at: www.archive360.com

As a Senior Advisor focused exclusively on compliance, ethics and corporate governance, I leverage my 20 years of experience as a Chief Compliance Officer to help companies in insurance and other industries develop and strengthen their compliance programs; conduct compliance risk assessments; manage required remediation of compliance issues; and address laws and regulations in critical areas including sales practices, data privacy, information governance and anti-corruption.

To schedule time with me, just send me an email:
jcohen@cslg.com

Jay Cohen I Senior Advisor, Compliance

Learn more at: www.cslg.com