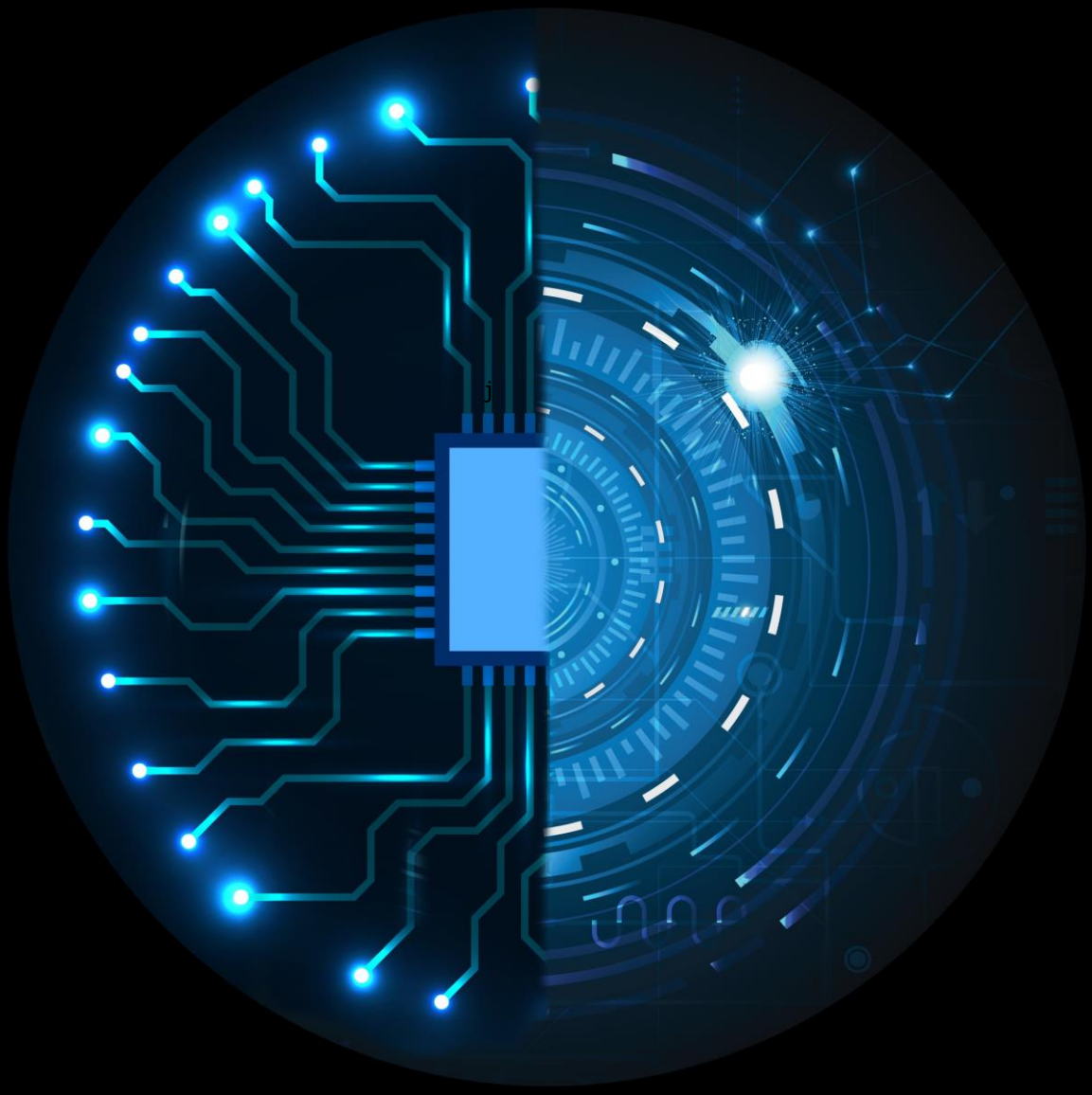
Deloitte.



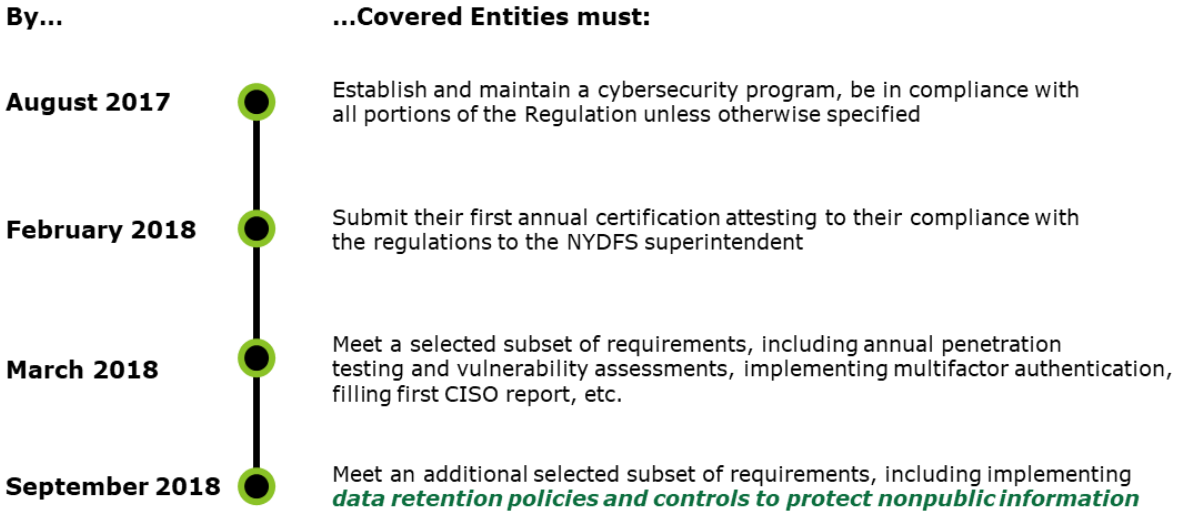
Data and records disposition under new cybersecurity regulations:

Is your organization ready?

April 2018

CENTER *for*
REGULATORY
STRATEGY
AMERICAS

The first compliance deadline under the New York State Department of Financial Services (NYDFS) Cybersecurity Requirements for Financial Services Companies (23 NYCRR 500, "the Regulation") went into effect in August of 2017. The Regulation applies to Covered Entities and includes additional requirements that these organizations must meet throughout 2018, including developing policies and procedures for the secure disposal of Nonpublic Information (NPI).



Challenges to Covered Entities' existing record and data retention programs:

One of the more complex sections of the Regulation relates to Covered Entities with existing record and data retention programs that have been implemented to comply with other regulatory retention requirements.

Section 500.13 of the Regulation outlines requirements for periodic disposal of certain NPI that is no longer required to be retained:

Section 500.13 of the Regulation	Requires that, as part of the cybersecurity program, Covered Entities: *Shall include policies and procedures for the **secure disposal** on a periodic basis of any **Nonpublic Information** [as defined by these rules] that is no longer necessary for business operations or other legitimate business purposes, **except where such information is required to be retained** by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.*

Covered Entities will be required to reconcile the new NYDFS requirements with existing business processes, technologies, and systems. It is common practice for some Covered Entities to retain records and data well beyond required regulatory retention periods, if not indefinitely. Until now, there have been limited regulatory mandates to discourage financial institutions from retaining records and data on an open-ended basis. Covered Entities often follow such retention practices to limit the complexity of retaining and disposing of records and data while mitigating against risks of non-compliance with existing regulatory requirements or outstanding legal holds.

Under the new NYDFS Regulation, Covered Entities will be required to establish policies and controls to protect NPI by implementing programs for secure periodic disposal of certain NPI not otherwise required to be retained for business or regulatory reasons. These programs will need to exist in harmony with existing business processes and technology systems.

Making a case for disposition (costs and risks):

Many firms have for years contemplated adopting a program of defensible disposition of records; but without a regulatory mandate, the cost and challenges associated with implementing such a program were too high, with the risk of premature deletion overriding the perceived benefits of regularly scheduled disposition. With the new NYDFS Regulation in place, firms will need to undertake the costs and challenges; but in doing so, they are likely to realize additional benefits.

These benefits generally fall into three categories: litigation, maintenance, and data security, as shown in Table 1.

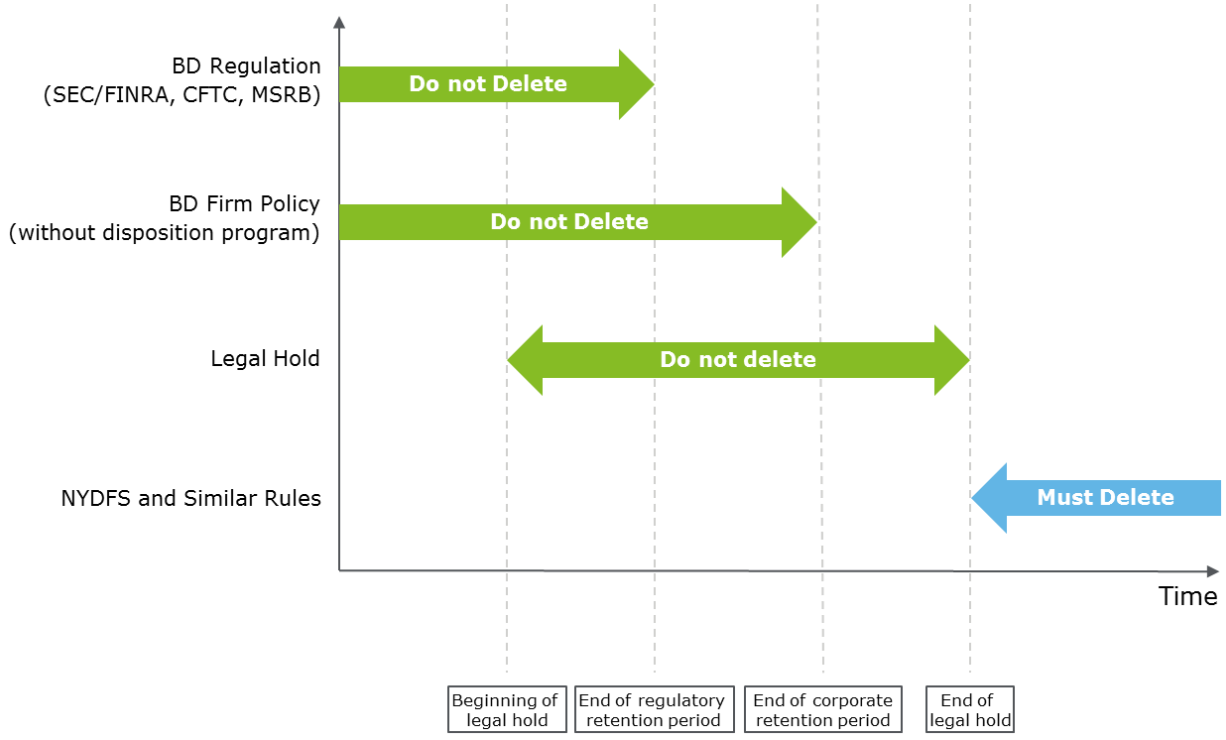
	Litigation	Maintenance	Security
Some challenges	• Every file kept unnecessarily opens the firm up to potential litigation • The more data or records that exist, the higher the cost of responding to discovery requests	• Storage technology hardware is typically refreshed every 3-5 years, and all records must be migrated • The more records, the higher the migration costs	• Cybersecurity breaches are happening more frequently • The more unnecessary data or records a firm retains, the more data or records are vulnerable to theft in the event of a breach
Potential benefits of disposition	• Lower litigation risk • Lower discovery costs	• Lower migration costs • Lower storage costs	• Cybersecurity breaches are happening more frequently • The more unnecessary data or records a firm retains, the more data or records are vulnerable to theft in the event of a breach

Challenges related to the regulation

For broker-dealers:

Broker-dealers regulated by the Securities Exchange Commission (SEC)/the Financial Industry Regulatory Authority (FINRA) and the Municipal Securities Rulemaking Board (MSRB) generally must follow strict regulations governing the manner in which their records must be kept. These regulations, such as 17 CFR 240.17a-3 and -4, generally require that records be kept for a minimum amount of time in a non-erasable manner. Because the Regulation specifies that records should be retained no longer than required by business or regulatory requirements, the Regulation does not conflict with 17 CFR 240.17a-3 and -4 and similar regulations, as shown in Figure 1.

Figure 1: Compatibility of NYDFS Regulation with Existing Retention Landscape



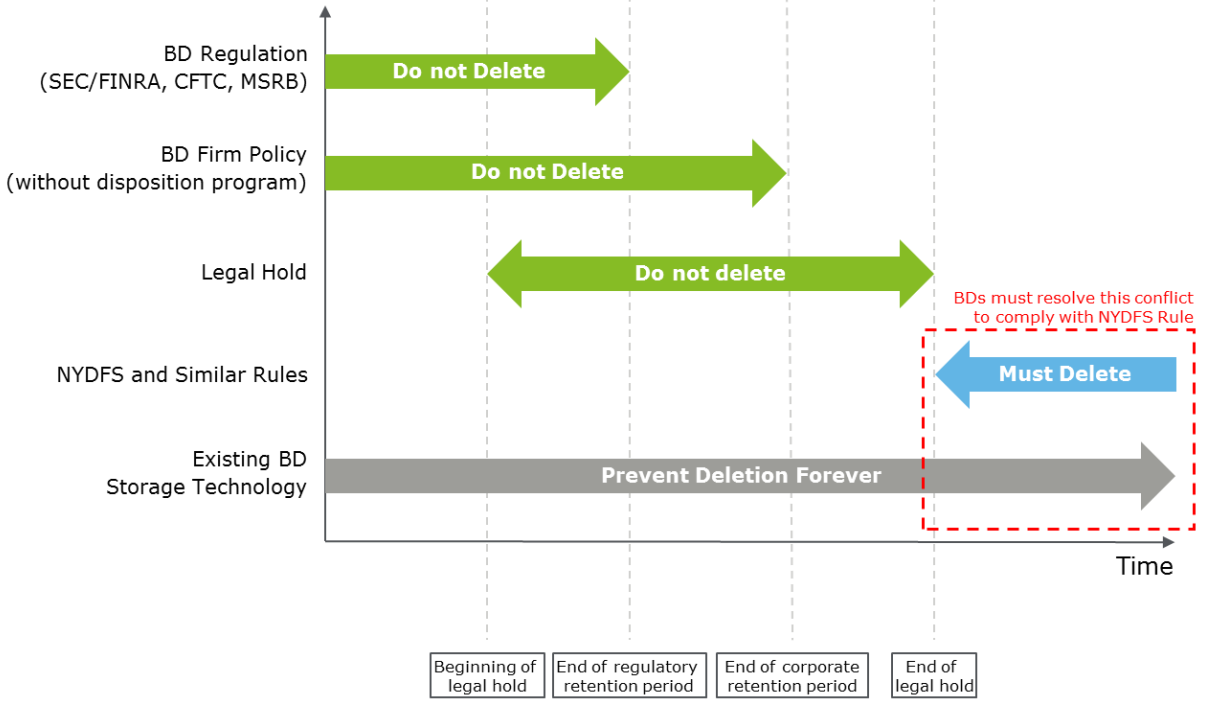
In spite of the seeming compatibility of the Regulation with existing broker-dealer regulations, it is common practice for Covered Entities to retain records well beyond regulatory retention periods. This over-retention of records is generally undertaken as a cost-effective and reduced-risk solution to a common retention requirement facing regulated entities. Existing regulations define the minimum

retention periods of many record types based on future-dated triggering events, such as the closure of a customer account. Unfortunately, many Covered Entities utilize record retention technology that cannot be made aware of these triggering events. By indefinitely retaining records, Covered Entities can ensure records are under retention control for at least as long as is required by their regulations. Though possibly acceptable from the perspectives of risk and cost management, these practices may impact the ability to delete records in a timely manner.

A similar complication arises when a Covered Entity addresses the need for a legal or regulatory hold in their record retention systems. If a record becomes part of a legal proceeding, the firm is required to retain the record for the duration of the legal proceeding. To mitigate the risk of prematurely deleting such records, firms often configure their record retention systems to retain records for pre-determined time periods that are longer than specifically required by the legal proceeding.

Broker-dealers using systems that retain records forever cannot comply with the Regulation, as shown in Figure 2.

Figure 2: Potential Incompatibility of the Regulation with Existing Retention Landscape



Resolving this technological incompatibility may require a substantial effort by broker-dealers to implement modified or altogether new electronic storage systems that can apply more granular retention controls to the records stored within them.

For all financial services firms:
Financial services firms may be subject to many different regulations in many different jurisdictions, including simultaneous obligations under both federal and state regulatory regimes. A universal challenge of meeting these regulations is how to deal with competing, perhaps conflicting, regulations. A robust books and records program should include provisions to resolve the challenges posed by overlapping regulations in addition to addressing a firm's contractual or litigation-related retention or disposition requirements.

In some industry sectors, regulators are proposing limits to the time a firm can keep certain information. For example, the National Association of Insurance Commissioners has released its Insurance Data Security Model Law[1] containing language instructing firms to "[d]efine and periodically reevaluate a schedule for retention of

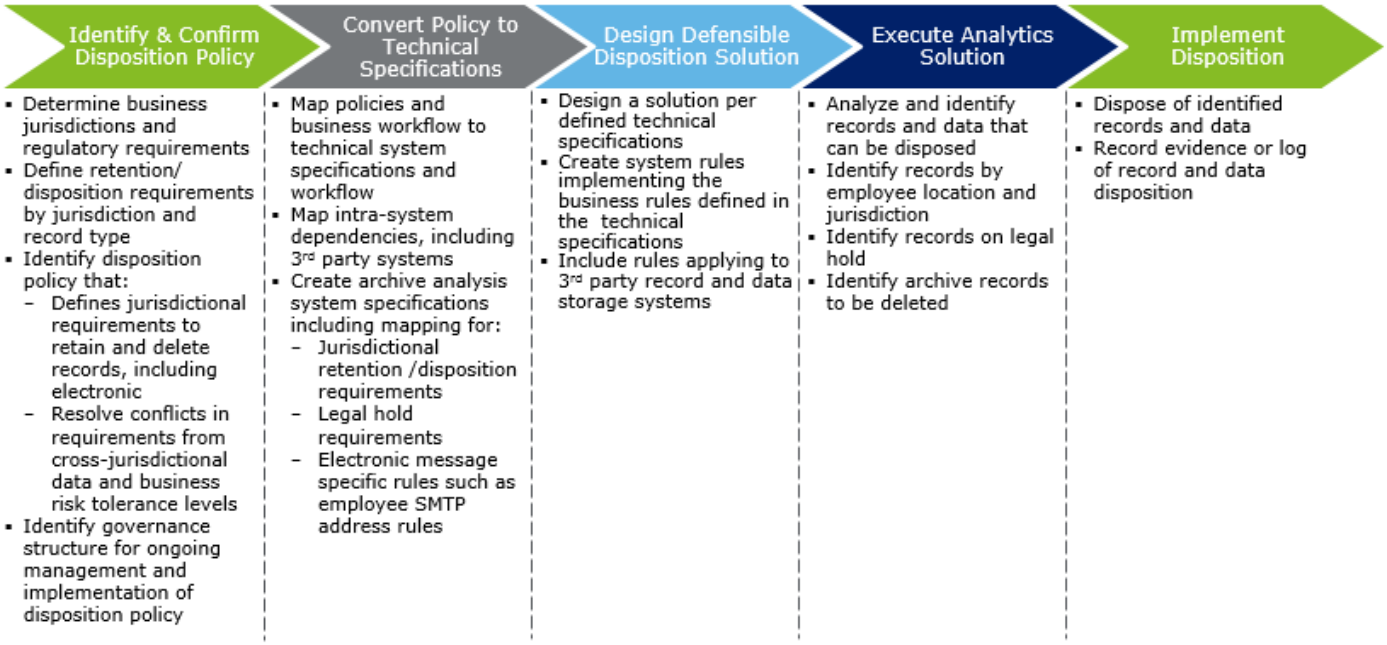
[1] http://www.naic.org/store/free/MDL-668.pdf

Nonpublic Information and a mechanism for its destruction when no longer needed." This law was constructed to adopt the provisions of the NYDFS regulation[2].

Deloitte's framework for implementing a defensible records disposition program

Designed to assist clients with an overall records management program, Deloitte's illustrative approach to implementing defensible records disposition follows the framework shown in Figure 3:

Figure 3: Illustrative Framework for Defensible Disposition Program Implementation Approaches



The framework shown in Figure 3 outlines two critical needs that can help a firm to implement a defensible records disposition program.

1) The first and most important step in implementing a defensible record disposition program is creating a full map of the data retained by the firm, including the lineage information (e.g., source, purpose of creation, owner, and creation time).

2) Once a full data map is created, each data type should be mapped to its applicable retention schedule in the form of a records inventory. The retention schedule should include retention requirements from all sources, including statutory regulation and internal firm policy.

Next steps

The steps outlined above are not trivial to complete and require coordination and participation from many different parts of the firm to achieve. A firm seeking to establish a program of defensible records disposition should focus efforts on creating these items. It is also important to understand that the data map and records inventory are not static documents but will grow and change with changes in the firm's business and the regulatory environment. Implementation of an operating model to manage the data map and records inventory is crucial.

[2] https://www.law.com/newyorklawjournal/sites/newyorklawjournal/2017/11/15/111517nycybervullo

To address longer-term needs, the time is now to begin to budget for a large-scale effort around record retention and disposition. Deloitte continues to analyze the potential impacts of the Regulation on data retention requirements for Covered Entities and will continue to provide our point of view on what steps organizations should consider taking to mobilize and implement defensible disposition programs.

We have designed a structured illustrative framework for implementation designed to help organizations not only comply with the Regulation and other regulatory requirements, but also reduce risks associated with retention of sensitive information. Organizations with interest in the effects of the Regulation may contact Deloitte with questions about the Regulation and activities to support planning, preparation, implementation and compliance.

Contacts

Jay Cohen
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
jaycohen@deloitte.com

Terry Bock
Managing Director | Deloitte Risk and Financial Advisory
Deloitte Transactions and Business Analytics LLP
tbock@deloitte.com

George Hanley
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
ghanley@deloitte.com

Josh Uhl
Senior Manager | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
juhl@deloitte.com

Paul Yackinous
Senior Manager | Deloitte Risk and Financial Advisory
Deloitte Transactions and Business Analytics LLP
pyackinous@deloitte.com

Joseph Conroy
Manager | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
jconroy@deloitte.com

Steve Allelujka
Senior Consultant | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
sallelujka@deloitte.com

Mat Kotowsky
Specialist Senior | Deloitte Consulting
Deloitte Consulting LLP
mkotowsky@deloitte.com