White paper

Playing data defense:

A look at financial regulations' impact on data management

Table of contents:

Introduction

When it comes to predicting what your Chief Executive Officer (CEO) wants, you may not have all the answers. One day they're asking you to hire more staff and "figure out big data," and the next day it seems they're concerned about the cost of data centers and storage.

One thing is certain, however: your CEO hates being fined by regulators for completely avoidable reasons. Moreover, your CEO probably has an aversion the ensuing media frenzy and uncomfortable shareholder meetings in which they have to explain why the company let it happen.

Remaining in compliance with international, federal, state, and industry regulations is a daunting task for financial institutions, particularly for the global systemically important banks (GSIBs). These banks are often the first to be subjected to such regulations and find themselves pioneering efforts to remain compliant.

However, financial institutions of all sizes must deal with compliance at some point. According to a 2015 study by Thomson Reuters, 70 percent1 of firms are expecting regulators to publish even more regulatory information in the next year, and banks must know them all inside and out.

Although it could be argued that being fined for noncompliance is likely the world's most predictable problem, since rules and regulations are published with plenty of advance notice, regulations can sometimes be vague and confusing to understand.

Many companies, therefore, have significant resources dedicated to staying on top of the latest regulations and ensuring that company-wide practices are in compliance. In fact, Reuters reports that more than two-thirds of financial firms (68 percent2) are expecting an increase in their compliance budget with 19 percent expecting significantly more.

Why, then, do so many large companies still incur steep penalties and public admonishment? Because although they typically know what they need to do to remain in compliance, many of them simply do not have the automated systems, infrastructure, and—you guessed it—data quality standards in place to meet these regulations.

68% of financial firms are expecting an increase in their compliance budget this year.

The purpose of regulations

Financial regulations are meant to protect consumers and banks alike. Since the financial crisis in 2008, regulators have applied significant pressure to the banking industry to ensure that financial institutions have the infrastructure, business processes, and the tools to ensure that data flowing into their finance, compliance, and risk functions are of the highest quality.

At its peak, poor data quality sat front and center during the financial crisis. Although not the cause of the crisis, gaps in the quality and completeness of the financial data contributed to the crisis by leaving the decision makers without the important and timely information they needed to make sound decisions. As a result, a new way of looking at data arose: data must be "fit for purpose."

Regulators across the globe are now focused on seeing that the financial community improves their data management and data quality practices to better understand the market and to avoid another crisis. Regulations like Dodd-Frank, BASEL Capital, FATCA, liquidity reporting, resolution planning, etc., all require accurate, timely, and complete data.

The need to be proactive

We recently surveyed data professionals in the financial sector for our annual global data management benchmark report, and we found that 90 percent of financial institutions believe increasing regulation has driven their need for better data analytics and management. However, not all organizations are at the same place with the complexity of their data management programs. Only 68 percent of financial institutions have a big data strategy in place to analyze large sets of data, and only 32 percent of such institutions intend to use their data to reduce risk.

However, the organizations that do take a proactive approach to their data management are better poised to adapt to new and changing regulations. In many cases, GSIBs tend to be first in line for regulatory enforcement and, thus, more proactive than the domestic systemically important banks (DSIBs) and smaller institutions, such as hedge funds and credit unions. However, even the GSIBs tend to focus their compliance efforts on being reactive, rather than proactive.

90% of financial institutions believe increasing regulation has driven their need for better data analytics and management.

Top regulations facing financial institutions

We know that keeping current on financial regulations can seem like an uphill battle, but good data management practices are the key to success. To help you get started, we've put together a closer look at some of the rules and regulations that might keep your Chief Data Officer (CDO) up at night.

Basel Committee on Banking Supervision (BCBS) 239

In 2009, the Basel Committee on Banking Supervision (BCBS), issued a directive known as the "Principles for effective risk data aggregation and risk reporting" in an effort to avoid a repeat of the financial crisis. Although it's not a regulation by itself, this principle-based document directed banks to improve their data and risk functions to ensure better understanding and control of their aggregate risk and exposure.

The central pillar of the data directive is data quality, although this seems to be where most banks are struggling, as data quality is often their lowest priority when tackling BCBS. For instance, principle one of the BCBS 239 states that a bank's board and senior management should promote an overall risk management framework that includes the identification, assessment, and management of data quality risks. Furthermore, principle three adds, "Supervisors expect banks to measure and monitor the accuracy of data and to develop appropriate escalation channels and action plans to be in place to rectify poor data quality."

GSIBs were the first banks required to comply with the data and risk principles of the BCBS 239 directive. Early indications show that the GSIBs have good progress in their data management implementations and capabilities, but they still have significant challenges and work to do (across their infrastructures and digging deep into their legacy environments). DSIBs are next in line, as the regulators will be turning to this segment of the market expecting the same adherence to data management best practices.

Basel III

BCBS introduced the Basel III regulation, which required banks to provide accurate and complete data and to make that data easily available for regulators to access in the event of a crisis. The regulation is based on three fundamental tenets: capital requirements, risk management, and disclosure. In addition, Basel III introduces liquidity requirements for banks, as well as increases capital requirements.

Basel III's new requirements for risk data aggregation have placed an added burden on organizations' data management systems. Financial institutions are now responsible for collecting and analyzing increasing amounts of data from their internal risk systems from across the enterprise. In addition, they must now consolidate and report this data for all business units so regulators can view the organization's total risk holistically.

This type of transparent, comprehensive data reporting is particularly challenging for banks who have legacy systems that operate in silos. In order to provide a holistic view of their risk, in compliance with Basel III, these banks may need to invest in sizable infrastructure upgrades.

Dodd-Frank Act

In 2010, the US federal government passed the Dodd-Frank Wall Street Reform and Consumer Protection Act in order to increase corporate transparency and protect customers from predatory lending practices. Specifically, the Dodd-Frank Act increases oversight on companies that are considered "too big to fail," and it places specific regulations on how swaps and derivative transactions are handled, cleared, and reported.

To this day, the Act remains a lightning rod for debate given the breadth of regulations that it encompasses.

The goal of the Act is well-intentioned: to provide deeper insight over systemic risk. However, the widespread regulations enacted by the Dodd-Frank Act created significant data management challenges for many organizations. For example, financial institutions are now required to aggregate, analyze, and report on enormous amounts of data from disparate sources across the industry.

In order to remain compliant, organizations need to invest in robust data management infrastructures to promote effective risk management and accurate reporting.

Know Your Customer (KYC)

"Know Thy Customer" sounds like a phrase your marketing professor probably had tattooed on his arm. But knowing your customer in a financial sense actually refers to the systematic process that companies must go through to identify and understand who their clients are prior to conducting financial business with them. KYC is not a single regulation, but instead is a term that describes a number of regulatory requirements around performing client due diligence.

In the US, for example, the Patriot Act mandates that all banks know their customers prior to doing business with them. This is a crucial step toward anti-money laundering and ensuring that banks are not funding individuals with links to terrorist organizations. As part of the screening process, client information is checked against trade embargoes, financial sanctions, politically exposed persons list, and other watch lists to ensure that they are cleared to do financial business with US organizations.

As you might imagine, KYC requires financial institutions to collect and analyze a lot of customer information for the screening process, including: names, aliases, titles, birth places, nationalities, passport numbers, and home addresses. However, inconsistent or incomplete customer information is often a challenge for many financial institutions, putting an emphasis on data quality. Many banks, therefore, have implemented data standardization processes to generate a single customer view, which facilitates client screening and allows them to onboard customers faster.

Foreign Account Tax Compliance Act (FATCA)
If conversations about tax compliance spark your interest, you're going to love FATCA. Introduced in 2014, this US government regulation requires foreign financial institutions to report taxes to the Internal Revenue Service (IRS). Currently, a tax withholding of 30 percent is enforced on dividends, interest, and insurance premiums for US-sourced income.

Although this regulation seems pretty straightforward, remaining in compliance with FATCA requires financial institutions to have robust data management infrastructures. That's because it requires them to aggregate customer information from a variety of sources. For instance, banks must compare client information against government databases to determine persons who have indicia of US status. This includes a US place of birth, a current US residence or mailing address, or a current US telephone number.

These financial institutions must also collect and manage sensitive client information, such as tax material, citizenship, residency, and account information over extended periods of time, and then they need to be able to generate reports for regulators.

The place for data management

Data management is integral to your organization's ability to remain in compliance. In order to increase oversight and transparency, today's financial institutions are responsible for collecting, aggregating, validating, and reporting on information in increasing complexity. And although many of these regulations have affected the GSIBs primarily, they will eventually trickle down to the DSIBs and smaller financial institutions.

These organizations would be wise to learn from the data management practices pioneered by the GSIBs, and begin to implement their own programs. This will likely be a collaborative effort between data stewards and members of the C-suite, including but not limited to the Chief Data Officer (CDO), Chief Risk Officer (CRO), and Chief Information Officer (CIO). Financial institutions that do not implement data management practices will likely struggle to remain in compliance, incur substantial fines, and be subject to public criticism as a result.

Creating a data management program can help your financial institution stay ahead of changing regulations and remain in compliance. With Experian Pandora's robust, easy-to-use data management features, getting started is easier than you think!

Learn more

Experian
53 State Street
Boston, MA 02109
T: 1 888 727 8822
www.edq.com

© 2016 Experian Information Solutions, Inc. • All rights reserved

Experian and the Experian marks used herein are trademarks or registered trademarks of Experian Information Solutions, Inc. Other product and company names mentioned herein are the property of their respective owners.