IBM Security

IBM

Turning the regulatory challenges of cloud into competitive advantage

How cognitive technology and frameworks are helping to automate compliance and change the game for financial services

Let's get started

IBM Security

IBM

Contents

Financial services' regulatory deluge

The regulatory and legislative fallout of the global financial crisis continues to place intense pressure on the financial industry. Not only is the volume of regulations growing, so is their complexity—a result of the diverse and inconsistent array of regional and jurisdictional mandates being imposed on financial firms. Each of the myriad of regulators and standards bodies representing national, international and state-specific interests has its own requirements and criteria. Some have conflicting requirements; others have redundant requirements but don't share the same regulatory point of view. The problem is that financial services firms need to heed all of these requirements and they need to do it quickly.

Balancing so many regulatory demands from so many different directions can be complicated and disorienting, not to mention costly. Nowhere is the complexity more evident than with cloud computing. While cloud offers financial services opportunities for new revenue, greater efficiency and flexibility, growing regulatory complexity has challenged financial firms' enthusiasm for implementing it. A 2016 Peak 10 survey found that 61 percent of financial services organizations view regulatory compliance as a major obstacle/concern for cloud adoption.[1]

Maintaining compliance with the daunting number of cloud security, privacy and data protection regulations is a major challenge, but it is also a major opportunity for the financial services industry to collaborate and establish uniform regulatory standards for cloud. Now that financial firms are accelerating their adoption of public cloud, they are actively addressing the many challenges they face from a risk and compliance point of view. One of the biggest is the labor-intensive effort required to continuously monitor the escalating number of regulatory changes. In many cases, companies are employing large staffs to do nothing but monitor the internet for new regulations and changes to existing regulations. What's more, the disproportionate allocation of resources employed to address regulatory and compliance issues leaves fewer resources for innovation and other business initiatives that could otherwise build on new cloud capabilities.

So what's it going to take for financial firms to jump through these regulatory hoops with ease? This white paper addresses that question. It explores some of the regulatory obstacles that stand in the way of cloud deployment and business growth, and it explains strategies and technologies for overcoming them.

79%

of CEOs cite over-regulation as a top threat to their organizations' growth prospects[2]

The importance of cloud governance with cognitive regulatory compliance

Organizations that have implemented public cloud can understand the importance of cloud governance for managing compliance, security, operational, strategic and financial risks. The very nature of public cloud services as amorphous, external and shared can increase those risks and necessitates that deployments satisfy stringent requirements for data protection, data privacy and business continuity. Many cloud service providers (CSPs) are not familiar with the regulatory landscape, and this adds another level of complexity for financial services companies that adopt cloud.

Cloud may be viewed as another form of outsourcing, but in heavy regulated industries, it is often seen as an extreme form. For highly regulated industries like financial services, that view translates to increased scrutiny, sweeping regulations and rigorous compliance. The resulting maze of requirements from internal and external sources governs how firms store and use data in the cloud and who can access it. Firms must understand the many regional requirements for data protection and privacy in a cloud marketplace that is not yet mature. Moreover, the ability to monitor the entire regulatory ecosystem becomes more important with cloud, not just the infrastructure that supports cloud services, but the frameworks and controls that are necessary for resilience, backup and data recovery.

The compliance challenge for financial services is especially formidable for multinational companies that must comply with the regulations of every country and jurisdiction in which they conduct business. Many financial services companies that are adopting cloud have to satisfy requirements for more than 20 regulatory jurisdictions, none of which have adopted the same requirements. However, the bigger challenge for all firms may be figuring out how to maintain continuous compliance without putting too great a burden on the way the business needs to operate. This includes the increasing reliance on human capital to manage complex regulatory demands.

Regulators have become skilled at expanding obligations through the reinterpretation of existing regulations. For the firms that have to deal with them, it is often not clear what changes need to be made to their own security frameworks, policies and controls. The task is labor-intensive because it requires considerable examination that is handled manually for the most part. Firms are forced to expend substantial time and resources to avoid regulatory jeopardy. The burden of this manual effort has proven to be a huge inhibitor to cloud adoption, and it has spurred the need for automation and simplicity.

The compliance challenge for financial services is especially formidable for multinational companies that must comply with the regulations of every country and jurisdiction in which they conduct business

Cognitive regulatory compliance uses cognitive computing, analytics and artificial intelligence technologies to drive financial services' alignment with regulators and the controls they are enforcing

While CSPs are increasingly including governance in their cloud service offerings, those mechanisms only facilitate compliance when the service is deployed. Every time a regulation changes or a new regulation is introduced, the associated security controls and frameworks need to be updated. Both CSPs and their customers are still left to figure out the corporate implications. Both need to ensure that they are compliant and that privacy and resiliency requirements are being met.

What if a firm's frameworks, policies and controls could be updated dynamically in near real time in response to changes from regulators? And what if compliance staff could be automatically notified when regulatory changes occur and receive definitive direction about their obligations and the subsequent updates required internally and by CSPs? These capabilities have come to be known as cognitive regulatory compliance, and they are actually possible today through "augmented intelligence"—that is, advances in cognitive computing, analytics and artificial intelligence.

Cognitive regulatory compliance uses these technologies to drive financial services' alignment with regulators and the controls they are enforcing. It allows firms to stay on top of regulatory changes through rigorous monitoring and automatic notification. As such, it does away with the manual processes and procedures that impede cloud adoption. It also allows financial services firms to monitor the cloud ecosystem end to end, which is essential for widespread cloud adoption.

However, cognitive regulatory compliance will require the development of an industry-standard control framework for cloud, one that supports transparency and portability between clouds so that workloads can move freely and still be secure and compliant. Such a framework would be groundbreaking, not only because of what it would accomplish but also because of how it would be built. It creates an incredible opportunity for sustained collaboration between financial institutions, regulators and technology service providers.

Financial services' industry-standard control framework for cloud and the collaborative effort required to build it are discussed in greater detail later in this paper. First: the nuts and bolts of regulatory compliance for cloud and what it all means for the financial services industry.

Consumed by global requirements for cloud

The global legal and regulatory landscape surrounding cloud is by no means static. Financial services firms continue to be consumed by regulations and standards at home and abroad. The General Data Protection Regulation (GDPR), revised Directive on Payment Services (PSD2) and Competition and Markets Authority's (CMA) requirements to implement Open Banking will all become active in 2018 and come on top of existing regulations.

The US banking industry alone must comply with regulations from the Federal Reserve Board (FRB), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency, and Consumer Financial Protection Bureau (CFPB). The burden can be overwhelming, soaking up substantial bandwidth for the majority of financial organizations. They need to understand the wide range of regulatory ramifications for cloud and ensure compliance with applicable security and privacy regulations wherever their data is accessed, stored or transferred.

Despite some geopolitical calls to reduce regulatory oversight, a series of high profile compliance breakdowns and recent cyber attacks across the financial services industry, including Equifax and the US Securities and Exchange Commission (SEC), continue to suggest that regulatory mandates will only increase. These events reinforce the need for data protection and privacy, and they amplify public pressure on the industry for greater transparency, trust and accountability.

The enormous strain on resources

Financial firms dedicate substantial resources to regulatory risk management. Even though some firms are beginning to pare down the massive compliance staffs hired following the financial crisis, compliance employees can number in the thousands. That is not surprising considering the cost of regulatory failures—USD 328 billion since 2008[3]—and the largely manual nature of compliance work.

Today a firm's compliance employees are its frontline defense against regulatory risk, painstakingly combing the internet daily for new and changing legislation, then parsing complex legal language for rules and requirements to determine the impacts on current controls. When updates are needed, they are most often made by hand. It's a costly but necessary expenditure of resources.

20%

of financial services' IT budget goes toward satisfying government mandates and regulations[4]

Consumer and data protection requirements

While many financial regulators have published opinions about cloud, the industry is lacking clear, formal guidance that is consistent across all of them. This is true for consumer and data protection, which is the focus of much of the current regulation. For example, some regulators require notification only when moving sensitive data or critical services to a public cloud. Others require notification no matter which data or services are being moved.

The result is that most financial organizations using cloud are struggling to satisfy data protection requirements from all of the regulators and across all of the jurisdictions in which they conduct business. The rules for how and where data can be stored, processed and accessed are harder to follow when they vary, and more so when data moves around constantly and crosses international borders. CSPs' servers can be virtually anywhere, which means data can be processed virtually anywhere.

The Data Protection Act governs the protection of personal information that is processed in the UK. Companies may not do business in the UK, but if they process data on servers there, they must comply with the UK data protection laws. Other countries have the same provision in their data protection laws.

The GDPR regulation, which becomes law across the EU in May 2018, shifts some of the regulatory responsibility to CSPs. It is designed to protect personal data collected for or about citizens of the EU, especially by those who process, use or exchange that data in the cloud. It requires CSPs to develop and implement a number of internal practices to protect citizens' personal data and requires greater processing transparency. It also gives regulators the right to hold companies and CSPs responsible for not adhering to the principles of the regulation. This is good news for financial firms, which have shouldered all of the responsibility for compliance to date.

Still, financial firms have much to do to meet the GDPR's new data protection and privacy regulations. They should be evaluating the legitimacy of their data processing operations and verifying existing contracts, terms and conditions and implementing appropriate controls. With a potential fine of four percent of global revenues for non-compliance, the GDPR is a top priority for financial firms, one that is expected to cost millions to address.

68%

of US companies plan to allocate between $1 and $10 million to address GDPR obligations[5]

Now the regulatory obligations to mitigate service disruption and to protect and recover data following an outage are equally imposed on financial institutions and cloud service providers

The primary privacy regulations impacting US financial firms are laid out in the Gramm-Leach-Bliley Act (GLBA). The legislation was created, in part, to stop banks from sharing personal information about their account holders with third parties without customers' explicit agreement. The law specifies handling requirements for personal data and applies to a broad range of US financial services.

Disaster recovery and business continuity requirements

Regulatory and cybersecurity demands necessitate that financial services firms pay a considerable amount of attention to disaster recovery and business continuity. Uptime and the availability of systems, applications and data are essential to daily financial operations. Regulators mandate that customer data and systems be available without fail. If an outage does occur, restoration must occur in a timely manner.

Cloud services have raised concerns about disaster recovery since the location of data is not always clear. The US-based Federal Financial Institutions Examination Council (FFIEC) states that good practices for data recoverability should be followed and appropriate plans around disaster recovery should be in place.[6] The GDPR will take it a step further. It will require that firms and their CSPs demonstrate their ability to restore availability and access to personal data.[7] In addition, firms and CSPs must regularly test their disaster recovery procedures.[8] Many of the recent cloud-based outages, such as those at Deloitte and Amazon Web Services (AWS), have reinforced the importance of having proper controls and frameworks in place to address business resiliency and disaster recovery requirements.

In the past, CSPs were typically unable to commit to the same levels of uptime that financial institutions could guarantee for themselves. Now the regulatory obligations to mitigate service disruption and to protect and recover data following an outage are equally imposed on cloud providers. The problem for CSPs is that their current control capabilities struggle to meet today's diverse and constantly changing regulatory requirements. Certainly, it would be in the financial industry's best interest to collaborate with CSPs to build a common set of cloud regulations as well as controls.

The implications of non-compliance

Regulatory violations involving data protection, privacy and disaster recovery can have severe and unintended consequences. Financial penalties and even criminal sanctions can be imposed following a breach.

Firms can find themselves liable for fines and sanctions from multiple regulators and law enforcement agencies for a single breach, with retribution based on criteria that is often unclear. In 2012, for example, an international bank paid USD 340 million to the New York State Department of Financial Services and a day later USD 327 million to the Federal Reserve. It's no wonder that nine in ten firms expect the cost of compliance to rise.[9]

There is also a less visible yet equally disturbing and potentially more lasting effect of non-compliance: a tainted reputation. Customer confidence and market share can erode quickly in the aftermath of a regulatory violation, thanks in large part to the rapid dissemination of news on social media. Reputational damage can hurt an organization strategically, leading to customer abandonment and brand avoidance.

Regulatory clarity on the upswing

While cloud regulations are becoming more plentiful, they are also becoming somewhat easier to understand and respond to. The fact is, regulators are becoming better at articulating guidance for cloud. As regulatory bodies such as the Financial Industry Regulatory Authority (FINRA) begin to leverage cloud for their own purposes, they are getting a more realistic picture of cloud security, risks and the best practices needed to safeguard critical data from exposure.

The UK's Financial Conduct Authority (FCA) "Guidance for firms outsourcing to the cloud" published in 2016 is one such example. The FCA updated its original guidelines following objections from financial firms and cloud providers. The FCA's current handbook gives firms the green light to use cloud computing and encourages firms to "agree on a data residency policy with the provider upon commencing a relationship with them, which sets out the jurisdictions in which the firm's data can be stored, processed and managed." Firms must also ensure that cloud providers do not store data "in jurisdictions that may inhibit effective access to data for UK regulators."[11]

84%

of people say breaches of data privacy and ethics causes them to lose trust in companies[10]

Shared responsibility not accountability

In a traditional data center with infrastructure deployed on premises, regulatory responsibility was owned by the financial institution and its onsite managed services provider, if one existed. Internal security and compliance teams bore the brunt of that responsibility and the risks that went along with it. Regulators held the institution accountable for maintaining a secure, compliant IT environment.

Public cloud has caused a major shift in regulatory responsibility but not accountability. Regulatory responsibility is now shared both by the financial institution and by the CSPs that deliver cloud services. This means that a single firm can share the compliance burden with a wide range of CSPs. Firms and CSPs must maintain compliance, and they must be able to demonstrate it. CSPs have to satisfy regulatory requirements for the infrastructure, platform and software services they provide, but firms are still ultimately accountable for any services they outsource. This lack of regulatory clarity is blurring the lines of responsibility and accountability for both firms and CSPs.

Accountability is one of the main principles of new cloud regulations and a heavy concern for financial firms. It creates new challenges for firms in the procurement and contracting of cloud services. It is incumbent on firms to understand the controls that CSPs will provide to meet regulatory requirements on a continuing basis, and it demands that CSPs stay informed about the changing regulatory landscape. Firms must have the processes and controls in place to supervise and monitor all of the services they source from CSPs. They have to keep records of cloud processing operations and maintain oversight of the larger cloud ecosystem which requires them to understand CSPs' subcontracting arrangements.

CSPs have to satisfy regulatory requirements for the infrastructure, platform and software services they provide, but financial institutions are still ultimately accountable for any services they outsource

Trust and assurance in the cloud

Regulators' concerns about cloud security, privacy and data protection come from a lack of trust in cloud and cloud service providers. New regulations expect CSPs to be more transparent about the controls they use to protect customer data in the cloud. Transparency is key to building trust in CSP services.

New regulations increasingly stipulate that financial services contracts with customers (for loans, accounts, insurance policies and so on) need to spell out how customers' personal data and privacy will be managed and protected in the cloud. Firms need to communicate that information to customers in a clear and concise manner, and they need to gain customers' consent for all processing operations that involve their personal data. Undoubtedly CSPs will play a big part in fulfilling those obligations. Regulators and firms alike want greater assurance that CSP security and privacy practices meet compliance standards. However, it's not enough for CSPs to talk about their security controls. They need to be able prove it by offering greater transparency of their operating environments.

Transparency through self-assessment

Security and privacy certifications and frameworks have proven to be some of the most effective means of increasing trust in cloud and CSPs because they allow for greater transparency. A prime example is the Security, Trust and Assurance Registry (STAR), launched by the non-profit Cloud Security Alliance (CSA). STAR gives CSPs a platform to assess and report their cloud controls and their compliance with the best practices, standards and regulations across multiple domains relevant to customers and regulators. It makes CSPs' compliance information publicly available in a registry that firms can use in their decision-making process.

STAR certification identifies cloud providers adhering to best practices and validates the security and compliance posture of their cloud offerings. Several of the most well-known CSPs, including Amazon, IBM, Microsoft, HP, Red Hat and Symantec, participate proactively in STAR for the purposes of market differentiation and to simplify their customers' assurance processes.

Solving the regulatory compliance challenge

While steps have been taken to ease the regulatory compliance burden for financial services, these measures have done little to alleviate the cause of the problem. The volume and diversity of new regulations inundating compliance departments is consuming too many resources operationally and financially. Certainly, solving this regulatory compliance conundrum is not easy. But it is possible and, in fact, a solution is already underway.

IBM sees it as a two-pronged solution. The first prong answers the desperate need for an industry-standard framework for cloud regulations. Standardizing regulator requirements for controls, policies and processes will enable firms to simplify and automate many of the manual tasks involved in compliance today. The second prong brings together key industry participants to build the framework. Sustained collaboration between financial services firms, regulators and technology providers is essential to hammering out the components of the industry-standard framework and then leveraging the right technologies to build it. Cognitive systems, including artificial intelligence and machine learning, are the engines behind better, more efficient cloud governance. These technologies help make cognitive regulatory compliance possible.

Building an industry-standard cloud control framework

Today there are multiple security and controls frameworks for cloud from a variety of standards organizations, including Control Objectives for Information and Related Technologies (COBIT), International Standards Organization (ISO) and National Institute of Standards and Technology (NIST). These frameworks establish standard processes for implementing cloud security. They were designed to help organizations integrate controls into their operation to manage cloud risk. They weren't designed to manage the barrage of regulations hitting organizations today, with their tangle of standards and conflicting requirements.

The lack of a single, agreed-upon regulatory standard for cloud hampers day-to-day compliance efforts. More importantly, it hinders wide scale industry adoption of cloud and limits what automation can do to replace manual tasks and improve efficiency. If industry-standard regulatory requirements and controls could be established for cloud, and agreed to by all regulators and standards organizations, then it would be possible for firms to access regulatory requirements and controls from one central library. They could learn about new regulations and changes to existing regulations from one place. They could update their own policies and controls in a more uniform way and stay compliant more easily. That is the mission of the industry-standard cloud control framework for financial services—to provide the foundation for simplified and continuous compliance against a constantly changing regulatory landscape.

The industry-standard cloud control framework for financial services is fundamentally a repository of regulator-sanctioned controls and requirements for cloud for each country, jurisdiction and use case. It also factors in CSP and software as a service (SaaS) native controls and proprietary frameworks. The industry-standard framework is cloud- and vendor-agnostic: applicable to any cloud services from any cloud provider. This allows firms to avoid lock-in to specific services or providers. Firms' workloads can move more freely between clouds and still maintain their compliance—helping deliver on the promise of hybrid cloud.

The industry-standard cloud control framework spells out standard controls for deploying new regulations, modifying existing regulations and notifying firms when updates are required to their internal frameworks. Internal frameworks mirror the industry standard but allow each firm to customize for their own corporate policies, standards and procedures.

When a regulation is changed or a new regulation added to the industry-standard framework, firms would be alerted automatically. Their internal frameworks could tap into the industry-standard framework to access the updates. The automated process would eliminate the need to manually search for regulatory updates. Instead, firms could use their time reviewing updates and identifying whether any internal policies, requirements or controls need to be changed.

The goal is to get to a point where firms are in complete alignment with their regulatory obligations, where all of firms' regulatory obligations worldwide are continuously and rigorously monitored and updated automatically in response to changes from regulators. Firms would be able to access the industry-standard library as a utility service, as needed, to dynamically adapt to and consume updates to policies, requirements and controls and still maintain their own proprietary policies, requirements and controls libraries, as shown in Figure 1.

The goal is to get to a point where firms are in complete alignment with their regulatory obligations, where all of firms' regulatory obligations worldwide are continuously and rigorously monitored and updated automatically in response to changes from regulators

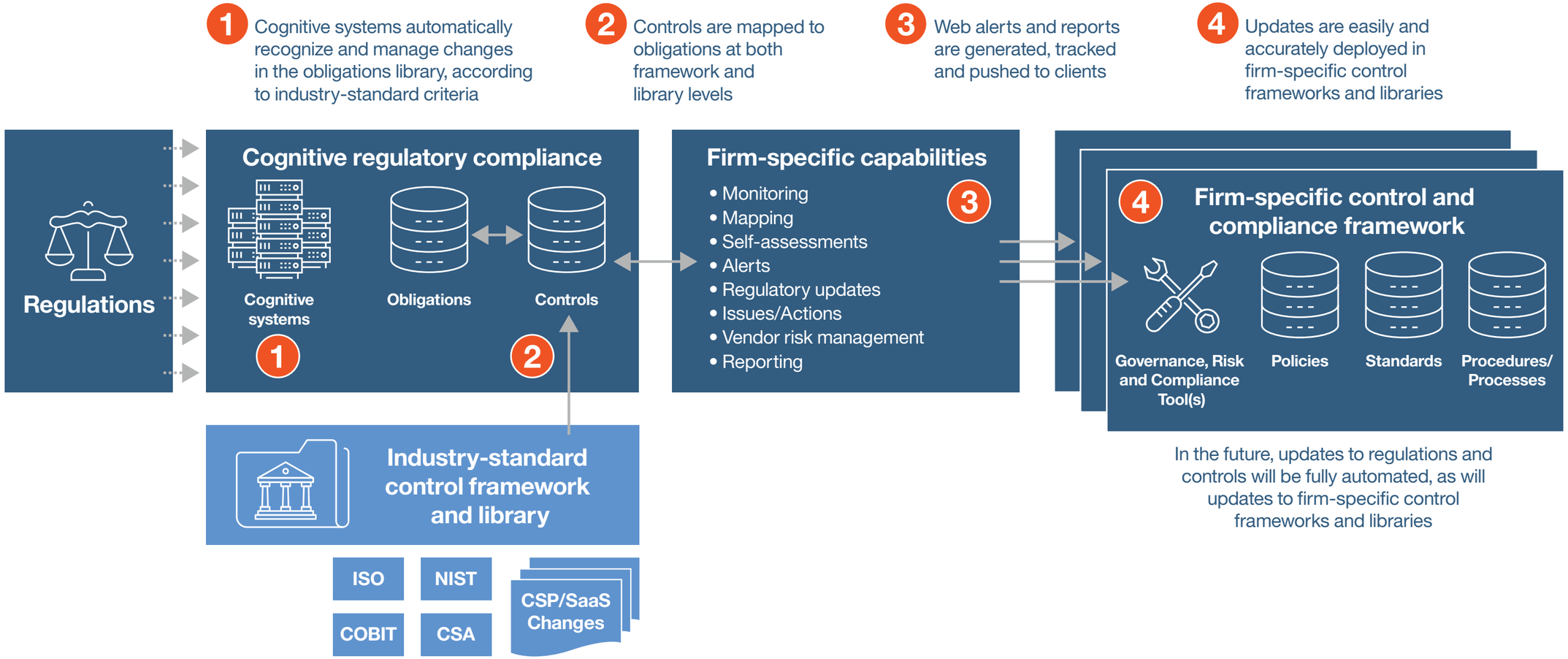

Figure 1. ***Cognitive regulatory compliance model at work.*** *Cognitive tools like artificial intelligence, machine learning and predictive analytics allow new regulatory obligations to be identified and assimilated into industry-standard frameworks and controls in near real time.*

Financial services firms, CSPs and regulators all want more streamlined governance, and all recognize the answer lies in standardizing the current excess of regulatory controls and requirements and then automating compliance

Collaborating for a common goal

Financial services firms, CSPs and regulators share a common objective when it comes to cloud. All want more streamlined governance, and all recognize the answer lies in standardizing the current excess of regulatory controls and requirements and then automating compliance. Collaboration is the best and most pragmatic way to accomplish that objective.

To that end, IBM launched a groundbreaking initiative in May 2017 to build an industry-standard cloud control framework for financial services. The hope was to create a working group of financial services stakeholders who would join together to create a standard regulatory framework and controls for the financial services industry. As of this writing, within a few months' time, 30 financial services organizations have agreed to participate in the project.

This strong show of force is indicative of the industry frustration with regulatory compliance and the urgent need for a solution. In fact , all but two of these firms have identified regulatory compliance as the number one obstacle to cloud adoption. All want to take greater advantage of public cloud but worry that any economic gains will be negated by the high cost of compliance. So they have eagerly agreed to lend their support and knowledge to this game-changing initiative for the financial services industry. The group's objectives are to:

- Define and agree on industry-specific regulatory standards, policies and controls for all off-premises services including cloud-based services, infrastructure as a service (IaaS) and platform as a service (PaaS)
- Establish an industry-standard governance framework that serves as a central repository for agreed-upon standards, policies and controls
- Make the completed industry-standard framework available to the industry as a whole

Steps every firm should take

Financial services' migration to public cloud is inevitable, even and especially for mission-critical business applications. It's critically important for firms to know their regulatory risks. A regulatory compliance assessment can uncover these exposures and improve an organization's risk posture. In addition, every financial firm also has an opportunity to lessen the compliance burden of cloud by working more closely with regulators and cloud service providers. Those that do will be in the best position to affect how regulators understand and legislate cloud services.

Assess regulatory compliance risk

Given all of the global regulation for cloud, it's hard for firms to be certain that they're in complete compliance. Performing a regulatory compliance assessment helps firms identify and mitigate gaps in compliance. A good assessment identifies external and internal risks, security requirements, and business continuity and resiliency requirements for cloud. It also determines whether current security and control frameworks are meeting regulatory mandates, such as data location and privacy regulations, in all relevant countries and regions.

Engage with regulators to shape requirements

Instead of relying on regulators to determine regulatory standards and requirements, financial services firms can and should help shape the policy discussion by working with regulators and educating them about cloud and security. This can lead to better regulation and policies that foster cloud innovation. Additionally, firms can get a leg up on upcoming requirements and the implications for their compliance operation and their business.

Negotiate cloud services contracts and compliance

When it comes to compliance, the onus is on financial services firms, not cloud providers. Firms need to make sure compliance obligations are being upheld by CSPs, and that can be challenging due to inconsistencies and a lack of transparency in CSPs' regulatory approaches and their interpretation of data protection requirements. Furthermore, getting CSPs to commit to a specific location for data storage and processing can be extremely difficult. They want the freedom to shift data to different servers for load balancing and to take advantage of lower costs.

Financial firms have justifiably expressed concern about executing CSP contracts with inadequate service levels and vague regulatory commitments. Firms need to do their due diligence and use tools like STAR to assist in CSP selection. Leading providers are taking steps to help their financial services clients meet regulatory obligations. These providers are increasingly bundling compliance services into their offerings to satisfy requirements for the GDPR, GLBA, Basel, Payment Card Industry Data Security Standard (PCI-DSS), Sarbanes Oxley and others.

Once firms have chosen a CSP, they need to negotiate each party's compliance responsibilities rather than blindly accepting what CSPs are offering. Roles, responsibilities and risk exposures for data protection should be spelled out definitively. Firms need to take the lead in understanding data privacy and security regulations, specifically those related to cross-border data flow and localization, and use that knowledge to impact the execution of quality CSP contracts.

Why IBM?

IBM has long supported financial services with innovative security solutions tailored to the needs of the day. We understand the extraordinary compliance challenges facing the industry, and we are developing cognitive regulatory strategies and technologies to help address to them. These transformative RegTech solutions are radically changing how firms manage compliance and driving down the cost by introducing efficiencies never before possible. They are enabling firms to satisfy their security and legal obligations dynamically with far less operational and financial risk. In that way, they are enabling firms to use compliance as a competitive advantage.

IBM's initiative to create an industry-standard cloud control framework for financial services is just one of many cognitive solutions helping firms overcome the complexity and momentum of regulatory change. IBM® Watson® Financial Services offers a suite of cutting-edge governance and compliance solutions. The services use the machine learning and analytics embedded in Watson to help transform regulatory surveillance and visibility; speed the identification, understanding and deployment of new regulatory requirements; and streamline ongoing compliance efforts.

All of these services are designed to mesh seamlessly with the IBM Security portfolio, which provides an integrated suite of advanced enterprise security products, services and intelligence to help organizations holistically protect their infrastructures, data and applications against all manner of physical and cyber threats. Today IBM operates one of the world's broadest security research, development and delivery organizations, monitors billions of security events each day in more than 130 countries and holds more than 3,500 security patents.

Join the initiative and learn more

Are you ready to help transform regulatory compliance for the financial services industry? To learn more about the IBM-led initiative and become a member of the regulatory compliance working group for financial services, contact Gary Meshell, Worldwide Financial Services Sector Security Leader, at gary.meshell@ibm.com

To learn more about IBM security and compliance offerings, please contact your IBM representative or IBM Business Partner, or visit:
ibm.com/security

Follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog

About the author

Gary B. Meshell is a recognized thought leader in the areas of security and cloud within the financial services industry. He has worked with a number of large insurance companies, international banks and investment management companies, supporting the design and implementation of their hybrid cloud and security programs. Gary is currently the global sales and business development leader for IBM Security for the financial services sector.

IBM Security

IBM Security
75 Binney Street
Cambridge MA 02142

Produced in the United States of America
October 2017

WGW03347-USEN-00

1 "The Peak 10 Financial Services and IT Study: Tackling the digital transformation," Peak 10, October 2016.

2 "Redefining business success in a changing world: CEO Survey," PwC, January 2016.

3 "Banks Trimming Compliance Staff as $321 Billion in Fines Abate," Bloomberg, March 22, 2017.

4 "How Cloud is Being Used in the Financial Sector: Survey Report," Cloud Security Alliance, March 2015.

5 "Pulse Survey: US companies ramping up General Data Protection Regulation (GDPR) budgets," PwC, 2017.

6 "Business Continuity Planning," FFIEC IT Examination Handbook, February 2015.

7 "GDPR Series: Part 12 – Security of Personal Data and Breaches," Lexology, May 16, 2017.

8 "The GDPR's impact the cloud service provider as a processor," PDP Journals, Volume 16, Issue 4, 2017.

9 "Global Regulatory Outlook 2017: Opinions on global financial services regulations and industry developments for the year ahead," Duff & Phelps, 2017.

10 "20 years inside the mind of the CEO…what's next?" PwC, 2017.

11 "FG 16/5 – Guidance for firms outsourcing to 'cloud" and other third-party IT services– Finalised guidance," Financial Conduct Authority, July 2016.