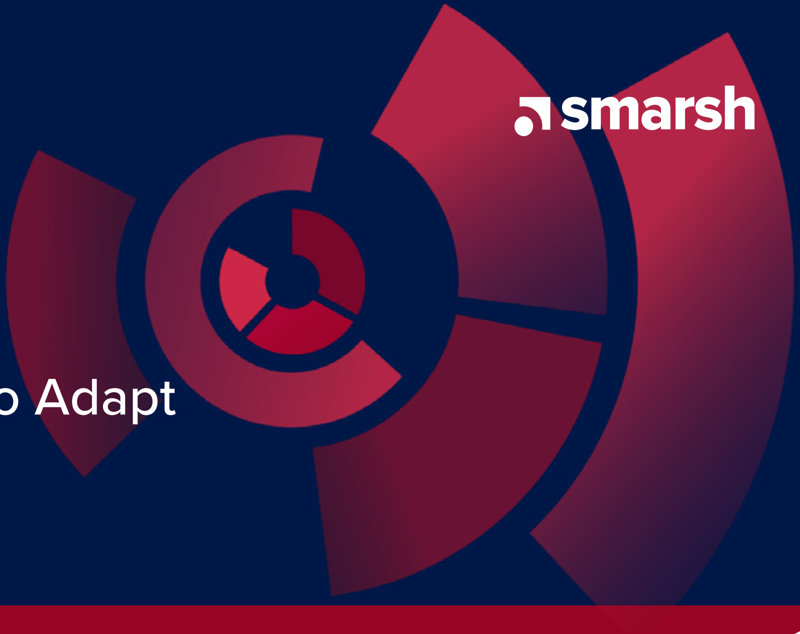
State of Supervision

Inability of Current Systems to Adapt

By Gregory Breeze



Between a Rock and a Hard Place

The inability of supervision systems to adapt has placed financial services firms in a difficult position. A recent survey of 400 CEOs in financial services[1] indicated that regulatory compliance is one of the top two concerns that can impact their businesses. For those compliance and IT organizations that must work together to tackle the compliance obligations of electronic communications supervision, there are multiple trends converging to make life challenging. Many of these factors are related to seismic shifts in the technology landscape. These are greatly exacerbated by both a rapidly evolving regulatory environment and dramatic changes in compliance software.

Think of it this way: each technological advancement, whether it be related to cloud storage, artificial intelligence, or advanced analytics, for example, brings its own unique set of migration, deployment, and integration challenges – as well as corresponding risk to mitigate. Unfortunately, the expectation from compliance executives is that solutions to manage that risk can be rapidly deployed, include bulletproof security, and cover a broad set of mobile devices and communication methods — all while reducing costs. It's a lot to ask, even if those risks and compliance obligations remain static, which they don't. The supervisory challenges created by the conflict between technology and compliance include:

- The adaptions to cloud computing
- The evolving regulatory landscape
- Understanding the impact Office 365 has on archiving and supervision
- Stricter regulations on data breaches and personal data privacy

The Adaptions to Cloud Computing

The rapid adoption of cloud services represents one of the most significant shifts in the history of the technology industry. In Financial Services, this trend has recently accelerated. A year and a half ago, a large percentage of financial institutions were reluctant to consider moving any data from on-premises applications due to security and privacy concerns. Now, it is difficult to find any FinServ organization that is not at least in the planning stages of a migration to the cloud.

At the same time, organizations are still governed by stringent security requirements that, in many cases, assume required levels of control available only in on-premises deployments. The challenge comes when trying to apply perimeter-focused security requirements that were defined for on-premises infrastructure to newer, cloud-based services.

It's not that cloud-based systems are insecure. In fact, a strong case could be made that modern encryption requirements, an army of security consultants, and intrusion detection systems leveraging machine learning infrastructure makes some cloud environments more secure than the on-premises infrastructure of most organizations.

The even bigger challenge is the interoperability of existing supervision applications with new, cloud-based collaboration systems. For example, will IT need to route all my messaging traffic to cloud-based repositories, only to re-route a copy to my existing on-premises supervision app? The added traffic, routing complexity, and inability to eliminate on-premises infrastructure adds risk and greatly diminishes lower cost/improved manageability value proposition of the cloud. For organizations that need to address interoperability challenges related to the supervision of data, it becomes critical for IT to evaluate third-party supervision solutions that provide different cloud deployment models (such as multi-tenant and private cloud options), and have a track record of success working with multiple Microsoft communication and collaboration tools. Flexibility and the ability to work seamlessly with broadly accepted cloud-based communications applications is critical to fully leverage the cloud.

The Evolving Regulatory Landscape

FinServ organizations must continually adapt to an increasing number of regulations, across multiple jurisdictions, with occasionally conflicting requirements. Factors complicating the compliance landscape include:

- Over 100 regulations that are introduced or changed each day[2]
- Different geographies with unique regulatory requirements
- Time frames for responding to audits that have compressed from weeks to days
- Stricter regulations on data breaches and personal data privacy

Legislation and regulatory enforcement of new data protection and privacy rules are changing quickly across the globe. These new restrictions, and the heavy fines that potentially accompany them, are creating a significant impact on the cybersecurity, privacy, breach notification, and data storage strategies of multi-national institutions.

Sometimes, these regulations can appear to be in conflict. This adds significant complexity in complying with regulations in different jurisdictions. Consider the European Union (EU) General Data Protection Regulations (GDPR). Even if your organization does not have a physical presence in the EU, collection of personal information from EU citizens can make your organization subject to GDPR, which necessitates a facility for deleting an EU citizens' data. However, SEC 17a-4 requires that any communications for regulated brokers or traders be stored immutably. This has caused firms to spend a good chunk of the past two years mapping data sources and ensuring that anything they capture and retain is done so solely for the business purpose of meeting regulatory requirements in order to meet GDPR provisions. It also means that an organization's supervision solution must allow for flexible options for data storage (both WORM and non-WORM) as well as deployment in different geographies globally.

The Impact Office 365 has on Archiving and Supervision

As is the case for other industries, Microsoft Office 365 is disrupting the email messaging and archiving marketplace. For those currently using a legacy email archive such as Dell/EMC, Veritas or Micro Focus for end-user access to historical content, adoption of Office 365 has produced an acceleration of 'end of life' product announcements, as well as decisions from those vendors to curtail investment in development and support for these products.

However, large enterprises with sophisticated compliance requirements continue to need more. Financial Services firms face the most pressing need for third-party compliance solutions, as many are now faced with a time-sensitive need to replace their current archive or supervision system which is being sunset. Any viable replacement option must deliver robust supervisory capabilities to be ready to meet proof of supervision requirements whenever the regulators call — now and into the future — as new content sources, regulatory mandates, and policies evolve. New supervisory systems must also provide an extensible data model that supports any communication type in its native format and provide open APIs for third-party applications for add-on capabilities. Because of the feature specialization, workflow complexity, and financial service regulatory domain knowledge required, use of third-party vendors with focused investment in supervisory review are a better source for ongoing innovation, as opposed to attempting to leverage a platform that is focused on serving the needs of the broader marketplace.

Defining the Role of Artificial Intelligence

Many organizations are looking to leverage artificial intelligence (AI) as a possible replacement for current supervision systems. While these new offerings provide a compelling story and offer great potential for surveillance applications, the products are still fairly immature and require significant training to identify potential risks.

Additionally, many of the vendors in the RegTech space are startups from the world of academia, rather than established vendors with a track record of success in the financial services compliance market. Simply put, *they don't know what they don't know*, which will require a steep learning curve to ensure they provide the basic functional requirements at the scale required by today's financial services firms.

One key area of concern with this new wave of surveillance technology is that the analysis that is enabled by training AI is a poor fit for the current regulatory obligations to supervise communications. Supervision requires the processing and review of large volumes of communications in a very short period of time, utilizing lexicons and contextual filters to find ***known*** risks, while eliminating false-positives. Application of these technologies to investigate and correlate disparate data sources to identify previously ***unknown*** risks requires significant training and investment.

Ultimately, supervision and surveillance systems should be interoperable and enhance one another. For example, a supervisory system can identify a point-in-time policy infraction related to insider trading. Data related to that infraction can be fed to a surveillance application to assess behaviors and patterns over time – and feed that insight back to the supervisory system for future policy refinement.

The conflicts of technology and compliance can seem insurmountable, but will be addressed by changing the way that firms view applications like supervisory review in the future. We will discuss the attributes and specifications that firms should be prioritizing in our final post.

1) https://home.kpmg/xx/en/home/campaigns/2016/06/ceo-outlook.html
2) https://www2.deloitte.com/us/en/pages/regulatory/articles/banking-regulatory-outlook.html

Gregory Breeze - Principal, Information Governance Practice, has over 25 years' experience in IT, focused primarily on data management and information governance solutions. He currently assists Smarsh enterprise customers to solve complex governance, risk and compliance challenges. Greg previously held Subject Matter Expert and Director-level technologist positions with HP/Autonomy, Iron Mountain Digital and Mimosa Systems. Greg's expertise in compliance, retention management and eDiscovery began by helping leading storage vendors bring object-based platforms to market.