Banking Communications Governance and Reporting
A RegTech Use Case
Table of Contents

Introduction

Banking Communications Governance and Oversight: The Business Problem

   Regulations and Communications Recordkeeping
   Why Govern Communications? LIBOR Currency Market and Interest Rate Scandal

Hitachi Vantara Solutions for Communications Governance

   Capabilities that Help Address the Rigors of Global Communications Governance
   Business Value and Return on Investment (ROI)

Next Steps to Improved Communications Governance

Appendix: RaboBank, a Communications Governance Case Study

   The Solution
   The Outcome
For financial services organizations, managing regulatory risks is a must. The financial services sector is experiencing rapid changes driven by far-reaching initiatives, such as Anti-Money Laundering (AML) regulations, GDPR, FATCA, CRS, Dodd-Frank, Basel III, MiFID II, MiFIR and EMIR II. These regulations impact all key stakeholders in the financial services sector and have profound implications for corporate risk, compliance and operational strategies. Multinational organizations face additional levels of complexity as they must comply with the regulatory requirements of every jurisdiction in which they operate.

Over time, compliance challenges have become even more acute as industry consolidation has left many financial services firms with intricate organizational structures and siloed infrastructure. This complexity can make it problematic to apply a unified approach to the rules that govern geography, communication type, line of business and product specifics within communications governance. As a result, the costs associated with risk operations, compliance and audit (ROCA) have continued to climb.
One of the main challenges for risk and compliance officers is their ability to access, gather and interpret data at the center of an investigation in a timely manner. For instance, access to some data may require assistance from outside the risk or compliance organization, creating dependencies on IT or other groups that can impede the response. Involvement of other groups may also hamper investigations because those groups may not use uniform data gathering processes, which can compromise the accuracy of conclusions. The massive volumes of unstructured and nontraditional data (for example, social media, video) pose new types of challenges for compliance teams and legacy systems. Even if the data integrity is sound, analysis can be arduous and time-consuming due to the limited capabilities of legacy systems and technologies.

Clearly, new digital tools, processes and methods are required to help speed data aggregation, reduce reliance on nonessential resources, improve accuracy and enable better decision-making.

Fortunately, emerging RegTech solutions hold the potential to help financial services organizations accelerate productivity and control costs by moving from tactical and manual solutions to more strategic, automated and digitized processes. Even though they are nascent, these solutions are delivering new methods for addressing some of the most time-consuming and perilous compliance-related functions, including:

- How to investigate, monitor and proactively prevent market abuse across the organization.
- How to adhere to constantly evolving rules governing over-the-counter (OTC), stock market, foreign exchange and futures trading, and detect breaches quickly.
- How to reduce the time required to conduct investigations from months or weeks to days, minutes or even in real time.

By leveraging new data ingestion, integration and analytics technologies, RegTech solutions can more effectively and efficiently address investigations, fraud prevention and regulatory requirements. While some financial institutions are already applying RegTech solutions, recent innovations in predictive analytics, data visualization and artificial intelligence (AI) offer an exciting glimpse into the future of how RegTech may truly transform the industry.
Key RegTech Characteristics

**Intelligence**
Discern value from information and apply rules to information mobility based on content and relevance.

**Centralized Control**
Apply policies globally or individually to any data stored on your system. Extend controls to determine how data from edge devices, such as ATMs, is backed up, synchronized and shared.

**Security Measures**
Apply security policies simultaneously in the data center, the cloud, or at the network edge. Dictate the who, when and where of data access and exactly how mobile data can be throughout its life cycle.

**Compliance-Related Features**
Quickly and reliably detect anomalies or unauthorized data behaviors. Act quickly to remediate breaches and mitigate risk.
Today's financial services organizations must adhere to strict recordkeeping requirements regarding trading activities. These mandates extend to the recording and capture of all forms of communication in relation to a single trade or transaction.

Recent regulations such as MiFID II and MiFIR are imposing strict rules concerning the recording, surveillance and assurance of digital and voice communications. The monitoring of communication and trading patterns in banks has become more extensive, with a variety of new risk management guidelines, recommendations and technical standards.

It is necessary for compliance officers to analyze communications between traders, trading partners and customers. They must also consider actual communications associated with pretrade, trade and post-trade activity, the transactions of employees, and the transactions of a bank for its own account.

1 According to Celent Research, 75% of accountholders assessed being able to see all their finances in one mobile app as “highly valuable.” This was higher even than the value given for the ability of online transfers.
As part of a banking or financial institution's operational risk management program, trade communications oversight and governance is a major area of concern for compliance officers pursuing investigations around market abuse. New regulations have expanded the requirements, and oversight has had to expand beyond traditional email and phone records to include new types of unstructured data such as text, social media and video.

As a result, compliance officers require the ability to operate on a variety of data types. Enterprise search with analytical and business intelligence tools is therefore critical and must be able to effectively scale to handle ever-increasing amounts of content in very specific categories and time frames.

With respect to a number of specific infringements, MiFID II makes appropriate administrative measures available to regulators, including bans against members of the management body and other responsible individuals, and maximum fines of up to 10% of total annual turnover (in the case of legal persons), at least EUR 5 million (in the case or legal or natural persons), and at least twice the benefit derived, where this can be determined. Competent authorities may impose sanctions exceeding these amounts or additional types of sanctions.²

² MiFID II Fact Sheet http://www.linklaters.com/pdfs/mkt/london/MiFID2-Fact-sheet.pdf
Regulations and Communications Recordkeeping

The wide scope of industry regulations targets several key objectives:

1. Market integrity.
2. Investor protection.
3. Abuse prevention.

The Dodd-Frank Wall Street Reform and Consumer Protection Act is among the most comprehensive regulations that have had a sweeping global impact. Dodd-Frank introduced recordkeeping and mobile recording requirements that have presented new challenges for many financial institutions.

The Dodd-Frank Act permits the imposition by the Securities and Exchange Commission (SEC) of civil monetary penalties in addition to cease and desist orders. These provide considerable advantages to the SEC, such as the absence of juries in administrative proceedings, the absence of meaningful pretrial discovery and motion practice in administrative proceedings, and less strict application of the rules of evidence during administrative trials. Additionally, for cease and desist proceedings instituted under the Securities Act, the Dodd-Frank Act adopted the existing three-tiered penalty grid, but raised the penalty amounts by 50%.

For instance, under the “oral recordkeeping” requirement of the act, all companies operating or doing business with an organization in the U.S. for certain regulated trading activities have to record all communications from mobile devices that lead to a trade.
Different entities are responsible for setting rules to comply with the broad “Oral Recordkeeping Requirements” framework created by Dodd-Frank Wall Street Reform. For instance, the Commodities Futures Trading Commission (CFTC) and the SEC may issue rules in response to Dodd-Frank.

Additionally, Dodd-Frank requires that each futures commission merchant, retail foreign exchange dealer, introducing broker and member of a designated contract market or swap execution facility (SEF) keep full, complete and systematic records of all transactions relating to its business dealings in commodity interests and related cash or forward transactions. The Final Rule includes a requirement for such records to be maintained in a “form and manner identifiable and searchable by transaction.”

**Why Govern Communications? LIBOR Currency Market and Interest Rate Scandal**

The 2008 LIBOR currency market and interest rate rigging scandal related to manipulation of interbank lending rates highlighted the importance of monitoring digital conversations between traders. As detailed in the plea agreements, these traders used their exclusive electronic chats to manipulate the LIBOR rate in different ways. The ramification of this circumstance led to the Financial Conduct Authority (FCA) shifting supervision of the LIBOR away from the banks and into oversight of the Intercontinental Exchange (ICE) Benchmark Administration. It also led to six banks agreeing to pay nearly $6 billion to the U.S. Justice Department and other regulators.

“The U.S. Department of Justice intends to vigorously prosecute all those who tilt the economic system in their favor; who subvert marketplaces; and who enrich themselves.”

Loretta Lynch
Former U.S. Attorney General
Today’s financial markets are heavily regulated, through a myriad of interlinking global regulations. Preventing market abuse and insider trading by collecting, curating and analyzing communications among employees, traders and other market participants is a must. A solution is needed to centrally capture, curate and consume all regulated employee communications across the front, middle and back office.

Hitachi understands the issues and concerns organizations face when trying to protect critical information. We focus on understanding our customers’ business requirements and priorities and tailor our solution offerings accordingly. We also rely on innovative research and development (R&D) initiatives and partner with select technology providers from around the world.

Hitachi Vantara technologies support compliance efforts by improving visibility into all communications streams, including SMS, chat, email, social media feeds and voice recording.

*Three Key Areas of Communications Governance.* Effective communications governance strategies consider the full breadth of data use and employ sound methods for maintaining compliance across all phases of the data life cycle.
Capabilities That Help Address the Rigors of Global Communications Governance

Hitachi Vantara technologies can help enable secure and compliant communication aggregation across multiple channels, including voice, video, messaging and electronic trading, regardless of location or device. Our technologies form a scalable, flexible foundation for the future of communications governance and reporting, helping deliver capabilities that include:

- Support of multiple application workloads that are important to lines of business.
- Intelligent search across all digital and voice communications to significantly reduce time and manual error during searches.
- Proactive monitoring of all communications to automatically raise alerts on noncompliant activities and enable faster resolutions.
- Reconstruction of all trade communications via the different channels to ascertain or ensure that corporate policies were maintained; proactive fraud and data breach detection by compliance officers.

Hitachi Vantara also helps financial services organizations comply with regulations, such as Dodd-Frank and MiFID II, that require a comprehensive approach to communications recording and recordkeeping. In this way, organizations can automatically analyze the content of interactions and categorize them according to various risk management questions, such as:

- What was a conversation about?
- Did certain conversation patterns occur?
- Did the trader comply with all regulations?
- Were corporate policies followed?

Each module of the Hitachi Vantara framework provides additional capabilities for a structured risk management process and helps firms to establish complete control over regulated employees’ communications.
Business Value and Return on Investment (ROI)

Hitachi Vantara brings business value to communications governance by helping financial institutions efficiently and proactively aggregate all digital and voice communications data across multiple channels. This capability helps banks and financial services enterprises detect illicit activities such as market abuse violations, insider trading and customer front running.

With the right tools, compliance officers can take a proactive approach to monitor and reduce the risk of regulatory penalties, that can include personal criminal and financial liability and reputation damage to the enterprise. Hitachi Vantara assists financial services organizations by providing tools that help dramatically reduce investigatory time and effort, as well as investigation and auditing resources. At the same time, Hitachi Vantara solutions enhance compliance coverage and meet regulatory burdens, all without the need for manual retrieval and archiving.

By leveraging advancements in artificial intelligence, machine learning and modeling techniques (for classification and anomaly detection), it is possible to proactively monitor communications data streams and multiple data sources so compliance officers can identify risks and take action before serious noncompliance events occur.

**Mitigating Risk with RegTech Solutions.** Much of the business value associated with communications governance solutions stems from risk management, but it also offers an opportunity to consistently strengthen the enterprise through strategic measures that can uncover value, even as they help ensure compliance.
Regulation is changing how financial services firms govern, monitor and prevent suspicious and fraudulent activity and market abuse. Compliance officers in every financial institution are looking for next-generation toolsets, skillsets and mindsets for digitizing compliance.

New expectations for proactive communications surveillance and compliance assurance solutions are gaining attention, especially as companies seek to eliminate breaches of internal controls and policies that result in considerable fines and potentially irreparable damage to corporate reputation.

Digital transformation of compliance creates new requirements for the investigative tools that constitute the management framework and for the “bottom-up” processes of risk identification, assessment, management, reporting and supervision.

RegTech solutions deliver business value by:

- Reducing costs and resource expenditure by empowering compliance officers with automated capabilities.
- Maximizing protection by monitoring all communication and presenting indicators for potential risks.
- Providing comprehensive compliance monitoring based on sophisticated data search and analytics.
- Decreasing penalties by implementing an automated risk management solution.

Learn more about how Hitachi Vantara helps financial services firms manage compliance obligations in the era of RegTech.
Headquartered in Utrecht, Netherlands, the banking and financial services company Rabobank serves more than 10 million customers in 47 countries. Employing over 51,000 people worldwide, Rabobank manages around EUR 674 billion of assets and reported a net profit of EUR 2.1 billion in 2015.

Walter Hendriks, change manager for global compliance at Rabobank's Financial Economic Crime Unit, explains: “Rabobank, like all financial institutions, is subject to a wide range of strict government regulations in each of the countries in which it operates. With banks facing evermore scrutiny since the 2008 financial crisis, and with new regulations always on the horizon, we wanted to enable a solution that would be rapid, flexible and comprehensive for current and future compliance investigations.”

**Challenge**

Give compliance teams the tools to work more effectively and flexibly on regulatory investigations.

**Solution**

Build an “ingest and search” data platform based on the Hitachi Content Platform to transform compliance operations.

**Outcome**

Provide auditable life cycle, control and structured access to large volumes of nonstructured communication data to reduce the burden of compliance.
“Previously, IT, on behalf of Rabobank’s Global Compliance Group, gathered communications data from multiple sources in multiple countries,” adds Colin Chatelier, head of Data Center (U.K.) and Global Storage at Rabobank. “This might include email, recorded voice calls, instant messaging and chat applications, as well as Instant Bloomberg and Eikon Messenger from Thomson Reuters. A time-consuming, resource-intensive and error-prone task.”

Chatelier continues, “When the compliance division needed to examine a particular set of corporate actions, we collected the data from these diverse sources: some from third-party vendors, and some held on backup tapes. If an inquiry changed scope, we might have to search the same systems with different criteria. We wanted to address the problem of consistently mining multiple data sources spread across many disparate silos with no obvious way of joining one communication type to another by helping compliance teams work more flexibility and collaborate more easily.”

The Solution

To search for and retrieve digital assets more efficiently, Rabobank engineered a solution that would collect every piece of relevant data into a single place.

By creating a central repository, Rabobank could complete compliance investigations without the need to return to source systems, even if the investigation scope changed. Further, the data could be correctly managed, with compliant access control, audit trails and automated policy-driven deletion. Secure audited retention at the object level replaces the need to throw a retention blanket over the entire data silo.
In a project sponsored by the Global Compliance Group, the company approached Hitachi to build a cutting-edge ingest-and-search platform based on Hitachi Content Platform (HCP) technology. This solution was expected to automatically collate, secure and index both structured and unstructured data across the business.

As data are ingested into HCP, they are simultaneously indexed and made searchable. Data are then separated by source, such as email or voice, and by country. In this way, access and retention policies can be applied according to the requirements of each jurisdiction.

“\nThe regulatory landscape is constantly shifting. The HCP solution enables compliance investigations to be completed rapidly and securely, across global business units. Most importantly, HCP gives Rabobank control of its data, with a flexible, comprehensive solution and the ability to meet future compliance needs.\n
Walter Hendriks
Change Manager for Global Compliance, Rabobank Financial Economic Crime Unit

Overlaying this system is an easy-to-use, interactive web interface that enables investigative searches by pre-approved individuals of the compliance teams. The solution allows Rabobank’s Global Compliance Group to define its own queries, and only the right people on the right teams have access to the data sources relevant to their investigations. Additionally, because the solution is based on a single, comprehensive data store, all potential data sources, such as email, voice, SMS, documents and more, can be screened to ensure proper regulatory compliance.

To ensure solution resilience, two HCP appliances run as an active-active pair, one in the Netherlands and one in the U.K.; should one site suffer a catastrophe, the other HCP system simply continues uninterrupted. This twinned arrangement acts as a backup and archive for all the local systems, removing a major headache for the IT team. Simultaneously, the high-availability HCP pairing ensures that a comprehensive, consolidated record of bank interactions is always accessible for compliance investigations.
The Outcome

With the HCP-based ingest-and-search platform, the global compliance group has simplified access to the data needed for investigations, which is now at its fingertips in a single, central portal.

“The HCP solution has significantly improved the efficiency and flexibility of investigations and cut the time needed for discovery searches from weeks to hours,” says Chatelier. “Approved users can get all the data they need from their desks, and simply get on with their jobs, without having to ask for help from IT. The compliance team is able to work more effectively and efficiently, while reducing the workload impact on IT staff.”

He adds, “As a result, the IT team is released from administrative data search and retrieval tasks and can move to proactive business matters. The HCP solution gives us control over the uncontrollable. As an immutable source of data, compliance teams can be safe in the knowledge that information has not been altered in any way. Data held in the HCP solution is complete, comprehensive and auditable. It allows us to both prevent deletion and apply automated, irretrievable erasure according to compliance policies.”

Given the success of the project, Rabobank plans on adding further data sources to the platform, including trading applications messaging and Skype for Business.

“With our HCP-based solution, Rabobank is setting a new standard for compliance investigations in the banking sector. We are confident that other institutions will follow in our footsteps,” says Chatelier.

“The regulatory landscape is constantly shifting. The HCP solution enables compliance investigations to be completed rapidly and securely, across global business units. Most importantly, HCP gives Rabobank control of its data, with a flexible, comprehensive solution and the ability to meet future compliance needs,” Hendriks concludes.
Take These Next Steps

- **Support more content**, data types and access points for deeper data insights with Hitachi Content Platform.
- **See the results** from ESG Lab’s Test Drive Evaluation of Hitachi Content Platform Anywhere.
- **Support cloud deployments** in your core data center with Hitachi Data Ingestor.
- **Discover Hitachi solutions** for your organization’s digital transformation.
  Access e-books, guides and other tools.
- **Join our content mobility community** for easy access to our latest blog posts, webinars and videos.