Modernizing mobile supervision at enterprise scale

May 2023

Background and recent developments

The increased adoption of multiple communication channels (e.g., mobile phones; text messages, app-based chat platforms, video collaboration tools) is forcing compliance and supervision programs to be nimble and flexible in order to easily respond to changes. Firms are increasingly implementing automated monitoring solutions that support emerging communication channels. Some firms continue to supplement their programs through the use of manual procedures such as random sampling reviews to select voice communications and monitor them on a periodic basis or based on market events.

In response to this shift, the Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA) and the Commodity Futures Trading Commission (CFTC) have opened a series of inquiries into how firms are tracking their employees' electronic communications (e-comm). There was enhanced regulatory scrutiny in 2022 as the SEC and CFTC announced fines of $1.8b in September 2022 against 15 global banks and one affiliated investment adviser for widespread and long-standing failures by the firms and their employees regarding their use of unapproved communication channels. Since then, many asset managers (AMs) have received letters from the SEC about their e-comm programs. Additionally, regulators have signaled that the current investigations are the first of many and that financial institutions and investment advisors should be prepared for additional scrutiny.

Statistics (as of 2022)

Mobile

300%[1] — Increase in mobile capture post- vs. pre-COVID-19

Text analytics

5.4[2] — Average number of hours spent every day on mobile devices based on industry resources

Employee survey

262[3] — Number of times the average person checks their phone every day

Industry drivers

Regulatory scrutiny

- Enhanced regulatory scrutiny around e-comm oversight programs.
- 15 global banks fined $1.8b.
- Multiple asset managers received letters from the SEC.

Device decisions

- Broker-dealers (BDs) are increasingly moving toward corporate-owned devices.
- Asset managers with BD arms are leaning towards BD device policies.
- Pure AMs favor bring your own device (BYOD).

Cost vs. risk

- Corporate-owned higher costs (device, service and software license) but potentially less compliance risk.
- BYOD has lower upfront costs but raises oversight complexity and compliance risk.

Ease of doing business

- BYOD is more business-centric and more friendly to mobile apps.
- A corporate-owned policy is risk-centric and can be restrictive to business.

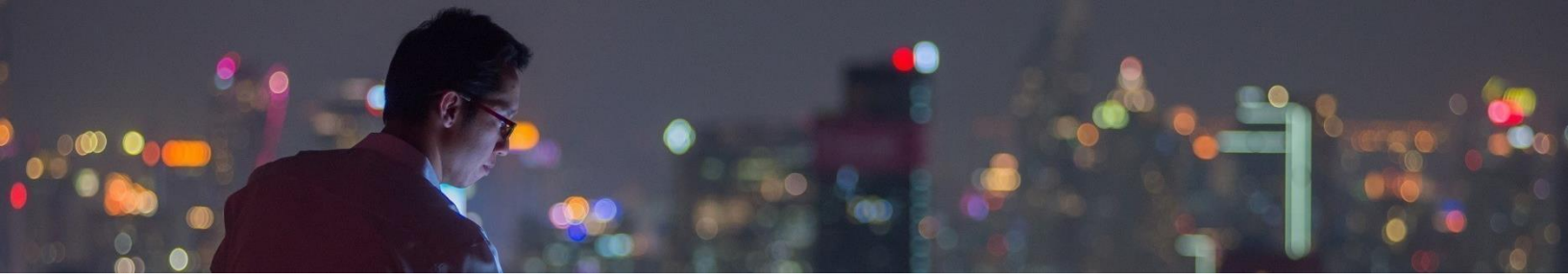
Prohibition vs. permission

- Employees can't use communication tools for business purposes unless compliance teams believe they can sufficiently mitigate the risks via capture and storage technologies, policies and procedures, and training.

Spend

- BDs are spending more up front on devices and making significant investments in data capture, retention and monitoring to augment their current systems.

[1]Smarsh Internal Analysis
[2]"How Much Time Does the Average American Spend on Their Phone in 2023?" *TechJury*, April 19, 2023.
[3]"2023 Cell Phone Usage Statistics: Mornings Are For Notifications," *Reviews.org*, May 9, 2023.



Key industry challenges

Emergence of new communications tools

Firms must stay informed about new capabilities, social media platforms and other trends that may impact their business to stay ahead of the curve.

Ineffective technology and cross-regulatory harmonization

Legacy systems do not allow for certain data types to be presented accurately, making it more difficult to meet protocols for different regulations across regions.

Inadequate control framework

Control frameworks may be inadequate due to outdated venue inventory or ad hoc venue management frameworks across different e-comm channels.

Inadequate data retention policies

Retention policies may not reflect the capabilities of mobile and social apps, which impacts oversight effectiveness.

Policy/culture

"Frequent change"/communications tools frequently add new features and change methods of access, which requires resources to stay current.

Ineffective testing and monitoring

Insufficient reviews, testing, checks and challenges outside of the first line of defense (LOD) to monitor for use of unapproved channels.

How firms are addressing the challenges

Spending has increased significantly in the last few years to enhance governance and oversight, data capture, data management and retention capabilities, and overall monitoring.

Oversight

- **Enhancing oversight functions** to address recent regulatory scrutiny
- Increased focus on **clearly defining roles and responsibilities** (R&R), governance, enforcement, policies and procedures, and how technology enables change management activities
- Develop **clear policies and procedures** that are well defined and accessible to all employees

Data management

- **Focus on data quality, completeness and enrichment as a prerequisite for applying smart automation to downstream monitoring processes**

Monitoring

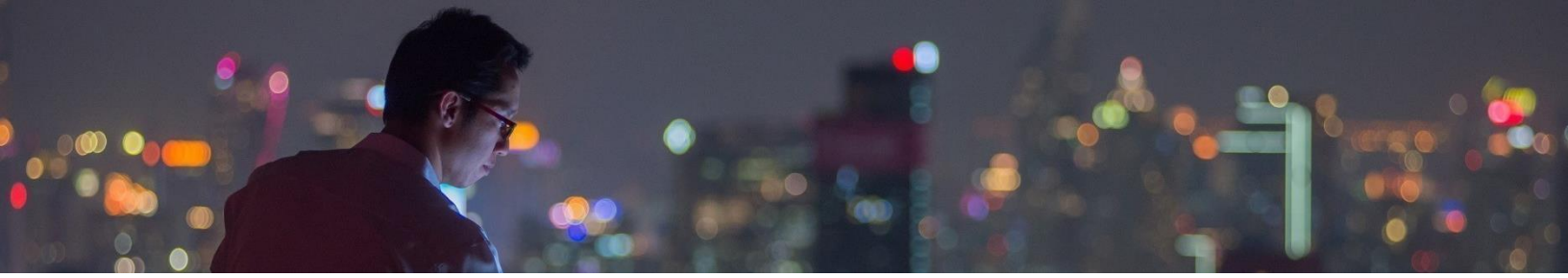
- **Consolidating data retention platforms with a shift towards a strategic vendor**
- **Increased focus on disposal policy – records maintained past their retention date increase not only costs but also risk**

Data capture

- **Significant investment is being made in this field**
- **Consolidating data capture platforms with a shift toward a strategic vendor that provides capabilities for an evolving e-comm environment**
- **While firms continue to look for vendors that detect unapproved channels with limited success, some have resorted to prohibiting channels altogether as an interim solution**
- **A consolidated data capture platform would reduce the risk of data redundancy and save on storage space, thus improving system processing efficiency**

Data retention

- **Centralized e-comm surveillance monitoring process with dedicated resources specializing in communication compliance review**
- **Shift towards offshore service models to manage cost and scale as channels for monitoring increase**
- **Periodic review and evaluation of lexicon policies to ensure effectiveness and leveraging machine learning (ML)/natural language processing (NLP) or artificial intelligence (AI) to assist in managing volume/false positives or anomaly detection**
- **Investments in automated workflow solutions for case management and metrics reporting to gauge the health of the surveillance program**



Impact

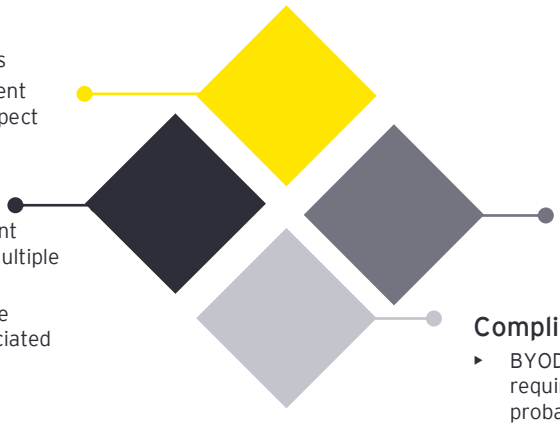
Along with other functions in an organization, Compliance must work closely with in-scope businesses to understand the changing business landscape, and how it is impacted by regulations. It also helps make effective decisions as regulatory changes from governing bodies are not a "risk-only" decision. They impact other functional areas such as Technology, Business and Operations as well.

Business stakeholders

- BYOD has ease of doing business
- Certain regions may have stringent employee and target client/prospect communications preferences

Operations

- BYOD generally has lower upfront cost but higher cost to surveil multiple languages
- Multiple applications may require multiple data archives and associated surveillance capabilities



Technology

- Location of supervisory staff and data storage locations; ability of supervisory technology to understand communication modalities and data volume
- Technology either needs to support the application inventory for company-owned devices or help build a broader set of capture platforms for BYOD

Compliance

- BYOD has high risk associated with the investment required to achieve the desired level of risk mitigation, the probability and expected size of enforcement action, and the presence of other risk vectors (privacy, InfoSec, IP)

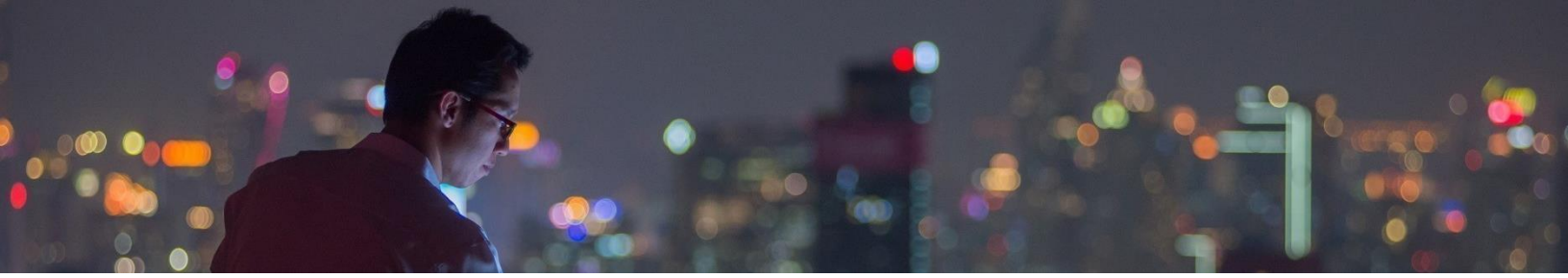
Key decisions to implement an optimal e-comm oversight solution

The following decisions and implications should be considered as firms look to evaluate the effectiveness of their own data capture, retention and monitoring capabilities – with each decision having its own risk and cost implications. As an example, the language policy is generally the smallest focus area of the six key factors, but it can have significant impacts on costs, risks and operations. Though AM functions within banks typically mirror the bank's BD policy, which is trending towards corporate-owned devices, pure AMs are moving towards BYOD with an ability to restrict applications and opting for the business platforms of third-party mobile applications for capture. This requires firms to implement solutions that can capture mobile SMS/text and data from app-based chat platforms and video collaboration tools.

Decisions and implications

Key decisions	Additional implications
Device Broker-dealers are moving towards corporate-owned devices while asset managers who initially favored CYOD (choose your own device) now prefer BYOD or corporate-owned personally enabled (COPE).	**Oversight/supervision** Firms define written supervisory processes including choice of sampling, lexicons and/or analytic models to provide oversight.
Applications Firms make decisions to support or prohibit communications tools based on assessments of business benefits vs. the ability to mitigate risk. Additionally, firms assess the ability to capture and retain modalities (e.g., persistent chat, voice, video, collaborative authoring) available in each communication tool.	**Privacy** Firms determine policies, aligning user groups with data privacy protections required within each geographic region.
Languages The decision to limit the number of approved business languages or to allow a broader set of languages can have a significant impact on risk and costs. Nuances in jargon, dialect, etc. can often require additional lexicons or models.	**Archive** Firms are examining storage capabilities to meet updated 17a-4 requirements while providing performance to address today's communications data volume and variety.

Note: Regardless of the decisions made, the risk of individuals using unapproved devices and applications is still present and firms are building additional controls to manage this risk. Attestations and training are generally not considered to be controls by regulators.



Illustrative industry spectrum

Firms that trend toward the more restrictive end of the spectrum tend to choose more stringent policies across the board compared to firms with less stringent policies. However, in certain cases, even less restrictive firms are considering enhanced risk mitigants in the near term. Application policy, device policy and language policy all interplay in that; regardless of which level of restriction is chosen, the ability to manage the risk compounds.

Wealth managers

Allow BYOD and multiple applications to meet communication needs

Asset managers

Prefer BYOD to have flexibility to do business, which increases compliance risk and the cost of data capture, retention and monitoring

Private equity

Restrictive approach to prevent the loss of confidential data and regulatory fines

Hedge funds

Restrictive approach to prevent sharing fund strategies, confidential data and regulatory fines

Less restrictive

More restrictive

Investment advisors

Focused more on client communication and preferences and, therefore, have less-restrictive policies

Retail

Mix of both BYOD and corporate-owned devices to have flexibility to do business as needed

Broker dealers

- Restrictive approach due to recent regulatory scrutiny and fines
- Corporate-owned devices offer them better control and data security

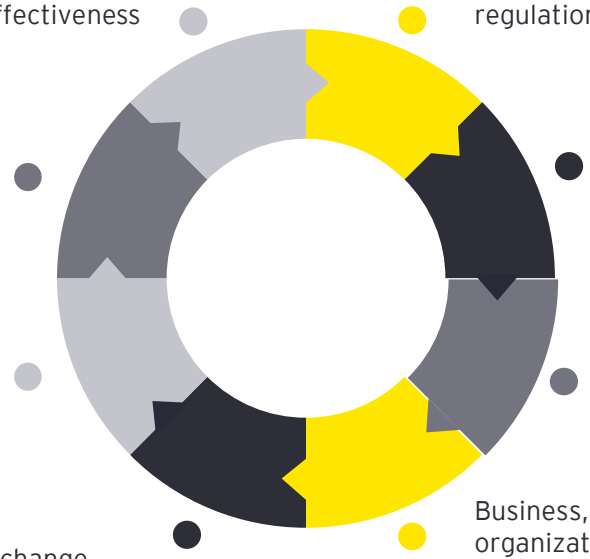
Note: The above represents a composite of the respective sectors. Individual firms, depending on their risk profile/tolerance, program maturity and technology architecture, may behave differently.

What should firms do?

Evaluate existing models and data sets to review alert quality and assess the compliance program's design effectiveness

Perform a review of the existing understanding and interpretation of regulations relevant to the business

Review current policies and procedures regarding surveillance and retention



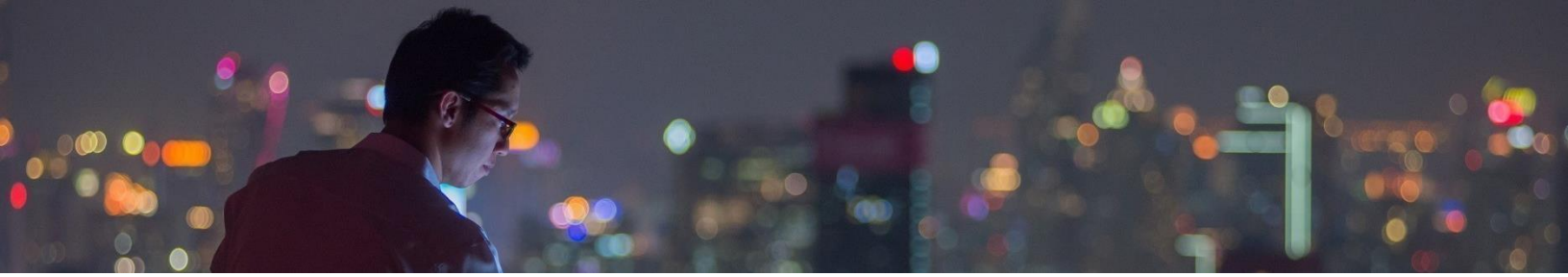
Conduct compliance assessments aimed at identifying gaps and perform enhancements to policies and controls to better align with regulatory and legal requirements

Assess the company's voice and e-comm supervision/ surveillance capabilities and seek improvements both from a procedure and system point of view

Assess the mapping between relevant regulation and oversight controls

Build and maintain an effective change control process to anticipate and respond to changes in business, technology, regulation and behavior

Business, Compliance, Technology and Risk organizations need to work closely and make effective decisions earlier in the new/changed business and product approval processes



Illustrative use case: monitoring population

Regulators have been clear that **infractions can happen anywhere across the business** – from regulated users to compliance staff to senior executives.

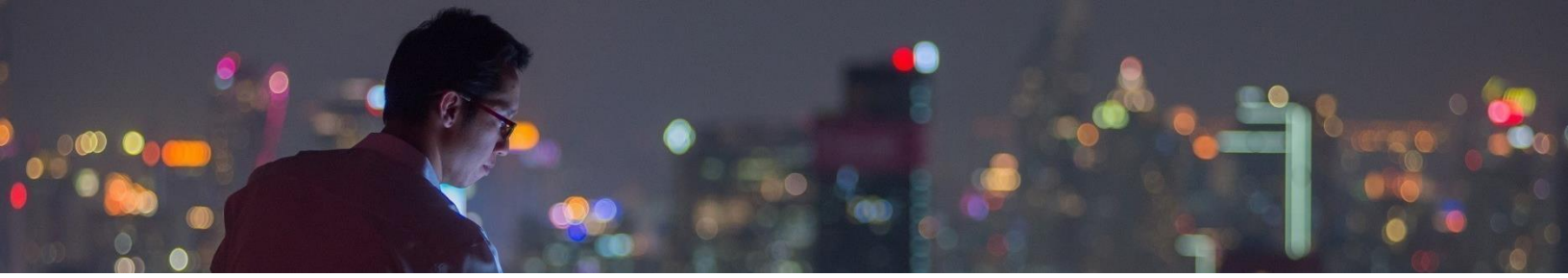
While applying monitoring to an entire organization raises numerous data privacy, scale and logistical concerns, firms can consider borrowing from the processes, infrastructure and workflows established to regularly monitor regulated users and apply them to other segments of the business.

Monitoring may not follow the same frequency or published written supervisory procedures (WSPs) but **can be leveraged** on a less-frequent basis to periodically inspect communications to spot potential red flags that surveillance and investigative teams can pursue further. Monitoring for false positives and negatives and continuously looking for improvements in existing lexicons/policies to ensure the **effectiveness of the program** can be achieved through a combination of trend analysis, statistical methods and ML/AI capability.

Monitoring communication channels is an integral part of ensuring the security and integrity of financial institutions. In fact, regulators have stated that all communications regarding "the business as such" should be considered under not only the **recordkeeping obligations** but also the firm's **supervisory obligations**.

Firms must decide on **how different groups of employees** should be captured, retained and monitored in their organization. **Multiple factors** should be considered such as region, role, hierarchy and exposure to confidential data. Less advanced, or mature, firms typically manage joiners/leavers/movers through performing manual checks, whereas more mature firms employ automated checks to track movers'/joiners' details.

Regulators have enforced the failure to record and supervise not only external communications but also internal communications. By capturing, retaining and reviewing your firm's internal and external communications, you not only meet your regulatory obligations but you are given the needed data to provide valuable insights into your business. By excluding seemingly administrative communications, you run the risk of not only a compliance gap but also not gaining insights into possible communications on unapproved channels.



Illustrative use case: data capture and retention

For most firms, the question of saying "yes" can start with an assessment of whether there are **technologies available in the marketplace** to safely and securely capture and store those communications in order to meet recordkeeping obligations to preserve "compete and accurate" records.

This may be a choice of the native capabilities of communications tools themselves, including their ability to provide capabilities to retrieve historical content and metadata at required throughput along with the accompanying certifications and attestations that **demonstrate the skills, proven processes and data protections that are sufficient** for the requirements of financial services.

Those capabilities may be provided by **specialized third parties** that have proven engineering resources to leverage existing application programming interfaces (APIs) or other methods of access to ensure that the modalities required by users (e.g., voice, video, collaborative authoring) can be preserved. This is **complemented** by the ability to store and retrieve that content to meet regulatory requirements, including SEC 17a-4, as well as the ability to meet on-demand requests from regulators with the speed, security and accuracy to address high-speed, high-value content requests.

Mobile devices complicate capture strategies

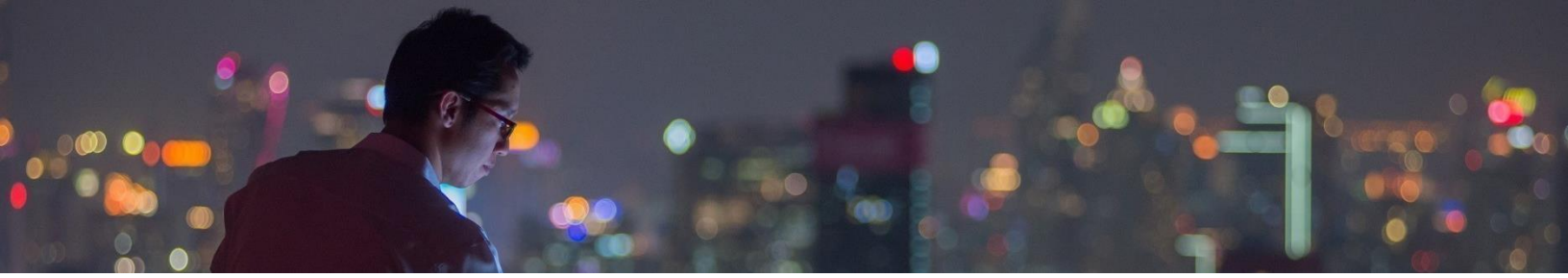
- Prospective clients, brokers, advisors and compliance staff are regularly remote, and the common denominator is often a mobile device to connect at least one party that is in an uncontrolled location.
- The challenge for firms is to **determine the optimal strategy to segregate** and control these communications.

Collaborative technologies create the challenge of keeping up

- App-based chat platforms and video collaboration tools add the complexity of keeping up with an ever-expanding set of features and modalities that can easily extend beyond the boundaries of existing compliance controls.
- **Voice, video, AI, collaborative authoring** and other features may be released before existing controls can catch up or before proven APIs or other methods of content capture can be tested and validated.
- **Content vendors can change licensing requirements** for data that is being extracted from those systems.
- **Firms need to remain diligent in staying close to content providers** or rely upon third parties that have the dedicated expertise and focus to minimize the gap between collaborative technology innovation and compliance controls.

Breaking down silos can help you reduce risks and improve compliance

- Moving larger and more heterogeneous data objects across supervisory workflows has created an enormous strain on IT systems, which has caused **many firms to move toward a rationalization of control points, rationalizing information silos** in favor of aggregated views across content sources.
- Firms can begin this journey by inventorying and evaluating all the communications channels currently in use.
- **Moving towards a centralized data platform** that can aggregate multiple, disparate content sources to feed supervisory and conduct surveillance applications.



Illustrative use case: monitoring unapproved communication channels

Unapproved electronic communication channels have emerged as a prevalent risk in business communications in both internal and external communications. This poses a challenge to firms in the inventorying, tracking and monitoring of such communications and increases the risk of nonconformance with various regulations and internal guidelines related to recordkeeping, data privacy, personally identifiable information (PII)/personally sensitive information (PSI) and supervisory controls. Firms need to increase focus on how to identify and manage these communications while at the same time applying tighter controls to prevent the usage of unapproved e-comm channels. Below are focus areas that firms should prioritize when developing a successful monitoring program.

5-step cycle

1. Policy

Identify risk themes and typologies associated with the usage of unapproved e-comm channels, leverage risk coverage assessment and identify gaps which need to be remediated, and pinpoint avenues to integrate e-comm monitoring across the trade lifecycle in the organization.

2. Data

Retaining data in accordance with regulations for surveillance and recordkeeping purposes of approved and unapproved tools used for e-comms within the organization helps improve overall data quality.

3. Technology

App-based chat platforms, video collaboration tools, text messages and other new methods of communication can be leveraged to capture data. A firm should evaluate current e-comm surveillance tools for model coverage and add/enhance as required as it looks to integrate the surveillance tools in trade lifecycles across multiple groups.

4. Process

Activities such as qualitative and quantitative review of the models, output, and data for optimization and improving effectiveness can improve risk coverage and data gaps with periodic assessment and validation.

5. Culture

Firms must understand not only whether individuals are following policies but also why they might not be. Similarly, even if controls are working, risk, compliance and technology functions need to be ready to make rapid changes to support the business.

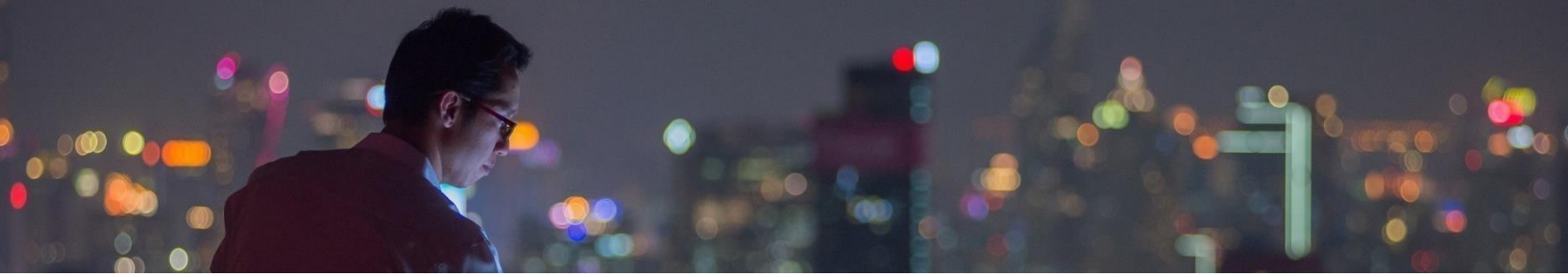
Key enablers

Policy

- Conduct periodic policy updates based on cadence and trigger events
- Obtain periodic attestations from supervisors
- Conduct cyclical trainings

Data, technology, process

- Data patterns and behavior analytics using trading and comms data to Identify outliers. Significant deviations in trading and comms patterns can point to potential red flags
- Trade reconstruction by combining trade and comms data to identify unauthorized channel usage
- Update lexicon library to capture references to unauthorized channels in comms (e.g., "connect on WA" in voice comms). Retrain NLP models to identify nuances indicative of masking behavior

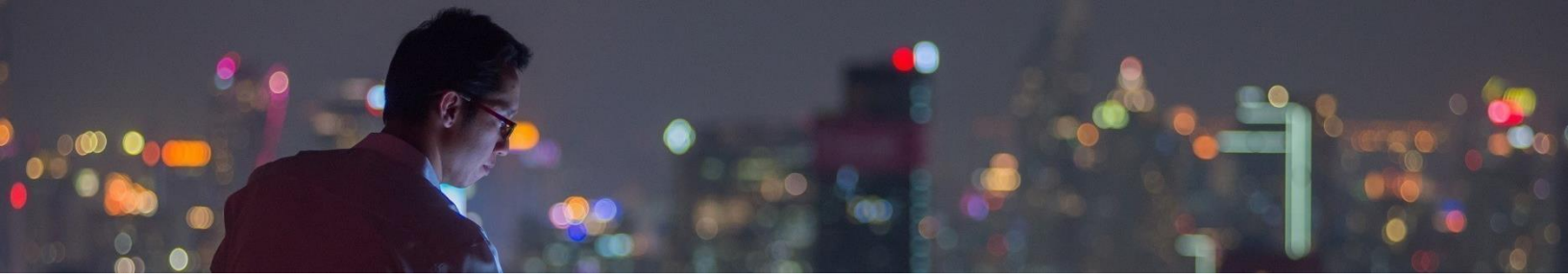


Key takeaways

The increased adoption of multiple communication channels has led firms to **implement automated communications monitoring solutions** that support emerging communication channels, and **regulatory scrutiny around electronic communications oversight programs has increased**. To stay ahead of the curve, firms need to be informed about new capabilities, social media platforms and other trends that may impact their business. Firms need to **stay vigilant in monitoring changes** to permitted collaborative platforms and features, as well as licensing requirements for data extraction.

To address current challenges, firms are **investing heavily in enhancing their oversight functions; consolidating data capture and retention platforms;** focusing on data quality, completeness and enrichment; and centralizing electronic communication surveillance monitoring processes with dedicated resources specializing in communication compliance review. These efforts **require clearly defining roles and responsibilities, governance, enforcement, policies and procedures**, and leveraged technology to enable change management activities.

Unapproved electronic communication channels pose a significant challenge for businesses as they are difficult to track and monitor. This increases the risk of noncompliance with regulations and guidelines related to recordkeeping and supervisory controls. Developing a **successful monitoring program for off-channel communications requires firms to prioritize data, technology, policy and process**. This includes retaining data in accordance with regulations, leveraging technology to capture data, identifying risk themes and typologies associated with unapproved electronic communication channel usage, and optimizing processes through periodic assessment and validation.



Ernst & Young LLP and Smarsh contacts

EY

Robert Mara
Principal
New York, NY
robert.mara@ey.com
+1 212 773 1025

Abhishek Chaki
Senior Manager
Hoboken, NJ
abhishek.chaki@ey.com
+1 201 551 5120

Anuj Puri
Senior Manager
Hoboken, NJ
anuj.puri@ey.com
+1 201 551 6197

Devarajan Kootam
Senior Manager
Hoboken, NJ
devarajan.chithrakootam@ey.com
+1 201 551 5298

Smarsh

Robert Cruz
VP, Information Governance
San Francisco, CA
robert.cruz@smarsh.com

Tiffany Duncan-Magri
Regulatory Advisor
Tampa, FL
tiffany.magri@smarsh.com

EY | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

US Score# - 19877-231US.

2304-4219445
ED None

ey.com