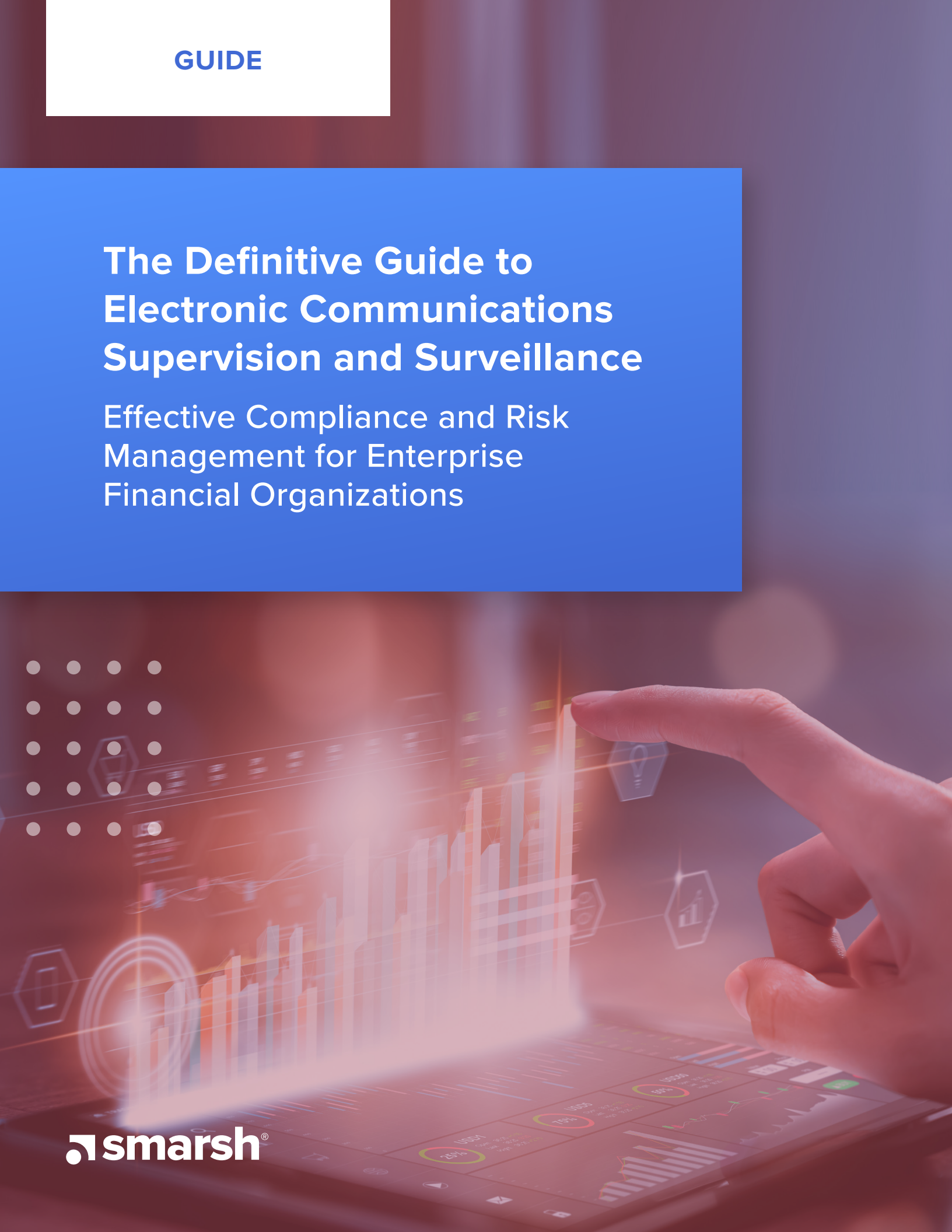
GUIDE

The Definitive Guide to Electronic Communications Supervision and Surveillance

Effective Compliance and Risk Management for Enterprise Financial Organizations



smarsh®

Overview

The supervision of electronic communications is foundational to maintaining regulatory compliance and mitigating risk. However, an organization's supervisory and surveillance processes deserve renewed focus. Making regulatory supervision more effective and efficient requires robust, user-friendly technology. As businesses lean more heavily into collaboration tools that enable hybrid work, financial services organizations need a single supervision and surveillance system with policy controls that can quickly and accurately identify and mitigate red flags. The solution must also make the review process less complicated for compliance teams.

Supervision is more than just a necessity. Applied holistically, electronic communications supervision can enable other business functions and company strategies. Unfortunately, a clear understanding of the benefits and risks of available supervision and surveillance technologies is often missing from the overall compliance strategy.

Additionally, outside of financial services, many non-regulated organizations seek to monitor business-related electronic communications. These organizations can leverage supervisory and surveillance technologies to increase visibility into their information assets, monitor behavior, and manage areas of risk.

Under the pressure of an ever-increasing volume and diversity of communications data, staying on top of supervision is a distinct challenge. Evaluating technology options to streamline, automate and improve the supervision process by adding a surveillance solution doesn't always get prioritized, despite its importance.

The Definitive Guide to Electronic Communications Supervision and Surveillance is a comprehensive resource filled with relevant definitions, considerations and guidance for developing effective, high-value supervision and surveillance systems. It focuses on managing and supervising electronic communications in a modern, highly regulated financial services organization. In addition, it explores the increased use of supervision and surveillance tools by non-regulated industries. This guide also covers when to consider implementing a single system of supervision and surveillance — using the surveillance component to spot new risks quickly.

Get the tools and information needed to understand the compliance risks and benefits of today's various communication channels. Become familiar with the latest supervision and surveillance technology options and be able to evaluate and improve your existing supervision and surveillance solutions to support business objectives.

Table of Contents

Introduction

What is "supervision?"

"Supervision," the First Line of Defense (1LoD), refers to the inspection of communications of registered representatives and investment advisers according to the firm's written policies. This includes regulations such as FINRA 3110, SEC 206(7), IIROC Rule 29.7 (Canada), FCA Chapter 9 (UK), and FCA Chapter 10A (UK). Regulators do not mandate that firms use an explicit policy, nor do they mandate with what frequency communications need to be reviewed. Regulators only require that firms create and follow their written supervisory policies and that procedures (WSPs) are designed to reasonably prevent violations of securities laws. The result is a wide variety of supervisory practices, from manual inspection and random sampling to risk monitoring.

What is "surveillance?"

"Surveillance," the Second Line of Defense (2LoD), refers to the oversight of 1LoD to uncover anomalies and trends to identify risks and opportunities. The supervision regulations also apply here regarding looking for red flags to detect and prevent violations. AI/ML is another tool to amplify supervision and surveillance teams' ability to uncover hidden risks in huge datasets.

What are "electronic communications?"

In the context of this guide, "electronic communications" is a term that refers to the communications generated by regulated firms for business purposes that therefore need to be supervised. This includes any electronic data — emails, chats, text messages, posts, recordings, emojis, application or document sharing, and attachments — transmitted entirely or partially digitally. Electronic communications can be sent using a variety of different communication channels, including email, IM & collaboration, conferencing technologies, mobile, voice and social media.

Why is specialized electronic communications supervision technology important?

Inspecting communications of registered broker-dealers and investment advisers is a well-established compliance business process for every financial services firm. Today, financial services firms must keep pace with complex and evolving domestic and international regulations, and a rapidly changing risk landscape (e.g., security, privacy, financial risks, and internal threats). At the same time, as communication channels emerge and evolve, employees are adopting new tools for connecting with clients and partners.

Every new collaboration tool or messaging application, such as Zoom, Microsoft Teams, and WhatsApp — also known as multi-modal communications solutions — adds more complexity to virtual supervision. These solutions are complex due to their use of video, mobile, text, IM components, and other features such as file attachments and emojis. These solutions are "persistently on" and generate large, complex data files, making it difficult to conduct supervision because conversation threads constantly change, lasting days, months or years. Many firms do not have the technology solutions they need to adopt and monitor these new channels — and maintain regulatory obligations.

Key strategic considerations for supervision

There are several important considerations that financial firms should bear in mind when evaluating their supervision strategy, including:

- The all-too-common mismatch between legacy supervisory review technologies and today's dynamic, multi-modal communications
- The challenge of getting past the status quo by moving from familiar yet outdated supervisory systems to modern approaches
- The tendency to "set it and forget it" when it comes to internal lexicon policies and off-channel communications reviews of solutions like WhatsApp, Telegram, Signal, or WeChat
- The over-emphasis on the mechanics of review versus the higher-value focus on reducing information risk
- Compliance teams using lexicons want a more efficient method for reviewing electronic communications, especially with multimodal communications which generate large volumes of communications with big data files that outstrip existing review solutions

- They want to use AI/ML to reduce the “false positives,” allowing them to focus on other compliance tasks while simultaneously increasing the effectiveness of the review by increasing the “true positives” found within the system.
- The increased demand for firms to proactively inspect communications of non-regulated employees to identify potential data loss and ensure that information assets are adequately protected
- The growing proliferation of advanced analytics technologies and the resulting definitional ambiguity between supervision (determined by pre-defined rules) and surveillance (identification of anomalous behavior)
- Operational issues including the increased demand to proactively inspect high-risk products sold to older clients, surfacing and addressing employee conduct concerning sexual harassment and bullying, geopolitical issues such as cybersecurity threats and Ukraine sanctions. Also, for firms looking to “do more with less” to reduce or maintain a flat headcount and cover more surface area with mergers or expansions
- An all-in-one supervision and surveillance workbench system that improves the compliance team’s efficiency without sacrificing effectiveness

Each of these conditions has made the discussion of supervisory review more complex than a simple examination of email review lexicons and workflows. These conditions also explain why the “failure to follow written supervisory procedures” remains a common problem raised in regulatory enforcement actions. First, you need adequate procedures; then, you must ensure the supervision activities you conduct follow these procedures.

The concepts, best practices and directional insights offered in this guide will help firms keep their supervisory practices out of the regulatory spotlight. At the same time, this guide can help compliance teams be more agile and more responsive to the needs of their respective businesses.

Overcoming the status quo

Adopting a modern supervision and surveillance strategy requires aligning key stakeholders around the need for change. In the case of supervisory review, which could mean upending the review staff's familiarity with policy sets — in which they've invested significant time and energy — to meet new expectations. This is especially critical when regulators release annual examination findings identifying expanded enforcement priorities like cyber, inadequately written supervision procedures, non-specific surveillance thresholds, and surveillance-related deficiencies.

It also convinces compliance executives and technology buyers of the need to migrate to cloud-native platforms. The public cloud infrastructure benefits firms can take advantage of includes scaling compliance resources quickly and eliminating costly capital investments in hardware, which leads to more agile and robust compliance processes.

How technology can help

Technology plays a central role in automating policy enforcement, which improves review efficiency. This is true in managing policies and applying the latest technological advances to AI and machine learning to identify red flags — especially across large, heterogeneous datasets.

Needs of the organization

Supervision

1st Line of Defense (1LoD) uses lexicons and AI/ML to conduct supervision to inspect communications of Registered Investment Advisers (RIAs) and Broker-Dealers (BDs).

Surveillance

2nd Line of Defense (2LoD) in organizations uses lexicons and AI/ML to reveal anomalies and trends, reduce "false positives," or noise, to identify the risks and opportunities for the compliance team to focus on within large volumes of communications data. This provides the companies with more robust supervision and surveillance capabilities across the organization.

Both FINRA and the SEC are employing advanced analytical approaches in conducting examinations and expect more firms to use this technology when conducting their own reviews.[1] For the UK, the FCA is evaluating their regulatory frameworks, as are other international regulatory bodies for their country or regions because they recognize firms are embracing surveillance as part of their review procedures.[2]

Chapter 1 – Why Supervise and Surveil Business Communications?

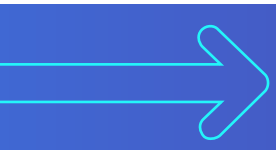
The scope of regulations, guidelines and legislation covering supervision obligations worldwide is extensive. Regulated firms in most countries are challenged with how to adequately monitor and supervise employees. Non-compliance with supervision rules and accompanying recordkeeping requirements can subject firms to many legal, operational and financial liabilities.

The adoption of more communications and collaborative networks amplifies the complexity that firms must address to meet the supervisory requirements of financial regulators. Supervisory obligations do not distinguish one communications tool from another. We saw a record-breaking year for enforcement in 2022, with enforced regulations across all forms of communications — including the channels firms have prohibited their workforce from using.

However, regulators have periodically issued guidance around specific areas of technology, such as guidance on blogs and social networking websites (FINRA Notice 10-06), social media websites and the use of personal devices for business communications (FINRA Notice 11-39), and social media and digital communications (FINRA Notice 17-18). Most recently, FINRA also provided guidance (Notice 20-16) to ensure that firms can continue to follow supervisory procedures as more employees move to a remote work environment. They've noted actions some firms have taken to ensure that unauthorized applications are not being used, as well as those applying to the Taping Rule (FINRA Rule 3170) to use voice recordings to address potential communications gaps. In addition to FINRA Reg Notices, the 2023 priorities report on FINRA's Examination and Risk Monitoring Program has included developing WSPs and controls for live-stream public appearances, scripted presentations, and video blogs as a best practice for Video Content Protocols.

In the UK, the FCA issued guidance (FG15/4) on social media and customer communications. The finalized guidance on social media intends to help firms understand how they can use media in financial promotions and comply with FCA rules.

You can find additional information and an overview of specific regulations addressing form supervisory obligations in our "Global Regulatory Communications Compliance Guide." They are segmented by country, including several cross-industry regulations and their implications for financial services firms.



LEARN MORE **The Global Regulatory Communications Compliance Guide For Financial Services**

Since all financial services firms have recordkeeping requirements, leveraging retained data to conduct periodic supervisory reviews can reduce the uncertainties of ad-hoc content inspection. Firms can iteratively build policy sets to target risk areas with daily, automated reviews, the likeliest probability and highest potential impact on the business. Standardizing a common tool for content inspection can also drive greater collaboration among stakeholders and a shared view of risk.

Extended benefits of supervision for non-regulated organizations

For organizations that do not have an explicit regulatory-driven supervision requirement, the need to inspect employee communications for potential policy violations has never been greater. Investigating a workplace harassment issue or possible leak of intellectual property is one thing when employees are physically present nearby; it can be a very different exercise when employees are virtual and distributed.

However, supervisory or surveillance approaches across non-regulated industries continue to play catch-up. According to Gartner research highlighted in their article, "The Right Way to Monitor Your Employee Productivity," the number of large employers using tools to track their workers has doubled since the beginning of the pandemic to 60%. Moreover, this number is expected to rise to 70% by 2025.

Applying supervisory practices beyond the industry-mandated domain means opening the aperture to view policy violations and vulnerabilities across multiple functions and business processes. Legal, HR, infosec, audit and investigative teams are all engaged in spotting red flags ranging from losses of intellectual property, security exposures and privacy violations to various workplace policy infractions. Before the pandemic, each held its own budgets, risk priorities and tools, resulting in a plethora of siloed approaches to managing risk. Today's hybrid workforce is changing that.

Chapter 2 – Key Supervision Challenges

Evolving regulations and technology

Regulated firms must keep pace with complex and evolving domestic and international regulations and a rapidly changing risk landscape (e.g., security, privacy, financial risks and internal threats). At the same time, they now have access to vast amounts of data, inexpensive computing power and innovative technologies that can help to partially automate compliance and supervision.

New ways of communicating

Today's social and collaborative technologies are dynamic, context-sensitive and multi-dimensional. With the popularity and advancements in collaborative technology, such as WhatsApp, Zoom and Microsoft Teams, many intersections of channels form more complicated communication maps that are increasingly difficult to track. A conversation may start through email, move to instant messaging or social media and then jump to SMS text messaging, resulting in a video conference call — and all could be further contextualized with emojis. None of these active or interactive elements translate well into a static review environment.

Too many solutions flatten this content into email for archive and review, which removes important metadata and critical context which is useful to compliance and for legal teams for e-discovery.

Siloed archiving systems

Many companies add a further layer of complexity to the situation by using an assortment of data storage tools. Email, IM & collaboration, social media, mobile and voice and video/conferencing technology content is archived across individual data stores. Managing different storage stacks makes it likely that conversations across platforms are being reviewed multiple times.

Competing interests

Policies designed for email may need reinspection to reflect the ways employees can use new channels. An organization's rules should, of course, include supervision and retention of email. Problems can arise if they overlook the fact that employees are shifting their preferred channels. According to **Putnam**, 95% use direct messaging to reach customers via text, social media or voice through mobile and messaging solutions. Organizations must consider customers' choice of communication methods.

Managing risk

Compliance risk is pervasive and ongoing. Firms must keep up with the latest trends, from mandated remote and hybrid policies to continued regulatory enforcement. It's not just about retention and supervision of communications data; additional consideration should be given to security, privacy management and operational governance.

The SEC has stated that the content of an electronic communication determines whether it must be preserved. While communication channels quickly evolve, we need to understand where communication occurs and how to record, retain, and supervise these as part of our regulatory obligations.

Data privacy breaches are a key concern for many companies. Ground-breaking regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are meant to ensure the data privacy rights of individuals. The fines resulting from breaches and inattention to these rights can devastate a business.

An organization's data privacy must also be considered. The loss of confidential information (e.g., intellectual property, financial information) can also be disastrous.

The ease with which data can be transferred, and the many communication modalities that can be used, make keeping on top of these risks a challenge. Supervision tools must be efficient and flexible enough to manage the massive amount of communication information that can flow around an organization.

Distributed work environments elevate the need to understand the behaviors of employees to a level never seen before. The result has been more firms acting in unison to share resources, tools and business practices to identify and mitigate risk. This has included leveraging supervisory systems to review employee communications. More frequent inspection can be provided for higher-risk employees, client-facing staff and executives. Uncovered patterns can be fed back into supervisory policies to help stay ahead of areas with the greatest potential to impact the organization.

Chapter 3 – Common Supervisory and Surveillance Methods

Regulatory supervision is especially critical as many people continue to work from remote locations following the pandemic. This new workplace dynamic has not changed regulatory obligations. Regulators expect member firms to establish and maintain reasonable systems designed to supervise the activities of each employee, no matter where they do business.

However, FINRA, the SEC, FCA, and other regulatory bodies offer only guidelines or best practices about how firms should conduct supervisory reviews, instead of concrete rules. Consequently, supervisory practices vary dramatically from small to large firms and from broker-dealer to investment adviser. It's also true that regulatory enforcement actions range from highly complex schemes to the basic failure to follow a firm's WSPs.

Supervision and surveillance processes

While employees and customers can collaborate and engage more effectively and easily than ever, organizations face oversight and supervisory challenges. One of the biggest challenges with modern supervision and surveillance systems is separating the real risk from the 'noise.' Review teams must sift through a vast and often unmanageable number of false positives to get to relevant and targeted content.

The oversight of this massive collection of communications data is required for those in regulated industries, and it's a drain on their compliance teams. Not all supervision and surveillance technologies are created equal, so organizations must choose wisely. Implementing the right supervision and surveillance technology and processes is paramount to streamlining compliance workflows, managing risks and avoiding costly penalties.

There are three levels of supervision technologies, ranging from limited to optimal options:

Mostly human supervision

At the basic level, organizations rely on lexicons, which filter electronic communications against a list of keywords or phrases. This level also uses random review sampling — a process that reviews a selection of correspondence without first narrowing the corpus for purpose, meaning you're not using lexicons to surface risk. This is a way to test whether your lexicons are adequately capturing risk or

whether there is a need to fine-tune your lexicons. With mainly human supervision, organizations may meet regulatory requirements but can miss many risks and experience overwhelming false positives. This is why random sampling becomes another key tool to ensure your lexicons are up to date.

Mix of human and automated processes

There's a blending of human and automated supervision at the intermediate level. Technologies at this level use untrained machine learning and standard scenarios with echo cancellation — a method that speeds up the review process by filtering out a specific source of noise that accounts for low-value alerts. While this mix of human and automated supervision removes replies and repeats in digital communications data, it lacks industry-specific training and produces limited predictive results.

Mostly automated processes

The upper echelon of supervision and surveillance approaches is a mostly automated process. Here, organizations need automated industry scenarios containing a machine learning model trained over datasets of millions of communications to surface specific risks such as "secrecy" or "change of venue." Once the dataset has been trained, firms need the ability to filter out 'noise' like email newsletters or sender exclusion filters and the ability to set filters to alert for real risks such as "don't talk about this with anyone" or a text saying "call me on an unmonitored phone".

Filtering the real risks from the 'noise' has always been one of the biggest challenges that review teams face. This level sifts through the vast and often unmanageable number of false positives to get to relevant, targeted content. As a result, review teams save time, increase accuracy and uncover more risks.

For example, Smarsh Enterprise Conduct provides review teams with:

500%	40%	Up to 95%
more identified risks	smaller volume of discoveries	fewer false positives

While automated machine learning models need the occasional tuning and validation from data scientists, with Smarsh Enterprise Conduct's prepackaged scenarios, there is no need for model retraining or any additional model review board augmentation meetings. Smarsh takes on the costs of the time-consuming, difficult work of pre-training models — so you don't have to. Pre-trained models are ready for use, enabling a faster ROI. This approach not only saves time and resources, but it also limits false positives and uncovers more risks than any other approach.

Managing policies and lexicons

Whether firms develop their own or use vendor-developed lexicons, addressing the regulatory activity and internal risks specific to the firm and its business is important.

Lexicons should include search terms specific to a firm's business – using the right words and phrases. These keywords or phrases can be customized to allow the firm to control which items are flagged and to adjust them as business changes or new risks emerge.

To test whether advisers are using unsanctioned communication channels, it's a good idea to set up automated keyword searches to flag advisers potentially using unauthorized communication channels. Examples include:

- "I'll call you from my personal phone"
- "Send to my Gmail"
- "Text me"
- "Hit me up on WhatsApp"

Especially for global firms, another important consideration for creating lexicons is keywords or phrases in all the languages advisers use. Some tools offer automated lexicon language translations.

Policies should apply across all the communication channels — collaboration and conferencing platforms, text messages, social media, email, voice and video apps. Policy filters can cut down on white noise and make reviews less complicated. Organizations should plan reviews and determine how much time to spend on random sampling versus keyword search. If review is based on percentage, the sample size should be included. Adherence to this requirement is highly recommended.

Managing Machine Learning Models

Organizations outstripped their lexicon capabilities when their operational needs changed. Examples include:

- Higher-risk products require proactive monitoring to reduce risk and fines
- Greater opportunity for customer manipulation such as older clients
- Higher distributed workforce at home, in fewer offices, and on multiple channels
- Desire to "do more with less" as headcounts and budgets fluctuate
- More focus on cyber threats and sanctions (Ukraine)
- Greater regulatory emphasis on addressing sexual harassment and bullying
- Larger surface area to cover because of mergers and acquisitions

Machine learning models may be designed by the customer or a vendor. Customers that choose to build their models must build out a data scientist team, build industry-specific models that must be trained over millions of communications, and can take years to deploy. Once tested, the models must pass a Model Risk Management review that explains the models to the firm's board and regulators at the state, country, and global levels. Firms are also responsible for regularly retraining the models and passing the MRM reviews.

Firms preferring to purchase a vendor-built model can utilize models vetted by global industry regulators. The benefits of partnering with an industry expert are:

- Eliminates the need to hire their own data scientist teams with a prepackaged solution
- Leverages the vendor's years of experience building machine learning models using millions of communications
- Deploys within weeks, not years
- Access to support and vendor's data scientists when periodically retraining models

As noted by FINRA:

"Firms are reminded that outsourcing an activity or function to a third party does not relieve them of their ultimate responsibility for compliance with all applicable securities laws and regulations and FINRA rules."

Mixing machine learning supplemented by the customer-designed lexicons enables the firm to proactively surface the real risks, reduce the "false positives," and improve the efficiency of review teams. This allows them to focus on the real risks and proactively mitigate reputation harm and fines.

Firms should develop a plan to revisit lexicons annually (at a minimum) to ensure they are current and specific to the risk activity of the business. Smarsh or other independent consulting resources should be engaged periodically to evaluate and update the lexicons.

Chapter 4 – Supervision Best Practices

Regulators require firms to be able to monitor and review conversations promptly. However, the requirement for firms to proactively monitor all electronic communications has proven challenging, especially when tracking the “change of venue” conversations that occur when people continue the same conversation across multiple channels.

Below is an outline of the four best practices to achieve an effective supervisory system.

1. Establish clear policies and procedures

To have an effective supervisory system, firms must establish clear policies and procedures regarding the use and monitoring of electronic communications. Policies and practices should regularly evolve, as should your technology, to cover new methods of client communication. Firms should have a reasonable system to monitor for compliance with their electronic communication policies.

There is no prescribed rule for when to review the messages, but it must be timely to find and escalate red flags. Reviewing as many messages as are specified by the firm’s policies is crucial. If the policies call for a review of four percent of all emails each month, reviewing only two percent in a quarter is missing the mark. For example, suppose your policies and procedures say you will review five percent of your social media communications in a month. In that case, you may do a random sampling if you fall short of your five percent in your policies.

Also, setting a percentage on what flagged messages you’re reviewing misses the mark. All flagged messages should be reviewed to prevent “failure to follow up on red flags” by the regulators. Regulators care that any potential threats are reviewed. You’re risking not finding misbehavior by only reviewing a certain portion of flagged messages.

Firms also must ensure that employees have access to these policies and procedures. Considering the current regulatory enforcement actions regarding off-channel communications, address these in your policies and procedures. What communications are prohibited, how are you reviewing for these communications, and what actions will be taken for non-compliance. Organizations should also have a policy in place for client communications on unauthorized channels. This includes employee training and how to report, capture, retain, and make sure employees know when to move off-channel conversations to an approved channel.

Best practices noted in the FINRA Examination and Risk Monitoring Program report:

Providing employees with a list of sanctioned channels

"Clearly defining permissible and prohibited digital communication channels, tools and features, and blocking those prohibited channels, tools and features that prevent firms from complying with their recordkeeping (and supervision) requirements."

Enforcing repercussions for unsanctioned channel use

"Temporarily suspending or permanently blocking from certain digital channels or features those registered representatives who did not comply with the policies and requiring them to take additional digital communications training before resuming use."

The goal of reviewing electronic communications is to ensure employees and executives are not committing any wrongdoing. Examples of misconduct include undisclosed outside business activities, private security transactions, promising investment returns and sharing non-public information. In the case of a potential violation, a firm's procedures should identify the person(s) responsible for determining whether a violation has occurred (and their job role) and whether they are reporting under regulatory rules.

Firms should provide a protocol for escalating violations (and potential violations) to such person(s) and a protocol for reporting internal conclusions of the violations. Minor violations can be resolved in-house, while significant violations must be reported to FINRA and other authorities. Another best practice for organizations is to conduct an annual review or risk assessment by looking at the violations that occurred to identify where additional measures should be taken or training needed. For violations of the policies, it's critical to include fair and documented consequences. Ensure you have documentation you can share with regulators to show that you handled the violations to your policies and procedures.

2. Demonstrate compliance

Firms need to demonstrate to regulators that they are supervising the activities of their representatives. Establishing a reasonable supervisory system that flags, escalates and enables actions to address potential fraud and violations is essential.

To best ensure compliance obligations are being met, supervision technology capabilities should include:

- Advanced supervision workflow
- Multi-tier review queues
- Visual dashboards
- Action panels
- Roles reporting
- Escalation
- Customizable policies
- Model risk governance processes
- Above and below-the-line testing

The timely review of electronic communications is a first-line defense for firms against improper employee conduct. Organizations should partner with a technology vendor that can provide efficient and effective tools to actively monitor risks and demonstrate compliance. Technology solutions should also come with real-time moderation and pre-review capabilities that can be added for specific channels.

With these capabilities, firms can proactively monitor communications with control. This includes alerts, message blocking, ethical walls and disclaimers to prevent compliance issues before they happen. It is critical to document the review process as well. Engage an archiving provider that has the technical ability to electronically document reviews and create an audit trail. If a message in question is spam, it can be noted as “not material” or “junk message.” Documentation of procedures can be a powerful tool to evidence your supervision process.

3. Conduct effective employee training

Staff should be trained in the firm's electronic communication policies. FINRA notes training as a best practice, "implementing mandatory training programs prior to providing access to firm-approved digital channels, including expectations for business and personal digital communications and guidance for using all permitted features of each channel." Employees required to comply with the monitoring requirements must also be prepared. This training should focus on areas such as:

- Prohibitions on particular means of communication (e.g., encrypted messaging apps)
- All applicable privacy laws
- Requirements for lost or stolen devices
- Use of unsecured wireless networks
- Rules for sending corporate data through personal communication channels (e.g., email, text messaging)

When employees understand the consequences of violating the established rules, the chance of non-compliance to supervision diminishes.

Firms should periodically gather feedback from employees and peers who regularly adopt new technology. Policies should reflect today's evolving digital communications landscape. Since new channels frequently emerge, it's important to keep employee training up to date to keep pace with the latest technology.

4. Check and double-check supervisory controls

Supervisory review processes should be evaluated at least yearly as part of the regulatory requirements, including watching for regulatory changes. Reviews should be documented formally and approved by the appropriate internal authorities. It's also recommended to periodically test the systems to ensure communications are being captured for review and retention. Testing will ensure processes are being followed and gaps are quickly identified and addressed.

Supervising content is critical, and implementing the best practices outlined above will help achieve a compliant supervisory system. It only takes one non-compliant message among millions for a firm to ruin its reputation, shatter customer trust and receive million-dollar fines.

Chapter 5 – The Future of Supervision

There are three key factors informing the future of supervision that warrant exploration:

1. Regulatory change

There are many regulatory bodies worldwide, and they all have different priorities. This results in many different regulations and directives. For example, the European Union alone has the FCA, ESMA, ECB, SSM, EBA and EIOPA, while the U.S. has the SEC, OCC, FINRA, CFTC and FDIC, and Canada has IIROC. (This is not an exhaustive list and doesn't include regulatory bodies in other continents.)

Today's business is done globally, which means there could be touch points in many different jurisdictions with different regulations and requirements. However, there are some common themes:

Individual protections

Data accessibility and protection have been a key focus with EU regulations and directives like MiFID II and GDPR — as well as CCPA, California's version of GDPR. There will be even more crossover in the future, and with the increase in data volume and variety, this will prove to be an ongoing challenge.

Cyber risk

Regulators today are increasingly focused on cyber risk management. For firms, it means more oversight for vendors and firms conducting due diligence when engaging with them. Cyber risk will continue to pose difficulties and should be regularly considered in compliance strategies. An integrated cyber compliance and vendor risk management solution enables organizations to assess third-party vendor security and manage risk across the virtual supply chain.

Anti-Money Laundering (AML) or Combating the Financing of Terrorism (CFT)

New business models, modularization or unbundling of the financial services industry and proliferation of cryptocurrencies will continue to exacerbate the risk and reduce the transparency of transactions. A review of your communications can also be used to identify atypical customer behaviors, helping you to identify potential AML red flags, i.e.: "high pressure language."

2. Consumer preferences

Always connected

Generation Z, now the largest generation in the United States, is the first generation of true digital natives, having been raised in a world where the internet, social media and smartphones are the norm. In 2021, the spending power of Generation Z reached $360 billion, and they accounted for 40% of global consumers. Their preferences must be considered.

But it is not just Gen Z that wants to stay connected. In 2011, 35% of adults in the U.S. had smartphones. Today that figure is over 85%.

For most workers, there is a distinct preference for instant messaging over more traditional methods of communication like email. Another preference, albeit dwindling, is for in-person meetings. In-person meetings have become challenging now that more people than ever before are working from home and have access to popular and sophisticated collaboration software tools such as Microsoft Teams and Zoom.

Data privacy

There has been a keen focus on data privacy with regulations like GDPR and CCPA, which ensure that consumers are in more control of their data privacy rights. As challenging as it has been for financial institutions to reconcile the need to comply with data privacy regulations and financial regulations over recent years, the future will be even more complex. With a global workforce and consumer base, ensuring compliance with multiple countries' rules and regulations will be a challenge.

The perceived security of the application will influence the choice of communication method. WhatsApp, with its end-to-end encryption, has two billion active users. Other secure chat applications such as WeChat, Signal and Telegram have grown significantly. The number of communication channels requiring supervision will only increase.

Reputational risk has always been a key concern for financial services. Data privacy will be a significant part of this risk going forward.

3. Technology advancements

New tools and methods of communication

While text messaging and tools like Zoom, Microsoft Teams and Slack have been around for decades in one form or another, they are now ubiquitous in the workplace and at home. Workers spend much of the day sending messages, video calling and collaborating on documents. We can expect text messaging and mobile applications like WhatsApp and WeChat to continue to grow.

More data

By 2025, worldwide data volume is expected to hit 175 zettabytes — a 61% growth since 2018. In addition to this, the complexity of this data is going to prove problematic for compliance teams. We have already discussed that the variety of communication channels is growing; maintaining context and parity across them will be essential.

It is predicted that around 50% of all data will be stored in the cloud by 2025. Financial services institutions are embracing the cloud, which is critical to keep up with the scale of the data problem. Cloud is no longer "future tech." It is the norm now. And it is not just about the ability to scale data storage requirements but also about scaling compute requirements.

Artificial intelligence and machine learning

One of the key areas in which modern compute requirements will be necessary is machine learning and artificial intelligence. The proliferation of new channels and the explosion of digital communications data is why organizations need more AI. The adoption of AI and ML are growing as firms recognize the benefits.

AI and ML at Smarsh can reduce false positives and help surface more true risk. Smarsh Enterprise Conduct includes a catalog of both prepackaged standard and cognitive scenarios, echo cancellation, augmented scenario structure, lexicon-filtering and industry-trained machine learning models. The benefit is you can deploy in weeks not years with a non-Data Science compliance team. Implementing Cognitive Scenario decreases false positives by 10x compared to a lexicon-based approach.

GET THE BRIEF **Smarsh Enterprise Conduct Solution Brief**

Future solutions

- **Cloud-native technology:** Cloud-native architecture shortens time-to-value by providing a consistent development and automated management experience across leading public cloud infrastructure (e.g., Amazon Web Services). It delivers the flexibility and scale required for global enterprises seeking a future-proofed, business-critical information platform
- **Scalability:** Scaling to meet data storage requirements is just one piece of the puzzle. Scaling to meet compute requirements will be just as important. Effective use of cloud technologies allows for horizontal scale to meet demand with end-to-end security
- **Speed:** Considering the increase in communications data that a compliance team will need to review, time is of the essence. Sub-second search, instant message and data preview and efficient review workflows with granular role management are table stakes for a cloud archive and supervision application
- **AI/ML:** There are many ways that AI and ML will contribute to the future of supervision and surveillance:
  - Intelligent identification of personally identifiable information to reduce data privacy risk
  - Reduction of false positives
  - Echo cancellation
  - AI-assisted review
  - "Low hanging fruit," identifying data most likely to need further review, as well as data with the highest risk to the business
- **Consolidation of data and effort:** Many financial services institutions have siloed archives, with emails, chats, text messages and other data formats stored in separate systems. Combining this information into a comprehensive, scalable, performant archive creates a "single pane of glass" supervision solution.

Chapter 6 - Conclusion

Electronic communications supervision is a complex reality for regulated financial institutions worldwide. Specifics vary under geographical regions and associated governing bodies, but across the board, those regulations are unyielding. And for good reason — regulations for the retention and oversight of electronic communications are there to demonstrate a commitment to protecting consumers and maintaining consistent procedures and policies across the industry.

At the same time, organizations should be able to communicate on their terms. Their infrastructure should allow customers and staff to use preferred channels securely and without risk to the organization. However, as we move more and more business interactions and processes online, the obligation to monitor communications has become even more urgent and complicated. And the need to understand employee behaviors has never been greater. As we touched on earlier, many non-regulated organizations are taking proactive measures to mitigate potential risk by establishing supervisory or surveillance approaches.

Work from home

Recent record-breaking fines demonstrate that the shift to remote working has not deterred regulators. They continue to expect member organizations to establish and maintain reasonable supervisory systems designed to monitor the activities of each employee, no matter where their work location happens to be.

Compliance teams had already been challenged by the ever-increasing volume and variety of communication types that must be reviewed to meet regulatory requirements. In just the last few years, the scope has widened to include text messaging, social media, collaboration platforms, conferencing tools, and all the modalities and metadata therein. Breaking up and converting these dynamic communications to email format is no longer an effective strategy for maintaining efficient review. Current events have only escalated those concerns.

Supervision and surveillance

Reviewers need an easy-to-use application to identify violations and risks — and act as quickly and efficiently as possible. Accordingly, supervision applications must provide the policy sophistication necessary to automatically reduce false-positive search results with precision. Solutions must be flexible to customize workflows and escalation processes for supervised participants.

To prepare for future evolutions in communication and business, financial institutions must think big and go beyond traditional lexicon-based monitoring of the communications of regulated users. They must seek to leverage supervision and surveillance technologies and incorporate more context, metadata and other data sources to surveil a broader population.

As the adage goes, the only constant in life is change. In this case, financial organizations must brace themselves for any combination of regulatory developments to address new and evolving cyber threats, evolving communication preferences for digitally native workers and technology advancements.

A holistic approach

Fortunately, there are intelligent technology solutions that help organizations future-proof their supervisory processes and stay ready for changes in the compliance landscape. Cloud-based technology provides scalability, efficiency and the ability to integrate with new data sources and third-party applications. AI and machine learning can assist in the review process by reducing false positives and mitigating data privacy risk with intelligent identification of personally identifiable information. A supervision solution with a “single pane of glass” view simplifies the process by bringing all communication content together into one place.

And while technology solutions make the process more efficient and precise, effective governance is a critical part of a comprehensive supervision program, too. Organizations must establish clear policies and procedures for supervision, effectively document those procedures, dedicate resources to training compliance personnel and revisit all supervisory controls regularly.

Regulated financial organizations have the added business challenge of maintaining communications compliance. Meeting those needs requires a successful combination of preparedness: adaptability to changes in the marketplace, enabling workforces to use the communication tools that will keep them competitive and maintaining proper governance to mitigate risks.

How Smarsh can help

Meet the next generation of communications intelligence with the Smarsh Enterprise Platform. The first-of-its-kind, this SaaS platform is AI-powered, cloud-native, and built to scale to meet the communications data needs of the modern enterprise. Architected for the public cloud, Enterprise Platform is a powerful, end-to-end solution for data collection, retention, monitoring and analysis.

With increased support for new communication types, improved data management and security that is years ahead of others, only Smarsh enables enterprise organizations to take a global approach to compliance management.

The Enterprise Platform is made up of these built-for-purpose solutions:

Capture

Smarsh captures even more of the most popular mobile, IM & collaboration, social, video and voice tools, and email/email mass marketing used today. Retain and index important contextual details to speed up and improve supervision and e-discovery reviews.

Enterprise Archive

Enterprise Archive is the context-aware compliant storage solution that covers the most stringent communications retention and immutability regulations, including FINRA, IIROC, FCA, MiFID II, and GDPR.

Enterprise Warehouse

At the core of the Enterprise Platform is the Enterprise Warehouse. With petabyte scale and elastic compute, the warehouse provides a centralized location to retain, analyze and enrich your communications data.

Enterprise Conduct

Enterprise Conduct provides a prepackage catalog of Standard (lexicon) and AI/ML scenarios for communications supervision and surveillance so you can quickly set up your lexicons, policies and scenarios. Cognition Studio is your workbench to build, tune, test, and analyze your newly designed scenarios to identify the right scenario to act upon risk in your organization, all while dramatically reducing noise in your review queues. Confidently explain why you selected the scenario to your board and regulators.

Enterprise Discovery

Collect, preserve, review and export digital communications data on-demand to allow your legal team to get an early view of the case to enable strategic decision-making on legal matters and reduce the time and cost of e-discovery.

Meet the evolving needs of your business

Smarsh has architected its solutions specifically to support your business as it evolves. Our products are equipped with open APIs for ingesting, enriching and exporting content, meaning you can take advantage of integrations with third-party applications. Partnerships with the latest content sources and elastic scaling capabilities help you to stay one step ahead of risk within your communications. Additionally, flexible deployment options enable alignment of your capture, archiving, discovery, and monitoring solutions with your business's IT strategy as it develops.

Additional Resources

Brief: Using Machine Learning to Power Regulatory Compliance in Financial Services
Guide: Expanding the Sphere of Supervisory Value
Brief: Smarsh Enterprise Conduct: Cognitive Scenarios

References:

1. The case for placing AI at the heart of digitally robust financial regulation (brookings.edu)
2. Financial markets' regulatory outlook for 2023: Resilience, vigilance & positioning for change - Thomson Reuters Institute (old)
3. Social media for business building – Putnam Investments
4. https://www.wordstream.com/blog/ws/2022/08/09/gen-z-stats
5. https://www.zippia.com/advice/us-smartphone-industry-statistics/
6. https://backlinko.com/whatsapp-users

smarsh®

Smarsh® enables companies to transform oversight into foresight by surfacing business-critical signals in more than 100 digital communications channels. Regulated organizations of all sizes rely upon the Smarsh portfolio of cloud-native digital communications capture, retention and oversight solutions to help them identify regulatory and reputational risks within their communications data before those risks become fines or headlines.

Smarsh serves a global client base spanning the top banks in North America, Europe and Asia, along with leading brokerage firms, insurers, and registered investment advisers and U.S. state and local government agencies. To discover more about the future of communications capture, archiving and oversight, visit www.smarsh.com.

Guide - 05/23

1-866-762-7741 www.smarsh.com @SmarshInc SmarshInc Company/smarsh