The Broadening Scope of Communications Supervision:

From Regulatory Obligation to Proactive Risk Management

smarsh®

Table of Contents

What to Know About Information Risk

The inspection of business-related employee communications is a well-established compliance business process for every financial services firm.

- Each firm must establish written supervisory procedures (WSPs) that require regular review
- WSPs must include reporting for regulatory examination, for every individual who carries a license to sell (or advise on the sale of) securities

These responsibilities serve a clear purpose: to protect investors, ensure market transparency, and adhere to numerous regulations designed to protect the health of the financial system.

But there's also a broader, fundamental purpose for adopting these processes: to help all types of organizations identify and remediate *information risk.*

INFORMATION RISK

A calculation based on the likelihood that an unauthorized user will negatively impact the confidentiality, integrity and availability of data that you collect, transmit or store.[1]

It is within that broader definition that we encounter the incongruence: supervisory review obligations are explicit for only a subset of a regulated firm's employees. And, for every regulated firm, there are thousands of employees who do not have the same rigorous oversight requirement.

This is at odds with the simple, undisputed fact that, today more than ever, information risk lives everywhere.

From every mobile device, on every downloadable app, and likely in many virtual meetings, individuals could be violating company policies at this very minute. The "sphere of supervision" is a way to describe this paradigm.

The Sphere of Supervision

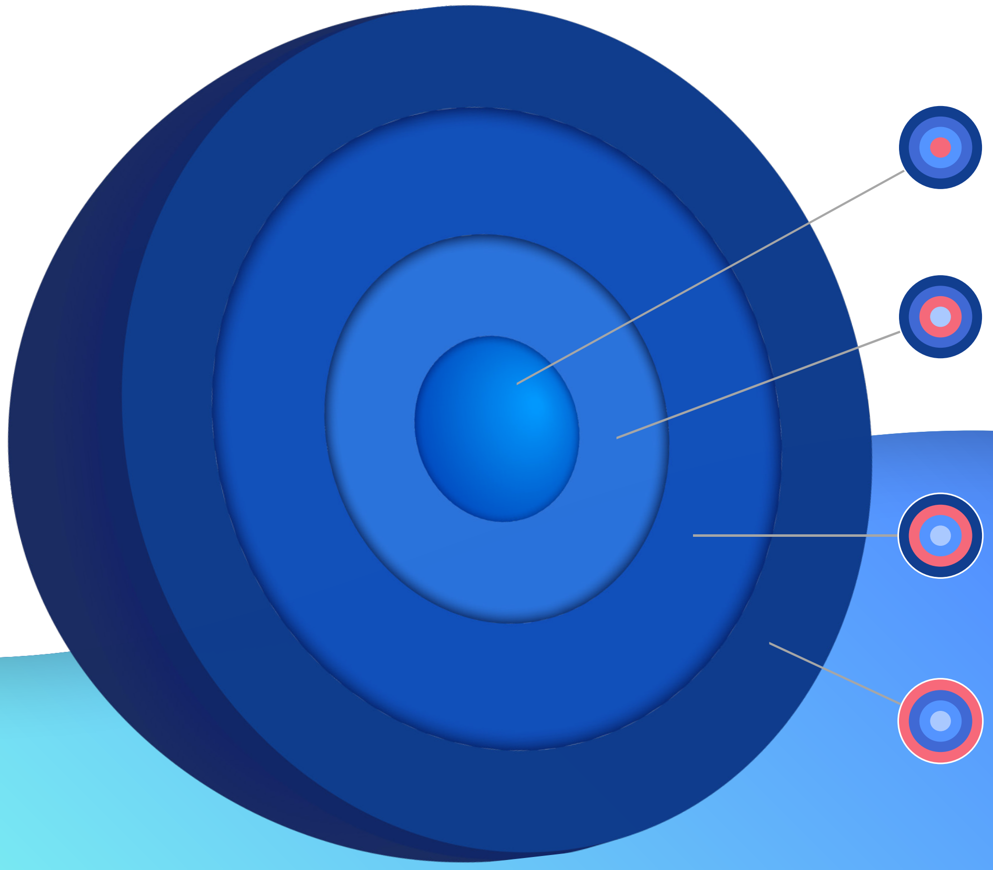
In this guide, we will explore supervisory dynamics faced by organizations in the following tiers:

Supervision Mandated: for firms with broker-dealers (BDs) and/or registered investment advisors (RIAs) who are subject to explicit supervisory review obligations, and where the process is non-discretionary

Financial Services Records: referring to financial services firms that retain historical content to meet recordkeeping requirements, and commonly practice some method of supervision or surveillance

Other Regulated Industries: similar to financial services firms, these organizations also have recordkeeping obligations to retain content that can be made available for periodic inspection

All For-Profit Organizations: for all other corporations where inspection or oversight is most typically demand-driven or done on an ad-hoc basis



Supervision Mandated (Broker-Dealer and Investment Advisor)

Financial Services Records (SEC 17a-4, FINRA 4511, MiFID II)

Other Regulated Industries (Energy, Pharma, Healthcare, Utilities, Government)

All For-Profit Organizations (Code of Conduct, SEC, Insider loss)

Supervision Mandated: Broker-Dealers and Investment Advisors

Smarsh has written extensively about supervisory review, so we won't replicate the details of FINRA 3110, SEC Rule 206(7) or FCA Chapter 9 here. Instead, please refer to the "Global Regulatory Communications Compliance Guide" for a detailed list of global regulations.

However, what's impacting the management of information risk continues to evolve. We've highlighted common trends and challenges faced by firms large and small in today's business landscape.

- **The mismatch between legacy supervisory technologies and today's interactive, multi-modal communications.** As many regulated users are now operating full-time over conferencing and collaborative tools, it is only a matter of time before a complex persistent chat causes a legacy supervisory tool to fail over. Firms are realizing that they can't effectively identify and manage risk using tools designed for a bygone era.
- **The challenge of getting past the status quo.** Firms have spent multiple years wrestling, cajoling and nurturing review policies that are not easy to abandon, even with high rates of false-positives and overwhelming review queues. Like most of their underlying archives, legacy supervisory systems often stay in place way past their useful lives because firms cannot generate the cross-functional inertia to move past the status quo.
- **The policy tendency to "set it and forget it."** In our survey of supervisory practices, we continue to see firms that wait too long to adjust policies and reinspect those policies far too infrequently.[2] This trend is more pronounced for resource-constrained, smaller broker-dealer and registered investment advisor firms. Still, it is also true for firms whose communications and regulatory mix would seem to necessitate more frequent inspection.
- **The growing proliferation of advanced analytics technologies, and the blurry line between supervision and surveillance.** More and more data sources have led to the idea that only machines can make sense of behaviors and spot anomalies across distinct data types. Consequently, more firms are planning to integrate supervisory review tools with those providing AI-driven content surveillance. This would enable supervisory policy inspection to spot red flags, which then would be delivered to advanced surveillance tools for further behavioral and sentiment analysis.

At the core of the sphere, the value of supervision is straightforward. It is to enable a balance of **improved efficiency** in the basic blocking-and-tackling **supervisory requirements** with the need to improve effectiveness in **spotting risk in emerging content sources.** Given that FINRA enforcement actions consistently highlight basic failures to follow firms' own written supervisory procedures, it's apparent that the need to maintain this balance remains a top priority.

Financial Services Records

The second layer of the sphere can be added to include those in financial services firms that have recordkeeping requirements under SEC 17a-4, FINRA 4511, MiFID II Article 16, and similar retention requirements outlined by other financial regulatory bodies. This group includes non-registered employees within BDs, RIAs and other financial institutions that are subject to supervisory obligations.

This group is unique for two main reasons:

1. Employees work for firms with retention requirements mandating that records be stored for a minimum of six years. (So, they tend to leverage the same archiving infrastructure as their registered colleagues.)

2. Conversations on collaborative networks frequently happen among a mix of registered and non-regulated users.

As a result, creating lighter-weight supervisory policies that apply to groups outside of the regulated pool (for example, members of executive staff) could be done leveraging the same technology infrastructure. Policies could be evaluated on a less frequent or ad hoc basis or could be defined and regularly monitored for specific infractions, such as ethical wall violations.

One specific example where this use case is common is within firms that must comply with the European Union's MiFID II Article 16(7) requirements to "capture and reconcile all communications and activities that lead to a financial transaction." In this scenario, reconciling communications and transactional data can surface non-regulated users that may be parties in activities that were violations of regulatory requirements. The use of supervisory tools to an expanded set of regulated and non-regulated users can help to surface and address issues sooner, before they become exposed to regulators.

A key challenge for using supervisory tools for this expanded group is determining what is a "record." FINRA 4511 states only that firms must "preserve for a period of at least six years those FINRA books and records for which there is no specified period under the FINRA rules or applicable Exchange Act rules," without defining what precisely constitutes a "record."

This has resulted in many firms following the axiom that a record is determined by the context of a conversation, regardless if the channel is email, social media or a text message.

Relevant regulations governing the **supervision** of electronic communications:

- FINRA 3110, 3120 & 3130
- SEC 206(4)-7
- IIROC NI 31-103
- CFTC 1.31

Relevant regulations governing the **recordkeeping and storage** of electronic communications:

- SEC 204.2
- SEC 17a-3 & 17a-4
- FINRA 4511
- FINRA Regulatory Notice 11-39
- FINRA Regulatory Notice 17-18
- IIROC 29.7
- MiFID II

This works fine for written messages, but not as clearly when you bring the multiple modalities of collaboration tools like video, voice, whiteboards, bots and emojis into the discussion.

One can make a strong case that if any of these capabilities are used to deliver content that pertains to the business of the firm, the retention obligation applies. Unfortunately, these features are not always made accessible by content providers for capture and inspection, so practices will continue to vary. Explicit regulatory guidance on obligations to retain voice, bots and collaboration features will change the equation dramatically.

Ultimately, the value of supervision for those with financial services record retention requirements is to extend the reach of existing supervisory investments, improving their ability to identify and respond to information risk beyond their regulatory user base.

Other Regulated Industries

The concept of periodically inspecting employee communications is much different for organizations that have regulatory obligations to retain business-related communications versus those that don't.

Moving out to the third layer of the sphere, this regulated category includes financial services firms outside of those involved in the sale of securities (e.g., insurance, banking, infrastructure, etc.), including verticals such as pharmaceuticals, healthcare, utilities, energy and government.

Each of these sectors has at least one regulatory-driven mandate to capture and retain communications for a minimum duration (although none, aside from energy traders regulated by the CFTC, have a supervisory review obligation). For this group, periodically reviewing communications can simply entail running searches against retained content to identify and investigate potential policy violations. Consequences for not proactively identifying violations can be severe. Examples of high-profile mishaps include:

- **Pharmaceuticals:** Drug makers were sued by 44 states for generic price fixing based upon evidence from text messages and phone call logs[3]
- **Energy/Utilities:** Pacific Gas and Electric Company (PG&E) was ordered to pay $3M for providing false information to regulators over the San Bruno fire. PG&E said it was "unaware of the records inaccuracies" before the incident[4]
- **Healthcare:** A dental practice in Texas agreed to a settlement with the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services over the disclosure of a patient's personal health information on social media. This was considered a potential violation of the Health Insurance Portability and Accountability Act (HIPAA)[5]
- **Government:** In a well-publicized controversy, former FBI staffers Peter Strzok and Lisa Page brought lawsuits against the FBI and the Department of Justice (DOJ) after their text messages were released to the public[6]

For non-financial organizations with record retention requirements, supervision can reduce the uncertainties of purely ad-hoc content inspection. **Organizations can leverage historical archived content and iteratively build policy sets to target risk areas with 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.

All For-Profit Organizations

We describe the outermost layer of the sphere of supervision as “all for-profit organizations” versus “non-regulated” for a simple reason: virtually every for-profit organization is obligated to fulfill contract, employment, workplace safety and other laws that require inspection, auditing and reporting.

Additionally, all publicly traded firms have a plethora of obligations under the SEC, including Regulation Fair Disclosure (FD), which requires that companies do not release non-public information except through approved communications channels that are known and available to all investors. Elon Musk tweeting that Tesla would go to $420 per share became the “$40M Tweet” after the SEC took notice. The incident became a cautionary tale for public corporations to monitor their executives’ social media posts.

In fact, 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.

Well-publicized samples of internal policy and other code of conduct violations happening on mobile, collaborative and social networks are extensive. Here are a few examples:

- **HR/Code of Conduct:** The CEO of luggage company Away resigned after “Slack bullying” incidents were brought to light[7]
- **Confidential information:** Boeing employee chats and emails alluded to 737 Max design issues, prior to the two large-scale fatal plane crashes in 2018 and 2019[8]
- **Data leaks:** Apple warned employees about leaking information to media via LinkedIn and Twitter, invoking potential legal action including criminal charges. Similarly, Tesla had also warned about leaks and fired an employee for sharing confidential information with journalists on Twitter[9]
- **HR/Code of Conduct:** McDonalds sought to recover severance from its fired CEO over workplace affairs occurring over text and video calls[10]
- **Intellectual Property loss:** “Gigaleaks” (a term coined to describe leaks of private company information such as emails, source code and creative prototypes) over Twitter and Discord plagued Nintendo and worried other tech gaming firms[11]

Consider that these examples arose while, on average, less than 25% of employees were working remotely. Similar mishaps will increase in frequency, variety and potentially severity, now that many employees are working remotely or in a hybrid capacity.

However, the use of supervisory or surveillance approaches across *all* outer layers is catching up. By 2025, 45% of regulated enterprise customers will conduct supervision of audio/video content to meet compliance requirements, up from less than 10% in 2021. By 2025, 35% of enterprise customers will archive workstream collaboration and meeting solutions for nonregulated requirements, **an increase of more than sevenfold from 2021.**[12]

By 2025

45%

of regulated enterprise customers will conduct supervision of audio/video content to meet compliance requirements

By 2025

35%

of enterprise customers will archive workstream collaboration and meeting solutions for nonregulated requirements

For this outermost layer of the sphere — firms that lack regulatory retention obligations — the inspection task can be significantly more complex. Content needs to be sampled via in-stream controls or advanced analytics, or manually collected after an incident is flagged by an employee via an “ethics hotline.”

This reactive approach is time-consuming, expensive and counts on a well-meaning employee to report (and not fear retaliation). These inefficiencies are driving some organizations toward approaches that provide more consistent, real-time visibility into possible infractions. A proactive response can consist of multiple components, including:

- Updating code-of-conduct policies to ensure that they fully address the risks and policy infractions that can be encountered by distributed workforces
- Revising employee training programs to provide guard rails for employees using mobile and collaborative technologies
- Examining supervisory technologies that can automate the identification and response to the most likely and impactful policy infractions

More Benefits of Supervisory Review

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, including:

- Intellectual property (IP) loss
- Security exposures
- Data privacy violations
- Workplace misconduct

Just a few years ago, each held their own budgets, risk priorities and tools, resulting in a plethora of siloed approaches to managing risk. Today’s work-from-anywhere workforce is changing that.

Moreover, distributed work environments elevate the need to understand employee behavior to a new level. The result has been more firms acting in unison to share resources, tools and business practices to identify and mitigate risk.

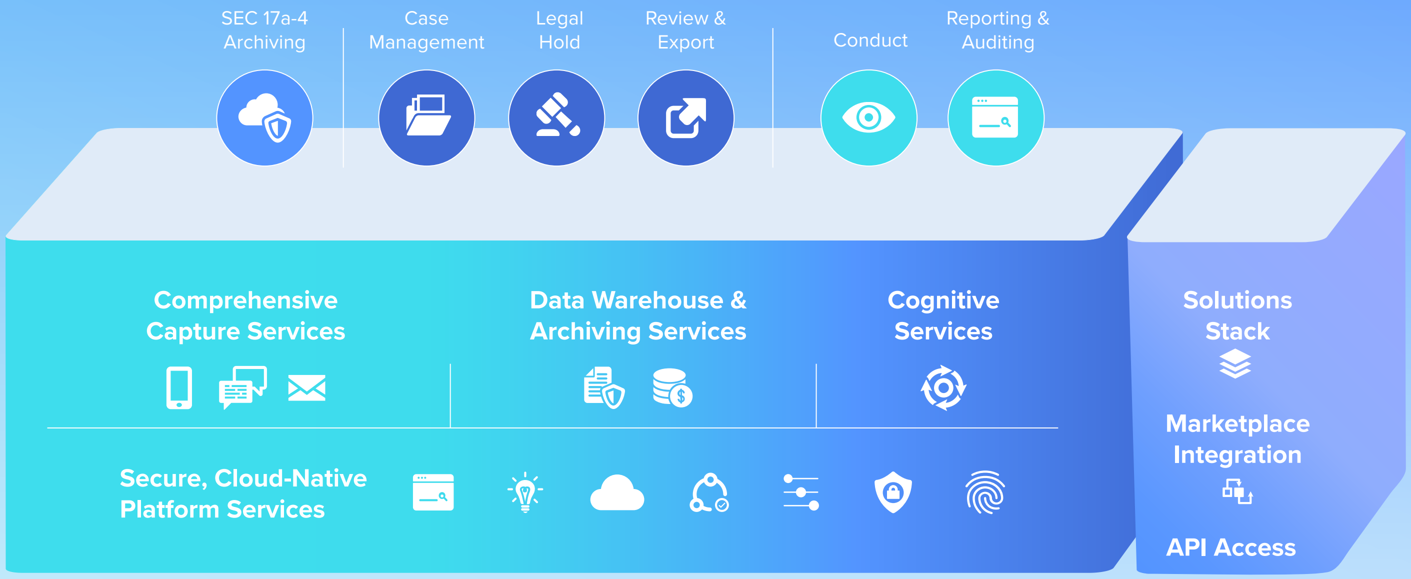
This includes leveraging supervisory systems to review employee communications. More frequent inspection can be provided for higher-risk employees, client-facing staff and executives. Then, uncovered patterns can be fed back into supervisory policies to help stay ahead of areas with greatest potential impact to the organization.

How Smarsh Can Help

Enterprise Platform

Meet the next generation of communications intelligence with the 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 email, mobile, social, IM & collaboration, video and voice tools used today. Retain and index important contextual details to speed up and improve supervision and e-discovery reviews.

Enterprise **Archive**

Enterprise Archive is the 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.

Conduct

For communications supervision and surveillance, Conduct Intel is AI-powered so you can quickly identify and act upon risk in your organization, all while dramatically reducing noise in your review queues.

Discovery

Collect, preserve, review and export digital communications data on-demand to reduce the time and cost of e-discovery.

Meet the evolving needs of your business

Smarsh has architected its solutions specifically to be able to support your business as it evolves. Our products are equipped with open APIs for the ingestion, enrichment and export of 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.

References:

1) https://securityscorecard.com/blog/what-is-information-risk-management

2) https://www.smarsh.com/guides/electronic-communications-supervision-survey-report-common-practices-procedures-financial-firms

3) https://www.npr.org/sections/health-shots/2019/05/13/722881642/states-sue-drugmakers-over-alleged-generic-price-fixing-scheme

4) https://www.justice.gov/usao-ndca/pr/pge-ordered-develop-compliance-and-ethics-program-part-its-sentence-engaging-criminal

5) https://www.hhs.gov/about/news/2019/10/02/dental-practice-pays-10000-settle-social-media-disclosures-of-patients-phi.html

6) https://www.wsj.com/articles/former-fbi-agent-sues-justice-department-over-firing-11565116096

7) https://www.theverge.com/2019/12/5/20995453/away-luggage-ceo-steph-korey-toxic-work-environment-travel-inclusion

8) https://www.theverge.com/2020/1/9/21059420/boeing-employees-messages-737-max-investigation-simulator-crash

9) https://www.bloomberg.com/news/articles/2018-04-13/apple-warns-employees-to-stop-leaking-information-to-media

10) https://www.cnbc.com/2019/05/03/tesla-email-warns-employees-stop-leaking.html

11) https://www.bloomberg.com/news/articles/2020-08-10/mcdonald-s-sues-former-ceo-easterbrook-to-recover-severance-pay

12) https://www.smarsh.com/report/gartner-magic-quadrant-2022

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 electronic 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 advisors and U.S. state and local government agencies. To discover more about the future of communications capture, archiving and oversight, visit www.smarsh.com.

Smarsh provides marketing materials for informational purposes only. Smarsh does not provide legal advice or opinions. You must consult your attorney regarding your compliance with applicable laws and regulations.

White Paper - 08/03/2022

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