GUIDE

Supervision Best Practices

Being proactive instead of reactive about your compliance

smarsh®

Introduction

Supervising business communications and monitoring for regulatory compliance is essential to ensuring the smooth functioning of business operations while minimizing legal and reputational risks. However, compliance has become especially challenging for firms with the boom of communications technology and the massive amounts of data being produced because of this growth. On top of that, regulatory requirements continue to evolve and penalties for non-compliance grow more severe.

By implementing best practices around policies and guidelines, employee training, and monitoring mechanisms, supervisory teams can effectively mitigate risks and ensure that their organization's electronic communications are managed in a responsible and compliant manner.

Supervision Best Practices

Regulators require firms to be able to monitor and review conversations in a timely manner. 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.

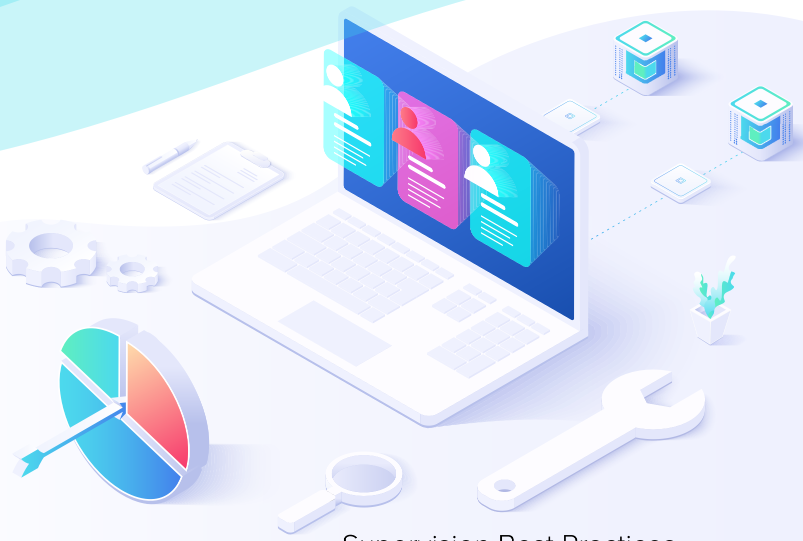
Below is an outline of four best practices to achieve an adequate supervisory system.

1. Establish clear policies and procedures

To establish an effective supervisory system, firms must create clear policies and procedures regarding the use and monitoring of digital communications. Policies and practices should be regularly reviewed and updated, as should technology, to cover new client and employee communication methods. Firms should have a reasonable system to monitor for compliance with the firm's WSPs.

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 the five percent designated 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 risk not finding misbehavior by only reviewing a certain percentage 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 steps will be taken in the case of non-compliance. Organizations should also have a policy 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 have fair and documented consequences. Ensure you have documentation you can share with regulators to show that you handled the violations of 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 ensure compliance obligations are being met, supervision technology capabilities should include the following:

- Advanced supervision workflow
- Multi-tier review queues
- Visual dashboards
- Action panels
- Roles reporting
- Escalation
- Customizable policies
- Model risk governance processes where the paperwork for each model is provided
- Above and below-the-line testing to show regulators why they've set model thresholds at specific levels

The timely review of electronic communications is a first-line defense for firms against improper conduct by employees. Organizations should partner with a technology vendor that can provide efficient and effective tools to 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 with the technical ability to electronically document reviews and create an audit trail. If a message 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 diminishes.

Firms should periodically gather feedback from employees and peers who 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 annually 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 any 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 garner million-dollar fines.

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.

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.

Guide - 06/23

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