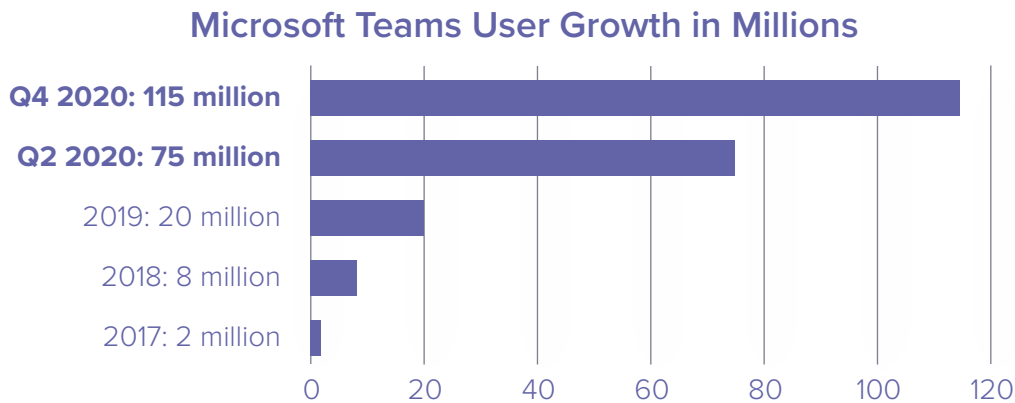


# Checklist

## Microsoft Teams Communications Compliance



Microsoft Teams is the fastest growing workplace collaboration tool available today. It has been critical to many organizations during the work-from-home era, resulting in a major increase in users from 44 million in March 2020 to 115 million in the final quarter of the same year.<sup>1</sup>



As the workplace has dispersed to home offices, the Teams platform has taken the place of the brick-and-mortar office. It's replaced the watercooler for quick chats, the conference room for collaboration and meetings, and the board room for making strategic decisions. In short: Teams is where business happens.

In the most recent *Smarsh Annual Risk & Compliance Survey Report 2020*, Microsoft Teams was the most popular collaboration platform, used by 53% of respondents—more than almost all other options combined.

## Microsoft Teams: risks and benefits

For all its benefits as a business hub, without the right solution in place to govern its usage, Teams opens organizations up to risk. These include legal or conduct breaches, data loss and/or noncompliance with regulatory recordkeeping or oversight mandates. Organizations don't have to slow down their pace of business if they take appropriate measures.

If you've already chosen Microsoft Teams for collaboration, you've taken the first step toward achieving harmonious communication organization-wide. Now it's time to put guidelines and technology in place that will increase productivity and address potential risks at the same time.

This **Microsoft Teams Communications Compliance Checklist** will help you cover all your bases, whether you are:

- Using Teams to support remote work, but not archiving the communications
- Using Teams to support remote work and archiving communications, but not satisfied with your current archiving solution
- Interested in using Teams, but held up on deployment because of risk and/or compliance concerns

Find out where you stand now and where you need to be to enjoy the benefits of Teams' robust collaboration capabilities. And keep your organization protected from regulatory and legal risk.

<sup>1</sup> <https://www.businessofapps.com/data/microsoft-teams-statistics/>

## Did you know?

On July 31, 2021 Microsoft finalized its end-of-life (EOL) program for Skype for Business Online, requiring current users to migrate to Microsoft Teams. Smarsh can help you maintain compliance through the transition by providing support for whichever communications tools you're using for business.

## Questions to get started

Before diving into the checklist, we recommend that you consider the following questions to see how prepared you are for an examination, audit or legal request that includes content from Teams.

Yes No

### Did you know that Teams messages are subject to regulatory scrutiny?

Regulators like FINRA and the SEC require financial organizations to preserve and monitor electronic communications. This includes email, text messages and content from newer communications technologies like Teams. Adopt an archiving solution that can support Teams to stay ahead of recordkeeping compliance, now and in the future.

Yes No

### Does your agency have a mobile device policy?

Whether your organization uses company-issued mobile devices, or you enable a bring-your-own-device (BYOD) policy, employees should be aware of and understand the rules for being compliant with regulatory obligations. These rules should be updated to account for any new mobile applications that employees are using to communicate—like Teams. Document your mobile device policies, be explicit about allowed and prohibited mobile applications, and share mobile policies with staff regularly.



### Compliance Gap

According to the [2020 Smarsh Annual Risk & Compliance Survey Report](#), almost a third of companies surveyed (28%) indicated they do not have an archiving or supervision solution in place for collaboration platforms like Microsoft Teams, even though they allow employees to use them. If content from Teams is requested in a regulatory examination or is needed for a legal proceeding, organizations without a retention and oversight solution are vulnerable to regulatory or legal consequences.



## Microsoft Teams communications archiving checklist

### Evaluate your current archiving and supervision solution.

Compliance and legal teams need to be able to search, review and understand the context of an expansive, complex and interactive conversation among an organization's participants. When it comes time to review content for misconduct, it must be precise and contextual for reviewers to be effective. If content needs to be retrieved for an audit or investigation, it will need to be delivered promptly and comprehensively. These can be laborious, expensive processes if the data is hard to access and missing key details.

A robust archiving solution will have the following capabilities:

- Handles multiple content types
- Preserves original message format (doesn't convert to email)
- Captures full, contextual message threads
- Capable of long-term storage
- Flexible cloud-deployment options
- Scalable and extensible to accommodate more data and new channels
- Provides supervision and/or surveillance monitoring
- Features user-friendly search and review capabilities

Consider the power and reliability of a centrally managed solution for capturing, archiving and producing complex, potentially high-volume historical content on demand.

### Collect and preserve *all* content that is generated on Teams.

One of Teams' benefits is the diverse range of communication and collaboration that converge within. However, activities like editing or deleting Teams messages, file sharing in direct chats, collaboration on a document, etc. can also be material to an investigation. Unfortunately, many tools for capturing message content miss important "event" information, as well as interactive activities. Here's a list of data types that now fall into the category of business communications with the use of Teams:

- |            |                |               |                    |
|------------|----------------|---------------|--------------------|
| • Links    | • Leaves       | • Videos      | • Group chats      |
| • Comments | • Dates        | • Emojis      | • Private chats    |
| • Replies  | • Time         | • Gifs        | • Video calls      |
| • Edits    | • Images       | • Stickers    | • Voice calls      |
| • Deletes  | • Screenshares | • Hand raises | • File sharing     |
| • Joins    | • Attachments  | • Questions   | • In-meeting chats |

Teams helps businesses maintain continuity by providing a virtual office setting. Conversations and collaboration now happen through video meetings, voice calls and chats. A solution that can capture communications in all formats, in native context, and directly from the source, is the most reliable way to mitigate potential risk when the time comes.

## □ Review applicable regulatory requirements for supervising communications.

Many regulated organizations face dual priorities of 1) performing an ongoing systemic review of content to meet SEC, FINRA, CFTC and MiFID II requirements, and 2) the need to periodically perform ad-hoc searches against their entire collection of data to investigate policy violations. These dual priorities require a two-pronged solution.

### Firms must have:

- Supervisory capabilities to test enforcement of regulatory compliance policies
- A powerful supervision system that allows them to spot other potential infractions and respond to unplanned regulatory inquiries

These requirements can be best provided by a policy engine that enables multiple methods (i.e., lexicon policies, random sampling and AI surveillance) to identify risky behavior with precision. Policies make the supervision and review process less laborious and more effective. They can be fine-tuned to drastically cut out white noise and reduce the number of messages that require review in the first place.

## □ Consider potential data privacy, security, human resources and legal risks that may arise due to wide-scale adoption of Teams.

In the event of a discovery request or investigation, companies may be required to process and submit large volumes of content from Teams and all other communication channels, and in short order. This can be a disruptive and expensive process. An archive with advanced preservation, search and surveillance capabilities is crucial if any of the following are potential occurrences:

- Data privacy investigation
- Code of conduct violations
- Regulatory audit or data request
- Intellectual property loss
- Information security breach
- Internal investigations
- Other litigation

This is a good time to review applicable and emerging data privacy laws (think GDPR in the European Union, California's CCPA, etc.) and consider those parameters in your data collection strategy. Organizations that operate in multiple geographies must maintain and store data to meet specific regulatory requirements in various regions.

### Recommended Reading:

*Managing Global Data Privacy Laws and Communication Regulations in Financial Services*






## □ Develop and implement a training program to address employee use of Teams.

Training employees on appropriate Microsoft Teams usage policies early and often is a key part of managing comprehensive compliance. We recommend putting together documented guidelines for how employees should conduct themselves on each communication application. Make sure training is explicit and outlines both acceptable and prohibited terms of communication.

Wherever possible, automate policy enforcement with existing infrastructure and incorporate into onboarding processes. If an employee's content is being captured and supervised, make sure they know it at the outset. Require signed attestation that they have gone through training. Stay engaged with employees as the tool and its integrations evolve, and reassess your policies as needed.

## Smarsh & Microsoft Teams: Better Together

A longtime relationship between Smarsh and Microsoft provides a unique vantage point into how to best leverage the investment in Microsoft products and enable recordkeeping and legal preparedness for regulated and litigious organizations.

-  **Capture:** Smarsh directly captures Teams content from the source through API integration. This includes video, voice, chat, point-in-time snapshots of joins, leaves, edits, deletes, comments, emojis, replies and attachments, all of which create multi-layered, ongoing conversations. No matter what type of communication data is produced in Teams, and regardless of a user's device, location or network, Smarsh preserves its chain of custody, context and original format.
-  **Archive:** Microsoft Teams communications can be sent seamlessly to the Smarsh archive, an immutable and context-aware data store. You can perform an advanced search for Teams-specific records, and data is produced quickly and easily, making the process faster and more accurate.
-  **E-discovery and risk mitigation:** Users can quickly collect, organize and cull data to enable informed strategic decisions during early case assessment, while managing risk. The combined solution provides a highly secure, defensible and auditable workflow across all electronic communication.
-  **Compliance:** Smarsh provides native compliance and governance for all Teams content. Employees can collaborate seamlessly while meeting strict SEC, FINRA, FFIEC, CFTC, NFA, MiFID II, FCA, IIROC and other records retention and oversight requirements around the world.
-  **Supervision and surveillance:** Microsoft Teams content is processed through high-powered Smarsh policy engines, and conversations are classified as they enter the archive. Important or problematic keywords, phrases or other criteria are flagged on qualifying messages. Policy controls can be fine-tuned to help meet regulatory, legal and corporate obligations. Surveillance for employee misconduct is also a major legal concern. A combined supervision and surveillance solution with AI and NLP capabilities provides a proactive, single line of defense for regulatory inquiries and misconduct issues.

Empower your teams to confidently communicate and check risk and regulatory compliance off the list with Microsoft Teams and Smarsh.







Smarsh® enables companies to transform oversight into foresight by surfacing business-critical signals in more than 80 electronic 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](http://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.