Aware

WHITEPAPER

COLLABORATION DATA GOVERNANCE

ALIGNING IT, LEGAL, & SECURITY RISKS

5 BEST PRACTICES
For managing the risks of the digital workspace

THE ALIGNMENT **OF LEGAL, IT & SECURITY RISKS**

The digital workplace generates massive amounts of data, and it's growing all the time. **By 2023, more than 40% of workers will be working remotely at least one day a week.**[1] This transformation increased the adoption collaboration tools, building a mountain of technical debt that now looms large over the modern enterprise.

As an IT leader, you've watched this growing digital exhaust. You understand that without proper controls it can result in chaos, disorganization and the loss of business-critical information. But tackling collaboration data sets is time-consuming, expensive and incredibly complex. At this point, it may be beyond the capabilities of a single person or department to identify all the ways that unstructured collaboration data impacts the enterprise.

Despite the risks, organizations have embraced the use of workstream collaboration tools such as Slack and Microsoft Teams as a primary way of doing business. At a people level, collaboration makes sense. So much that a Gartner Research Panel found 58% of participants considered collaboration tools to be their most important workplace applications.[3] That means executives expect IT leaders to establish proper policies and procedures to maintain compliance and keep collaboration safe.

To achieve those goals, IT leaders must align with their colleagues in legal and information security departments to understand the true extent of risk within collaboration. Here's what you need to know to make that happen.

Common use cases for governance, risk, & compliance in collaboration include

- **Records Retention**
- **eDiscovery**
- **Compliance Monitoring**
- **Internal Investigations**
- **Data Loss Prevention**
- **Analytics**

THE ALIGNMENT **OF LEGAL, IT & SECURITY RISKS**

Managing Collaboration Chaos is a Team Sport

Legal and infosec teams are often the driving force behind information governance in collaboration, but they rarely grasp the full scope of their requirements. As a technology or application owner, how do you save time and protect your ROI while securing workstream tools to the satisfaction of your colleagues in other departments?

Collaboration tools break down silos and accelerate information-sharing. That's what makes them so powerful as productivity enhancers. It is also the source of the risks they introduce. Out of the box, they lack the governance and retention controls that legal and infosec teams require.

> By 2025, Gartner expects that at least **25% of corporate legal application** spending will go to non-specialist technology providers.[2]

Establishing a partnership between IT and information security is critical to ensuring a cross-functional, sustainable strategy toward tech spending. Together, you can build a stack that future-proofs governance, compliance and legal obligations as this data set evolves and grows.

But what does that partnership look like? How do IT leaders prioritize interdepartmental requirements to balance risk, cost and usability of collaboration tools? In this whitepaper, we'll share the five best practices that leading enterprises use when considering a unified strategy for governance, risk and compliance in collaboration.

Make it Actionable with the Following Best Practices:

BEST PRACTICE
01
Understand the Collaboration Ecosystem, Together

BEST PRACTICE
02
Scope Your Specific Needs & Stakeholders

BEST PRACTICE
03
Understand Where the Data Resides, and Educate on Legacy Vendor Gaps

BEST PRACTICE
04
Clearly Articulate Your Overall Business Requirements for the Project

BEST PRACTICE
05
Think About End Goal Processes & Permissions

BEST PRACTICE #1

UNDERSTAND THE COLLABORATION ECOSYSTEM *(TOGETHER!)*

01

Fully scoping out collaboration data governance across your organization might be a new concept, but the looming risks have always been top of mind for your legal and compliance colleagues.

Your enterprise collaboration ecosystem extends far beyond one or two sanctioned platforms. IT leaders are best positioned to see the true extent of the tools in use, and the risks they represent. Without full visibility across the ecosystem, and the ability to position controls that lock down, preserve and purge where necessary, the organization faces enhanced risk of insider threat, IP loss, data exfiltration and regulatory noncompliance.

To solve this, your first action should be to take stock of your collaboration ecosystem and understand where and how employees communicate. What tools do they use, and who owns and administers them? Where do shadow IT or freemium solutions reside? What conflicting requirements must you resolve for a streamlined, secure ecosystem to be successful?

Only by understanding the needs of collaboration users can you make informed, deliberate decisions about the platforms that should be in use and scope your overarching risk management strategy.

WORKSHEET: BEST PRACTICE #1 UNDERSTAND THE COLLABORATION ECOSYSTEM *(TOGETHER!)*

Platforms	Admins	Users (ex. Departments, all company)	Active?	Sanctioned?	Notes
					
					
					
					
					
					
					
					
					
Other:					
Other:					
Other:					

BEST PRACTICE #2

SCOPE YOUR **SPECIFIC NEEDS & STAKEHOLDERS**

Now you understand your collaboration ecosystem.

Next you should consider the specific needs of your new stack, including:

Operational Requirements: Articulate the driver of each requirement to better evaluate conflicting stakeholder perspectives.

Tech Support: Who is the current administrator of the tool, and how would a consolidated collaboration ecosystem impact their workflow?

Stakeholder: Who ultimately is driving the business need?

Priority: Is the priority a dealbreaker in vendor selection?

Here is a simple example how forward-looking enterprises have approached vendor vetting and decision processes.

Requirement	Tech Support	Stakeholder	Priority
Deletion of Slack public message within 90 days	Slack Admin	Information Governance	High
List of 56 slack channels in which messages must be retained for 12 months	Slack Admin	Information Governance	High
Enablement of legal hold creations & removals	Slack Admin & Legal Ops	Legal	High
Keyword searches across Slack & Zoom chat	Slack & Zoom Admin	Internal Investigations & eDiscovery	Medium

BEST PRACTICE #3

UNDERSTAND WHERE THE DATA RESIDES & EDUCATE ON LEGACY VENDOR GAPS

Collaboration tools are notorious for creating sprawling data sets across multiple locations. Identifying where data resides for each part of your ecosystem is critical to strengthening your overall governance policies and procedures.

Centrally managing the data from even a single collaboration tool is often more complex than first considered. For example, Microsoft Teams integrates into O365 and from there distributes data across multiple silos, making centralized control challenging to implement.

A helpful reference on where data resides within Microsoft Teams

Data Type	Data Format
1:1 Chat, Private Chats & Channel Chats	User Exchange Mailbox *(e.g. Jenna@AwareHQ.com)*
1:1 Chat Files & User's Private Content	User OneDrive Site
Private Channel Files	Dedicated Private Channel Sharepoint Site
Teams Content	Team SharePoint Site
Meeting Recordings	SharePoint for Channel meetings or OneDrive for other types

BEST PRACTICE #3: UNDERSTAND WHERE THE DATA RESIDES & EDUCATE ON LEGACY VENDOR GAPS

Rethink Your Legacy Vendors

As best practice, examine your legacy collaboration vendors and consider how they meet the needs of records retention, eDiscovery, compliance and content monitoring. Your current administrators may believe these risks are under control, but the liability falls to you if they are not appropriately mitigated. That makes uncovering legacy gaps mission-critical to securing your collaboration tools.

The following checklist can help as you work with stakeholders to assess each vendor's performance.

The bullets provide examples of how operational leaders may assess technology to meet the demands of legal and information security departments.

Audience:
Data Management

Goal:
Build a record with full context and data privacy

- Does the platform offer simple administration and user permissions to suit tight data access controls?
- Where is the data stored? Is it easy to capture all of it?
- Is collaboration data converted to email format dependent on license type, losing critical context?

Audience:
Legal

Goal:
Meet eDiscovery and records retention requirements

- Will the platform require manual, intensive processes for full contextual search, export, and analysis for legal workflows?
- Are searches able to be conducted based on various filters, and not just a user?
- Is the system compatible with leading eDiscovery tools, with flexibility to determine what collaboration data is included?
- Are records retention requirements adequately met through granular policies and overarching requirements?

BEST PRACTICE #3: UNDERSTAND WHERE THE DATA RESIDES FOR EACH & EDUCATE ON LEGACY VENDOR GAPS

Audience:
Compliance

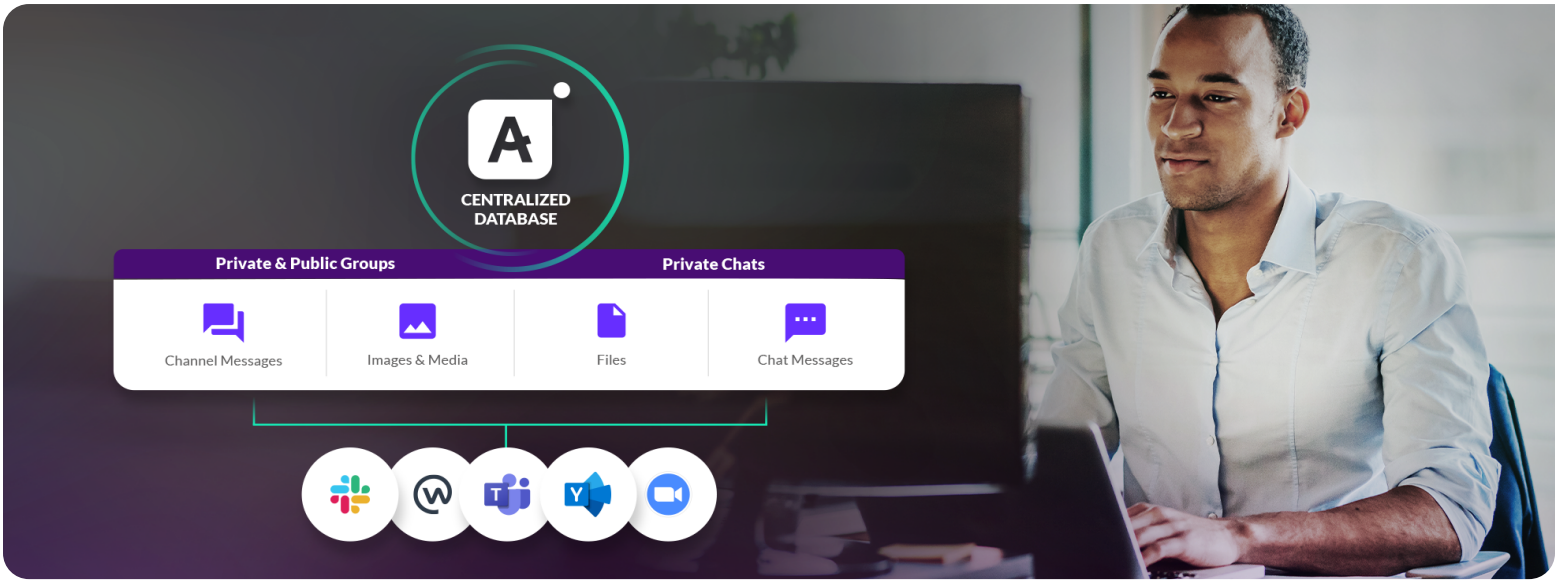
Goal:
Real-time monitoring and moderation to reduce liabilities and coach employees

- Will you need multiple tools for real-time monitoring (i.e., one tool for data loss prevention and a separate tool for compliance or general content moderation)?
- Are monitoring tools automated in-real time to ensure proper remediation, risk mitigation, and data purges as required?
- Do policies within monitoring ingest data in batches or in near real time?
- Will the system easily support all the languages used within your global organization?
- Can granular logic, or AI analysis such as employee sentiment & toxic speech be leveraged to home in on risks and narrow false positives on ethical or unethical behavior?

Audience:
Information Security

Goal:
Normalize and integrate datasets to gain efficient oversight of the entire ecosystem

- Does the platform offer third-party connections to collaboration tools that do not have native, out-of-the-box solutions for risk management (i.e., Slack, Zoom)?
- Is data from other collaboration tools converted into email across consoles, eliminating context and losing business critical data?



BEST PRACTICE #4

CLEARLY ARTICULATE YOUR **BUSINESS REQUIREMENTS FOR THE PROJECT**

The most critical step in the process, after doing your collaboration data discovery work, is to articulate your business requirements clearly and simply. Think carefully about the purpose, scope and business impact you hope to achieve and write them down.

Next, share your goals with all involved counterparts. Chances are they are considering the same problems. There may also be a larger enterprise-wide initiative around information archiving with policies already set up. A simple brief articulating your business requirements could enable existing committees to expand their scope of implementation to employee collaboration.

Note: This is a simple, yet critical step in the process. Do not finalize your purpose, scope or business impact without carefully thinking through all stakeholders that should be involved in shaping the project.

Purpose

The Collaboration Data Governance Team must establish formal records retention, data discovery, and knowledge management practices across company collaboration systems. This may include collaboration data between employee, customers, vendors, and business partners.

Scope

Platforms in scope include: Slack (Messages & Files), Microsoft Teams (Chats & Files), Zoom (Video, Chat & Transcripts)

Business Impact

Formal retention, discovery, and management of this data will mitigate risks to the organization such as:

- Reducing costs of data storage
- Reducing litigation risks
- Reducing potential data breach attack surface
- Ensuring regulatory compliance

BEST PRACTICE #5

THINK ABOUT END GOAL **PROCESSES & PERMISSIONS**

Lastly, don't forget about the end goal once strategies are aligned and the right tools are available for implementation.
Ask yourself a couple simple questions:

- Who should ultimately have access to this data, and does the technology in consideration support the right controls?
- Will new processes need to be set up among team members to manage this data set?
- Should certain teams have varying levels of data access and permissions dependent on data sensitivity level and usage?

The following may be a helpful worksheet to scope out user permissions with the platform you are working on:

Department	Stakeholder	Business Requirement(s)	Data Sensitivity
Example Legal & Compliance	Legal Operations Compliance Manager	Investigations & Litigation	High

CONCLUSION

SO THERE **YOU HAVE IT.**

Five best practices and helpful perspectives to align various stakeholders who have responsibility of IT, legal & security risks across the enterprise when it comes to collaboration data. We hope this templated approach can serve as a simple aid as you build a strategy to manage collaboration chaos in your organization.

Sources

[1]Gartner's Technology to Support Collaboration for a Hybrid Workforce
[2]https://www.gartner.com/smarterwithgartner/5-legal-technology-trends-changing-in-house-legal-departments
[3]Gartner's Market Guide For Workstream Collaboration