



A Framework for Managing Digital Communications Governance and Archiving (DCGA)

By Ryan Thorpe, Director – Financial Services

Sole Consulting

www.soleconsulting.co

Why Companies Need A New Approach

Unified Communications have become the backbone of the financial services industry, revolutionizing how transactions and interactions are conducted. Over the past 20 years, electronic communication channels have evolved rapidly, from emails and instant messaging to complex financial trading systems and collaborative productivity applications. However, this digital transformation has also brought increased regulatory scrutiny from entities like the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA), making compliance a critical challenge.

The rise of hybrid work and the proliferation of digital communication platforms have further complicated record keeping requirements. Employees now rely on a vast array of productivity applications, chat tools, collaboration platforms, and social media to stay connected. Organizations must track, archive, and monitor these communication channels to comply with industry regulations.

\$3 BILLION

IN FINES LEVIED SINCE 2022*

With over \$3 billion in fines levied since 2022 for record keeping and surveillance failures, companies must move beyond siloed compliance teams and adopt a more agile, scalable approach. The future of Digital Communication Governance and Archiving (DCGA) lies in shared accountability, cross-functional collaboration, and a comprehensive strategy for managing people, processes, and technology. Companies that fail to modernize will struggle to scale compliance operations and risk severe financial penalties and reputational damage.

Our Framework for an Effective Digital Communications Governance and Archiving Capability

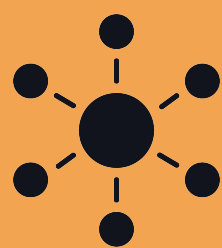
SOLE'S 4-PART DCGA FRAMEWORK

OVERSIGHT



Evolve DCGA capabilities to drive better outcomes

CAPTURE



Collect and archive UC correspondence and business records

RETENTION



Produce, preserve, and review correspondence

MONITORING



Supervise UC correspondence for policy violations and risk

A successful DCGA strategy requires focusing on four key pillars: Oversight, Capture, Retention, and Monitoring. Together, these pillars provide a robust framework for compliance in today's complex communication environment.

*Sources:

CFTC (Commodity Futures Trading Commission) FY 2024 Enforcement Results [Link](#)

SEC Recordkeeping Failures Reports [Link](#)

Oversight

A well-structured oversight function brings together key stakeholders across the enterprise, defining strategy, roadmaps, and governance models that establish a foundation for regulatory adherence.

However, oversight is not just about setting policies. It is about continuous engagement, accountability, and the ability to pivot as new challenges emerge in the digital communication space. Oversight ensures alignment across business units, enabling organizations to shift from reactive adjustments to proactive risk management and continuous improvement.

Organizations go wrong by taking a siloed approach to compliance, relying on IT to implement technology solutions with minimal collaboration from Legal and Compliance teams, who define regulatory requirements and guide business operations. This fragmented approach results in compliance programs that address immediate challenges but lack a cohesive long-term strategy. Without a clear roadmap, organizations risk redundant technologies, inefficient processes, and compliance gaps as regulations and business needs evolve. A well-structured oversight function fosters collaboration across IT, Legal, Compliance, and Business stakeholders, ensuring compliance solutions are integrated, scalable, and strategically managed.

KEY CONSIDERATIONS FOR DIGITAL COMMUNICATION GOVERNANCE

To build a robust compliance framework, organizations must be able to answer the following critical questions:

1

What unified communication (UC) applications do employees have access to?

This could include, but is not limited to, video conferencing platforms, SMS, email, collaboration tools, web-based applications, social media, and digital whiteboards.

2

Which applications are preferred, and which require capture, archival, and supervision?

Understanding usage patterns helps organizations prioritize compliance efforts and better understand where risk resides in an organization's data. Without visibility into preferred applications, organizations risk the rise of Shadow IT, where unapproved tools are used for business communication, leading to compliance vulnerabilities and regulatory violations.

3

What data needs to be preserved, made accessible, and supervised?

Defining the scope of data retention and supervision ensures alignment with regulatory requirements and reduces the risk of non-compliance. However, not all communications may need to be captured. Distinguishing between relevant and irrelevant data is essential for an efficient compliance strategy.

To stay ahead of regulatory expectations, organizations must implement a dynamic and forward-thinking governance framework that continuously monitors communication trends, encourages proactive collaboration among stakeholder groups, and adopts advanced compliance technologies. By understanding employee communication behaviors and implementing a comprehensive governance strategy, organizations can confidently navigate the evolving regulatory landscape.

Capture

Effective capture is the backbone of a compliant digital communication strategy. It ensures that required data is collected, stored, and retrievable for regulatory and business purposes. A structured approach to capture prevents data gaps, compliance failures, and operational inefficiencies, allowing organizations to maintain control over their digital communications.

However, many organizations struggle to scale capture capabilities because they centralize responsibility within a single IT team. With new communication solutions and features constantly emerging, expecting one team to stay fully informed on every technology roadmap is unrealistic. Without cross-functional collaboration, compliance requirements may be overlooked and capture processes may fail to keep pace with business needs. To scale effectively, organizations must embed capture requirements into the technology roadmaps of IT, architecture, and product teams responsible for individual applications. This proactive approach ensures compliance is integrated into development rather than addressed reactively. In turn, this makes it a shared responsibility across the organization.

KEY STEPS FOR DEFENSIBLE CAPTURE

1

Establish Consistent Data Capture Patterns:

Standardized capture methods streamline compliance, ensure data integrity, and enable scalability as new communication applications emerge. A consistent approach reduces complexity, making validation and troubleshooting more efficient.

2

Map and Monitor Data Lineage:

Organizations must understand their data's entire journey, from its source application to its final archive destination. Mapping data lineage helps identify potential failure points, ensuring that every step of the capture process functions as intended, and that no critical information is lost.

3

Validate and Reconcile Captured Data:

It is not enough to send data to an archive—companies must have robust validation processes to confirm that all required records have been successfully ingested. Regular reconciliation checks and automated monitoring help ensure completeness, reducing the risk of non-compliance due to missing or corrupted records.

A defensible capture strategy combines scalability and consistency by integrating capture requirements into application roadmaps and maintaining reliable data processes. Regular audits, reconciliation checks, and automation help uphold data integrity and completeness, while human- and machine-readable formats enable compliance reviews, eDiscovery, and AI analytics. Embedding transparency and rigor into the capture process minimizes the risk of incomplete or lost data, strengthening compliance.

Retention

Retention is fundamental to maintaining compliance, ensuring digital communications are systematically preserved, accessible, and governed by regulatory mandates. It serves as the foundation for effective capture, supervision, and eDiscovery. A well-defined retention approach ensures that organizations manage data efficiently, reduce risks, and maintain accessibility for legal and regulatory needs.

Companies without a cohesive retention strategy often accumulate redundant archive technologies, storing outdated or unnecessary data, which drives up platform and storage costs. These inefficiencies create a fragmented search and discovery process, where dispersed and inconsistent data slows down access, leading to operational delays and a frustrating user experience. As a result, responding to legal or regulatory requests becomes more difficult, with delays in eDiscovery or compliance audits, ultimately increasing the organization's risk exposure.

KEY PRINCIPLES FOR AN EFFECTIVE ARCHIVING STRATEGY

- **Keep Only What's Necessary:**
Store data based on tailored retention policies to meet global regulatory requirements while avoiding unnecessary risk and cost.
- **Preserve Data in a Usable Format:**
Ensure that captured data is both human- and machine-readable for review and compliance processes.
- **Centralize Where Possible:**
Consolidate archives to simplify supervision, reduce costs, and improve efficiency.
- **Optimize for Search and eDiscovery:**
Archived data should be structured for fast, accurate retrieval to support eDiscovery, audits, and investigations.
- **Secure and Govern Access:**
Protect data with strict access controls and audit trails to ensure compliance and security.

A well-executed retention strategy enables organizations to maintain compliance, control costs, and respond efficiently to legal and regulatory inquiries. Common symptoms of outdated or fragmented strategies are excessive data storage costs, inefficient search and discovery processes, and difficulty responding to legal or regulatory requests. Retention is not merely about storing data, it is about governing information in a way that supports supervision, eDiscovery, and long-term compliance objectives.

Monitoring

Effective monitoring is essential for identifying and mitigating compliance risks in digital communications. As organizations adapt to evolving regulatory expectations, traditional lexicon-based surveillance methods are proving inadequate, leading to high alert volumes, excessive false positives, and inefficient review processes. To address these challenges, modern compliance programs are shifting toward NLP/ML-driven surveillance models, enabling organizations to take a data-driven approach to refine policies, improve detection accuracy, and focus on genuine risks rather than noise.

NLP/ML is not a “set it and forget it” solution. Compliance teams must regularly review and refine surveillance models to keep pace with evolving risks and regulatory requirements while ensuring the models consistently operate within expected parameters. For many, this requires a shift from the traditional approach, where lexicons were occasionally updated with IT support, to adopting a product mindset. In this model, Compliance teams must treat policies as products that demand ongoing attention, development, and improvement. They will need to establish processes for analyzing alert data, extracting insights, and implementing policy changes. Effective product lifecycle management requires close collaboration between Compliance and IT teams, along with robust change management and disciplined documentation. Transparency and explainability will be essential, as both regulators and internal stakeholders will need insight into how these models operate and impact compliance outcomes.

HOW TO BUILD AN EFFECTIVE MONITORING STRATEGY

Develop Targeted Surveillance Policies:

A one-size-fits-all approach to monitoring is no longer sufficient. Organizations should tailor policies to specific business risks, leveraging NLP/ML to refine detection models, reduce false positives, and enhance alert quality.

Continuously Review and Optimize NLP/ML Models:

Model-driven monitoring requires ongoing oversight. Compliance teams should establish governance processes to regularly assess model performance, ensuring alignment with regulatory and business objectives.

Ensure Explainability and Documentation:

As NLP/ML adoption grows, compliance teams must be prepared to explain how models operate and how they influence decision-making. Explainability is key to regulatory trust and effective risk management.

Level Up Team Skillsets:

Individuals with a deep understanding of both technology and compliance issues will be in high demand. Compliance teams looking to leverage AI/ML must enhance their technical acumen, supporting their regulatory technology transformation journey.

Looking Forward

AI-powered review assistants represent a pivotal advancement, enabling compliance teams to scale operations more effectively by reducing manual workloads and enhancing risk detection. As AI and machine learning continue to evolve, technology-savvy compliance professionals will play an increasingly critical role. To stay ahead, organizations must prioritize developing technical expertise within their teams, ensuring they can navigate the intersection of regulatory expectations and technological advancements.

Moreover, the importance of model explainability cannot be overstated. As AI/ML solutions play a more prominent role in compliance, teams must be able to articulate how these models function and are applied within business processes. Regulators like the SEC, FINRA, and CFTC have collectively stressed the importance of transparency, robust oversight, and comprehensive risk management in the deployment of AI technologies. Organizations need clear governance mechanisms, such as human-in-the-loop (HITL) oversight, to validate AI outputs and mitigate regulatory risks. This ability to explain and justify AI-driven decisions will be a critical competency for compliance teams, ensuring transparency, accountability, and alignment with regulatory standards and organizational goals.

By embracing these principles, organizations can achieve compliance and unlock new opportunities for growth and resilience in the digital era.

Why Sole Consulting?

1

Sole Consulting brings a unique perspective to the challenges experienced by financial services firms, built from on-the-ground experience with leading companies.

2

Our DCGA framework offers organizations a scalable and adaptable solution to navigate the complex and ever-evolving landscape of digital communication regulations.

3

By integrating strategic oversight, robust data capture, disciplined retention, advanced monitoring, and comprehensive support systems, businesses can ensure compliance while fostering growth and innovation.

4

Sole embeds within your organization, engaging as a partner to help your IT, compliance, legal, and business teams define and deliver the target state.

Headquartered in Los Angeles, Sole Consulting is a management consulting firm serving enterprise companies. We help clients realize meaningful business and technology change by leveraging our decades of experience, ensuring the solution fits the unique needs of each client, and building strong client relationships. We work with our clients as partners and advocates. Many of our clients have worked with us for years — a testament to our approach.

Let's Connect



Adam Vagley
Partner, Financial Services
adam.vagley@soleconsulting.co



Ryan Thorpe
Director, Financial Services
ryan.thorpe@soleconsulting.co

