Modern eDiscovery & Surveillance for Regulated Entities

A perspective for 2026 and beyond

Tech Brief | March 2026

Contents

Summary

Across the financial services, government, and critical infrastructure sectors, regulators are redefining what effective compliance looks like. The focus is shifting from simple record-keeping to demonstrable visibility, accountability, and defensibility across every communication channel.

The volume and variety of digital communications have created an increasingly fragmented and risk-prone landscape. Regulators expect firms to monitor, capture, and preserve all business communications that could influence market integrity or regulatory reporting outcomes.

At the same time, privacy and data protection frameworks such as GDPR, the Australian Privacy Act, and Singapore's PDPA impose obligations to minimize data collection and processing. This intersection of surveillance and privacy obligations results in complex and overlapping compliance requirements that cannot be met by technology alone. To support organizations in understanding these evolving expectations, this paper:

- Examines how regulatory, operational, and privacy drivers are converging across communication governance.
- Explores the need for a unified, risk-based, platform-centric approach to eDiscovery and surveillance.
- Contrasts tactical "just good enough" practices with defensible governance models that strengthen organizational accountability.
- Outlines how integrated visibility enhances transparency, resilience, and trust across modern regulatory operations. .

Objective and Audience

The purpose of this paper is to help compliance, risk, and technology leaders in regulated industries understand how evolving expectations are reshaping the landscape of eDiscovery and communications surveillance. It examines the core challenges faced by institutions that rely on fragmented or native tools, and outlines how modern platform architectures capable of aggregating, classifying, and governing content from multiple sources provide operational efficiency and regulatory confidence.

Specifically, it aims to:

- Clarify the implications of evolving obligations for communications monitoring and data governance.
- Highlight the limitations and risks associated with tactical approaches to compliance
- Demonstrate how a platform-centric model improves defensibility, reduces operational complexity, and enhances resilience

In doing so, Arctera helps decision-makers move beyond cost-driven compliance toward outcome-driven governance, ensuring that eDiscovery, surveillance, and data management systems serve both regulatory intent and organizational trust.

Key Terms

For this document, the following terms are used consistently throughout:

Surveillance

Surveillance refers to systematic monitoring, capture, and analysis of communications and activities within an organization to identify potential risks, misconduct, or regulatory breaches. In regulated industries, surveillance extends beyond traditional email review to include voice, video, chat, collaboration tools, and social media. Its purpose is to support transparency, detect inappropriate or unlawful behaviors, and demonstrate compliance with legal and regulatory obligations. Effective surveillance combines technology, governance, and human oversight to provide assurance that relevant communications are visible, traceable, and defensible. Increasingly, it incorporates AI and automation to support proactive monitoring and risk detection.

eDiscovery

eDiscovery is the process of identifying, preserving, collecting, and analysing electronically stored information (ESI) that may be relevant to investigations, litigation, regulatory inquiries, or internal reviews. It enables organizations to locate and produce digital evidence from sources such as emails, chat messages, documents, and structured data systems. In regulated environments, eDiscovery underpins legal defensibility by ensuring that information is preserved, searched, and produced in a manner that is accurate, transparent, and verifiable. It plays a central role in demonstrating compliance, maintaining accountability, and supporting informed decision-making through controlled and auditable digital information management.

Content Aggregation

Content aggregation refers to the process of capturing and consolidating communications and information from a wide range of disparate sources into a unified environment for classification, tagging, and indexing. This enables organizations to apply consistent governance, search, and review processes across diverse data types, including email, chat, voice, video, collaboration tools, social media, and AI-generated communications. In regulated settings, content aggregation supports both eDiscovery and surveillance by ensuring that relevant communications can be located, analyzed, and preserved in a defensible manner. It also enables transcription, translation, and contextual processing to support business, compliance, and investigative objectives within an integrated governance framework.

The Compliance Imperative

Modern compliance is driven by the principle of transparency. Regulatory requirements such as APRA CPS 230, CPS 234, CPS 235, ASIC INFO 283 (Australia), MiFID II (EU), FINRA/FCA (USA), impose explicit expectations for organizations to capture and produce complete communication records. These rules are no longer confined to financial transactions but extend to internal collaboration, remote work, and third-party service providers.

Regulators, including the Financial Conduct Authority (UK) and authorities enforcing MiFID II (EU) mandate the retention of all business communications—not just email—that are relevant to financial transactions. Between 2021 and 2024, the Financial Conduct Authority (FCA) issued fines of more than US$2 billion in civil proceedings to companies such as JPMorgan Chase, Goldman Sachs, Morgan Stanley, Citigroup, Barclays, Bank of America, UBS, and Credit Suisse.

The direction of travel is clear. To remain compliant, organizations must be able to locate, preserve, and produce all regulated communications, or more precisely, must have the right tools and governance in place to capture communications across channels and devices.

Expectations for Visibility and Accountability

Across jurisdictions, regulators are redefining what it means to maintain compliance visibility. No longer satisfied with record-keeping in isolation, they now expect continuous monitoring, demonstrable accountability, and proactive governance across all communication channels, including emerging and encrypted technologies and platforms.

ASIC (Australia) has issued Information Sheet 283: Supervising Your Representatives' Business Communications, directing market intermediaries (entities or individuals that participate in, facilitate, or provide services for trading or investment in financial markets) to actively monitor and retain business communications, including emails, voice calls, and messaging apps. ASIC stresses that unmonitored or unapproved channels such as WhatsApp and Signal represent compliance blind spots. A 2024 media release reinforced that failure to monitor new communication channels may breach both the Corporations Act and Market Integrity Rules.

APRA (Australia), Prudential Standard CPS 234, mandates that regulated entities identify, classify, and secure all information assets, including communication systems, with controls proportionate to their criticality and sensitivity. APRA has reinforced that boards must maintain oversight of information security controls and demonstrate how incidents and data risks are managed. These expectations directly link governance visibility to operational resilience, including obligations under CPS230.

The Office of the Australian Information Commissioner (OAIC)'s 2025 report reinforced the same principle: most agencies using encrypted messaging apps failed to meet archival or Freedom of Information (FOI) obligations. This created heightened risks of unlawful destruction under the Archives Act. The recommendation is that all digital communications, including disappearing messages, be treated as official records requiring capture and classification.

MiFID II (EU) requires firms to record, retain, and monitor all relevant communications for at least five years, ensuring compliance, transparency, and preventing unmonitored business communications. This includes emails, phone calls, instant messages, social media, and other electronic communications related to transactions. MiFID II has a broad scope, in that, anything that could lead to a transaction must be captured, per Article 16(7), firms are required to record both telephone conversations and electronic communications "relating to" orders, transmissions, or executions, even where a transaction does not ultimately occur.

Under MiFID II, non-compliance with communications-recording obligations can result in administrative fines of up to €20 million or 4% of global annual turnover, whichever is higher, as stipulated under Article 70 of the Directive. While few firms have reached this threshold, national regulators have already imposed significant penalties for failures to record or retain required communications.

FCA (UK) has adopted a more direct surveillance posture such as its Multi-Firm Review on Off-Channel Communications (August 7, 2025) and Market Watch newsletters (issues 66 and 79). These publications emphasise that firms must monitor, capture, and retain all transaction-related communications, including those conducted remotely or on personal devices. The FCA has urged firms to move beyond reactive controls toward proactive detection of off-channel communications, citing persistent gaps in supervising non-approved chat tools and personal devices. These findings reinforce that effective surveillance must apply consistently across the organization, regardless of role or seniority.

Enforcement Signal – FCA

41% of off-channel communication breaches involved individuals at the Director level or above, reinforcing the need for proactive detection across all roles.

The FCA has also highlighted weaknesses in vendor oversight and surveillance systems controls, including data gaps and missing records that undermine compliance reporting. Importantly, these findings have been framed as governance failures rather than isolated technical issues, reinforcing senior accountability for communication monitoring controls.

Governance Expectation – FCA

Weak communication controls are increasingly being assessed by the FCA as governance failures rather than technical shortcomings.

In the United States, the **Securities and Exchange Commission (SEC)** and FINRA have imposed substantial fines on firms for failing to capture off-channel communications such as WhatsApp and personal text messages. FINRA's 2024 Oversight Report calls for end-to-end supervision of all digital communications, periodic testing of surveillance systems, and remediation of unmonitored channels. Communication oversight is now treated as a core governance requirement central to market integrity.

Since 2021, the SEC has led a sweeping series of enforcement actions against major financial institutions for breaching their legal duty to preserve business-related communications under the Securities Exchange Act. With cumulative penalties now exceeding US $2 billion, these actions demonstrate a sustained and escalating focus on off-channel communications and recordkeeping controls. Enforcement outcomes make clear that monitoring and retention obligations apply across all employee levels, devices, and locations.

Key enforcement actions to date:

- **Twelve firms—January 13, 2025–approximately US$63.1 million combined**
  The SEC charged Apollo Global Management, Blackstone, Charles Schwab, Guggenheim Partners, Houlihan Lokey, KKR, Moelis & Company, Oaktree Capital, PJT Partners, Santander US, The Carlyle Group, and TPG for failures to preserve business-related electronic communications on unapproved channels. Employees routinely used WhatsApp, Signal, and text messages for client and investment discussions.
- **Twenty-six firms—August 14, 2024—approximately US$390 million combined**
  The SEC charged 26 broker-dealers and investment advisers, including BNY Mellon Advisors, BNY Mellon Securities, Fifth Third Securities, Mizuho Securities USA, Moelis & Company, MUFG Securities Americas, RBC Capital Markets, SG Americas Securities, SMBC Nikko Securities America, Stephens Inc., Wedbush Securities, and Wells Fargo Advisors, among others, for widespread recordkeeping failures. Personnel used WhatsApp, Signal, and text messages on personal devices for business communications that were not preserved or monitored in accordance with the Exchange Act recordkeeping rules.
- **Six credit-rating agencies—September 3, 2024—approximately US$49 million combined**
  The SEC fined A.M. Best, Demotech Inc., Fitch Ratings, HR Ratings de México, Moody's Investors Service, and S&P Global Ratings for failing to maintain and preserve business communications conducted through text and messaging applications. The failures were discovered during compliance inspections, showing weak controls over non-email communication.
- **Eleven firms—August 8, 2023—approximately US$289 million combined**
  The SEC fined Canaccord Genuity, CIBC World Markets, Invesco, KeyBanc Capital Markets, Loop Capital Markets, Moelis & Company, Oppenheimer & Co., Perella Weinberg Partners, Robert W. Baird & Co., Stifel Financial, and William Blair & Co. for failures to preserve off-channel communications. Employees, including senior managers, used personal messaging platforms such as WhatsApp, iMessage, and Signal to conduct business that was neither retained nor supervised.

For foreign banks that trade with or operate in the United States, SEC recordkeeping rules apply to any business activity that touches U.S. markets, clients, or personnel. Using unapproved apps like WhatsApp or Signal for business communications, even outside of the U.S., may still constitute a breach of U.S. record-keeping laws where those communications relate to U.S. trade/banking activity. Consequences typically extend beyond financial penalties and include mandatory remediation programs, ongoing regulatory monitoring, and heightened global supervisory scrutiny. In practice, once an institution operates in U.S. markets, it must meet stringent standards for communication monitoring and recordkeeping, regardless of where conversations take place.

MAS (Singapore) reflects similar expectations through its Technology Risk Management (TRM) and Operational Resilience guidelines. While not prescriptive in mandating specific communication surveillance mechanisms, MAS expects regulated financial institutions to monitor and control all digital interactions that may influence conduct, risk, or data security. Firms are expected to demonstrate governance oversight across both internal and third-party communication systems, ensuring accountability, traceability, and defensible control over digital communications.

Collectively, these regulatory positions reflect a converging expectation: organizations must be able to demonstrate visibility, accountability, and continuous assurance across all business communications. The obligation extends beyond capture and storage to proving that monitoring is effective, governance is active, and surveillance controls are proportionate to risk.

Risk-Based Approaches and Regulatory Alignment

Regulators in Australia, Singapore, and, increasingly, the United States encourage regulated entities to adopt a risk-based approach to meeting their compliance obligations. This model recognises that not all systems, data types, or communication channels present the same level of regulatory, operational, or reputational exposure. Rather than applying uniform controls across the enterprise, organizations are expected to prioritize risks based on likelihood and potential impact, and to apply proportionate monitoring, governance, and assurance measures.

Risk-based approaches are reinforced through alignment with broader cybersecurity, technology, and operational risk frameworks, including APRA CPS 234 in Australia, MAS Technology Risk Management (TRM) guidelines (Singapore), and U.S. NIST frameworks covering cybersecurity, privacy, and emerging AI governance. These frameworks consistently emphasise active risk assessment, continuous monitoring, and the integration of security and governance into daily operations.

Importantly, a risk-based approach does not diminish accountability. Instead, it increases expectations for demonstrable oversight, documented decision-making, and clear evidence that governance controls are informed by risk evaluation rather than a one-size-fits-all compliance activity. Boards and senior executives remain accountable for ensuring that risk decisions are appropriate, proportionate, and defensible.

Core Challenges and Risks

eDiscovery and surveillance environments face a series of interlinked challenges arising from the rapid expansion of digital communication channels, overlapping regulatory obligations, and a continued reliance on tactical or "just good enough" technology solutions.

Government findings reinforce the scale of these challenges. The Office of the Australian Information Commissioner (OAIC) reported in 2025 that 73% of agencies now use messaging apps such as Signal and WhatsApp, yet most fail to meet archival and record-keeping obligations. This gap highlights how communication diversity, when not supported by governance, directly translates into compliance risk.

The central issue is no longer the availability of compliance tools, but their effectiveness across the full communications and data landscape.

Fragmented Data and Shadow Communications

Financial institutions, government agencies, and critical infrastructure providers operate across increasingly complex digital ecosystems spanning cloud services, collaboration platforms, and legacy repositories. Business communications now span platforms such as Bloomberg, Microsoft 365, Slack, Teams, Zoom, WhatsApp, and on-premises repositories, alongside numerous bespoke and third-party systems. As a result, information is often dispersed across silos that remain partially or entirely invisible to compliance and risk teams.

The growing use of personal devices and unauthorised messaging applications further compounds the problem. So-called "shadow communications" bypass formal corporate controls altogether, leaving organizations exposed to regulatory, legal, and evidentiary risk. Where critical business communications cannot be located, retained, or reconstructed, institutions risk breaching obligations under frameworks such as the Corporations Act, ASIC Market Integrity Rules, MiFID II, and GDPR.

Conflicting Obligations

Regulated entities operate within a web of regulatory frameworks that can impose competing requirements. Privacy frameworks such as GDPR, the Australian Privacy Principles, and Singapore's PDPA stipulate strict data minimisation and purpose limitations while financial and market regulators require long-term retention and active surveillance of business communications.

Balancing these obligations requires governance, not just tooling. Failure to manage competing requirements coherently can lead to inconsistent enforcement, reputational damage, and operational disruption during investigations, audits, or discovery exercises. At a minimum, effective coordination is required between data custodians, legal teams, privacy officers, and compliance functions.

The increasing use of AI introduces a further layer of complexity. Regulators are signaling that automation must be governed with the same rigour as data retention and surveillance. Proposed reforms, such as Australia's Privacy Act changes relating to decision-making (expected from December 2026), reflect growing expectations that organizations demonstrate human oversight, auditability, and continuous testing of AI models. These controls are intended to prevent false assurance and ensure that automation strengthens, rather than weakens, governance or introduces unintended bias.

Operational Inefficiency

Many organizations rely on native compliance tools embedded within existing productivity or collaboration platforms, often assuming these provide a cost-effective compliance solution. In practice, such tools frequently deliver partial coverage with search limitations, incomplete indexing, unverified chain-of-custody, and an inability to ingest or reconcile historical data all reduce the defensibility of outputs.

The result is **"convenience compliance"**, a perceived sense of assurance that data is being managed appropriately, while eDiscovery and surveillance functions remain fragmented or incomplete. Regulators are increasingly scrutinising such approaches and questioning whether tactical solutions provide sufficient assurance during inspections and enforcement actions.

Organisational Misalignment

eDiscovery and surveillance programs are often shaped by technology or procurement priorities rather than by first- and second-line risk owners. Where cost or license considerations take precedence, regulatory intent, evidentiary defensibility, and operational resilience may be undermined.

True compliance maturity requires governance to be led, or run in close partnership with risk, legal, and compliance functions that understand the intent of regulatory obligations. When ownership is misaligned, controls tend to become reactive rather than preventative, increasing the likelihood of fragmented oversight and inconsistent outcomes.

Modern Governance

Effective compliance increasingly depends on unifying eDiscovery, surveillance (markets and trading, fraud, and business context), and record-keeping within a single governance framework. Fragmented approaches—where capture, supervision, retention, and discovery operate independently—make it difficult to demonstrate consistency, accountability, and assurance. Modern governance, therefore, requires alignment across technology, process, and ownership. In practice, this requires a unified governance architecture.

The Arctera Unified Platform is designed to support this integrated governance model. At its foundation is enterprise-grade capture, establishing a trusted and defensible record at the point of origin. Built on this capture layer, the platform unifies eDiscovery, Surveillance, and governance controls within a single architecture, providing a consistent environment for data classification, retention, and lineage across multiple communication channels. It supports ingestion across more than 130 content types, from Microsoft 365 and Google Workspace to Bloomberg, Slack, Symphony, Zoom, WhatsApp, and AI-generated comms. By applying governance controls at ingestion, organizations can enforce consistent policies across diverse data sources and reduce gaps in oversight.

By contrast, other vendor solutions, such as Microsoft Purview, offer convenience for managing native Microsoft 365 content but remain limited by tenant boundaries and lack the native capability to capture non-Microsoft or historical data sources. This results in governance blind spots and weakens legal defensibility for organizations operating in regulated environments. This limitation is not unique to Microsoft. Other platforms such as Google Workspace, Slack, Salesforce CRM, Zoom, and even compliance-specific tools like Shield exhibit similar constraints. While effective within their own environments, they offer limited visibility and control across external or historical data sources, creating potential governance and discovery blind spots.

Artificial intelligence is increasingly used to accelerate review and strengthen assurance. Arctera's indexing and analytics engines deliver near-instant search results and contextual relevance rankings that significantly outperform traditional in-place discovery processes. AI-driven analytics uncover patterns of misconduct, anomalies in sentiment, and behavioral trends across conversations, empowering compliance teams to act before risk materialises.

A sustainable compliance framework integrates technology, process, and accountability. Legal and compliance teams define policy and evidentiary requirements; IT ensures secure, auditable infrastructure; and governance functions oversee classification, retention, and lifecycle management. Together, these disciplines enable organizations to demonstrate defensibility, readiness, and confidence in responding to regulatory, legal, or internal inquiries.

The Just Good Enough Theory

The "Just Good Enough" theory describes a recurring cultural and operational pattern observed across many regulated organizations: the belief that meeting minimum compliance requirements is sufficient. Under pressure to reduce costs, simplify tooling, or consolidate licenses, organizations may adopt embedded or native compliance tools as a tactical response rather than as part of a broader governance strategy. While such approaches can provide basic coverage for certain data types or platforms, they often lack the depth, interoperability, and assurance required for defensible governance in complex, multi-channel environments. As communication ecosystems expand, these limitations become more pronounced.

In practice, this pattern often emerges where compliance tooling decisions are made primarily through a technology or procurement lens, without sufficient involvement from first- and second-line risk owners who understand the risk factors that attract regulatory scrutiny.

Microsoft Purview and eDiscovery Premium exemplify this mindset, reflecting a perception that embedded or native tools are sufficient for regulated environments. Microsoft's model supports standard productivity workloads but struggles with complex, multi-system environments. Its discovery capabilities extend primarily to Exchange, SharePoint, and Teams, while coverage of non-Microsoft data depends on third-party connectors that often provide only limited functionality. Search operations are slower and less transparent, and preservation relies on in-place holds that are not immutable—a critical weakness under evidentiary scrutiny.

It is important to note, however, that the Just Good Enough theory does not reflect shortcomings of any single platform or vendor. Rather, it highlights organizational behaviors that prioritize convenience or short-term efficiency over long-term governance outcomes. When compliance architecture is shaped primarily by licensing considerations or tooling availability, rather than regulatory intent and risk exposure, controls are more likely to remain reactive and fragmented.

Compliance cannot rely on perceived adequacy; it must be demonstrably effective. Regulators and courts increasingly expect organizations to prove that information is complete, accurate, and managed according to risk. Where Just Good Enough approaches persist, legal defensibility and regulatory confidence are weakened.

True compliance maturity, therefore, requires independent validation, continuous testing, and clear assurance mechanisms (e.g., evidence trails) that confirm controls are operating as intended. Without these elements, even well-intentioned compliance programs may fail under regulatory scrutiny.

Lessons from Practice: Why Assurance Matters

Experience across regulated industries consistently demonstrates that technology alone does not guarantee compliance. Without effective assurance, meaning the systematic verification that controls are functioning as intended, organizations may be unable to demonstrate that controls are operating as intended, leaving them exposed to discovery failures, data gaps, and regulatory penalties.

A frequently cited example is the 2022 Cabo Concepts Ltd v MGA Entertainment (UK) Ltd & Anor case, in which the High Court of Justice of England and Wales highlighted the consequences of incomplete and inadequately validated eDiscovery processes. The court emphasised the importance of evidencing data integrity and demonstrating that reasonable and proportionate steps had been taken to identify, preserve, and disclose relevant communications. The case illustrated that, without auditable quality controls and validation processes, organizations may struggle to demonstrate that all relevant communications have been preserved and produced.

Assurance transforms compliance from a largely reactive function into an active form of risk management. It provides confidence that surveillance and eDiscovery systems are independently validated, that captured data is accurate and complete, and that governance processes are transparent and repeatable. In this way, assurance acts as the bridge between governance design and regulatory trust.

Modern compliance platforms that embed assurance into their operating models through features such as capture verification, audit logging, automated classification, and reconciliation reporting enable organizations to demonstrate not only compliance but confidence. Assurance is what converts good governance into defensible governance.

In the MGA case, deficiencies in the tools and processes used to manage large-scale disclosure led to the application of incorrect search parameters, the production of inaccurate results, and inadequate quality assurance. In a properly managed disclosure exercise, reliable systems, established methodologies, and rigorous validation processes are expected to ensure accuracy, completeness, and compliance. In this instance, the deficiencies were sufficiently serious to undermine confidence in the disclosure process and ultimately contributed to the collapse of the trial.

Arctera's model is designed to address these types of deficiencies by embedding assurance across the capture, governance, and discovery lifecycle. Journal-based capture supports the integrity and immutability of preserved communications, while AI-powered analytics operate across both structured and unstructured data to enable consistent review at scale, and its forensic search executes in seconds regardless of archive size. Search and classification capabilities are supported by more than 1,400 configurable classification patterns and policies, enabling organizations to align compliance controls with industry- and jurisdiction-specific requirements.

Market Recognition

Arctera's approach to digital communications governance, eDiscovery, and Surveillance has been recognised by independent industry analysts and research firms. These assessments reflect the platform's breadth of capability and its applicability to regulated environments operating across hybrid and multi-vendor ecosystems.

In October 2025, Arctera was recognised for the second consecutive year as a Leader in the Gartner Magic Quadrant for Digital Communications Governance and Archiving (DCGA) Solutions. During the same period, Arctera was named a Leader in the IDC MarketScape for Worldwide End-to-End eDiscovery Software Vendor Assessment, 2025, and a Top Player in the Radicati Group Information Archiving Market Quadrant for the seventh time.

Collectively, these recognitions highlight Arctera's ability to support regulated organizations in managing communications governance, eDiscovery, and surveillance across complex operating environments.

Underpinned by a common governance model, The Arctera Unified Platform brings together capture, classification, archiving, supervision, and discovery across a broad range of communication sources, including Dubber, NICE, Teams, Verint, Zoom, and integrates with Microsoft Azure Voice Whisper for transcription and translation.

A globally scalable SaaS architecture supports data residency, sovereignty, and regulatory alignment across jurisdictions, while maintaining consistent governance, security, and evidentiary integrity.

AI-driven analytics, classification, and automation are applied to support scalable review, supervisory oversight, and defensible decision-making in complex regulatory environments.

Taken together, these recognitions reflect not only Arctera's technology maturity but also its alignment with the broader compliance principles outlined in this paper, including visibility, accountability, and defensibility across every communication channel. The convergence of eDiscovery, surveillance, and governance within a unified framework illustrates how modern compliance has evolved beyond isolated tools toward integrated, risk-based oversight. This shift from tactical enablement to structured assurance reinforces the need for modern governance and contrasts with the limitations of the Just Good Enough approaches, where fragmented or convenience-driven solutions fail to deliver complete regulatory confidence.

A Platform-Centric Approach – Capture and Discover Everything

The evolution of regulatory compliance increasingly depends on effective content aggregation, bringing enterprise communications together into a unified, searchable, and policy-governed repository. This approach enables organizations to apply consistent governance controls across diverse communication types and sources, reducing the risk that material communications fall outside oversight.

Regulatory obligations described earlier make this approach essential. Business communications now span a wide range of sources, including collaboration platforms, messaging platforms, such as Bloomberg, Cloud9, Microsoft Teams, Viva Engage, Zoom, WhatsApp, and Signal, as well as structured data exports (for example, CSV and JSON), voice recordings, video streams, and generative AI, should be captured and retained with added context. Where capture and retention are fragmented across multiple tools or repositories, organizations face increased uncertainty in locating, reconstructing, and evidencing communications during audits, investigations, or discovery exercises. Unified aggregation, by contrast, supports confidence in completeness and defensibility.

The central aspect of a platform-centric model is the rationalisation of surveillance and eDiscovery tools. Many organizations continue to operate multiple, disconnected systems for communication capture, supervision, and discovery, resulting in duplicated effort, inconsistent coverage, and increased operational complexity. Consolidating these capabilities within a single, or tightly integrated, governance framework improves transparency, consistency, and assurance across the communications estate.

Comprehensive Visibility and Reduced Blind Spots

Unifying all communication types, including email, chat, voice, video, and collaboration platforms, within a governed environment provides a more complete and auditable view of organizational activity. By centralizing capture and oversight, organizations can reduce monitoring gaps and limit the risk that business-critical communications fall outside governance controls, strengthening evidentiary integrity and compliance readiness.

Regulatory Coherence

Supervisory bodies such as the FCA and regulators enforcing MiFID II increasingly expect firms to maintain continuous oversight and consistently retain business communications. A consolidated platform supports these expectations by standardising capture, classification, and retention controls across channels, making it easier to demonstrate compliance and respond to audits, supervisory reviews, and regulatory inquiries with confidence.

Operational Resilience

Disconnected tools frequently introduce integration challenges, inconsistent monitoring outcomes, and operational friction during investigations. Consolidation reduces these weaknesses by improving the reliability of search, alerting, and review workflows, and by enhancing the speed and consistency of compliance investigations, particularly under time-critical conditions.

Scalability and Cost Efficiency

Reducing the number of systems lowers administrative overhead, simplifies maintenance and training, and improves the organization's ability to scale as communication volumes and sources grow. A unified architecture is better positioned to accommodate new communication channels and evolving regulatory requirements without adding complexity or creating additional blind spots.

Platform Application

Arctera's platform-centric architecture is designed to operationalise this approach. Its ingestion framework aggregates communications from a broad range of sources, normalises data into a unified structure, and applies governance policies at the point of ingestion. AI-driven classification supports the automatic identification of sensitivity, context, and retention value, enabling consistent governance across diverse data types.

This approach supports unified visibility, consistent retention, and defensible responses to regulatory requests, including Freedom of Information (FOI) obligations. The same governance model can be applied across enterprise content repositories, such as SharePoint Online and OneDrive, too, extending oversight beyond messaging and collaboration platforms.

Broadening Sources and Applying AI

Surveillance is no longer limited to written communications. Electronic communications (eComms), together with voice and video communications (vComms), are now integral to modern compliance monitoring. Trading floors, call centres, and government (shared) service hubs generate substantial volumes of audio and visual data, much of which may contain regulated, sensitive, or business-critical information.

Arctera's surveillance capabilities extend these modalities, combining AI-driven transcription, translation, and behavioral analytics to uncover risk in real time. Speech-to-text technologies transcribe calls and video meetings across multiple languages, while language models analyze the resulting text for lexicons, keywords, and sentiment associated with insider trading, market manipulation, bribery, or misconduct.

Advanced analytical models also detect evasion techniques, such as code-switching, abrupt shifts between communication channels or media, and attempts to move sensitive discussions off-platform. Machine Learning flags anomalous tone, sentiment, or behavioral patterns that may indicate undue influence or collusion. For government and public sector use cases, similar techniques detect breaches of conduct, policy violations, unauthorized information sharing, or irregularities in procurement processes.

Beyond alerting on individual events, Arctera's AI capabilities are designed to filter noise, prioritize relevance, and provide contextual insight at scale. By combining transcription, translation, and content analytics, reviewers are better equipped to assess not only what was communicated, but the surrounding context in which it occurred. This multi-layered analysis supports a shift from reactive review toward more proactive risk detection, while reducing manual effort and strengthening evidentiary accuracy across large volumes of recordings.

Arctera's artificial intelligence capabilities incorporate a Continuous Active Learning (CAL) model, enabling algorithms to refine performance over time based on reviewer feedback rather than relying solely on periodic retraining cycles. For regulated entities, this approach helps maintain alignment with evolving communication patterns, policy changes, and emerging risk signals. Unlike static models, which can drift over time or require frequent manual recalibration, a Continuous Active Learning (CAL) approach supports ongoing adaptation based on reviewer input. This helps reduce bias, improve accuracy, and maintain defensibility as communication patterns, behaviors, and risk signals evolve. Importantly, it also supports regulatory expectations for human oversight, transparency, and explainability in automated decision-making.

Business Owners and Technology Teams Working Together

Regulatory resilience requires more than technical enablement; it depends on organizational alignment across compliance, governance, and business accountability. eDiscovery and surveillance, as core components of electronic records management, should be treated as enterprise-wide disciplines rather than as isolated IT utilities.

Where organizations view these capabilities primarily through a technological or licensing lens, they may expose themselves to longer-term risk, operational inefficiency, and heightened regulatory scrutiny. A recurring pattern in regulated sectors is the tactical adoption of compliance platforms based on perceived cost efficiency. Such initiatives are often sponsored by procurement or technology management functions seeking to rationalize tooling with enterprise licensing arrangements. While these decisions may appear efficient from a cost perspective, they can overlook the distinct operational and evidentiary requirements of first and second-line risk owners, as well as the legal and compliance teams responsible for regulatory outcomes.

When these stakeholders are not sufficiently involved, the result is often visibility without assurance. Organisations may be able to demonstrate the presence of systems and processes, yet lack confidence in the completeness, accuracy, execution, or control of those systems under regulatory or legal scrutiny.

Regulatory expectations reinforce the need for enterprise-wide alignment. Obligations across privacy, prudential, and market-conduct regimes increasingly require organizations not only to comply with formal requirements, but to demonstrate ownership, oversight, and control across their information and communication environments.

Statutory Accountability – GDPR (Article 5(2))

"The controller shall be responsible for, and be able to demonstrate compliance with paragraph 1 ('accountability')."

This obligation applies to the core GDPR principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality.

Prudential Accountability — APRA

APRA's prudential framework places accountability for risk management with boards and senior management, requiring them to manage risk, and to demonstrate ownership, control, and assurance over how risk is identified, governed, and mitigated.

Standards, including CPS 220, CPS 230, CPS 234, and CPG 235, reinforce these expectations by requiring institutions to assign clear responsibility for critical risks such as data management, operational resilience, and information security, and ensure that governance decisions are based on accurate, verified, and trusted information.

Together, these statutory and prudential expectations reinforce that accountability cannot be satisfied by policy statements or tooling alone. Organisations must be able to evidence how governance ownership is assigned, how controls are applied in practice, and how assurance is obtained across the full lifecycle of communications and data.

From a governance perspective, decision-making around compliance architecture must therefore be appropriately balanced. Technology functions play a critical role in enabling support rather than dictating the compliance model. Platform choices and operational workflows should be evaluated through the lenses of risk ownership, evidentiary defensibility, and data privacy, rather than licensing convenience alone. Achieving this balance requires engagement across first-line business units, second-line risk and compliance functions, and third-line assurance teams to establish a cohesive governance framework.

The adoption of a "discover everything" strategy reflects both a risk-management and efficiency imperative. Aggregating relevant content sources into a unified, policy-governed environment supports timely regulatory response and enables proactive identification of anomalies, privacy risk, and potential misconduct. It also allows legal and compliance teams to respond to DSARs more efficiently, supports consistent retention and disposal practices, and reduces unnecessary data duplication and storage cost.

Finally, the organizational culture remains a critical factor in compliance maturity. Effective governance depends on clear accountability and a shared understanding of roles across the eDiscovery and surveillance lifecycle. Technology should reinforce governance rather than replace it. By integrating eDiscovery, surveillance, and content aggregation within a single, risk-aligned governance model, organizations can strengthen their regulatory posture while also enhancing transparency, operational efficiency, and trust.

Move Beyond "Just Good Enough".

Visit arctera.com to see how our unified platform provides the demonstrable visibility and defensibility modern regulators now demand.

Further Reading

1. https://www.kirkland.com/publications/kirkland-aim/2025/01/off-channel-communications
2. https://www.reuters.com/business/finance/whatsapp-use-by-credit-suisse-staff-scrutinised-by-uk-regulator-documents-show-2024-12-06/
3. https://www.regulationtomorrow.com/eu/fca-multi-firm-review-into-off-channel-communications/
4. https://www.fca.org.uk/publications/multi-firm-reviews/multi-firm-review-off-channel-communications
5. https://www.acaglobal.com/industry-insights/mifid-ii-asset-managers-communications-record-keeping/
6. https://www.acaglobal.com/industry-insights/fca-review-of-off-channel-communications-highlights-global-compliance-risks
7. https://www.esma.europa.eu/publications-data/questions-answers/1770
8. https://www.fca.org.uk/publications/newsletters/market-watch-66
9. https://www.asic.gov.au/regulatory-resources/markets/market-supervision/supervising-your-representatives-business-communications
10. https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2024-releases/24-134mr-asic-calls-on-market-intermediaries-to-strengthen-supervision-of-business-communications/
11. https://caselaw.nationalarchives.gov.uk/ewhc/pat/2022/2024
12. https://www.arctera.com/surveillance
13. https://www.arctera.com/ediscovery
14. https://www.arctera.com/capture
15. https://www.apra.gov.au/information-security-cps-234
16. https://www.apra.gov.au/managing-data-risk-cps-235
17. https://www.asic.gov.au/regulatory-resources/markets/market-supervision/supervising-your-representatives-business-communications/
18. https://www.businesswire.com/news/home/20251017922541/en/Arctera-Named-a-Leader-in-the-Gartner-Magic-Quadrant-for-Digital-Communications-Governance-and-Archiving-Solutions
19. https://www.arctera.io/press-releases/arctera-named-a-leader-in-idc-marketscape-for-worldwide-end-to-end-ediscovery-software-2025
20. https://www.arctera.io/press-releases/radicati-group-names-arctera-a-top-player-in-its-latest-information-archiving-market-quadrant-for-the-seventh-time
21. https://www.oaic.gov.au/about-the-OAIC/information-policy/information-policy-resources/messaging-apps-a-report-on-australian-government-agency-practices-and-policies

About Arctera

Arctera, a Cloud Software Group company, is the leading global provider of compliance and governance solutions that enable firms to unleash game-changing technologies into their organizations while minimizing risk. Created in 2024 from Veritas Technologies, Arctera helps the biggest companies in the world monitor and control exactly how their information is being accessed, used and shared. The Arctera Unified Platform is able to capture data from over 130+ different content sources, and more than 280 AI policies help firms streamline compliance and adapt to evolving regulations.

arctera™

Learn more at arctera.com

Connect with us on LinkedIn

Contact: press@arctera.com

A0001 03/26