



Guide



2026 Banking Communication Compliance Handbook

Executive Summary

The financial and banking sector has recently been shaken by a surge of regulatory actions, with eleven institutions fined nearly \$2 billion for using messaging apps such as iMessage and WhatsApp for business communications. These incidents are not isolated; they underscore a fundamental truth: communication compliance is not optional or peripheral anymore.

This handbook has been compiled as a definitive resource for banking and financial professionals, providing actionable guidance and insights drawn from decades of regulatory evolution. Readers will learn:

- How banking communication compliance has transformed and what this means for operational risk.
- The regulatory landscape across the USA, the EU, and global standards, with clarity on obligations and expectations.
- Best practices for governance, auditability, and control of customer communications, ensuring that every message is defensible and traceable.
- Practical guidance on monitoring, retention, and avoiding the common pitfalls that attract regulatory scrutiny.

By mastering the principles in this handbook, institutions can secure operational integrity, build regulatory confidence, and turn compliance into a strategic advantage.



Table of Contents

1. What Has Changed in Banking Communication Compliance	4
2. Regulatory Landscape: USA, EU, and Global Standards	4
3. Governance and Audit Control of Customer Communications	7
4. Retention, Supervision, and Ongoing Monitoring of Customer Communications	9
5. Common Communication Compliance Failures and Regulatory Readiness Guide	11
6. Conclusion	12

What Has Changed in Banking Communication Compliance



For decades, regulatory communication in banking was largely procedural and inconsistent, with auditors and authorities exchanging information without uniform expectations. Oversight focused on financial reporting and basic governance, leaving operational resilience and digital communication unaddressed. The landscape has shifted decisively. In the EU, DORA and GDPR formalize requirements for ICT governance, data protection, and auditable reporting. Accessibility standards, once largely optional, now find legal grounding through the Americans with Disabilities

Act (ADA) in the United States and the European Accessibility Act (EAA), obliging institutions to ensure inclusive access to services and information.

These frameworks represent a departure from ad hoc compliance toward integrated, enforceable standards, mandating transparency, accountability, and operational rigor. Banks must now navigate a regime where communication, data, and accessibility are inseparable from governance and risk management, reflecting a sophisticated, enforceable evolution of regulatory expectations.

Regulatory Landscape: USA, EU, and Global Standards

United States

In the United States, communication compliance is tightly linked to governance, auditability, and operational accountability. US regulators employ a prescriptive, rules-based approach, requiring financial institutions to maintain auditable, retrievable communications.

- **Dodd-Frank Wall Street Reform and Consumer Protection Act:** Mandates comprehensive recordkeeping and reporting of communications relevant to trading, risk, and consumer protection. Ensures transparency and traceability in all electronic correspondence.

- **Securities and Exchange Commission (SEC) Rules:** Require retention, indexing, and retrieval of emails, instant messages, and other communications tied to securities transactions.
- **Financial Industry Regulatory Authority (FINRA) Rules:** Enforce robust surveillance, retention, and supervisory review of employee communications to support compliance and regulatory investigations.
- **Commodity Futures Trading Commission (CFTC) Rules:** Impose similar obligations on derivatives and commodities market participants for communication monitoring and retention.
- **Sarbanes-Oxley (SOX) Act:** Introduces corporate governance and audit requirements, emphasizing internal controls over financial reporting, including electronic communications.
- **California Consumer Privacy Act (CCPA):** Protects the privacy rights of California residents, requiring that communications containing personal data be collected, stored, and transmitted in compliance with privacy standards.
- **Americans with Disabilities Act (ADA):** Ensures accessibility of communication platforms, including electronic messaging, for persons with disabilities.
- **Federal Financial Institutions Examination Council (FFIEC):** Prescribes uniform supervisory principles, standards, and reporting forms, supporting consistency in communication compliance across US financial institutions.

US regulations are explicit and prescriptive, leaving minimal ambiguity. The focus is on auditability, supervisory readiness, and strict operational implementation, with state-level privacy laws layering additional obligations.



European Union

In the European Union, communication compliance is treated as a supervisory enabler, not merely an evidentiary obligation. The EU follows a principles-based model, where the quality, clarity, and reliability of communication directly support financial stability and effective supervision.

- **European Banking Authority (EBA) Guidelines:** Establish a structured framework for timely, accurate, and meaningful communication, enabling supervisors to assess the safety and soundness of credit institutions.

- **Markets in Financial Instruments Directive and Regulation (MiFID II / MiFIR):** Require recording and retention of communications related to investment services, trade execution, and client instructions, ensuring transparency and market integrity.
- **General Data Protection Regulation (GDPR):** Governs the lawful processing, storage, and transmission of personal data embedded within customer and regulatory communications, with strict accountability and enforcement.
- **Digital Operational Resilience Act (DORA):** Elevates communication systems to critical ICT assets, requiring resilience, traceability, and incident reporting to protect operational continuity.
- **European Accessibility Act (EAA):** Introduces binding accessibility standards for digital communications, correcting historic gaps where accessibility was optional rather than enforceable.

Unlike the US, the EU evaluates communication compliance through the lens of governance quality and supervisory outcomes, allowing regulators discretion while expecting demonstrable effectiveness.

Global Standards

For banks operating across borders, national compliance alone is insufficient. Global standards provide a baseline discipline for communication governance where jurisdictions intersect.

- **Basel Committee on Banking Supervision (BCBS) Principles:** Embed communication, recordkeeping, and information integrity within governance, risk management, and operational resilience expectations.
- **Financial Action Task Force (FATF) Recommendations:** Require robust communication records to support anti-money laundering and counter-terrorist financing controls across jurisdictions.
- **IOSCO Principles:** Set expectations for retention, monitoring, and supervisory access to communications related to market conduct and investor protection.

For cross-border institutions, these standards ensure that communication practices remain coherent, defensible, and regulator-ready, even when local rules diverge.

Governance and Audit Control of Customer Communications



Knowing the applicable rules and regulations is only the starting point. In supervisory reviews, regulators focus on whether communication controls operate in practice, not on whether policies exist on paper. Governance and audit readiness are therefore examined together, as they are inseparable in enforcement actions.



Governance expectations for customer communications



Approved content only

All customer communications must be formally reviewed and approved before use. Content that is discovered after distribution, even if later approved, is treated as a control failure rather than an administrative oversight.



Controlled creation and modification

Communication content must follow a defined lifecycle from drafting through approval, release, amendment, and withdrawal. Informal edits, local copies, or parallel versions undermine control and are frequently cited in supervisory findings.



Clear ownership and accountability

Each communication must have a designated business owner responsible for the message and a designated compliance owner responsible for regulatory accuracy. Shared or unclear ownership is viewed as weak governance.



Separation of duties

The roles of drafting, approving, and distributing communications must be performed by different individuals or functions. This is a baseline supervisory expectation, aligned with long-standing financial control principles.



Auditability and evidence readiness

What regulators expect to see

Regulators expect immediate access to evidence showing how a communication was approved, which version was active at a given time, and where it was distributed.

Required proof

- Approval records
- Complete version history
- Distribution and delivery logs

Why intent is irrelevant

Statements such as “we intended to comply” or “this was an exception” have no evidentiary value. In regulatory reviews, compliance exists only where it can be demonstrated through records.



Retention, Supervision, and Ongoing Monitoring of Customer Communications

Once communications are governed and approved, banks are expected to retain, supervise, and monitor them in a manner that allows regulators to reconstruct events without ambiguity. Retention and supervision are not treated as technical obligations; they are viewed as evidence of operational discipline and control maturity.



Retention of customer communications

➤ Complete and tamper-resistant records

All customer communications must be retained in full, including content, attachments, and metadata. Records must be protected against alteration or deletion, whether intentional or accidental.

➤ Retention aligned to regulatory timelines

Retention periods must meet or exceed applicable regulatory requirements across jurisdictions. Shorter internal retention policies are not accepted where regulations require longer preservation.

➤ Centralized retention

Communications must be stored in systems that allow controlled access, consistent application of retention rules, and reliable retrieval. Decentralized storage across inboxes, shared drives, or local systems is treated as a control weakness.



Supervision and monitoring expectations

➤ Ongoing supervisory review

Banks are expected to actively supervise customer communications, not merely archive them. Supervisory reviews should assess regulatory accuracy, consistency, and appropriateness on a continuous basis.

➤ Risk-based monitoring

Monitoring intensity should reflect communication risk, including product complexity, customer vulnerability, and regulatory sensitivity. Uniform sampling without risk differentiation is often challenged by regulators.

➤ Issue identification and escalation

Where deficiencies are identified, banks must demonstrate timely escalation, corrective action, and documented remediation. Unaddressed or repeatedly identified issues are treated as governance failures.



Regulatory perspective

➤ Reconstruction over explanation

Regulators expect institutions to reconstruct what was communicated, when, by whom, and to whom, without relying on narratives or assumptions.

➤ Systems over assurances

Verbal assurances and policy statements carry little weight if systems cannot produce records promptly and accurately.

Regulatory perspective



Common Communication Compliance Failures and Regulatory Readiness Guide

Regulators do not approach communication reviews with curiosity. They approach them with a presumption that weaknesses exist and with a clear view of where those weaknesses usually surface. Institutions that understand this prepare differently from those that rely on policies and assurances.



Communication failures that consistently trigger findings

- 
Process bypass disguised as urgency
 Communications sent outside approved workflows are one of the most common findings in examinations. Time pressure is never accepted as justification. If a process can be bypassed, regulators assume it is not a real control.
- 
Inability to establish a single source of truth
 When institutions cannot demonstrate which version of a communication was authoritative at a specific point in time, credibility is lost quickly. This failure becomes decisive in complaint investigations and conduct reviews.
- 
Evidence gaps, not content errors
 Enforcement actions are rarely driven by poor wording alone. They are driven by missing approval records, incomplete audit trails, and inconsistent retention across channels.
- 
Diffuse accountability
 Communications owned by committees, teams, or functions rather than named individuals lead to delayed responses and weak remediation. Regulators treat this as a governance defect, not an organizational choice.
- 
Supervision after the fact
 Monitoring that begins only after customer harm or regulatory inquiry signals a reactive culture. This is interpreted as ineffective control, regardless of monitoring quality.



Regulatory readiness standard for customer communications

An institution is considered ready only when the following conditions are met:

- Any customer communication can be reconstructed in full without explanation or interpretation.
- Approval, version control, and distribution evidence are immediately available and internally consistent.
- Retention is enforced uniformly across channels, geographies, and business lines.
- Supervisory reviews are routine, documented, and tied to identifiable risk drivers.
- Remediation is tracked to completion and produces durable control improvement.

Institutions that meet this standard do not argue intent during examinations. They present records. Those that cannot are managed through findings, remediation plans, and, where necessary, enforcement.

Conclusion

Banking communication compliance has progressed from informal practice to a rigorously governed discipline. Every communication must be controlled, documented, and defensible, reflecting governance, operational resilience, and regulatory expectations. Institutions that embrace these standards demonstrate credibility, mitigate risk, and sustain trust with supervisors and clients alike. Neglecting these obligations undermines oversight and invites scrutiny. Mastery of communication compliance is a strategic imperative that shapes both the institution's integrity and its operational viability in an increasingly regulated environment.

Missed messages cost millions. Don't be next.

Try a live demo to see how compliance, supervision, and audit control come together seamlessly.

[Book a Demo](#)



Testimonials:



As new technologies come out, we want to make sure that we are able to take advantage of them if we choose to do so. And I think Cincom is also right in line with that—as new things emerge, they are very quick to respond and make sure it is on their radar to be integrated in, so that their customers can take advantage of it if they want to. I think we're aligned in the same way.

~ Kathy Biwer, Director of Business Applications Services, MTL Insurance



Cincom Eloquence has allowed us to create complex document templates that could not have been done before, and it's allowed us to handle our growing communication volumes with ease.

~ Yogesh Patil, Technical Lead, Molina Healthcare, Inc.

About Cincom Eloquence

Cincom Eloquence is a leading Customer Communication Management (CCM) solution that helps organizations streamline and personalize customer interactions across all channels. Trusted by global leaders, it simplifies complex document processes to reduce costs, speed time-to-market, and boost retention. With seamless integration, minimal IT support, and flexible cloud or on-premise deployment, Cincom Eloquence empowers businesses to drive revenue, ensure compliance, and deliver impactful communications at scale.

To learn more about Cincom Eloquence, visit our website:

[Customer Communication Management - CCM Software | Cincom](#)