

SELF-ASSESSMENT CHECKLIST

Ephemeral Messaging Governance: Organizational Readiness Checklist

A Self-Assessment for Legal, Compliance, and Risk Leaders

Regulatory enforcement around off-channel communications and auto-deleting messaging apps is at an all-time high.

Failing to govern ephemeral messaging can expose your organization to severe regulatory fines and reputational damage.

Use this checklist to assess your organization's risk posture across the four core pillars of information lifecycle management: **Oversight, Capture, Retention, and Monitoring.**

01 Oversight

- ☐ **Regulatory Translation:** Has your organization translated global off-channel and ephemeral communication mandates into enforceable internal policies backed by documented, repeatable supervisory procedures? Do those policies and procedures:
 - ☐ Address the use of personal devices for business-related activities,
 - ☐ Set forth approved communication platforms for business communications,
 - ☐ Prohibit the use of unapproved platforms, particularly ephemeral messaging solutions (e.g., Snapchat, text messaging, Signal), and
 - ☐ Address data retention and disposal requirements?
- ☐ **Operating Model:** Is there an active governance cadence that integrates perspectives from IT, Legal, Compliance, and Business leadership?
- ☐ **Visibility & Shadow IT:** Do you have visibility into the specific messaging apps your employees, clients, and counterparties actively prefer, enabling you to proactively mitigate unapproved communication channels?
- ☐ **Risk Assessment:** Does your organization assess its ephemeral messaging risk on an ongoing basis, including whether the use of personal devices or ephemeral messaging apps has impaired its ability to conduct internal investigations or respond to regulatory requests?
- ☐ **Training & Communications:** Does your organization provide training for its employees and communicate regularly about appropriate versus inappropriate messaging platforms and data retention and disposal mandates?
- ☐ **Policy Enforcement:** Are employees at your organization consistently held accountable for failing to follow your organization's policies regarding business communications and the management of business data?

02 Capture

- ☐ **Shared Responsibility:** Are capture and preservation requirements for all authorized communication platforms embedded directly into product and IT roadmaps from day one?
- ☐ **Data Lineage:** Can you clearly map the data lineage of your digital communications, understanding exactly how messages flow from the source application to the final archive while identifying potential points of failure along the way?
- ☐ **Reconciliation:** Do you rely on automated reconciliation checks to validate that every required ephemeral message is successfully ingested?

04 Monitoring

- ☐ **Ongoing Monitoring:** Does your organization routinely monitor employees' business communications and use of communication platforms?
- ☐ **Efficient Risk Detection:** Has your organization moved beyond traditional, rules-based lexicon surveillance to NLP/ML or AI models that actively reduce false positives and focus on genuine risk within complex ephemeral platforms?
- ☐ **Continuous Improvement:** Do your compliance teams treat surveillance policies as living products utilizing a defined process to continuously review, tune, and optimize models?
- ☐ **Regulator-Ready Explainability:** Can your organization transparently explain how its surveillance methodologies operate and detect risk within ephemeral apps, utilizing clear documentation and human-in-the-loop oversight supporting processes that are defensible and ready for regulatory scrutiny?

03 Retention

- ☐ **Lifecycle Management:** Do your retention policies systematically keep only what is strictly necessary to meet global regulatory mandates?
- ☐ **Technology Strategy:** Have you consolidated all communications requiring supervision into a single archive so they can be evaluated against the exact same risk policies?
- ☐ **eDiscovery & Usability:** Is your captured data preserved in both human- and machine-readable formats and structured for fast, accurate retrieval, so you can respond efficiently to regulatory inquiries without operational delays?

NEXT STEPS

Strengthen Your Governance Framework

Unsure where your organization stands on off-channel communication compliance?

Unchecked boxes represent immediate exposure to regulatory enforcement. Rethink Compliance, LeapXpert, and Stratis LLC help organizations benchmark their current state, close policy gaps, and implement appropriate controls.



ANDREA FALCIONE
RETHINK COMPLIANCE

Contact Rethink Compliance at hello@rethinkcompliance.com to discuss training and communications or to schedule a tailored risk evaluation.



SETH NOONE
LEAPXPRT

Contact **LeapXpert** to discuss technology solutions.



RYAN THORPE
STRATIS

Contact Ryan Thorpe at Stratis (ryan.thorpe@thinkstratis.co) to discuss strategies for modernizing your risk and compliance programs, operating models, and technology strategy.