ARCHIVE360

6 QUESTIONS TO ASK VENDORS BEFORE CHOOSING THEIR DIGITAL COMMUNICATIONS GOVERNANCE & ARCHIVING SOLUTION

INTRODUCTION

The way businesses communicate has evolved. While email remains a critical tool, organizations now rely on **Microsoft Teams, Slack, WhatsApp, Zoom, and social media** to conduct business. However, many legacy archiving solutions are still built for an email-only world, leaving organizations exposed to **compliance risks, security vulnerabilities, and operational inefficiencies**.

IT leaders must rethink their approach to **Digital Communications Governance & Archiving (DCGA)** to ensure they can effectively **capture, retain, and manage** communications across all platforms. Before selecting a vendor, ask these six key questions to ensure your solution is **future-proof, secure, and compliant**.

01

CAN THE SOLUTION CAPTURE AND GOVERN ALL COMMUNICATION CHANNELS—NOT JUST EMAIL?

Many vendors still focus primarily on email archiving, but modern business communications extend far beyond email. **Regulatory bodies now require organizations to retain and govern all forms of business communication.**

Ensure the platform supports:

- Microsoft Teams & Slack chats

- WhatsApp, iMessage, and SMS

- Social media (LinkedIn, Twitter, etc.)

- Collaboration tools like Zoom & Webex

Why it matters: Compliance, legal, and risk management teams need a single source of truth across all communication channels to avoid gaps that could lead to legal exposure.

02

HOW DOES THE PLATFORM ENSURE COMPLIANCE WITH EVOLVING REGULATIONS?

Regulatory frameworks such as **GDPR, SEC, FINRA, HIPAA, and FOIA** now apply to a broad range of communication platforms, making compliance more complex than ever.

Ask vendors:

- Does the platform support automated compliance enforcement for retention, deletion, and legal hold policies?

- Can it adapt to evolving regulations without costly upgrades?

- Does it provide audit trails and defensible data management for regulatory reporting?

Why it matters: A proactive approach to compliance minimizes risk and ensures that regulatory changes don't lead to operational disruptions.

03
DOES THE PLATFORM OFFER MODERN SECURITY AND ENCRYPTION?

Many legacy archives **lack modern security controls**, making them prime targets for cybercriminals. **Sensitive data stored in outdated platforms is a major risk.**

Key security features to look for:

- **End-to-end encryption for data at rest and in transit**

- **Role-based access controls to prevent unauthorized data access**

- **Zero-trust security models to reduce insider threats**

- **Integration with advanced threat detection & AI-driven risk monitoring**

Why it matters: Legacy archives are **frequent targets for ransomware and data breaches**. Protecting archived data is just as critical as securing live systems.

04

HOW SCALABLE IS THE PLATFORM AS DATA VOLUMES GROW?

Business communication generates **massive volumes of data daily**. If your archive can't scale efficiently, you may face increasing costs and degraded performance.

Ask vendors:

- Does the platform offer predictable pricing as data volumes grow?

- Can it ingest, store, and retrieve large volumes of data without performance slowdowns?

- Does it provide cost-efficient storage models that eliminate overages?
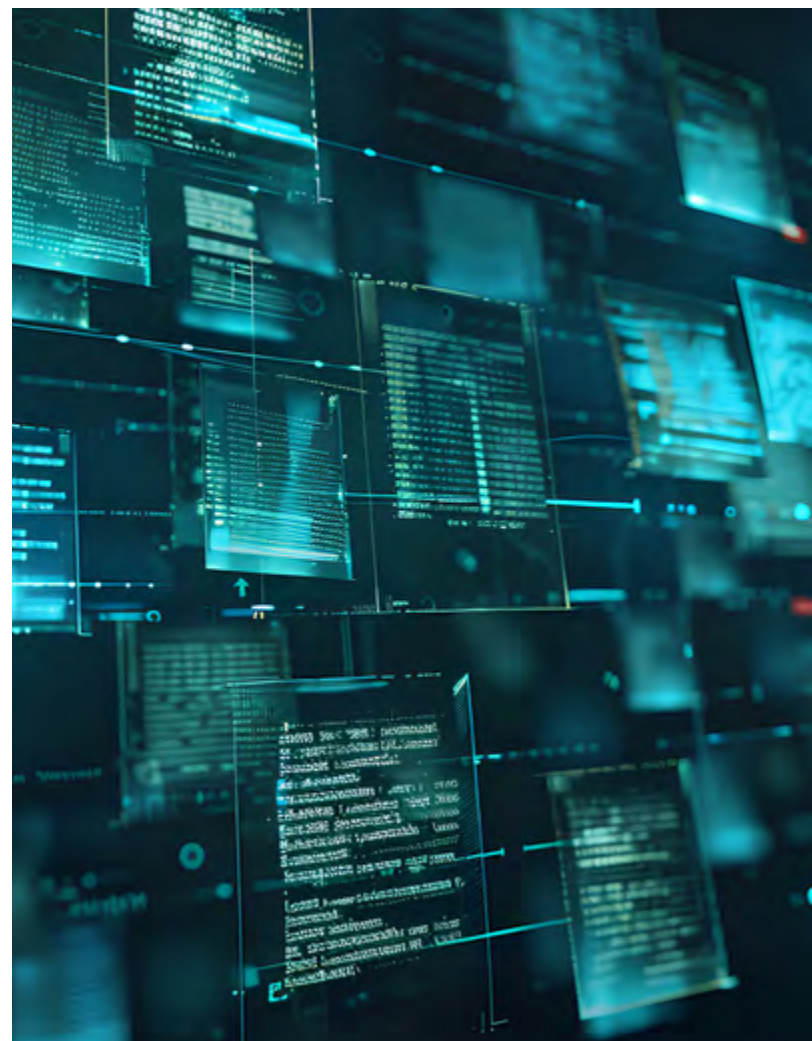
Why it matters: Scalability and cost predictability prevent your organization from being trapped in an expensive, inflexible system.

CAN THE PLATFORM SUPPORT SEAMLESS EDISCOVERY AND LEGAL HOLD PROCESSES?

Legal teams need fast, **precise search capabilities** across all archived communication channels. Legacy systems often require **manual intervention**, making eDiscovery slow and costly.

Look for:

- AI-powered search and automation tools to reduce manual workload

- Easy-to-apply legal holds across Teams, Slack, WhatsApp, and email

- Advanced filtering to quickly locate relevant data during investigations

Why it matters: Faster, more accurate eDiscovery can **significantly lower legal costs** and ensure compliance with regulatory requirements.

DOES THE VENDOR PROVIDE FLEXIBILITY AND AVOID VENDOR LOCK-IN?

Many vendors make **migrating data difficult and costly**. Ensure you **maintain full control** over your archived data.

Key considerations:

- How accessible will your data be?

- Will there be extra costs to retrieve your data?

- Are there open APIs to integrate with your existing IT ecosystem?

Why it matters: Avoiding vendor lock-in ensures **your organization can adapt to future business needs** without facing unexpected migration challenges.

CONCLUSION: FUTURE-PROOF YOUR DIGITAL COMMUNICATIONS GOVERNANCE & ARCHIVING

IT leaders can no longer rely on email-only archiving solutions. The modern enterprise requires a **scalable, compliant, and secure approach** that captures, manages, and governs **all digital communication channels**—from email and Teams to WhatsApp and social media.

AI-driven analytics now play a critical role in governance and compliance, helping organizations **automate retention policies, detect risks in real time, and streamline eDiscovery**—reducing manual overhead and ensuring greater accuracy.

Choosing the right DCGA solution with AI capabilities ensures long-term compliance, security, and operational efficiency across your organization.

Want To Learn More?

Discover how Archive360 can help your organization future-proof its governance and archiving strategy.

Learn more

ARCHIVE360

Archive360 is the modern archiving company that empowers organizations worldwide to solve complex data governance and compliance challenges, while enabling AI and analytics. We enable customers to provide accurate, trusted, secured data to any of their AI and analytics tools - including Open AI, CoPilot Studio, Snowflake and Databricks - transforming archived data into a strategic asset, ready to support their business goals and strategic initiatives.

To learn more, please visit www.archive360.com