piler

Email Compliance Checklist
Assess your archiving and compliance posture

Use this checklist to evaluate your organization's email archiving practices against regulatory requirements and industry best practices. Check each item that applies, then calculate your compliance score at the end.

1. Retention Requirements

General Requirements

- ☐ **Defined retention periods** - Documented retention periods for different email types
- ☐ **Regulatory alignment** - Retention periods meet your industry's legal requirements
- ☐ **Consistent application** - Retention policies apply to ALL email (not just select mailboxes)
- ☐ **Deletion procedures** - Process exists for deleting emails after retention period expires

Retention by Regulation

Regulation	Applies To	Minimum Retention
SEC 17a-4	Broker-dealers, financial services	6 years (first 2 immediately accessible)
FINRA 3110	FINRA member firms	3-6 years depending on record type
HIPAA	Healthcare, health plans	6 years from creation or last effective date
SOX	Public companies (US)	7 years for audit-related communications
GDPR	EU resident data handlers	As long as necessary (must justify)
IRS	All US businesses	7 years for tax-related communications

- ☐ **Identified applicable regulations** - You know which regulations apply to your organization
- ☐ **Documented justification** - Retention periods documented with regulatory justification

2. Archive Integrity

Capture Completeness

- ☐ **All mailboxes archived** - Every user mailbox captured
- ☐ **Shared mailboxes included** - Distribution lists, shared inboxes
- ☐ **External email captured** - Inbound and outbound
- ☐ **Internal email captured** - Between internal users
- ☐ **Attachments preserved** - Stored with parent message
- ☐ **Calendar invites archived** - Meeting invitations captured

Tamper Protection

- ☐ **Immutable storage** - Cannot modify after capture
- ☐ **Hash verification** - Cryptographic integrity check
- ☐ **Audit trail** - All access logged
- ☐ **Chain of custody** - Documentation exists

3. Search & Retrieval (eDiscovery Readiness)

Search Capabilities

- ☐ **Full-text search** - Body, subject, attachments
- ☐ **Metadata search** - Sender, recipient, date range
- ☐ **Boolean operators** - AND, OR, NOT, phrases
- ☐ **Attachment search** - Inside PDF, Office docs

Legal Hold & Export

- ☐ **Export formats** - EML, PDF for legal review
- ☐ **Legal hold capability** - Freeze from deletion
- ☐ **Audit logging** - Searches/exports logged

Access Control

- ☐ **Role-based access** - Admin, auditor, user levels
- ☐ **User self-service** - Search own archived email
- ☐ **Access logging** - Logged with user identity

4. Data Protection

Encryption

- ☐ **Encryption at rest** - Encrypted in storage
- ☐ **Encryption in transit** - TLS for capture and access
- ☐ **Key management** - Securely stored and backed up

Data Sovereignty

- ☐ **Data location known** - Know where data is stored
- ☐ **Jurisdiction acceptable** - Meets regulatory requirements

Backup & Disaster Recovery

- ☐ **Regular backups** - Backed up on schedule
- ☐ **Backup verification** - Tested for successful restore
- ☐ **Geographic redundancy** - Separate location
- ☐ **DR plan tested** - Tested annually

5. Modern Messaging Channels

Microsoft Teams

- ☐ **Teams archiving enabled** - Chats and channels captured
- ☐ **Private chats included** - 1:1 and group chats
- ☐ **File shares captured** - Files in conversations

Slack

- ☐ **Slack archiving enabled** - Messages captured
- ☐ **Private channels included** - Not just public channels
- ☐ **Direct messages included** - DMs captured per policy

6. Policies & Procedures

Documentation

- ☐ **Email retention policy** - Written and approved
- ☐ **Acceptable use policy** - States email may be monitored/archived
- ☐ **Legal hold procedures** - Documented process
- ☐ **eDiscovery procedures** - Process for legal requests

Training & Awareness

- ☐ **IT admin training** - Administrators trained on system
- ☐ **Legal/compliance training** - eDiscovery procedures understood
- ☐ **Annual review** - Policies reviewed annually

7. Calculate Your Score

Your Compliance Score

_____ / 50

Score	Rating	Recommendation
45-50	Excellent	Maintain and continuously improve
35-44	Good	Address gaps in high-risk areas
25-34	Fair	Prioritize retention and integrity items
15-24	Needs Work	Significant compliance risk - act quickly
<15	Critical	Major gaps - seek expert guidance immediately

Tip: Focus first on items in "Retention Requirements" and "Archive Integrity" sections - these carry the highest regulatory risk.

Next Steps

- Schedule quarterly compliance review
- Test eDiscovery process with mock legal request
- Verify backup restoration works
- Review and update policies annually

Need help with email archiving compliance?
mailpiler.com