

i-ARM Data Compliance Extender for Microsoft Purview

Document Control

- **Version:** 1.0 (Focused Edition)
- **Status:** Draft for Review
- **Date:** 17 Jan 2026
- **Owner:** Infotechtion Product & Engineering (i-ARM)
- **Audience:** CIO, CISO, Heads of Information Governance, Records Managers, Storage/Platform Owners

i-ARM Data Compliance Extender for Microsoft Purview	1
Document Control	1
1. Overview	2
2. Scope of Service	2
3. Capabilities	3
4. Architecture Overview	3
5. High Availability & Resilience	4
6. Hosting Options	4
7. Prerequisites	4
8. Service Modules & Workflows	4
8.1 Retention & Fileplan Orchestration.....	4
8.2 ROT & Duplicate Management	5
8.3 Storage Optimization.....	5
8.4 Records Archival (Including WORM/Immutability)	5
9. Security & Compliance	5
10. Service Interface	5
10.1 Channels & Entry Points.....	5
10.2 Authentication & Authorization.....	6
10.3 Functional Areas (Focused).....	6
10.4 Accessibility & Usability	6
10.5 Observability & Audit	6
10.6 Client Support & Interoperability	6

10.7 Data Handling	6
11. Reporting & Success Measures	7
12. Onboarding & Change Management	7
13. Support & SLAs (Focused).....	7
14. RACI Summary	7
14. Information Security Policies and Processes	8
15. Glossary	8

1. Overview

i-ARM is an intelligent governance extension for **Microsoft Purview** that delivers end-to-end **records retention**, **ROT (redundant, obsolete, trivial) management**, **storage optimization**, and **long-term archival** across Microsoft 365, Azure Files/Blobs, on-prem file shares, and selected multicloud sources. i-ARM orchestrates policy synchronization, in-place enforcement, evidential disposition, and cost-saving archival through dashboards and automated workflows.

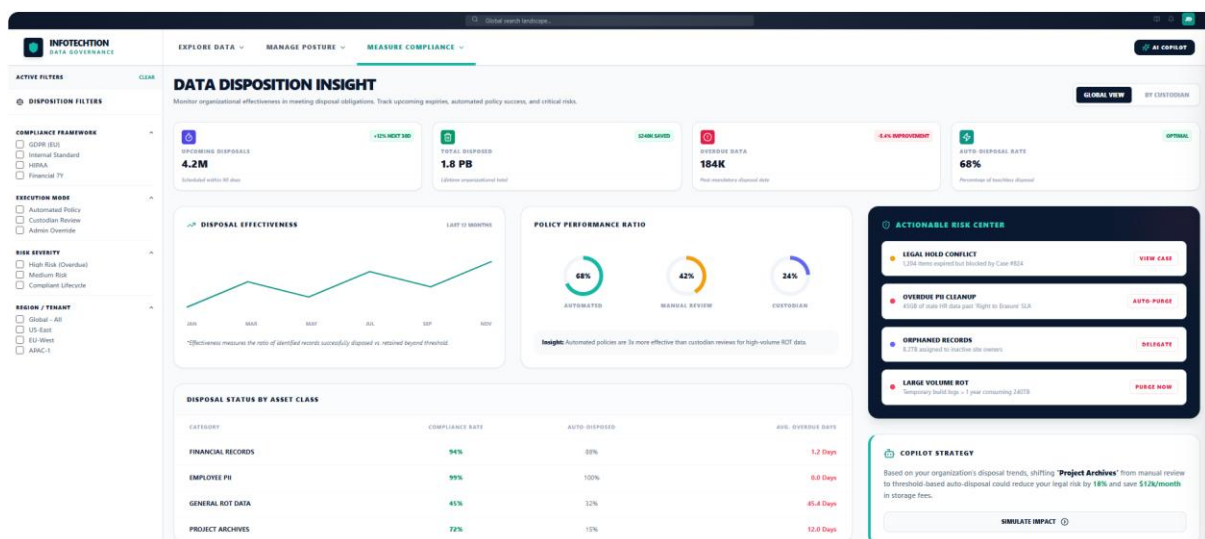


Figure 1: Data Lifecycle Posture

It embraces Purview's retention engine while extending control to non-M365 repositories and structured data bridges where applicable.

2. Scope of Service

This focused service definition covers:

- Retention & fileplan orchestration with Microsoft Purview (labels, schedules, events).
- ROT/duplicate discovery, review, and defensible remediation.
- Storage optimization via archival, tiering, and in-place minimization actions.
- Records archival including WORM/immutability patterns and evidence packages.

Out of scope: workspace provisioning, physical records (unless tied to archival flows), or general analytics beyond the four domains above.

3. Capabilities

- **Universal Retention Connector (URC):** Synchronize retention fileplan to Purview; align labels and selected properties (retention duration, review stages, default record behavior, post-retention relabel).
 - **In-place Retention & Discovery:** Apply Purview retention labels across M365, Azure Files/Blobs, and file servers; i-ARM surfaces end-of-retention queues and aggregates reviewer decisions.
 - **ROT & Duplicate Analytics:** Identify stale/dark data, ROT, and duplicates using dictionaries, rules, and AI signals; provide owner-assignable review backlogs with bulk actions.
 - **Storage Optimization Orchestration:** Quarantine, archive, or delete per policy; cost dashboards show storage reductions through ROT/duplicate remediation and archival moves.
 - **Records Archival & Immutability:** Archive to customer-managed Azure Blob (immutability/WORM) or integrate with existing archives; preserve audit and chain-of-custody evidence.
-

4. Architecture Overview

Cloud-native on Azure (App Services/Functions, SQL, Storage, Key Vault) with Microsoft Graph and Purview APIs. Data remains **in-place**; i-ARM operates via policy sync, scans/metadata reads, and orchestration. Structured data posture/lineage bridges can surface into Purview where enabled; archival flows use secure transfer to cheaper storage tiers with label/state preservation.

Key flows (illustrative):

1. **Fileplan → Purview → i-ARM:** URC syncs/updates retention labels; i-ARM publishes and monitors application at sources.

2. **ROT/Duplicate → Review:** Scans/telemetry populate ROT backlogs; owners review, approve actions; exceptions carried forward.
 3. **End-of-Retention → Disposition:** i-ARM aggregates candidates, applies legal-hold aware exclusions, records decisions, issues evidence packages.
 4. **Optimization/Archival:** Approved items move to archival storage; immutability set where required; lineage of actions logged.
-

5. High Availability & Resilience

Azure availability zones for compute, **ZRS/GRS** for state and audit where applicable; automated retries and resumable jobs maintain governance continuity. i-ARM leverages Purview as master for label/retention state, enabling rebuild of orchestration metadata after incidents while preserving reviewer evidence via database backups.

6. Hosting Options

- **Customer-Hosted (PaaS):** Deployed in customer subscription with managed identities and private networking where required.
- **Infotechtion-Hosted (Dedicated SaaS):** Fully managed in an isolated subscription per customer.

Both models support CI/CD and change windows agreed with the customer.

7. Prerequisites

- Active Microsoft 365/Purview tenant with appropriate RBAC; Azure subscription for PaaS or archival targets.
 - Network egress to Microsoft endpoints; private endpoints/DNS where mandated.
 - Optional: Sentinel/Log Analytics for SIEM integration of audit streams.
-

8. Service Modules & Workflows

8.1 Retention & Fileplan Orchestration

- **Capabilities:** Import/sync from policy centers; publish Purview labels; monitor coverage; event-based retention and staged disposition; post-retention relabel.
- **Workflows:** Business rules → URC sync → Label publishing → Coverage KPIs → End-of-retention queues → Evidence.

8.2 ROT & Duplicate Management

- **Capabilities:** Dark-data inventory, ROT keyword dictionaries, duplicate detection, sensitivity exceptions (label overrides), owner assignment, bulk remediation.
- **Workflows:** Scan & classify → Owner review → Quarantine/retain/delete → Exceptions & audit.

8.3 Storage Optimization

- **Capabilities:** Data minimization and archival moves to lower-cost tiers; self-service transfer of records to Azure Files/Blob while preserving classification/retention state.
- **Workflows:** ROT/duplicate reduction → Archival candidate selection → Transfer with policy carry-forward → Ongoing tiering and reporting.

8.4 Records Archival (Including WORM/Immutability)

- **Capabilities:** Archive approved items to customer-managed Azure Blob with immutability (WORM) where mandated; integrate with external archives; maintain chain-of-custody and per-item audit for life of record.
 - **Workflows:** Disposition decision → Archive/transfer → Set immutability → Certificate/evidence packaging.
-

9. Security & Compliance

- **Secure SDLC, encryption in transit/at rest, managed identities, RBAC,** and audited APIs.
 - **Legal-hold awareness** in disposition; **lifecycle-long audit** extractable to BI/SIEM.
 - Alignment to records standards (e.g., SEC 17a-4/WORM scenarios) through immutable storage options and evidence artifacts.
-

10. Service Interface

10.1 Channels & Entry Points

- **Web portal:** Primary interface for retention orchestration, ROT backlogs, storage optimization, and archival workflows.
- **Automation APIs:** Authenticated endpoints for bulk operations (label publishing, archival moves, evidence export) and integrations.

10.2 Authentication & Authorization

- **Azure AD SSO** with MFA per customer policy; **role-based access control (RBAC)** for Records Managers, Data Owners, Compliance Admins, and Operators.
- **Least-privilege** service identities for background jobs; actions are executed under auditable identities with correlation IDs.

10.3 Functional Areas (Focused)

- **Retention & Fileplan:** Label publishing, coverage dashboards, event triggers, end-of-retention queues, reviewer worklists.
- **ROT Management:** ROT/Duplicate explorer, owner assignments, bulk remediation (quarantine, delete, re-label) with pre-flight policy checks.
- **Storage Optimization:** Cost dashboards, archival candidate selection, tiering recommendations, execution progress with resumable jobs.
- **Records Archival:** Archive pipelines to customer-managed Blob (optional immutability/WORM), chain-of-custody tracking, certificate/evidence packaging.

10.4 Accessibility & Usability

- Aligns to **WCAG 2.1 AA**: keyboard navigation, high-contrast themes, ARIA labels, screen-reader support, and responsive layouts.
- Consistent navigation, meaningful labels, in-context help, and error recovery patterns.

10.5 Observability & Audit

- Every user and system action is **audited** (who/what/when/where), exportable to **Power BI/SIEM**; advanced filtering by label, site, owner, or action.
- **Health panels** for connectors, jobs, and pipelines; alerts via email/Teams webhooks.

10.6 Client Support & Interoperability

- Optimized for latest **Microsoft Edge** and **Google Chrome**; responsive for common desktop resolutions.
- Data export to **CSV/Excel**; APIs support idempotent retries and back-pressure for long-running jobs.

10.7 Data Handling

- **In-place operations** wherever possible; portal stores orchestration metadata and evidence only, not customer content.

This interface model is consistent with the 2024 template's service-interface principles and extends them for retention, ROT, optimization, and archival.

11. Reporting & Success Measures

Operational KPIs

- % data under retention labels; % sources with ≥95% coverage.
- ROT reduction (GB/TB) and duplicate elimination rate.
- Archival volume moved to cheaper tiers and associated cost avoidance.
- Disposition throughput and evidence completeness.

Analytics & Dashboards

- ROT/Duplicate explorer, labeling and lifecycle coverage, archival pipeline status; export to Power BI and SIEM.
-

12. Onboarding & Change Management

1. **Discovery & Readiness:** Sources, policies, ROT dictionaries, archival targets, legal constraints.
 2. **Foundation:** Deploy components, connect Purview, enable URC, configure roles and connectivity.
 3. **Enablement:** Import fileplans, publish labels, tune ROT rules; pilot end-of-retention and archival flows.
 4. **Operate:** Hyper-care; weekly KPIs; handover to steady-state operations with cost/benefit reporting.
-

13. Support & SLAs (Focused)

Support Locations & Hours: India & Australia; UK & Ireland; Europe; Canada; US. Business hours Mon–Fri 08:00–17:00 local; extended/24×7 by agreement.

Incident SLAs (modules in scope): Critical 20m/2h; High 20m/4h; Medium 3h/29h; Low 7h/44h. Resolution may be a stable workaround pending permanent fix.

14. RACI Summary

- **Customer:** Tenancy controls, data-owner assignments, legal-hold management, archival storage ownership.

- **Infotechtion:** URC/retention orchestration, ROT analytics, archival workflows, monitoring & incident/change/problem management.
 - **Joint:** Success KPIs, approvals for deletion/archival, periodic posture reviews.
-

14. Information Security Policies and Processes

The product architecture ensures the confidentiality, integrity, and availability of organizational data while complying with regulatory standards.

Key Principles:

- **Access Control:** Implement role-based access to sensitive information.
- **Data Encryption:** Use encryption for data at rest and in transit.
- **Incident Response:** Maintain a documented process for identifying, reporting, and mitigating security incidents.
- **Compliance:** Adhere to relevant standards such as ISO 27001 and GDPR.
- **Monitoring:** Continuous monitoring of systems for vulnerabilities and threats.

Processes:

1. **User Authentication:** Multi-factor authentication for all critical systems.
 2. **Data Backup:** Regular backups stored securely offsite.
 3. **Audit Trails:** Maintain logs for all system activities for accountability.
 4. **Training:** Mandatory security awareness programs for all employees.
 5. **Review:** Quarterly review of security policies and procedures.
-

15. Glossary

- **ROT:** Redundant, Obsolete, Trivial information.
 - **URC:** Universal Retention Connector.
 - **WORM/Immutability:** Write-Once-Read-Many storage enforcing non-erasable, non-rewritable records.
 - **End-of-Retention:** Point at which policy permits disposition or archival.
-

16. Notes and References

- This focused service definition intentionally excludes features unrelated to retention, ROT, optimization, and archival.
- Detailed runbooks, architecture diagrams, and customer-specific data flows are provided during onboarding.

- Target Operating Model - [Target Operating Model | i-ARM Docs](#)
- Detailed technical architecture [Architecture | i-ARM Docs](#)