MultiCloud Data & AI Risk Compliance (Dedicated SaaS)

Service Definition — 2026 SaaS Edition

Contents

1. Executive Overview 2
2. Scope & Outcomes 2
3. Capability Catalogue 2
4. SaaS Architecture & Connectivity (SPN) 3
    4.1 Service Principal (SPN) Requirements 3
    4.2 Required Permissions 3
    4.3 Automated Provisioning 4
5. Supported Data Sources & Capability Matrix 4
6. Unified DSPM for Microsoft Security Copilot 5
7. Azure Marketplace & Procurement Simplification 5
8. Advanced Data Disposal & AI Training 6
9. SaaS Evergreen Strategy 6
10. Exit Strategy & Data Portability 6
    10.1 Onboarding and Offboarding 7
11. Service Interface 8
12. Target Operating Model (TOM) 8
13. Roles & Responsibilities (RACI) 9
14. Support, SLAs & Residency 9
15. Information Security Policies and Processes 9
16. Glossary 10

1. Executive Overview

Infotechtion delivers data and AI risk management solutions, supported by managed services that help organizations understand their data, reduce exposure, and govern AI with confidence.

When you know your data, you can control risk—and safely unlock AI value.

Infotechtion Data & AI Compliance platform is an enterprise-grade SaaS platform designed to centralize and automate data compliance risk remediation, integrating seamlessly with Microsoft Purview and other industry-standard compliance frameworks to secure the heterogeneous data estate.

The platform provides the advanced orchestration and risk remediation execution engine essential for modern agentic AI adoption, risk-based data disposal, and long-term audit evidence.

2. Scope & Outcomes

The Data & AI compliance platform is a SaaS service is designed to deliver four primary outcomes:

- **Govern Agentic AI:** Visibility and auditability into interactions (e.g., M365 Copilot) with automated remediation for oversharing.
- **Unified Security / Compliance Posture:** Integrates with Microsoft Purview, Security Copilot and other data governance platforms to enforce classification, encryption, access and retention logic across non-Microsoft repositories (S3, Box, File Shares).
- **Reduce Digital Waste:** Automated identification of ROT (Redundant, Obsolete, Trivial) data and defensible disposal supported by time-bound quarantine before disposal.
- **Unified Evidence:** A single audit trail for lifecycle events contextualised with User and AI interactions across all connected nodes.

3. Capability Catalogue

- **AI Risk & Copilot Governance:** Oversharing analytics, prompt/response auditing, and readiness assessments.
- **Unified Data Discovery (DCSPM):** Sensitive data discovery across cloud/on-prem with automated owner assignment.
- **Universal Retention Connector (URC):** Bi-directional sync between retention systems of records and labels within Microsoft Purview or other governance platforms.

- **Lifecycle, Archival & Disposition:** Multi-stage review queues with legal-hold awareness and WORM archival options.
- **Proactive Disposal Wizard:** Advanced UI for custodians to define and automate data minimization.
- **Unified DSPM for SOC:** Integration with Microsoft Security Copilot for centralized security analysis.

4. SaaS Architecture & Connectivity (SPN)

The platform operates on a Dedicated SaaS model. While the engine resides in a managed Infotechtion cloud environment, it utilizes In-Place Governance.

Detailed architecture is available at: https://docs.infotechtion.com/docs/tech-docs/Architecture

4.1 Service Principal (SPN) Requirements

To facilitate secure communication, a Service Principal (SPN) must be established within the customer's Microsoft Entra ID.

4.2 Required Permissions

The following application scopes are required for the SaaS platform to govern the customer environment:

Data Source	Permission Type	API / Scope	Justification
Microsoft Graph	Application	Directory.Read.All	Syncing custodian identities and group ownership.
SharePoint	Application	Sites.FullControl.All	Required for the Data Disposal Wizard to execute actions.
Exchange	Application	Mail.Read	Metadata analysis for communication governance.
Azure Storage	RBAC	Storage Blob Data Contributor	Managing lifecycle on unstructured containers.

Note: The above table is a short list if permissions per data sources, a full list of permissions is available at https://docs.infotechtion.com/docs/tech-docs/ConfigurationDesign

4.3 Automated Provisioning

The platform provides automated scripts via Azure marketplace to simplify setup. Custodians can copy pre-formatted PowerShell commands directly from the Data Sources configuration page:

Grant-PnPAzureADAppSiteAdmin -AppId "{The platform-App-ID}" -Site "https://{customer-tenant}.sharepoint.com"

5. Supported Data Sources & Capability Matrix

The platform provides tiered levels of integration depending on the source platform's API maturity.

Data Source	Classification	Tagging/Labelling	Retention/ Disposal	Archival (WORM)	ROT Minimization	AI Interaction Audit
SharePoint Online	Full (AI + SIT)	Native Purview	Automated + Review	Supported	Full (Auto-Purge)	Full Visibility
Exchange Online	Full (AI + SIT)	Native Purview	Automated + Review	Supported	Policy Based	Prompt/Response
OneDrive / Teams	Full (AI + SIT)	Native Purview	Automated + Review	Supported	Full (Auto-Purge)	Full Visibility
Azure Blob / AWS S3	Discovery Only	Metadata Only	Policy Driven	WORM/Immutable	Policy Driven	Metadata Only
Snowflake	Table/Column	Tag Bridge	Archival Trigger	Snapshot Archive	Archival Trigger	N/A
Box / Google Drive	AI Classifier	App-Specific Tags	Manual Review	Supported	Manual Review	Metadata Only
On-Prem File	Local Crawler	Metadata Only	Defensible Deletion	Move to Cloud	Defensible	N/A

Data Source	Classification	Tagging/Labelling	Retention/ Disposal	Archival (WORM)	ROT Minimization	AI Interaction Audit
Shares					Deletion	

6. Unified DSPM for Microsoft Security Copilot

The platform leverages the Infotechtion Data Connector to deliver a unified Data Security Posture Management (DSPM) experience within the Microsoft Security stack.

- Centralized Analyst Interface: Security analysts can now use Microsoft Security Copilot as a common place to query data security and compliance insights across the entire estate.
- Agentic Insights: By pushing cross-platform signals into the Microsoft Sentinel ecosystem, analysts can identify "toxic combinations" across Snowflake, AWS S3, and M365.
- Compliance Grounding: Security Copilot leverages The platform metadata for grounding, allowing natural language queries regarding data risk and archival status.

7. Azure Marketplace & Procurement Simplification

To ensure a seamless experience for enterprise customers, The platform is available as a transactable offer on the Azure Marketplace.

- Seamless Deployment: Customers can provision their dedicated SaaS tenant directly from the Azure portal. The integration uses automated handshakes to initialize the environment, significantly reducing onboarding time.
- MACC Credit Eligibility: Spend on The platform via the Azure Marketplace contributes 100% toward a customer's Microsoft Azure Consumption Commitment (MACC). This allows organizations to leverage pre-committed cloud spend for data governance and AI compliance.
- Unified Billing: Costs for the The platform service are consolidated into the existing Microsoft Azure invoice, simplifying vendor management and internal procurement approvals.

8. Advanced Data Disposal & AI Training

The 2026 edition introduces Agentic Discovery for data disposal, allowing custodians to automate complex cleanup tasks.

- Disposal Pillars: Targeted workflows for Redundant (ROT), Obsolete (stale), and Official Records.
- Interactive Training Mode: Before global deployment, custodians specify a test location to evaluate agent behavior.
- Accuracy Telemetry: The AI Agent generates a real-time Accuracy % telemetry, providing a confidence score to stakeholders before automated policies are promoted to production.
- Feedback Loop: Custodians provide Thumbs Up/Down feedback to refine agent reasoning before bulk execution.

9. SaaS Evergreen Strategy

The platform follows an Evergreen Deployment Model to ensure continuous synchronization with evolving cloud provider APIs and AI models.

- API Parity Monitoring: Automated regression testing against Microsoft Graph, Purview, and AWS APIs ensures policy stability.
- Zero-Touch Feature Rollouts: Updates to classification SITs and AI agents are applied globally in the SaaS backend without requiring customer downtime.
- AI Model Evolution: Discovery agents are fine-tuned based on anonymized feedback loops to improve cross-tenant accuracy.

10. Exit Strategy & Data Portability

The platform's "In-Place Governance" philosophy ensures the customer retains full control of their primary data assets throughout and after the service lifecycle.

- In-Place Preservation: 100% of the customer's primary data remains in its original source.
- Metadata & Evidence Export: Customers can export all Audit Trails, Disposal Certificates, and Classification Maps.
- Service Principal Revocation: Offboarding is completed by deleting the The platform App Registration and revoking RBAC permissions.

10.1 Onboarding and Offboarding

- User Onboarding to the service - Infotechtion service implementation team includes business change and adoption services. The implementation plan includes a business adoption track, to inform, educate and onboard users to the service. The onboarding process includes the functional training, process for reporting issues, and service desk support.
- Service Documentation / User Manual
    - Formats
    - Accessibility Standards Company Confidential
- End of contract process - The end of contract process is managed via a well document exit strategy and exit plan. The exit strategy is discussed and agreed with the customer ahead of service onboarding, regular checks are performed during the service period to ensure the exit plan is practical. A date is agreed with the customer to invoke the exit plan, delivered via a joint customer and Infotechtion team.
- Product Deactivation: is achieved via an Azure administrator disabling all runtime services associated with the Infotechtion-ARM product. Another option to deactivate product is by disabling all source integrations from the Infotechtion-ARM administrative settings.
    - Product deactivation does not delete any data or product features but stays dormant including notifications.
- Product Uninstall: The primary code removal is done through automated deployment pipelines established to manage feature release.
    - Uninstalling custom Azure services, storage accounts, and Azure SQL databases involves deleting the resources from the Azure portal.
    - This can be done by navigating to the specific resource, selecting the 'Delete' option, and following the prompts.
        - It is important to note that deleting these resources is permanent and cannot be undone.
        - Before uninstalling, the uninstall instructions provide details of any relevant data extractions or backups as per customer request.
    - User offboarding is done via removing users from Azure AD groups associated with the product features. Subsequently, the groups are also deleted by accessing the Azure portal by an authorized administrator.
- End of Contract Data extraction - The data / metadata extraction is supported via a service request. Customer administrator can submit a request and data is made accessible within the customer Microsoft Azure / other cloud subscription

11. Service Interface

The The platform platform features a high-fidelity, web-based control center designed for performance and ease of use. It follows a Custodian-First design philosophy, ensuring that complex governance tasks are simplified through visual telemetry and guided workflows.

- **Unified Web Portal:** A modern Single Page Application (SPA) built with a minimalist slate and electric-blue aesthetic. It provides specialized dashboards for Executive Insights, Operational Posture, and Source Data Exploration.
- **AI Copilot Sidebar:** A permanent, context-aware AI assistant integrated directly into the UI. The Copilot provides natural language support for grounding queries, agent calibration, and policy analysis.
- **Hierarchical Asset Browsers:** Advanced explorers for Source Data and Archive Vaults that allow custodians to navigate across sites, libraries, and containers with a "Drill-to-Item" capability.
- **Guided Policy Wizards:** Task-oriented wizards (e.g., Access Review Wizard, Data Disposal Wizard) that break down complex compliance configurations into manageable steps, including the exclusive "AI Training Mode."
- **Real-time Telemetry:** Dynamic SVG charts and gauges providing immediate feedback on platform throughput, sync health, and resource utilization.

12. Target Operating Model (TOM)

The platform implements a modern Target Operating Model that shifts organizations from reactive manual data management to proactive, AI-assisted governance. The model balances centralized oversight with federated accountability.

- **Centralized Governance:** Compliance and Security teams define global policies, taxonomies, and risk thresholds within the The platform control plane.
- **Federated Execution:** Data Custodians and Business Owners are empowered with AI-assisted tools to validate discoveries and execute disposal within their specific domains.
- **Continuous Lifecycle:** The model relies on a recursive loop of Discovery → Classification → Remediation → Audit.
- **Agentic Accountability:** AI agents perform the heavy lifting of content analysis, while humans remain "in-the-loop" for high-stakes decisions and model training.

For a detailed breakdown of the Target Operating System framework, visit: https://docs.infotechtion.com/docs/tech-docs/Targetoperatingsystem/

13. Roles & Responsibilities (RACI)

- Customer: Ownership of identity governance (Entra ID), legal-hold management, and final approval for disposal actions.
- Infotechtion (SaaS): Management of platform availability, AI model tuning, connector health monitoring, and security patching.
- Joint: KPI definition and periodic posture reviews.

14. Support, SLAs & Residency

- Support: Global coverage with incident response tiers (Critical: 2h, High: 4h).
- Residency: Instances are deployed in the customer's preferred Azure region.
- Encryption: All data in transit is secured via TLS 1.3; secrets managed via Azure Key Vault.

  Note: for more details on service level agreement (SLA), refer to https://docs.infotechtion.com/docs/tech-docs/Targetoperatingsystem#The platform-support-sla

15. Information Security Policies and Processes

Information security is a key priority for Infotechtion, a company that delivers high-quality software solutions to its clients.

Infotechtion follows the secure software development life cycle (SSDLC) framework, which integrates security best practices into every stage of the software development process, from planning to deployment. Infotechtion applies various security controls, such as encryption, authentication, authorization, logging, and auditing, to safeguard the data and systems from unauthorized access, modification, or disruption.

Infotechtion also performs regular security risk assessments, vulnerability scans, and penetration tests to detect and fix any potential threats or weaknesses in the software. Infotechtion has a dedicated information security team that monitors and responds to any security incidents or breaches and reports them to the relevant stakeholders and authorities in a timely manner.

Infotechtion also educates its employees and contractors on the information security policies and processes and ensures compliance through audits and reviews.

Infotechtion strives to maintain the trust and confidence of its clients by delivering secure and reliable software solutions.

16. Glossary

Term	Definition
DSPM	Data Security Posture Management.
MACC	Microsoft Azure Consumption Commitment.
ROT	Redundant, Obsolete, and Trivial data.
SPN	Service Principal Name (App Registration).
WORM	Write-Once, Read-Many (Immutable storage).
SIT	Sensitive Information Type regex, dictionary keyword patterns.
SSDLC	Secure Software Development Life Cycle. A framework that integrates security best practices into each phase of software development, from planning to deployment.
SLA	Service Level Agreement. A formal agreement outlining the expected level of service, including response times and support coverage.
TLS	Transport Layer Security. A protocol ensuring encryption and secure data transmission over networks; the document references TLS 1.3 for data in transit.
Azure Key Vault	A Microsoft Azure service for securely managing secrets, such as encryption keys and passwords.
Incident Response Tiers	Levels of urgency for addressing support incidents, such as Critical (2 hours) and High (4 hours).
Penetration Test	A security assessment in which testers attempt to exploit vulnerabilities in a system to identify weaknesses.
Vulnerability Scan	An automated process to identify security flaws in systems and software.
Authentication	The process of verifying the identity of a user or system.
Authorization	The process of granting or denying access rights to resources based on identity.
Logging	Recording events and activities for monitoring and auditing purposes.
Auditing	Reviewing and analysing logs and activities to ensure compliance and detect security incidents.