



HARMAN DATA GOVERNANCE AND DATA PROTECTION OFFERING USING PURVIEW

2025



EXISTING CHALLENGES

- High manual fragmented effort
- Reduced customer satisfaction
- No global reporting views
- Lack of trust in data
- Past efforts focused on data cleansing and governance frameworks
- Efforts were not sustainable improvements
- Need to institutionalize and operationalize efforts across the enterprise

HARMAN PROPOSES AN ASSESSMENT LED IMPLEMENTATION APPROACH

- Implementing data discovery, cataloguing, and governance controls
- Developing a business glossary, ensuring data lineage, and establishing data classification
- Enhancing collaboration, tracking usage analytics, and managing metadata effectively
- Knowledge & best practices from similar engagements with global corporates

Achieve growth & become data-driven Organization



SECURITY CONCERNS: Harman identifies amplified and emerging security risks such as data leakage, hallucinations, harmful content, model theft, prompt injections, and training data poisoning. Security leaders are particularly concerned about data security, regulatory compliance, and the accuracy of AI outputs.

SECURITY IS PRIORITY :

- **Form a Dedicated Security Team:** Establish cross-functional teams to manage AI security, with a median team size of 24 employees.
- **Optimize Resources:** Allocate increased IT security budgets to address AI-specific challenges and ensure compliance with regulations.
- **Implement a Zero Trust Strategy:** Adopt a Zero Trust approach to continuously validate identities and access, minimizing risks.
- **Adopt Comprehensive Security Solutions:** Procure specialized tools and platforms to secure AI usage and development, ensuring continuous protection and compliance.

KEY INDUSTRY TRENDS FOR IMPLEMENTING MICROSOFT PURVIEW



DATA SECURITY:

Visibility into Data Risks:

Organizations need comprehensive visibility into data security risks, especially with the rise of generative AI.

Continuous Risk Assessment:

Continuous monitoring and assessment to mitigate risks.

COMPLIANCE:

Finance Sector: Ensuring compliance with AML and KYC regulations.

Healthcare Sector:

Managing patient data privacy and compliance with HIPAA and GDPR.

DATA GOVERNANCE:

Unified Data Governance:

Implementing a unified service to discover, catalogue, and classify data.

Data Privacy: Ensuring robust data privacy and protection measures.

AI & ML INTEGRATION:

Enhanced Data Insights:

Leveraging AI and machine learning for deeper insights and improved decision-making.

Fraud Detection: Using advanced analytics to detect and prevent fraud.

INDUSTRY-SPECIFIC USE CASES:

Finance: Driving compliance and fraud detection.

Healthcare: Empowering patient data management and privacy.

Retail: Enhancing customer analytics and personalized experiences.

HOW PURVIEW HELPS IN PUTTING THE RIGHT DATA STRATEGY



Data Discovery and Cataloging: Identifies and catalogues data assets, making it easier to locate and utilize relevant data.

Example: A pharmaceutical company can easily catalogue research data, clinical trials, and patient records, ensuring they are discoverable and accessible for analysis.

Data Quality Management: Enhances data quality and consistency across the organization.

Example: A BFSI company can maintain consistent and high-quality customer data across all their systems, reducing errors and improving service.

Data Mapping: Provides a clear view of data relationships and lineage, which aids in strategic decision-making.

Example: A logistics company can map the relationships between shipment data, delivery times, and customer feedback, optimizing their delivery processes.

Data Policy Enforcement: Establishes and enforces data policies to ensure governance and compliance.

Example: A media company can enforce content access policies, ensuring only authorized personnel can access sensitive production data.

WHY IS MICROSOFT PURVIEW REQUIRED?



Unified Data Governance: Combines data governance and compliance solutions into one platform.

Example: A large multinational company like Microsoft deals with vast amounts of data spread across various departments. Purview unifies the data governance framework, ensuring consistent policies and procedures are followed organization-wide.

Visibility and Control: Provides comprehensive visibility into data across the organization and helps manage sensitive data effectively. Secure by default with Microsoft Purview and protect against oversharing.

Example: A financial services company can have visibility into all transactions, customer details, and regulatory compliance documents across multiple branches.

Regulatory Compliance: Ensures compliance with various regulatory requirements and aids in managing data risks.

Example: Healthcare providers using Purview can ensure patient data complies with regulations like HIPAA, tracking all data access and modifications.

1

DATA DISCOVERY

Use connectors, REST APIs and data finger-printing to extract and tag business & technical metadata from systems or databases

2

DATA LINEAGE

Track where data originated, how it flows physically through to data consumption, with visualisation via knowledge graphs

3

METADATA MANAGEMENT

Common repository used to document, manage, rate and publish metadata and its relationships, incl. reference data

4

DATA COLLABORATION

Pre-defined, customizable, AI/ML-augmented workflows for metadata crowd-sourcing, endorsements and curation

5

BUSINESS GLOSSARY

Develop, publish and manage business term definitions, lists of values (reference data), synonyms, exceptions and usage

6

DATA MARKETPLACE

Browse, request and access data sets (data shopping); Catalog Monitoring with data set history and audit trail

7

DG OPERATIONS

Mapping/governance of DG organization structure, stakeholders, roles, program timeline, activities

8

DATA PROFILING

Basic data quality analysis, using dash-boards to visualize data completeness, accuracy etc.; Data sampling

9

DATA CLASSIFICATION

Automatic or manual tagging of data, data sets or documents into different levels of security/protection, using AI/ML/NLP

10

DATA RULES & POLICIES

Define and enforce business rules, policies and restrictions that are related to data elements and associated metadata

11

CATALOG INTEROPERABILITY

Support open-source data catalog industry standards and ontologies, and interact with other data catalogs

12

USER ACCESS & ANALYTICS

Tracking trends in levels and types of user activity such as data discovery, looking up definitions, tracing data origins

SENSITIVE DATA PROTECTION:

Microsoft Purview protects sensitive data across clouds, apps, and devices using discovery, classification, and encryption tools.

DATA CLASSIFICATION:

Tools like sensitive info types and classifiers help identify and monitor sensitive data and user actions.

ENCRYPTION:

Double Key and Customer Key encryption secure data, ensuring only authorized users can decrypt it.

DATA LOSS PREVENTION:

Prevents accidental sharing of sensitive data with policies that monitor, and block based on conditions.

INSIDER RISK MANAGEMENT:

Identifies and mitigates risky user activities through Microsoft 365 and Graph logs.

INFORMATION BARRIERS:

Restricts communication between groups to prevent conflicts of interest in regulated sectors.

PRIVILEGED ACCESS:

Limits ongoing access to sensitive data with just-in-time permissions, reducing breach risks.



Example:

- An ecommerce platform can protect customer payment details, addresses, and order history from breaches.
- A healthcare provider can identify and mitigate risks associated with patient data by tracking access and modifications.
- A government agency can ensure compliance with data protection laws like GDPR by classifying and labeling sensitive data appropriately.

MICROSOFT PURVIEW HELPS ORGANIZATIONS GOVERN, PROTECT, AND MANAGE THEIR DATA ESTATE

KEY SOLUTIONS INCLUDE:

- **Data Classification and Protection:** Automatically classify and protect sensitive data, like credit card numbers, ensuring only authorized access.
- **Data Loss Prevention (DLP):** Monitor and block unauthorized sharing of sensitive data through email, Teams, etc.
- **Insider Risk Management:** Detect and mitigate insider threats by identifying risky behavior patterns.
- **Data Lifecycle Management:** Implement retention policies to manage data from creation to deletion, such as deleting emails older than seven years.
- **eDiscovery and Audit:** Conduct investigations and audits using eDiscovery tools and audit logs.
- **Communication Compliance:** Monitor and enforce communication policies to detect and flag inappropriate communications.



DEFINE STRATEGY

- Set Goals: Improve data quality, ensure compliance, enhance security.
- Align with Business: Support overall business goals.

KEY FEATURES

- Data Map & Catalog: Visualize data landscape.
- Automated Discovery: Discover and catalog data across environments.
- Classification & Labels: Identify and protect sensitive data.

BEST PRACTICES

- Domains & Collections: Organize data governance structure.
- Automation: Reduce manual effort, keep catalog updated.
- Security: Implement network security measures.

START SMALL

- Pilot Projects: Begin with manageable projects.
- Iterative Approach: Gradually expand and refine.

REVIEW & UPDATE

- Compliance Checks: Regularly update policies.
- Feedback Loop: Continuously improve practices.

Consulting

- Data Governance Assessment
 - Identify gaps in current governance practices.
- Strategy and Roadmap Development
 - Create a roadmap for operationalizing data governance.
- Technology Evaluation
 - Recommendations for Purview deployment.
- Zero Trust Strategy Roadmap
 - Design a framework for secure access and data protection

Custom Solutions

- Data Classification Models
 - Build AI-driven data classification frameworks.
- Integration Frameworks
 - Custom solutions for seamless integration with tools like Power BI, Salesforce, and SAP.
- Automated Security validation
 - Develop scripts to automate governance and compliance checks.

Training & Enablement

- Workshops and Tutorials
 - Comprehensive training programs for teams.
- Best Practices Sharing
 - Knowledge transfer from Harman's implementation experience.
- Security Awareness Training
 - Educate teams on governance, compliance, and cybersecurity best practices.

Development & Implementation

- Data Cataloging and Lineage
 - Implement end-to-end data discovery and lineage tracking
- Business Glossary Creation
 - Build and deploy customized glossaries.
- Metadata Management
 - Enable centralized metadata management for organization-wide access.
- Access and Permissions Management
 - Set up robust security and access control measures.
- Real-Time Security Alerts
 - Configure security monitoring and alerting using Microsoft Defender and Azure Sentinel.

Support & Managed Services

- 24x7 Support
 - Round-the-clock monitoring and troubleshooting.
- Continuous Improvement
 - Preventive maintenance and periodic optimizations.
- Backup and Recovery
 - Comprehensive data protection and recovery plans.
- Policy Management
 - Ongoing updates to governance and compliance policies.



HARMAN IMPLEMENTATION APPROACH

INITIAL ASSESSMENT

DEPLOYMENT PHASE

FULL IMPLEMENTATION

3-4 weeks

to assess a tech company's current data governance practices.

5-6 weeks

to deploy and configure Purview for a multinational corporation.

4-5 months

for full integration and operationalization at an organization level.

ASSESSMENT:

Conduct a thorough assessment of current data governance practices to identify gaps and areas for improvement.

- Evaluate data governance maturity.
- Identify gaps in compliance, security, and governance.

Example: Conduct an assessment for a healthcare provider to identify data governance gaps and areas for improvement.

IMPLEMENTATION:

Deploy Microsoft Purview solutions tailored to the specific needs of the organization.

- Configure Purview for data cataloging, lineage, and classification.
- Integrate with enterprise systems (e.g., Azure, Power BI, SAP).

Example: Deploy Purview for a financial services firm, customizing it to their specific regulatory and operational requirements.

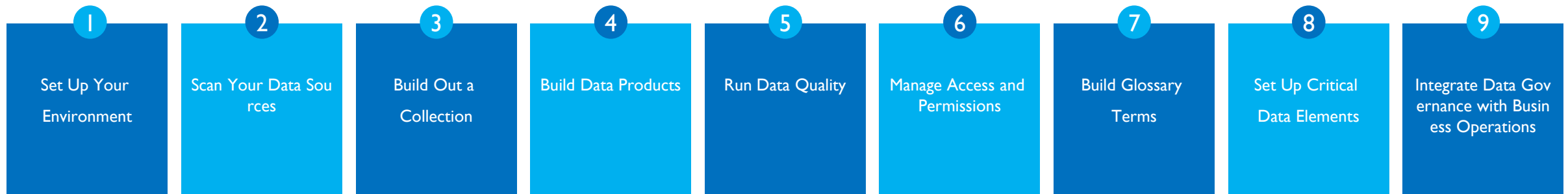
TRAINING AND SUPPORT:

Provide comprehensive training and ongoing support to ensure effective use of Purview.

- Operationalize governance with automated workflows.
- Ensure enterprise-wide adoption and compliance.

Example: Provide comprehensive training sessions for a retail company's staff to ensure effective use of Purview.

STEPS



HARMAN PROPOSITION MICROSOFT CENTER OF EXCELLENCE

HARMAN has a dedicated Business Unit for **Microsoft – Strategic partner for 3 decades**. Following are few highlights of our MS capability:

Technology Stack

250+ TRAINED RESOURCES ON FABRIC, PURVIEW, DYNAMICS 365, POWER APPS, POWER AUTOMATE, DATAVERSE, ETC. AND ARE READY TO DEPLOY

Continuous Trainings

Data Governance, Insider Risk Management, Security and Compliance with Microsoft Purview
Batch of 50 members trained

Microsoft Fabric, Purview PowerBI ,Copilot and Semantic Kernel
Batch of 130 members trained

TRAINING AND CAPABILITY BUILDING
ENABLING LARGER RESOURCE POOL ON MICROSOFT PURVIEW PLATFORM/TECHNOLOGIES TO CREATE CAPACITY AND CAPABILITY FOR LATEST MICROSOFT TECHNOLOGIES

Key Customers

MS CoE Highlights

100+ MS Technical SME, Architects & Sr Developers in Dynamics 365, Power Apps, Power Automate, SharePoint, SPFX Bots, Adaptive cards, Custom Apps, Teams Lifecycle Management, Policy Implementation, Microsoft Graph, Microsoft Fluent UI, Azure, Teams Adoption Management, etc.

Library of reusable components for faster Time to Market

Leverage the best practices & learnings across programs

Deep expertise for Fabric, Purview, Dynamics 365 CRM, Teams & Power Platform

HEALTHCARE



Patient Data Management: Efficiently manages and protects patient data, ensuring privacy and compliance with healthcare regulations like **HIPAA**.

Example: Purview helps a hospital manage **patient records**, ensuring they are secure and accessible only to authorized personnel.

Compliance: Ensures that all data handling meets healthcare standards.

Example: Ensures that patient data handling processes comply with **HIPAA** regulations.

AI Integration: Utilizes AI-driven insights to enhance patient care and operational efficiency.

Example: AI-driven insights from patient data can help improve treatment plans and patient outcomes.

BFSI



Data Security: Protects sensitive financial data from unauthorized access and breaches.

Example: Protects customer account details and transaction history from unauthorized access.

Regulatory Compliance: Helps meet stringent financial industry regulations.

Example: Helps meet financial regulations like PCI DSS by ensuring secure handling of payment card information.

Risk Management: Effectively manages financial risks through enhanced data governance.

Example: Identifies potential fraud risks by analyzing transaction patterns and alerting the relevant teams.

RETAIL



Customer Data Protection: Safeguards customer information, ensuring privacy and security.

Example: Safeguards personal information of customers, ensuring privacy and security during transactions.

Operational Efficiency: Improves decision making by providing accurate and timely data insights.

Example: Uses data insights to optimize inventory management and supply chain operations.

Compliance: Ensures adherence to retail industry standards and regulations.

Example: Ensures that data handling processes comply with retail industry standards like CCPA.

HITECH



Intellectual Property Protection: Secures proprietary technology data from unauthorized access.

Example: Secures proprietary algorithms and technological innovations from unauthorized access.

Innovation Support: Facilitates innovation by ensuring secure and accessible data.

Example: Facilitates secure and easy access to data for R&D teams, fostering innovation.

Regulatory Compliance: Ensures compliance with industry-specific regulations to protect data.

Example: Ensures compliance with industry regulations, protecting sensitive technological data.



THANK YOU

