Chapter 5

Implementing Data Governance with Azure Purview

Introduction

In today’s data-driven world, organisations are collecting and processing vast amounts of information. However, with great data comes great responsibility. Ensuring that data is well-organised, secure, and compliant with regulations is critical for business success. This is where data governance comes into play. Data governance establishes the policies, procedures, and standards necessary to manage data assets effectively. Microsoft Azure Purview stands out as a modern, cloud-native solution, empowering enterprises to implement robust data governance while seamlessly integrating with other Azure services.

Azure Purview is Microsoft’s unified data governance solution designed to empower organizations to manage, discover, and govern their on-premises, multi-cloud, and software-as-a-service (SaaS) data. As data landscapes grow increasingly complex, organizations face the challenge of maintaining data quality, ensuring compliance, cataloging assets, and establishing a robust governance framework. Azure Purview answers these needs with a scalable, cloud-native solution.

Azure Purview enables users to automatically discover data, classify sensitive information, map data lineage, and manage metadata across diverse data estates. At its core, Purview connects disparate data sources, providing a central view and control point for enterprise data governance. It supports organizations in achieving regulatory compliance, maintaining data security, and driving data democratization while mitigating risk.

Azure Purview is a unified data governance service from Microsoft designed to help organisations discover, catalogue, and manage their on-premises, multi-cloud, and software-as-a-service (SaaS) data. Its primary focus is to provide a holistic view of data assets, enabling businesses to understand their data landscape, ensure compliance, and drive trustworthy analytics.

Key Features and Capabilities:

* **Automated Data Discovery**: Scans and catalogues data across various sources, offering a central inventory for all data assets.
* **Data Classification**: Automatically classifies sensitive data (such as personal information or financial records) using built-in and custom classifiers.
* **Data Lineage**: Visualises how data flows across systems, helping trace data origins, transformations, and usage.
* **Business Glossary**: Establishes a common vocabulary, ensuring consistency and clarity in data definitions across the organisation.
* **Role-Based Access Control (RBAC)**: Ensures secure access to data assets, supporting compliance with data privacy requirements.

Key capabilities of Azure Purview include automated data discovery, sensitive data classification, end-to-end data lineage, metadata management, and policy enforcement. By integrating seamlessly with other Azure services such as Azure Data Lake, Azure Synapse Analytics, and Power BI, Purview provides a holistic view of the data ecosystem, ensuring that data is findable, accessible, interoperable, and reusable (FAIR).

## Implementing Data Governance with Azure Purview

Implementing data governance with Azure Purview is a structured process that empowers organisations to manage data proactively. Below is a step-by-step approach, along with best practices:

1. **Define Governance Objectives and Scope** - Begin by identifying your organisation’s data governance goals—such as regulatory compliance, improved data quality, or enhanced data discovery. Clearly outline the scope by determining which data sources and departments will be included in your governance project.
2. **Set Up Azure Purview Account** - Provision an Azure Purview account within your Azure subscription. Assign appropriate roles and permissions to your governance, security, and data engineering teams.
3. **Register and Scan Data Sources -** Add data sources such as Azure Data Lake, SQL databases, on-premises servers, or even non-Microsoft clouds. Configure scanning schedules to automatically discover and catalogue new and existing data assets.
4. **Classify and Label Data -** Leverage Purview’s built-in classification rules or create custom classifiers to automatically tag sensitive information. This step is crucial for meeting compliance requirements and managing data risk.
5. **Establish a Business Glossary -** Collaborate with business users to create a central repository of data definitions, terms, and policies. This promotes a shared understanding of data across the enterprise.
6. **Monitor Data Lineage -** Use Purview’s data lineage visualisations to track the journey of data from source to destination. This transparency is invaluable for auditing, troubleshooting, and understanding data transformations.
7. **Implement Access Controls and Policies -** Enforce security by assigning data access roles and policies. Regularly review permissions to ensure only authorised users can access sensitive data.
8. **Continuous Improvement -** Data governance is an ongoing process. Periodically review and update your governance framework, data catalogues, and policies to adapt to evolving business needs and regulatory changes.

## Integrating Azure Purview with Other Azure Services

One of Azure Purview’s greatest strengths is its ability to integrate seamlessly with other Azure services, enhancing the overall data engineering ecosystem. Let us look at some key integration scenarios:

* **Azure Data Factory** - Integrate Azure Purview with Azure Data Factory to enable automated data discovery and lineage tracking for pipelines. This ensures data engineers always have visibility into where data is coming from, how it is transformed, and where it is going.
* **Azure Synapse Analytics -** By connecting Synapse Analytics with Purview, organisations can easily explore, query, and analyse catalogued data assets. Data lineage information provides transparency for analytics workflows, aiding in compliance and troubleshooting.
* **Power BI -** Power BI users can discover and understand data assets catalogued in Purview, ensuring that reports and dashboards are built on trusted and well-governed data. This integration promotes data democratisation across the enterprise.
* **Azure Security and Compliance Services -** Purge integrates with Azure security services to enhance compliance monitoring and risk management. Sensitive data tags and access policies can be enforced across platforms, reducing the risk of data breaches.

## Benefits of Using Azure Purview

Implementing Azure Purview brings a host of benefits to organisations seeking to strengthen their data governance practices:

* **Improved Compliance**: Automated classification and lineage tracking make it easier to meet regulatory requirements like GDPR or India’s Data Protection Bill.
* **Enhanced Data Discovery**: Centralised data catalogues empower users to find, understand, and trust data quickly, boosting productivity.
* **Collaboration Across Teams**: A shared business glossary and transparent data lineage foster better communication between business, IT, and compliance teams.
* **Reduced Data Risks**: Automated policies and access controls help safeguard sensitive information and minimise the risk of data leaks.
* **Accelerated Analytics**: With clear visibility into data assets and their origins, analytics projects can be executed faster and with greater confidence.

## Recipe: Setting Up Your Azure Purview Account

Getting started with Azure Purview, Microsoft’s unified data governance solution, is an essential step for organizations looking to manage, discover, and govern their data assets across on-premises, multi-cloud, and SaaS sources. If you’re planning to set up your Azure Purview account, this recipe will walk you through each stage—from preparing your Azure environment to the final deployment—while highlighting the critical Azure services involved along the way.

### Understanding the Building Blocks: Azure Services Required

Before diving into the recipe, it’s important to know the Azure services you’ll need to bring your Purview setup to life:

* **Azure Active Directory (Azure AD)**: Handles authentication and access control for users and applications connecting to Purview.
* **Azure Storage Account**: Provides storage for Purview’s scan results, asset metadata, and other operational data.
* **Azure Key Vault**: Securely stores secrets, keys, and credentials that Purview may need when accessing other data sources.
* **Azure Virtual Network (VNet)**: Ensures secure connectivity if you want to restrict Purview’s access within a private network.
* **Azure Monitor & Log Analytics**: Enables monitoring and logging activities for operational visibility and compliance.

### 2. Recipe Development: Step-by-Step Setup

Let’s break down the process of setting up your Azure Purview account into a series of clear steps, making it easy to follow and adapt for your needs.

### Step 1: Prepare Your Azure Environment

Begin by ensuring you have an Azure subscription with appropriate permissions—typically, you’ll need to be at least a Contributor or Owner. Make sure your organisation’s Azure Active Directory is set up, as this will manage your access to all Azure resources, including Purview.

### Step 2: Create a Resource Group

It’s a good practice to create a dedicated resource group for your Purview resources. This helps keep everything organised and makes management easier. In the Azure Portal, navigate to “Resource groups” and click “Create”. Give it a name that reflects its purpose, such as rg-purview-demo, and select your preferred region.

### Step 3: Deploy an Azure Purview Account

Now, head to the Azure Marketplace and search for “Purview”. Click “Create” and fill in the basics:

* Subscription: Select your active Azure subscription.
* Resource Group: Choose the resource group you just created.
* Name: Enter a unique name for your Purview account.
* Region: Choose the region closest to your data sources for optimal performance.

You can also configure advanced options, such as enabling managed private endpoints to tighten network security.

### Step 4: Assign Permissions Using Azure Active Directory

Once your Purview account is created, you’ll need to assign roles to users and service principals. Use Azure AD to grant “Purview Data Curator” or “Purview Data Reader” roles as appropriate. This step is crucial to ensure only authorised users can scan, label, or access data assets.

### Step 5: Connect and Register Data Sources

With the basics set up, it’s time to connect Purview to your data landscape. Use the Purview Studio (web interface) to register data sources such as Azure Data Lake Storage, SQL Databases, or even on-premises data stores. You may need to provide credentials—secure them using Azure Key Vault for best practices.

### Step 6: Set Up Scanning and Classification

Configure scan rules to schedule and automate the discovery of data assets. Purview provides built-in and custom classifiers for identifying sensitive information, such as PAN numbers or Aadhaar data, which is especially relevant in the Indian context.

### Step 7: Monitor, Audit, and Optimise

Enable Azure Monitor and Log Analytics to keep track of Purview activities, monitor usage, and audit changes. Regularly reviewing these logs helps you stay compliant and optimise your governance processes.

## 3. Bringing It All Together: How the Recipe Works

This recipe is carefully developed to ensure a seamless and secure setup for your Azure Purview account. By following these steps, you create a robust foundation for data governance:

* Start with a secure and well-organised Azure environment.
* Use Azure AD for access management, ensuring only the right people can interact with your Purview account.
* Leverage Azure Storage for storing critical metadata and scan logs.
* Protect secrets with Azure Key Vault, particularly when integrating with sensitive data sources.
* Utilise monitoring and logging tools to maintain oversight and compliance.

Setting up your Azure Purview account is more than just a technical task—it’s a strategic move towards better data management and compliance. With the right Azure services in place and a stepwise approach, you not only simplify the setup but also future-proof your data governance framework. Whether you’re working with data stored in India or globally, this recipe ensures you have a reliable and secure foundation for all your governance needs.

Lets try this recipe as below

* Navigate to the Azure Portal <https://portal/azure.com> .
* Search for “Purview” in the top search bar and select Azure Purview Accounts.
* Click + Create.
* Fill in the required fields:
* Subscription: Choose your Azure subscription.
* Resource Group: Select an existing resource group or create a new one.
* Account Name: Enter a globally unique name for your Purview account.
* Region: Choose the Azure region nearest your data sources.

Review and click Create. Deployment typically takes several minutes.

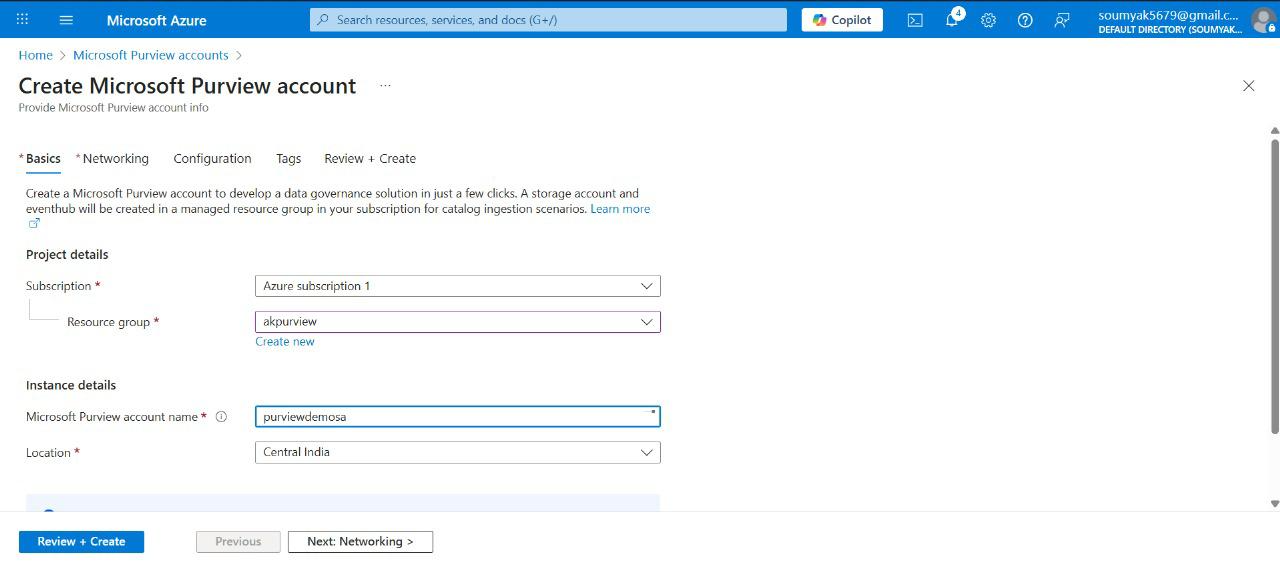


Figure: Azure Portal showing the 'Create Purview Account' form with fields highlighted.

# **Setting Up Purview Accounts**

As organisations increasingly rely on vast amounts of data to drive decision-making, the importance of efficient data governance cannot be overstated. Azure Purview, a unified data governance service from Microsoft, is designed to help enterprises discover, classify, and manage data across hybrid environments. Setting up an Azure Purview account is the first step towards establishing a robust data governance framework. This article aims to walk you through the process, clarify key concepts, and offer practical advice for a smooth setup experience.

## Understanding Azure Purview Accounts

Before diving into the setup procedure, it is essential to grasp what Azure Purview accounts are. In simple terms, an Azure Purview account acts as the central hub for all your data governance activities. It provides a workspace where you can register data sources, scan and classify datasets, manage metadata, and enforce data policies across your organisation. Each account is linked to an Azure subscription and is typically scoped to a particular region and resource group for organisational convenience.

## Prerequisites for Setting Up Azure Purview

Setting up an Azure Purview account is straightforward, but you’ll need a few things in place:

* **An active Azure subscription**: You can’t create any Azure service without this.
* **Proper permissions**: You must have the necessary rights, such as Contributor or Owner access, to create resources in Azure.
* **A resource group**: Think of this as a folder that helps organise your Azure resources logically.
* **Choice of region**: Purview accounts are region-specific, so pick a location close to your main data sources for better performance.

## Step-By-Step Guide to Creating an Azure Purview Account

1. Log in to the Azure Portal - Begin by accessing the Azure Portal with your organisational credentials. The portal is your dashboard for managing all Azure resources.
2. Search for Azure Purview - In the search bar at the top, type “Purview” and select Purview accounts from the results. This will take you to the Purview management blade.
3. Click on ‘Create’
4. Once inside the Purview section, click the ‘Create’ button to start the account setup process.
5. Fill in the Basic Details
6. Subscription: Pick the subscription where you want the Purview account to reside.
7. Resource Group: Select an existing resource group or create a new one.
8. Account Name: Choose a unique name for your Purview account. This will be used to identify the account within your organisation.
9. Region: Select the Azure region that best fits your data residency and performance needs.
10. Configure Networking (Optional) - Depending on your organisation’s security requirements, you may set up private endpoints or restrict public access. This step ensures your Purview account is accessible only from authorised networks.
11. Assign Tags (Optional) - Tags help you manage billing, organisation, and automation. You can add key-value pairs to classify the Purview account under different departments, projects, or environments.
12. Review and Create - Double-check all your entries. If everything looks good, click ‘Create’ to provision the Purview account. The deployment usually takes a few minutes.

## There are certain post-setup actions. Once your Purview account is live, you can:

* Register Data Sources: Connect your databases, data lakes, and other repositories for scanning.
* Configure scans: Set up scanning schedules to automatically discover and classify data.
* Manage users: Grant access to team members using Azure roles and permissions.
* Explore the Purview Studio: Dive into the Purview Studio, a user-friendly interface for browsing your data catalogue and managing governance tasks.

## Best Practices and Tips

* Plan your resource groups and regions carefully: This helps optimise costs and performance.
* Use tags liberally: They make it easier to track spending and manage resources as your Purview usage grows.
* Secure your account: Consider integrating Purview with Azure Active Directory for robust access control.
* Regularly review scans and classifications: Data landscapes change quickly, so periodic reviews help maintain accuracy.

Setting up Azure Purview accounts is a crucial foundation for modern data governance. By following the steps above, you can ensure your organisation is well-positioned to manage, classify, and protect its data assets. With thoughtful planning and attention to best practices, Azure Purview can become a powerful ally in your data management journey.

Azure Purview offers two main deployment options: public access and private endpoints. For enhanced security, organizations should consider configuring private endpoints to restrict access to the Purview portal and scan operations.

## Configuring Roles and Access

After deployment, assign users to appropriate roles:

* Purview Data Curator: Can create, edit, and delete assets, classifications, and glossary terms.
* Purview Data Reader: Can view assets and metadata, but cannot modify.
* Purview Data Source Administrator: Manages access to data sources and scanning credentials.

Use Azure Active Directory (AAD) groups to streamline role management and maintain principle of least privilege.

## Recipe: Connecting Data Sources

Azure Purview is Microsoft's unified data governance solution, designed to help organisations discover, classify, and manage data spread across on-premises, multi-cloud, and SaaS environments. One of the most crucial steps in leveraging Azure Purview is connecting it to various data sources, which enables Purview to scan, catalogue, and govern the enterprise data landscape efficiently. This recipe walks you through the process of connecting data sources to your Azure Purview account, detailing the Azure services involved and the development approach for this "recipe".

The aim of this recipe is to enable Azure Purview to access and scan data from different repositories—be it Azure Data Lake Storage, SQL databases, or other cloud/on-premises sources. By connecting these sources, Purview can automatically discover metadata, classify sensitive information, and provide a unified map of your organisational data assets.

## Azure Services Required for This Recipe

* Azure Purview Account: The central service for data governance and cataloguing.
* Azure Data Lake Storage Gen2: Commonly used for storing structured and unstructured data. Purview scans this for metadata.
* Azure SQL Database: Relational data source often catalogued by Purview.
* Azure Key Vault: Securely stores credentials and secrets needed for authentication when connecting Purview to data sources.
* Azure Active Directory (AAD): Handles identity and access management, ensuring secure connections.
* Integration Runtime (Self-hosted or Azure): Facilitates connectivity to on-premises and cloud data sources during scanning.

## Step-by-Step Development of the Recipe

Here’s a detailed walkthrough of how the recipe for connecting data sources to Azure Purview is developed:

1. Setting Up the Azure Purview Account - Begin by creating an Azure Purview account in the Azure portal. This account acts as the central hub for all data governance activities. During setup, you’ll configure networking options, assign roles via Azure Active Directory, and set up resource groups for better organisation.
2. Configuring Required Permissions - Next, permissions must be established. Use Azure Active Directory to assign the necessary roles—such as Data Reader or Data Source Administrator—to users and services that will interact with Purview. This ensures secure, role-based access control across all data sources.
3. Registering Data Sources - Within the Purview portal, navigate to the "Data Map" section and choose "Register" to add a new data source. Select the type of data source (e.g., Azure Data Lake Storage Gen2, SQL Database, or others) and provide the required details, such as the resource ID or connection string.
4. Setting Up Integration Runtime - For data sources located behind firewalls or on-premises, set up a Self-hosted Integration Runtime. This acts as a bridge between Purview and your data source, enabling secure and reliable scanning. For cloud-native sources, the Azure Integration Runtime is sufficient.
5. Configuring Authentication Using Azure Key Vault - To facilitate secure connections, store your credentials—such as service principal secrets or database passwords—in Azure Key Vault. When registering the data source, link Purview to these secrets. This ensures that sensitive information is not hardcoded or exposed.
6. Initiating and Customising Data Scans - With the data source registered and authentication configured, trigger a scan from the Purview portal. Define the scope (folders, tables, databases), set up scan schedules, and choose classification rules to identify sensitive or critical data. The scan fetches metadata, schema, and classification results, populating the data map.
7. Reviewing Scan Results and Managing Data Assets - Once the scan completes, Purview provides insights via its data catalogue. You can browse assets, review classifications, and manage metadata. Further governance actions—such as labelling, lineage tracking, and access control—are now enabled for the connected data.

Connecting your data sources is essential for cataloging. Here’s how:

* Within the Purview Studio, navigate to Data Map > Sources.
* Click + Register and choose your data source type (e.g., Azure Data Lake Storage, SQL Database, Amazon S3).
* Enter the connection details. For Azure sources, select from your available resources. For external sources, input the necessary URL and credentials.
* Test the connection and save.

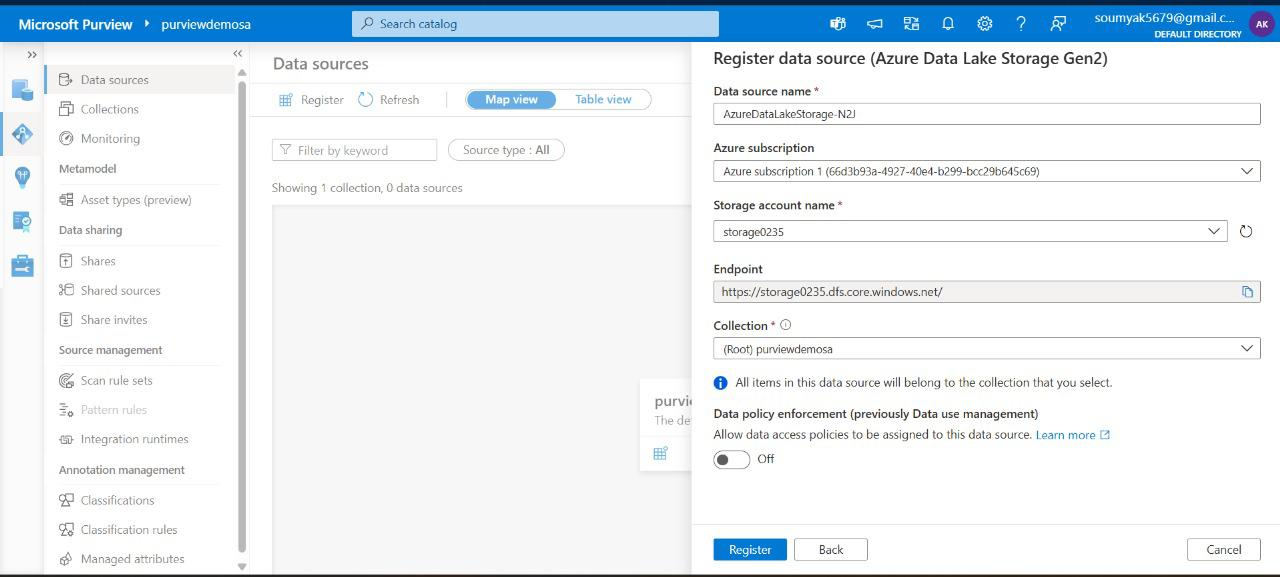


Figure: Purview Studio, 'Register Data Source' modal with options for Azure and non-Azure sources.

## Best Practices and Tips

* Always use managed identities and Key Vault to avoid exposing secrets.
* Leverage role-based access control in Azure AD for security and compliance.
* Schedule regular scans to keep your data catalogue up to date.
* Integrate Purview with other services (e.g., Azure Synapse, Power BI) for broader governance and analytics capabilities.

Connecting data sources to Azure Purview is a foundational step towards effective data governance in the cloud. By following this recipe—setting up your Purview account, configuring permissions, registering data sources, and securing authentication—you enable automated discovery and management of your organisational data. The process harnesses several Azure services in tandem, ensuring the solution is both robust and secure. This lays the groundwork for advanced governance features such as data lineage, sensitive data classification, and compliance tracking, giving you full visibility and control over your data estate.

Cataloging Data Assets

Cataloging is at the heart of data governance. Azure Purview’s data catalog provides a comprehensive inventory of all registered data assets, automatically capturing metadata, lineage, and classification details.

In today’s digital landscape, data has become the cornerstone of organisational success. Managing, understanding, and securing data assets is no longer a luxury—it’s a necessity. Cataloging data assets enables organisations to keep track of what data they possess, where it resides, and how it can be used responsibly. Microsoft Azure Purview offers a modern solution, helping IT professionals and data managers streamline this process. With Azure Purview, users can gain a holistic view of their data landscape, ensuring assets are properly organised and accessible while maintaining compliance standards.

* **Automated Data Discovery**: Purview connects to multiple data sources, scanning and cataloging assets with minimal manual intervention.
* **Data Classification**: The service uses machine learning to tag sensitive information and apply relevant policies.
* **End-to-End Data Mapping**: Purview tracks data lineage, helping users understand how data flows across systems.
* **Collaboration Tools**: It facilitates sharing, searching, and annotating data assets within teams.

## Importance of Cataloging Data Assets

Cataloging data assets is crucial for several reasons. Firstly, it enhances visibility, enabling organisations to know exactly what data they own and where it is stored. This clarity supports compliance efforts, especially with regulations like GDPR and India’s Data Protection Act. Secondly, a centralised data catalogue streamlines access, reducing duplication and inefficiency. Finally, it establishes a foundation for effective data governance, allowing teams to set policies and monitor usage with confidence.

* **Improved Compliance**: Maintain accurate records for audits and legal requirements.
* **Enhanced Security**: Identify and protect sensitive data assets.
* **Operational Efficiency**: Reduce time spent searching for data and avoid unnecessary duplication.
* **Better Decision-Making**: Ensure data is up-to-date and reliable for analytics and reporting.

## Steps to Catalog Data Assets in Azure Purview

Cataloging data assets in Azure Purview involves several well-defined steps. Each step builds upon the previous, ensuring a thorough and accurate catalogue.

1. Setting Up Azure Purview - Begin by creating an Azure Purview account within your organisation’s Azure portal. Assign necessary permissions to data stewards and IT administrators, ensuring they have access to manage and configure Purview resources.
2. Connecting Data Sources - Azure Purview supports a wide range of data sources, including Azure Data Lake, SQL databases, and SaaS platforms. Use the built-in connectors to establish secure links to your data repositories. Each connection should be authenticated and authorised, following your organisation’s security policies.
3. Scanning and Classification - Once data sources are connected, configure scanning schedules. Purview will automatically crawl through the repositories, identifying and cataloging files, tables, and other assets. The service applies classification labels, tagging sensitive information such as personal data, financial records, or intellectual property.
4. Organising Assets - After scanning, assets are catalogued within the Purview data map. Organise them using logical collections or hierarchies that reflect your organisational structure. Add descriptions, business glossary terms, and relevant metadata to make assets easy to find and understand.

## Best Practices for Effective Cataloging

* **Ensure Accuracy**: Regularly review and update asset metadata. Involve business users to validate descriptions and classifications.
* **Automate Where Possible**: Take advantage of Purview’s automated scanning and classification features. Set up recurring scans to capture changes and new assets.
* **Maintain Ongoing Management**: Data cataloging is not a one-time task. Assign ownership for data collections, and schedule periodic audits to keep the catalogue current.
* **Promote Collaboration**: Encourage teams to use Purview’s search and annotation capabilities, fostering a culture of shared data understanding.

After connecting data sources, configure scans to populate the Purview catalog:

* In Purview Studio, under Sources, select the desired data source.
* Click + New Scan and choose a scan rule set. Default rule sets are available for common sources.
* Configure authentication (managed identity or service principal).
* Set up scan triggers (manual, scheduled, or event-based).
* Run the scan and monitor progress via the dashboard.

Purview extracts technical metadata (schemas, tables, columns) and, when enabled, samples and profiles data for quality insights.

## Recipe: Scanning Data Assets

*Example using Azure SDK (Python):*

*from azure.purview.catalog import PurviewCatalogClient*

*from azure.identity import DefaultAzureCredential*

*client = PurviewCatalogClient(*

*endpoint="https:// .purview.azure.com",*

*credential=DefaultAzureCredential()*

*)*

*scan\_payload = {*

*"scanRulesetName": "AzureSQLDatabase",*

*"scanTriggerType": "Manual"*

*}*

*response = client.scans.begin\_create\_or\_update(*

*resource\_name="AzureSQLDatabase",*

*scan\_name="DailyScan",*

*body=scan\_payload*

*)*

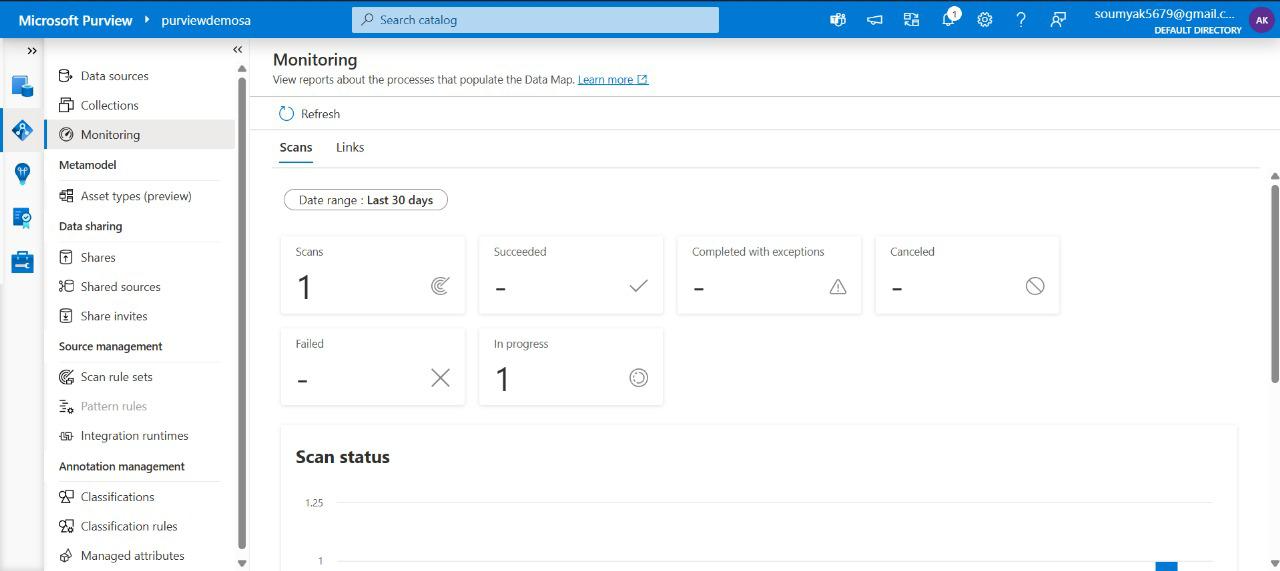


Figure: Purview Studio 'Scan Management' panel showing active and completed scans.

### Challenges and Solutions

Cataloging data assets, especially in large organisations, can present challenges. Data silos, inconsistent metadata, and rapidly changing environments are common obstacles. To overcome these, prioritise integration with all relevant data sources and establish clear metadata standards. Use Purview’s automation to reduce manual effort, and foster cross-team communication to ensure catalogued assets remain relevant and accurate.

* **Challenge**: Incomplete data coverage

**Solution**: Perform regular scans and integrate new sources as they come online.

* **Challenge**: Metadata inconsistencies

**Solution**: Define organisation-wide metadata standards and review asset annotations periodically.

* **Challenge**: Resistance to adoption

**Solution**: Demonstrate the value of cataloging through training sessions and success stories.

Cataloging data assets in Microsoft Azure Purview is a strategic step towards robust data governance and compliance. By following a systematic process—setting up Purview, connecting sources, scanning, and organising assets—IT professionals and data managers can ensure their organisations gain maximum value from their data. Adhering to best practices and addressing challenges proactively will lead to a well-maintained, reliable data catalogue, empowering teams to make informed decisions and maintain regulatory compliance. Leverage Azure Purview to transform your data management journey and unlock new potential within your organisation.

## Classifying and Tagging Data

In today’s digital landscape, businesses are inundated with massive volumes of data pouring in from a variety of sources—be it transactions, customer interactions, or operational systems. Effectively managing, organising, and securing this data has become paramount. Microsoft Azure Purview steps in as a comprehensive data governance solution, empowering organisations to discover, classify, and tag their data efficiently. Let us delve into how you can leverage Azure Purview to classify and tag data, ensuring compliance, security, and better data utilisation.

Azure Purview is a unified data governance service from Microsoft designed to help organisations map, catalogue, and manage their data estate across on-premises, multi-cloud, and SaaS sources. It enables businesses to gain a holistic view of their data, set up effective governance policies, and most importantly, classify and tag data for improved discoverability and compliance.

## Understanding Data Classification

Data classification is the process of categorising data according to its sensitivity, type, or relevance. For instance, sensitive information like financial records, health data, or personal identifiers needs to be handled with the utmost care. By classifying data, organisations can enforce appropriate security measures, streamline access controls, and meet regulatory requirements such as GDPR or India’s Data Protection Bill.

## The Role of Tagging in Data Management

Tagging, in the context of data management, refers to assigning descriptive labels or “tags” to datasets. These tags help in categorising and identifying data, making it easier for users to search for, filter, and manage information. Tags could represent data owner, sensitivity level, department, project, or any other relevant attribute.

# How Azure Purview Enables Data Classification and Tagging

## 1. Automated Data Discovery and Scanning

Azure Purview comes equipped with robust scanning capabilities. It can connect to various data sources, both on-premises and in the cloud, and automatically scan metadata and content. During this scanning process, Purview uses built-in and custom classifiers to identify data types—such as credit card numbers, Aadhaar numbers, email addresses, or proprietary business information.

## 2. Applying Data Classifications

Once the data is scanned, Azure Purview applies data classifications based on predefined or custom rules. For example, it can automatically detect columns containing sensitive information and label them as “Confidential” or “Personally Identifiable Information (PII)”. Users can also define their own classification rules to suit specific organisational needs.

## 3. Tagging Data Assets

After classification, users can further enrich datasets by tagging them with business-relevant information. For instance, you can assign tags like “Finance”, “HR”, “Customer Data”, or “Project ABC”. These tags facilitate data discovery, making it easier for business users to search for and find the right datasets using familiar business terminology.

## 4. Custom Classifications and Tags

Azure Purview doesn’t restrict you to default settings. Organisations can create custom classifiers and define unique tags matching their industry or internal requirements. This flexibility ensures your data governance framework is finely tuned to your business context.

## 5. Data Lineage and Impact Analysis

Purview also tracks data lineage—essentially, the journey data takes from its origin to its endpoint. When data is classified and tagged, lineage information helps you understand how sensitive data flows across systems and who accesses it. This is invaluable for compliance audits and impact analysis when changes occur in your data processes.

# Benefits of Classifying and Tagging Data with Azure Purview

* **Improved Data Visibility**: Classification and tagging make it easier to locate, understand, and utilise data across your organisation.
* **Enhanced Security and Compliance**: Sensitive data is clearly identified, allowing for stronger access controls and compliance with regulations.
* **Streamlined Data Governance**: Automated processes reduce manual labour and ensure consistency in how data is classified and managed.
* **Better Collaboration**: Tags make it simpler for different teams—IT, compliance, business analysts—to communicate about and find relevant data.

Automated classification detects sensitive data types (e.g., PII, financial data) during scans. You can also create custom classifications and apply them via rules or manually.

## Recipe: Classifying Data

Data classification is an essential process for organisations that wish to manage their information assets effectively. By categorising data based on its sensitivity, importance, and compliance requirements, businesses can ensure proper data governance and security. Azure Purview is a cloud-based data governance solution from Microsoft that helps enterprises discover, classify, and manage their data estate, whether on-premises, in the cloud, or across hybrid environments.

### Overview of Azure Purview and Purview Studio: Key Features and Benefits

Azure Purview offers a unified data governance service that allows organisations to map, catalogue, and manage their data assets. At the heart of this solution is Purview Studio, the web-based interface that simplifies interaction with Purview’s capabilities. With Purview Studio, users can:

* Register and scan data sources across various environments.
* Discover, classify, and label data automatically or manually.
* View data lineage and track the flow of information through business processes.
* Establish and enforce data governance policies and compliance standards.
* Enable secure access and sharing of data across teams and departments.

By leveraging these features, organisations can gain valuable insights into their data, minimise risks, and comply with regulatory requirements.

### Azure Services Required: List and Role of Each Service in the Recipe

Before beginning the data classification process, it is crucial to understand the Azure services involved:

* **Azure Purview Account**: The central service for data governance, where all classification activities occur.
* **Azure Data Lake Storage (ADLS)**: Acts as a repository for storing structured and unstructured data, which Purview scans and classifies.
* **Azure Active Directory (AAD)**: Manages user identities and access permissions for secure operations within Purview Studio.
* **Integration Runtime**: Facilitates connectivity between Purview and data sources, especially for on-premises and hybrid environments.

These services work together to provide a secure, scalable, and efficient platform for data classification and governance.

# Developing the Recipe: Step-by-Step Guide to Data Classification in Azure Purview

1. Provision the Azure Purview Account - Begin by creating an Azure Purview account through the Azure portal. Assign appropriate roles to users via Azure Active Directory to ensure only authorised personnel can access sensitive data.
2. Set Up Data Sources - Register your data sources, such as Azure Data Lake Storage or SQL databases, within Purview Studio. This involves specifying connection details and configuring authentication using Azure Active Directory.
3. Configure Integration Runtime - If your data sources reside on-premises or in a different cloud, set up an Integration Runtime to allow Purview to connect and scan these sources securely.
4. Scan Data Assets - Initiate a scan of your registered data sources from within Purview Studio. Define the scope, schedule, and frequency of scans based on your organisational needs.
5. Apply Classification Rules - Use Purview’s built-in classifiers or create custom classification rules to identify sensitive data, such as personal information or financial records. These rules can be configured to detect specific data patterns or keywords.
6. Review and Refine Classifications - After the scan, review the results in Purview Studio. Manually adjust or validate classifications as needed to ensure accuracy and completeness.
7. Label and Tag Data Assets - Assign labels and tags to classified data for easier search, access control, and compliance tracking. This step helps in categorising data according to business needs.
8. Establish Data Governance Policies - Define and enforce data access, retention, and compliance policies using Purview’s policy management features. Monitor policy adherence through Purview Studio’s dashboards and reports.

Now, lets get into the steps for data classification in Purview studio using following steps.

* In Purview Studio, go to Classification Rules.
* Click + New Classification to define a custom rule (e.g., “Internal Confidential”).
* Associate the classification with specific patterns or column names.
* Re-scan assets to apply the new classification automatically.

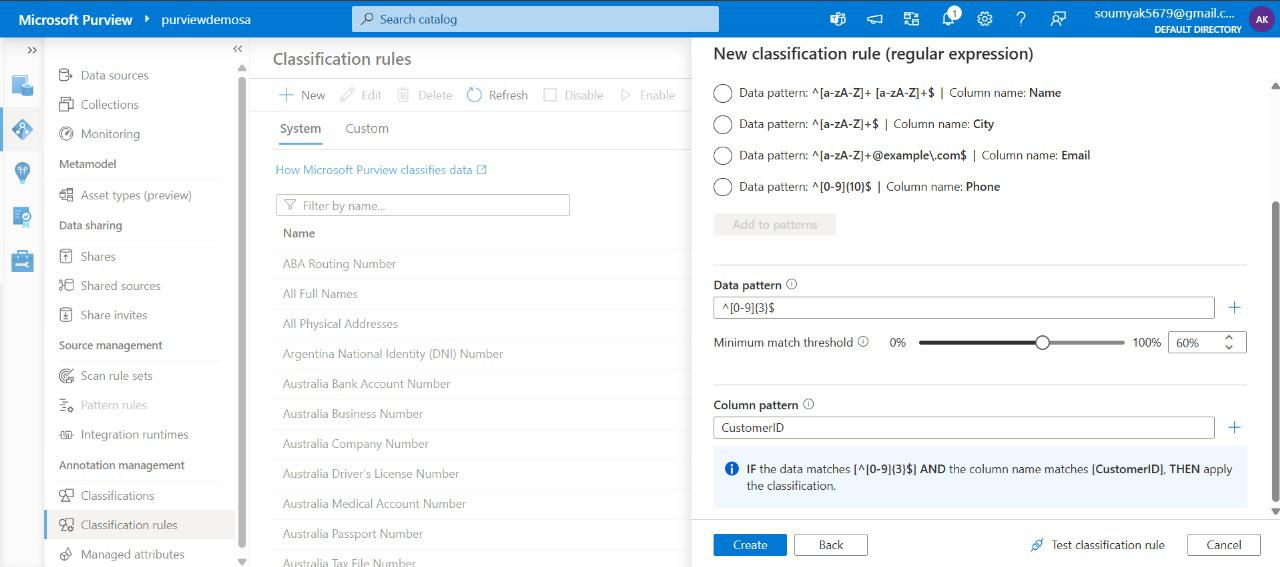


Figure: Custom classification rule editor and resulting asset tags in the catalog.

## Managing Metadata

In today’s digital era, businesses are inundated with data coming from countless sources—databases, data lakes, cloud services, and more. To turn this sea of information into something truly valuable, organisations must not only store and process data efficiently but also manage its metadata effectively. This is where Azure Purview steps in, acting as a comprehensive data governance solution from Microsoft, designed to help enterprises discover, classify, and manage their data assets.

## Importance of Metadata management

At its core, metadata is simply “data about data”. It tells you the who, what, where, when, and how about your actual data. For example, a customer database’s metadata might include information about when it was last updated, who owns it, what kind of data it holds, and where it lives. Managing this metadata is crucial for data governance, data compliance, security, and ensuring your teams can easily find and use the right data for their needs.

Azure Purview is Microsoft’s unified data governance service designed to help you map, catalogue, and manage your entire data estate—whether it resides on-premises, in the cloud, or in hybrid environments. It offers a centralised platform to automatically scan and classify data sources, build an up-to-date data catalogue, and enforce data governance policies. With Purview, you can break down data silos, improve data discovery, and ensure that your organisation’s data assets are being used responsibly and effectively.

## Key Features for Managing Metadata in Azure Purview

* **Automated Data Scanning and Discovery** - Azure Purview can connect to a wide range of data sources—Azure SQL, Blob Storage, Data Lake, Power BI, and more. It automatically scans these sources to extract metadata, making it easier to keep your data catalogue current without manual effort.
* **Unified Data Catalogue** - All discovered metadata is organised into a searchable, browsable data catalogue. Users can easily find data assets, see their lineage, and understand how they’re related to other assets across the organisation.
* **Data Classification and Labelling -** Purview leverages built-in and custom classification rules to tag sensitive data—like personal information or financial records—helping you meet compliance requirements such as GDPR or India’s Data Protection Bill.
* **Data Lineage Visualisation** - Understanding where data originates and how it flows through your systems is vital. Purview maps out data lineage, offering visual representations of how data moves from source to destination, and through various transformations along the way.
* **Role-Based Access and Collaboration -** Purview allows you to assign roles and permissions, ensuring that only authorised users can access or modify metadata. This enhances data security while promoting collaboration among data stewards, analysts, and engineers.

Metadata management is performed through glossary terms, asset descriptions, tags, and relationships. Data stewards can enrich the catalog, making data assets more searchable and meaningful.

## Recipe: Managing Metadata

* Navigate to Glossary in Purview Studio.
* Create business terms and definitions.
* Link terms to relevant assets for consistent business context.
* Edit asset descriptions and assign tags as needed.

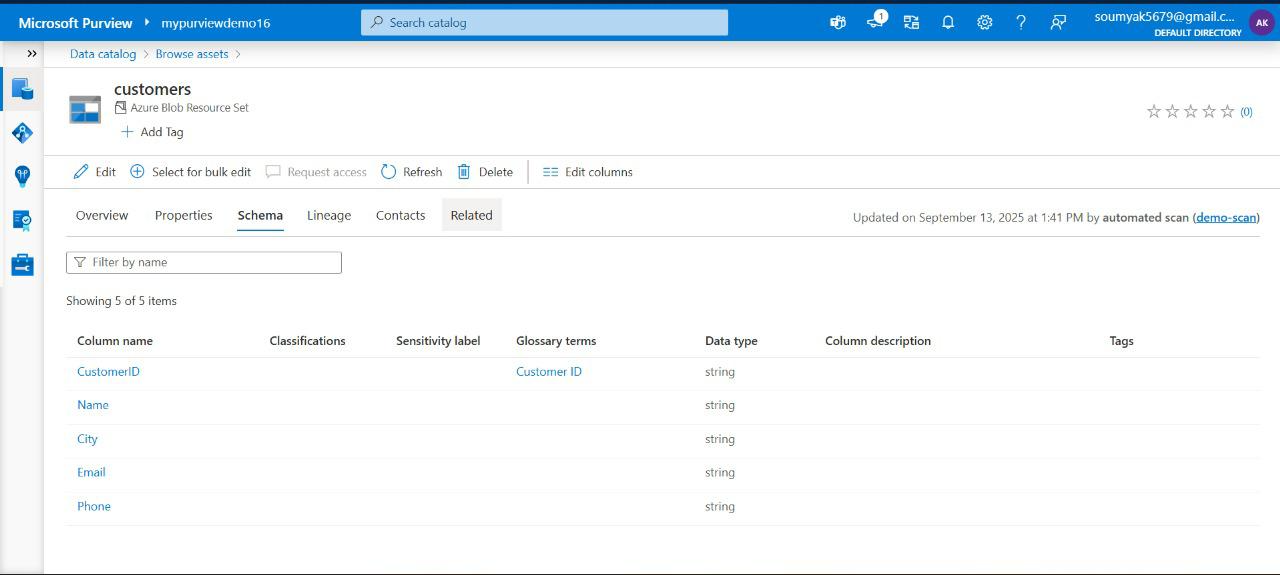


Figure: Glossary term management interface and asset detail page showing linked terms.

# Please keep following tips while handling Data classification with Purview studio.

1. **Define Clear Classification Policies**: Establish what constitutes sensitive, confidential, or public data within your organisation.
2. **Engage Stakeholders**: Involve business units, IT, and compliance teams to create meaningful classifications and tags.
3. **Automate Where Possible**: Leverage Purview’s automated classification and tagging features to handle large volumes of data consistently.
4. **Review and Update Regularly**: As your data landscape evolves, periodically review your classification schemes and tags for relevance.
5. **Train Your Teams**: Ensure staff are aware of classification policies and understand the importance of proper tagging.

Microsoft Azure Purview stands out as a powerful platform for classifying and tagging data, bringing clarity and control to even the most complex data estates. By automating discovery, classification, and tagging, it enables organisations to maintain data security, support compliance, and unlock the true value of their data assets. Embracing these capabilities not only future-proofs your data governance efforts but also fosters a culture of responsible data management in the digital age.

## Simplifying Metadata Management

Managing metadata used to be a laborious, manual process involving spreadsheets and scattered documentation. Azure Purview automates much of this work, making it easier to stay organised and compliant. By continuously scanning your environment, Purview ensures your metadata stays up to date, even as data sources evolve. Its intuitive interface means you don’t need to be a data expert to find what you need; anyone across the organisation can search for data assets, view their details, and understand how they’re being used.

## Best Practices for Using Azure Purview

1. **Automate Regular Scans**: Schedule periodic scans for all your data sources to ensure your metadata catalogue remains current.
2. **Define Clear Classification Rules**: Tailor Purview’s classification engine to match your industry’s compliance needs and your organisation’s policies.
3. **Encourage Collaboration**: Involve business users, data stewards, and IT teams in using and curating the data catalogue for richer metadata and better data utilisation.
4. **Monitor Data Lineage**: Regularly review lineage maps to track data flows, dependencies, and impact analysis for changes.
5. **Enforce Role-Based Access**: Set up access controls to protect sensitive metadata and ensure compliance with data privacy regulations.

## Real-World Applications

From large IT firms in Bengaluru to financial institutions in Mumbai, Indian organisations are embracing Azure Purview to streamline data governance. Whether it’s cataloguing data across hybrid cloud environments, classifying sensitive customer information for compliance, or enabling self-service data discovery for analysts, Purview is helping teams unlock value from data while minimising risks.

Managing metadata has never been more critical—or more manageable—than with solutions like Azure Purview. By automating discovery, classification, and catalogue creation, Purview empowers organisations to take control of their data assets, stay compliant, and foster a culture of responsible data use. As the data landscape grows more complex, investing in robust metadata management tools is not just smart; it’s essential for any business looking to thrive in the digital age.

Classifying data in Azure Purview using Purview Studio is a structured process that empowers organisations to manage their data assets effectively and securely. By following the step-by-step approach outlined above, IT professionals and data engineers can confidently implement a robust data classification strategy. To further enhance data governance, consider exploring advanced Purview features, integrating with other Azure services, and staying informed about best practices in data management. With Azure Purview, you are well-equipped to meet both current and future data governance challenges.

## Building a Data Catalog

The data catalog is automatically built as assets are scanned and classified. Users can search, filter, and view detailed metadata—including ownership, lineage, and classification—across all registered sources.

Organisations are collecting vast amounts of information from various sources. As this data grows in volume and complexity, locating, managing, and making sense of it becomes challenging. This is where a data catalog comes into the picture. A data catalog helps you organise, discover, and govern your data assets efficiently. Among the many tools available, Azure Purview stands out as a modern, cloud-based data governance solution from Microsoft.

## Looking into the importance of Data Catalog

A data catalog is like a library catalogue for your data assets. It helps users discover, understand, and trust the data available within the organisation. By providing metadata, business context, and data lineage, a data catalog ensures that anyone looking for information can easily find the right dataset, know its source, and assess its reliability. Azure Purview also integrates seamlessly with other Azure services, providing a holistic approach to data governance.

## Key Features of Azure Purview

* **Automated Data Discovery**: Purview scans and automatically catalogues data assets from a wide range of sources, including Azure Data Lake, SQL Server, Power BI, and many more.
* **Data Classification**: The tool uses built-in and custom classifiers to tag sensitive and critical information, aiding in compliance and risk management.
* **Data Lineage**: Track data movement and transformations across your systems, giving you a clear picture of data flow and dependencies.
* **Business Glossary**: Build a common vocabulary for your organisation, ensuring everyone speaks the same language when it comes to data.
* **Search and Discovery**: Purview’s intuitive interface allows users to quickly search for and find the datasets they need, complete with metadata and descriptions.

## Step-by-Step Guide to Building a Data Catalog with Azure Purview

### 1. Setting Up Azure Purview Account

Begin by creating an Azure Purview account through the Azure portal. Assign appropriate permissions to your team members—typically, you’ll want to designate collection admins and data curators. Ensure your environment meets the prerequisites, such as having the necessary subscription and network configuration.

### 2. Connecting Data Sources

Azure Purview supports a wide range of data sources, from Azure-native data stores (like Azure Data Lake, Azure SQL Database) to on-premises databases and even SaaS platforms. Set up connections to these sources by providing credentials and specifying scanning rules. These connections lay the foundation for automated data discovery.

### 3. Scanning and Cataloguing Data

Once your sources are connected, configure scan rules to determine how frequently Azure Purview should scan your data. The tool will automatically extract metadata, classify sensitive information, and build a comprehensive inventory of your data assets. You can customise these scans to focus on specific folders, databases, or tables as needed.

### 4. Enriching Metadata and Business Glossary

After the initial scan, your data catalog will contain rich technical metadata. To make it truly useful, involve business users and data stewards to add business context—such as definitions, owners, and usage guidelines—using Purview’s business glossary feature. This step ensures that the catalog is not just technically accurate, but also meaningful to end users.

### 5. Managing Data Lineage

Azure Purview tracks data lineage, helping you visualise how data moves and transforms within your ecosystem. This feature is invaluable for troubleshooting data issues, understanding dependencies, and demonstrating compliance with data governance policies.

### 6. Setting Up Security and Access Controls

Data security is paramount. Azure Purview enables you to manage permissions at various levels—collections, assets, or even specific metadata fields. Ensure that only authorised users can view or modify sensitive information within your catalog.

### 7. Enabling Data Discovery and Self-Service Analytics

With your catalog in place, business analysts and data scientists can use Azure Purview’s search and filter capabilities to quickly find relevant datasets. This self-service approach reduces bottlenecks and empowers users to make data-driven decisions.

## Recipe: Building a Data Catalog

Organisations are inundated with information coming from a multitude of sources. Making sense of this data, ensuring it is well-organised, discoverable, and governed properly, is crucial for business success. This is where a data catalog comes in. Building a data catalog using Azure Purview helps organisations create a single, centralised inventory of all their data assets, whether on-premises, in the cloud, or across hybrid environments. In this recipe, we’ll walk through the process of developing a robust data catalog using Azure Purview, highlighting the essential Azure services involved, and outlining each step in a clear and detailed manner.

Azure Purview is Microsoft’s unified data governance solution. It helps organisations discover, classify, catalogue, and manage their data assets across various environments, ensuring data is easy to find, secure, and compliant. With Azure Purview, you can automate the discovery of data sources, build a comprehensive catalog, and set up policies for data governance.

## Azure Services Needed for This Recipe

1. Azure Purview Account: The core service for data cataloguing and governance.
2. Azure Data Lake Storage (ADLS) Gen2: Storage account for hosting data assets and storing Purview metadata.
3. Azure Active Directory (AAD): For user authentication and role-based access control.
4. Azure Key Vault: To securely manage credentials and secrets required for connecting to data sources.
5. Azure Synapse Analytics (optional): For integrating advanced analytics, if you want to extend cataloguing to Synapse workspaces.
6. Azure SQL Database, SQL Server, or other supported data sources: Sources to be registered and scanned in the catalog.

## Step-by-Step Recipe: Building a Data Catalog with Azure Purview

### Step 1: Set Up Azure Purview Account

Begin by creating an Azure Purview account in your Azure portal. This involves specifying the subscription, resource group, region, and the name for your Purview account. The account acts as the central management plane for your data catalog.

### Step 2: Configure Access and Permissions

Leverage Azure Active Directory to manage access to the Purview account. Assign users and groups to roles such as Data Reader, Data Curator, or Data Source Administrator, depending on their responsibilities. This ensures that only authorised personnel can access or modify catalog information.

### Step 3: Register Data Sources

Next, register the data sources you wish to catalogue. Azure Purview supports a wide range of sources, including Azure Data Lake, SQL databases, on-premises servers, and more. Registration establishes a connection between Purview and each source, laying the groundwork for automated scanning.

### Step 4: Set Up Scanning and Classification

Configure scan rules in Purview to automatically scan registered data sources. Scanning helps discover all datasets, tables, files, and other assets present in the sources. During this phase, Purview’s built-in classifiers can automatically tag sensitive data such as PAN, Aadhaar, or other PII, helping with compliance and governance.

### Step 5: Build and Customise the Data Catalog

Once scans are complete, Purview ingests metadata into its catalog. You can then enrich this metadata by adding business glossary terms, custom classifications, and descriptions to make assets more meaningful and easier to find. This step is crucial for building a catalog that resonates with your organisation’s unique business language.

### Step 6: Enable Data Search and Discovery

Azure Purview offers a friendly web portal where users can search for data assets using keywords, filters, or business glossary terms. This empowers data analysts, scientists, and business users to quickly locate the data they need, understand its lineage, and assess its quality and relevance.

### Step 7: Set Up Data Governance Policies

To ensure data is handled responsibly, configure governance policies in Purview. These might include access policies, data retention rules, and sensitivity labels. Integrating Azure Key Vault at this stage ensures that credentials for connecting to sensitive sources are managed securely.

### Step 8: Monitor, Maintain, and Expand

With your catalog in place, monitor usage patterns and scan results regularly. Azure Purview provides dashboards and reports for ongoing insights. As your data landscape evolves, continue registering new sources, updating the business glossary, and refining policies to keep the catalog current and valuable.

Lets try these steps in implementing data catalog solution as below:

* Register multiple sources and run comprehensive scans.
* Enrich assets with business glossary.
* Promote frequently used datasets as “certified” or “endorsed.”
* Encourage stakeholder adoption for catalog accuracy and completeness.

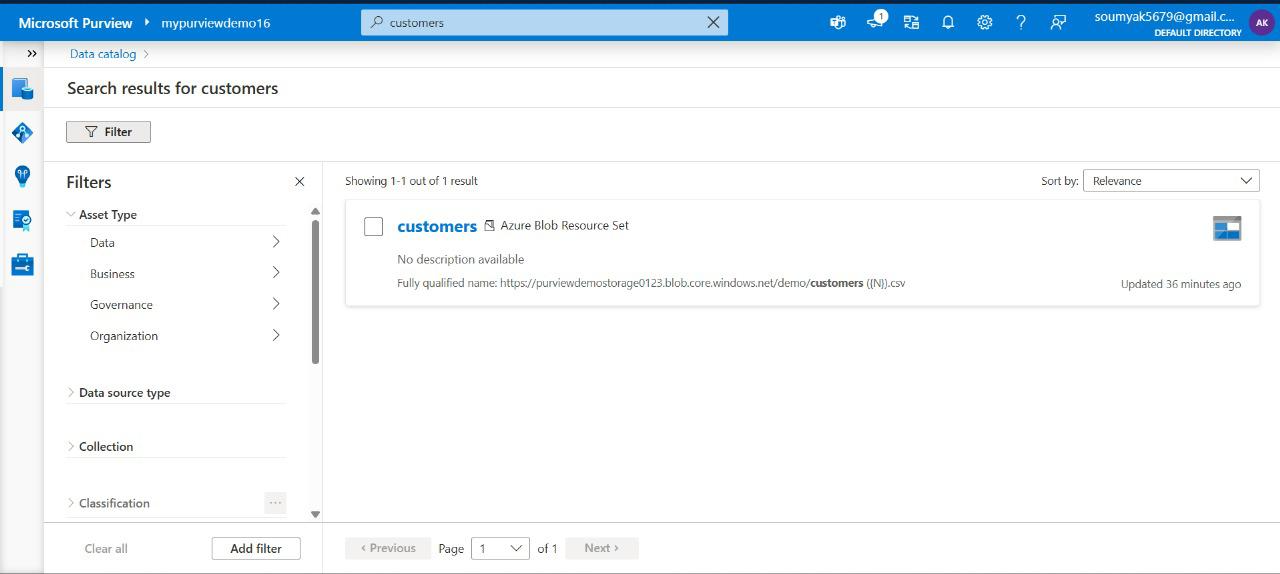


Figure: Catalog search interface with facets for data type, source, classification, and owner.

## Data Lineage and Impact Analysis

Tracking the movement of data through various transformations is critical for governance, troubleshooting, and compliance. Azure Purview captures lineage at the asset, column, and process levels.

## Recipe: Data Lineage and Impact Analysis

In today’s fast-paced digital world, organisations are generating and handling massive volumes of data every single day. As data continues to expand in both complexity and scale, understanding where it comes from, how it moves through systems, and how changes can ripple through the ecosystem becomes crucial. This is where data lineage and impact analysis step in, and with tools like Azure Purview, businesses have never been better equipped to gain clarity and control over their data assets.

## Introducing Data Lineage

Data lineage is like a map tracing the entire journey of your data—from its original source, through the various transformations and touchpoints, right up until it lands in its final destination, such as a dashboard or report. Imagine being able to follow a piece of information as it weaves its way through your databases, ETL processes, and business intelligence tools. With data lineage, you get a transparent, end-to-end view of this journey, which is essential for ensuring data quality, compliance, and overall trust in your analytics.

## Understanding Impact Analysis

Impact analysis, on the other hand, is all about foresight. It’s the process of assessing what happens if you make a change to a dataset, a column, or a process. If you alter a calculation, retire a table, or update a field, impact analysis helps you predict which reports, dashboards, or downstream systems will be affected. This means fewer surprises, less risk, and more confidence when implementing changes across your data landscape.

Azure Purview is Microsoft’s unified data governance solution designed to help organisations manage, discover, and understand their data across on-premises, multi-cloud, and software-as-a-service (SaaS) environments. At its core, Purview helps you catalogue data, enforce data governance policies, and—crucially—visualise data lineage and carry out impact analysis with ease.

## Azure Purview Empowering Data Lineage

With Azure Purview, data lineage isn’t just static documentation—it’s dynamic, interactive, and automatically updated as your systems evolve. Here’s how Purview makes data lineage practical and powerful:

* **Automated Lineage Capture**: Purview can automatically scan and capture lineage information from a wide range of sources, including Azure Data Factory pipelines, SQL databases, Power BI datasets, and more.
* **Visual Lineage Diagrams**: It provides intuitive diagrams that let users see how data flows from source to destination, including every transformation step along the way.
* **Custom Lineage Integration**: For unique or custom data sources, Purview allows users to manually input lineage information or integrate via APIs.
* **End-to-End Visibility**: Whether your data lives in Azure, on-premises, or third-party clouds, Purview can provide a holistic view of its journey.

## Impact Analysis with Azure Purview

When it comes to impact analysis, Azure Purview shines by letting users trace dependencies and relationships across datasets, tables, columns, and reports. A few standout features include:

* **Downstream Impact Visualisation**: Instantly see which assets or reports depend on a given data element, helping you anticipate the effects of any planned changes.
* **Upstream Traceability**: Understand where your data is coming from and which processes contribute to its creation, aiding in root-cause analysis and troubleshooting.
* **Change Management Support**: By providing clear insights into data dependencies, Purview reduces the risk of unintended consequences during system upgrades or migrations.

## Impact Analysis with Data Lineage

For any enterprise, the benefits of effective data lineage and impact analysis are significant:

* **Regulatory Compliance**: With stricter regulations like GDPR and India’s Data Protection Bill, being able to demonstrate where data comes from and how it is used is no longer optional.
* **Data Quality Assurance**: By tracing data flows, organisations can pinpoint and resolve quality issues more quickly.
* **Efficient Troubleshooting**: When something goes wrong, lineage and impact analysis help IT teams isolate problems and resolve them with minimal disruption.
* **Improved Collaboration**: Clear visibility into how data moves and changes encourages better communication between business and technical teams.

Lets try this recipe by following these steps

* Enable lineage extraction during scans for supported sources (e.g., Azure Data Factory, Synapse).
* View lineage diagrams in Purview Studio from an asset’s detail page.
* Use lineage view to trace upstream and downstream dependencies, identifying the potential impact of changes.

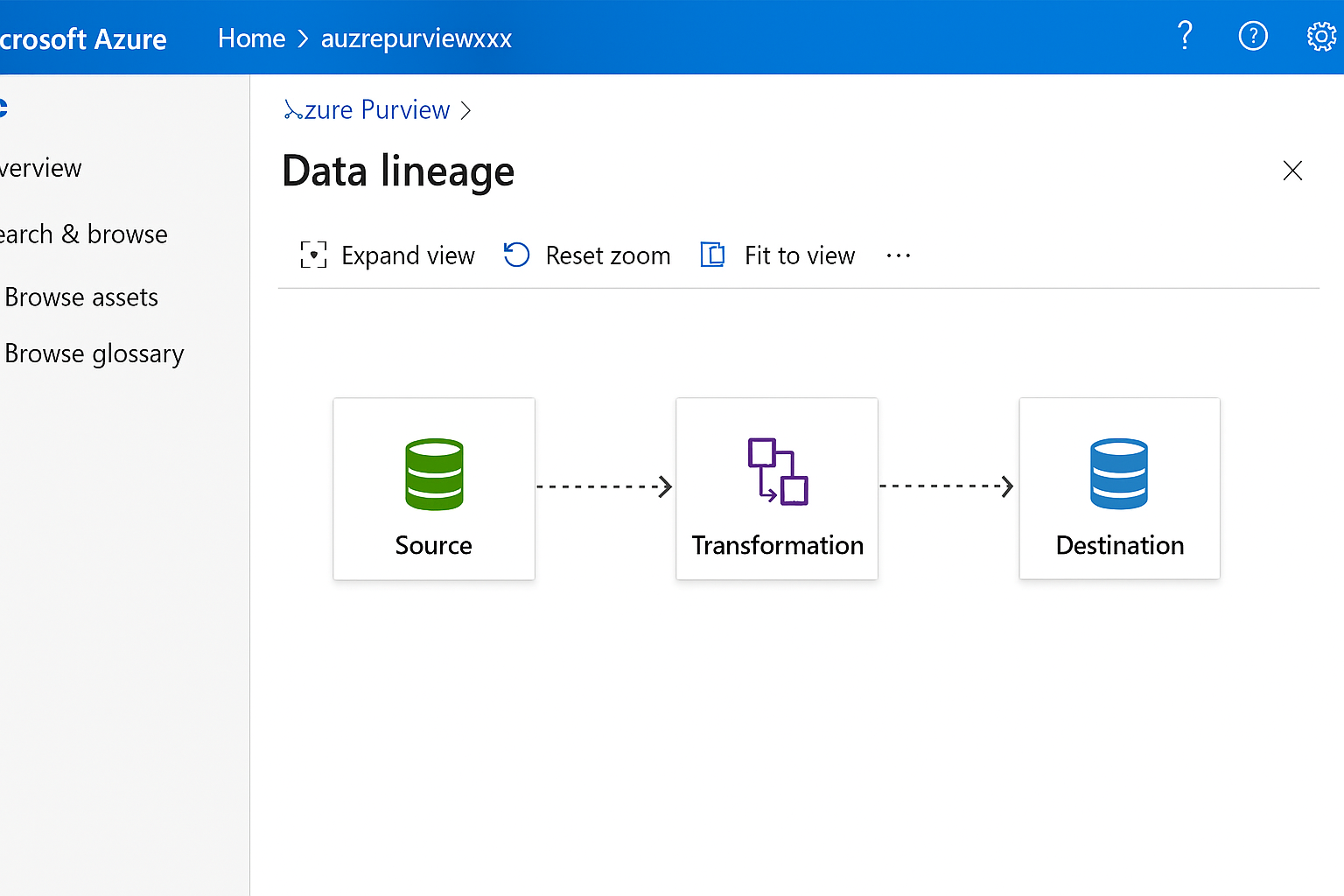


Figure: Data lineage visualization showing source, transformation, and destination nodes.

## Best Practices for a Successful Data Catalog Implementation

* **Engage Stakeholders Early**: Involve business users, IT, and data stewards from the start to ensure the catalog meets everyone’s needs.
* **Keep Metadata Updated**: Schedule regular scans and encourage users to update asset information as your data landscape evolves.
* **Promote Data Literacy**: Offer training and resources to help your teams make the most of the data catalog.
* **Monitor Usage**: Use Azure Purview’s analytics to track catalog adoption and identify areas for improvement.
* **Integrate with Other Tools**: Connect Purview with Azure Synapse, Power BI, and other analytics platforms to maximise value.

Building a data catalog with Azure Purview is a strategic move for organisations looking to harness the full potential of their data. By providing automated discovery, robust governance, and an intuitive user experience, Purview helps break down data silos and fosters a culture of data-driven decision making. Whether you’re just starting out or looking to enhance your existing data governance framework, Azure Purview offers the tools needed to manage and make sense of your data assets in a secure and scalable way.

Building a data catalog using Azure Purview isn’t just about technology—it’s about empowering your organisation to discover, understand, and govern its data assets confidently. By following the steps outlined above and leveraging key Azure services, you can establish a centralised, secure, and scalable data catalog that supports both compliance and innovation.

If you’re just starting out, remember—begin with a pilot involving your most critical data sources, gather feedback from users, and iterate as you expand. With Azure Purview, the journey to data governance is both streamlined and flexible, making it an excellent fit for the diverse needs of modern Indian enterprises.

Adopting Azure Purview is straightforward, especially for organisations already using the Azure ecosystem. The platform provides guided onboarding, automated scans, and integration with popular tools like Power BI, Azure Synapse, and SQL Server. Here’s a suggested approach:

1. Register your data sources and configure scanning schedules.
2. Leverage automated and custom lineage capture to build your data map.
3. Use Purview’s visual tools to explore lineage and carry out impact analysis.
4. Establish governance policies and collaborate with data owners to keep your data estate healthy and compliant.

In a world where data drives decisions, having a clear understanding of how information flows and how changes propagate is invaluable. Azure Purview empowers organisations to see the bigger picture, confidently manage change, and ensure that their data assets deliver real business value. By making data lineage and impact analysis accessible and actionable, Purview helps you transform data chaos into data clarity.

Managing Data Policies

Data policies enforce access restrictions and usage rules across your data landscape. Purview’s policy management integrates with Azure RBAC and supports centralized policy definitions.

Large organisations handling high volume of data (both internal and client facing data) face mounting pressure to manage their data responsibly. As data volumes surge and regulations tighten, ensuring data is secure, private, and well-managed has become paramount. Data governance is the discipline that brings structure, accountability, and oversight to an organisation’s data assets. Within this context, Azure Purview emerges as a powerful solution, enabling organisations to implement robust data policies and streamline governance activities.

## Understanding Data Policies

Data policies are formal guidelines that dictate how data is accessed, used, shared, and protected within an organisation. These policies help set expectations, standardise practices, and reduce risks associated with data misuse. For organisations, effective data policies are essential for meeting regulatory requirements, protecting sensitive information, and fostering trust among stakeholders. By clearly defining roles and responsibilities, data policies lay the groundwork for a culture of accountability and transparency.

## Key Features for Managing Data Policies

Azure Purview is Microsoft’s unified data governance service that enables organisations to discover, classify, and manage their data estate, whether on-premises, in the cloud, or in hybrid environments. Some of the standout features that help manage data policies include:

* **Automated Data Discovery**: Azure Purview scans and catalogues data across diverse sources, providing a centralised, up-to-date inventory.
* **Data Classification and Labelling**: It automatically tags data based on sensitivity, usage, and custom business definitions, supporting consistent policy application.
* **Policy Authoring and Assignment**: Users can define, apply, and manage access and usage policies directly within the platform.
* **Data Lineage Tracking**: Purview maps the journey of data from source to destination, offering transparency and simplifying compliance audits.
* **Integration with Security Tools**: Seamless connectivity with Azure Active Directory and other security solutions ensures that policies are enforced organisation-wide.

## Safeguarding Sensitive Information

Protecting sensitive information is a cornerstone of any data governance strategy. Azure Purview strengthens data security through:

* **Access Controls**: By assigning role-based access and usage policies, Purview ensures that only authorised users can view or manipulate sensitive data.
* **Classification-Based Protections**: Automatically classified data can trigger specific security measures such as encryption or additional authentication requirements.
* **Continuous Monitoring**: Real-time monitoring and alerts help detect unusual access patterns, enabling rapid response to potential breaches.

Through these mechanisms, Azure Purview reduces the risk of data leaks and unauthorised access, helping organisations maintain a strong security posture.

## Tools and Processes for Compliance to ensure Data privacy

With privacy regulations like GDPR and India’s Personal Data Protection Bill shaping the data landscape, compliance is no longer optional. Azure Purview supports data privacy by:

* **Identifying and Tracking Personal Data**: Automated classification highlights personal and sensitive information, supporting privacy impact assessments.
* **Managing Data Subject Requests**: Clear data lineage allows organisations to efficiently locate and act on requests for data access, correction, or deletion.
* **Policy-Driven Data Masking**: Purview can enforce data masking policies, ensuring that personal information is only visible to those with a legitimate need.

These tools enable organisations to demonstrate accountability and meet regulatory obligations with greater ease.

## Organising and Controlling Data Assets for effective data management

Efficient data management is about more than just storage—it requires a structured approach to organising, categorising, and controlling data. Azure Purview facilitates this through:

* **Centralised Data Catalogue**: A single source of truth for data assets, making it easy for users to discover and understand available data.
* **Metadata Management**: Rich metadata, including business and technical descriptions, enhances data discoverability and usability.
* **Lifecycle Policies**: Organisations can set rules for data retention, archival, and deletion, ensuring compliance and optimising storage costs.

As a result, teams can collaborate more effectively, reduce duplication, and derive greater value from their data assets.

## Defining Data Governance Processes: Steps and Best Practices Using Azure Purview

Establishing a successful data governance process with Azure Purview involves several key steps:

1. **Assess the Data Landscape**: Begin with automated scanning and discovery to understand what data exists and where it resides.
2. **Classify and Label Data**: Use Purview’s classification engine to tag data according to sensitivity, ownership, and usage requirements.
3. **Set Policies and Controls**: Define clear access and usage policies, assigning them to appropriate data sets and user roles.
4. **Monitor and Audit**: Leverage built-in monitoring to track policy compliance and data usage, enabling continuous improvement.
5. **Educate and Engage**: Foster a culture of data responsibility by providing training and resources for stakeholders across the organisation.

## Defining and Implementing Data Policies

* Navigate to Policy Management in Purview Studio.
* Create policy definitions such as “Mask Social Security Numbers” or “Restrict Access to HR Data.”
* Assign policies to specific data assets, resource groups, or users.
* Monitor policy compliance and adjust as needed.

## Recipe: Defining Data Policies

*Example Azure CLI to define a data access policy:*

*az purview policy create \*

*--account-name \*

*--resource-id \*

*--policy-name RestrictHRData \*

*--permissions read \*

*--principals*

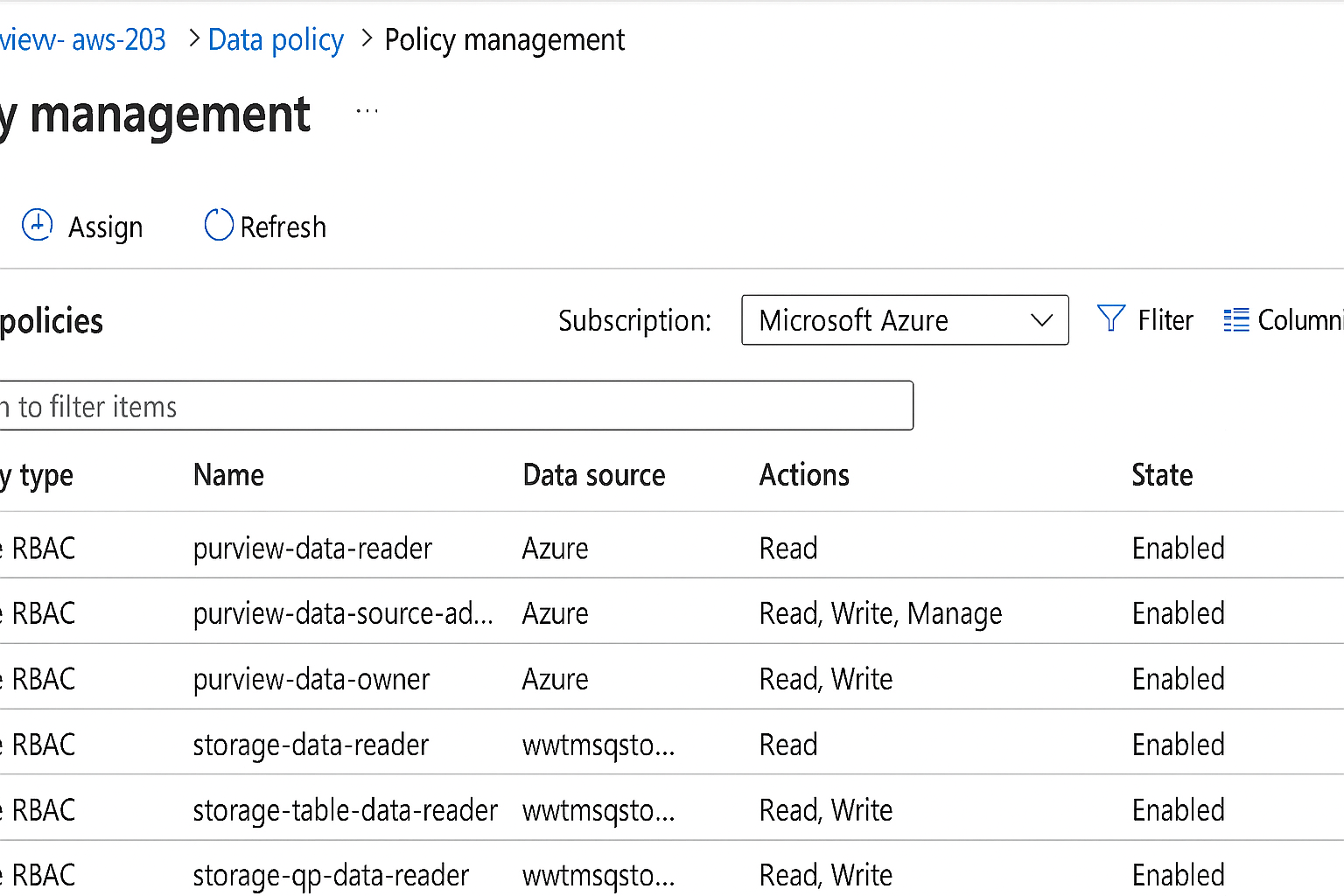


Figure: Policy management dashboard with list of active policies and compliance status indicators.

Best practices include starting with high-risk or high-value data, engaging cross-functional teams, and regularly reviewing and updating policies as business needs and regulations evolve.

Implementing strong data policies with Azure Purview empowers organisations to secure sensitive data, uphold privacy standards, and unlock the full potential of their data assets. By providing a unified platform for data discovery, classification, and policy management, Purview lays the foundation for effective data governance. As data continues to grow in volume and complexity, tools like Azure Purview will be essential for organisations looking to build trust, ensure compliance, and drive innovation in a fast-changing digital landscape.

Ensuring Data Quality

Data quality is fundamental to trustworthy analytics and decision-making. Purview supports quality monitoring through profiling, validation, and collaboration features.

## Profiling and Validating Data

* Enable data profiling during scans to generate statistics: null counts, distinct values, patterns, and outliers.
* Review profiling reports to identify quality issues.
* Integrate with Azure Data Factory for advanced data validation and cleansing pipelines.

## Recipe: Data Quality Monitoring and Reporting

Ensuring high-quality data is crucial for any organisation that relies on data-driven decision-making. Data quality issues can lead to inaccurate insights, compliance risks, and operational inefficiencies. To tackle these challenges, Microsoft Azure offers a modern, cloud-based approach to data quality monitoring and reporting, with Azure Purview at its core.

Azure Purview enables you to discover, classify, and map your data landscape, making it easier to ensure your data’s quality, security, and compliance.

## Key Azure Services Involved

* **Azure Purview**: The main service for data cataloguing, classification, and governance.
* **Azure Data Factory**: Orchestrates data movement and transformation, and supports data quality checks through pipelines.
* **Azure Synapse Analytics**: Stores, processes, and analyses large volumes of data, and can serve as the data warehouse for reporting.
* **Azure Logic Apps or Azure Functions**: Automates workflows like alerting and reporting based on quality checks.
* **Power BI**: Visualises and reports data quality metrics for business users and stakeholders.

## Step-by-Step: Developing the Data Quality Monitoring Recipe

### 1. Data Discovery and Cataloguing with Azure Purview

The journey starts by setting up Azure Purview to scan and catalogue all your data assets across various sources. Purview automatically discovers datasets, classifies them based on sensitivity (like personal data, financial data), and builds a comprehensive data map. This step lays the foundation for effective data quality monitoring, as it gives visibility into the data landscape.

### 2. Defining Data Quality Rules and Policies

Next, you need to establish what “good quality” means for your data. This involves defining data quality rules and policies, such as completeness (no missing values), consistency (values follow a certain format), accuracy (values match source systems), and timeliness. These rules can be set up in collaboration with business stakeholders and data stewards.

### 3. Data Quality Checks with Azure Data Factory

Azure Data Factory (ADF) plays a key role in operationalising data quality checks. You can design ADF pipelines to extract datasets from various sources and run validation activities. For example, you might use Data Flow activities in ADF to check for nulls, duplicates, or out-of-range values. When a data quality rule is violated, the pipeline can flag the issue and trigger downstream actions.

### 4. Storing and Aggregating Data Quality Metrics

The results of these data quality checks—such as the number of errors, percentage of missing data, or records failing validation—are stored in a central repository, often in Azure Synapse Analytics. This allows for historical tracking of data quality metrics and makes it easy to spot trends or recurring issues over time.

### 5. Automation and Alerting with Logic Apps or Functions

To streamline operations, automation is critical. Azure Logic Apps or Azure Functions can be configured to automatically notify relevant teams when data quality issues are detected. For instance, if a data quality threshold is breached, an automated email or Teams notification can be sent to the data owner, prompting immediate action.

### 6. Data Quality Reporting with Power BI

All the aggregated metrics and quality reports are then made accessible to business users through Power BI dashboards. These interactive reports can highlight key metrics such as data quality scores, trends over time, and areas needing attention. This visibility drives accountability and continuous improvement in data quality practices.

Now, lets create the recipe as below:

* After scanning, navigate to an asset’s detail page and view the Profile tab.
* Download quality reports for further analysis or auditing.
* Establish data quality KPIs in Purview and monitor trends over time.

A screenshot of a computer

AI-generated content may be incorrect.

Figure: Data profile summary with histograms, null value counts, and pattern detection results.

## To bring it all together, the typical workflow of this recipe has the following activities.

1. Azure Purview scans data sources, catalogues assets, and classifies data.
2. Data quality rules are defined and stored within Purview and/or ADF.
3. ADF pipelines run scheduled data quality checks and validation tasks.
4. Results are pushed to Azure Synapse Analytics for storage and aggregation.
5. Logic Apps or Functions automate alerts and notifications on issues.
6. Power BI provides comprehensive reporting to stakeholders.

By leveraging Azure Purview alongside other Azure services like Data Factory, Synapse Analytics, Logic Apps, and Power BI, organisations can build a robust, scalable, and automated data quality monitoring and reporting solution. This approach ensures that data remains trustworthy, compliant, and fit for purpose, enabling better business decisions and reducing operational risks.

Compliance and Security

Maintaining compliance with data privacy regulations—such as GDPR, HIPAA, and CCPA—is a major driver behind data governance initiatives. Azure Purview aids compliance by automating the discovery and classification of sensitive data, enforcing policies, and providing detailed audit logs.

In today’s digital ecosystem, organisations handle an ever-increasing volume of data, making compliance and security more crucial than ever. Azure Purview, Microsoft’s unified data governance solution, stands out by providing robust tools to manage, discover, and secure data across on-premises, multi-cloud, and SaaS sources. Let’s delve into how Azure Purview addresses compliance and security concerns, ensuring that data remains both accessible and protected.

As we have understood that Azure Purview is a data governance service designed to help organisations map, catalogue, manage, and secure their data assets. It empowers businesses to understand the data they have, trace its lineage, and ensure it meets compliance requirements, all while maintaining tight security controls. Whether your data lives in Azure, AWS, on-premises databases, or SaaS platforms, Purview brings a single view of your entire data landscape.

## Compliance in Azure Purview

Compliance involves adhering to regulations, laws, and internal policies that dictate how data should be handled. This is especially important in sectors like finance, healthcare, and government, where regulations such as GDPR, HIPAA, and others mandate stringent data controls.

* **Automated Data Discovery and Classification** - Azure Purview automatically scans connected data sources to identify and classify sensitive information, such as personal identifiers, financial records, or health data. This helps organisations locate regulated data swiftly and understand where compliance risks may lie.
* **Custom Labelling** - You can apply custom labels to data assets to match your organisation’s internal policies or compliance needs. Labels make it easier to track and manage sensitive data, ensuring that compliance requirements are met consistently.
* **Audit Trails** - Purview keeps comprehensive logs of all activities, such as data access, modifications, and sharing. These audit trails are invaluable when demonstrating compliance to auditors or investigating incidents.
* **Data Lineage Tracking** - By mapping the journey of data from its source to its current location, Purview helps teams understand how data moves through the organisation. This transparency is crucial for compliance, as it reveals where sensitive data is stored and processed.

## Security in Azure Purview

Security is at the heart of Azure Purview’s design. Microsoft leverages decades of experience in building secure cloud platforms, and Purview inherits many of these capabilities to safeguard your data.

* **Role-Based Access Control (RBAC)** - Only authorised users can access or modify data assets within Purview. RBAC ensures that users see only what they are permitted to, reducing the risk of unauthorised access.
* **Data Encryption** - All data stored and transmitted by Purview is encrypted using industry-standard protocols. This ensures that even if data is intercepted or stolen, it remains unreadable to unauthorised parties.
* **Integration with Azure Security Centre** - Purview integrates seamlessly with Azure Security Centre, providing unified visibility into security risks and compliance issues across your Azure environment.
* **Secure Connectivity** - When Purview connects to external data sources, it uses secure authentication methods and encrypted channels to protect data in transit.
* **Continuous Monitoring** - Ongoing monitoring of activities within Purview enables early detection of suspicious behaviour, allowing organisations to respond quickly to potential threats.

## Implementing Security Controls

* Use classification rules to flag sensitive data types (e.g., credit card numbers, health records).
* Apply access policies to restrict data visibility to authorized users only.
* Integrate with Azure Sentinel and Microsoft Defender for advanced threat detection and response.
* Regularly review audit logs for suspicious activity or policy violations.

## Best Practices for Compliance and Security in Azure Purview

1. **Define Clear Data Policies**: Establish comprehensive data governance policies outlining who can access data, how it should be handled, and compliance expectations.
2. **Regularly Audit and Review**: Use Purview’s audit capabilities to periodically review data access and classification, ensuring continued compliance.
3. **Educate Your Team**: Regular training helps employees understand the importance of compliance and security, and how to use Purview’s features responsibly.
4. **Automate Where Possible**: Leverage Purview’s automation features to reduce manual effort, minimise errors, and maintain consistent security and compliance practices.

Azure Purview takes the complexity out of data governance by marrying comprehensive compliance features with robust security controls. Its ability to automatically discover, classify, and monitor data assets, combined with advanced security mechanisms, makes it an essential tool for modern organisations. By adopting Purview, businesses can ensure they are not just compliant with today’s regulations, but also prepared for the evolving demands of tomorrow’s data landscape.

## Recipe: Monitoring and Reporting

Ensuring your organisation has a clear view of where its data resides, how it’s being used, and who has access to it is more critical than ever is a complex stage in Data engineering. Azure Purview, Microsoft’s unified data governance solution, offers robust monitoring and reporting capabilities that empower organisations to achieve clarity, compliance, and confidence in their data landscape. In this guide, we take a closer look at how to develop a “Monitoring and Reporting using Azure Purview” recipe, the Azure services involved, and the step-by-step process to bring this recipe to life.

Azure Purview, with its comprehensive cataloguing and data lineage tracking, Azure Purview becomes the backbone for monitoring and reporting on your organisation’s data assets.

## Core Azure Services Required

To build a robust monitoring and reporting solution using Azure Purview, you’ll typically utilise the following Azure services:

* **Azure Purview**: The central data governance service for cataloguing, scanning, and managing data assets.
* **Azure Data Factory**: For orchestrating data movement and transformation, often used to trigger or schedule scans in Purview.
* **Azure Synapse Analytics or Azure SQL Database**: For analysing data and storing reporting results if advanced analytics or warehousing is required.
* **Power BI**: For visualising reports and dashboards based on the metadata and insights generated by Purview.
* **Azure Monitor and Azure Log Analytics**: To gather, analyse, and visualise operational logs and metrics, extending monitoring to performance and operational health.
* **Azure Logic Apps or Azure Functions**: For automation—triggering alerts, notifications, or custom workflows based on monitoring outputs.

## Developing the Monitoring and Reporting Recipe

Let’s break down the steps to develop a monitoring and reporting solution using Azure Purview and its supporting services.

### 1. Set Up Azure Purview Account

Begin by provisioning an Azure Purview account in your Azure subscription. This is your workspace for all data governance activities. You’ll define data sources (like Azure Data Lake, SQL databases, Blob Storage, etc.), and set up authentication and permissions to ensure secure access.

### 2. Scan and Catalogue Data Sources

Once your Purview account is ready, configure scans for your connected data sources. Azure Purview will explore these sources and automatically collect metadata, classifying data using built-in or custom classifiers. This builds a comprehensive inventory of your data assets, their schema, and relationships across your organisation.

### 3. Enable Data Lineage Tracking

With scanning set up, enable data lineage to visually map how data flows through your systems—from source to transformation to destination. This is especially useful for compliance and root cause analysis.

### 4. Set Up Monitoring and Alerts

Connect Azure Purview to Azure Monitor and Azure Log Analytics to keep tabs on scan activity, system health, and operational logs. Configure custom alerts to notify your team about critical events—such as failed scans, new sensitive data detected, or policy violations.

### 5. Aggregate and Store Monitoring Data

For in-depth analysis, pipeline logs and metadata from Purview and Azure Monitor into an analytics store. Azure Synapse Analytics or Azure SQL Database are good options for storing and querying this data, enabling you to perform trend analysis and historical comparisons.

### 6. Build Reports and Dashboards

Now, use Power BI to create dynamic dashboards and reports. Connect Power BI to your Purview metadata or the analytics store to visualise data coverage, classification breakdowns, data lineage paths, scan frequencies, and compliance statuses. Tailor reports to your stakeholders, whether they’re data stewards, security officers, or executive leadership.

### 7. Automate Workflows and Notifications

Integrate Azure Logic Apps or Azure Functions to automate repetitive tasks. For instance, automatically send emails if a scan fails, escalate issues to a ticketing system, or trigger remediation workflows when sensitive data is detected in an unexpected location.

* Access the Insights dashboard in Purview Studio for compliance status and usage patterns.
* Generate scheduled reports on asset classification, access trends, and policy enforcement events.
* Export logs to Azure Monitor or Power BI for custom visualization and alerting.

Figure: Compliance insights dashboard with classification coverage and access risk heatmap.

## Best Practices and Considerations

* **Regular Scanning**: Schedule frequent scans to keep your data inventory up to date.
* **Custom Classification**: Develop custom data classifiers to meet your organisation’s unique sensitivity and compliance needs.
* **Role-Based Access**: Implement role-based access control in Purview to ensure only authorised personnel can view or modify data assets.
* **Continuous Improvement**: Use monitoring and reporting insights to refine your data governance policies and practices over time.

By following this recipe, you’ll equip your organisation with a robust, automated, and insightful monitoring and reporting system powered by Azure Purview and its suite of complementary Azure services. This approach not only enhances transparency and control over your data estate but also enables ongoing compliance and data-driven decision-making, all in line with the latest industry best practices.

Elevating Data Governance

Implementing sustainable data governance requires a strategic, ongoing approach involving people, processes, and technology. The following best practices can help maximize the value of Azure Purview:

* Establish a dedicated governance team: Assign clear ownership for data stewardssship, catalog curation, and policy management.
* Define data domains and business glossaries: Enable consistent understanding of data assets across the organization.
* Automate where possible: Leverage Purview’s scanning, classification, and lineage capabilities to reduce manual efforts.
* Promote data literacy: Provide training and documentation for stakeholders to drive adoption and responsible data usage.
* Iterate and improve: Regularly review governance policies, scan schedules, and data quality metrics to adapt to evolving needs.
* Integrate with broader cloud ecosystem: Combine Purview with Azure Data Factory, Synapse Analytics, and security services for a unified governance solution.

## Recipe: Data Governance Best Practices Checklist

Data governance is all about ensuring that your organisation's data is accurate, secure, accessible, and used responsibly. In today's digital landscape, managing data effectively is more crucial than ever, especially when working with vast and complex datasets. Microsoft Azure Purview is a powerful solution for implementing data governance at scale, offering robust tools for data discovery, classification, and management.

## Understanding the Role of Azure Purview in Data Governance

Azure Purview acts as a unified data governance platform, allowing you to get a clear picture of your data assets, track their lineage, classify sensitive information, and establish policies for access and usage. It helps teams avoid data silos, comply with regulatory requirements, and make informed decisions about data. Think of it as your central nerve centre for managing data governance across the organisation.

## Data Governance Best Practices Checklist

Here’s a detailed checklist to guide you through setting up effective data governance using Azure Purview:

1. **Define Clear Objectives and Policies -** Identify what you want to achieve with data governance (e.g., regulatory compliance, improved data quality, better analytics).
2. Draft and document policies regarding data ownership, stewardship, access, and usage.
3. **Catalogue All Data Sources -** Use Azure Purview to automatically scan and catalogue data sources including Azure Data Lake, SQL databases, Power BI, and on-premises systems.
4. Maintain an updated inventory of data assets for visibility and management.
5. **Classify and Label Sensitive Data -** Leverage Purview’s built-in and custom classifiers to tag sensitive data such as personal information, financial records, or intellectual property.
6. Apply labels to help enforce policies and meet compliance standards.
7. **Establish Data Lineage -** Track the movement and transformation of data across your environment using Purview’s lineage capabilities.
8. This helps you understand data flows, troubleshoot issues, and demonstrate compliance.
9. **Set Up Roles and Access Controls -** Define roles such as data owners, stewards, and consumers within Purview.
10. Use Azure Active Directory (AAD) for identity management and enforce access controls to restrict sensitive data exposure.
11. **Monitor and Audit Data Usage -** Enable auditing of data access and usage to detect anomalies and ensure adherence to policies.
12. Regularly review logs and generate reports for compliance and governance oversight.
13. **Automate Policy Enforcement -** Integrate with Azure Policy and Purview to automate enforcement of data governance rules.
14. Set up alerts for policy violations and remediation workflows.
15. **Foster a Data-Centric Culture -** Educate teams about the importance of data governance and their roles.
16. Encourage feedback and continuous improvement of governance practices.

## Azure Services Required for the Recipe

To bring your data governance checklist to life, you’ll need a combination of Azure services working together:

* **Azure Purview**: The core platform for data catalogue, classification, and lineage tracking.
* **Azure Data Lake Storage**: For storing structured and unstructured data, which Purview can scan and catalogue.
* **Azure SQL Database**: A common data source integrated with Purview for metadata management.
* **Power BI**: For visual analytics and reporting, with datasets discoverable in Purview.
* **Azure Active Directory (AAD)**: For managing identities, roles, and access controls.
* **Azure Policy**: To automate and enforce governance rules across resources.
* **Azure Monitor & Log Analytics**: For auditing, monitoring, and generating compliance reports.

## Developing the Data Governance Recipe

Building the recipe for data governance using Azure Purview is a systematic process that blends planning, configuration, and ongoing management. Here’s how you can develop it:

1. **Assessment and Planning -** Start by evaluating your current data landscape. Identify key stakeholders, data sources, and compliance requirements. Develop clear objectives and map out the governance framework tailored to organisational needs.
2. **Deployment of Azure Purview -** Spin up an Azure Purview account in your subscription. Configure connectivity to all relevant data sources using Purview’s integration capabilities. This might include setting up scanning for on-premises systems using Purview’s self-hosted integration runtimes.
3. **Data Scanning and Cataloguing -** Initiate scans to automatically discover, catalogue, and classify data assets across your environment. Review and refine the metadata to ensure accuracy.
4. **Sensitive Data Classification -** Apply built-in and custom classifications for sensitive information. Tag and label data as per regulatory and business requirements.
5. **Establishing Lineage and Metadata Management -** Leverage Purview’s lineage feature to visualise data flow and transformations. Document metadata and ensure data owners and stewards are assigned.
6. **Configuring Access Controls -** Set up roles and permissions using Azure Active Directory. Define stewardship responsibilities and limit access to sensitive datasets as necessary.
7. **Policy Automation and Enforcement -** Integrate Azure Policy with Purview to automate governance rule enforcement. Configure alerts and remediation workflows for policy violations.
8. **Monitoring and Auditing -** Enable Azure Monitor and Log Analytics to track data usage, access patterns, and compliance. Generate regular reports for stakeholders.
9. **Iteration and Improvement -** Continuously review governance practices, update policies, and educate teams. Use feedback mechanisms to refine the governance recipe over time.

Now, lets following below tips when implementing this recipe

* Maintain an up-to-date inventory of all data sources and assets.
* Schedule regular scans and policy reviews.
* Monitor lineage to assess business impact of changes.
* Document data ownership and stewardship responsibilities.
* Engage business users in catalog enrichment and validation.
* Implementing a robust data governance framework with Azure Purview is a strategic move for any organisation seeking to maximise value from its data while staying compliant and secure. By following this checklist and leveraging the right Azure services, you can build a scalable, efficient, and sustainable data governance recipe tailored to your needs. Remember, data governance is not a one-time exercise—it’s an ongoing journey of improvement, collaboration, and adaptation.

## Real-world Use Cases

Let’s consider some practical scenarios where Azure Purview makes a tangible impact:

* **Banking and Financial Services** - A large bank uses Purview to catalogue sensitive customer data across multiple systems, ensuring compliance with RBI regulations and streamlining reporting for audits.
* **Healthcare -** A hospital network integrates Azure Purview with its data lake and analytics tools, enabling secure discovery and management of patient records, while maintaining HIPAA and local privacy requirements.
* **Retail Analytics -** A leading retailer uses Purview to improve collaboration between marketing and IT teams, ensuring campaign data is accurate, consistent, and accessible for analysis across locations.

Azure Purview is a powerful ally for organisations aiming to harness the full value of their data while maintaining robust governance and compliance. Its intuitive interface, rich integration capabilities, and automation features make it an essential tool for data engineers and IT professionals. By implementing Azure Purview as a cornerstone of your data governance strategy, you not only protect your data assets but also unlock new opportunities for innovation, collaboration, and growth in the digital age.