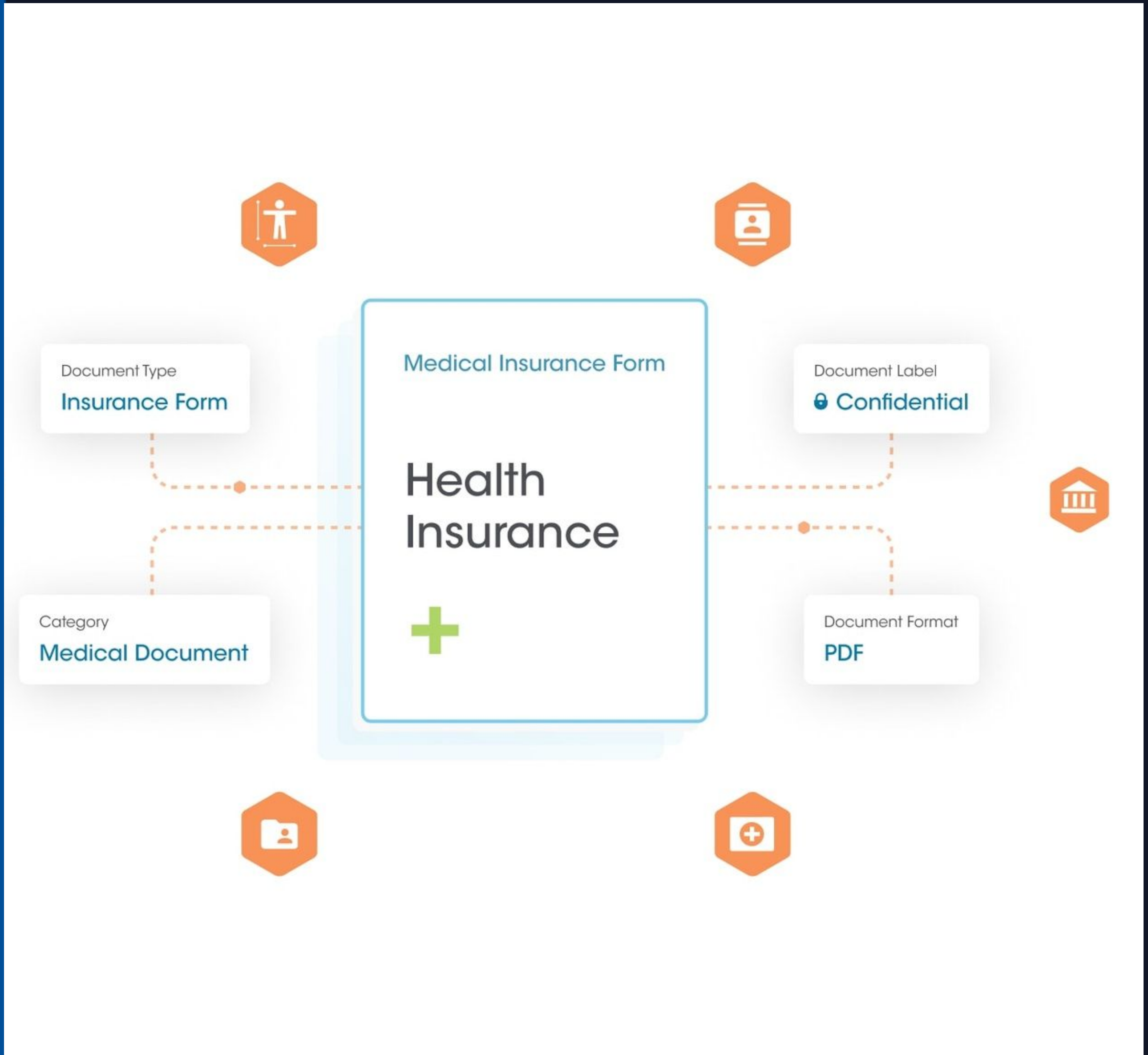
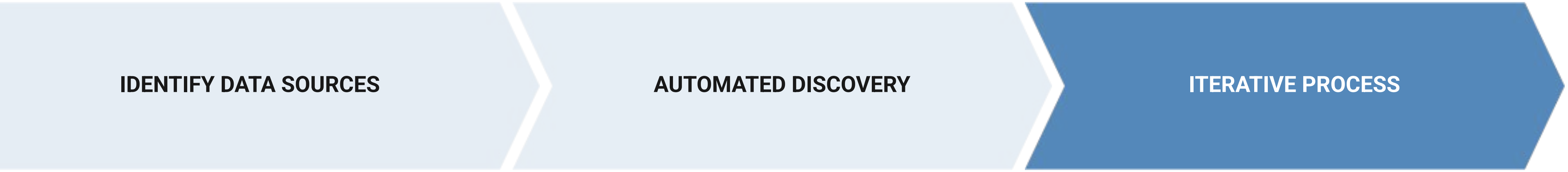


Safeguarding Data in the Cloud: A Classification-Driven Approach

Data Inventory and Discovery



IDENTIFY DATA SOURCES

Locate and catalog all data assets, including databases, file storage systems, SaaS applications, and third-party services, across on-premises and cloud environments.

AUTOMATED DISCOVERY

Deploy pattern-matching tools to scan for specific data types, such as personally identifiable information (PII) or financial records, to streamline the detection of critical data assets.

ITERATIVE PROCESS

Continuously re-scan and update the data inventory to reflect newly generated data or changes in cloud storage configurations, ensuring the organization maintains a comprehensive understanding of its data landscape.

Data Ownership

DEFINING OWNERSHIP

Data ownership establishes accountability for data protection. An owner is typically responsible for defining usage policies, ensuring data is accurately classified and secured, and authorizing access requests.

OWNERSHIP IN CLOUD ENVIRONMENTS

In cloud environments, ownership can become complex because multiple stakeholders, including cloud service providers, internal teams, and external vendors, share responsibilities. Clear delineation of ownership roles helps avoid ambiguities and ensures consistent application of classification labels.

OWNER RESPONSIBILITIES

The data owner is responsible for defining usage policies, ensuring data is accurately classified and secured, and authorizing access requests for users or applications.

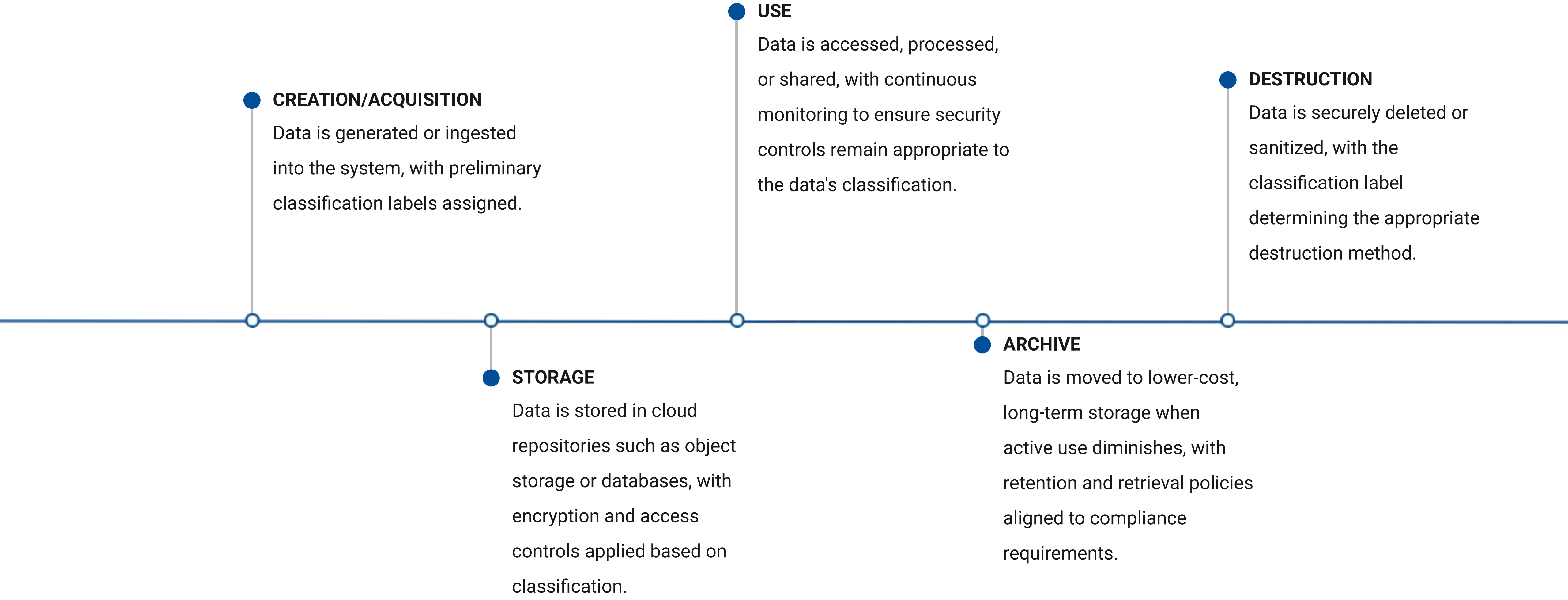
ALIGNING WITH GOVERNANCE

Clearly defining data ownership roles is important and aligns with discussions on governance and risk management, emphasizing the importance of assigning responsibilities for any data residing in the cloud.

AVOIDING AMBIGUITY

Clear delineation of ownership roles helps avoid ambiguities, ensuring that classification labels are applied consistently across the organization.

The Data Lifecycle



CREATION/ACQUISITION

Data is generated or ingested into the system, with preliminary classification labels assigned.

STORAGE

Data is stored in cloud repositories such as object storage or databases, with encryption and access controls applied based on classification.

USE

Data is accessed, processed, or shared, with continuous monitoring to ensure security controls remain appropriate to the data's classification.

ARCHIVE

Data is moved to lower-cost, long-term storage when active use diminishes, with retention and retrieval policies aligned to compliance requirements.

DESTRUCTION

Data is securely deleted or sanitized, with the classification label determining the appropriate destruction method.

The Data Categorization.

The data owner will be in the best position to understand how the data is going to be used by the organization. This allows the data owner to appropriately categorize the data.

The organization can have any number of categories or types of information; these might be clearly defined and reused throughout the organization, or they might be arbitrarily assigned by data owners during the Create phase.

Here are some ways an organization might categorize data:

1- Regulatory Compliance:
2- Business Function:
3- By Project:

Introduction to Data Classification

DEFINE DATA CLASSIFICATION

The process of categorizing data based on its sensitivity, value, and criticality to an organization.

IMPORTANCE OF DATA CLASSIFICATION

Helps prioritize protection efforts and ensure appropriate security controls are in place, aligning with compliance requirements.

CONNECTION TO SECURITY FUNDAMENTALS

Data classification ties directly to encryption best practices, privacy concerns, and other security foundations covered in Domain 2.

APPLYING CLASSIFICATION IN CLOUD ENVIRONMENTS

Establishes the basis for discussing data protection methodologies, such as encryption tiers and access control mechanisms, in cloud environments.

DATA CLASSIFICATION IS A CRITICAL PROCESS THAT ENABLES ORGANIZATIONS TO PRIORITIZE SECURITY EFFORTS, MEET COMPLIANCE REQUIREMENTS, AND LAY THE FOUNDATION FOR COMPREHENSIVE DATA PROTECTION IN THE CLOUD.

The Data Classification.

Much like categorization, data classification is the responsibility of the data owner, takes place in the Create phase, and is assigned according to an overall organizational policy based on a specific characteristic of the given dataset. The classification, like the categorization, can take any form defined by the organization and should be uniformly applied.
Types of classification might include the following:

Sensitivity:
Jurisdiction:
Criticality:

The Data Mapping.

Data between organizations (or sometimes even between departments) must be normalized and translated so that it conforms in a way meaningful to both parties. This is typically referred to as data mapping.

The Data Labeling.

When the data owner creates, categorizes, and classifies the data, the data also needs to be labeled. The label should indicate who the data owner is, usually in terms of the office or role instead of an individual name or identity (because, of course, personnel can change roles with an organization or leave for other organizations).

Data Discovery Methods

Comparison of data discovery methods by accuracy percentage

The Data Labeling.

To determine and accurately inventory the data under its control, the organization can employ various tools and techniques.

Label-Based Discovery.
Metadata-Based Discovery.
Content-Based Discovery.

Case Study: Classification and Discovery in a Financial Services Cloud Migration

This case study showcases how a global financial institution leveraged data classification and discovery to securely migrate large volumes of client data to a hybrid cloud environment while maintaining strict compliance with regulations such as PCI-DSS and GDPR.

Maintaining Continuity

CONSISTENT DATA PROTECTION

SCALABLE SECURITY CONTROLS

STREAMLINED REGULATORY COMPLIANCE

ADVANCED THREAT MITIGATION

Key Takeaways

DATA CLASSIFICATION PRIORITIZES PROTECTION

Categorizing data based on sensitivity, value, and criticality enables organizations to apply the appropriate security controls and meet compliance requirements.

DEFINED DATA OWNERSHIP AND ACCOUNTABILITY

Assigning clear responsibilities for data protection, including usage policies and access authorization, is essential in complex cloud environments.

COMPREHENSIVE DATA INVENTORY AND DISCOVERY

Identifying and locating all data assets, both structured and unstructured, across on-premises and cloud environments is the first critical step.

AUTOMATED DISCOVERY AND CLASSIFICATION METHODS

Leveraging pattern matching, machine learning, and metadata-based techniques streamlines the data identification and labeling process.

BY ESTABLISHING A ROBUST DATA CLASSIFICATION AND DISCOVERY FRAMEWORK, ORGANIZATIONS CAN BUILD A STRONG FOUNDATION FOR CONSISTENT DATA PROTECTION PRACTICES IN THE CLOUD, ENABLING THEM TO ADDRESS SOPHISTICATED THREATS AND REGULATORY CHALLENGES.