Overview

Be it on-prem or hybrid set-up; organizations continuously face multiple data security challenges from multiple end-users. The context behind adopting Data Access Governance (DAG) frameworks has evolved significantly due to several factors, reflecting the increasing demand for data governance in modern enterprises. Some key influences and historical context that have shaped the development of DAG frameworks are:

Explosion of Data Volume and Variety

The rapid growth of data generation due to digital transformation, IoT devices, the increasing influence of social media, too many online interactions among internal and external users, and more — has made effective data management crucial. Not only data volume, but also more diverse types of data proliferate the requirement of robust data governance frameworks to manage access appropriately.

Regulatory Requirements

Increasing regulatory scrutiny around data privacy and protection has driven the need for formal governance frameworks. Most of the regulatory standards demand organizations to implement strict data access controls to protect sensitive information.

Ambiguous Ownership of data assets

Ambiguous ownership of data assets is a growing concern for organizations, especially as data becomes increasingly central to business operations and decision-making. Lack of clear policy, cross-functional data use, and random data sharing are some key aspects that illustrate the challenges and implications of ambiguous data ownership

Access permissions are not standardized based on security group

Several issues can arise when access permissions are not standardized based on security groups. Some of them are inconsistent access control, increased risk of data breaches, inconsistent permissions, management complexity, audit and compliance challenges, and operational inefficiencies. Moreover, managing access permissions on an individual basis instead of in groups can become cumbersome

Approvals dispute/ delays

Delay in giving approvals results in delay of projects, reduction in work efficiency, loss of opportunities and eventually impacts stakeholders' relationships. Hence, on-time approvals play a crucial role in maintaining and managing access to enterprise data assets

Key Features

The key features of Data Access Governance (DAG) mechanism are:

Data Visibility Across Shared Folders

The importance of data visibility comes with the ability to access, monitor, and track data throughout its entire lifecycle. It is the most important feature of the Data Access Governance (DAG) module as it ensures that enterprise data is available, understandable, and usa ble by only those who need it. As a result, data visibility is indispensa ble in shared folders, NFS (Network File Sharing) drives for Unix/ Linux environments, or SaaS storages.

Who, What, When of Data Access

DAG module helps to remove the ambiguity of who is accessing which data file, when, for what reason, and for how long. This is the foremost condition to prevent unauthorized/ suspicious access to enterprise data assets. Even while sharing or transferring data files from one user to another, it configures and customizes end-user access and sharing permissions. As part of ARCON's My Vault solution, DAG can customize end-user access and sharing permissions by restricting the random transfer of data files internally and externally

Ownership of Critical Files/Folders/Data

The DAG module ensures a seamless administrative experience with ARCON's My Vault by transferring/ customizing ownership of data files. It allows one user to transfer file rights to another user when the former leaves the organization or joins another line of business/ department.

Shared Access to Unnecessary/Irrelevant files/folder

Accessing irrelevant and unnecessary files can pose several risks to an organization. If shared access is allowed to users who can access multiple files/ folders at any given point in time, then it poses risks of unauthorized access or data misuse. ARCON's DAG module helps organizations identify relevant folders/ files that are required for any shared access

Benefits at a Glance

- **Builds data visibility across multiple shared folders**
- **Provides continuous governance of enterprise data assets**
- **Provides end-to-end data encryption with the help of ARCON My Vault**
- **Ensures data integrity and desired data confidentiality**
- **Meets compliance with the global & regional IT standards**