DATA ACCESS GOVERNANCE
BEST PRACTICE

DESIRED OUTCOMES
• Enable business users to take ownership and a more active role in the governance of their data resources
• Easily see ownership and entitlements across hundreds or thousands of file shares, servers and SharePoint sites
• Leverage a common and consistent platform for access governance across applications, data and platforms
• Enable a closed-loop validation process for changes to data access permissions, ensuring that non-compliant access is correctly and quickly revoked
• Manage data access risk and provide auditable evidence of compliance with internal and external policies
• Achieve a significantly improved risk posture, reducing the likelihood and severity of potential data breaches

DATA ACCESS GOVERNANCE OVERVIEW
The Data Access Governance (DAG) module gives organizations the ability to extend access governance to unstructured data, including SharePoint sites and Windows file shares, providing the same level of access visibility and control for their data resources that is in place with applications and platforms. This solution gives an organization the ability to provide context to the types of data and accountable business ownership for various data resources. Additionally, enterprises can leverage the product to verify and validate that user access to files, shares and SharePoint is appropriate given users’ roles and responsibilities within the organization.

PARTICIPANTS
For a timely and successful DAG deployment, participation from a varied number of resources is recommended. Business owners of the various data resource types (shares, SharePoint sites, etc.) as well as related IT custodians are required to help identify the scope of targets for on-boarding, either through the types of data contained and/or outstanding audit/regulatory risk associated with the assets. Business Analysts are recommended for the definition of governance activities and supporting the business. Finally, technical leads for each of the in-scope targets will be required for any troubleshooting and data validation activities.

PROCESS

DATA SHEET

EMC²
PLANNING
The planning phase should be approached with the mentality of “measure twice, cut once.” A key output of planning is listing in-scope targets and any related/defensible methodology used to arrive at the in-scope list. Organizations should determine what will be included in the governance program supported by business and risk partners. It is also very important to gain the support and commitment from the business AND technical resources responsible for the in-scope assets. If either does not support the efforts, it will be extremely difficult to deploy anything sustainable. Finally, organizations should procure the specific infrastructure required for a DAG deployment and scope out any processes needed to support the deployment in their specific environment. RSA Consulting Services can provide typical questions that should be answered in planning.

COLLECTION
Collection will involve much more involvement from technical resources. Here, the DAG components should be deployed on the related infrastructure and configured to collect all relevant access information for in-scope targets. There are two key points here where technical resources are crucial to success in terms of schedule/timing. First, a service account (or multiple depending on the environment) with appropriate access rights to target servers must be in place prior to any collections. RSA Consulting Services can provide detailed requirements for these rights based on the target, and customer technical resources should begin lining these up immediately. Second, once data is collected from the targets, technical resources should validate that data collected appears as expected. These resources do not need to comment on appropriateness of access, however, they should be able to confirm that access on the targets matches what is being collected.

GOVERNANCE
This phase requires heavy input and involvement from business owners, business analysts, and ultimately business end-users. The DAG solution offers two types of high-level activities with data resources: Data Ownership Reviews and Data Access Reviews. It’s best to complete ownership reviews first.

- Data Ownership Reviews allow organizations to build a user-friendly process and workflow where business ownership of a data resource is identified, confirmed and documented. The solution can be configured to start with suggested owners of resources, if available, or with pre-defined owners to begin the process. From there, business owners and business analysts will need to determine their organization’s “rules of engagement” for allowing individuals to identify owners, suggested owners confirming their ownership, and resolving situations when individuals do not want to claim/accept ownership. Key business end-user input is also highly recommended so any glaring issues/questions can be addressed and support for the program (to the extent possible) is in place prior to a full roll-out.

- Data Access Reviews allow organizations to build a user-friendly process and workflow where identified and confirmed business owners can then make decisions regarding the individuals with access to their resource(s). Business owners and business analysts must determine their organization’s “rules of engagement” for the frequency of these reviews, their scope, the delegation of review decisions, and any required approvals prior to removing access identified as inappropriate. Key business end-user input is also highly recommended so any glaring issues/questions can be addressed and support for the program (to the extent possible) is in place prior to a full roll-out.
REMEDICATION

Remediation requires combined efforts from technical and business resources. One key output of governance activities is a collection of access rights that need to be remediated after being identified as inappropriate. The solution can support a closed-loop remediation process via fully automated fulfillment activities leveraging the RSA platform or fulfillment activities that integrate with other existing processes/tools (i.e. Remedy ticketing system, email requests to a mailbox, reports generated for security administrators, etc.).

The desired fulfillment process should be defined by business resources with input from technical resources in terms of feasibility. This phase should also include the design and execution of any lifecycle activities related to removing targets from the in-scope list, as well as on-boarding new assets. Business analysts should define the triggers for various lifecycle activities and work with technical resources to confirm a process for notification, action and confirmation of these lifecycle activities.

ADDITIONAL INFORMATION

For additional information, please speak to your RSA Sales Representative or call 781-487-7700. You can also check out our RSA community site at community.RSA.com.