coenterprise

Why You Should Consider Role-Based Access Control (RBAC) for Your Business

Error #003509
Direct grants from object owners are not authorized in a managed access schema. Use the schema owner role or a role with the MANAGE GRANTS privilege.

Statement executed successfully (success)

Role Based Access Control (RBAC) can be a challenge to implement. It's not appropriate for all organizations, and its business value is at times elusive. What seems like a straightforward set of administrative tasks turns out to involve a wide collection of tools, patterns, and organizational skills. Though often ignored, decisions on implementing and investing in RBAC are as important decisions as a new Snowflake business owner can face.

Note that the value of RBAC is considered broadly here, but its importance to Snowflake implementations are the focus.

This eBook looks at the business case for implementing RBAC in Snowflake in five fundamental areas:

What is RBAC?

Before we dive into the main crux of this eBook, it's important to outline exactly what is RBAC? Role-based access control or role-based security is an approach companies use to restrict system access to authorized users. It is used by the majority of enterprises with more than 500 employees and can implement mandatory access control or discretionary access control. It enables administrators to better understand who has access to specific datasets, and more importantly whether they should have access to this data. RBAC enables companies to align their access controls with their overall IT security strategy.

Technical Challenges & ROI

Before considering the benefits of an RBAC implementation, its worth noting that the decision is not entirely straightforward and involves investment, skills, and training that may be unanticipated.

Snowflake enables a best-in-class data cloud environment for simple, scalable, and extensible data cloud solutions. But to realize these benefits, database administrators must deal with a daunting array of interconnected tools that make this possible in a Snowflake environment. Administrators need to master the following principles (for starters):

- Managed access architecture
- Ownership configurations
- Delegation of administrative permissions to the environmental level
- Separation of data object ownership from permissions
- Role hierarchies
- Differentiation between data access and functional layers
- Best practices for automated generation of new environments and roles

A thoughtful implementation of Snowflake's RBAC toolkit–which is powerful, but complex–makes good on its breakthrough capabilities in sharing information. Whether data is being shared through reader accounts, private exchanges, or the data marketplace, confidence sharing information is particularly critical to the Snowflake's data cloud and both data providers and third-party consumers. The more data is exchanged, the greater the need is to establish a strong RBAC implementation.

So, are the costs worth the benefits? Let's look at them.

User Administration

Nowhere in a growing Snowflake environment is the value clearer than in managing the user lifecycle.

In early environments, with a user base still in the teens, user administration can be managed directly. But as users onboard and offboard from your data cloud application in the hundreds, then, hopefully, in the thousands, permissions become increasingly complex and time intensive.

Once implemented, the administration of users shifts from a Snowflake administrator's responsibilities to an organizational responsibility. It's no longer who they are, it's what they do. These questions and statuses are delegated to the parts of the organization that are closest to the users and roles. Even with the advantages of the Snowflake data cloud, costly database administrators don't have the time to focus properly on these areas.

Here are the core benefits to RBAC in user administration that impact simplicity, speed and risk:

1. Reduction in errors when a new user's permissions are being granted
2. Speed and simplicity of provisioning and deprovisioning users
3. Administrative "paperwork"
4. Ease of integrating third parties
5. Protection against the following high-risk scenarios:
   - Employees who've left the enterprise, but retain identity and access privileges
   - Users transferring roles and responsibilities but retaining legacy privileges
   - Managers transferring roles and responsibilities (but retaining privilege oversight)
   - Disgruntled former employees
   - Informal access grants that elude oversight

Financial Benefits

A handful of factors drive the financial value of an RBAC implementation. They are:

- Complexity and auditing impact of configuring permissions at the user level
- Cost of database administrators managing and coordinating with user managers
- Time investment to create testing and development environments
- Tightly scoping per-minute utilization of compute
- Cost per service desk support, provisioning, and deprovisioning tickets that range from $3 to $50

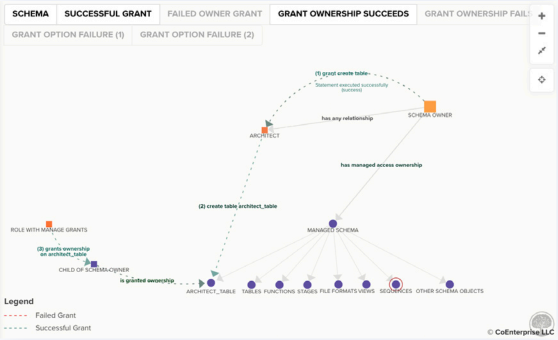
The structured delegation of permissions to organizational roles decreases the need for bespoke, one-off permissions. In turn, this reduces the complexity of privilege reviews and auditing. Permissions oversight can be reviewed directly by functional managers and the individuals involved.

Both activities diminish the costs for a database administrator to monitor, research, and coordinate with the appropriate managers. As a Snowflake implementation grows beyond its initial users, the scale makes this untenable and involves costly, technical resources. One of the core promises of working in Snowflake's data cloud is the simplicity and ease of administration, but managing permissions at a user level threatens that promise.

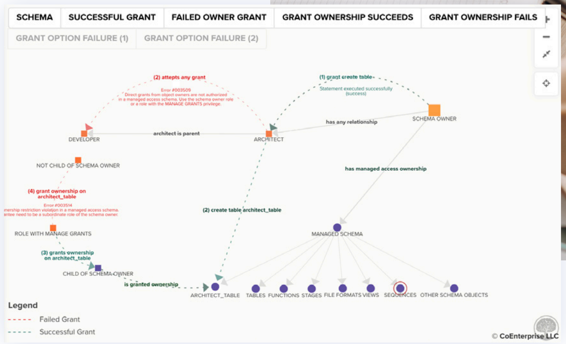
Consider also the complexity of creating new development and testing environments as permissions grow. Snowflake allows for effortless cloning of databases, but no such functionality exists for cloning roles. Getting the creation of new environments wrong is to compromise security. Getting it right without RBAC demands a slower creation time that is likely inconsistent resulting in even further delays and unexpected permissioning obstacles.

Because Snowflake charges per minute (compute * warehouse size), tightly scoped permission of least access ensures that users are spending their valuable minutes scoped to their responsibilities and no more. RBAC enables tightly controlled access to appropriately sized virtual warehouses neither too large nor too small for their use cases. Users shouldn't be consuming BI reports on an X-Large warehouse sized for an AI/ML use case. Notably, the ability to control warehouse access by project and/or function also supports auditable chargebacks to business units.

Critically, the bottom line of processing service desk tickets can't be ignored. Ticket handling time and agent utilization are directly affected. Aside from the opportunity cost and lost productivity while a user waits for resources to be made available, there are the direct costs of the tickets themselves. The average benchmark cost for a minute of ticket handle time is $1.60. Costs for tickets in aggregate average almost $16. Calculating the math for one's own organization is straightforward and prudent.



Statement executed successfully (success)



Error #003509
Direct grants from object owners are not authorized in a managed access schema. Use the schema owner role or a role with the MANAGE GRANTS privilege.

Statement executed successfully (success)

Error #003514
nership restriction violation in a managed access schema.
antee need to be a subordinate role of the schema owner.

Organizational Benefits

Architecting an RBAC solution is an initial challenge both at the technical and organizational levels. Defining roles for RBAC requires the thoughtful definition of roles, responsibilities, and scope of permissions. The up-front investment of effort, coordination, and administration for these decisions spans database administration, IdPs and business groups. It is possible to start small, but defining the relationships between roles and tying them to data access needs is no easy task. The benefits of RBAC are realized in the longer term after this initial investment.

While these upfront costs and the effort of establishing the appropriate scope of permissions can be daunting, the longer-term organizational benefits are appealing. By forcing organizational clarity into the business, managers structure their interactions with data to operate at the organizational rather than user level.

The security architecture benefits make it easier to implement separation of duties as well as to push privilege reviews to a delegated model–all within the natural structure of the organization. Employees get access to what they need to do their jobs and no more.

Enhancing Compliance

Since its adoption as a national standard in 2004, RBAC has become an explicitly identified component of numerous data protection regulations, including GDPR, HIPAA, GLBA, SOX among other local and international requirements. Companies managing sensitive data in finance and healthcare have significant obligations to demonstrate compliance.

A sampling of compliance requirements addressed directly by RBAC:

- Centralized management of permissions
- Principles of “least privilege” and segregation of duties
- Transparency of access rights
- Automated reporting and auditing
- Authentication based on data security risk

In an evolving landscape of requirements, the threat of fines for non-compliance are non-trivial.

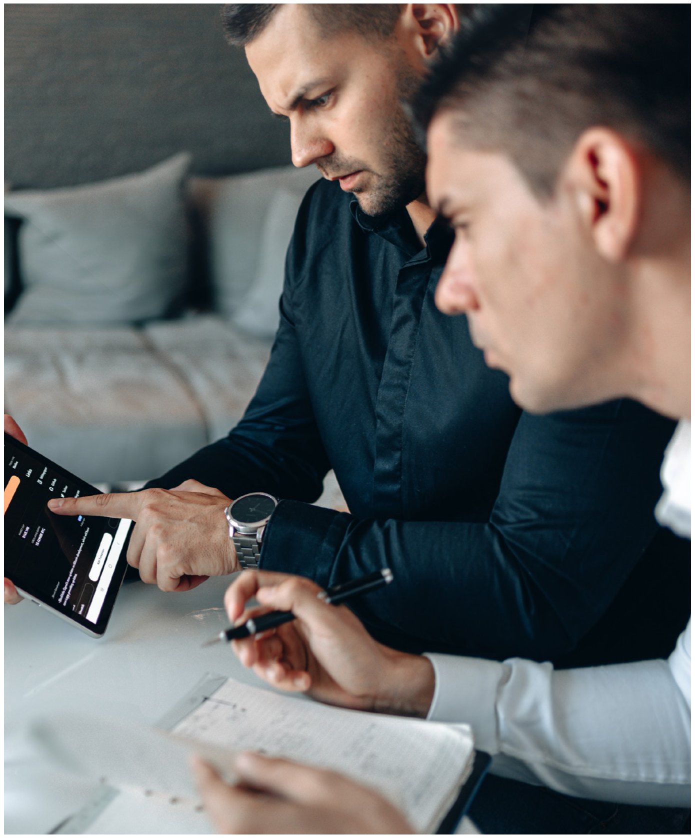
Security Breaches

Finally, there are the obvious risks of breaches and data leakage. The segregation of duties implicit in RBAC reduces the target for hackers and cybercrime. Once outside the permission structure of a hacked user, the attacker is stonewalled. Access to HR doesn't expose finance and vice versa. Nowhere is this more important than with high-value C-Level accounts. Hackers might penetrate a system, but they can't get outside their target's data access bubble.

Nationwide Insurance reports that the average cost of a cyberthreat is over $110K, and there is almost no difference between **the rates of attack between small and large organizations** (less than 1000 employees versus greater than 1000). In 2019 over 200,000 organizations were targeted.

The less visible costs of security breaches that a strong RBAC solution helps avoid are:

- Cybersecurity consulting fees
- Brand goodwill
- Productivity
- Staffing costs
- Business interruption



Conclusion

Benefits to organizations with large numbers of users, high turnover, numerous data sources, and significant investments and exposure in data sharing are significant and, in many cases, can be adequately quantified.

To enjoy the benefits of implementing RBAC controls in Snowflake, it is prudent to understand the benefits of implementing an RBAC model and determine the value in your own business case. Of course, it may not be.
Smaller organizations with tightly controlled data and stable organizational roles may not benefit substantially. So, it is worth assessing the value of an RBAC implementation and understanding the effort to implement–both to identify the benefits described above as well as to assess upfront costs that may not provide the desired return.

The value and the challenges of working with RBAC are real, best implemented from the outset, and unfortunately easy to overlook.

The First Step to Implementing RBAC Controls Is Finding a Modern Technology Partner

Now that you're ready to take command of your RBAC controls, you need a forward-thinking technology partner who can not only integrate with your legacy systems but will build atop world-class industry-standard platforms like Snowflake that keep up with ever-advancing technology. At CoEnterprise, we empower data analytics users globally with superior product know-how, informative training, and optimized implementation. We have more than 100 full-time consultants with extensive data analytics experience who can help you support your data strategy.

Let us guide you on your Snowflake journey.

Click here to learn more about our Snowflake RBAC solution or reach out to learn more and discuss your specific environment.

coenterprise

Created by CoEnterprise

CoEnterprise is a transformative, problem-solving enterprise software and services company. Founded in 2010, we are recognized as a leader in the supply chain and business analytics space, delivering innovative solutions and services that empower people with the resources to analyze their data to make faster, smarter decisions. Fueled by our commitment to people and building lasting relationships, we've helped over 250 customers on over 1,000 projects including some of the most recognized brands in the industry. Visit http://www.coenterprise.com for more information.