protiviti®
Face the Future with Confidence

Enterprise Role Management — Strategic Deployment of Role-Based Access Control in Today's IAM Landscape

In today's identity and access management (IAM) environment, companies seek the next new idea to help govern identity and access lifecycles. Some organizations have had difficulty implementing or maintaining role-based access control (RBAC). Others have been sold on moving to attribute-based access control, use of user-behavior analytics and other new solutions. This begs the question: Are roles still relevant?

The truth is that role-based access models and role management processes are mature, and that, when implemented and maintained properly, RBAC can provide substantial value to organizations.

Roles simplify access request, approval and recertification processes by tying access to business functions within the organization. This paradigm shift to thinking about access in business-friendly terms allows users and managers to understand which type of access they're requesting, approving and recertifying. It also allows them to make fewer, more meaningful access-related decisions. In addition to a streamlined user experience, RBAC can reduce access risk and increase business efficiency.

An effective RBAC environment starts with consideration of the end goal and is not possible without an appropriate enterprise strategy and an accompanying role governance framework.

When organizations do not implement RBAC properly, however, common implementation issues can render the RBAC environment ineffective. Role proliferation and the existence of non-meaningful roles without effective metadata or ties to business functions, as well as stale, unmaintained roles, hurt organizations that are unsuccessful in implementing RBAC. These pitfalls are easily avoided, however, if enterprises undertake a holistic strategy and implement a plan to govern role-based access.

RBAC still has a place in today's IAM landscape, but organizations must be smarter about implementation to avoid these common pitfalls and achieve maximum value. Businesses should avoid rushing into deployments without an enterprise strategy. If they first invest in strategy and governance, then incorporate technology and maintain the environment, RBAC can be an effective solution for access-related issues that numerous organizations face today.

Value First — Establish the Framework

An effective RBAC environment starts with consideration of the end goal and is not possible without an appropriate enterprise strategy and an accompanying role governance framework. The organization must set its RBAC strategy, determine policy and enforcement points, and plan for lifecycle management, technology implementation, and enterprisewide training and awareness.

An organization's RBAC strategy should include considering how to roll out the service across the enterprise. The company must give thought to which business unit, or units, will pilot the service and the order in which other units will roll out the service. Similarly, the organization must balance risk, value and effort when prioritizing application inclusion in roles.

Strategy should also account for the desired goal. Over-proliferation of roles has been the cause of many failed RBAC projects. As a rule of thumb, a typical user may get about 70–80 percent of his or her access from enterprise roles, while the rest may remain discretionary or may consist of exceptions assigned outside of enterprise roles.

Too often, it is tempting to dive straight into role definition, but this approach leads to over-proliferation and uncontrolled and decentralized IAM processes without proper governance. Eventually, this environment becomes unmanageable, resulting in a failed or abandoned RBAC model.

Instead, key stakeholders from both IAM and other groups within the organization should work together to document pain points and key potential wins in an RBAC environment. Doing so allows for the value-first perspective that helps drive successful RBAC implementations.

As the organization establishes its strategy and works on its role governance framework, it must account for establishment or enhancement of role and entitlement taxonomies and metadata requirements, set the approach for role development, and identify key role monitoring and maintenance triggers to inform the upkeep of defined and approved roles.

Key stakeholders from both IAM and other groups within the organization should work together to document pain points and key potential wins in an RBAC environment. Doing so allows for the value-first perspective that helps drive successful RBAC implementations.

Finally, the framework must be compatible with and repeatable in the organization's technology environment. Only once key stakeholders have developed and approved an effective framework should role development commence.

Take Control of Entitlement Governance

Role definition, access request and approval, and recertification processes are difficult and inherently risky without effective entitlement governance. How do a company's users know what access to include in a role and which roles to request, approve and recertify if entitlements are not well-defined?

A central repository of an organization's entitlements is a key foundational element of a mature IAM program. RBAC implementation allows organizations to control their entitlements.

Many companies struggle with ineffective or uncontrolled processes around their entitlements, including significant numbers of entitlements without owners, descriptions and other critical metadata. When businesses establish a role governance framework, they must account for development or enhancement of entitlements governance.

In particular, entitlement metadata requirements must ensure that any entitlements entering the RBAC environment meet the new standards. This guarantees that those role definition, access request, approval and recertification decisions are well-informed and allow the organization to systematically reduce its access-related risk.

The use of roles can drive down access-related risk, promote business efficiency gains, and simplify and streamline the user experience around access request, approval, provisioning and recertification.

Also, organizations should plan and budget for cleanup of existing entitlements, either in advance of or during an RBAC rollout. As part of this effort, the company should understand that, during the rollout, they may identify new entitlements, which must meet the entitlement governance requirements. An effective RBAC environment is predicated on well-governed entitlements.

Build Smarter Roles

Enterprises should see IAM as an internal service organization and the business as the consumer. As such, customer outreach as part of role definition is vital. Roles should simplify the access management lifecycle for the business.

A common pitfall in RBAC deployments is going straight to the data and skipping the business engagement. Role mining tools that allow for data ingestion and perform role mining based on existing access patterns are a commodity in today's landscape. These tools can provide the company with a set of candidate roles but miss the top-down viewpoint, a key component to deriving maximum value for the business.

A hybrid role engineering model consists of top-down role mining via business engagement to understand role functions and access needs, and marries that understanding to the existing data via bottom-up access analysis. This approach allows the defined roles to be closely tied to the needs of the business, thereby allowing the organization to extract maximum business-efficiency gains.

Organizations today are increasing spend into new data analytics fields. Leveraging user behavior analytics and entitlement usage data that the organization may already have can be paired with the above role definition approach to make roles even smarter and more adaptable.

Including Complex Applications (i.e., ERP)

When organizations include applications with a complex security architecture like most ERP systems, they benefit from flexible, task-based application-level roles defined within the ERP system that can be ingested as enterprise entitlements into the IAM tool. This task-based architecture allows organizations to manage the fine-grained permissions within the ERP system, map them to defined enterprise roles and make changes at the IAM system level without having to update or create new permissions in the application whenever the business requests a change.

Without the flexibility of fine-grained, task-based application-level roles defined in an ERP application, implementing an RBAC model can increase risk by granting excessive access to users and can become difficult to maintain over time.

It is also important to include a segregation-of-duties risk review to ensure that all risks are identified and understood before they are included in an enterprise RBAC model.

Maintain the Environment

Organizations should identify key role monitoring and maintenance triggers as part of the process of developing a role governance framework. What if a role has not been provisioned in a year? What about when new applications onboard or when applications undergo changes or are retired? What if people from the same organization keep making the same entitlement requests outside of a role?

Business processes and accompanying responsibilities must be defined for events such as these to enable effective monitoring and maintenance of existing roles. Organizations must develop analytical capabilities to support these processes so that IAM and other appropriate groups receive the data required to make informed role maintenance decisions.

In the absence of effective role maintenance, roles will eventually become stale. More and more roles will have to be defined, and increasingly, ad hoc requests will take place outside of the roles, eroding the business value of an RBAC environment.

In Closing

The use of roles can drive down access-related risk, promote business efficiency gains, and simplify and streamline the user experience around access request, approval, provisioning and recertification. Too often, organizations have pursued deployments without proper strategy and governance. When those implementations have not provided the value promised, companies may not have had the appetite to try again.

By establishing an appropriate enterprise strategy and role governance framework with enhanced entitlements governance, identifying processes to monitor and maintain roles, and leveraging smarter data in the role definition process, companies can expect to take command of their access control environment. A well-governed RBAC environment provides huge value to the business, simplifies user experiences, and keeps audit, risk management and other similar groups happy with controlled and repeatable processes. Isn't that what we're all after?

Contacts

Scott Laliberte
Managing Director
+1.267.256.8825
scott.laliberte@protiviti.com

Matthew Kotraba
Director
+1.703.299.3503
matthew.kotraba@protiviti.com

Eli Hajjar
Manager
+1.571.382.9712
eli.hajjar@protiviti.com