

Top 10 Steps to a Successful Enterprise Role Management Deployment

The explosive growth in global networked communication has created an unprecedented challenge for access governance and access control compliance. Organizations are striving to meet regulatory compliance requirements and enforce information security fundamentals while minimizing downtime and increasing efficiency in their enterprises. This paper overviews best practices for developing and deploying an effective enterprise role management, or role-based access control (RBAC), framework that simplifies the complexity of security administration.

Efficiency Drives Adoption of Role-Based Access Control

The key factor driving organizations to adopt role-based access control is efficiency. The RBAC model helps achieve efficiency in three critical areas:

1. **Efficiency in business process:** Companies must minimize the time it takes new hires to access the applications they need to fulfill their job responsibilities. In addition, they want to ensure employees get the right access. This can be achieved through integration with a provisioning system, or going one step further to integrate with human resources for role-based level assignment.
2. **Efficiency in IT operations:** RBAC gives organizations the ability to manage a lower number of IT entitlements or roles, rather than handle a huge number of granular access requests.
3. **Efficiency in audit and compliance:** RBAC reduces the effort level for all players in the certification process. This is made possible by certifying roles, instead of each application and each entitlement. Standardized access for every job function also facilitates the audit and compliance process.

Developing an Effective Enterprise Role Management Framework

Adopting enterprise-wide role management can be a big change for organizations. There are ten key steps that companies can follow to simplify the process of developing an effective role management framework. These include:

1. Set well-defined goals
2. Conduct a role mining/role engineering assessment
3. Establish role life cycle management processes
4. Set achievable timelines
5. Identify roles and responsibilities
6. Select integrator and technology partners
7. Implementation planning
8. Enlist support center/help desk teams
9. Understand the role management maturity timeline
10. Be prepared for change

1. Set well-defined goals: Define measurable and focused goals, which are agreed upon by all stakeholders involved in the deployment. Roles (and a role project) can be as big or small as deemed appropriate. They can span the entire organization or include just a few key business units or job functions.

Companies should also benchmark themselves with others who have deployed an enterprise-wide role management model. Develop, modify and then document the processes associated with this change. Plan your implementation to include an achievable timeline and the right project participants.

2. Conduct a role mining/role engineering assessment: Begin with an assessment of your organization's current identity and access management (IAM) and role maturity. A role mining exercise can assist you in aggregating, correlating and cleaning existing data. Implement base roles for new hires and contractors (broken out by BU or job function). Create application/IT roles where you have users who cross organizational boundaries but need similar access, so you can manage sensitive privileges within some of your applications. Consider creating a transfer role to minimize collector access yet still keep your resources functional while they transition job functions. Use the top/down approach if you have a very accurate HR system/job title and codes.

3. Establish role life cycle management processes

A role's "life cycle" is the same as a user's "life cycle." It gets on-boarded, transfers, changes, affects others, gets promoted, evolves, or terminates. Define and document the business processes for role life cycle management and then map that process to technology to automate. Automation is key to preventing stagnate or inaccurate roles. Processes should be identified for:

- Creating new roles
- Managing role changes (including impact analysis)
- Disabling or terminating a role
- New certifications – add new certifications to your calendar and include role owner certification and role entitlement certifications.
- Assigning role ownership – a standardized written policy is the key to success.

4. Set achievable timelines: The length of a deployment is closely tied with the maturity of IAM in the organization. Other factors that help in determining the timeline are size of the organization, the scale of project and the resources assigned for the implementation. Based on these considerations, a deployment could take between six to 18 months.

5. Identify roles and responsibilities: A basic team should consist of:

- a. Business process owners and stakeholders
- b. IT application owners
- c. IT implementation team
- d. Internal risk management team
- e. Business process analyst
- f. Technical writer

New actors will often be introduced beyond the normal application owners, process owners, data owners, and business owners that you may already have identified. The chart below depicts some typical roles and responsibilities:

New Actors	Responsibilities	Skill sets
Role Administrator	<ul style="list-style-type: none"> • Create, modify, decommission roles • Generate reports 	Application administrator or possibly someone from your access administration team.
Role Engineer	<ul style="list-style-type: none"> • Reviews role consolidation & impact analysis reports and submit recommendations to role governance committee • Schedule recurring role composition reports and submit recommendations to role owner for review and certification 	Business process analyst with great verbal and written communications; someone who is highly organized.
Role Owner	<ul style="list-style-type: none"> • Initiate request for new roles or modification of roles • Responsible for role approval and role certification • Could be business or IT 	Has the greatest degree of understanding about the role and the entitlements to the role; Likely the person the auditors would deem responsible for the associated business process and/or data.
Roles Governance Committee	<ul style="list-style-type: none"> • Review role creation, modification and decommission requests (maintenance and aging) • Assign, replace role owners • Periodic review of roles to make sure they still map to business processes 	Mix of business and IT; consider a leadership position with reporting responsibility to CFO and CIO

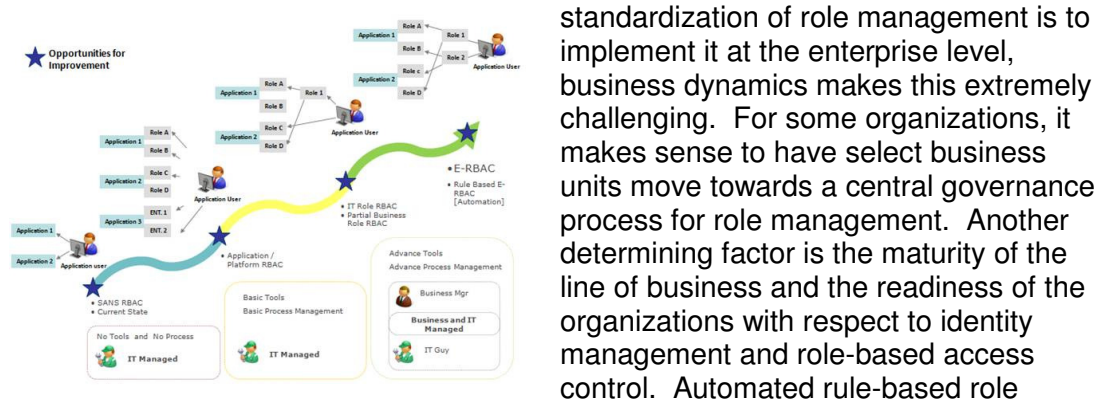
6. Select integrator and technology partners: Selecting the right systems integrator and technology vendor partner is an integral part of the process. Review the system integrator’s role development and implementation methodology before you make your selection. And from this point, create a seamless communication channel between the system integrator and the business process analyst. Together, they map the road to automation.

7. Implementation planning: Planning is the most critical factor. Consider the following steps:

- ◆ **Phase the rollout.** Phased deployment delivers incremental wins and demonstrates ROI.
- ◆ **Pilot the change.** This is a substantive change for the organization and how they think and administer people. It has to be tactically approached so you can achieve your strategic goals.
- ◆ **Recruit a business process analyst** to the team. They can build your Visio diagrams. Documentation and defined process reflects standardization, which is important for ongoing compliance. It also makes the auditors happy.
- ◆ **Measure, reassess, and report.** Document the number of entitlements, accounts, users, dormant accounts and sensitive entitlements within your organization. Then, take these metrics again and again as you implement the roles and associated certifications.
 - ◆ Auditors like the reduced footprint of data access
 - ◆ Executives like the return on investment
- ◆ **Develop naming conventions.** Work with the implementation and governance teams to develop a role naming convention that makes sense to the end users and the auditors.
- ◆ **Measure ROI:** Evaluate the ROI in terms of managing, provisioning and deprovisioning in your certifications. In one of the implementations done by Simeio Solutions, of 10,000 employees, 66% were granted job function enterprise roles. This resulted in a reduction from 340 individual roles/entitlements to 25 and a reduction in the average number of roles assigned per user from 40 to 4. This took just 60 days.
- ◆ **Consider these integration points:**
 - Role management system + identity management system
 - Role management system + access request system
 - Role management system + help desk system
 - Identity management system + HR system (and whatever other enterprise system holds contractor data)
 - Governance, Risk and Compliance (GRC) systems
- ◆ **Get the communications team involved.** They can help you develop the message and communicate it in a way that is appropriate to your organization. Deliver the information via as many different methods as you can (email, intranet, recorded training modules, policy and executive messages).
- ◆ **Build a full array of UAT cases.** Include role owners, managers, end users and your role administration team.

8. Enlist your support center/help desk team. You need to work closely with them to define sustainable support agreements and processes. This team is in a unique position to be able to market your message.

9. Role Management Maturity Timeline: While, the desired end state for standardization of role management is to implement it at the enterprise level,



business dynamics makes this extremely challenging. For some organizations, it makes sense to have select business units move towards a central governance process for role management. Another determining factor is the maturity of the line of business and the readiness of the organizations with respect to identity management and role-based access control. Automated rule-based role

provisioning is the zenith --business and IT roles assigned to a user’s profile based on certain authoritative source attributes. For example: If Center A, Location B, Job Code C then assign role “Consultant”.

10. Be prepared for change: Last but not least, be prepared for change. With an enterprise role management model, your organization and business processes will change significantly. But, when you look at the exponential decrease in turnaround time and costs which translate into immediate ROI, it is well worth the effort!