

A Methodology for Implementing Continuous Roles Based Access Governance

MARCH 2009

Executive Summary

The management of user access has long been an extraordinarily complex challenge for organizations. Central to this challenge is the concept of creating defined user roles. Used correctly, roles provide a means of simplification, and allow organizations to tailor enterprise access to the needs of the business. The result, in a perfect world, is greater IT operational efficiency, business agility and improved security through a set of preventative controls.

In practice, nearly every organization has struggled with how to define and implement access roles that will meet the objectives of the business. Because of this, the promise of IT administrative operational efficiency and improved security has remained out of reach. In many cases, role management at the application or information resource level has resulted in role proliferation, which has actually led to increased complexity and inefficiency. Adding to this problem is the ad hoc nature of how roles are managed over time. With the amount of change that occurs to access within a typical organization, roles can become ineffective if they are managed in a static fashion (on a project basis). The solution is to take a completely different approach to the creation, implementation and maintenance of roles through a business-centric, continuous process for enterprise role-based access governance.

First generation Identity and Access Management (IAM) solutions represented a significant investment for organizations that attempted to simplify identity administration within IT through technical roles and roles-based access control (RBAC). Roles were typically constructed from a technical perspective and applied within IT resources at a coarse grained level, which created an account or group level view of access. As a result, gaps remain in organizational readiness for continuous role based access governance. While this approach helped streamline the IT security administration of access, it did not provide the visibility needed to meet regulatory compliance and mitigate access related business risks. The most common hurdles organizations face today include:

- Roles definition and ownership exists at the technical information resource level, creating user access data silos that make it nearly impossible to get a unified business view of a user's access across the enterprise.
- Access approval, review and certification are made at a technical level, not through the business stakeholders where the context for what is appropriate for user access exists.
- Roles based on application-centric view of access precludes data-centric access views.

To move beyond the broken processes and inefficiencies of today, organizations will need to invest in a continuous and automated process of role-based access governance. Critical to driving returns in this area is solving the "language gap" problem that many corporations face. Business stakeholders do not speak the language of technical roles and entitlements, and as such lack the ability to meaningfully communicate with IT stakeholders to properly request and govern access. The steps required to implement such a process are not trivial, but are within the reach of all organizations:

- Clear definition of focus, goals and objectives for enterprise business roles.
- Setting expectations with and getting buy-in from the business by demonstrating future benefits.
- Building an automated framework that enables a continuous process for managing roles, beginning with design, discovery and engineering followed by a set of processes for change management and maintenance.
- Implementing business roles and an appropriate hierarchy of roles that extends down to the technical view of access and granular entitlements, including provisional roles implemented within user provisioning systems.

To move beyond the broken processes and inefficiencies of today, organizations will need to invest in a continuous and automated process of role-based access governance.

The pressing need for better operational efficiency for IT security teams as well as the business have become one of the key drivers behind leveraging enterprise roles to improve access delivery and change management.

- An automated rules based approach for continual access assurance, with the ability to run rules for “what-if” scenarios during the role design and engineering phases as well as enabling preventative control for use during access change management.
- Closed-loop validation processes that ensure access right violations have been remediated and change management requests have taken effect in target systems.
- Leveraging metrics and analytics to provide role owners in the business with decision support to help them maintain the effectiveness of roles over time.

Organizations that adopt roles based access governance will be rewarded with simplified processes that lessen organizational burden, improve IT operational efficiency, reduce overall risk and enable sustainable, auditable compliance.

Laying the Foundation: Implementation Goals and Objectives

In years past, improved security was generally the primary driver for most organizations. While pure security posture will never be a non-goal, it is more often taking a back seat to compliance and risk concerns in today’s highly regulated business environment. Examples are numerous, and include:

- Financial services organizations with segregation of duties (SOD) requirements under Gramm Leach Bliley (GLBA).
- Healthcare organizations, who are subjected to similar requirements in the Health Insurance Portability and Accountability Act (HIPAA).
- Energy and Utilities companies, who are subjected to segregation of duties requirements in FERC and NERC guidelines.
- All public companies, who must demonstrate internal control over financial reporting, including access controls for segregation of duties and the elimination of orphaned accounts in critical financial reporting systems under the Sarbanes Oxley Act.
- Government agencies, with access governance compliance requirements under FISMA and the OMB Circular.

Operational risk management can be a major driver for a role based access governance project, as well. This is a particular concern for financial services institutions like Societe General where a rogue trader was able to leverage inappropriate access, created by an entitlement drag that occurred when this person changed job roles from a back office to front office function, to manipulate back office systems in an effort to conceal losing positions that he had taken, costing the bank several billions of dollars in loss.

The pressing need for better operational efficiency for IT security teams as well as the business have become one of the key drivers behind leveraging enterprise roles to improve access delivery and change management. As a long-time goal of all identity and access management solutions, operational efficiency is back in full force as a key requirement with shrinking budgets and organizations being asked to do more with less. Role based access governance is the key to leveraging existing investments in provisioning systems and expensive IT administrative resources because roles creates a common language for how user access is expressed that can be leveraged by both business and IT stakeholders for requesting, changing, reviewing, and certifying access.

While all three benefits will follow from any successful role-based access governance project, careful planning can allow organizations to tailor their efforts, often starting with quick wins to drive progress in one area more quickly than the other two. As seen in the next section, getting executive buy-in and demonstrating quick results will be a critical success factors. Diligent up front planning will pay huge dividends down the line. One of our key goals will be to provide business insight into access entitlements through a role-based view of access. Business stakeholder ownership for roles is critical, and ensuring that up front simplifies the matter.

Using roles also enables a preventative control at the point of granting or changing access, which proactively eliminates compliance violations and mitigates access risk.

Herein lies one of the key distinctions between traditional access control and access governance. Access governance is based on a set of business processes and policies. Access control is really about the enforcement of technical authentication policies and authorization policies. While technical roles may be useful in defining these policies or grouping entitlements, the real value of roles is realized when business roles are crafted to operate at the governance level, based on the access required for specific job functions and/or business processes. These business roles simplify access on-boarding, change management, review and compliance.

Focus: Where to Start?

Given the role proliferation many large organizations have seen, it can be tempting to attempt to tackle far too big a segment of the problem space at once. Boiling the ocean has never worked, and it will not work in the implementation of role based access governance. Instead, organizations should view the task at hand through a pragmatic lens. There are generally some low effort, high benefit areas that can be addressed first.

It is often the best approach to start with the area of greatest pain for the business. An examination of access requests will typically shed light on which business units have had the most difficulty with access delivery. While it may sound counter-intuitive to start with a business unit that has the most challenges with getting access in a timely fashion, this approach will demonstrate the business value that can be derived from using a role-based approach for governing access. Look for a business unit that experiences a high degree of user churn and numerous access compliance violations on an annual basis. Using roles will speed up access delivery, ensure the accuracy of the access delivered and simplify access change management, ensuring that the IT organization meets its service level agreements with the business. Using roles also enables a preventative control at the point of granting or changing access, which proactively eliminates compliance violations and mitigates access risk.

Setting Expectations and Getting Buy-in

A strategic, business focused approach to role-based access governance is impossible without buy-in and active participation from business stakeholders. When it comes time to map roles to job functions or business processes, input from business stakeholders is essential. Demonstrating the potential benefits of role management to these stakeholders up front is critical to securing their buy-in.

If compliance is the primary objective for the organization, examine the specific requirements that consistently cause audit or regulatory issues. Addressing the huge overlap within IT compliance frameworks can alleviate a sizable set of pain points at once. For instance, a particular set of segregation of duties conflicts may cause regulatory compliance issues with SOX and FERC guidelines as well as best practice security issues with the ISO and NIST security standards. Targeting resolution of these SOD conflicts through role based access governance can produce measurable return on investment and would be an excellent starting point.

Resolution of audit requests themselves can also prove a significant drain on organizations. Business focused roles will simplify compliance. When starting with a specific compliance requirement, roles provide up front preventative controls. When an entitlement is granted, roles provide the business context necessary to spot a potential compliance violation up front. The result is fewer compliance violations downstream, which translates to greater operational efficiency and lower audit costs.

Finally, organizations should define a shared set of critical success factors for roles. Typically, those success factors include:

A hybrid role approach that performs both levels of analysis and combines the results is by far the most powerful.

- Agreement on how roles will be used in the organization.
- The establishment of a common language of access, expressed in the context of a job role, functional role or process role.
- Determine the level of granularity for roles (coarse or fine grained).
- Understanding that not all access needs to be explained through a role (out of role entitlements are appropriate and OK).
- The establishment of measurable metrics that create key performance indicators to determine the effectiveness of roles and aid in on-going role maintenance.
- Agreement on the ownership and management of roles.
- Identification of future benefits and proposed expectations.

With those success factors clearly defined, entities can move forward with shared expectations and vision.

A Best Practices Hybrid Approach to Roles

Traditionally, user access has been defined by technical roles (provisioning roles, application roles, etc.). These roles generally make sense in a specific technical context, but are often confusing when applied to a broader business context. For example, I may have access to the “Approve Purchase Order” function in the ERP system, but that specific entitlement says nothing about my functional role in the organization. The business context that is missing would tell a stakeholder or auditor why I have this particular access. A more meaningful business role, such as “Accounts Payable Clerk” provides the necessary clarity to then understand if the entitlements are appropriate for the functional or process role.

To define the roles necessary for an organization to model its operations, there are two approaches an organization may take – top down or bottom up. Both are necessary, but for maximum efficiency neither by itself is sufficient. A hybrid approach that performs both levels of analysis and combines the results is by far the most powerful.

The bottom up approach provides a view of access reality as it shows enterprise access as it exists today. This view of access reality is accomplished by role mining, which mines entitlements across enterprise information resources creating roles through logical grouping based on patterns and similarities. Clearly, automated role mining is an essential tool in this battle, as this can be a massive undertaking. Advantages to this method include the volume of data that can be collected, aggregated and then correlated, as well as the ability to automate the entire process. But the accuracy of the user access data can be role mining’s biggest weakness. While it shows a picture of access rights in the organization as it stands today, it ignores potential areas of improvement and organizational shortcomings. Just because a user has access to an information resource doesn’t mean it’s required for their particular job role. They may have dragged the entitlements with them from a previous role. Relying on mining alone can create roles where access isn’t necessary or can create toxic combinations of access that will result in compliance violations.

Out-of-role entitlements are not necessarily a bad thing, and can be used to keep simplicity in the overall model while still accounting for discrepancies as they are relevant.

A top down approach to role design engages key business stakeholders to map out job functions within the organization and the entitlements to information resources necessary to perform the function. The major benefit to this method is the simplicity, and logical nature of the model that typically results. Where this approach falls short, however, is the inability of business stakeholders to account for every nuance of the business. Invariably, businesses are more complex than our ability to model them conceptually. Additionally, human perception is often different than reality, and it is not uncommon for role designers to learn that business processes are frequently not being followed as perceived.

The best approach is to work with business stakeholders to design a set of business roles and then reconcile them with the access reality in order to understand what access was overlooked or not necessary. A hybrid approach is able to compensate for the shortcomings in either singular approach with the strengths of the other. In practice, an organization can utilize automated methods to gather data about who has access to what in the current environment and establish a view of reality. Bottom-up role mining against this view of access reality can yield a set of technical roles or improve existing ones, while a top-down focus on creating business roles layered over the technical roles, can yield a role hierarchy that effectively delivers a bridge from the business view of access to the technical view.

Typically, an organization will embark on a process of role engineering, leveraging metrics to provide decision support to refine the candidate roles that have been created. Considering alternate scenarios and testing will generate valuable insight into the viability of the model. Are the roles too finely grained? Are they too coarsely grained?

Organizations need to resist the temptation to explain all access in the confines of a role. Out-of-role (OOR) entitlements are not necessarily a bad thing, and can be used to keep simplicity in the overall model while still accounting for discrepancies as they are relevant. For example, when an application developer from one business unit is temporarily assigned to another business unit, out of role entitlements can be granted that are outside of the normal role. It wouldn't make much sense creating a specific role for this event-driven scenario as it is temporary in nature. Using OOR entitlements to manage access requirements that are out of constraint is the right approach.

A Continuous Process: The Key to Full Role Lifecycle Management

One expectation that is absolutely critical to set is the reality of the need for an ongoing process of role lifecycle management. Role based access governance is not a one time project as roles are not static but rather dynamic because they must change as the business changes. Effective role management requires a continuous process for monitoring and managing to ensure on-going effectiveness. For example, a primarily business-to-business organization seeking to divest a consumer business with telesales will achieve greater efficiency in doing so with continuous lifecycle role management. Changes in role membership are made pro-actively at the time of business process change and are fed back to ongoing role design and engineering. Under an ad hoc, project based model, access changes, including the de-provisioning of consumer telemarketing roles, would take significantly longer to take place, if they do take place at all.

Another example of the benefits of a continuous approach occurs when a business process changes, for instance due to a new regulatory requirement. An organization that tracks metrics associated with roles affected by the change might notice declining role membership, which would serve as decision support to be fed back into the front end of the process – guiding more intelligent and efficient role design.

A successful role based access governance implementation, therefore, must introduce an iterative and continuous process.

This highlights another key benefit to the continuous lifecycle approach -- it allows organizations to take advantage of what is learned through the discovery process. It is quite a common experience in successful role based access governance implementations to discover numerous realities that were unknown at the beginning of the project, such as:

- Technical roles that seem distinct at first, but upon further analysis are duplicates.
- Classes of users grouped into a common bucket that actually have distinct business responsibilities and require distinct access.
- Unclear regulatory requirements, or segregation of duties issues that had gone unnoticed due to a lack of oversight.
- Changes in business entity structure that were not accounted for in entitlements.
- Changing information resources that were not accounted for in entitlements.
- Changing regulatory requirements driven by external factors.

It is only through a continuous lifecycle of roles management that these unknowns can be accounted for accurately. Under the “boil the ocean” scenario, if an organization attempted to deal with every changing requirement as it was uncovered, the project scope would creep out of control. The result would be budget and timeline overruns, and could potentially jeopardize the success of the project altogether. This is precisely what caused many large scale first generation IAM implementations to fail. A successful role based access governance implementation, therefore, must introduce an iterative and continuous process. Such a successful process generally embodies the following steps:

Role Design and Discovery: perform top down modeling of in scope business processes as well as bottom up analysis of technical entitlements. Utilize goals and objectives to guide areas that require more detailed analysis. Design constraints and functional roles. Don't use HR titles, instead use business process roles.

Manage Exceptions and Variables: through out-of-role entitlements.

Dynamic Access Rights Remediation: to remedy violations of policies.

Access Request and Change Management continuously manages change by enabling the business to request access using a roles paradigm that applies the proper access control policies at the point of granting or changing access.

Regular Review and Certification of Roles: utilize the business context provided by roles to simplify periodic certification and review.

Metrics Management and Maintenance: utilize rule based automated analysis techniques to determine whether role key performance indicators are within tolerances. Utilize the results of this step to drive the access analysis for the next iteration of the cycle as a feedback loop to drive continuous process.

The net result is a framework that is continually adapting to changes in the business operating environment, internal corporate structural changes and changes in information resources. The result will be improved risk and compliance posture and streamline operational efficiency, as well as increased business agility and efficiency.

Automated rules can be used to proactively spot access governance issues and can save an organization significant risk exposure associated with entitlement drag and segregation of duties that may occur when a user's relationship with the organization changes.

Accounting for the Hierarchical Nature of Roles

Modern organizational structures in large corporations can be quite complex, and are often several layers deep in terms of business entities. An accurate model of organizational hierarchy can greatly simplify role based access governance. Roles and sub-roles can be utilized to simplify ongoing administration, and can greatly assist with managing organizational change.

For example, a large bank may have a role for retail branch associate. In this job role the person sells various banking and financial products, but based on the location of the retail branch their access may vary as the bank is allowed by regulators to sell life insurance in New York but not in California. Differences in access due to regional location and specific state level compliance requirements can be accounted for in a sub-role. In this respect, access delivery and change management is far simpler.

It is important to exercise due care not to utilize hierarchical roles when they are not warranted. For example, purchasing managers would require several entitlements, including the ability to create purchase orders. If there is only one specific purchasing manager in Chicago who also requires the ability to accept deliveries, it is not necessary and actually less efficient to create a sub-role. Instead, out of role entitlements should be used for their intended purpose – to account for unique situations such as this one.

Careful construction of sub-roles can minimize out of role entitlements, which will simplify ongoing operational overhead. This pays dividends in a few key areas, including on-boarding, de-provisioning certification, audit and organizational change. With carefully constructed roles and sub-roles, the business context allows business line stakeholders to efficiently grant access privileges. Annual or quarterly certification can be done in an automated fashion at the role or sub-role level, greatly minimizing the overhead associated with the compliance task. Compliance audits can also be performed, reducing audit costs across the organization and increasing compliance posture as audit departments can free up resources by auditing a role or sub-role as opposed to individuals and focus on other high risk audit areas.

Automation and Continuous Control Through Rules Management

The deployment of automated rules is a critical component to driving an efficient role lifecycle management in a role based access governance framework. Automated rules can be used to proactively spot access governance issues and can save an organization significant risk exposure associated with entitlement drag and segregation of duties that may occur when a user's relationship with the organization changes. The advantage of rules in a role based access governance framework is the level of abstraction and business context afforded therein. Business stakeholders can manage compliance and audit processes at a business level, without needing to understand the intricacies of low level technical entitlements or policy controls.

It is not uncommon for organizations without a strong role based access governance process in place to have three to as much as ten times more roles than users if they are trying to manage roles at the technical or application level.

A unified, business-centric view of access also provides the advantage of efficiency when implementing automated rules. Rules can be run against a set of roles, as opposed to individual users. As a result, processing is far simplified, and requires significantly less overhead. Related to this is the other major advantage for managing rules at a higher level is the level of heterogeneity available to rule constructors. It becomes possible to write rules that look across disparate systems and entitlements, and across silos. For example, a financial analyst who has the ability to request a bonus in the HR system may also have access to approve the request in the Payroll application. Managing this at an individual application owner level is quite difficult as there is no automation for user access data correlation. For organizations that have an IAM system in place, if the user provisioning system is not administering access for both applications it will be blind to the SoD conflict.

The major advantages here are in operational efficiency as well as the very nature of the controls being constructed. Automated rules can be fired dynamically, and therefore make the control preventative in nature, as opposed to a detective control that may be used after the fact in an audit process. The same principle also aids recertification. By recertifying at the role level, the process becomes far simpler and more efficient.

Change Management – Leveraging Analytics for Simplified Maintenance

Throughout the role based access governance lifecycle, metrics, analytics and reporting are a critical component to drive intelligent decision making. Throughout the role design process, metrics and key performance indicators can be useful indicators as to the quality of the roles in use.

For example, research has shown that most organizations reach an optimal level of efficiency when their role count is no more than 10% of the total number of all users. It is not uncommon for organizations without a strong role based access governance process in place to have three to as much as ten times more roles than users if they are trying to manage roles at the technical or application level. Clearly this represents an excessively complex model that can only lead to compliance issues and operational inefficiencies.

While it is impossible to know the ideal ratio of employees to roles for a given company (and this hypothetical number clearly varies across companies, industries and geographies), setting goals such as the 10% threshold is a valuable way to measure progress. On the other end, if within a particular role, a high percentage of users have an out of role entitlement, there may be a role that is missing that needs to be modeled. Regardless, organizations should seek to make incremental progress towards their goal.

Optimization is an iterative process, and the goal should be continually adjusted as more is learned.

To measure role quality, organizations should examine the following metrics:

- How well does the role simplify view of access?
- Is the role easily understood?
- Number of people it describes in some way.
- Number of granular entitlements eliminated from the vocabulary.
- How accurate is the role?
- Do members of the role actually use the access?
- How many out-of-role entitlements exist for all members?
- Establishing role membership constraints/assertions.
- How unique is the role?
- Do we see other roles with similar user sets?
- Do we see roles that describe similar access?
- Could the role be expanded?
- Are there additional users or entitlements that should be considered?
- How many compliance violations does the role have on a cyclical basis?

It may also be useful to quantify role quality, and to score role quality according to a set of metrics, such as:

- Number of users
- Number of groups
- Number of entitlements
- Number of out of constraint users
- Number of missing required entitlements
- Membership growth rate
- Membership change rate
- Role change rate

Doing such will provide measurable, quantitative standards to judge the effectiveness of roles in the organization, and can be used to drive ongoing improvements in processes.

Optimization is an iterative process, and the goal should be continually adjusted as more is learned.

A role-based access governance framework enables technical provisioning roles to be defined for a user provisioning system, while layering business roles above the provisioning roles.

Extending Technical Roles To Business Roles

A continuous role based access governance process should result in simplified user provisioning processes. To achieve the true benefits of this result, a bi-directional integration with user provisioning systems is essential. A role-based access governance framework enables technical provisioning roles to be defined for a user provisioning system, while layering business roles above the provisioning roles. Thus, business context is maintained in the business roles while provisioning context, which is limited by the scope of user provisioning deployment, is maintained in the provisioning role. As a result, access change management becomes seamless and more efficient and the overall role model is easy to maintain.

When changes occur at the user provisioning level, the access governance framework is easily updated. Moving in the other direction, changes made at the business role level in the access governance framework can automatically propagate down to user provisioning.

The net result is increased business agility through streamlined change management. Seamless, bi-directional automation provides the opportunity to govern access according to the needs of the business – not according to the technical constraints of the information assets being accessed.

Summary

Role based access governance, when performed as part of a continuous lifecycle, presents a significant opportunity for organizations to leverage investments in existing technology to simplify operations by putting complex, IT entitlements into a clear and understandable business context.

Getting to the end state requires careful planning, expectation setting, and a combination of top down planning and bottom up analysis. Organizations should start with quick wins – areas of greatest pain or low effort and high reward. Automation, in the form of rules based analysis, metrics and reporting, is a critical component, and data gleaned through the analysis of ongoing efforts must be used in an iterative fashion to guide future efforts. Organizations that are able to successfully do so, and put into place a framework for self-optimizing, continuous role based access governance processes will achieve greater operational efficiency, improved risk and security posture.

For additional information about Aveksa solutions visit us online at www.Aveksa.com

ABOUT AVEKSA

Aveksa provides the most comprehensive, enterprise-class, access governance, risk management and compliance solution.

Aveksa automates the on-boarding, change management, monitoring, reporting, certification and remediation of user entitlements and roles; enables role discovery and lifecycle management; and delivers unmatched visibility into the true state of user access rights. With Aveksa, business, security and compliance teams can effectively collaborate and enforce accountability.

Our growing customer base includes leading global Fortune 2000 organizations in financial services, healthcare, retail, transportation and manufacturing. For more information, go to www.aveksa.com.

Aveksa

Aveksa Inc.

265 Winter Street
Waltham, MA 02451
www.aveksa.com

© 2009 Aveksa Inc. All rights reserved. Aveksa and the Aveksa logo are registered trademarks of Aveksa Inc. All other company and product names may be the subject of intellectual property rights reserved by third parties. 01/08