

# Business Driven Access Management and Governance: Simplifying the Delivery and Governance of Access Throughout the Enterprise

NOVEMBER 2009

## Executive Summary

As organizational demand for user access has risen dramatically, the challenge of managing access change has increased exponentially due to the fragmentation of information systems and resources. From a business perspective, users require access to what they want, where they want it, when they want it such that business operations are not slowed or blocked altogether. From an IT perspective, operations and security personnel are challenged to field and fulfill requests in a secure and compliant fashion. Achieving these goals in a highly distributed and fragmented environment, and mapping that access to underlying information resources, is a persistent challenge. As a result, IT security and operations can become a bottleneck to the completion of the access fulfillment process that businesses cannot afford.

*Progressive organizations are adopting a new process for how access is requested, approved, fulfilled, validated and remediated.*

*The net result is simplified and streamlined processes, and greater operational efficiency. In effect, this is an opportunity for IT to allow the business to operate in a more agile, less constrained fashion.*

IT organizations have attempted to use various tools to keep pace with this increase in change and complexity. The lack of an automated process results in an unmanageable barrage of email and phone requests from the business. These approaches, like nearly all manual approaches, are fraught with disorganization, and are prone to costly errors. Making matters worse, policy and governance requirements are not very well understood by the IT organization and are often applied in an ad hoc and manual fashion, resulting in audit violations or introducing access related business risks.

Some organizations have tried to improve on manual processes to automate access delivery and governance. Such approaches include attempts to use technologies such as user provisioning or IT service management (e.g. helpdesk) for automation. These approaches, while providing some degree of increased efficiency, did not effectively work for the business. They were never designed to, and instead, were built for IT personnel to automate IT security administration processes. User provisioning, one such tool, took a distinctly bottom up approach, with a focus on applications, and the automation of account creation in the access fulfillment process. As a security administration tool, it proved to be effective at reducing the number of IT transactions for populating identity information into application user directories, but it was not extensible to the business.

Progressive organizations are adopting a new process for how access is requested, approved, fulfilled, validated and remediated. Such an approach can abstract the complexity that IT deals with, to simplify the process to the point where the business can be more autonomous and more successful. A business driven approach bridges the access language gap between how business stakeholders want access described and the technical language IT uses for fulfilling access. This new approach is far more scalable, and integrates into existing service and identity management infrastructures to provide end-to-end automation.

This approach ultimately results in a drastic reduction in IT related cost and complexity. Under an automated model, rules can be checked in real time at the point of request or change, removing the traditional IT operations and security bottleneck. The net result is simplified and streamlined processes, and greater operational efficiency. In effect, this is an opportunity for IT to allow the business to operate in a more agile, less constrained fashion.

## The Business of Access Request and Change Management

Access governance and delivery is evolving. The process of requesting, approving, fulfilling and validating access is becoming a business service that embeds policy administration that makes compliance transparent to the requestor. And for good reason: old methods simply aren't scalable. Aveksa finds that to meet access demands by the business, IT security organizations are staffing 1.5 full time identity administrators for every 1,000 employees. Scaling to meet increasing demands by adding headcount will drive costs higher and is still a manual, error prone approach that frequently leads to compliance violations and a loss of accuracy in the request and change management process. Security and compliance, long viewed by the business as necessary evils, were costly distractions in prosperous economic times. In an era of shrinking budgets and uncertainty, efficiency can be driven only by taking a preventative approach to security and compliance, by embedding control directly into the business process itself, making compliance a convenient by-product of a diligent and efficient process.

*In an era of shrinking budgets and uncertainty, efficiency can be driven only by taking a preventative approach to security and compliance, by embedding control directly into the business process itself, making compliance a convenient by-product of a diligent and efficient process.*

To drive this layer of efficiency, however, it is important to first realize the limitations of current approaches, which include

- Manual processes using email and phone requests
- User provisioning technologies
- Simulated provisioning, using IT Service Management and Service Resource Management technologies

### Manual Processes

Manual approaches have historically attempted to manage the process of requesting and fulfilling access through tools such as email and phone calls. These approaches to access delivery and governance largely fail due to a communications gap caused by a lack of relevance and context. For instance, a business stakeholder requesting access to an ERP system in an email would often receive a follow-up phone call from IT operations or security, asking which specific type of ERP access is required. This process may go back and forth through cycles of clarification, wasting valuable time and resources for all affected.

### User Provisioning

User provisioning was built with a workflow and user interface for IT security administrators, intended to provide a scalable approach to populating identities in different application directories to automate the account creation process for access fulfillment. Provisioning workflows were designed for security administration. The technical descriptions used to express access (e.g., accounts, groups and entitlements), and the user interface, were designed for use by security administrators. As a result, it is difficult to extend this view to the business and have them be successful because context is not business focused, and because it does not administer all applications.

The Burton Group expands further, saying, "user provisioning tools rarely achieved the breadth or depth of application coverage to provide sufficient certification data to satisfy auditors and regulators.<sup>1</sup>" In terms of context, cumbersome and overly technical interfaces, and an inability to translate granular entitlement data into business friendly views of information limit the ability of business stakeholders to properly understand the information presented to them.

---

<sup>1</sup> "Access and Identity Governance: Leading to Transparency and Visibility?" Gerry Gebel, Burton Group, July 13, 2009

*“Fully automated connections to user provisioning are not a reality for most enterprises.”*

Gartner expands on relevance issue for user provisioning systems with limited deployment to a sub-set of application systems, saying “fully automated connections to user provisioning are not a reality for most enterprises. Bridged connections of mixed manual and automated process workflow can extend provisioning usability and value.”<sup>2</sup> What Gartner’s statement alludes to is a broader shift underway in the market towards full, end-to-end automation. User provisioning will not ultimately solve the access request and change management challenge due to the fact that it is not integrated with every application and information resource (e.g., data, files, file shares, hosts, etc.), therefore it is incapable of providing end-to-end automation on its own.

A large organization may deploy a user provisioning system to ten to twenty applications where the highest change in user access occurs. That may leave hundreds of enterprise applications managed in silos by disparate application administrators. Access requests for each of these applications requires separate administration interfaces and technical expertise, and the fragmentation and complexity presented as a result leads to huge degrees of operational inefficiency and error.

### **Simulated Provisioning**

Simulated provisioning, using ITSM solutions repurposed to do access governance and delivery, suffers from many of the same problems inherent in user provisioning, as well as some problems of its own. SRM solutions, which can provide a unified means to request access, may have business friendly user interfaces, but the request itself is often freeform — e.g. “give this person access to the CRM system for marketing purposes” — and doesn’t provide the relevancy for the access to be selected that is appropriate of a specific job/functional role or business unit. As a result, there is an access language gap. This may result in iterative and inefficient access discussions, such as what happens when a request is made from a service catalog that contains all of the applications in the enterprise. The IT operations team will generally need clarification as to the specific access required, wasting valuable time.

Access policy enforcement was never a design consideration for ITSM solutions. As a result, companies relying on this approach to access, rely on good judgment and manual application of controls. In practice, such organizations are largely blind to potential compliance violations that can be introduced in the access request and change management process.

### **Consequences**

The consequences of these ad hoc and manual approaches are continually validated by various external surveys and data gathering activities. Deloitte, in its 2008 study of internal and external audit findings, has illustrated such problems.<sup>3</sup> Violations of compliance with procedure around access control are up to 30% from 28% since 2007.<sup>4</sup> In an era of increased regulatory scrutiny and massive internal and external audit efforts, one would expect drastic improvements in control. Instead, the results indicate minor improvements (such as a reduction to 30% incidence from 35% for segregation of duties violations) at best, and degradation at worst. This can be attributed to inefficiency in the access request and change management processes, and the resulting inability of organizations to embed control at the point of request or change.

---

<sup>2</sup> “Automation Hype vs. Manual Reality With User Provisioning,” Gartner, 27 May 2008

<sup>3</sup> 2008 Global Security Survey, Deloitte

<sup>4</sup> 2007 Global Security Survey, Deloitte

From an operational efficiency standpoint, implementing preventative checks at the front end of the process saves valuable resource cycles, as less time is wasted fulfilling requests that may violate policy. Audits also become far more efficient through the implementation of an access change management framework. Automated rules can be applied to ensure that changes in a user's access role or entitlements generates an incremental review, scoping down the number of users that need to be certified in a period based access audit. A rules based approach ensures organizations do not introduce compliance violations to begin with, by ensuring that approval and escalation workflows are part of the process.

*A truly automated and efficient approach will automate a business process for access delivery and governance, and will be architected such that business and technical stakeholders can collaborate and communicate in an effective fashion and the proper decision support is provided to understand if the access is appropriate or not.*

As further validation that these approaches are failing to meet organizational needs, many corporations are beginning to build access request systems themselves. Relevance and context suffers: user interfaces, while perhaps more tailored to organizational needs, tend to be poor, the solutions partial, and still lacking in end-to-end automation. A lack of back end integration can lead to large amounts of inefficiency. As a result, such projects are failing due to the high cost and complexity of building and supporting software in house, but are a natural reaction to the alternatives available.

## Relevance and Context: Building Blocks for Success

The shortcomings of current approaches have a common root cause. A scalable, business service approach to access delivery is characterized by two key capabilities, relevance and context:

- *Relevance* is achieved when business stakeholders are presented only the information necessary to request or approve access. If information is not relevant for a specific request task or does not apply to that business job role or operating unit, it is not presented to the user. For example, when requesting access for a job role within a bank's retail branch operations, trading desk applications for the wealth management operations are never presented.
- *Context* is achieved in proper balance when an access request can be evaluated and understood by the business user making or approving the request. The request is presented in business terms, not in IT technical descriptions. Context ensures a top down view, not a bottom up view for how access is described. In effect, the technical view is translated and presented in a business -friendly context. For example, an accounts payable administrator would be granted business rights such as payment issuance, rather than arcane application entitlement syntax within the ERP solution.

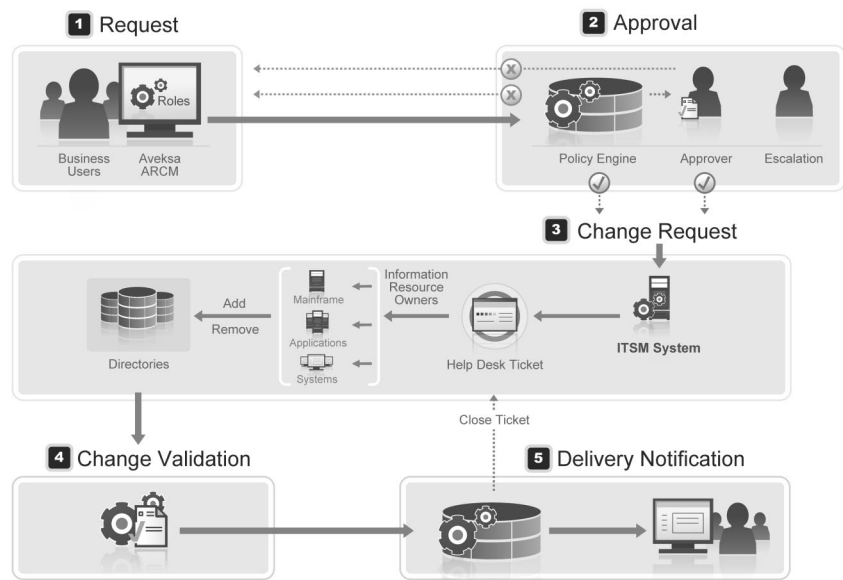
## A Continuous Process for Access Change Management

As discussed, ad hoc approaches to access delivery and governance, largely failed because they were architected for IT security and operations personnel to automate their processes. A truly automated and efficient approach will automate a business process for access delivery and governance, and will be architected such that business and technical stakeholders can collaborate and communicate in an effective fashion and the proper decision support is provided to understand if the access is appropriate or not. The basic steps of this process include:

- Request
- Approval & Escalation
- Fulfillment
- Delivery Validation and Notification
- Process Administration

These steps span various business and IT constituents, and may include sub-processes of their own.

*The access requestors can think in terms of the new user's business role or job function, rather than granular entitlements, and requesters are not presented with choices of user entitlements for applications that retail branch associates do not require to do their job.*



### Request

The initial access request may be a request for new access, a change to existing access, or a revocation of access. Where manual and ad hoc approaches may introduce a language gap, an automated process provides an intuitive interface for managing the request. This interface may be integrated into an SRM interface, or it may be a dedicated portal. It is important that the interface be optimized for a casual user. Where security management tools are designed for sophisticated IT users, business users will utilize the access request far less frequently, and will generally be less technically savvy by nature. The more quickly and easily business users can make such requests and get back to their core job functions, the more efficient the organization will become.

To facilitate that translation, business roles provide a means to an end to ensure that the business can understand access related information that is presented to them, and that only the information needed to execute the request transaction is presented, and nothing more. For example, a retail branch management making a request to on-board a retail bank branch associate would be comfortable requesting access consistent with the subordinate job role. The same requestor might have difficulty articulating this request if they were forced to phrase it in terms of application roles and technical software entitlements that the subordinate needed to do their job. The access requestors can think in terms of the new user's business role or job function, rather than granular entitlements, and requesters are not presented with choices of user entitlements for applications that retail branch associates do not require to do their job. Details related to the brokerage operations, such as a trading desk applications for example, are never presented to a requestor when the request is for a retail branch job function. Related, if a retail branch manager is requesting access, the system should be intelligent enough to filter available access to include only roles related to subordinates within that specific business unit.

Finally, business users require the ability to remain informed with respect to the status of the request. Many business users are familiar with tracking the delivery of a package through an online shipment application. While a business user does not need to be intimately familiar with the inner logistics of

shipping a package, they require the ability to understand the status of the package — where it is and when they can expect it — in terms that make sense to him. The access request and change management process should be similar.

*Attempting to apply control during the fulfillment process causes delays and error under manual processes. Under the automated process, control has been applied automatically during the request, saving considerable time during the access fulfillment process.*

### **Approval and Escalation**

Upon execution of the request, the request should be checked for compliance with organizational policy in real time. An automated rules engine can greatly assist this process, by filtering out many non-compliant requests before they are sent further into the cycle, consuming resources. Such a rules engine can drive efficiency by managing complex conditions and variables.

Some requests, especially those that create policy violations, will require additional approval. For highly sensitive access, such as access to a PCI database, organizational policy may require management authorization. For exceptions, or out of role entitlements, manual escalation and approval may also be required. For example, if one finance administrator has the ability to create purchase orders, and another to issue checks, and one of the administrators is going on vacation for two weeks, a temporary access exception may be needed. Such an access exception would likely require management sign-off, and a set of compensating controls to create an automatic revocation process to remove the temporary access after a set time period — managing a significant risk exposure related to entitlement drag that is all too common.

Business roles again play a key part in the approval process, by allowing business users the ability to think in business terms, to understand what exactly they are approving. For special access, and out of role entitlements, a rules engine can automatically require approval, and determine whether a request may create a problem. As a result, they make better decisions, leading to better efficiency and improved compliance and risk posture.

### **Fulfillment**

Fulfillment is the process of executing the access change. Generally, this becomes incumbent on the application administrator, or will be managed through the user provisioning system or SRM system. Most organizations utilize ITSM Helpdesks to automate many activities for IT operations and security personnel, and therefore, such systems must be integrated into the process. In practice, this generally involves the automatic opening of a helpdesk ticket for fulfillment, as well as closing out the helpdesk ticket upon validation of the request fulfillment.

Fulfillment is generally a major bottleneck in the access request and change management process. A single request for access may require ten application transactions and one hundred user entitlement bindings across the ten applications. Most large organizations have thousands of requests each month for new access or changes to existing user access. Due to this transactional volume, attempting to apply control during the fulfillment process causes delays and error under manual processes. Under the automated process, control has been applied automatically during the request, saving considerable time during the access fulfillment process.

To ensure maximum efficiency, the process should automatically translate the business language used to request the access to the necessary technical context the IT security administrator or user provisioning system needs to understand in order to fulfill the request. This may mean translating a single business request into multiple applications, each with multiple application permissions, updating target application directories. In the case where user provisioning is being used to fulfill the

access request for the information resources it administers, the access request and change management process needs to integrate with user provisioning system eliminating any manual steps to increase efficiency and accuracy.

*The delivery validation and notification process provides independent assurance that an access request or change has been fulfilled.*

### **Delivery Validation and Notification**

The delivery validation and notification process provides independent assurance that an access request or change has been fulfilled. It provides a closed-loop system that ensures that the ITSM, user provisioning system and/or application owners have performed their task to fulfill a request. For example, a request for access within a RACF system may be delivered to the mainframe application owner via notification from the helpdesk system. The owner would log into the application console, make the permission changes in the directory, and close the related helpdesk ticket. The automated validation process should hold the ticket open until it collects the user directory information for that application to validate that the specific change request has been executed in the target system. Upon validation, the helpdesk ticket can be automatically closed out, and business users are able to easily understand that the access change request has occurred in a familiar interface, similar to the one they might use to track a package.

Such validation is critical. For organizations relying on simulated provisioning models with ITSM technologies, Aveksa has seen failure rates ranging between 30%-40%, where a helpdesk ticket is closed when the change never actually occurred in the target system's user directory. In the case of an initial access request, this is often not a problem, since the users will follow-up on requests with a call or an email to the helpdesk if they do not receive access. But for change events such as with transfers and terminations, no one calls into the helpdesk to inform that access entitlements haven't been revoked and are still active when no longer needed. In the 2007 Deloitte study of the top five audit findings, 28% of organizations had failed to clean up access rules following a transfer or termination. While detective audits can catch these violations after the fact, a preventative and risk-oriented approach is far superior.

### **Administration and Reporting**

Following validation, the requestor is notified of the update to access, and the information is available for follow-on audit by affected stakeholders. IT security and operations personnel can view more detailed metrics, to ensure efficient orchestration and facilitation of the access request and change management process. Visual scorecards and process flows allow for root cause analysis, and identification of process bottlenecks.

A complete view of process throughput can yield metrics that can be used for process optimization, driving even higher levels of organizational efficiency. Such metrics can allow organizations to track adherence to service level agreements (SLA's) to determine, for instance:

- How many requests were fielded during a day, week, or month
- The number of transactions embedded within requests for specific access categories
- Approval and fulfillment times
- Escalations
- Which application administrators are slow or inaccurate during fulfillment
- Trend analysis for access request and change management process optimization

*The automated access delivery and governance process, while itself a business process, must integrate seamlessly with existing IT processes to drive maximum organizational adoption and efficiency.*

## **Integration for Automation**

Most organizations utilize solutions to automate existing IT processes. The automated access delivery and governance process, while itself a business process, must integrate seamlessly with existing IT processes to drive maximum organizational adoption and efficiency.

From a request standpoint, some organizations will utilize an SRM user interface as a front end. The access delivery and governance system must be able to push contextual and relevant business/job role information straight to the SRM interface, allowing business users to work in an interface with which they are familiar and with access terminology that is business friendly. Tighter integration can perform policy checks in real time, coupling the SRM interface directly to the authoritative policy engine, providing a greater level of relevance for the business user, and greater efficiency ensuring that requests that violate policy are not made in the first place.

For fulfillment, the access delivery and governance process must integrate with ITSM ticketing systems as well as user provisioning. The access delivery provides the ability to enforce policy and bridge the language gap, while pushing the request to the user provisioning system or the application owners in language they can understand.

This approach also facilitates the goal of recent direction towards the lifecycle aspects of service automation in frameworks such as ITIL v3. It is only through seamless integration with the business service desk of an organization that this is possible.

## **Benefits of an Automated Business Service Approach to Access Delivery**

Upon implementing such a model, organizations will start to reap numerous benefits, including greater operational efficiency. The business service approach to access request and change management is inherently simpler. As such, it achieves a reduction in the cost, complexity and burden inherent in governing access.

To combat complexity inherent in highly distributed and fragment information resources, organizations utilize human capital. From a human resources standpoint, organizations employ myriad employees involved in the performance and process maintenance aspects of fielding access requests. An opportunity to reduce that capital cost by driving efficiency represents a significant organizational win. From an opportunity cost standpoint, if resources can be freed up from spending as much time fielding requests, they have more time to devote to building and maintaining revenue-generating or core business applications.

From a governance standpoint, this approach provides complete access visibility, business controls and auditable evidence of compliance (who has what access, by whom it has been approved, and whether it is appropriate). Through access visibility and control, the cost of compliance with access governance policies is greatly reduced through the introduction of a preventative control framework. This results in less wasted effort and cycle times for businesses doing rework, and remediating improper access that has been granted, or has been failed to be revoked. It also reduces the compliance burden and cost of demonstrating compliance by scoping down the audit universe and avoiding expensive rework.

## **ABOUT AVEKSA**

Aveksa simplifies how access is delivered to the business and is governed across the enterprise. 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 2000 organizations in financial services, healthcare, retail, energy/utility, transportation and manufacturing. For more information, go to [www.aveksa.com](http://www.aveksa.com).

## **ABOUT AVEKSA ACCESS GOVERNANCE PLATFORM**

The Aveksa Access Governance Platform is the industry's first comprehensive solution for access governance, risk and compliance management which delivers unmatched visibility into the true state of user access rights. The Access Governance Platform is comprised of Aveksa Compliance Manager, which automates the monitoring, reporting, certification and remediation of user entitlements; Aveksa Role Manager, which enables role discovery, modeling and maintenance; and Aveksa Access Request and Change Manager, which combines a business-centric interface and an automated, streamlined request process with policy controls to ensure that access is always appropriate.

# Aveksa

### **Aveksa Inc.**

265 Winter Street  
Waltham, MA 02451  
tel 781-487-7700  
[www.aveksa.com](http://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. 11/09

As a result, IT operations and security are no longer the bottleneck, and business can operate more efficiently. Since less time is wasted fulfilling access requests, access is managed, changed, requested and revoked on demand, whenever it is needed. Businesses become more agile, and more quickly able to respond to market demands and changes in operating environment.

## **Conclusion**

As organizations evolve the way they request, deliver, fulfill and administer access, progressive companies should move to a business service based approach. Companies that rely on user provisioning technology, ad hoc and home grown approaches, will be constrained by a lack of context and relevancy, and an inability to dynamically embed governance into the process at the point of access change. Business-centric solutions provide simpler, more efficient business friendly interfaces and workflow, allowing all users to do their job more effectively.

Organizations that adopt a business service based approach should ensure that such an approach is based on organizational roles, and provides a business oriented, self-service interface to the management of access delivery. This business service should be architected in such a way to ensure that context and relevance is presented, such that business & IT stakeholders can efficiently govern, assign and fulfill user access requests. Such a service should be automated from end to end, and should be open enough to integrate with existing IT Service Management and user provisioning systems to leverage existing investments as well as to minimize resource costs and errors associated with manual approaches.

Organizations that adopt such a progressive approach will be rewarded with myriad benefits. Such an approach reduces the cost and complexity associated with the request and fulfillment of access, and subsumes formerly complex compliance processes, ensuring that security and control is applied as a byproduct of the service. The result is a drastic net reduction in organizational costs, streamlined operational efficiency, and increased business agility.