AVATIER™

Lifecycle | SSO | Governance | Password

TOP 10 ACCESS GOVERNANCE BEST PRACTICES

The proven working guide for successful implementations.

2025 EDITION

Lifecycle | SSO
Governance | Password

TOP 10 Steps to Success

Manual Processes Prove Labor-Intensive

Indeed, for most performing a manual IT audit is a labor-intensive effort. Although expensive paper and manual processes are historically the norm, they are unreliable and foster inconsistencies. These IT review processes are generally complicated, and ultimately never truly address the concerns they uncover, because most reviewers simply rubber-stamp the access rather than take corrective action.

Sustainable Compliance Management Software

Regulatory compliance management is an encumbrance that organizations in all verticals have learned to bear over the past years, and it's not going away any time soon. In fact, experts agree that this burden will steadily increase in the future, imposing even more rigid requirements on organizations for adherence to FIPS 200, SOX, HIPAA, NERC, FERPA, PCI DSS, Basel II, and other industry compliance regulations. Faced with more regulatory compliance, an increasing number of organizations are abandoning labor-intensive manual and paper-based audit processes in favor of new technologies that ease the audit burden.

But not all technologies are created equal. Organizations must carefully consider compliance management solutions that will enable ongoing sustainable cost-effective governance, risk and compliance for the long term. In addition, compliance management must be regarded as an ongoing process of continuous improvement, rather than a one-time event or quarterly fire drill. Only then will compliance management processes result in efficiency that reduces costs and ensures regulations are met with fewer headaches.

Lifecycle | SSO | Governance | Password

TOP 10 Steps to Success

The Many Challenges in Access Certification

Most information security managers of large organizations work with internal and external auditors on a routine basis. As part of an IT audit, a common area of scrutiny is user access validation to critical systems and access certifications. The breadth of the term "critical systems" continues to grow considerably over times as single sign on and integration technologies introduce new systems into most organizations. This, of course, increases the complexity and scope of access certification audits.

Step 1: Know your scope of systems.

Where a single ERP solution may have been in scope for an IT audit in the past, now the core directory environment along with ERP and other critical systems are also brought into scope. And as users are often assigned multiple access privileges across each platform, and each of those privileges is owned and understood by a different resource owner, regulatory challenges become further complicated.

☐ Approved by _____

☐ Date completed _____

Step 2: Choose the approval approach for your access audit.

Depending on the state of authoritative manager and resource owner data, organizations must decide on one of the following access certification approaches. These include:

- Manager-level access reviews – Access certifications of employees and consultants performed by a business manager.
- Resource owner-level access reviews – Access certifications performed by the assigned owner of the access privilege to validate they truly require it.

In some situations, both of these access certification types must occur to address IT audit concerns. Therefore, an organization must have a foundation in place to support either approach. This is not always easy, since some core data must be available to sufficiently identify managers and resource owners in the first place. Challenges exist for each type as described below:

- Manager-level access reviews – If managers are not tracked in a central HR system for both employees and consultants, it is nearly impossible to easily initiate a manager-level access certification process. Ideally, HR-driven manager data should be automatically pushed into the core directories so there is an authoritative source of manager data.
- Resource owner-level access reviews – On the other hand, if an organization does not assign and track owners to specific access privileges (i.e., ERP role assignment, group memberships, etc.), it is near impossible to easily initiate a resource owner-level access certification process. In this situation, an IAM solution is often needed to help automate the collection and tracking of these owners.

☐ Approved by _____

☐ Date completed _____

Lifecycle | SSO | Governance | Password

TOP 10 Steps to Success

Step 3: Identify authoritative sources for manager and resource owner data.

Once a method is chosen for approvals, it is necessary to identify the owner data tied to the access data so the appropriate approvers can be contacted. Ideally, an identity management environment is already implemented to update this data so leveraging an existing authoritative source for this data is possible. A solid IAM product tied to HR data and your IT service catalog is the ultimate solution.

Step 4: Resist the temptation to use the spreadsheet approach to access certifications.

Regardless of the selected access certification type, the act of actually performing an IT audit is the biggest challenge for most organizations. When presented with the dreaded IT audit review indicating an access certification must be performed, organizations historically had limited options to reliably and immediately respond to the request and later act on the findings.

☐ Approved by _____

☐ Date completed _____

Step 5: Choose the right software to meet your needs.

Replacing paper-based and manual processes with automated technology tools and software audit controls represent the only way to meet regulatory requirements and truly gain control of your auditing processes. With automated technology, you can establish consistent and reliable processes with predictable and repeatable value-adding compliance management tasks.

Still, only intuitive and flexible automated solutions truly allow organizations to improve security with minimal impact to the actual approvers. These unique solutions must possess the following abilities:

- Ability to interact directly with an existing IAM solution
- Ability to run access certifications in a standalone mode via data imports
- Ability to dynamically assign resource owners from an existing IAM solution
- Ability to pull access rights directly from source systems or existing IAM solutions
- Ability to dynamically determine user manager data from core directories
- Provide an intuitive interface for easy access validations from any device and any location

Lifecycle | SSO | Governance | Password

TOP 10 Steps to Success

Sustaining Compliance Strategy

Deploying an automated technology solution is an important first step in addressing compliance requirements, but diligence in performing operational review processes is equally vital. These best practices guidelines establish the right practices to build operational processes that reduce risk and compliance review costs.

- Provide fully automated notifications to free IT resources from manually managing the access certification process
- Report capabilities to demonstrate audit success
- Provide project-based certifications for granular audits for specific target resources and user communities

☐ Approved by _____

☐ Date completed _____

Step 6: Establish preventive controls.

Resist focusing solely on detecting areas of non-compliance. By taking a preventive approach, you can ensure that compliance violations are not introduced to your business environment.

☐ Approved by _____

☐ Date completed _____

Step 7: Measure risk.

Put processes in place to access and measure risk so that you may identify the highest risks and subsequently focus your internal controls on them. Over time, this reduces compliance management costs, as well as provides evidence that your identity management audit controls are effectively reducing your corporate exposure and risks.

☐ Approved by _____

☐ Date completed _____

Step 8: Centralize your view of identity data and business processes.

Better accountability, oversight, and successful compliance management can only be achieved with an enterprise view of all critical sources of user account activity. With this centralized view, you can more effectively meet IT auditors' reporting requirements. As an additional benefit, you streamline compliance processes across departments and business units to reduce risks and improve IT security.

☐ Approved by _____

☐ Date completed _____

Lifecycle | SSO
Governance | Password

TOP 10 Steps to Success

Companies of all sizes address increasing compliance and security requirements to protect and govern access to critical applications, systems, databases, and services. Access governance solutions play a vital role in enabling organizations to monitor, analyze and revoke the access privileges granted to their employees. By using an automated compliance auditor, your ready to report on access certification with complete accuracy and take corrective action as part of an audit review.

Step 9: Get buy-in from corporate and IT staff.

Don't rely on IT staff alone to tackle your organization's compliance regulations. Engage key stakeholders early and often to understand the true requirements in your organization, define policy and controls, and review user access privileges.

Never assume that you know all of the requirements relating to access certifications. Make sure you engage IT audit teams, access governance administrators, business users and other support groups to make sure everyone is on the same page. This not only helps uncover the requirements to configure the solution, but it will ensure that the business units assume accountability. Also, don't underestimate the importance of training your service desk on the user-facing components of the solution so they can quickly answer calls from approvers when they need help. This reduces frustration for the end users and improves adoption rates.

☐ Approved by _____

☐ Date completed _____

Step 10: Focus on continuous improvement.

As with any complex process, a focus on continuous improvement opportunities is critical to help streamline the access certification process. Recognize challenges that occur and identify solutions so the next round of audits is more efficient. Improving communications is a change that can make a significant difference. Challenges in this area will not be revealed until the first pass is complete. A lessons-learned meeting after the first access certification audit with a subset of key stakeholders helps identify critical areas of improvement.

☐ Approved by _____

☐ Date completed _____

TOP 10 Steps to Success

ACCESS GOVERNANCE DEPLOYMENT

Access Governance Success

When your strategic business imperatives include reducing risk as well as improving compliance, there's no doubt that an investment in a compliance auditor technology is the right choice. The value is evident: An access governance solution enables you to see where the greatest potential for risk lies in your organization. And when you can proactively identify your exposure, you thwart opportunities for more far reaching problems.

Now that escalating security and privacy concerns continue to push compliance requirements to prominence among organizations worldwide, this technology is a must. In fact, a critical combination of processes with the right technology namely— automated solutions that possess flexibility, innovation and intuition, stand out as the best approach for a secure compliant organization now and in the future.

Innovative Identity Management and Access Management Delivered

Avatier is a leading provider of enterprise identity management solutions. Avatier Identity and Access Management Software Suite (AIMS) enables business line managers to take control of the identity management life cycle through a patented IT storefront for service catalog user provisioning, a universal mobile client for access certifications, and self-service password management. Avatier solutions maximize operational efficiency through IT automation and self-service operations.

Lifecycle | SSO
Governance | Password

TOP 10
Steps to Success

Notes

AVATIER
800-609-8610 North America
+44 (0) 207 877 1807 EMEA
+61 (0) 2 9959 1047 APAC
www.avatier.com