An Oracle White Paper
January 2010

Governance, Risk, and Compliance: A Practical Guide to Points of Entry

ORACLE

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Table of Contents

1. Executive Summary

The implementation of new initiatives in governance, risk, and compliance (GRC) may be an overwhelming prospect for many organizations. With multiple views and aspects of GRC, it can be difficult to know where to begin. IT Governance continues to be a main focus for many security officers and IT administrators in tacking the constantly evolving regulatory requirements coupled with increased business complexity. Organizations today are being asked, not only to understand the regulations, but also to create the appropriate strategies in addressing their Governance, Risk and Compliance (GRC) needs. Adding to this is the reality that GRC initiatives are often broad and spread across different infrastructure silos managed by different business or IT organizations. Among all the regulatory compliance mandates, Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLB) and Health Insurance Portability & Accountability (HIPAA) are the ones we hear the most. Many of the key requirements revolve around elements of Identity Management where user access to systems, applications and data is being controlled. As a result, any IT GRC initiatives and considerations must put Identity and Access Governance on the top of the list.

This paper proposes that the solution is to break GRC initiatives into a number of constituent components that can be addressed one at a time, beginning with those that are easiest to plan for and implement.

Choosing the first area on which to focus may mean drilling down from the big picture of enterprise GRC to the IT framework that enables it, and then to some manageable aspect of that framework. An example of this is IT framework applications associated with instituting access, security, and other controls to support business policies. Because access and security are inextricably linked with identity, controls that can be automated through identity management are a good place to start.

This paper provides:

- Specific examples of identity-related access and security controls that can be instituted as part of an IT framework for GRC
- Guidance for selecting an identity-based solution for access and security controls within the IT framework
- Information about Oracle's portfolio of identity management products that may be useful in the initial effort to address GRC

2. Building a GRC Framework with Identity-Related Controls

The following are specific examples of identity-related access and security controls that can be instituted as part of an IT framework for GRC, whether across the enterprise or for a particular business area within the organization.

Authentication

Verifying that users who request access to enterprise resources are who they say they are and have permission to view or use what they are asking to view or use is fundamental to reducing risk and improving compliance in the enterprise. This requires access controls with a strong authentication component.

Identity-based access-control technology that includes a wide range of authentication capabilities can be implemented to provide the appropriate levels of authentication to support enterprise policy. At the minimum, an identity-based solution should include:

- Strong password management capabilities that dictate policies such as how often passwords are required to be changed
- Enterprise single sign-on (ESSO) capabilities that enforce password policy while improving the user experience by enabling users to use one password for access to different enterprise resources
- The option of even stronger controls such as multifactor authentication to strengthen the security of password-based access at the initial network-login level

Segregation of Duties Enforcement

Segregation of duties (SOD) enforcement prevents users from intentionally or inadvertently breaching security policy as a result of the roles they occupy and the duties they are assigned to perform. A classic example is not allowing someone who issues purchase orders to approve them as well. SOD enforcement directly impacts an organization's ability to comply with explicit requirements of the Sarbanes-Oxley Act and other regulations aimed at ensuring the integrity of enterprise financial operations.

Enforcing SOD policy in a GRC control environment requires identity provisioning and auditing capabilities that:

- Are fine-grained enough to identify imminent violations when users are provisioned, especially after job changes that may affect their duties
- Automatically prevent violations and report to management on when incidents occur
- Maintain an ongoing record of activities with the potential impact to SOD, such as job changes and password resets
- Record and notify management of all attempts to access confidential, restricted, or other sensitive enterprise resources

Once the policies are defined, they must be enforced during the day-to-day functions of the identity management system as appropriate controls.

Preventive Controls are the most common controls. As the name suggests, preventive controls are intended to prevent undesirable behavior from ever occurring. These controls can be put in place in several areas. An access control policy can limit who can log into a web application based on a relevant set of criteria – such as time of day or

location of the user accessing the application. Preventive controls can also be put in place where access is granted. A role may be granted to a user or a new entitlement may be mapped to a role, effective modifying the access for all the users belonging to the role. A preventive control such as a Segregation of Duties control can be put in place to evaluate such actions that may result in policy violations and prevent them from occurring. Notifications or approval workflows can be coupled if human intervention is required.

While policies, processes and preventive controls can prevent undesirable activities from occurring, no system of controls is perfect. Inevitably situations arise where an inappropriate action has been taken. *Detective Controls* are used to identify situations where violations have already occurred where a user's actual access is not aligned with the policies defined. This may be the result of a fraudulent attempt. Or it may be a case of access accumulation in legacy systems that have traditionally been lacking preventive controls.

When exceptions or violations are detected by the detective controls, corresponding *Corrective Controls* must be put in place to handle the violations. For example, email alerts can be routed to the appropriate reviewers where remedial action may be taken on the violation. Depending on the severity of the exception the inappropriate access may need be removed or modified programmatically or manually depending on the type of corrective controls implemented. The controls may be integrated with a notification framework or a ticketing system for manual remediation – or with a provisioning system for automated remediation.

Role-Based Access Control

Enterprise rules and policies that dictate who has access to what resources in the enterprise can be applied based on the role of the user. Role-based access control simplifies administration by making it possible to apply policy against roles rather than individual user accounts.

As in the preceding SOD-enforcement scenario, an identity-driven solution may be ideal. The key is to find a product that can:

- Identify conflicting access privileges and automatically prevent users from being granted rights when a conflict is identified
- Offer combined capabilities to manage roles, grant access, and report comprehensively on access throughout the process of auditing and certifying access privileges and activities
- Automate access controls to simplify the access certification process for managers

Roles can also be used to automate access certification controls, which greatly simplify the access certification process for managers. When based on role management, the tasks of auditing and certifying access to resources enable the enterprise to establish a practical framework for interjecting tight controls. Management can efficiently secure the

enterprise and comply with internal security policy or external regulatory requirements. Additionally, role-based access auditing and certification greatly reduce the operational inefficiencies associated with managing user access in an ad hoc manner.

Audit and Compliance Automation

The importance of automation to implementing controls for GRC initiatives cannot be overstressed. Implementing automation for audit and compliance makes it easy and cost-effective to enforce access policies, monitor access, and conduct ongoing audit and compliance reporting.

The processes and procedures that are associated with auditing and compliance cannot be sustained manually because they are labor-intensive, costly, and time-consuming – not to mention subject to human error. For example, without automation, an organization may spend weeks at the end of a quarter detecting access violations and remedying them manually. And even then, there's no assurance that every violation will be caught and properly addressed. By contrast, an identity-driven, automated solution can instantly and accurately detect violations, such as a user who changed roles in the organization and inappropriately retained access privileges to resources associated with the previous role.

Ideally, an identity-based solution for automating audit and compliance processes should bring together diverse capabilities to automate multiple related processes, with:

- A combination of automated capabilities for provisioning, access management, and reporting to enable the delivery of sustainable comprehensive audit and compliance support
- Directory capabilities for automatically consolidating identity and access information from throughout the enterprise, providing a first line of authentication services to applications, and offering strong security mechanisms such as encryption of directory data
- Support for automatic logging and encryption of transactions to provide a complete, tamper-proof forensics trail for the audit team to review as needed

Access certification is typically performed by a line of business manager or an application owner to periodically review user access. The support for access certification includes the automation of the process itself (scheduling, email notifications, approval routing, status reporting etc.) as well as the documentation or auditing of these activities. The certification may be performed at different levels depending on the nature of the certification task itself. An application owner may be interested at a high-level certification of user access based on application accounts created to access the application. A business owner may be interested at the user entitlements, which determine the types of business functions exposed to the end users. Similarly, where roles are used for granting access, role memberships will be of interest as they ultimately determine user access. An effective access certification solution must provide the right level of information since the target audience is often business users rather than IT administrators. Business-friendly description of the resources, entitlements and roles must be presented.

Analytics

With the wealth of information collected, the data can be analyzed to look for trends and behaviour, which may be signs of potential risks. For example,

- What is the percentage of accounts that has been attested in this quarter?
- Does any approver have an abnormally large amount of approval requests during a given period of time?
- Is there any trend with respect to rogue accounts being detected?

While it is not entirely possible to prevent risk, the goal of an Identity and Access Governance solution is to mitigate risk. The analysis can be triggered manually but can also be scheduled periodically along with proper notification to alert business owners or application owners where appropriate.

A key aspect of Identity and Access Governance is the ability to monitor the health of the systems as well as user behaviour. With all the controls in place, along the audit support in the products, a useful amount of identity information can be collected - information such as user creation, account requests, access requests, approvals, violations, exception remediation, role grants, user login, etc. A comprehensive reporting framework allows the viewing of this information by different types of users. In addition to static reports, dashboards provide additional insight into the information through graphical representation of the data collected.

3. Criteria for Selecting an Identity-Based Solution for Controls

Automation is at the top of the list for any organization that is considering using an identity-driven approach to the controls environment in the IT infrastructure for GRC. But beyond automation, having an identity-based solution for controls that provides the flexibility to bring together multiple processes – identity provisioning and auditing, access management, and role management – is also important.

- *Identity provisioning* and *identity auditing* capabilities that are available in a single streamlined offering are useful for efficiently fulfilling access requests while simultaneously detecting risks associated with access
- *Access management* that includes fine-grained authentication vital to establishing a line of defense against violations of policy or regulatory directives
- *Role management* capabilities are useful for enterprises with a large, diverse base of users because they can speed the process of managing access to resources

Finally, any identity-based solution for building a controls environment for GRC must have a strong reporting component. The solution should report on who has access to what (by both user and information owner); who actually accessed what, including applications, operating systems, and other resources (especially resources associated with confidential or other sensitive information); and who approved or authorized the access. Additionally, reporting capabilities should include a centralized log of all access activities from all resources, so that organizations can quickly and accurately gather the information needed for an audit.

4. Using Oracle Identity Management to Institute Controls

Oracle's complete portfolio of identity management offerings provides all the capabilities that an organization needs to begin implementing access and security controls as part of an IT framework for GRC.

Oracle Identity Manager

Converged identity provisioning and auditing capabilities make Identity Manager an ideal choice for the fine-grained functions that are needed to apply and enforce security policy and compliance requirements in the control environment. Key features include:

- Integrated provisioning and auditing for preventative and detective compliance
- Identity controls consistently applied across provisioning and auditing
- Policy violation tracking and expiration capabilities to handle exceptions

Oracle Access Manager

Oracle's federated identity products provide the single sign-on, authentication, and authorization capabilities that are essential to access control in the IT framework for rolling out GRC initiatives. Key features include:

- Centralized control over application security
- Policy agents to enforce rule- and role-based authorizations
- Pre-integration with ESSO capabilities
- Extension of core authentication and authorization services to partners

Oracle Identity Analytics

By applying enterprise access policies based on user roles rather than individual access privileges, Oracle Identity Analytics dramatically simplifies access control within the IT framework for GRC. Key features include:

- Role engineering and ongoing role maintenance
- Ongoing role certification by business unit managers or role owners
- Enterprise-level monitoring of access for policy conflicts
- Dashboard view of certification status and policy exceptions

Oracle Directory Offerings

OID, OVD and Directory Server Enterprise Edition provide a complete directory service for consolidating access information from throughout the enterprise. Key features include:

- Robust security with data and communication encryption and password protection
- Multi-level access control instructions (ACIs) to secure data and minimize risk
- Sustained search performance and near-relational database write performance
- Highly flexible replication environment to help ensure data availability

5. Conclusion

For enterprises that are eager to roll out enterprise GRC initiatives, the greatest challenge may be in not knowing where to begin. Focusing on one aspect of GRC at a time will bring about optimal results, particularly if an organization starts with something that is easy to plan for and implement, such as identity-related infrastructure controls. Oracle's identity management portfolio includes a number of products that can be used to establish controls in the areas of authentication, Segregation of Duties Analysis, Identity Analytics, role-based access management, and automation of audit and compliance processes.

To learn more about Oracle's identity management and identity-related controls, visit Oracle.com/identity.

Governance, Risk & Compliance
January 2010
Author: Neil Gandhi

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Oracle is committed to developing practices and products that help protect the environment

0109