

Improving Compliance with Role Based Access Control

Daniel Poliquin
Deloitte & Touche LLP
January 2009





Agenda

Common Audit Findings

Current Access Controls

Role Based Access Controls

Compliance

Q & A



Common Audit Questions

- Is there a documented process for user account management (creating, modification, termination etc) ?
- Does the process require approvals before user accounts are established?
- Is there a unified security system in place for your business?
- Is there a periodic review of all user access?
- Is there adequate logging or monitoring to display the audit trail to ensure only valid access to critical systems is occurring?
- Is access to production systems limited?
- Are changes to the systems controlled?
- Do workers have least privileged and appropriate authorization for access?
- Is Segregation of Duties considered before a user is granted access?
- Is User provisioning providing the efficiency sought after?



Current Access Controls

- Multiple system requests are required to get a user online
 - Multiple business to IT translations are performed by a Requestor to decipher the access needed on each request
- Varied approvals per request are needed to get the user a single form of access
 - Overall compliance is difficult to review upfront, as multiple requests are needed cannot be co-related



Current Access Controls

- Request Process results in:
 - Lengthy delays in getting a user online to perform their job duties
 - Users with similar jobs have various different access due to irregular translation
 - Compliance violations exist across applications because there is no single view
 - Business does not have a strong understanding of the access their user's have or need
 - IT does not understand the job's that their users are performing



Auditing Access Controls

- Time consuming to review multiple reports
- Inefficient as most reviewers do not fully understand the detail
- Expensive to generate the reports
- Compliance issues are difficult to discover
- Compliance issues are still prevalent



Role Based Access Control

Role Based Access Control (RBAC) helps clients streamline access control issues.

This includes but is not limited to:

- Role Engineering
- Defining role lifecycle management processes
- Selection and deployment of RBAC technology solutions



Role Based Access Control

- Is a method of defining, managing and enforcing access control privileges to users by leveraging Enterprise Roles
- Simplifies the process in assigning user's access based on their job function
- Roles simplifies enforcing Segregation of Duties rules



RBAC Benefits

- Improved Security
 - Strengthened Access Controls
 - Access Management
 - Scalable – Management of Thousands or Tens of Thousands of Users
 - Approvals, Administration, Validation
- Process Improvement
 - Simplified Access Control
 - Requestors, Approvers, Application Owner/Grantors, Security Administrators
 - User Access Management
 - More Accurate and Timely
 - Identification of Inefficiencies
 - Inefficient or Outdated Access Standards and Processes
- Regulatory and Audit Compliance
 - Sarbanes-Oxley, GLBA, HIPAA
 - Internal Audits



Compliance & RBAC

Business Drivers	Description
<ul style="list-style-type: none">• Regulatory Compliance<ul style="list-style-type: none">– Sarbanes-Oxley Act– Payment Card Industry Data Security Standard (PCI DSS)– U.S. Gramm-Leach-Bliley Act (GLBA)– Breach notification laws (CA SB1386)– EU Data Protection Directive– Industry-specific mandates (HIPPA, FFIEC, NERC, and others.)	<ul style="list-style-type: none">• Management must report on internal controls within the enterprise• Provide evidence that controls over user accounts and access privileges function as intended<ul style="list-style-type: none">–Preventive, detective, and monitoring controls–Issue remediation• Protect Personally Identifiable Information (PII) such as customer data from unauthorized disclosure or modification
<ul style="list-style-type: none">• Audit Management<ul style="list-style-type: none">– Address audit issues– Perform periodic user access reviews– Test control effectiveness	<ul style="list-style-type: none">• Review user identities, job functions, and access privileges• Audit access requests, approvals, and administrative actions• Assign resource owners to review and recertify user access to enterprise information resources• Identify and remove user access not justified by job role/function



Audit Compliance

- Compliance can be addressed more easily as
 - Access is assigned to users in well defined terms for both business and IT
 - Compliance is addressed early in the Role Definition stage
 - User's access is controlled by restricting the number of roles assigned to a user
 - User efficiency increases as access can be gained immediately for their job to be performed
 - Single request & approval process eliminates the on-going effort required to get a user online



Disclaimer

This presentation has been modified from the original presented at the ISACA Meeting.

For more information, please contact:

Daniel Poliquin

Principal

Deloitte & Touche LLP

111 S. Wacker Drive

Chicago, IL 60606

USA

(312) 486-5627

dpoliquin@deloitte.com

www.deloitte.com

Questions?

Closing comments

