Privilege, Role, and Policy Management

The Role of Roles in Compliance – A Practical Approach

2nd European Identity Management Conference
April 2008

Dr. Ron Rymon, Founder, Eurekify
rrymon@Eurekify.com
Enterprise role management is quickly becoming a critical technology for enabling organizations to verify and enforce regulatory policies and to audit the effectiveness of internal controls over user access. But due to complexity and marketplace confusion, many companies struggle to find an approach that delivers practical and timely results.

This workshop is designed to help technical leaders adopt a pragmatic strategy for managing roles as part of a successful governance, risk management, and compliance initiative. SailPoint’s Chief Technology Officer, Darran Rolls, will provide an in-depth look at role management concepts and technologies. And, he’ll offer recommendations that can help organizations achieve practical benefits with roles. Points of discussion include:

Introduction: What is role management?
Business drivers and use cases for role management
Where do roles fit in the world of compliance?
How do compliance roles relate to provisioning roles?
How useful is the NIST RBAC model?
Real-world deployment issues:
Engaging the business user in the process
Achieving flexibility, usability, and ease of deployment
Role model interoperability
Future directions for role concepts and technologies
Workshop participants will gain the theoretical and practical knowledge they need to develop clear action plans for tackling role management in their organizations and to determine the most appropriate approach for the needs of their identity infrastructure and compliance objectives.
• Real-world deployment issues:
• Achieving flexibility, usability, and ease of deployment
• Future directions for role concepts and technologies
ERM Market Trends

- ERM shifts from Nice-to-have to Must-have
  - 70% of IdM RFPs require role management capability
  - Roberta Witty, Gartner: "Role management is becoming a must-have rather than a nice-to-have capability in large, multinational enterprises…."  
  - Roles are essential for IdM value

- ERM shifts from Post-IdM to Pre-IdM activity
  - Roles are essential for IdM value
  - Roberta Witty, Gartner: "RME is likely to be a prerequisite for many user-provisioning initiatives"

- Customers demand role models that cover 80% of access rights
  - Role-based provisioning cannot be done with only 20-50 roles
  - Kevin Kampman, Burton: "The trend of RM following IdM is changing. Roles are seen beneficial in their own right"
  - But roles are essential for effective communication with business managers
The History of Roles

2002 (Eurekify): In most cases, you simply cannot do IAM without roles. And we have the technology to do it quickly and effectively.

• 2003: Roles are too difficult and if you start with roles, you will not finish your Identity Management implementation. If you insist, please postpone roles until step 9999.

• 2004 (Eurekify): Roles and access compliance go hand-in-hand, and are a must for effective management. Use one to simplify the other.

• 2005: Roles are important to successful IAM implementations.

2006 (Eurekify): Privileges quality management is a necessity for both roles & compliance management, but also a big benefactor from both.

• 2007: IAM implementations shall start with roles. Enterprises shall consider roles for their independent value.

• 2008: Roles are also important for GRC…
GRC Implementation Challenges

- Privileges data collection
  - Many systems (usually several tens) with many different representations

- Account correlation & consolidation
  - All sorts of accounts, naming conventions, meanings

- Data cleanup
  - With the current mess, compliance project is 10x more complex without cleanup

- Privileges classification and categorization
  - Roles help categorize privileges by business structure, processes, relevant risks, etc.

- Creation of a Compliance Model
  - Automated IT controls that reflect company policies and regulations

- Initial verification and reporting
  - Verification, remediation or mitigation of policy violations

- Establishing ongoing processes
  - Automated detection of violations (real-time and/or post-hoc)
  - Compliance verification and reporting

- Who should do what?
  - IT, Security, Auditors, Business, …

Easy Import & Merge
Unique User ID Tool
Automated Detection of Inconsistencies
Analytics to Quickly do Compliance Roles
Analytics for IT Controls & Risk Modeling
Fast Policy Verification & Reports
Policy Violations Reviews & Certification
Cohesive Solution and Cohesive Team
Future Directions & Role Concepts

- **Role Types**
  - Business roles (*organizational, functional, location*), Applicative roles (*system, technical*)
  - Compliance roles are primarily *process* roles at L1 and primarily *applicative* roles in L2

- **The Importance of Role & Compliance MODELS**
  - You cannot run provisioning, nor GRC, without clear models
  - You cannot push the job of creating the model to business people

- **Modeling is difficult without analytical technology**

- **Role Management and Compliance Management**
  - Roles and compliance are intertwined and you cannot have one without the other
  - There is a third wheel, which is privileges management (a.k.a. entitlements)

- **Role & Compliance Management and Identity Management**
  - ER&CM is an independent system, with its own value
  - But, must provide decision support for IAM & Provisioning system in real-time
<table>
<thead>
<tr>
<th>OUT</th>
<th>IN</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM projects without a clear business case and careful planning</td>
<td>Quick gap analysis to identify most important needs and easy wins</td>
</tr>
<tr>
<td>Role modeling at “business level” only, based on preconceptions, whether or not they fit</td>
<td>Identify the “right” modeling for each business unit; work in all levels; use data to guide and corroborate</td>
</tr>
<tr>
<td>Delegation of role modeling to the business through nice interfaces</td>
<td>Role modeling requires expertise, and cooperation of all stakeholders</td>
</tr>
<tr>
<td>Lets start with few roles covering most obvious 10% of access</td>
<td>Quickly create role models that cover 70-80% of all access rights</td>
</tr>
<tr>
<td>Delegation of compliance to the business through dumb certification</td>
<td>Automated IT controls + decision supportive certification</td>
</tr>
<tr>
<td>Separate solutions for certification vs. role modeling, vs. IT controls vs. privileges cleanup</td>
<td>Cohesive solutions for Privileges, Roles, and Policies</td>
</tr>
</tbody>
</table>
Privilege, Role, and Policy Management

- **Policies**
  - Model: IT controls, SoD, and risks
  - Manage: certify, verify, enforce, and report

- **Roles**
  - Model: define and assign
  - Manage: review and adapt

- **Privileges**
  - Cleanup
  - Control quality and risk
Eurekify-based Identity Management Solutions

- Directly from target system
- IdM data integration

**IdM process Integration**

Web services

- Analysis
- Test Change
- Privileges
- Roles
- Policies

**IdM Provisioning**

- Operational Database
- Unix
- RACF
- SAP
- HR
- Share

Directly from target system

IDM data integration

- Directly from target system
- IdM data integration

API or data files

Dr. Ron Rymon, Founder, Eurekify