Use This Eight-Step Process for Identity and Access Management Audit and Compliance

Roberta J. Witty, Ant Allan, Jay Heiser

Authentication, separation of duties, role management and enforcement, and reporting address the identity and access management requirements of regulatory compliance. Use this eight-step process to establish an ongoing management program.
WHAT YOU NEED TO KNOW

For maximum effectiveness, take an enterprisewide approach — not a siloed application approach — for all separation of duties and role design and management activities. These must be included in the system development life cycle to ensure early coverage of a new system or a major change in the development cycle. Wherever possible, automate processes to streamline and reduce identity and access management audit and compliance costs.

STRATEGIC PLANNING ASSUMPTION(S)

By 2007, investments in identity management tools will increase 60 percent to address regulatory compliance requirements (0.8 probability).

By 2008, companies with a standard, centralized authorization service will achieve a 30 percent reduction in their joint application development/security administration costs (0.8 probability).

ANALYSIS

The need to prove, enforce and monitor the identity and access management (IAM) process, or "who has access to what" and "who accessed what," isn't new to mature security administration programs — especially those in regulated industries (for example, financial service firms bound by regulations from the U.S. Office of the Comptroller of the Currency, the U.S. Securities and Exchange Commission, the Securities Industry Association, the U.S. Gramm-Leach-Bliley Act of 1999 and Basel II). The recent focus on IAM audit and compliance (A&C) is mainly driven by the U.S. Public Company Accounting Reform and Investor Protection (Sarbanes-Oxley) Act — the Section 404 separation of duties (SoD) requirement and the enforcement "teeth" behind it. The U.S. Health Insurance Portability and Accountability Act's privacy regulation in healthcare also requires SoD to protect patient information.

Although Sarbanes-Oxley's Section 404 SoD is focused on financial reporting and the associated applications and IT infrastructure, companies quickly learn that a complete IAM A&C process can expand to include many corporate business processes. It can go all the way back to the initial network logon. Thus, Sarbanes-Oxley's Section 404 SoD touches more than just the financial reporting process.

Here, we'll define an eight-step process for companies to use in meeting their IAM A&C process needs. Use consultants to implement some of the steps — for example, SoD and gap analysis, role-based access control and SoD enforcement.

Step 1: Authentication Enhancement

Enhancing your authentication policies (and enforcing them) is the first step in the process. Start with password formation and aging policies. Best-practice password formation is an eight-character alphanumeric password. The current practice for password aging is 30 days for access to sensitive information and 90 days for access to the network and all other information. However, some companies are rethinking their password-aging policies to accommodate a longer time frame, based on limited evidence that frequently changing passwords reduces the number of security breaches.

We advise using strong authentication technologies to enhance network-level access as a general control — or on a per-application basis, depending on the classification level of the information that's being processed. We also advise companies to use single sign-on (SSO) tools to enhance password management policies, and to provide ease of use for the end user. SSO
tools automatically change the passwords for all participating systems (platform and application), enabling companies to implement a shorter password-aging policy without burdening users. Also, because the passwords are machine-generated, stronger password formation policies can be implemented; thus, some social engineering attacks will be ineffectual because users don't know their new passwords. Stronger authentication should be engaged to close the security gap of a password being used at the initial network logon.

Step 2: SoD and Gap Analysis

SoD is a control mechanism that limits an individual’s ability to perform damaging transactions — for example, you can create a purchase order, but not approve one (static); or you can create and approve a purchase order, but not approve your own (dynamic). SoD takes a business policy and expresses it through rules defined at the application level. For Sarbanes-Oxley, start defining your SoD with those functions that have the biggest violation impact — for example, money-related transactions, such as creating a purchase order, paying a vendor or credit overrides. The enterprise resource planning (ERP) application is the application focal point for SoD definition and implementation. As soon as it's defined, a gap analysis of the "desired" state vs. the "actual" state is needed to uncover SoD violations.

Theoretically, defining SoD can be done on paper. However, the complexity of defining and mapping SoD to application-specific functions (or transactions) quickly makes the manual process unmanageable. Most applications don't provide an SoD rule management and enforcement framework; therefore, more is needed. Companies must use roles to help manage SoD complexity.

Step 3: Role-Based Access Control

The defined SoD and associated application rules can be grouped into business-oriented roles. To simplify administration, rules are applied not against individual user accounts, but rather against named roles to which individual users belong. Separate roles can be used to separate "conflicting" rights, but this doesn't stop a user from being given both roles — unless the application's access control system knows that they can't be combined.

Roles can be granted in three ways:

- **Explicitly** (for example, management approval is required and must be documented)
- **Implicitly** (for example, the company agrees that the role needs no documented approval, such as a full-time employee role)
- **Inherited** (typically due to poor role design or implementation at the platform or application level)

Like SoD, roles must be implemented at the application level, but this gets complex to maintain. User provisioning tools are one way to manage pre-defined SoD and roles, grant access and generate management reports, but they don't enforce access in real time.

During the process of SoD and role development, consider testing the definitions against actual examples within your company. For example, see what a purchasing agent has compared with her boss, the purchasing department head. This is a bottom-up approach to SoD and role definition. You need the top-down approach described in Step 2 and this step for ongoing control.

Step 4: Role Matrix Management

The formal organization structure (for example, the "organizational chart") rarely reflects how day-to-day business is conducted. Companies must show multiple operating views, such as:
• A new marketing campaign project whose participants have specific IT resource access for the duration of the project (for example, six months).

• Country managers have revenue and operational responsibilities for the country, but the formal reporting relationships of employees within the country are to line managers in another country.

• Access to applications can be approved by the requester's manager, except in cases when the approver must have a higher-level title than the requester or the manager. This is called "dynamic approval."

We define this multiple operating view method of managing access and approvals as role matrix management (RMM). All business views must filter down to IT infrastructure access controls. Therefore, the results of the RMM process should feed the user provisioning process. However, most user provisioning tools only manage one view of the organization — the one defined in the corporate directory. Therefore, look to RMM tools to manage this identity management problem. A few user provisioning vendors are starting to extend their tools by providing links to RMM tools, or by providing the functionality as a core service of their tools.

**Step 5: SoD Enforcement**

As soon as SoD and roles are defined, they must be enforced so that violations aren't executed in real time. Unless the application has a fine-grain SoD framework, third-party tools are required for enforcement purposes — that is, identifying violations before they happen, disallowing the function to be performed in real time and notifying appropriate parties that a violation has been attempted.

User provisioning tools can manage SoD, roles and target-specific group membership, but they can't perform the real-time enforcement. Extranet access management (EAM) tools can perform the real-time enforcement of SoD and roles, as well as "dynamic authorization" — for example, finding out who created the purchase order to ensure that he or she can't also approve it. Although this logic is possible in some EAM tools, and is supported by the Organization for the Advancement of Structured Information Standards' XACML, it's far from ubiquitous in applications. In many legacy applications, it will be hard-coded into program logic. To date, most EAM implementations only perform SSO. The integration of a fine-grain authorization structure has only been attempted by complex portal implementations, in which a fair amount of application integration has been required. By 2008, companies with a standard, centralized authorization service will achieve a 30 percent reduction in their joint application development/security administration costs (0.8 probability).

SoD in ERP applications can quickly become too complex to manage without automation. It's a "hot button" for auditors. Because SoD is such a fundamental form of control, and because it's typically so poorly implemented, auditors can be expected to ask for verification and documentation. The use of ERP application-specific tools that manage and enforce SoD and roles is rapidly increasing. Some of these tools can also perform transaction-level monitoring of SoD.

**Step 6: IAM Activity Reporting**

Reporting needs for IAM activities are vast. There seems to be no end to requests to review specific applications, or a group of applications related to a business process. In some cases, access reviews are performed daily on sensitive activities — for example, only two changes can be made each day to the price table. In other cases, once or twice a year — or quarterly — is adequate.

There are three types of IAM reports:
"Who has access to what" reports that are grouped by user, line manager and information owner, including documentation of the day-to-day access request process (requests, approvals, denials of access and unauthorized changes to access privileges).

"Who did what" reports for sensitive information. The entire IT infrastructure — applications, operating systems, databases and directories — must be included.

SoD violations, remediation and exception reporting.

Also, a centralized audit event repository for logging all authentication, authorization and administration activities is needed across the entire IT infrastructure, not just from the user provisioning, EAM and ERP tools. The use of a central repository can greatly reduce the labor needed to report on IAM activities. It can also ease security breach investigations. Basic events to be logged are:

• Moves, adds and changes for all users
• Password resets made from the password management feature/tool and target platforms
• All sign ons and sign offs
• Successful and unsuccessful attempts to access IT assets that are classified as confidential, trade secret or "for your eyes only."

This functionality can be provided by some security information management tools, and also by audit tools that some of the IAM providers offer.

Step 7: Management Review

For IAM A&C, a process must be in place by which management signs off on (or certifies, attests to) the accuracy and appropriateness of access rights assigned to individuals for their job functions at a certain point in time. These reports are produced for each line manager and information owner, then "rolled up" to the highest level of management. The actual access granted to users may not match what's required for them to perform their job functions. Therefore, requests can be made for excessive access to be revoked, or additional access to be provided.

These reports provide an irrefutable "point in time" review of user access, because the information and documentation of the review must be securely stored in a central repository.

Step 8: Ongoing Management Process

Most reviews of IAM activity have been initiated on an ad hoc basis — for example, by an IT auditor, a customer or the security administrator for the application. However, for IAM A&C, an ongoing review of all IAM activity must be established, including a review of SoD, role/access conflict reviews, escalation procedures for conflicts and role implementations. The process must also include a regular review of the information stored in the centralized audit event repository.

The chief information security officer is often responsible for ensuring that such a process exists and is followed.

IAM A&C Automation Infrastructure

The IAM A&C process can be conducted "on paper" once — maybe twice — but companies can't keep spending large amounts of money on the labor-intensive process of managing IAM activities. Automation can reduce such spending and help maintain a secure access control infrastructure. However, there are some obstacles:
• Identity and access information is incomplete and scattered throughout the company.
• Few companies have rationalized their IAM processes across the company.
• There's no enterprisewide strategy for role management, thereby maintaining the disconnect between business needs and the IT access control infrastructure.

The benefits of automating the IAM A&C process include:
• Reduced redundancy and streamlining of the access request process
• Increased efficiency by centralizing administration and reporting activities
• More-easily enforced business rules for "who can do what" and monitoring "who did what"
• Reduced costs for ongoing IAM maintenance and IAM A&C reporting

Many tools automate some portion of the IAM process. However, no single tool provides a complete IAM A&C offering. Therefore, a combination of tools is required: user provisioning, EAM, enterprise SSO, RMM, SoD and centralized audit event logging tools. All of them must be tied to the application portfolio and supporting IT infrastructure (see Figure 1).

Figure 1. IAM and Compliance Automation Infrastructure
Ultimately, an enterprisewide role management process and repository will be required to address the relationship of all business roles and mappings to their associated IT resources.

Key Issues

How will identity and access management evolve as an enterprise infrastructure?

Acronym Key

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A&amp;C</td>
<td>audit and compliance</td>
</tr>
<tr>
<td>EAM</td>
<td>extranet access management</td>
</tr>
<tr>
<td>ERP</td>
<td>enterprise resource planning</td>
</tr>
<tr>
<td>IAM</td>
<td>identity and access management</td>
</tr>
<tr>
<td>RMM</td>
<td>role matrix management</td>
</tr>
<tr>
<td>SoD</td>
<td>separation of duties</td>
</tr>
<tr>
<td>SSO</td>
<td>single sign-on</td>
</tr>
</tbody>
</table>

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509