SCC
Security Compliance Corp

Success Criteria for Entitlement Reviews

Background

When evaluating tools to automate your user entitlement review efforts, determining the evaluation and success criteria is one of the most important steps in the process. On the surface, many types of solutions appear to perform the same functions. Only after using the product for several months in your own environment will you realize that the nuances of **how** the solutions are designed greatly impact your project success.

Success Criteria for Entitlement Review Tools

To help bring clarity to the challenge of conducting entitlement reviews, SCC is publishing this list of some of the most important considerations for identity governance tools. Rather than just a simple checklist, we are including details in plain English. The below six factors will ensure your success.

1. Speed of Implementation

Perhaps the most important criteria in a successful project is how soon you can begin using the new tool and process. Information security tools are notorious for requiring armies of consultants to implement and configure the product. At SCC, we believe that if a software product is truly well-designed, you should be able to install, configure, and use the product in a matter of hours or days, not weeks or months. When deploying Access Auditor, we recommend reserving no more than 2-5 days for full installation, configuration, and training.

2. Identity Mapper and Fuzzy ID

One of the greatest challenges when managing and auditing user access rights is the lack of a username that is consistent for each user across all applications. Most companies have evolved and grown over time, and the number and scope of critical applications have followed suit. User login IDs are often similar but different on many systems (e.g. john.doe vs. jdoe), while others, especially legacy applications, use somewhat cryptic login IDs that have little direct relationship to the user's name.

Avoid the Legacy of IDM Shelfware

According to Deloitte, nearly 50% of Identity Management purchases become "shelfware", undeployed software due to the overwhelming project complexity.

Access Auditor is the Solution

- Discover Who Has Access To What
- Automate User Access Rights Certifications
- Enforce Separation of Duties
- Define and Manage Role Definitions
- Alert to Privilege Changes

Security Compliance Corporation
120 Village Square, Suite 76
Orinda, CA 94563
(866) 657-4550
www.securitycompliancecorp.com
info@securitycompliancecorp.com

The solution to this problem has typically been one of two options. You either spend weeks reviewing these thousands of IDs by hand, or else accept the limitation and never get a complete profile of access rights. Your entitlement review tool should be able to solve this challenge for you.

SCC's Access Auditor includes the powerful Fuzzy ID tool that automatically links and suggests possible matches of user names and login IDs based on a variety of proprietary mathematical models. Within minutes, Access Auditor will identity the multiple login IDs belonging to each person, and allow you to link these disparate accounts.

Customer response has been so strong that our Fuzzy ID is often used as a stand-alone tool to review and clean-out systems before mergers or other data migration projects.

3. Flexible Review Workflows

The core component of a user access review is ensuring that the right people within your company are designated as the approvers of your entitlement review. The tool you select to automate this labor-intensive process should be flexible enough to map to your existing processes and organizational structure, not the other way around.

Access Auditor gives you unlimited flexibility to define your approvers. Beyond the simple rules such as a manager or application/business owner, Access Auditor provides a customizable rules-based workflow engine that assigns reviewers based on any combination of user data, organizational structure, privilege, role, or application. By layering multiple rules, Access Auditor can map to any existing certification process.

4. Full Governance Life Cycle

Automating your user entitlement review efforts should be a complete process. Your solution should provide a full life cycle from data discovery and launching the review, to final compliance reporting and cleanup of inappropriate rights. Access Auditor automates the entire process by:

- **Automating data imports**
- **Reminding approvers with pending work and escalating where needed**
- **Initiating tickets or other workflow to remediate inappropriate access rights**
- **Monitoring the systems of record to ensure the privileges and roles that were flagged as invalid are in fact removed from the appropriate application(s)**
- **Providing full reporting on the evidence of compliance**

5. Cross-Application Separation of Duties

Separation of Duties (SOD) alerting and reporting is very difficult without some type of automated tool such as Access Auditor. Identity governance tools should also provide the additional benefit of automatically reporting and alerting to separation of duties violations. Many enterprise applications provide SOD reports for their own system. However, they are limited to a single application and only a tool that imports data from all applications, like Access Auditor, can allow you to define SOD rules that span disparate systems.

When evaluating access rights solutions, investigate the SOD engine to determine how flexible your rules can be. Any tool should let you define conflict rules based on any combination of privileges, applications, systems, or roles, and further apply them to specific organizational hierarchies.

6. Ease of Use

IT and security tools are notorious for being laden with complicated and busy screens, and a dizzying array of configuration settings that are never used. This will lead to project delays and a difficult user acceptance.

Access Auditor is the easiest-to-use identity tool in the world. End users generally require no formal training and easily “get it”, just like using any common web banking or shopping site. By making the user experience exceptional, our customers succeed in 100% completion.

For over 11 years, SCC takes great pride in our 100% customer success rate. Access Auditor is so simple to use that it is primarily managed by non-technical staff. Our simplicity is the reason that our typical deployment of Access Auditor can be completed in only a matter of days.

Summary

User entitlement review efforts should be simple and efficient. For more information on SCC and our Access Auditor product, please visit us at: **http://www.securitycompliancecorp.com/**. We look forward to helping you gain control over your user access rights and automate the extremely labor-intensive task of user entitlement reviews.

Access Auditor Key Features

FEATURE	DETAILS	BENEFITS
Entitlement Reviews and Access Certification	• Managers review and approve the access rights for their direct reports • Business owners certify entitlements for all audited applications	• Provides company-wide attestation of employee access rights and privileges required for IT best practices and compliance-related audits (SOX, HIPAA, GLBA, ISO 17799, and others)
Consolidated View of User Access Rights	• Identity mapper and Fuzzy ID link user privileges from disparate systems • Access data is organized by business application	• Establishes a single repository of all access data across the entire enterprise • Enhances understanding by relating privileges to applications that are familiar to users
Integration with Existing Systems and Processes	• No agents required for deployment • Compatible with all identity management products and data repositories	• Accelerates deployment by minimizing impact to existing enterprise systems and applications • Provides simple data import methods from both off-the-shelf and custom applications
Real-Time Alerting	• System monitors for changes to user access data • Simple interface for configuring custom alerts and actions	• Generates alerts if access data has changed since the last audit scan • Detects unauthorized changes to systems
Automated Discovery	• User access rights and group memberships are automatically discovered and processed • Support provided for wide variety of commonly used applications without product customization	• Consolidates user data from diverse systems and groups by user and application • Enables Access Auditor to provide a near real-time view of user entitlements
Executive Dashboard	• Progress of on-going reviews reported in real-time • Remediation efforts tracked for inappropriate rights	• Presents current status of compliance efforts at a glance
Role-Based Reporting	• Custom reports show both real-time and historical access data	• Provides documentary evidence of meeting access-related compliance controls • Discovers orphaned or lost user IDs • Reveals users with inappropriate combinations of access rights

Security Compliance Corporation

120 Village Square, Suite 76
Orinda, CA 94563
(925) 255-5686
www.securitycompliancecorp.com
info@securitycompliancecorp.com

Security Compliance Corporation (SCC) was founded in 2005 with the mission of simplifying IT compliance. Based in the San Francisco Bay Area, SCC is revolutionizing the compliance industry by promoting new solutions to common business challenges. Our mission is to help customers realize tremendous business value and cost savings through compliance automation. We are promoting a paradigm shift in compliance by developing automated solutions to labor-intensive compliance efforts.

® Security Compliance Corp, SCC, Access Auditor, and the SCC logo are registered trademarks of Security Compliance Corporation.