CASE STUDY: Cloud Marketing Leader Responsys Automates Identity Governance (IAG) with Access Auditor®

Background

Responsys is a leading provider of email and cross-channel marketing solutions that enable companies to engage in relationship marketing across the interactive channels customers are embracing today—email, mobile, social, the web and display. Responsys serves world-class brands such as: Southwest Airlines, LinkedIn, LEGO, Orbitz, United Airlines, Dollar Thrifty, Newegg, Qantas, Avis Europe, Deutsche Lufthansa, UnitedHealthcare and American Family Mutual Insurance Company. For more information about Responsys, visit responsys.com.

Following a successful IPO in 2011, Responsys wanted to automate identity and access governance (IAG) controls including periodic entitlement reviews, monitoring and alerting to access rights changes, and detecting and removing orphaned accounts from terminated users. CIO Don Smith launched an IAG project to streamline the highly labor-intensive manual process.

The Challenge

Like most companies, Responsys uses Active Directory and several custom applications driven by databases such as Oracle, SQL server, and MySQL. Because Responsys manages information from some of the world's most trusted brands, many unique and custom built applications were in-scope for SOX and needed to be monitored and reviewed.

As a leading Cloud Computing provider, Responsys also relies heavily on products from other Software as a Service (SaaS) vendors such as salesforce.com, Workday, Coupa, and others. A crucial success metric was finding a solution that can automate user access reviews for both the on-premise and Cloud applications.

Another common challenge facing most enterprises is the ability to work with a variety of formats for user login IDs. Some applications relied upon Active Directory while others used an email address or another random format. Each person in the company had multiple login IDs, making it impossible to easily link users across all applications.

The key project goals included finding a solution that can:

The Challenge

To help meet SOX requirements and manage various Cloud applications, Responsys wanted to automate the management and certification of user access rights from both in-house and Cloud vendors such as salesforce.com, Workday, and Coupa.

The Solution

Access Auditor from Security Compliance Corp stood out as the clear choice and the only product to meet the requirements without a large capital expense.

The Results

Within weeks, data from all key applications were imported, and user access reviews underway. The entitlement reviews were simple for approvers across the company, providing high marks for the IT department.

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

- Automate the discovery of user access rights from various on-premise and cloud applications
- Link user accounts from disparate systems
- Automate the entitlement review process to save time and energy
- Ensure that accounts from terminated users are promptly removed

The Solution

One of the first questions to answer when leading an identity-related project is whether or not to pursue a full identity provisioning solution. As Don Smith reviewed the potential solutions, he quickly realized a provisioning tool was not the ideal answer for several reasons:

- Responsys developed and managed a large number of custom applications that had no standard connectors.
- Responsys already deployed Single Sign-On (SSO) connections to their cloud applications via Active Directory SAML, making the automated de-provisioning capabilities redundant.
- At approximately 1000 users, Responsys was not large enough nor did it have enough employee turnover to justify the over $500,000 estimated project costs of a full provisioning deployment.

The ideal solution would primarily address the specific pain points around simplifying entitlement reviews, making it simple for approvers to perform reviews and avoid a spreadsheet nightmare. In addition, the company wanted a solution that was fast and easy to deploy, requiring little ongoing maintenance.

After reviewing various IAG solutions, Access Auditor from Security Compliance Corp stood out as the clear choice and the only product to meet the requirements without a large capital expense. According to Smith, “The Access Auditor product provided the right balance of features and simplicity, being able to handle both our in-house custom applications as well as our cloud vendors like salesforce.com, Workday, and Coupa.”

The Results

Access Auditor provided excellent results for Responsys. Deployment time was rapid, with the team importing data from several key systems within only a few days. A simple to use configuration page allowed Responsys to define the data imports and identity mapping in less than 5 minutes for each application.

Another important result was the ease of linking user accounts from different

“The Access Auditor product provided the right balance of features and simplicity, being able to handle both our in-house custom applications as well as our cloud vendors like salesforce.com, Workday, and Coupa.”

Don Smith
Chief Information Officer, Responsys

systems without a consistent login ID. Since several applications used different login ID formats, the Identity Mapper and Fuzzy ID features provided the ability to link disparate accounts from users across all systems in a matter of minutes.

Additional key success points included:

- The core entitlement review functionality allows reviewers to complete their quarterly reviews in a matter of minutes, ensuring 100% employee participation.
- Access Auditor delivers an automated solution to detect and remediate orphaned user accounts left behind from terminated employees.
- Access Auditor provides simple options for alerting to changes in sensitive privileges and SOD violations.
- Responsys now has a centralized location of all user accounts, essential for saving time and preventing mistakes with transfers and terminations.

A final success for the IT team at Responsys was the rapid adoption by business users across the company. As CIO Don Smith summarizes, “At most companies, user access reviews are a painful process for all managers, causing frustration aimed at IT. In our case, Access Auditor was so simple to use that it required no formal training for approvers throughout the company to gain 100% completion. What could have been a time-consuming requirement for the entire company is instead a non-event, giving IT high marks for easy-to-use automation.”

“At most companies, user access reviews are a painful process for all managers, causing frustration aimed at IT. In our case, Access Auditor was so simple to use that it required no formal training for approvers throughout the company to gain 100% completion. What could have been a time-consuming requirement for the entire company is instead a non-event, giving IT high marks for easy-to-use automation.”

Don Smith
Chief Information Officer, Responsys

Access Auditor Key Features

FEATURE	DETAILS	BENEFITS
Entitlement Reviews and Access Certification	• Managers and business owners certify access rights with a simple web-based solution • Flexible rules-based workflow defines custom approvers at various phases of a certification	• Provides company-wide attestation of employee access rights and privileges required for IT best practices and compliance-related audits (SOX, HIPAA, GLBA, ISO 27001, PCI, and others)
Fuzzy ID and the Identity Mapper	• Links users from disparate applications when no consistent login ID exists • Proprietary name-matching algorithms automatically identify the same user in multiple systems with no common attribute	• Solves one of IT's largest challenges, how to view access rights when no common attributes exist • Eliminates the need to modify applications to insert a unique identifier • Establishes a single repository of all access data across the entire enterprise
Role-Based Certifications and Role Definition Tool	• Defines roles and role memberships • Performs certifications by roles and exceptions to improve accuracy and relevance • Performs what-if scenarios to define cross-application enterprise roles	• Improves relevance of certifications by reviewing a handful of roles instead of hundreds of privileges • Defines and manages roles by comparing role memberships and exceptions
Consolidated View of User Access Rights	• Custom reports show real-time and historical data • Orphaned user accounts from transfers and terminations are detected and reported • Historical record of access rights compliance	• Reveals users with inappropriate combinations of access rights • Discovers orphaned or lost user IDs • Provides documentary evidence of meeting access-related compliance controls
Real-Time Access and SOD Alerting	• System monitors for changes to user access data • Simple interface for configuring custom alerts and actions • Comprehensive cross-application separation of duties reports and alerts	• Generates alerts if access data has changed since the last audit scan • Detects unauthorized changes to systems • Warns business owners if users violate separation of duties rules
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

Security Compliance Corp

Security Compliance Corporation

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

Security Compliance Corporation's (SCC) Access Auditor® automates the periodic review and certification of user access rights and entitlements. SCC's workflow engine provides the ultimate flexibility in defining and managing the periodic attestation of user access rights. The enhanced Identity Mapper™ utilizes a proprietary algorithm to link user accounts from disparate systems back to the correct person, even when common identifiers or login IDs do not exist. Access Auditor's consolidated view of user access rights enables customers to identify orphaned accounts left behind from terminated users, thus reducing the risk of fraud and audit findings. By automating labor-intensive tasks related to user access rights and separation of duties, SCC's customers improve security while minimizing the costs of compliance. Founded in February 2005, Security Compliance Corporation is based in Orinda, CA.

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