CLOSING THE AUDIT GAP WITH
IDENTITY & ACCESS MANAGEMENT

With high-risk applications, significant audit pressures and manual access governance procedures in place, Royal and Sun Alliance, (RSA Group) needed a scalable, business-driven identity and access management (IAM) solution. RSA Insurance utilized the RSA® Via Governance solution to automate collection and certification of user entitlements across critical applications. This resulted in streamlined, business-driven processes that shortened the application review cycle, uncovered orphaned accounts and simplified audit of reviews. With the RSA solution in place, The RSA Group now has an authoritative source for user access of critical systems within their enterprise.

ABOUT RSA INSURANCE GROUP

With a 300 year heritage, the RSA Group is one of the world’s leading multinational quoted insurance groups. Currently they have major operations in the UK, Scandinavia, Canada, Ireland, Asia and the Middle East, Latin America and Central and Eastern Europe, employing over 20,000 people, and have the capability to write business in around 140 countries.

RSA Group selected the RSA Via Governance solution to kick-start a strategic program to improve user access management in the company.

As a leading general insurer, RSA Group is subject to extensive regulatory, risk and audit pressures. Information security is important to them to help lower the risk of insider fraud and ensure that internal applications and related data are properly governed.

ACCESS GOVERNANCE CHALLENGES

With a manual access certification process in place, RSA Group carried out a review of their capability and concluded that it did not provide the scope and depth that they needed. It did not therefore meet their compliance requirements going forward.

Prior to implementing the solution, the security team had tried to gain business backing to implement an end-to-end IDM solution. The costs and complexity had meant that this failed to get off the ground. The RSA solution offered a different approach to the issue – assurance through governance. RSA Group is now recommending this approach across the Group.

OVERVIEW

With a 300 year heritage, RSA Insurance Group (rsagroup.com) is one of the world’s leading multinational quoted insurance groups. RSA Group has major operations in the UK, Scandinavia, Canada, Ireland, Asia and the Middle East, Latin America and Central and Eastern Europe, employing over 20,000 people, and has the capability to write business in around 140 countries.

CHALLENGES

- Manual data collection and certification process resulted in long review cycle times
- RSA Group needed a more efficient and effective process
- RSA Group needed to increase the level of visibility into orphaned, shared and multi-user accounts hampering the ability to scale to the enterprise level with additional applications

BENEFITS

- Efficient and business-user-friendly access reviews
- Scalable solution to add more systems and entitlements into the scope of reviews
- Ability to provide visibility and evidence to auditors
- Established RSA Group as a “single source of truth” for entitlements within critical applications

VISIBILITY AND CERTIFICATION

POLICY AUTOMATION

ROLE AND GROUP MANAGEMENT

REQUEST MANAGEMENT

ACCESS CHANGE FULFILLMENT

Task Notification

Service Desk Integration

Automated Fulfillment

Maturity

SUCCESS STORY
In general, enterprises approach access governance through four phases, as shown in the previous value path. Organizations typically begin with Visibility & Certification, followed by Policy Management. More advanced initiatives will include Role and Group Management efforts, as well as the deployment of an access Request Management system. RSA Group, in their initial project, focused on Visibility and Certification, collecting entitlements from key enterprise applications, and performing certification reviews on them.

**APPRAOCH**

RSA identified several areas of focus needed for the implementation project, while aiming to streamline the existing process for user access reviews and free up time to extend and improve the scope of systems and entitlements reviewed.

**Identify and validate orphan accounts**

Orphan accounts were an issue and couldn’t be included in their review process, resulting in a considerable security and audit gap.

**Change validation processes**

Each set of quarterly access reviews resulted in changes to users’ access – cleaning up any remaining leavers accounts and making revocations in cases where supervisors decided that a user no longer needed a specific entitlement. However, RSA Group was unable to validate whether these access changes were properly executed by IT, or executed in a timely manner, until checked at the next quarterly review.

**Audit and compliance efficiency**

The audit process was a completely manual effort for RSA I.G. in terms of both the business process and data collection process. RSA I.G.’s goal was to be able to meet reporting and regulatory audit requirements more effectively and efficiently.

---

**We were able to make better use of the resources on our team by focusing on process improvements, rather than running business-as-usual reviews**

---

**METRICS TABLE**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Before RSA</th>
<th>with RSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reviewer must proactively maintain or revoke all entitlements</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Clear and central audit trail of delegated recertification</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Post review validation of access changes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>orphan application accounts</td>
<td>Not actively managed</td>
<td>Identified and managed</td>
</tr>
<tr>
<td>Unused AD accounts</td>
<td>Not actively managed</td>
<td>Identified and managed</td>
</tr>
<tr>
<td>Mid-stream review - actions on access changes</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>
Benefits of the RSA Via Governance Solution

With the RSA Via Governance solution in place, RSA Group has been able to streamline and standardize business-driven identity and access processes for their users, reviewers and managers. So far, critical applications have been identified and are managed. Considering these applications are high risk, the creation of a more efficient certification process has significantly enhanced their security posture.

RSA I.G. has realized a number of benefits from the solution, including:

**Improved security posture**
- In-depth review process gives managers visibility into security-compromising scenarios such as shared and multi-user accounts in critical applications
- The entitlement collection process detects old, test and service accounts to further help reduce risk in the business environment
- Orphaned accounts are identified, understood and managed
- A closed loop process introduces a change validation process

**Visibility and clarity**
- With the RSA solution in place, managers have the necessary business context to manage user access
- Reviewers can easily access the online portal to work on their review, save it and go back to it at their convenience

**Flexible Reviews**
- The review cycle can be amended to meet business, regulatory and audit requirements
- Entitlement reviews can be run on an ad-hoc basis to evaluate high-risk applications or entitlements

**Simplified Audits**
- Access review procedures were manual, making audit preparation and participation time-consuming
- Now, RSA Group can share the reporting system with auditors in an easily-understood format

**Next Steps**

The next phase of the project will expand beyond the critical applications that have been connected. Adding new applications into the RSA Via solution will not only improve the review coverage, but increase manager visibility, maintain auditable tracking and establish deeper role mining capabilities. Royal and Sun Alliance now has a firm foundation to build user access reviews, increasing security and satisfying regulatory and audit expectations.

“We were able to gain visibility into system entitlements that we never thought possible.”
<table>
<thead>
<tr>
<th>Why RSA?</th>
<th>Benefits to Customers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designed for Access Governance</td>
<td>The RSA solution is built to address access governance. Unlike competing solutions (which may be bolted onto a provisioning system or created from a collection of unrelated parts), RSA provides a single, unified and extensible data model, designed for the types of data needed for enterprise access governance.</td>
</tr>
<tr>
<td>Enterprise-Class Scale</td>
<td>The RSA Access Management Database (XMDB™) is built on a highly scalable relational database, and processes incoming data at the database layer rather than the application layer. This provides unmatched performance, allowing customers to easily and efficiently manage millions of user entitlements.</td>
</tr>
<tr>
<td>Rapid Time-to-Value and Low total Cost</td>
<td>The RSA Via Lifecycle and Governance platform is designed for rapid deployment, with a focus on configuration rather than coding. Unlike competing solutions that require heavy customization and scripting, the RSA solution reliably delivers customer value rapidly. Over 70% of customers go live within 4 months of purchase.</td>
</tr>
<tr>
<td>Business-Driven Identity and Access Management</td>
<td>The RSA solution uniquely enables business users to be accountable and responsible for making access decisions, while maintaining control and oversight by Information Security. This allows the people with the most relevant identity context to make the best possible access decisions, while ensuring that compliance policies and processes are met.</td>
</tr>
<tr>
<td>Closed-Loop Access Change Management</td>
<td>RSA provides enterprises with confidence (and proof) that access changes have been correctly executed, within a timely manner. Whether access changes are initiated via Service Desks, provisioning systems, email, or through the RSA Via Lifecycle, organizations can be sure that all pending changes are tracked for timeliness, and validated for correctness.</td>
</tr>
<tr>
<td>Designed for Access Governance</td>
<td>The RSA solution is built to address access governance. Unlike competing solutions (which may be bolted onto a provisioning system or created from a collection of unrelated parts), RSA provides a single, unified and extensible data model, designed for the types of data needed for enterprise access governance.</td>
</tr>
</tbody>
</table>