RSA® IDENTIY GOVERNANCE AND LIFECYCLE SOLUTION OVERVIEW

Act with Insight to Drive Informed Security Risk Decisions

BENEFITS

- Gain control and visibility over user access
- Make informed security risk decisions
- Gain rapid time to value
- Attain operational efficiency at lower costs
- Empower your users
- Strengthen your enterprise security and compliance postures

ACT WITH INSIGHT

RSA® Identity Governance and Lifecycle enables the ability to act with insight based on rich identity analytics and decision support metrics that improve management of identity services. RSA Identity Governance and Lifecycle provides a single, centralized repository which houses complete information about identities and data resources, as well as policies around compliance controls, birthright, and user transfer and termination events. With identity context across all resources, users, and attributes, organizations can drive informed security and risk decisions based on insights gleaned from today's state of operations, rather than data points from past reviews and assessments.

- Gain visibility and control over who has access to what, and how they received it, to demonstrate compliance and reduce security risk at lower cost
- Make better informed decisions based on near real-time insight of your current identity and governance posture
- Visualize your core identity and governance activities to better prioritize and manage security and compliance risks. Quickly answer the question, "what should I be working on today—where are my risks and what are suggested recommendations to address them?

DELIVER BUSINESS AGILITY

RSA Identity Governance and Lifecycle makes it easy for users to securely gain appropriate access to resources, while also making it simpler for them to perform "housekeeping" tasks that are necessary for compliance and security, such as delegating temporary access to applications or managers performing access reviews. When the business is empowered, Information Security teams become valued partners.

- Ensure users seamlessly receive appropriate and compliant access to the right resources needed to do their jobs at the speed the business demands
- Achieve business objectives with access to tools and resources that improve employee productivity and effectiveness—providing the business the agility to respond and act to changing market and operational needs
- Gain rapid time to value – RSA's flexible, configuration-based integration approach reduces the heavy burden of customization associated with traditional identity management solutions, allowing for rapid on-boarding and efficient governance and provisioning integration across your IT infrastructure

ACHIEVE A SUSTAINABLE IAM PROGRAM

RSA Identity Governance and Lifecycle helps reduce risks, lower costs and boost operational efficiencies to help organizations achieve a sustainable Identity Governance and Administration (IGA) program.

With RSA Identity Governance and Lifecycle, staff can connect to target systems, administer and manage on-going policy creation, certification campaigns and system maintenance without use of costly customized coding to get up and running, delivering self-sufficiency and enabling repeatable success.

- Attain more efficient IGA operations at lower cost
- Develop and manage measureable and enforceable access policies
- Achieve process optimization for governance and lifecycle

RSA IDENTITY GOVERNANCE AND LIFECYCLE: A PHASED APPROACH TO SUCCESS

RSA® IDENTITY GOVERNANCE

RSA Identity Governance simplifies how user access is governed across the enterprise. RSA Identity Governance makes it possible to achieve sustainable, compliance by fully automating the monitoring, reporting, certification and remediation of user entitlements.

- Gain enterprise-wide visibility into all user access privileges—who has access to what--to safeguard information assets and provide evidence of compliance
- Identify orphan accounts and inappropriate user access to reduce risk of audit failure and data breaches
- Automate access review and certification processes for greater operational efficiency, cost and time savings—flag issues between formal review campaigns
- Transfer responsibility and accountability for access certification to the people who understand access needs best—the business. Business-driven certification negates "rubber stamping" of access approval.
- Implement security and compliance controls (e.g., segregation of duties, unauthorized access permissions) to ensure that policy and control objectives are continuously being met

RSA® IDENTITY LIFECYCLE

RSA Identity Lifecycle streamlines access request and fulfillment processes using business language to ensure users, both new and those changing roles, gain timely and appropriate access to the resources they need in accordance with compliance objectives.

- Automate the entire access request, approval, and provisioning process—in business-friendly and easy to understand language--to ensure users quickly obtain appropriate access
- Automate the fulfillment of access requests and changes to significantly reduce the time, cost and effort of manual provisioning processes that expose the organization to access errors and audit failures
- Simplify the user access request and approval experience, enabling the business with an easy way to request and approve access and prevent users from circumventing policy and process
- Transfer responsibility and accountability for access approval to the people who know their access needs best—the business
- Enforce Joiner, Mover and Leaver (JML) processes to reduce security and compliance risks

Complementary Add-Ons

RSA® DATA ACCESS GOVERNANCE

RSA Data Access Governance provides visibility, monitoring, certification and reporting of user access permissions to unstructured data resources stored on Microsoft Windows, Linux and UNIX file servers, network-attached storage devices and Microsoft SharePoint servers.

- Achieve visibility and control of who has access to unstructured data resources for greater protection of information assets and ease of compliance
- Define business owners, and perform access reviews for data resources for faster, more cost efficient access certification
- Enable the business to be accountable and responsible for who has access to what data to increase security and compliance
- Meet new compliance requirements around data access while lowering costs associated with legacy or manual processes
- Establish a closed-loop validation process for changes to data access permissions to more quickly detect out-of-band access that may indicate a security breach

RSA® BUSINESS ROLE MANAGER

RSA Business Role Manager delivers top-down and bottom-up role discovery, creation, modeling and suggestion. RSA Business Role Manager helps streamline access based on 'birthright' entitlements associated with specific job roles (e.g., HR Managers receive access to HR system)

- Ensure more accurate and complete governance and provisioning of users in accordance with Joiner, Mover, Leaver policies based on job roles
- Take a metrics-driven approach to role modeling based on pattern analysis and policy validation, resulting in a simplified process for collecting, assessing and analyzing established roles as well as defining new roles
- Achieve automated role certification, which ensures that business managers participate and buy into role assignments
- Build a trusted system of record for reporting and analytics, enabling organizations to optimize roles by monitoring usage and effectiveness and to track role changes for audit and compliance

EXTEND THE VALUE OF YOUR RSA PORTFOLIO INVESTMENTS

Today's solutions are being asked to solve bigger security challenges than originally intended. RSA Identity Governance and Lifecycle helps reduce 'identity' security risks by integrating with complementary RSA solutions to extend the value of your RSA investments.

- Works with RSA® SecurID® Access to provide a *complete, integrated* Identity & Access Assurance solution that removes the need to tradeoff between security and convenience and eliminates "Islands of Identity"
- Works with RSA Archer for:
  - Continuous monitoring of identity controls to reduce risk
  - Improved incident response with business and identity context
  - Access decisions based on application risk
- Works with RSA Security Analytics to:
  - Provide general identity context for the security analyst including access logs
  - Make identity information available to better inform the investigative process
  - Provide identity information to the behavior analytic engine as input data to discover risky user behavior
  - Provide privileged user information to the security monitoring system

RSA

www.RSA.com