SecurID™

The Six Essentials of Identity Governance and Lifecycle Management

With a constantly changing workforce connecting to more resources from more devices and locations, it's critical to deliver the right access efficiently—and manage it effectively. To do that, you need identity governance that puts your team at an advantage in every aspect of identity governance and lifecycle management.

The full set of capabilities on the following pages isn't a wish list or a collection of nice-to-haves. It's everything you need to ensure identity managers can handle everything they're called on to do. With an identity governance solution that delivers every essential capability, you'll be ready to make short work of today's unprecedented access challenges.

1 Empower Users With Self-Service Password Management

Self-service password management empowers users to set and manage their own passwords at their convenience. That not only improves the user experience; it reduces the burden on your team and lowers helpdesk costs.

It starts with onboarding…

Look for password management that provides:

- Self-directed one-time onboarding and identity confirmation
- Enrollment from anywhere, anytime
- Browser-based self-service AD password resets

…and goes way beyond AD

Choose a self-service solution that offers:

- Simple workflows for updating passwords for Salesforce, Workday and other integrated enterprise applications
- Tracking and documentation of password updates and requests
- Approval workflows for shared or service accounts—including non-human accounts

Deliver a better user experience, reduce the administrative burden and lower helpdesk costs.

2 Improve Compliance With Easy Access Certification

As access rights have grown more complex, so have access certifications—which can lead to inefficiencies at best and compliance failures at worst. Automating the process of ensuring the right people have the right access eases demands on your team and increases compliance success.

Less effort…

Speed access reviews with technology that enables:

- Quick, simple setup, plus maximum scheduling flexibility
- Analysis and guidance to ensure an efficient, focused process
- Automatic prioritization of high-risk review items

…more compliance

Improve compliance with a certification process that provides:

- Audit evidence that leverages identity analytics
- Reports mapping to major compliance frameworks
- Templates, dashboards and charts to document results

Speed and simplify the process of ensuring the right people have the right access.

3 Reduce Access Risk With Automated JML Processes

Joiners, movers, leavers: They all represent weak points in your organization's access security—whether a result of conferring excess access when someone joins, neglecting to adjust privileges when their role changes or failing to terminate access when they leave. Automation shores up every point of weakness.

Secure access at every stage…

Make sure your identity governance solution has processes in place for:

- Data-driven, pinpoint-accurate granting of birthright access and entitlements
- Automatic changes to access privileges when someone's role changes
- Application-specific access policy management with fine-grained controls

…and insights for improvement

Gain insights from visibility into entitlements, such as:

- Number of joiner-mover-leaver transactions
- Breakdown of cost savings through automation
- Calculation of return on your investment in automation

Start with the right access, and easily keep it that way to the end—no matter how a user's role changes.

4 Support Compliance With Role-Based Access Control

In a role-based access control (RBAC) framework, access privileges are aligned to job functions based on a user's role within the organization. This streamlines access management and makes it easier to address compliance requirements for user access.

The easier you make role management…

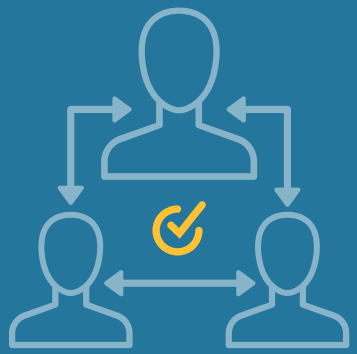
RBAC simplifies role management with:

- Access and entitlements that are linked to roles
- Ability to delegate role management to immediate supervisors
- Role mining to connect roles to entitlements

…the more effectively you can manage access and compliance

Streamlined role management makes it possible to:

- Apply policies and grant access across multiple users based on role
- Provide business context for entitlements and permission that require review
- Meet regulatory requirements through close management of how data is accessed and used



Streamline access management and ease compliance by decentralizing role management.

5 Manage Unstructured Data Risk With Data Access Governance

Because unstructured data comprises most of the data in the digital universe today, it presents the biggest governance challenge—not just because there's so much, but because its unstructured nature makes it hard to protect. That makes managing the access risk it poses a critical part of identity governance.

First, lay the right groundwork

Adopt comprehensive data access governance to gain:

- Visibility into unstructured data stores
- Comprehensive mapping of data use and ownership
- Remediation of user access permissions

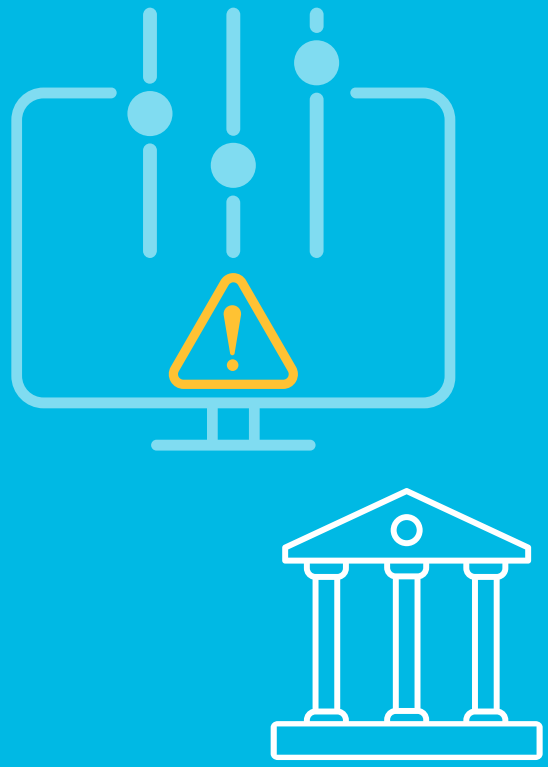
Next, realize the benefits

A strong foundation of data access governance provides the knowledge to:

- Get unstructured data to the right teams to unlock new ideas
- Stop the exfiltration of sensitive financial data, PII and IP
- Meet regulatory requirements for protecting access to information

Understand and manage the access risk posed by vast amounts of unstructured data.

6 Ensure Machine Accountability With Strong Governance



Thanks to robotic process automation (RPA), people are doing fewer sequential, repetitive tasks—and enjoying more freedom to take on higher-value work. But the "bots" entering the workforce pose identity risk just as human workers do, and strong governance of machine accounts is essential.

Establish complete visibility into machine identities

Strong governance of machine accounts starts with visibility into:

- Machine access privileges, permissions and powers
- Tracking of bot accounts that have been issued but not used
- The roles machine accounts have been assigned

Automate governance of machine accounts

Automating governance-related tasks enhances access risk management:

- Provisioning and deprovisioning of machine accounts
- Time-binding that ties robotic access to project completion parameters
- Ability to delete (or designate inactive) an unused machine account

The "bots" entering the workforce pose identity risk just as humans do, and strong governance of machine accounts is essential.

SecurID Governance & Lifecycle

Comprehensive capabilities for today's governance challenges

SecurID Governance & Lifecycle delivers everything you need across the entire spectrum of capabilities for identity governance and lifecycle management.

- **Self-service password management** provides self-directed user onboarding for both remote and onsite users and extends self-service to password resets for enterprise applications, with out-of-the-box workflows to enforce application-specific password policies.
- **Easy access certification** makes the process fast, repeatable and error-free, and includes the ability to schedule access certifications by type of review; a multi-step review capability to streamline workloads; and features designed to avoid review fatigue and improve audit performance.
- **Automated JML processes** ensure appropriate, compliant access throughout the user lifecycle and provide visibility and dashboards for insights from user actions—in a flexible, simple to deploy solution with a straightforward, configuration-based approach to creating JML rules.
- **Role-based access control** capability centers on a unique Business Role Manager module that allows a diverse line of business and IT personnel to participate in role development and management, including role mining and bottom-up or top-down role engineering.
- **Data access governance** provides a dedicated module for owners of data—especially hard-to-protect unstructured data—to control access and map data users, owners and access permissions. The goals are threat reduction, regulatory compliance and improved digital risk posture.
- **Governance of machine accounts** empowers organizations with knowledge of the access and actions available to machine accounts and with capabilities to govern machine access in the same way traditional human identities and access are governed.

Learn more about **SecurID Governance & Lifecycle** and **SecurID Governance & Lifecycle Cloud**.

About SecurID

SecurID, an RSA business, is the trusted identity platform for 13,000 organizations around the world, managing 50 million identities and providing secure, convenient access to 30 million users. SecurID empowers organizations to thrive in a digital world, with complete capabilities for modern authentication, lifecycle management and identity governance. Whether in the cloud or on-premises, SecurID connects people with the digital resources they depend on everywhere they live, work and play. For more information, go to **securid.com.**

SecurID™
An RSA Business