CA Identity Governance

At a Glance

CA Identity Governance helps improve the efficiency and effectiveness of identity governance initiatives by automating processes based on a business-relevant foundation. It is designed to embed the business context and security controls required in activities such as entitlements certification, role management and privilege cleanup in order to drive better alignment between the security, IT and business organizations. This helps deliver reduced cost, better service to users and minimized security exposure.

Key Benefits/Results

- Establish a clean set of user entitlement data to support risk and compliance efforts.
- Prevent security vulnerabilities through consistent identity governance policy enforcement.
- Increase compliance efficiency by streamlining certification processes.
- Reduce resources required to develop and maintain accurate role-based models.

Key Features

Privilege cleanup. Examine existing system entitlements and highlights excessive or unnecessary privileges.

Identity and access governance policies. Centralized engine helps establish and enforce a consistent set of business and regulatory compliance policies.

Entitlements certification. Provide an easy-to-use interface through which managers or resource owners can view and certify that privileges are appropriate or should be removed.

Role modeling. Advanced patent-pending analysis engine helps efficiently sort through extremely large volumes of user and privilege information to discover potential roles.

Simple deployment. Pre-configured common use case templates, along with a virtual appliance deployment model make deployment easy, with no custom coding.

Business Challenges

IT organizations face ongoing pressures to reduce operational expenses while managing compliance with a growing list of industry and governmental regulations. With today's highly distributed and evolving organizational structures, organizations require business-wide processes to review and approve entitlements and maintain accurate roles. Such processes should involve the business (since line managers often best understand their users' needs), so it is important to minimize the time and cost of reviewing, editing and approving entitlements, while providing the proper business context.

Unfortunately, the compliance framework incorporating review and approval of access rights and policies is often manual. Many IT organizations still manually email spreadsheets to business managers. Similarly, they send printed reports of user entitlements as an ad-hoc dump to auditors. These approaches are labor-intensive and inefficient and make adherence to segregation of duties and other compliance policies arduous.

Automating these processes around the proper business context drives genuine collaboration, which helps meet compliance requirements while improving security.

Solution Overview

CA Identity Governance is designed to automate identity and access governance processes and provide continuous identity controls. This starts with leveraging a business-friendly role foundation to present information to users in the context that makes sense to them. It also checks security policies and highlights violations to business managers during identity processes such as entitlements certification.

CA Identity Governance's patented advanced analytics improve the time-to-value of activities such as privilege cleanup and role discovery. Combined with a powerful policy engine, this provides the foundation to help align security, IT and business organizations.

By automating processes and controls based on more accurate entitlements, organizations can be confident that users' access is maintained at the level they actually need, thereby reducing the organization's security risk profile and enabling it to more easily demonstrate compliance.

Critical Differentiators

The graphic on the right highlights the components of the CA Identity Suite, including the role management and analysis, access request, and entitlement certification capabilities of CA Identity Governance. The identity portal provides an intuitive, business-oriented experience that is specifically tailored for the needs of the business user. It greatly simplifies management and governance of user access and improves user and manager productivity. CA Identity Governance can lower operational costs while improving compliance with an enterprise-scale architecture and a robust set of capabilities tailored to both business and IT personnel. It surpasses traditional solutions by automating compliance processes and leveraging a powerful analytics engine to quickly assess, build and maintain accurate entitlements and roles.

By automating processes and controls based on a more accurate entitlements, role and policy foundation, organizations can be confident that access is maintained at an appropriate level. This can reduce the organization's security risk profile and enable it to more easily demonstrate compliance to internal and external auditors.

CA Identity Governance also delivers integration to other CA Technologies solutions, including CA Identity Manager and CA Single Sign-On.
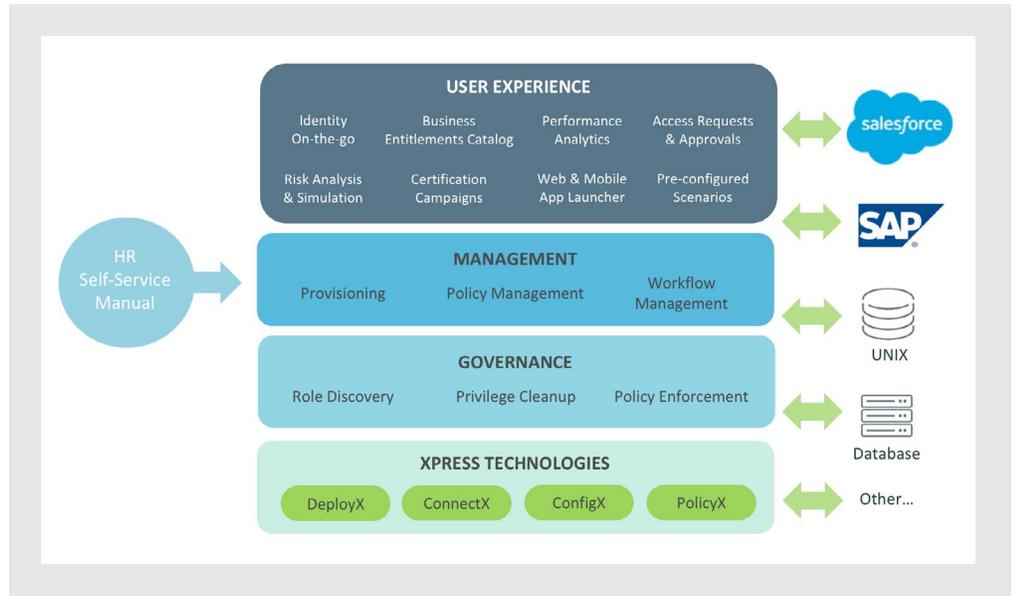
CA Technologies supports a comprehensive approach to identity and access governance by supplementing technology with robust services and educational offerings. CA Technologies has the experience and proven methodologies needed to help you implement identity management in a way that delivers rapid results now and into the future.

Related Products/Solutions

CA Identity Manager (formerly CA IdentityMinder) provides identity management for a user's entire lifecycle.

CA Privileged Access Manager controls the actions of privileged users. The Identity Suite provides full governance of these users, for a complete privileged user solution.

For more information, please visit **ca.com/ca-identity-governance**