BUYER'S GUIDE • MARCH 2018

ca technologies

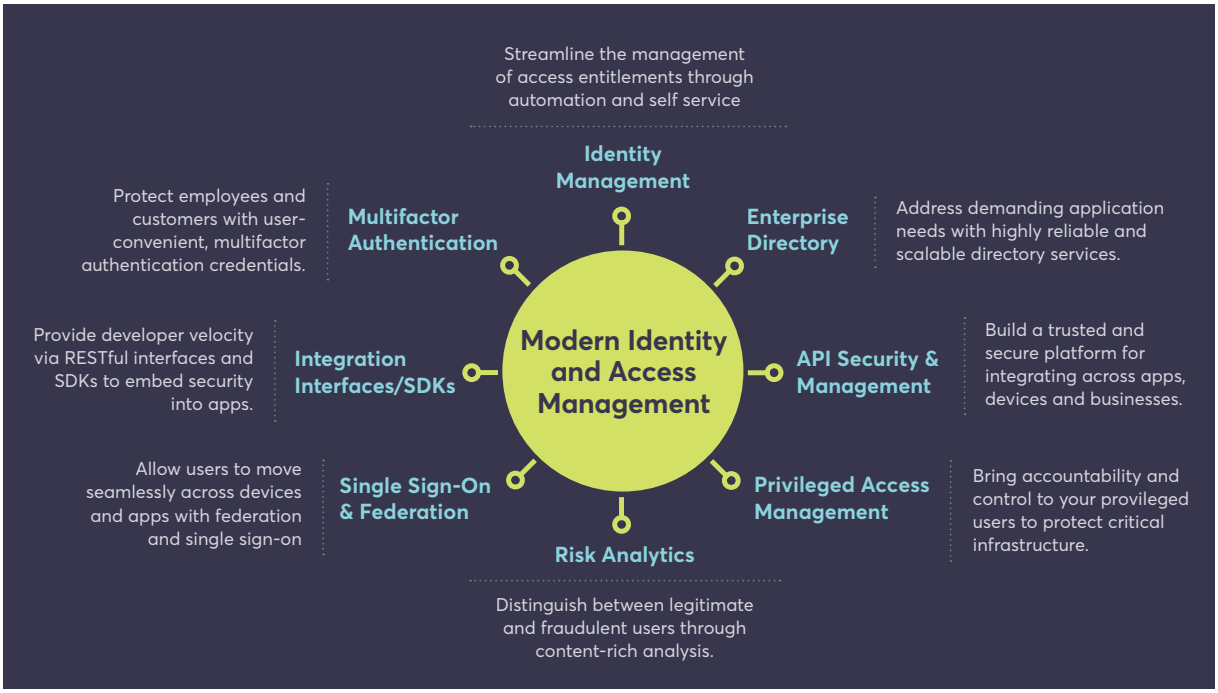
Identity Management and Governance

Overview

For those charged with selecting all or part of their organization's identity management and governance solution, making the right decision may seem like a daunting task. A comprehensive solution can involve many different components, including identity compliance, role management, user provisioning, service request management, password management and some other functions. These elements are often intertwined, presenting both an opportunity for greater value and a risk of increased complexity. Today's end users are inundated with data—they need modern identity governance solutions that provide risk analytics and insight to make better decisions. As part of an integrated solution, we provide a single source of truth unifying governance and provisioning data that can streamline audit and service request management.

Organizations must also choose solutions that can accommodate multiple consumption models, including containerized solutions for deployment in the cloud and on-premises, production-ready monitoring and workflow catalogs that accelerate time to value. Today's end users are also mobile and expect a more "consumerized" user interface. As a trend, organizations are extending internal provisioning solutions to address consumers as well, because this streamlines customer onboarding and protects access to customer data. Buyers must also think about the technology integrations. Time to value is critical today, and solutions must support workflow catalogs that allow security teams to accelerate deployment. As organizations implement privileged access control and enforce the use of named accounts versus the use of administrative accounts, the governance solutions must integrate out-of-the-box with privileged access control tools. In the current cyber-risk landscape, buyers must select a solution that can accommodate a defense-in-depth approach integrating single sign-on, advanced authentication and threat analytics. This document provides a guide to help you determine what's most important in selecting an identity management and governance solution.

Today, organizations need to choose a modern IAM solution that can provide economies of scale managing internal employees and external users, while providing flexibility to address the requirements of businesses today and scale to accommodate digital business transformation. CA's modern identity and access management provides a foundation for trust in the digital economy.



Identity Management and Governance Landscape

According to a leading market survey, one out of three companies had failed an external audit in the preceding three years, while an equal number had failed an internal audit. Meanwhile, two-thirds of IT security officers said their identity and access management processes were too manual and insufficiently automated.

Another research report indicated that 87 percent of organizations believe individuals have too much access to information resources that are not pertinent to their job description. Another 61 percent of organizations did not check access requests against security policies before access was approved and assigned.

These findings highlight many of the security and compliance challenges that organizations face in today's ever-changing and competitive business environment. As organizations push to acquire new companies and address new, emerging markets, IT departments are faced with an overwhelming burden to enable the business with new services, maintain security and reduce risk exposure, all while streamlining operations to reduce cost. Providing "IT at the speed of business" demands the use of innovative technology to scale beyond manual human limits. Identity management and governance solutions provide this agility and speed by automating the processes involved in enabling and managing access to applications and information in an efficient, scalable and secure way. Additionally, this technology allows organizations to reduce risk and comply with ever-changing compliance mandates in an efficient and repeatable way.

Identity Risk and Compliance Challenges

For most organizations, compliance is not optional. Compliance teams need to prove that adequate controls are in place and achieved in the most cost-effective manner. Automating compliance processes such as entitlement certification or identification of orphaned accounts allows compliance teams to stop their continual scramble to meet audit deadlines.

Most organizations address external regulatory and internal security requirements through a combination of security policies and procedures that mandate appropriate behavior and validate that users have appropriate access on a regular basis. These processes require proactive monitoring for inappropriate access and/or activity on enterprise systems. This "needle in a haystack" approach relies on experienced business managers, application owners and often heroic efforts by the compliance team and is not only time-consuming but also error-prone and difficult to repeat.

Identity management and governance proactively enforces security policies during the provisioning process and automates the remediation of inappropriate access when it is identified. Comprehensive role-modeling and strong compliance policies enhance the provisioning and access certification process to further streamline compliance activities and enable users to have appropriate access. By automating these processes and controls, organizations can remove the reactive, fire-drill tone from compliance initiatives.

Operational Efficiency of Identity Processes

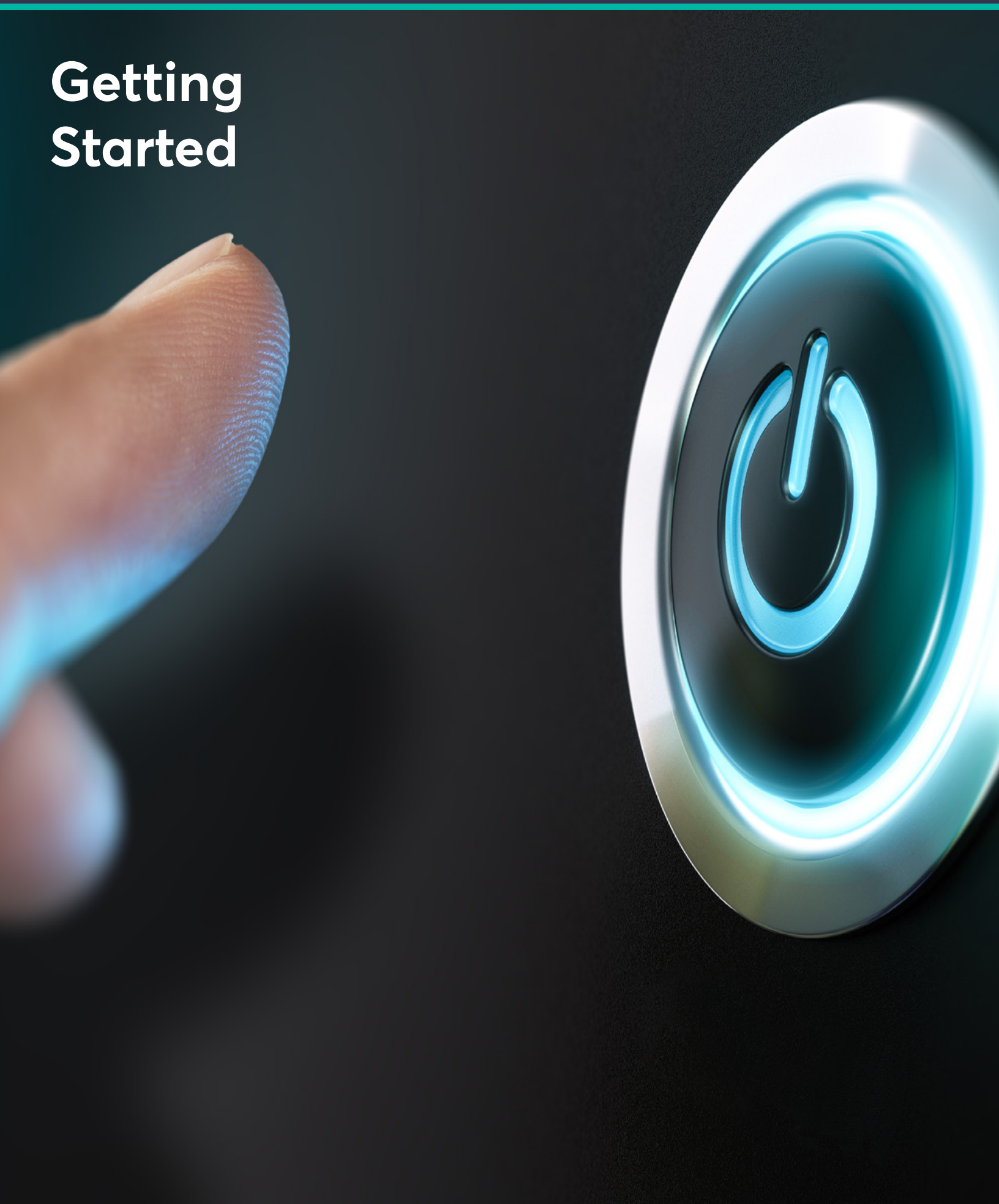
Managing user identities and their access to critical information over the full lifecycle involves many different processes, including user onboarding/enrollment, password management, self-service, service requests, access certification and de-provisioning. In many organizations, these processes are performed manually or are only partially automated. Through automation, your organization can achieve reduced administrative costs and reduce security risk introduced by inconsistent or manual processes.

In addition, perhaps more than any other enterprise security domain, identity management and governance processes require active and meaningful participation from end users. This involvement can be difficult to foster through manual and ad-hoc processes. By providing consistent, automated processes, users are provided with a better experience, delivering higher satisfaction and increased efficiencies across the organization. Identity management and governance solutions also offer additional security controls, such as workflow approvals, preventative segregation of duties policies, role-based access control and auditing, further securing and simplifying the organization's processes.

Focus on Business Users

Identity management processes today, including the request for new access, are far more user-centric than in the past. Users request access when they need it and can now perform many of the functions that were previously done by a central IT group. As identity processes become accessible by a wider variety of business users, user experience becomes critical to the success of any deployment. Interfaces and available capabilities can no longer be oriented toward the IT-savvy user only. They must be simple and intuitive for the business user and must provide consistent experiences across the device of their choice without compromising IT needs. In fact, a recent Aberdeen report indicates that a focus on the user experience can increase user productivity by 60 percent and improved user satisfaction by 80 percent.

Getting Started



Often, one of the biggest challenges with identity management and governance projects is determining where to start. Because these projects involve multiple areas of the business, it is important to consider breaking it down into smaller, more manageable phases. Taking an incremental approach enables you to develop a robust, long-term strategy and roadmap while providing quick wins to the business. These wins draw support from key stakeholders, raise awareness and deliver immediate ROI to help drive future phases of the project.

To help you through the process of evaluating solutions, CA Technologies has created this buyer's guide. Designed to help your organization develop a clear understanding of the key characteristics and components of an effective solution, it provides guidelines to help you think through what really matters as you evaluate a variety of products and technologies.

The successful implementation of an identity management and governance solution goes well beyond a focus on the supporting technology. Additional focus areas should include:

- Current and emerging best practices, both general practices and those specific to your industry
- Regulatory changes that can impact what you implement and how and when you implement it
- Engaging and communicating with numerous stakeholders, both within and outside of your organization

Identity management and governance has many potential capabilities, each of which offers valid business value. The key is determining which components are most relevant to your unique business challenges and prioritizing those that will deliver the most value. Careful planning and the identification of long-term objectives will be key to a successful implementation. This planning includes the selection of a technology and a flexible approach that can adapt as your business changes, allowing your organization to get in front of the next generation of business and compliance requirements.

Solution Evaluation Matrix

Designed by CA to assist you in your selection process, the Identity Management and Governance evaluation matrix presented here details the features most critical to a comprehensive solution. Each section provides a brief overview of the major categories of a solution and discusses specific capabilities that should be considered.

Current State Assessment

One of the most critical elements of a successful identity management and governance initiative begins well before the solution deployment begins. To lay the groundwork for future success, the first step is to understand where your organization is today and build a business case for moving forward. The key is to perform a quick assessment of core areas to identify the sources of greatest need and potential. The assessment stage usually involves a high-level analysis of all of the key identity management and governance components. Each component area will be discussed in more detail in subsequent sections.

Current State Assessment: Does the solution ...	CA	Others
Import real data from other systems and establish an understanding of your current identity, role and privilege state within five days?	✓	
Quantify the number of users, groups, roles and privileges in each of your key target systems?	✓	
Assess current privilege quality and role definitions?	✓	
Identify simple cleanup opportunities (e.g., orphaned, redundant, unnecessary accounts/ groups/ privileges)?	✓	
Identify and quantify: • Exceptional and suspected privileges? • Inconsistent privilege assignments? • Users with excessive access rights? • Shared and privileged accounts that may pose security risks?	✓	
Identify risk and compliance needs, existing process flaws and potential deployment roadblocks?	✓	
Deliver results of various role discovery methodologies and the ideal combination to meet your organization's needs?	✓	
Provide estimates of the time and effort required to implement full identity compliance, role management, provisioning or other projects?	✓	
Create custom segregation of duty policies or business process constraints and identify violations?	✓	

Easy to Deploy, Configure, Scale and Maintain

The market for identity governance and administration has matured, and as a result buyers find they need to extend the solutions across the entire company, as opposed to a single department. Buyers should select a solution that can quickly configure to accommodate the volume and variety of compliance processes they need to automate. Time to value is critical: Select products that can deploy and allow upgrades to be done without the complexity of upgrading multiple layers of technology. Today, operational scale is not optional—it is mandatory. Choose solutions that can accommodate more than exist today and can scale to accommodate the extended attributes required across the entire company. When companies are adopting provisioning solutions, they are also using the same solution to provision their consumer users.

Easy to Deploy, Configure, Scale and Maintain: Does the solution offer...	CA	Others
Flexible deployment model—containerized solution for public, private cloud or on-premises?	✓	
Upgradeability—can the solution upgrade all components in a singular upgrade process?	✓	
Simplified deployment—drag-and-drop deployment and ability and elastic scale?	✓	
Scalability—provide out-of-the-box configurations for scalable production deployments?	✓	
Easy to test—provide predefined demo and sandbox environments for testing?	✓	
Production readiness—dashboard to monitor and report on all components production?	✓	
Workflow catalogs—provide an updatable catalog of workflows to select from?	✓	
Deployment templates—to build on which simplify workflow and policy definition?	✓	
Workflow collaboration—provide the ability to share workflows among groups?	✓	
Ease of policy definition—provide a policy definition and maintenance tool?	✓	

Privilege Cleanup and Quality Control

The assessment often reveals that the current state of users, roles and entitlements does not accurately represent how your organization functions today. The first step in many identity projects is to correct this current state by establishing an accurate baseline of users and their access rights. This involves creating an identity repository based on the data from existing authoritative sources and applications, correlating this access and then identifying any out-of-pattern entitlements or user anomalies. This stage is critical, as it will become the foundation for all of the other identity management and governance stages. This step is also commonly a recurring one, periodically collecting and analyzing user access information to further refine policies and processes.

Privilege Cleanup and Quality Control: Does the solution...	CA	Others
Support the creation of an identity repository across the entire IT landscape?	✓	
Provide a consolidated view into users, roles, their associated privileges and the linkages between each?	✓	
Support import and export to/from: • SAP (including users, roles and authorizations)? • Microsoft Windows® file shares? • Mainframe systems (including RACF and Top Secret)? • Active directory? • UNIX® systems?	✓	
Allow import and data management processes to be immediately executed or scheduled to run on regular intervals?	✓	
Support generic data import and export through CSV and LDIF?	✓	
Automatically identify and remediate privilege exceptions such as: • Out-of-pattern entitlements? • Orphaned accounts, roles or resources? • Privileged collectors?	✓	

Privilege Cleanup and Quality Control: Does the solution…	CA	Others
Automate processes to ask user managers or role/resource owners to validate necessary exceptions?	✓	
Have powerful reporting capabilities providing the ability to generate standard out-of-the-box reports and build ad-hoc/custom reports through a rich point-and-click user interface?	✓	

Identity Governance

Evolving external compliance and internal security requirements continue to exert pressure on organizations to regulate access to their applications and systems. Specifically, they must ensure that users only have access to the resources they need to perform their job function. This can be accomplished through a combination of proactively preventing users from gaining conflicting access rights in the first place and promptly identifying instances where inappropriate access has been assigned. Identity management and governance solutions address these challenges by providing centralized identity compliance policy controls and automating the processes associated with meeting security and compliance demands.

Identity Governance: Does the solution…	CA	Others
Provide a point-and-click interface for defining business and regulatory policies?	✓	
Support the building of policies based on: • Segregation of duties? • Business constraints such as location, job function, ownership or other criteria? • Cross-system policies?	✓	
Support the assignment and monitoring of risk for any combination of access rights?	✓	
Allow risk score assignment based on a combination of business conditions (e.g., user location, function, etc.)?	✓	
Automate entitlements certification based on: • Users? • Roles? • Resources?	✓	
Identify relevant accounts and easily execute certification campaigns for subsets of data, for example: • Potentially "toxic combinations" of entitlements identified through pattern-based analysis? • Entitlement changes between a set of dates? • Orphaned accounts?	✓	
Highlight policy violations to users during the context of certification campaigns?	✓	
Provide native integration with provisioning systems for automated remediation?	✓	
Reveal insight to compliance status through dashboards and reports?	✓	
Include a comprehensive integrated approval system?	✓	
Expose its policy engine via Web services for use by third-party systems (e.g., provisioning, help desk solutions)?	✓	
Allow administrators to set up automated email reminders and alerts?	✓	
Provide the ability to require comments when certifying user access that contains a policy violation?	✓	

Identity Governance: Does the solution...	CA	Others
Natively integrate with privileged user management solutions to import data from and define an access certification for shared/privileged accounts?	✓	
Provide out-of-the-box integration with privileged access management?	✓	

Role Management

While the direct impact of roles is sometimes not obvious on the surface, they are the critical enablers that make all other identity management and governance processes more effective. They provide a critical layer of abstraction that simplifies management of users and their access by eliminating the need to examine each instance on an individual basis. A good role model also provides the business context that makes identity processes relevant and understandable to business users.

Role Management: Does the solution...	CA	Others
Support comprehensive role lifecycle management, including role discovery, administration and adaptation?	✓	
Instantly discover roles using pattern-based analytics?	✓	
Support role discovery using top-down, bottom-up and hybrid approaches?	✓	
Provide proven role discovery methodologies out-of-the-box, each with easily customizable parameters?	✓	
Discover roles based on: • HR attributes (e.g., department, title and location)? • A combination of HR attributes? • Patterns between existing users and privilege assignments?	✓	
Visually display linkages between users, roles and resources?	✓	
Help merge the results of multiple role discovery methodologies?	✓	
Provide reports that show the coverage of access rights?	✓	
Support "what if" simulations of proposed role changes?	✓	
Complement identity management and help desk solutions with closed-loop import and export?	✓	
Scale to accommodate millions of users and tens of millions of access rights?	✓	
Enable Web-based role administration and flexible workflow?	✓	
Detect business changes that require changes to the role model?	✓	
Automate business processes for role approval, self-service requests and role adaptation?	✓	
Support processes for review, approval and change requests for roles and privileges?	✓	
Expose its role analytics engine via Web services for use by third-party systems?	✓	

User Provisioning

Diverse user populations require timely access to multiple applications and systems. Managing this access is a daily concern that cannot be ignored. Ideal provisioning tools minimize the complexity of identity management by automating the process of creating, modifying, disabling, removing or deleting accounts in an effective and reliable way. In addition, these solutions provide powerful yet easy-to-use tools for security administrators to define and configure these processes.

User Provisioning: Does the solution…	CA	Others
Support user communities both inside and outside of the enterprise (e.g., employees, partners, contractors, suppliers)?	✓	
Scale to support provisioning to millions of users and administration of tens of millions of identities?	✓	
Proactively evaluate segregation of duties and identity policies as provisioning events are initiated?	✓	
Provide fine-grained delegation, with support for start and end dates for each delegation?	✓	
Enable creation of business logic and workflows without coding?	✓	
Include a comprehensive integrated workflow system?	✓	
Support role-based access control with fine-grained entitlements?	✓	
Enable administrators to schedule task execution for a future point in time?	✓	
Support reverse synchronization of entitlements changes made at endpoint systems?	✓	
Provide the ability to synchronize Active Directory with cloud-based endpoints?	✓	
Evaluate changes made at endpoints against established identity policies before synchronizing them across systems?	✓	
Provide out-of-the-box integration with key mainframe and distributed systems (e.g., SQL, PeopleSoft, SAP)?	✓	
Provide a wizard-based interface for building connectors to custom applications?	✓	
Expose all user-interface tasks as Web services for embedding in third-party interfaces?	✓	
Provide out-of-the-box identity reports, a reporting engine and open reporting database?	✓	
Enable as-built configuration reporting, difference comparison and the seamless import and export of configuration data between environments (development, test, production)?	✓	

Service Request Management

When users encounter issues related to their identity or access rights, their default reaction is often to contact your IT or help desk organization. This can be costly for the organization and can present the user with a less-than-ideal experience. Identity management and governance solutions empower users to initiate or resolve identity issues on their own for activities such as password resets, access requests or profile updates.

Service Request Management: Does the solution…	CA	Others
Support self-registration and self-administration capabilities for global users?	✓	
Provide a Web interface through which business users can: • Update elements of their user profile? • Manage their passwords and set challenge/response questions? • Request access to a role or entitlement? • Request access to a business service or application? • Request creation of a new role? • Retrieve or reset a forgotten password after validating a user's identity?	✓	
Provide integrated user management capabilities to Web access management systems or corporate portals?	✓	
Include a ticket management system?	✓	
Provide interactive login services through Windows graphical identification and authentication (GINA)?	✓	
Enforce strong password policy requirements, including password expiration, password inactivity, dictionary verification and percent different, in addition to the standard requirements (min./max. length, require upper, lower, number, special characters, etc.)?	✓	

Business-Oriented Interface

Many solutions have user interfaces that are unduly technical and non-intuitive, especially for business users such as managers, compliance executives and other employees who just want to perform basic operations. A business-oriented interface that provides a convenient, simple user experience is essential to improving business productivity and user satisfaction.

Business-Oriented Interface: Does the solution…	CA	Others
Provide a "shopping cart" where users can conveniently select roles and entitlements needed to perform their job duties, view current access privileges and check the status of previous requests?	✓	
Provide a business-friendly entitlements catalog that makes entitlement certification more understandable for businesspeople?	✓	
Offer a one-stop shop for all user identity information and settings?	✓	
Have a centralized Web and mobile application launcher?	✓	
Provide risk analysis to highlight risky access requests?	✓	
Have embedded identity process analytics?	✓	
Provide a mobile interface for users to access on tablets and phones?	✓	

Identity Management and Governance Solutions From CA Technologies

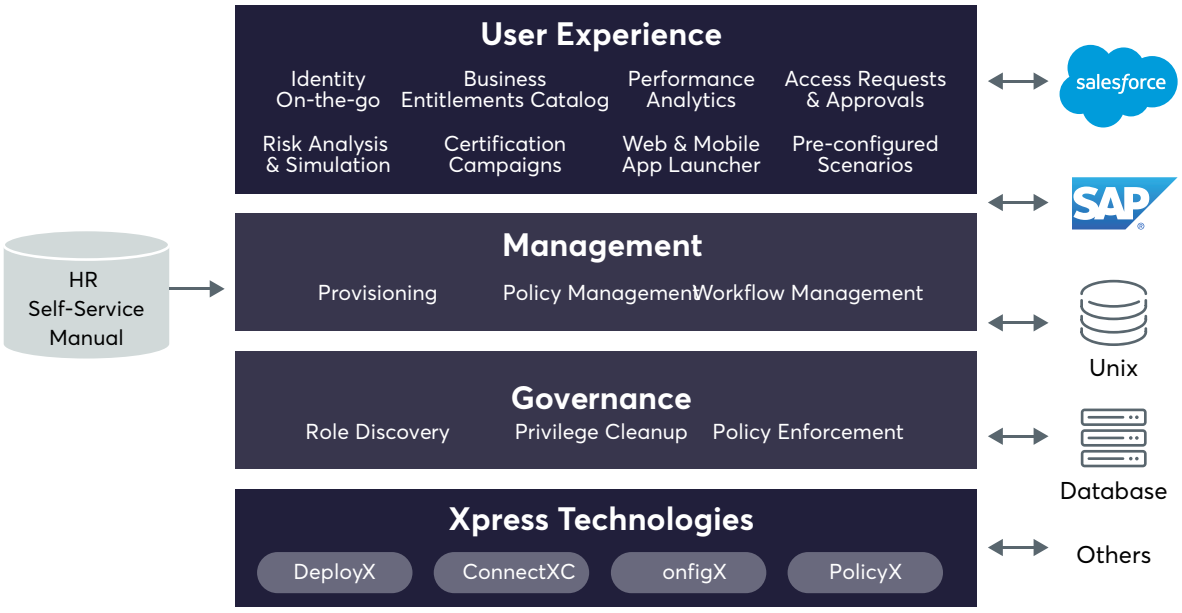
Identity management and governance solutions from CA Technologies deliver the extensive capabilities required to effectively manage and secure user identities, govern their access and control the actions of privileged users and shared accounts. These capabilities include user management, access governance, role management and mining and user provisioning, as well as fine-grained access controls and shared account management to reduce the risk of privileged users.

The products that comprise identity management and governance solutions from CA Technologies include:

- **CA Identity Manager.** Provides identity administration, provisioning/de-provisioning, user self-service, and compliance auditing and reporting. It helps you establish consistent identity security policies, simplify compliance and automate key identity management processes.
- **CA Identity Governance.** Leverages analytics and workflow to automate identity governance processes, including entitlements cleanup, certification, segregation of duties and role management. By automating these processes and controls, it helps you reduce risk, improve compliance and increase operational efficiency.

The CA Identity Suite combines CA Identity Manager and CA Identity Governance with a simple, intuitive business-oriented interface, CA Identity Portal, which dramatically simplifies the access request process for business users through an intuitive "shopping cart" where users can conveniently select roles and entitlements needed to perform their job duties, view current access privileges and check the status of previous requests. By automating the risk analysis and certification processes and enabling remediation actions in real time during the access provisioning steps, CA Identity Suite improves audit performance and risk posture with preventive policy enforcement.

These components and their core capabilities are illustrated in this graphic:



Connect with CA Technologies

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

CS200-346564_0318