Simplify Identity Governance and Reduce Risk With the CA Identity Suite
Section 1: Challenge

Identity Governance Challenges

Ensuring that each user of IT systems has the correct entitlements is one of the most important challenges facing IT today. Because of the importance of this capability, the following functional areas are the most important when designing a governance program:

• **User experience**—Identity services are often plagued with inconvenient user interfaces that focus on the IT-savvy user rather than the business user. This reduces user satisfaction and hinders more widespread adoption across the enterprise. For governance activities this is particularly important because it is often business managers who have to interact with the identity services.

• **Privileged user governance**—Most organizations have no formal governance of privileged users or have inconsistent mechanisms for privileged and regular users. This increases management costs and the risk of breaches.

• **Role discovery and lifecycle management**—Ineffective role models can be identified by many symptoms. Some organizations have more roles than users, while others have too many users or resources associated with a given role, or are managing too many exceptions to the role model. In many cases, the organization doesn’t even know that it has “de-facto” roles that create high management costs and increase risk.

• **Identity compliance**—Particularly with today’s highly distributed organization, enterprises require business-wide processes to review and approve entitlements, maintain accurate roles and help ensure identity compliance. Such processes should involve the business since line managers often best understand their users’ needs. An automated, business-centric approach to certifications is critical not only for proof of compliance but also for improving productivity of business managers who have to conduct the certifications.

• **Quality of entitlements**—“Entitlement creep” is a familiar problem to all IT security managers. All users’ entitlements must be carefully monitored to ensure that unneeded ones are removed and that existing ones don’t violate segregation of duties (SoD) or other security policies.

Identity Governance Challenges—The Details

Identity Compliance

Identity compliance activities focus on verifying that the access maintained by users is in adherence with regulatory requirements and internal security policies. This requires a lifecycle approach with iterative processes, typically including the following steps:

• Collecting data, correlating access rights to their owners and basic cleanup of unnecessary entities (e.g. orphan accounts, excessive access, etc.)

• Formulating an identity compliance model, including mapping of regulations to written policies (in the form of control objectives), then mapping these control objectives to an implementation of IT controls, such as segregation of duties constraints

• Verifying IT controls in real-time as part of privilege cleanup, certification, provisioning and other identity processes

• Periodically testing the IT controls by conducting business/IT reviews or certification tests

• Remediating or mitigating key findings and refining related IT controls
Role Management

Role management focuses on the complete lifecycle of building, testing, maintaining and optimizing the role model quickly and cost effectively. A typical role lifecycle process includes the following steps:

- Collecting data, correlating access rights to their owners and basic cleanup of unnecessary entities (e.g. orphan accounts, excessive access)
- Simulating multiple-candidate role models in a sandbox environment, comparing their technical and business merits and establishing an initial role model
- Business and IT review of the proposed role model
- Ongoing or periodic review and comparison of the approved role and access model and actual assignments to identify exceptions
- Cleanup of unnecessary exceptions as well as refining the model as the organization continues to evolve
Although identity compliance and role management are frequently viewed as distinct activities, the two disciplines are highly interdependent, with shared processes and information. For example, both require the same foundational steps of data collection, correlation and privilege clean-up and both can employ certification for certain processes.

Section 2: Solution

CA Identity Suite—Key Capabilities

The CA Identity Suite is an integrated suite of identity management and governance capabilities that combine robust functionality with an intuitive, convenient and business-oriented experience. By improving business user productivity and satisfaction, the CA Identity Suite user experience is designed to dramatically increase the IAM solution value proposition for large enterprises while removing a significant administrative burden from the IT organization. The components of the CA Identity Suite are represented by the following graphic:
CA Identity Governance addresses identity compliance and role management challenges with an integrated lifecycle approach based on a centralized entitlements warehouse, process automation and powerful analytics engine. This approach can deliver rapid time-to-value, for example, enabling organizations to establish a role model quickly (weeks rather than months), with better access rights coverage (often 70 to 80 percent) and better alignment to business needs and preferences.

Let’s look at the key governance capabilities of CA Identity Suite in more detail, starting with analytics and role management.

**Analytics Engine**

A unique and powerful aspect of CA Identity Governance is its patented pattern-recognition engine. This robust analytics engine can quickly examine entitlements and roles to highlight abnormal access rights. It then suggests entitlements that should be reviewed for potential removal or considered for aggregation into business roles. These analytics are the key to quickly building a role model with sufficient privilege coverage or developing an accurate entitlements foundation.

Analytics can reveal the patterns that are hidden in existing sets of privileges, as well as discover out-of-pattern privileges that indicate access which may require removal. This process is not trivial—modern organizations that have evolved through mergers, acquisitions and organizational restructuring often end up with excessive privilege assignments. Adding to this complexity is the amount of data and relationships that must be analyzed, since even medium-sized organizations with only a few thousand employees can often have hundreds of thousands of access assignments.

CA Identity Governance features robust analytic capabilities (in terms of scalability and the strength of algorithms used) that uniquely leverage these capabilities not only as a preliminary role-discovery tool, but also as a strategic decision-support engine that streamlines many identity-related business processes. Examples of activities which may benefit from analytics include:

- Mapping of users to the accounts they own across enterprise applications
- Cleaning up of excess and erroneous access rights
- Discovering candidate roles using existing users and account information or optimizing role structures
- Comparing different strategies for role modeling and finding an optimal approach for balancing business and IT requirements with the reality of current access assignments
- Highlighting suspected assignments in entitlement certification processes
- Highlighting suspected privilege assignments as a preventative control during provisioning actions

Role Discovery

CA Identity Governance provides the ability to examine user, role and privilege relationships and suggest candidate roles. The analytics engine applies pattern recognition and other advanced algorithms to automatically discover common access assignments that may represent roles. A number of discovery methodologies are provided to identify these commonalities and role engineers can choose to use one, some, or all, depending on the nature of their organization. Each discovery method has modifiable inputs such as scope of search, tolerance thresholds or attribute-related parameters. These methodologies include:

- **Basic roles** identify individuals sharing common entitlements to resources, but who have been left unclassified by the existing role structure. This is often referred to as a “bottom-up” approach, as search is started from existing privilege assignments.

- **Obvious roles** group users that share exactly the same resources or a set of resources that have exactly the same users.

- **Characteristic roles** leverages patterns of resource assignments existing around logical groups, such as organizational units, functions, locations and reporting structure. This is often referred to as a “top-down” approach, as search is started from the organizational structure and maps users to business functions.

- **Rule-based roles** identify users or resources that meet some set of user attribute criteria, such as organization and organization type and share access to common resources.

- **Hierarchical roles** discover relationships between parent/child roles or related roles which share users and/or resources but are neither parent nor sub-role. End points including SAP or mainframe systems consume hierarchical and related roles, therefore, these relationships are important to consider.

- **Modeled-after roles** construct roles based on the entitlements of an existing group of users or resources. CA Identity Governance can use these groups as models for other users or resources.

CA Identity Governance also provides quantifiable key performance indicators for each potential role model, such as coverage percentage, role-to-user ratio and role-to-resource ratio. This allows role engineers to consistently assess the value of each methodology and combinations of resulting role models. Role discovery can be applied to environments without existing roles (to suggest an initial role model) or those with existing roles (to suggest optimizations and improvements).

Role Lifecycle Management

CA Identity Governance provides a robust set of capabilities for visualizing and managing a role model after discovery. This includes create, update and delete operations, workflow-enabled approval processes and a simple, intuitive user interface. In addition, roles can be enhanced by providing business context, including business terminology, role descriptions, ownership, aggregation into logical groups and organizational orientation. This additional context becomes critical as roles are exposed to business users during identity-related processes.

As a best practice, role models should be regularly analyzed for potential updates based on organizational or other business changes. To this end, CA Identity Governance supports importing existing role models and optimizing them without disrupting the production environment. This is done by using multiple sandbox configurations that are separated from the production environment. Configurations can be compared, merged or promoted to production. Multiple sandbox configurations provide a safe way to test what-if scenarios and continually adjust and improve the role model until it is ready for deployment in the production environment.
Privileged User Governance

CA Identity Governance has been integrated with CA Privileged Access Manager to provide a common, consist governance mechanism across both regular and privileged users. This supports consistency and reduces the risk of users with improper privileged access.

The CA Identity Suite enables provisioning of access to privileged accounts, as well as identification of current privileged users to help remediate users with excessive entitlements. Access to privileged accounts can be requested, approved and certified using the regular capabilities of the CA Identity Suite, including the simple, business-focused user experience. The fact that most breaches are caused by improper access to privileged accounts makes this capability a critical one for overall risk reduction.

Pattern-Based Audit

Audit cards are on-demand reports of users, roles and privileges that meet specific criteria based on pattern-based algorithms or compliance policies. These are the basis for examining existing entitlements in CA Identity Governance to identify orphaned accounts, excessive access and otherwise improve privilege quality. For example, an audit card using the “suspected collector user” criteria will identify users with a higher than normal number of privileges—the degree of which is specified by the analyst. These users and their access rights are marked as “suspected” and require further review and possible clean-up of excessive rights.

Audit card results can be used immediately, stored persistently in the database or exported to a file system via Extensible Markup Language (XML). They can be used by various types of users, including auditors, IT personnel and business users. For example:

- Auditors can use audit cards in offline mode to answer ad-hoc forensic queries about archived sandbox configurations.
- Role engineers can use audit cards to check what-if scenarios by applying role model changes to a configuration snapshot and running audit card queries on top of both production and sandbox configurations and comparing results.
- Business managers can use audit cards indirectly, when business processes such as entitlement certification use the results to highlight key findings and scope down the amount of data presented to business users.
Identity Policy Enforcement

CA Identity Governance allows organizations to create and enforce sets of business process rules (BPRs) to implement segregation of duties and other logical constraints on relationships between users, roles and privileges. For example, a BPR can enforce that “people with permission to access X cannot have permission to access Y,” or a dependency relationship such as “only people with access A can have permission to do B.”

The BPR syntax supports the definition of constraints at the level of roles, privileges or combinations of the two and can leverage the organization’s role model to define a minimal number of policies to cover the necessary constraints. BPRs can include extensive business context, including business description, risk score, organizational area and grouping of rules into a logical hierarchy. This is an important part of defining BPRs, as they are often used by many types of users with varying levels of business and technical understanding.

The BPR engine was designed to act as a centralized service for all identity-related compliance rules and across all related business processes, supporting flexible controls:

- **Detective control.** Utilizing BPRs as the basis for audit cards, this ad-hoc query method identifies policy violations found against a single BPR or multiple sets of compliance policies.

- **Corrective control.** Incorporated into the entitlement certification process, BPR violations can be visually highlighted in the context of users validating the need for certain entitlements.

- **Preventative control.** BPR, integrated with CA Identity Manager provisioning actions, help prevent access changes that will introduce new compliance policy violations.

Access Certification

A common approach to meeting regulations and corporate compliance mandates is to periodically validate that users have appropriate access to corporate resources. During access certification, managers must review lists of their direct reports’ privileges and either confirm or reject the need for this access. The CA Identity Suite makes this process simple and intuitive, thereby increasing user satisfaction and productivity.

Tailoring a certification process to an organization’s specific needs is critical to effectively validate access and encourage participation in the process. CA Identity Suite can solicit review from multiple perspectives, such as user managers, resource owners or role engineers. Certification processes, called campaigns, can be executed for each of these perspectives, using different schedules, workflows and approvers. In addition, multiple campaigns can be executed concurrently, each scoped to portions of the organization (e.g. users in a specific business unit) or highlighting different types of access (e.g. only suspected assignments or access gained outside the role model).

CA Identity Suite includes robust administrative controls and workflows to help ensure campaigns progress according to requirements. This includes email notifications, reminder alerts and escalation processes for requesting approval from higher-level managers. In addition, robust realtime analytics are provided so that the actual efficiency and effectiveness of key identity processes (such as certifications) can be easily determined. Bottlenecks can be identified and corrected quickly so as to ensure that SLAs can be met.
The user experience for access certifications is simple and business-oriented. Managers can easily certify access for a single user or a group of users. They can also delegate approval to another manager and the workflow will reassign the certification to the other manager. In addition, they can “consult” with another manager, who will get a request for an opinion so that the correct authority can be brought into the certification process easily. In addition, the approving manager can easily see (in one-click) the responses that they gave at the last certification, greatly simplifying the entire process.

In addition, each certification operation includes contextual information about current policy conformance and the risk level for each access entitlement. This information is essential to the manager so as to reduce the risk of improper access being certified.

The screen shot below highlights the intuitive nature of the certification interface.

Figure D. Access Certification Interface

Workflow

Various pre-defined workflow parameters can be set during the creation of a campaign. In addition, workflow can be customized to create alternate behaviors that address specific business needs, such as support for multi-level approvals, email notifications, requiring a minimal number of certifiers and many others. Workflows are externalized as a set of editable processes.

These processes are constructed using building blocks that expose core CA Identity Governance functionality in modular packages. Modification to default processes or creation of new processes can be accomplished using a library of building block modules. Building block behavior can be changed through parameter settings. Administrators then map these processes to CA Identity Governance workflow tasks to make custom behaviors available.
The following illustrates some examples of workflow processes that can be achieved:

- Parallel approval is allowed by multiple reviewers.
- X out of Y approvals is allowed, for example, requiring three out of five approvers to approve an access right. Requiring a minimum number of approvals is similar to voting on a business change.
- Allow a higher level reviewer to override other reviewers to approve or reject a privilege link.
- Weighted approval allows assignment of a numerical weight to the approval response of each reviewer. Overall approval is then determined by a threshold value for approvals. When the weighted sum of approval responses meets or exceeds the threshold, the review action concludes.
- Delegation allows users to specify another person to direct their tasks to while they are out of the office. When a task is delegated to another user, that user becomes the owner of the task.

Reports and Dashboards

CA Identity Suite includes embedded identity process analytics that provide detailed, easy-to-process information that highlights the operation of key identity processes (such as user onboarding). These analytics help identify and remediate bottlenecks and help ensure that you are meeting your service level agreement commitments.

CA Identity Governance includes an extensive set of out-of-the-box reports and dashboards while supporting ad-hoc queries for forensic requirements. Reports vary in the level of business and technical information provided in order to address the needs of the different user types. This includes separate reports for business managers, role engineers, compliance officers, auditors and IT personnel, for example. Reports are categorized in the following groups:

- **Privilege quality** provides key metrics and supporting details about the quality of existing or proposed access. This includes statistics on users, roles, resources, lists of overlapping roles and suspected inappropriate access. These reports are often used to understand the gap between the current and desired state or to highlight areas for privilege cleanup.

- **Entity-centric** provides a complete view for a specific user, policy, role, resource or other type of entity. These reports also highlight key findings such as entities that violate BPR policies or appear to be suspicious, out-of-pattern entities.

- **Role analysis** compares the results of various role modeling methodologies and provides detailed analysis of current role structure (e.g. users with similar privileges that are currently not members of the same roles). Role engineers can use these reports to review suspected roles or to provide evidence that roles conform to best business practices.

- **Compliance** provides business managers, compliance officers and auditors with a robust view of policy controls, campaign progress and associated risk. This includes audit card reports which review key findings such as explicit policy violations and suspicious assignments. Entitlement certification reports display the process progress status as well as the process details.
Section 4: Benefits

Benefits of a Business User-Centric Approach to Identity Governance

The identity governance capabilities of the CA Identity Suite enable organizations to simplify access requests and approvals, streamline certifications, reduce role management complexity and remediate improper access rights. The solution also provides capabilities and benefits that are significantly better than those available in other solutions, such as:

An Intuitive, Business-Oriented User Experience

The CA Identity Suite provides an outstanding user experience. Key identity governance capabilities such as access requests, certifications and role management are available in an intuitive, business-oriented experience. Access requests and approvals can also be localized to the language of the respective user, providing improved usability especially for multi-national companies. The result is improved user satisfaction as well as increased productivity.

This business-oriented user experience can help bolster the success of any major governance program. We want business managers to be directly involved in these processes because they understand the roles and entitlements of their users. As identity services are being used directly by a wider range of users, especially somewhat non-technical users, the user experience becomes critical to the success of the program. Wider adoption usually means wider support of the entire program.
Reduced Risk

By automating processes and controls based on a more accurate entitlements, role and policy foundation, organizations can help ensure that the access entitlements for each user are appropriate for their specific roles. In addition, privilege cleanup capabilities can highlight excessive privileges and identify potential security policy violations across the large set of user entitlements. Risk-based access approvals also give approvers important contextual information about the risk level of each access request. These capabilities can improve the organization’s security risk profile and enable it to more easily demonstrate compliance to IT auditors. Finally, privileged user governance helps ensure that all privileged accounts are accessed only by properly authorized users.

Simplified Role Management

An advanced patent-pending entitlement analysis engine helps efficiently sort through extremely large volumes of user and privilege data to help identity de-facto roles and simplify the underlying role model. This capability enables your organization to quickly assess, build and maintain accurate entitlements and roles. A centralized engine simplifies the management of roles and helps establish and enforce a consistent set of business and regulatory compliance policies.

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.

Connect with CA Technologies at ca.com