

TECHNOLOGY BRIEF

CA Role & Compliance Manager | December 2010

CA Role & Compliance Manager: Capabilities and Architecture

Michael Liou

CA Technologies Security Management

we can



table of contents

executive summary

SECTION 1

The Market Need **4**

SECTION 2

Introduction CA Role & Compliance Manager **5**

Identity Compliance 5

Role Management 6

Architecture 7

Analytics engine 9

SECTION 3

Key Capabilities **10**

Pattern-based audit 10

Identity Compliance policies 10

Entitlements certification 11

Role discovery 13

Role lifecycle management 14

Workflow 15

Reports & dashboards 15

SECTION 4

Conclusion **17**

executive summary

Challenge

IT organizations face ongoing pressure to reduce operational expenses while stringent industry and governmental regulations make the ability to demonstrate regulatory compliance more critical than ever. A key to dealing with these challenges is implementing procedures to secure user identities and the access they have to applications and systems. For example, validation processes, such as entitlements certification, can be effective in showing auditors that access is secure and appropriate but they are often costly and manually driven. Meanwhile, the identity, entitlements and role foundation on which business processes are built are often based on poor data, leading to additional inefficiency or security exposure.

Opportunity

By automating processes for managing and validating user access, IT can significantly improve security, operational efficiency and the business user experience. CA Role & Compliance Manager delivers centralized policy controls and process automation to help meet these demands. In addition, its pattern-recognition engine enables IT to identify inappropriate access and develop a role foundation in a fraction of the time required by traditional methods. Leveraging an accurate identity, entitlements and role model for Identity Management and Governance activities can improve the success for various activities including provisioning, certification and service request management.

Benefits

Streamlining Identity Compliance processes can simplify regulatory compliance by helping enable the organization to demonstrate adherence with government and industry regulations while following the access principle of least privilege. Further, by improving the fundamental quality of entitlements and roles, IT reduces costs and minimizes impact on the business by simplifying the administrative burden of assigning and maintaining access rights to resources. Security may also improve as IT can appropriately revoke or reassign entitlements when individuals leave or change job functions within an organization.

Section 1: The market need

Many organizations face ongoing challenges in cost-effectively demonstrating compliance with corporate and regulatory policies. Particularly with today's highly distributed and evolving organizational structures, 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), 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 business review and approval of access rights and policies is often manually driven. For instance, many IT organizations still manually email spreadsheets to business managers, listing their employees' roles and entitlements for review. Similarly, they send printed reports of user entitlements as an ad-hoc dump to auditors. Not only are these approaches labor-intensive and inefficient, but they also make adherence to segregation of duties and other compliance policies extremely arduous.

Using traditional approaches, improving existing privilege quality and building an optimal role structure can require significant investments to understand how users actually access computing systems and which groups of users should have access to what resources. In particular, companies often struggle with developing and maintaining a role structure that accurately covers the most privileged assignments with as few roles as possible, especially as the organization evolves.

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. A role model with too few roles, for example, may mean Identity Management systems are used only for rudimentary account management operations (e.g. creating accounts), while IT administrators are still required to manually assign entitlements for finer-grained access management (e.g. making users members of application groups).

Section 2:

Introducing CA Role & Compliance Manager

CA Role & Compliance Manager 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.

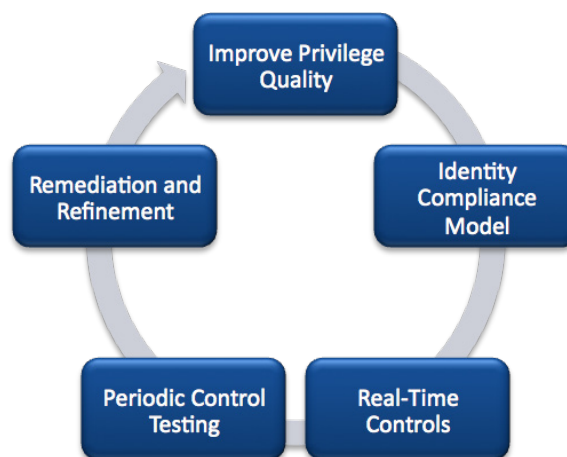
Identity Compliance

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

Figure A

Identity Compliance involves a series of related activities designed to help ensure that users have the appropriate access on an ongoing basis.



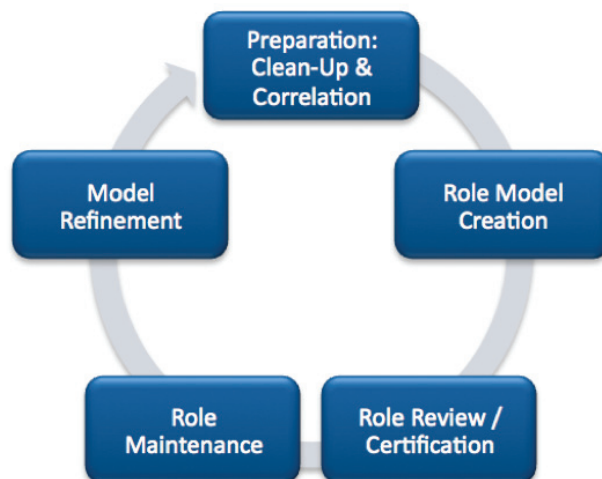
Role Management

Role Management focuses on the complete lifecycle of building, testing, maintaining and optimizing the role model quickly and cost effectively, and doing so in a way that covers most of an organization's access assignments. 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

Figure B

Role Management activities create a clean entitlements foundation and build a simplified model of who should have access to what resources.



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. CA Role & Compliance Manager enables organizations to build effective role foundations while delivering the policies and processes to help ensure that privileges are appropriately assigned to users.

Architecture

CA Role & Compliance Manager has been designed for enterprise-grade scalability with the ability to perform sophisticated analysis on massive amounts of information. It provides a Web-based user interface to address the needs of business users, as well as a client-based user interface for technical analysts to navigate and drill down into various levels of detail about users and their access rights.

In CA Role & Compliance Manager, a snapshot of users, roles, resources and related entitlements is called a configuration. An organization can maintain multiple configurations simultaneously, each containing knowledge about entitlements at a given point in time or a segment of the user or resource population. Configuration data can be saved locally as a file or directly to the server.

Key product components include the following:

CA Role & Compliance Manager (RCM) Server. Provides a Web-based, business-oriented user interface, as well as back-end services including the analytics engine, workflow service and reporting engine. The server is implemented as a Java 2 Platform, Enterprise Edition (J2EE) application and follows service oriented architecture concepts with a loosely coupled set of services that communicate via sets of externally available Web-service application programming interfaces (APIs) which support a range of queries and interactions, including:

- **Data update/exchange.** Endpoints can submit provisioning changes directly to the CA RCM Server which will update the appropriate configuration and deliver related provisioning updates.
- **What-if queries.** Provisioning solutions can use CA Role & Compliance Manager analytical tools to test proposed provisioning changes for compliance or out-of-pattern issues.
- **Service extension/integration.** External applications or resources can be directly integrated into CA Role & Compliance Manager workflows. For example, CA Role & Compliance Manager entitlements certification campaigns and other processes can interface with SMS or other messaging platforms to send users task or status notifications.

CA Role & Compliance Manager (RCM) Client. Designed for role analysts and technical auditors, these tools provide a complete environment for development and maintenance of the role and compliance model. This includes functions such as import/export of entitlements data, privilege quality reviews, role discovery and modeling, compliance risk and policy modeling, audit queries and simulation of what-if scenarios. The CA RCM Client supports both online and offline work modes.

Database layer. An entitlement warehouse stores a master configuration, representing current user, role, resource and privilege relationships, as well as any number of additional configurations representing variants of these relationships. Additional configurations are used for storing historical and sandbox snapshots allowing role engineers to test what-if scenarios and potential model changes without interfering with the organizational production operation. A runtime database stores the system configuration information, including general parameters, workflow templates, workflow instances and audit.

Workflow server. This component supports the implementation and processing of customizable, ticket-based workflows. For example, certification and approval campaigns are modeled as workflow processes, then implemented through coordination between the CA RCM server and the workflow server.

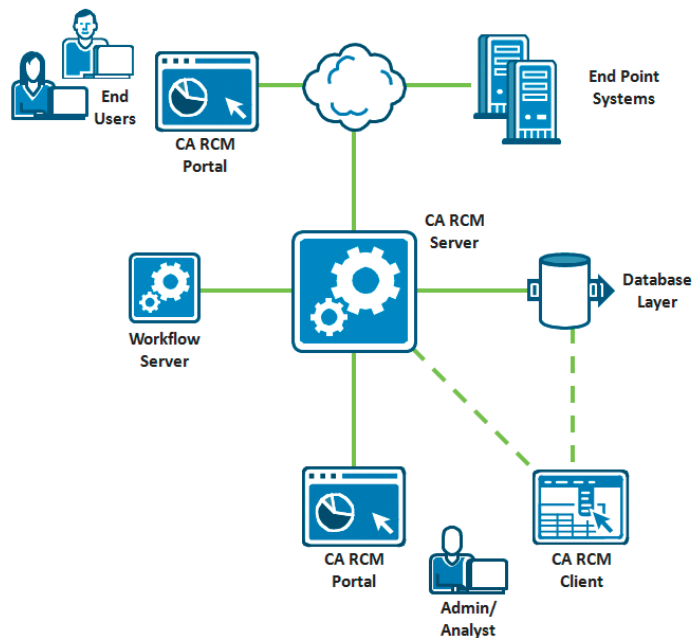
Integration. CA Role & Compliance Manager has the ability to communicate with business applications across the organization, including Human Resources Management Systems (HRMS), Enterprise Resource Planning (ERP) applications, operating system user stores, data collaboration systems and others.

There are several types of supported integrations:

- **Native connectors.** Enables import and export of entitlements and role information from enterprise software systems, such as Microsoft Active Directory, CA Top Secret, IBM RACF, SAP and others.
- **Generic connector.** Provides the ability to import and export data via LDAP Data Interchange Format (LDIF) and comma separated value (CSV) files.
- **Identity Management connectors.** Supports integration with Identity Management or provisioning solutions, such as CA Identity Manager.
- **Web-service APIs.** Provides the ability for external applications to access and update role-based information in real-time in order to achieve a higher level of proactive and continued compliance.

Figure C

CA Role & Compliance Manager is powered by a J2EE server which also exposes portal functionality via Web services.



Analytics engine

A unique and powerful aspect of CA Role & Compliance Manager is its patent-pending, 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 Role & Compliance Manager also exposes its analytic capabilities for use during everyday identity processes. Applying analytics in this manner is based on a fundamental observation that role-based management revolves around patterns of privileges and access. Even in organizations where privileges are not currently managed via roles, the actual assignment of privileges can roughly follow role-based patterns. Deviations and exceptions that become readily apparent can be surfaced in identity processes, helping to make them more effective.

CA Role & Compliance Manager's robust analytic capabilities (in terms of scalability and the strength of algorithms used) 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

Section 3:

Key capabilities

This section reviews the key functional areas of CA Role & Compliance Manager and highlights the ways in which the product can accelerate time to value, reduce costs and improve overall quality of Identity Governance processes.

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 Role & Compliance Manager 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). The results of an audit card can be accessed through the CA RCM Client as well as the Web portal interface. Audit cards are used directly or indirectly 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 Compliance policies

CA Role & Compliance Manager allows organizations to formulate, enforce and validate sets of business process rules (BPRs) to implement segregation of duties and other logical constraints regarding relationships between users, roles and privileges. For example, a BPR can model a constraint of “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 imperative part of defining BPRs, as they are often used by many types of users with varying levels of business and technical understanding throughout various identity processes.

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.** Integrated with CA Identity Manager provisioning actions to help prevent access changes that will introduce new compliance policy violations. Organizations reduce the risk of exploiting temporary violations and the cost of the corrective process which usually requires manual approval.
- **Extendable.** BPRs are also exposed via Web-service APIs and can be integrated with external applications.

Entitlements certification

A common approach to meeting regulations and corporate compliance mandates is to periodically validate that users have appropriate access to corporate resources. During entitlements certification, managers are typically asked to review lists of their direct reports' privileges and either confirm or reject the need for this access. CA Role & Compliance Manager provides scalable and flexible automation, workflow and auditing of this review and validation process.

Tailoring a certification process to an organization's specific needs is critical to effectively validate access and encourage participation in the process. CA Role & Compliance Manager 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 Role & Compliance Manager 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, when discrepancies are found and changes to access rights are required, remediation processes can be triggered by assigning remediation tickets to the correct owners or through integration with CA Identity Manager.

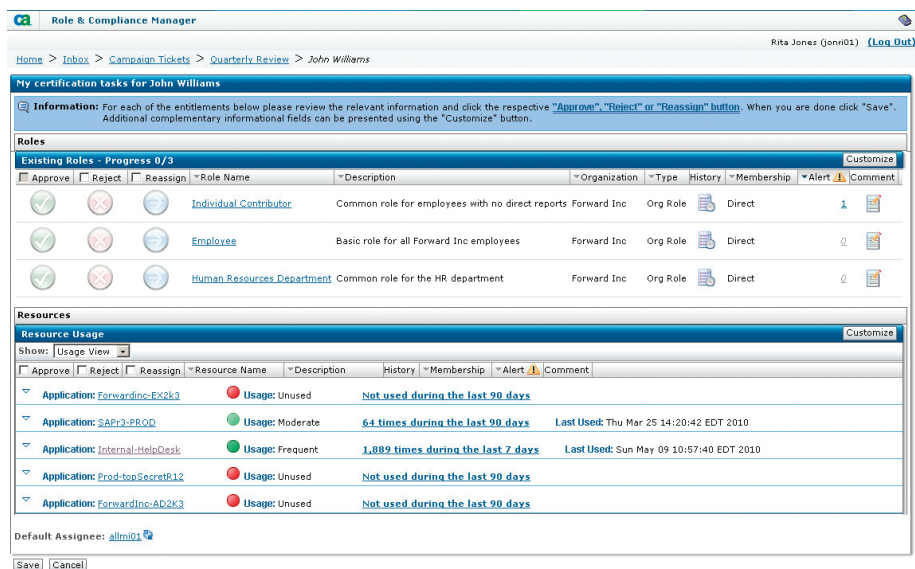
CA Role & Compliance Manager supports many types of certification campaigns including:

- **Entity certification.** Used to certify the access rights associated with selected users, role, or resource entities by managers, role owners and resource custodians, respectively.
- **Recertification.** Allows organizations to repeat the certification process based on a previous campaign. The results of the previous campaign can be visually indicated to the user if desired.
- **Differential.** Initiates a certification campaign based solely on the entitlements which have changed between the current time and a previous campaign.
- **Self-attestation.** Allows each user to certify their own privileges as opposed to a manager or resource owner. This type of campaign may satisfy some legal requirements for data security certification and is also useful during construction of the role hierarchy, and as a starting point for subsequent certification by managers.

CA Role & Compliance Manager promotes active participation by providing reviewers with relevant business context during the certification process. For example, suspect assignments can be highlighted by leveraging user, role and resource data, risk and policy information, or various audit card results. In addition, usage data showing how frequently a user has accessed a resource over a period of time can be displayed on the certification review screens. This type of in-context data can help business managers make better, faster certification decisions.

Figure D

Business managers, resource owners or role custodians use the Web interface to validate existing entitlements and can view relevant business context including how frequently a user has accessed a particular resource.



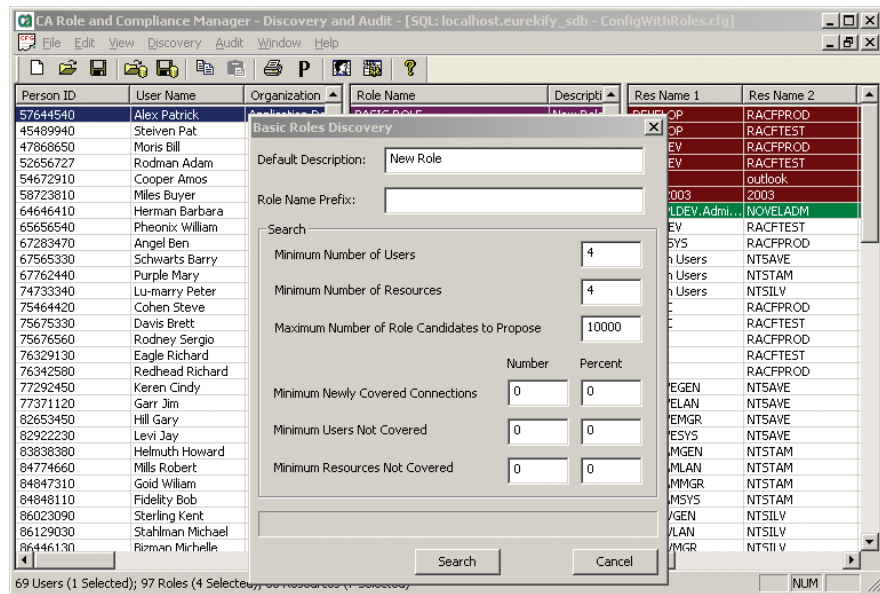
Role discovery

The CA RCM Client 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.** Identifies 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.** Groups 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.** Identifies 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.** Discovers 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.** Constructs roles based on the entitlements of an existing group of users or resources. CA Role & Compliance Manager can use these groups as models for other users or resources.

Figure E

The RCM Client provides a means to quickly discover roles by analyzing existing access rights or user attributes.



CA Role & Compliance Manager 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 Role & Compliance Manager 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 user interface designed for both business and IT users. 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 Role & Compliance Manager 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.

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 Role & Compliance Manager 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 Role & Compliance Manager workflow tasks to make custom behaviors available.

The following illustrates some examples of workflow processes that can be achieved:

- Parallel approval by multiple reviewers.
- X out of Y approvals — 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.
- Allowing a higher level reviewer who can 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 — users can 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 & dashboards

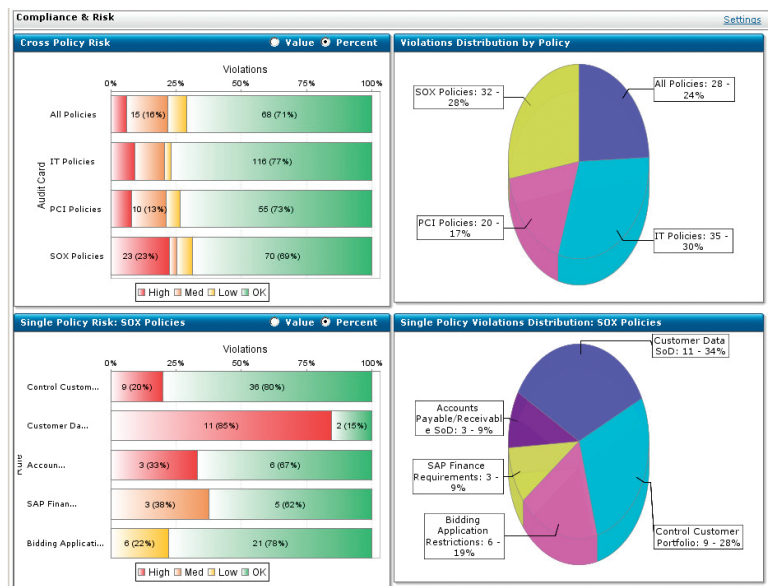
CA Role & Compliance Manager includes an extensive set of out-of-the-box reports and dashboards while supporting ad-hoc queries for forensic requirements. Reports vary in the level of business and technical information provided in order to address the needs of the different user types. This includes 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.** Provide 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.

Figure F

The Audit Card Dashboard provides a single page overview of multiple sets of policy violations.



Section 4:

Conclusion

Over the past few years, Identity Compliance and Role Management have emerged as promising disciplines for providing transparency into the quality of enterprise-wide access management practices, promoting compliance efficiency as well as enabling successful Identity Management implementations. Effective implementations can lower operational costs while improving compliance, which is critical for today's IT security environment.

CA Role & Compliance Manager delivers on both goals 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 help ensure that the access maintained by is at the level they actually need. This can reduce the organization's security risk profile and enable it to more easily demonstrate compliance to internal and external auditors. CA Role & Compliance Manager has been architected to deliver superior scalability with easy customization that helps ensure processes and controls achieve high adoption and effectiveness in the organization.

CA Technologies is an IT management software and solutions company with expertise across all IT environments—from mainframe and distributed, to virtual and cloud. CA Technologies manages and secures IT environments and enables customers to deliver more flexible IT services. CA Technologies innovative products and services provide the insight and control essential for IT organizations to power business agility. The majority of the Global Fortune 500 rely on CA Technologies to manage their evolving IT ecosystems. For additional information, visit CA Technologies at ca.com.

Copyright ©2010 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. This document is for your informational purposes only. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document "as is" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or non-infringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill, or lost data, even if CA is expressly advised in advance of the possibility of such damages.

CA does not provide legal advice. No software product referenced herein serves as a substitute for your compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, standard, policy, administrative order, executive order, and so on (collectively, "Laws")) referenced herein or any contract obligations with any third parties. You should consult with competent legal counsel regarding any such Laws or contract obligations.

CS0311_1210