

WHITE PAPER

Identity Governance: The Business Imperatives | August 2010

# identity governance: the business imperatives

Michael Liou

CA Technologies Security Management

we can



## table of contents

---

executive summary

---

### **Identity Governance Challenges**

Ongoing Cost of Compliance	4
Ineffective Role Foundations	4
Changing Business Environments	5

---

### **Can You Afford Not to Act?**

Identity Compliance	5
Role Management	7
Organizational Restructuring	8

---

### **The Need for an Identity Governance Solution**

**8**

---

### **Combining Disciplines for Greater Value**

**10**

---

### **Conclusions**

**11**

---

### **About the Author**

**11**

---

### **About CA Technologies**

**11**

# executive summary

---

## Challenge

The typical IT organization manages a large and diverse set of user identities ranging from employees to partners to customers. In turn, each of these users requires access to certain resources to be productive. The challenge is in managing users and their substantial number of privileges in a manner which provides users with access as quickly as possible while also taking steps to ensure that access is granted in accordance with security policy. Accomplishing this requires an efficient method for categorizing users and their privileges, controls to facilitate granting access according to security policy and processes to validate or correct inappropriate privilege assignments.

---

## Opportunity

While managing users on an individual by individual basis provides a reasonable likelihood that they get appropriate access, the overhead incurred by such an approach makes this cost prohibitive. Many organizations have recognized the opportunity to manage users and their privilege assignments efficiently by utilizing roles. This intermediate layer translates users to privileges, resulting in a smaller subset of entities for the IT organization to manage. Meanwhile, these assignments can be managed more securely by using a proactive and preventative approach. This includes enforcing policies that prevent users from receiving harmful combinations of privileges and processes to validate that users have appropriate privilege assignments.

---

## Benefits

Identity Governance — segmented at a high level as Role Management and Identity Compliance — involves various identity-related processes including cleaning up existing user entitlements, building accurate role models and enacting policies and processes which help ensure delivery of appropriate privileges to users. Identity Governance solutions deliver a variety of benefits including:

- Increased security by automating processes needed to meet compliance audits and establishing cross-system identity security policies
- Reduced costs associated with identity administration by utilizing roles and streamlining the steps involved in projects such as role discovery, privilege clean-up and certification
- Improved Identity Management time to value and adherence to policy by more quickly delivering a consistent, accurate role and security foundation

## Identity Governance Challenges

At the root of many compliance requirements and risk mitigation activities is a desire to understand who has access to what and whether such access is appropriate. Unfortunately, accomplishing this objective requires a multi-faceted approach and unlike periodic compliance audits, these challenges affect organizations on a daily basis.

### **Ongoing Cost of Compliance**

Organizations must deal with an evolving compliance landscape and business globalization, both of which affect identity security and privacy controls. While the specific impact varies by regulation and organization, these generally require organizations to secure their critical applications, data and systems, and manage the process by which individuals gain this access. The implication for compliance audits is a requirement to both establish security controls and regularly validate the appropriateness of user access rights across all relevant environments — physical, virtual and cloud-based.

In response, some applications include the ability to implement controls such as segregation of duties. However, these application-specific policies cannot generally be leveraged across systems and maintaining these policy silos becomes a costly effort. Another approach is to institute entitlements certification processes to periodically have user, role or resource owners validate that each has appropriate access rights. Unfortunately, these processes are often largely manual; for example, requiring security administrators to circulate spreadsheets listing employees and their associated entitlements to their respective managers and painstakingly following up with each to ensure that the necessary review is completed. So even when regulatory compliance requirements are being met, it is often accomplished at an unreasonable cost.

### **Ineffective Role Foundations**

Roles are not a new concept. For years, organizations have deployed solutions which provision access rights or authorize users to take action based on their role attributes. This means the degree of effectiveness with which these solutions function is highly dependent on the accuracy of the underlying role model. Virtually all organizations have existing roles, yet when they step back and examine them, it is common to find issues such as having far too many roles defined, poor assignment of privileges to roles or over-accumulation of roles by users.

Many organizations implemented projects such as automated user provisioning using their existing role structure. Yet even after deploying such a provisioning solution, connecting it to target systems and building workflow approval processes, they are still not receiving the expected efficiency. This is because basing provisioning decisions on inaccurate role information tends to result in incorrect actions. Improving the accuracy of the role foundation will help deliver significantly better provisioning results. The challenge with any role project is taking enormous volumes of user, role and privilege information and reconciling it to build a new role model or adapt an existing one — without incurring substantial time and labor costs.

### **Changing Business Environments**

Evolving market conditions continually drive organizations to undergo massive business changes. Mergers and acquisitions, corporate downsizing or system consolidation events each present significant security implications for the IT organization. Restructuring can leave users in transition without access to the resources they need or, in a worst case scenario, users that are no longer with the organization retain access to sensitive resources or critical resources are left unmanaged.

The large scale personnel changes that accompany reorganizations frequently leave companies scrambling to understand who has access to what and, as importantly, reconciling this with who should have access to what. These events also trigger a combination of Identity Governance tasks — each of which must be performed promptly. Existing role structures must be quickly updated in light of personnel changes while compliance processes, such as access certification, often become necessary to maintain appropriate security in these times of change.

---

## Can You Afford Not to Act?

In a time when IT organizations are being asked to cut operational costs, some may worry they lack budget to take action on a new initiative. The difference with Identity Governance is that meeting compliance audits or managing roles and identities is not optional. More likely than not, your organization already has processes in place to accommodate compliance requirements or roles on which your existing identity management or enterprise IT systems make decisions.

The key is examining how these processes are being handled today — it is common to find that compliance is being achieved through some combination of manual or ad hoc processes. Or that a weak role model is preventing you from achieving the desired gains in your Identity Management systems. Or your IT team is shouldering the significant cost of maintaining a poor, overloaded role model.

The following scenarios illustrate ongoing projects in a typical organization and the implications of the current approach. If you see similarities in your organization, the more appropriate question to ask may be, “Can we really afford to maintain the status quo?”

### **Identity Compliance**

Compliance audits often require the validation on a regular basis that users have appropriate access rights. This can be accomplished through entitlements certification projects which ask managers to review lists of their direct reports’ privileges to confirm that each user has access only to the resources necessary to perform their job function. In doing so, the organization helps prevent users from accumulating unnecessary privileges and decreases their risk profile.

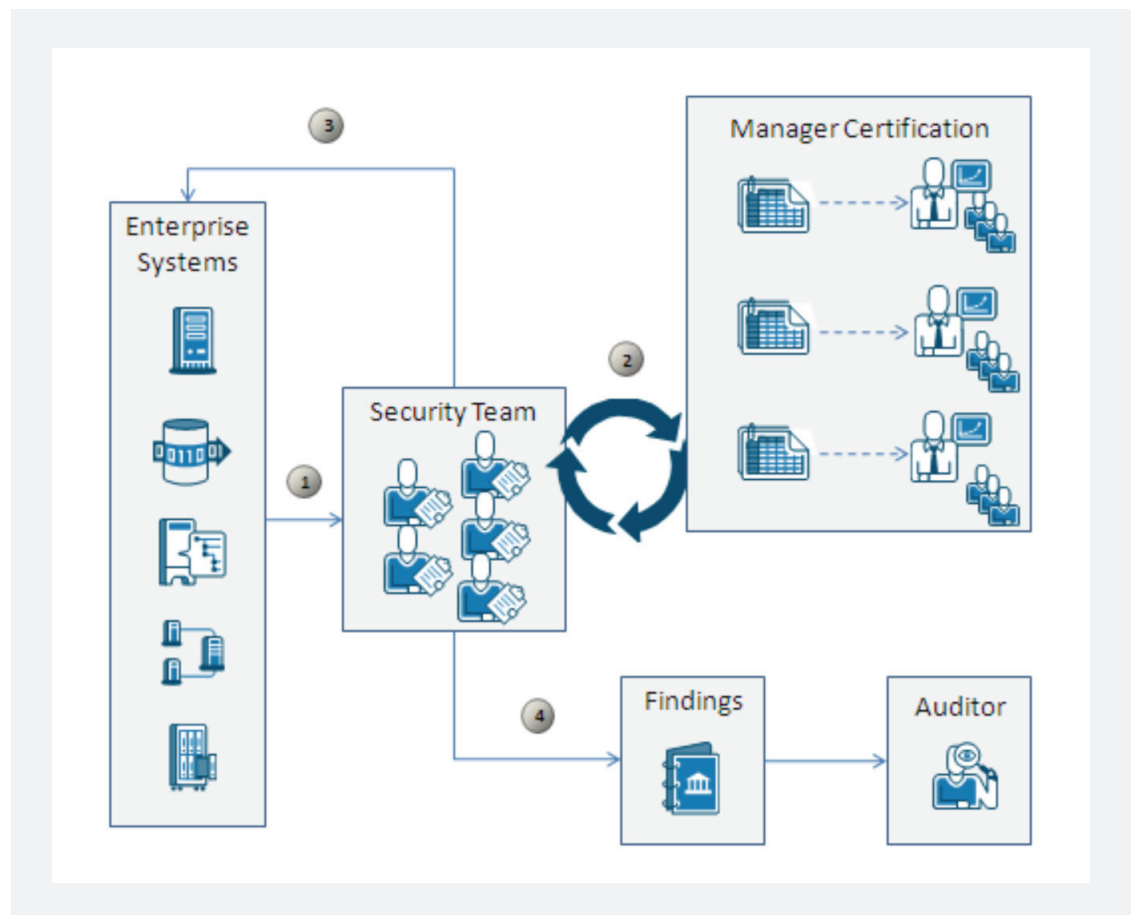
This often starts with dedicated entitlements certification teams querying key systems and developing spreadsheets for each manager which detail their users’ account entitlements. Advanced organizations will first check user entitlements against established compliance policies, such as segregation of duties, to highlight potentially non-compliant assignments. However, this step is often neglected as comparing privileges of thousands of users against hundreds of policies can be extremely time consuming.

The team proceeds by distributing these lists to each manager and then, at a later point in time, tracking down each manager’s confirmation that what was on the spreadsheet was accurate or what needed correction. As improper access rights are identified, the team has to work with IT or the application owners to ensure those privileges are removed. Finally, the results of these certifications must be rolled up into a central set of reports that can be presented to the auditor.

Figure 1  
**Traditional entitlements certification**

Managing entitlements certification through manual or ad-hoc processes can be time consuming and costly

1. Collecting existing identity and privilege data from key systems
2. Creating spreadsheets for each manager detailing their users’ entitlements and following up with manager for feedback
3. Working with the IT team or application owners to remediate inappropriate entitlements
4. Centralizing findings for presentation to auditors



The net result is a process, often based on manual or loosely coordinated actions, which has the potential to be extremely lengthy and labor intensive. This becomes not only a tremendous cost, but also an opportunity lost because organizations are using highly paid staff to do mundane tasks instead of focusing on strategic initiatives. In some circumstances, companies need to perform entitlements certification on a quarterly basis. Without the ability to automate these processes, often by the time they complete one certification cycle, they must reinitiate the process all over again.

### **Role Management**

Most organizations already have roles in place whether they are based on users' HR attributes, specific application authorizations or informally accumulated roles from various sources. A good barometer for the quality of your role model is to ask the question, "How many roles are we managing today?" If the answer exceeds the number of users in your organization or is "We don't know," then your organization stands to benefit from Role Management.

Role Management is a multi-step discipline which may vary depending on the organization, but a typical project will include the following:

1. The first step is gathering existing identity, role or privilege data from authoritative systems. An initial obstacle after consolidating this information is correlating accounts to unique user identities. Depending on the system of origin, accounts for "John Smith" may be represented by "JoSmith01," "John.Smith," "JSmith" or other variations. Some organizations spend months or dedicate teams of resources to interpreting these accounts and assigning them to an authoritative user ID.
2. Even after correlation, existing data will likely have outdated or incorrect information which needs to be cleaned up. This involves, again, poring through the enormous volume of collected data to identify out-of-pattern entitlements or exceptional users and resolving these anomalies as necessary. Unfortunately, due to the labor-intensive nature of this step, most organizations skip this and proceed to role discovery, which can be a costly mistake that negatively impacts the quality of their resulting role model.
3. Once a clean data set is established, organizations take the opposite approach to seek patterns in how privileges are assigned. As they identify commonalities in sets of users, their attributes and associated privileges, these can be suggested as roles. As a large set of potential roles is defined, they then need to re-examine the structure to minimize overlap in order to make future administration and maintenance easier. This step in particular, is one that tends to consume a lot of time and resources.
4. Once the role model has been established, it can be leveraged in other systems or processes. This involves mapping centralized role data into the desired format of each target and integrating it with that system.
5. Finally, but importantly, the role model needs to be maintained. The challenge is in reusing a consistent methodology the next time roles are examined. Organizations will often find changes in their role model, but need to confirm that changes are due to what is actually changing in the organization rather than a change in their role discovery approach.

While each step described above is distinct, they all have a set of common threads. Each step involves a reasonably manageable set of tasks when considering a small subset of data. For organizations with 100 employees and a handful of core systems, it can be fairly easy to develop a set of 20 roles that cover the majority of access requirements. This task becomes increasingly more difficult as you increase the number of users to thousands, tens of thousands or more.

Far too often, a tremendous amount of time and resources are devoted to Role Management initiatives that ultimately yield a model which fails to adequately represent the organization. Lacking the capacity to process the volume of complex data involved results in a role set that only covers a small percentage of user privileges or contains roles that are far too generic. Other times, after months of effort, customers decide to revert to an existing role structure as they run out of time or money required to properly complete the project.

### Organizational Restructuring

The impact of organizational restructuring is characterized by massive changes to IT systems in a short period of time. Even small reorganizations pose significant challenges regarding the need to adapt privileges in accordance with the changing business while maintaining alignment with organizational security and compliance standards. This effort can be significantly more taxing for projects involving a merger of two or more large organizations, which often necessitate migration and mergers of complex IT environments.

For IT teams, the result is often a fire drill situation where they must understand the impact that organizational changes will have on users and IT systems — and do so as rapidly as possible. The first step is identifying systems which are of critical business importance or contain potentially sensitive information. After that, a number of tasks can be in order, including:

- **System and Privilege Consolidation:** Accounts within each system must be aggregated and correlated to a user ID that can be compared to the HR record of users that have been affected. Similar to Role Management, the challenge is in correlating privileges with identities across multiple systems, particularly in the absence of consistent naming conventions.
- **Cleaning-Up Improper Access Rights:** Outdated, redundant or erroneous access rights must be identified to prevent potential security violations. For example, orphaned accounts can present a serious risk if former employees maintain accounts allowing them to access sensitive systems after they leave the company.
- **Role Modification:** In the aftermath of a restructuring event, when mass changes to user identities and access rights are occurring, it is critical to adjust the role model accordingly. Doing so will likely position the team to reduce the administrative overhead of managing an optimized role and privilege structure in the future.

Organizational restructuring projects are similar to role or compliance activities in that they rely on a clear understanding of what users exist and what they should have access to. The difference generally is the urgency which accompanies large scale changes made in a short window of time. Given the fixed timeframes during which IT organizations must respond to a restructuring event, the common approach is to allocate additional resources to complete these projects. Aside from being costly, this can be ultimately ineffective as those temporary resources can lack a true identity, role and system understanding.

---

## The Need for an Identity Governance Solution

The previous scenarios provide a sample of Identity Governance initiatives that are being undertaken by many organizations. Unfortunately, the value of these projects is often questioned — not because the objectives are unimportant, but because they were traditionally addressed at such great expense that it calls the resulting value into question. The good news is that solutions exist which can help significantly reduce the time and effort involved in dealing with these processes while also improving the accuracy and security coverage.

At a fundamental level, the ability to deliver this efficiency is often based on analytics and automation. For example, a recurring Role Management principle is the need to sort through tremendous volumes of data and identify patterns. Patterns between users' attributes and privilege assignments can indicate the need for a role while a lack of patterns may indicate the presence of potentially harmful exceptions. A strong pattern-recognition engine is critical for driving rapid time to value and accurate role results. Meanwhile, automating processes, including validation of existing privilege assignments or identifying identity policy violations, can reduce administrative overhead while improving security.

Some specific capabilities that you should look for in a potential Identity Governance solution include:

**Privilege Clean-Up** This involves examination of existing system entitlements, then adjustment of excessive or unnecessary privileges. This reliable information is required to perform analysis to build a role model that appropriately represents the needs of users supported by your organization.

- **Data Aggregation** Prior to privilege clean-up or role discovery, data must be collected from various sources into a consolidated environment.
- **Unique User Identification** Automatically correlates privileges with their owners (identities) across multiple systems, even in the absence of consistent naming conventions using fuzzy logic and account attributes.
- **Exception Identification** Identifies out-of-pattern privilege assignments such as individuals with significantly higher numbers of privileges than their peers or roles without associated users.

**Role Modeling** Allows you to efficiently sort through extremely large volumes of user and privilege information to more quickly discover potential roles.

- **Flexible Role Discovery** Effective solutions support top-down approaches which seek to discover roles based on organizational characteristics, bottom-up approaches which identify patterns amongst existing privilege assignments and hybrid approaches to suggest potential roles.
- **Built-In Methodologies** Many solutions include a number of proven role discovery methodologies which can be customized and combined to deliver the role model that accurately reflects the structure of your organization.
- **Ongoing Role Management** As individuals evolve from one role to another, the role model itself needs to adapt due to changes in the business while helping to ensure role changes are properly designed, managed and executed after following the appropriate approval processes.

**Entitlements Certification** Automates the processes through which managers, role custodians or resource owners can view the current entitlements of their respective entities, certify that they are appropriate or identify privileges that should be removed.

- **Delegation** In the event that a certification is inappropriately assigned to a manager or owner, delegation automatically routes the request to the queue of the designated person.
- **Risk Indicators** Highlights each user's highest risk entitlements by comparing them against the organization's security policies to help managers focus their attention on the highest areas of risk.
- **Alerting and Reminders** Allows administrators to set email alerts to remind managers to take action on their designated certifications if they have not been completed in a timely manner.

**Identity Compliance Policies** A centralized policy engine enables organizations to establish and enforce a consistent set of identity security policies to minimize their security risk.

- **Flexible Policy Definition** Rule types include constraints between combinations of roles and privileges, segregation of duties and count limits on use of roles and resources.
- **Risk Scoring** Risk scores assigned to each policy serve as valuable indicators that quickly highlight the most critical violations for administrators or managers who have to view a large list of entitlements.
- **Detective and Preventative Controls** Detective controls test actual user, role and entitlement data against Identity Compliance policies to generate a list of violations, high-risk scenarios and other exceptions. Preventative controls stop inappropriate access rights from being created in the first place by proactively checking policies on a provisioning transaction basis.

---

## Combining Disciplines for Greater Value

Although various Identity Governance activities are often addressed separately, the earlier scenarios illustrate that there are not clear boundaries between projects. Accurate roles are critical to providing the proper business context that makes processes such as entitlements certification reasonable. Similarly, Role Management is improved by incorporating certification cycles or compliance policy checks during the role modeling process.

Isolating Role Management from Identity Compliance activities as distinct disciplines often leads to less than ideal results, in the same way that provisioning projects built on a weak role foundation do not maximize value. An optimal approach involves “mixing and matching” project elements to take advantage of the additive effect of combining them. As such, any solutions employed during Identity Governance projects should provide the flexibility to mix, match and combine technical capabilities which complement and leverage one another.

Examining Identity Governance projects within the broader context of your overall security deployment will likely also expose opportunities for delivering greater incremental value for the same level of investment. Identity Management or Log Management solutions, in particular, are a natural complement as they often support the same user base and objectives as Identity Governance initiatives. A few examples of where this can be achieved include:

- **Using Roles for Identity Management** A more efficient role model reduces the administrative overhead of user provisioning while resulting in more accurate privilege assignments.
- **Displaying User Activity during Certification** Showing resource usage from a log management solution in the context of entitlements certification helps business managers determine if a user actually requires access to a certain resource.
- **Automated Entitlements Remediation** After inappropriate privilege assignments are identified during entitlements certification, Identity Management solutions can confirm these access rights are automatically de-provisioned.

- **Checking Compliance Policies during Provisioning** Checking segregation of duties policies, proactively, at the time of provisioning events helps to ensure correct privilege assignment and minimize security risk.
- 

## Conclusions

There is a good chance that Identity Governance processes are already in place in your organization. Compliance regulations and security requirements are not going away — if anything, they are increasing in scope as new regulations are introduced and highly publicized security breaches draw attention to the topic. Roles are a fundamental element which most identity management and enterprise IT systems already depend on to determine what users should be able to do. For these areas, the question is not how they can be avoided, but given the reality that you are already dealing with them, how can you use them to your advantage to deliver the maximum value for your organization?

The good news is that technologies exist which can both help reduce the required investment and increase the value of these projects. Organizations that have deployed these solutions have generally benefited from their ability to deliver fast time to value, improve business operation and improve security. As a fundamental element of most IT infrastructures, Identity Governance also provides the foundation to achieve greater effectiveness in your Identity Management and broader enterprise IT management initiatives.

---

## About the Author

Michael Liou is a Principal Product Marketing Manager at CA Technologies, where he is responsible for defining the go-to-market strategy for CA Role & Compliance Manager. He has spent over 10 years in the software industry, with experience in solution consulting and most recently, leading product management at an enterprise mobile application software company. Michael has a Bachelor of Science in Operations Research and Industrial Engineering from Cornell University and is a Certified Information Systems Security Professional (CISSP).

---

## About CA Technologies

CA Technologies is an IT management software and solutions company with expertise across all IT environments — from mainframe and physical 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](http://ca.com).

