SOLUTION BRIEF: IDENTITY AND ACCESS MANAGEMENT (IAM)

How can Identity and Access Management help me to improve compliance *and* drive business performance?

Transforming IT Management

CA Identity and Access Management automates the management of user identities and ensures that only properly authorized users can access critical IT resources from the Web to the mainframe. It empowers your organization to reduce IT costs, mitigate overall security risk, enable new business opportunities and deliver continuous regulatory compliance.

Overview

Challenge

Managing the identities and access rights of those inside and outside the enterprise has become a primary concern for IT organizations today. The interest in Identity and Access Management (IAM) is driven by the combination of increasing regulatory compliance requirements and the ongoing need for IT to reduce costs and manage risk, while improving business performance at the same time.

Solution

As the IAM market leader[1], CA provides the most comprehensive, modular, integrated and scalable IAM solution available. The CA IAM Suite provides broad coverage across applications and platforms including legacy, distributed and web environments, covering the three major elements of IAM: identity administration and provisioning, access management, and monitoring and auditing.

Benefits

Continuous and sustainable regulatory compliance — through automation, controls and proof of controls — is a primary benefit of the CA IAM Suite. But equally important are business benefits such as reducing cost and improving efficiencies by automating and centralizing identity management; reducing risk by improving security; and enabling greater business performance by improving competitive responsiveness, customer online experiences and partner ecosystems.

CA Advantage

The CA IAM Suite offers a unique combination of advantages including: comprehensive reach across applications, platforms and services; modular design based on common services and user interfaces; centralized and automated provisioning, workflow and entitlement; and global scalability. In addition to IAM, CA's approach is to "Unify and Simplify" overall enterprise IT environments by integrating the management of all IT functions. This vision, called Enterprise IT Management (EITM), is the key to developing a truly business-centric IT organization.

Next Steps

For more information on how CA's comprehensive and integrated IAM solution can help you improve regulatory compliance and business performance while reducing costs and risk, visit us at ca.com.

1 According to IDC's Worldwide Hardware Authentication and Identity and Access Management 2005 Vendor Shares, September 2006, CA is the clear leader in the IAM market with a 17.2 percent market share.

CHALLENGE

Compliance Is the Requirement; Business Improvement Is the Opportunity

Managing the identities and access rights of those inside and outside the enterprise has become a primary concern for IT organizations today. The interest in IAM is driven by the combination of increasing regulatory compliance requirements and the ongoing need for IT to reduce costs and manage risk while improving business performance at the same time.

The Rise of Regulatory Compliance

Governmental and industry regulations covering IT security typically have very specific requirements related to identifying IT users, knowing what applications and resources they are entitled to access, recording when they access them, and knowing what they do while they have access. Creating a set of automated and strong internal security controls around user identities and access, as well as data privacy, can greatly ease the burden of meeting these requirements.

We call this ability to deliver automated and integrated compliance "continuous compliance" because it allows compliance to be done efficiently on an ongoing and sustained basis. This notion requires that the enterprise:

- Automate manual processes and thereby do a better job of sustaining compliance and controlling costs
- Put proper controls in place for managing user access across all business platforms
- Provide proof of controls through monitoring and auditing capabilities
- Improve business performance by securing and better enabling web business applications

Reducing Costs and Risk While Enabling Business Growth

In addition to meeting regulatory compliance requirements, the IT organization continues to be challenged to "do more with less" across the board. These additional challenges include reducing overall IT management costs, managing risk, and helping to enable business growth and new opportunities throughout the enterprise.

MANAGING COST AND RISK As businesses expand and evolve they go through waves of transformation. New applications are adopted and made available to employees, business partners and customers, which creates a growing number of digital identities and escalating administrative costs. Because of emerging security mandates around privacy and data confidentiality, IT administrators are burdened with additional access and auditing projects. Increasing demands on existing limited resources require greater efficiency. Disparate existing systems and processes for user administration, provisioning and access rights management extend the problem, causing increased help desk costs, reduced security and increased IT-related risk.

GROWTH OF THE BUSINESS ECOSYSTEM Clearly, managing users and their access is no longer a simple task. In addition to employees, an organization's customers, suppliers and partners are now integral stakeholders who require access to applications and data as well. Business partners require a trusted relationship to execute business transactions. And your organization is

often required to provide public-facing websites and business processes via exposed Web services. The complexity of identity management is compounded because it must have the capability to manage identities and security in different types of legacy and distributed systems and applications, including HR, ERP and supply chain management systems.

Connecting IAM to Overall IT Management

Finally, effective IAM and security management cannot exist in isolation. It should be viewed as part of an overall IT management requirement that covers many disciplines. To optimize the performance, reliability and efficiency of enterprise-wide IT environments, you need to tightly integrate the control and management of distinct functions such as operations, storage, and life cycle and service management, along with IT security.

SOLUTION

Address Multiple Issues with an Integrated IAM Suite

To effectively address this broad range of issues, an IAM solution should be comprehensive and well integrated across its own components as well as with the rest of your IT management infrastructure.

A Comprehensive Solution

A full solution should address your organization's complete IAM requirements without disrupting current business processes. Broad coverage of applications and platforms, comprehensive capabilities including automated workflow processes and entitlement management, and the ability to connect legacy systems with distributed environments and web-based services all have become critical to meeting the needs of your enterprise.

A Modular Suite with Common Components

The ideal IAM solution should offer flexibility to protect current investments and enable your enterprise to address all aspects of IAM in the customer, partner and enterprise domains. It should also provide integration with business-critical applications as well as among its own components, avoiding the cost to perform time-consuming integration tasks. In addition, the suite should offer a common set of core services, a common web-based administrative interface to simplify management, and a simplified user experience to reduce the potential learning curve. A common auditing and reporting function is also mandatory.

Centralized and Automated User Provisioning, Workflow and Entitlement Management

Today's enterprise requires real-time access. When employees join the organization, it's critical that they are immediately able to access the resources required to perform their job functions. As a result, identity and access management become time-sensitive and critical for user productivity. Other essential capabilities such as self-service profile management — including password resets, "one-click" user provisioning, automated workflow processes, automated allocation/de-allocation of access rights based on roles and/or policies, and customizable security reporting and alerts — should all enable your organization to increase security, improve the user experience and reduce security administration costs.

Global Scalability

An IAM Suite must be highly scalable to meet the complex and growing needs of today's enterprises. It must support any number of identities and policies, and protect any number of systems, applications, files or Web services — locally or across a global environment.

The CA IAM Suite: The Most Comprehensive and Integrated Solution Available

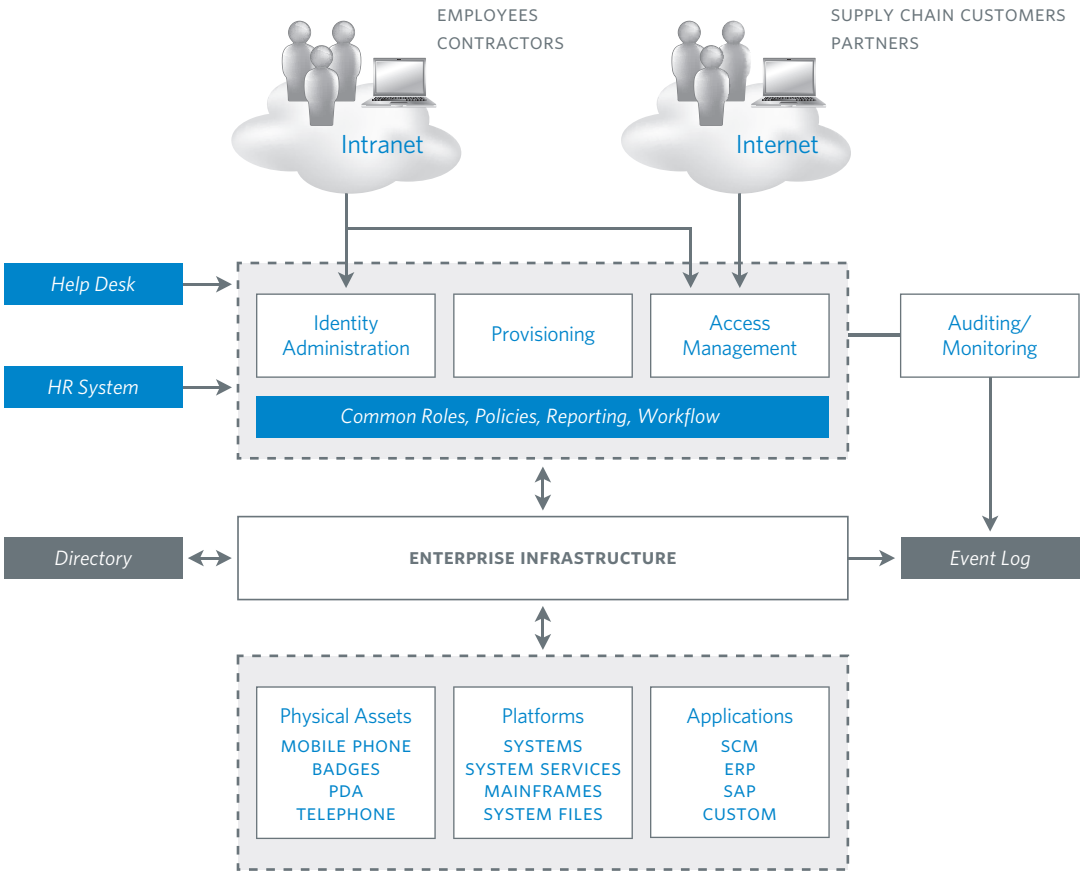
The CA IAM Suite provides the comprehensive, modular, integrated and scalable capabilities that you need, across the three major functional areas of IAM.

Figure A illustrates the functional areas of this solution (modules or component modules that can be purchased and deployed separately) and their integration into your IT infrastructure.

FIGURE A

The key capabilities of an IAM solution — Identity Administration, Provisioning, Access Management and Auditing/Monitoring — are shown in the context of your IT infrastructure.

A COMPREHENSIVE IAM PLATFORM



Identity Administration and Provisioning:

Complete identity administration and provisioning allow the centralized management of all user identities and automate the creation, modification, suspension or deletion of user accounts and entitlements on all IT systems.

CA Identity Manager	Provides an integrated identity management platform that automates the creation, modification and suspension of user identities and their access to enterprise resources that increase security levels and compliance, while reducing administration costs and enhancing the user experience. In addition, CA Identity Manager provides auditing services that can be used by both internal and external auditors to help determine if the entitlement granting practices of the organization are in control and effectively keeping private data private.

Access Management:

CA access management solutions provide comprehensive access control over all critical enterprise resources, including systems, system files and databases, and enterprise and web applications. They also provide access control capabilities for mainframe systems, including the automated removal of orphan user accounts.

CA Access Control	Enforces strong access policy across distributed platforms and operating systems. This solution provides policy-based control of who can access specific systems, applications and files; what they can do within them; and when they are allowed access. They also provide capabilities for granular management of "superuser" privileges for greater administrative security.
CA SiteMinder® Web Access Manager	Secures web resources by delivering policy-based access controls and single sign-on. It simplifies access to critical business processes exposed via internal- and external-facing websites, and enables identity federation.
CA SiteMinder® Federation Security Services	Enables browser-based identity federation (cross-security domain single sign-on) as an add-on set of services to CA SiteMinder. The FSS add-on enables a CA SiteMinder–protected site to be both an identity provider (authentication service) and a service provider (application provider) for federations. Identity federation provides an enhanced user experience, competitive differentiation, reduced costs and improved security.
CA SOA Security Manager	An identity-centric Web services security software product that secures access to critical Web services by inspecting the security information contained in the XML requests. Leveraging a core set of standards, CA SOA Security Manager uses centralized security policies to provide XML threat prevention, authentication, authorization, federation, session management, and security auditing services.
CA Single Sign-On	Provides full-featured single sign-on across the extended enterprise. It logs users into mainframe, middleware or web applications from a single authentication, providing a seamless user experience for both legacy and web applications in business settings and special environments such as kiosks or clinics.
CA Directory	A "backbone" directory that meets the most stringent demands of large-scale online business applications. It delivers the highest levels of availability, reliability, scalability and performance by combining LDAP V3 for access, X.500 for high-speed distribution and replication, and a relational database for reliability.

CA ACF2™ Security and CA Top Secret®	Provide leading-edge security for the z/OS, z/VM and VSE business transaction environments — including z/OS UNIX and Linux for zSeries. Built-in, comprehensive administrative and reporting tools, along with detailed event logging capabilities, simplify the management of users and their access rights. These solutions give you the tools to monitor the efficiency of your security policies and provide end-to-end security for the enterprise when deployed with other CA solutions.
CA Cleanup for ACF2™ CA Cleanup for Top Secret®	Provide automated, continuous and unattended security file cleanup by monitoring security system activity to identify security definitions that are currently unused. Specifically, these solutions identify accounts unused beyond a specified threshold and generate commands to remove unused user IDs, permissions, and profile and group connections that each user has but does not use. These solutions effectively resolve the accumulation of obsolete and excessive access rights that otherwise occur within a security file over time — a key requirement for compliance with many regulations.
CA Embedded Entitlements Manager	Enables organizations to meet the highest compliance and security standards in their custom applications while delivering significant development cost savings. Combining an easy-to-use, flexible SDK with a centralized management server, CA Embedded Entitlements Manager allows developers to embed fine-grained authorization, security auditing and identity components directly into their applications, and to simplify administration through externalized policy management.
	Monitoring and Auditing: The CA monitoring and auditing capability tracks virtually all identity and access change and usage activity across the entire enterprise, consolidating logs/events, compiling reports, and triggering alerts on services-based infrastructure with an open interface for easy integration.
CA Security Command Center	Collects enterprise-wide security and system audit data and provides comprehensive visualization and reporting of this information. It accomplishes this by converting advanced correlation of disparate audit data into intelligent, actionable and traceable information that can be managed from a single, centralized location.

BENEFITS

Reducing Costs While Improving Control and Business Performance

The CA IAM Suite provides a complete and proven solution for protecting your IT assets across all platforms and environments within your enterprise, delivering these important benefits:

IMPROVING REGULATORY COMPLIANCE The CA IAM Suite provides your organization with the necessary tools to support continuous compliance — automated and centrally managed compliance capabilities that help to reduce costs, while providing strong controls and proof of controls that can strengthen security and improve IT auditing.

REDUCING ADMINISTRATIVE COSTS AND IMPROVING EFFICIENCY The CA IAM Suite can help you reduce your security administration and help desk costs, as well as improve the overall productivity of your user population. By centralizing the management of all user identities and their access rights, management of your policies becomes easier, less error-prone and significantly less costly.

REDUCING SECURITY RISKS With centralized identity management and comprehensive access rights enforcement, the CA IAM Suite ensures that only properly authorized users gain appropriate access to your critical resources. Users are entitled by their role in your organization, and receive only the appropriate levels of access to protected resources and/or other non-IT resources to perform their job functions. It also reduces the possibility of expired identities remaining active in your system. When an employee leaves your organization, access can be immediately revoked or completely removed from all points of access. In addition, pre-existing unused ("orphan") mainframe system accounts and access rights can be automatically detected and removed.

IMPROVING BUSINESS ENABLEMENT Automating, centralizing and improving control over IAM functions helps organizations to better secure their online applications, and deliver more well-tailored and positive online user experiences to their growing ecosystem of employees, customers, suppliers and business partners.

CA ADVANTAGE

The CA IAM Suite offers a unique combination of advantages including: comprehensive reach across applications, platforms and services; modular design based on common services and user interfaces; centralized and automated provisioning, workflow and entitlement; and global scalability.

To optimize the performance, reliability and efficiency of your overall IT environment, you need to tightly integrate the control and management of distinct functions such as operations, storage, and life cycle and service management, along with IT security.

CA's vision for enabling this higher level of management control is Enterprise IT Management (EITM). EITM is a dynamic, secure approach that integrates and automates the management of information technology applications, databases, networks, security, storage and systems across departments and disciplines to maximize the full potential of each. CA's comprehensive portfolio of modular IT management solutions helps the enterprise unify, simplify and secure IT to better manage risk, costs and service, and ensure that IT meets the business needs of the enterprise.

ADD VALUE WITH CA TECHNOLOGY SERVICES An important part of CA's leadership in the IAM market involves the dedicated CA Technology Services™ IAM practice team. Our IAM specialists understand your unique requirements, appreciate your risk profile, and can help you meet your business drivers and regulatory requirements. Working in partnership with you, CA can help you build a security infrastructure and implement a foundation of well-defined IT processes and controls. In designing your IAM solution, CA Technology Services relies on blueprints based on the CA IAM Maturity Model (see Figure B), which incorporates our extensive security expertise and industry standards. Each blueprint plots the way to a progressively higher level of IAM maturity, delivering ROI-documented improvements to people, processes and technology.

REALIZE VALUE WITH CA EDUCATION As part of our service offerings, CA Education — a preferred source for IT management and best practices training — can help our customers realize the greatest value from their IAM investments. We do this by offering a combination of training need assessments; creating the right training plan with the required course offerings; and optimizing the training through advanced learning programs and industry certifications.

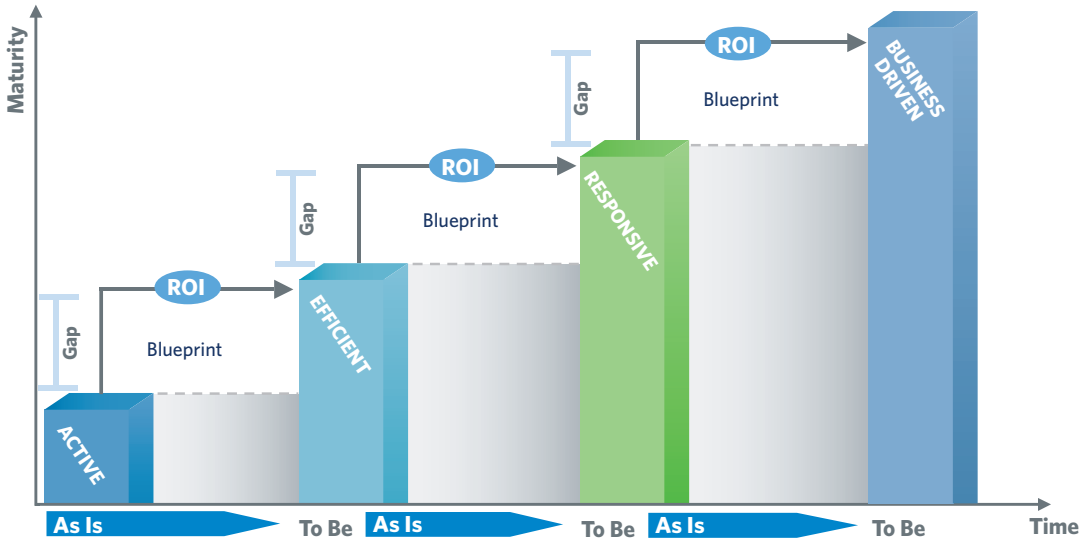
The cornerstone of CA Education is the Unified Learning Approach, which features five important steps:

1. Determine business goals and IT requirements
2. Determine an organization competency level required to achieve these goals considering people, process and technology requirements
3. Assess individual staff competency levels using CA software and IT best practices in Education Needs Assessment
4. Evaluate and measure staff post-training knowledge and skills
5. Map acquired expertise to IT maturity level to reassess training impact vs. business goals

FIGURE B

Using the IAM Maturity Model, CA can help you identify your current level of IAM process capability. This approach is the starting point in the creation of a solution blueprint that will help you achieve a higher state of IAM effectiveness, to quickly and reliably deliver predictable ROI and business results.

LEVELS OF IAM MANAGEMENT READINESS



NEXT STEPS

If you're finding that:

- Budgetary and regulatory pressures require higher efficiencies in administrative and security functions...
- You need more automated and secure IAM solutions...
- You want an IAM solution that's tightly integrated with your overall IT management approach...

Then take a look at the CA IAM Suite. It's the most comprehensive and integrated IAM solution addressing security for web applications, legacy systems, distributed computing environments and emerging Web services.

For more information on how CA can help you reduce security costs, protect corporate assets, and ensure regulatory compliance through a more integrated and comprehensive IAM solution, visit us at ca.com/iam.

CA, one of the world's largest information technology (IT) management software companies, unifies and simplifies the management of enterprise-wide IT for greater business results. Our vision, tools and expertise help customers manage risk, improve service, manage costs and align their IT investments with their business needs.

Quality Endorsed Company
ISO 9001 Lic. 2443

SB05GMIAM0E MP308901107

Learn more about how CA can help you transform your business at **ca.com**

Transforming IT Management