CA Technologies + Deloitte: Growing and Protecting the Business with Identity and Access Management

ca technologies | Deloitte.

Table of Contents

The Opposing Forces of Growing and Protecting the Business

A number of technology trends, including cloud, mobility, social media and the consumerization of IT, have transformed not only IT, but also the way employees, partners and customers interact with an organization. And as software as a service (SaaS) and cloud applications have grown in popularity, IT environments have become more distributed, fragmented and nebulous—with many components existing outside of the traditional security perimeter of firewalls and virtual private networks (VPNs).

As a result, protecting today's cloud-based, mobile enterprise requires a new approach—one that focuses on secure identity and access management (IAM), while at the same time driving two critical imperatives:

Enable business growth by:

- Quickly deploying new online services
- Leveraging new advances in cloud computing and virtualization
- Accommodating the needs of demanding, tech-savvy users (i.e., customers, partners, employees, etc.)
- Driving greater employee productivity and increasing business intelligence

Protect the business by:

- Mitigating the risk of fraud, breaches, insider threats and improper access—from both internal and external sources
- Safeguarding critical systems, applications and data

"S&R (security & risk) pros can only formulate explicit IAM policies to deal with threats that they have identified, understand, and know how to mitigate—but new and emerging threats hit quickly, before you can fully understand them. Risk-based IAM allows security teams to identify anomalous and potentially insecure behaviors and defend against these threats."

Forrester's Risk-Driven Identity And Access Management Process Framework Process: *The Identity And Access Management Playbook* by Andras Cser, August 11, 2015

Identity as the New Security Perimeter

Given the increasing complexity of security threats and the pace at which new ones emerge, it's a challenge to balance the competing priorities of protecting the business while granting appropriate access and controlling cost and effort. At the heart of this challenge is the fact that the traditional network perimeter has disappeared in recent years.

It used to be that enterprise applications were contained within a network firewall. Access was limited to internal employees, and it was easy to manage identities and understand the context of a user's actions. However, as online interactions expanded to include customers, mobile users and business partners—as well as on-premise and cloud—the traditional network perimeter has become less and less effective.

Identity is what enables you to connect everyone to the resources they need, from any device...all while ensuring strong security over all access. In this new landscape, identity must become the new security perimeter.

According to Ponemon Institute, the average cost of a data breach for an organization in 2015 was $3.79 million U.S. dollars — a 23% increase in total cost of data breach since 2013.

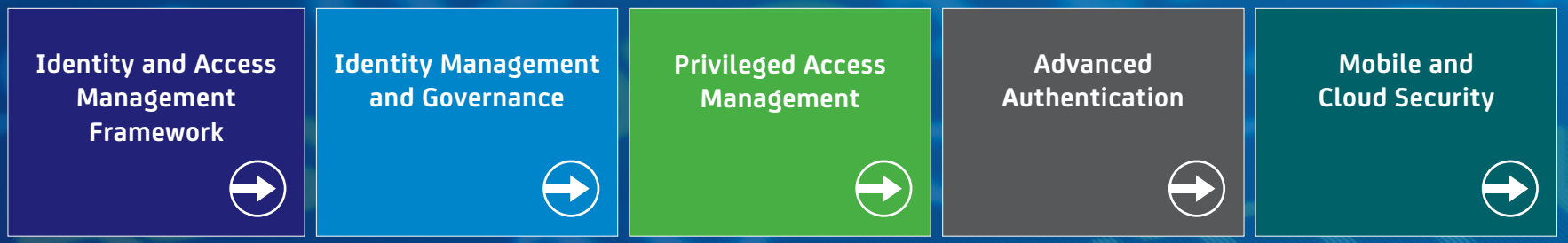
[1] Ponemon Institute, *2014 Cost of Data Breach Study: Global Analysis*, sponsored by IBM, May, 2014.

The Need for a More Holistic, Centralized IAM Approach

Traditionally, organizations have approached security from a technology-stack perspective, infusing IAM directly into the servers (physical and virtual), databases, applications, operating systems and networks that comprise their IT infrastructures. However, with the traditional perimeter disappearing and identity becoming the driving force behind new security paradigms, IT must take a more holistic, centralized approach to identity and access security—an approach where IT brokers security between itself and all of the application instances where business-critical data resides.

In order to effectively drive value and mitigate risk, such an approach requires not just IAM technology, but also alignment among business processes, people and that technology—which means organizations should follow a top-down approach to security transformation.

Together, Deloitte and CA Technologies take a broad, business-focused approach to helping clients address the identity and access security lifecycle. It starts with a demonstrated framework as the foundation, and builds out to help organizations address specific security vulnerabilities they may have. Specific solutions include:



Identity and Access Management Framework

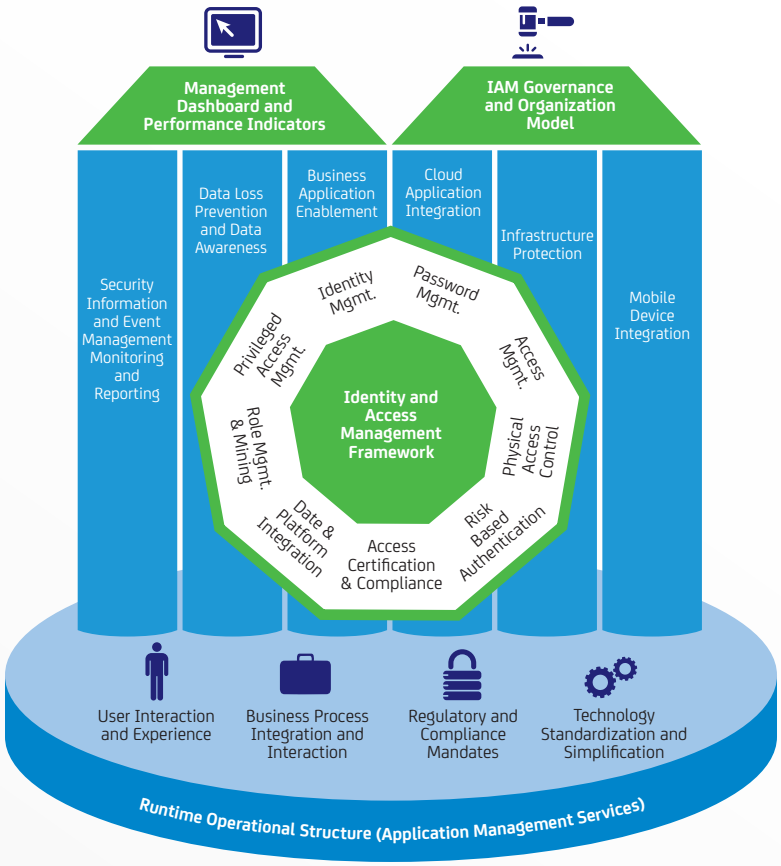
Managing and protecting sensitive customer, business and personally identifiable information (PII) is becoming increasingly complex and risky:

- External threats from cyber criminals and hacktivists can exploit identity-based data
- Internal threats occur when poorly followed security practices create holes for potential incursions
- Security breaches have increased in scope and frequency in recent years as more businesses store their data in digital files
- IT productivity suffers as an expanded digital footprint makes it difficult to manage increasing numbers of user identities and credentials

The joint Deloitte and CA Technologies Identity and Access Management Framework was designed to help organizations overcome these challenges from a business-process perspective. It begins with understanding where digital identities live—in enterprise, cloud or siloed services—what they can access, and to which job functions and processes they correspond.

The result? IAM solutions that interface with business processes to make access to specific functions more intuitive, helping boost user productivity, while maintaining a tight governance structure.

As pictured, the IAM Framework is composed of nine primary components that can be deployed individually or in combination to meet an organization's needs. In addition, the framework incorporates governance considerations, key IAM inputs, technical integration and ongoing support.



Identity Management and Governance

With today's highly distributed and evolving business structures, organizations are at greater risk of users having IT privileges that are not appropriate for their current job function. Users with excessive or inappropriate privileges can potentially wreak havoc on a business, including violating compliance mandates or causing leakage of confidential data.

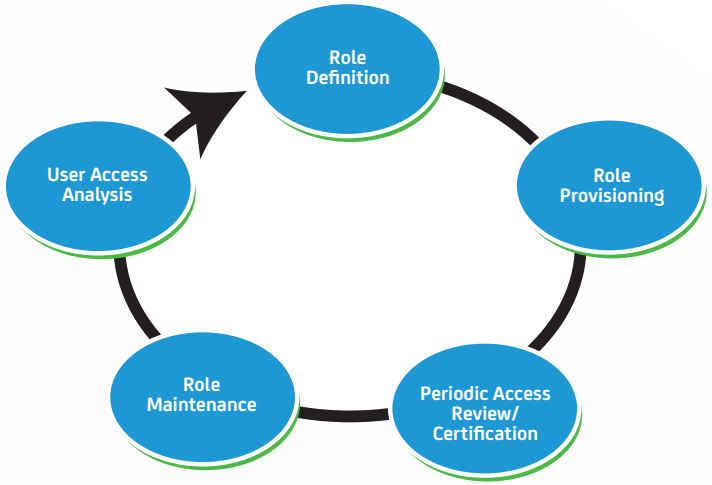
The joint Deloitte and CA Technologies Identity Management and Governance solution helps organizations avoid these risks by automating management of users' identities and what they can access in an integrated and scalable solution across physical, virtual and cloud-based environments.

Components of the Identity Management and Governance Solution

Deloitte drives the engagement with the IAM Framework and its complementary IAM Methods™ 2.0 methodology, an iterative-based approach that leverages industry standards to create a strategy and solution roadmap that clearly outlines IAM initiatives, timelines and associated costs. As part of this framework, Deloitte's Role Management for Enterprise (RM4E) methodology helps streamline access control issues using Role-Based Access Control (RBAC). This includes, but is not limited to:

- Defining enterprise role life cycle management
- Role engineering
- Deployment of technology to support role management

The diagram shows the high-level processes in role lifecycle management.



CA Identity Suite

A comprehensive and scalable solution for management and governance of user identities with an intuitive, business-oriented user experience. The Suite provides provisioning, workflow, self-service, role management and entitlement cleanup, access requests and certifications, along with realtime analytics and segregation of duties enforcement. It also is very easy to deploy and manage on an ongoing basis. The solution is validated to scale to 100M users, and has been successfully deployed in large environments across all industries.

Privileged Access Management

When privileged users are given all-powerful access (e.g., unrestricted “root” or “administrator” access) and are subject to limited accountability, their identities can pose a significant threat to network and data security.

The joint Deloitte and CA Technologies Privileged Access Management (PAM) solution helps organizations control the activities of privileged users across the entire hybrid enterprise, thus reducing the risks of a breach, compliance failure or Intellectual Property (IP) loss.

Components of the PAM Solution

Deloitte drives the engagement with the IAM Framework and its complementary IAM Methods 2.0 methodology. In addition, Deloitte’s RM4E provides a demonstrated process around role engineering which results in better investment from the business. The diagram on the following page shows the key activities to build roles for organizational groups.

CA Technologies powers the engagement with **CA Privileged Access Manager**, a simple to deploy, scalable solution that defends and controls the most critical and sensitive resources in your organization—privileged users and the credentials they use to access, manage, and control your digital infrastructure. This solution delivers the comprehensive functionality needed to prevent breaches, demonstrate compliance, and boost operational efficiency.

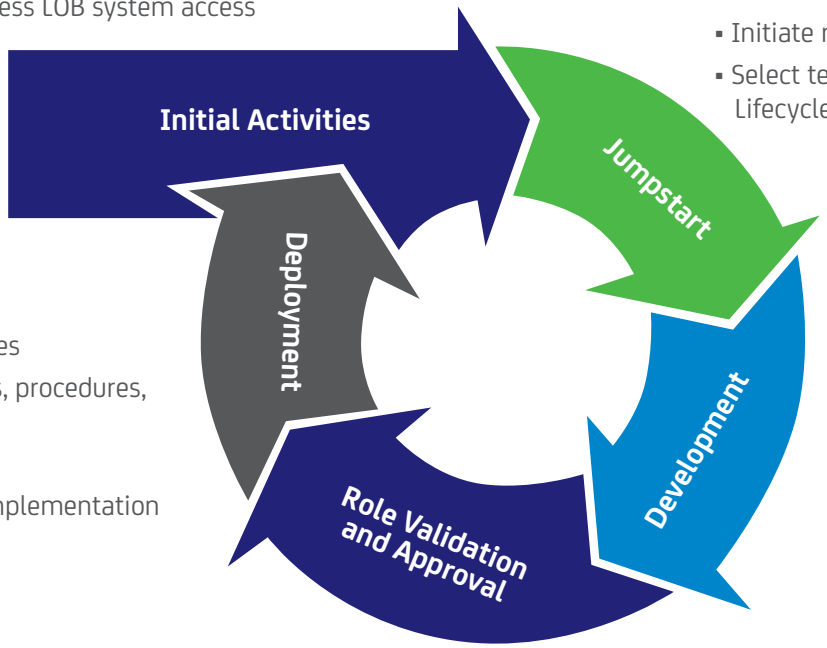
Privileged Access Management Continued

1. Initial Activities

- Set stage for RM4E implementation
- Gather and review line of business (LOB) information
- Gather, review and assess LOB system access information

2. Jumpstart

- Begin RM4E implementation
- Understand LOB functions and system access
- Initiate role design
- Select technology (Role Enginerring, Role Lifecycle Management)



3. Development

- Conduct detailed role development
- Design RM4E process
- Design technology solution
- Provide training

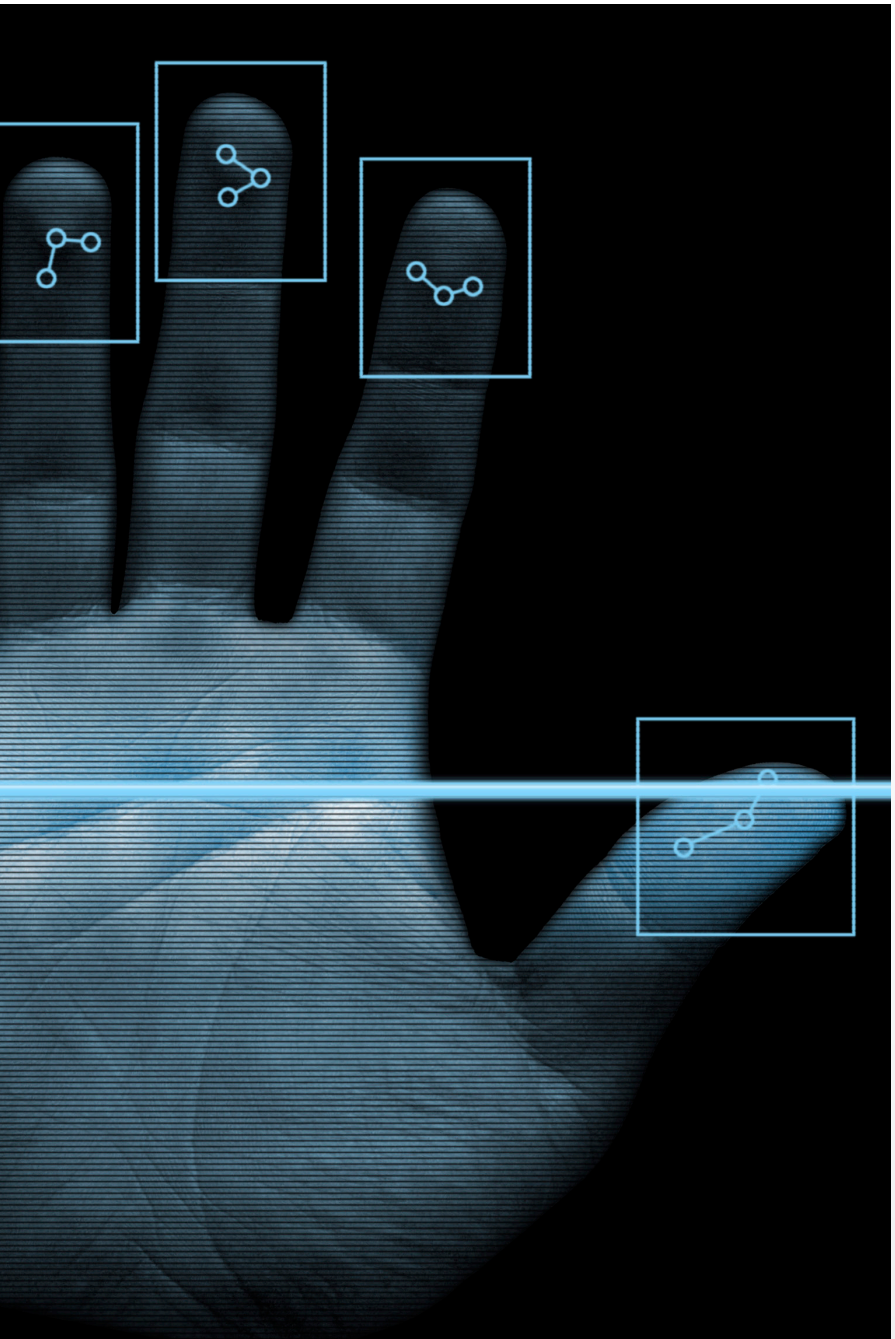
4. Role Validation & Approval

- Test roles, process and technology
- Identify exceptions
- Finalize roles with appropriate individuals and groups
- Obtain approval on roles

5. Deployment

- Deploy enterprise roles
- Deploy RM4E process, procedures, and guidelines
- Deploy technology
- Finalize LOB RM4E implementation

Advanced Authentication



As identity has become the new security perimeter, IT should respond by placing a stronger emphasis than ever before on authentication (i.e., the process of ensuring that users truly are who they say they are). How? By developing a secure, centralized method for providing layered, risk-appropriate authentication that simplifies the user experience while helping to ensure strong security.

The joint Deloitte and CA Technologies Advanced Authentication solution addresses these business imperatives via an authentication model that helps clients address these business imperatives, such as a user's identity, geolocation, device and past history.

Components of the Advanced Authentication Solution

Deloitte drives the engagement with the IAM Framework and its complementary IAM Methods 2.0 methodology.

CA Technologies powers the engagement with the following authentication solutions:

CA Risk Authentication combines risk-based analysis and user behavioral profiling to more accurately identify and authenticate legitimate users without interrupting their activity. The solution utilizes contextual factors such as Device ID, geo-location, IP address and user behavior profiling to calculate a risk score and recommend the appropriate action, such as step-up authentication, for login attempts and sensitive transactions.

CA Strong Authentication enables secure interaction for your end users by delivering two-factor authentication credentials for online and mobile applications. It allows you to deploy and enforce a wide range of software-based authentication mechanisms in an efficient and centralized manner.

Single Sign-On

As security becomes the next frontier for organizations looking to capitalize on digital transformation initiatives, businesses need to provide employees, customers, partners and suppliers secure, frictionless access to essential information and applications whether on-premises, in the cloud, from a mobile device or at a partner's site. As an organization's Web applications increase, it becomes essential to provide a seamless user experience by allowing users to sign on once to access all of their applications while protecting the organization from breaches and other threats. With CA Single Sign-On, you get flexible and secure identity access management.

CA Single Sign-On:

- Accelerate access management—Increase application availability by providing unparalleled access management options.
- Enhance Security—Reduce risk of access gaps with a common policy layer
- Reduce cost of ownership—support web applications, identity federation standards, and web service standards with a single platform

Mobile and Cloud Security

The growth in mobile apps, cloud services, developer communities and the IoT (Internet of Things) has driven the enterprise to open up valuable data through APIs. By exposing data and application functionality to external users, apps and machines, an organization can reshape its business model into an extensible platform that can take advantage of new routes to market and revenue streams. However, leveraging APIs can mean having to contend with new and unpredictable identity and access security risks.

The joint Deloitte and CA Technologies Mobile and Cloud Security solution combines advanced functionality for backend integration, mobile optimization, cloud orchestration and developer management, enabling organizations to leverage APIs for creating a consistent experience across web and mobile apps from both a service and security perspective.

Components of the Mobile and Cloud Security Solution

Deloitte drives the engagement with the IAM Framework and its complementary IAM Methods 2.0 methodology. In addition, Deloitte's Risk Intelligent Enterprise™ framework (see diagram on the following page) weaves important risk management principles throughout the organization, to manage risk associated with the Cloud Security solution implementation.

CA Technologies powers the engagement with the following solutions:

CA API Management and Security provides enterprises with a comprehensive set of solutions that externalize APIs in a secure, reliable and manageable way, so they can maximize mobile app development, bring your own device (BYOD), cloud connectivity, partner and cross-divisional SOA integration and API developer onboarding opportunities.

CA Identity and Access Management provides identity management, advanced authentication and federated single sign-on (SSO) capabilities for cloud and on-premise applications, helping organizations simplify security management and meet ongoing compliance requirements.

Mobile and Cloud Security Continued

Pathway to a Risk Intelligent Enterprise™

Cloud risk management strategy

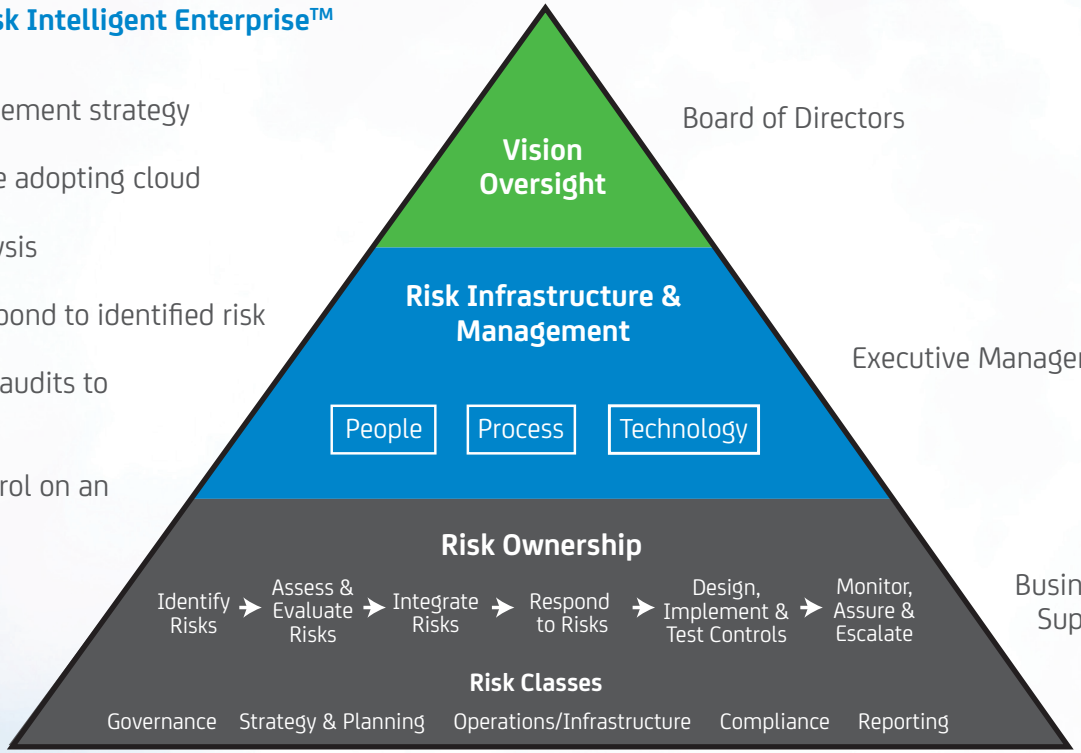
Identify risk while adopting cloud

Risk impact analysis

Prioritize and respond to identified risk

Conduct internal audits to identify gaps

Monitor and control on an ongoing basis



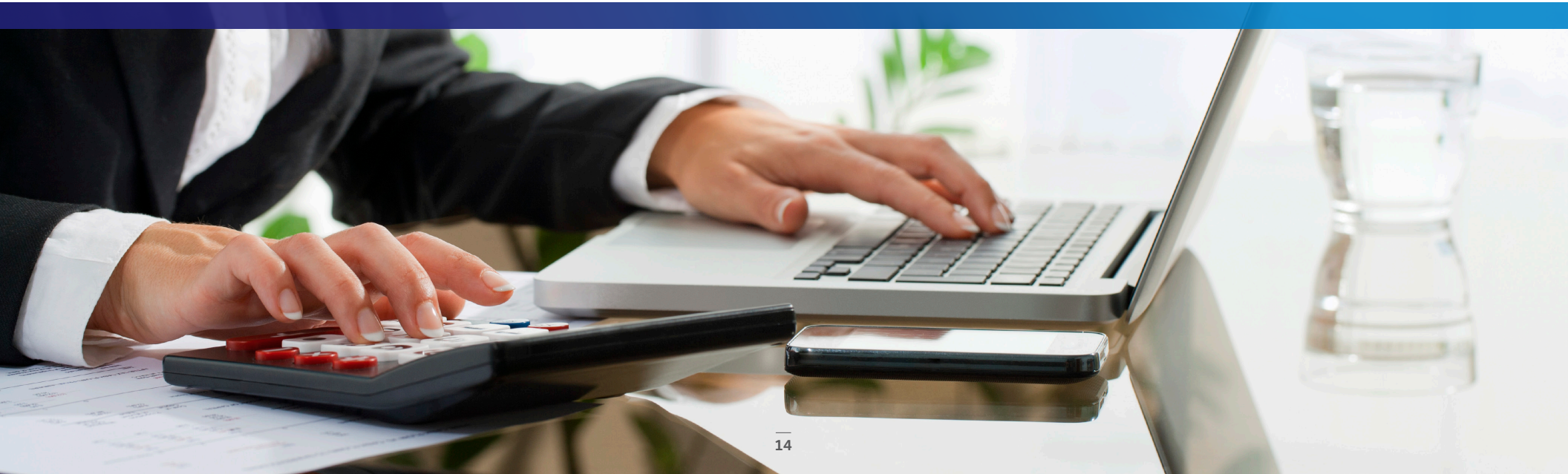
The Business Benefits of IAM

Together, Deloitte and CA Technologies can help organizations enable their business for growth and bring digital identities and access rights under control by deploying an IAM solution that:

- Controls access to applications and data residing on-premise or in the cloud
- Aligns user access rights with business responsibilities, while providing unique capabilities to track and manage the use of privileged user IDs
- Helps accelerate the delivery of secure, new business services, while improving the user experience
- Helps mitigate risk by enabling centralized, consistent security policies across the enterprise—including business units, individual locations, systems and the points of business partner and customer access
- Increases efficiency through business process automation
- Enhances compliance with federal mandates, laws and regulations and Federal Identity, Credential, and Access Management recommendations

As a result, organizations can effectively:

- Grow the business by remaining agile and accelerating the delivery of web and mobile applications
- Protect the business by helping ensure that operations are supported by security measures that protect critical corporate and personal data – without impeding the user experience



Leading Organizations Achieve Positive IAM Results with CA Technologies and Deloitte

Case Study: A Large, Vertically Integrated Marketer of Tires for the U.S. Automotive Replacement Market

Challenge:

The company was rolling out a new point-of-sale solution in 900 stores and needed a solution for efficiently and securely managing user roles, identities and access for more than 10,000 employees.

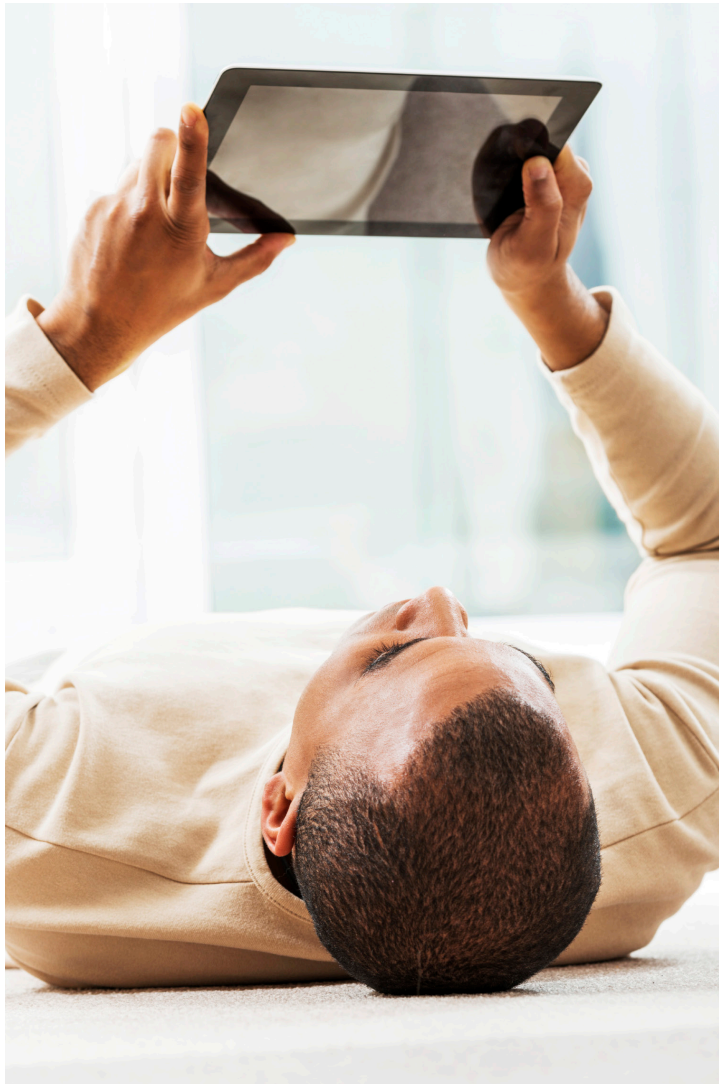
Solution:

The joint Identity Management and Governance solution from CA Technologies and Deloitte, including:

- Deloitte's IAM framework, which combined business processes, security and controls, enterprise resource planning, project management and technology skills with in-depth CA product knowledge to address the following areas:
  - Current-state analysis
  - Development of strategy, business case and roadmap
  - Solution design
  - Identity management program implementation and integration

Results:

- Improved productivity via efficient identity management of 10,000+ users
- Reduced risk profile via automation that helps the company address compliance and audit requirements
- Increased long-term security posture with a roadmap that includes future web access and privileged access management projects



Leading Organizations Achieve Positive IAM Results with CA Technologies and Deloitte Continued

Case Study: An Agency of a Canadian Provincial Government

Challenge:

The agency's in-house collection services application was suffering from performance issues and had become too expensive to maintain, so it was looking to implement a commercial solution with integrated security and service assurance capabilities.

Solution:

The joint Identity Management and Governance solution from CA Technologies and Deloitte.

Results:

- Improved performance and security of citizen services
- Accelerated implementation that sped time to value
- Simplified maintenance and improved support

About the Deloitte/CA Technologies Alliance

Deloitte has been providing enhanced services and solutions leveraging CA Technologies software for more than 10 years. Deloitte's global insights, knowledge and experience, combined with CA Technologies solutions, can assist customers in effectively integrating technology, processes and people to tackle tough enterprise challenges and provide value from IT investments.

Deloitte + CA Technologies at a Glance

- CA Technologies Security Partner of the Year 2013
- 15,000+ trained security professionals
- Specialized methodologies established for CA Technologies Security implementations
- Demonstrated, industry-specific solutions across Financial Services, Energy, Retail, Entertainment and more
- Active participation in CA Technologies product management and development via product beta evaluations, CA security roadmap reviews and sharing of product enhancement ideas and suggestions gathered from numerous client implementations

The Deloitte and CA Technologies alliance brings together the IT strategy and implementation skills of Deloitte's experienced practitioners with the applicable technologies from CA Technologies to help organizations better manage security risks and provide greater value from their IT portfolio.

Please visit **Deloitte's website** to learn more about how Deloitte and CA Technologies can help you realize more value from your IT investments and protect your enterprise assets.

Deloitte Contacts

Jeremy Britton
Managing Director
Cyber Risk Services
jebritton@deloitte.com
1.313.919.3558

Heather Varner
Senior Manager, Sales Executive
Cyber Risk Services
hvarner@deloitte.com
1.513.723.4152

CA Contact

Mike Gierkey
CA Technologies Global Account Director, Alliances
mike.gierkey@ca.com
1.214.802.8675

CA Technologies (NASDAQ: CA) 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 relies on CA Technologies to manage evolving IT ecosystems.

CS200-208919

technologies