Building a Roadmap to Robust Identity and Access Management
Elevating IAM from Responsive to Proactive

From cases involving private retailers to government agencies, instances of organizations failing to properly secure access to data have been in the headlines with alarming frequency. And yet, current Identity and Access Management (IAM) policy in many organizations remains only to address security issues, often through the implementation of point solutions when disaster strikes.

To operate at peak efficiency, the right data must be available to employees, partners and customers from any device at any time. However, necessary precautions must also be taken to prevent unauthorized and unnecessary access. While IT is the gatekeeper, IAM challenges touch every corner of the enterprise. Getting IAM right isn’t just a technology challenge, it’s a business challenge.

The Challenge

Each enterprise must determine how to strike the appropriate balance between necessary access to data and applications and security from external and internal threats.

The Insight

IAM is a business issue. The creation of a proactive, strategically driven and sustainable IAM program is essential to preventing security shortcomings from threatening organizational productivity, profitability and credibility.

The Solution

Following the five-step roadmap outlined in the succeeding pages helps to ensure that an IAM program is based in best practices and strategically aligned with business objectives and corporate policies and processes.

Holistic view of an effective infrastructure

**Management Identity**
- Achieve Operational Excellence

**Enable Access**
- Drive New Revenue

**Identity Governance**

**Self-Service Access Request**

**Shared Account Management**

**Provisioning**

**API Portal**

**API Security & Management**

**Mobile App Security**

**Advanced Authentication**

**Web Single Sign-On Federation**

**Protect Sensitive Data**
- Protect the Brand

**Protect the Brand**

**Mobile Device Management**

**Mobile Content Management**

**Email Control**

**File Control**
Business Challenges

Mobile. Cloud. Big data. Social identities. Today's users demand increasingly convenient access to huge repositories of data and applications across multiple platforms. This, in turn, introduces new security vulnerabilities that must be addressed with ever-more sophisticated IAM programs.

IAM isn't just about allowing or refusing access to data. It's about establishing protocols that strike the proper balance between security and the level of openness required to conduct business in today's wired (and wireless) marketplace.

Enterprises need to map a path that aligns process, policy and technology. And, that begins with determining where current measures fall short. Since this exercise can sometimes be painful, it can often be best facilitated by experienced, objective, third-party entities.

The top five reasons for revamping an IAM program:

1. Ineffective or inefficient operational approach to managing identities
2. Lack of an end-to-end governance process
3. Constant reactive responses to cyber threats, which lead to inefficient use of resources
4. Imbalance of solution focus between compliance and business enablement
5. Widening skills gap across IT that makes building and maintaining an effective IAM capability increasingly difficult
The good news is, once a strategic direction for a sustainable and robust IAM infrastructure is defined, it immediately delivers substantial benefits throughout the enterprise.

<table>
<thead>
<tr>
<th>Increased levels of trust across your business eco-system</th>
</tr>
</thead>
<tbody>
<tr>
<td>A proactive IAM strategy tells employees, partners and customers that the organization is serious about protecting its data and its interests. That trust translates into the confidence and goodwill necessary to support business growth.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Opportunities to deliver greater control over the extended enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recognizing and properly addressing those opportunities help create a secure infrastructure without sacrificing business agility or efficiency.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Address compliance and regulatory requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM policies must not be too lax to meet regulators’ requirements, nor more restrictive than requirements demand. Policies must be developed on a case-by-case basis to meet specific circumstances. One-size-fits-all policies can often “over-comply” and stifle business agility.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reduced costs, enhanced security and decreased complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>By simplifying processes, it’s possible to capture efficiencies and reduce risk. That results in OPEX savings that contribute to ROI.</td>
</tr>
</tbody>
</table>
Five-step Process

Getting IAM right requires a significant commitment of resources. CA Technologies advocates a comprehensive program that:

- Clearly identifies needs
- Creates objectives
- Drives change
- Continually evaluates performance against evolving issues, threats and challenges

Such a thorough and organized approach facilitates the development of metrics for overall success and ROI. Moreover, the ability to demonstrate tangible value will help build support for the program—and maintain momentum once it’s underway.

The five steps are:

1. Establish a program
2. Initiate a strategic assessment
3. Recruit a team
4. Execute projects
5. Repeat the strategic assessment
Too often, corporate IAM policy is designed to put out fires as they arise. But, it’s just a matter of time before a sweeping disaster strikes. How can IAM be turned into an asset instead of an exposure?

**Embrace the Need**

**What?**
The first step is to gain agreement from all relevant decision-makers and stakeholders regarding the need for an integrated program—and not a series of one-off fixes. It’s essential for all functions throughout the organization to understand the risk associated with a failure to enhance IAM, and the benefits to be derived from implementation.

**Who?**
A comprehensive IAM program will require both sponsorship and resource support from senior-level management. Meanwhile, planning, instituting and maintaining the IAM program will require participation and time commitments enterprise-wide.

**Why?**
Securing an early commitment from management will reduce resistance to necessary resource allocations. Helping stakeholders throughout the enterprise recognize the importance of IAM will create urgency and enthusiasm that will drive the participation required to make the program work.
Step 2 – Initiate a Strategic Assessment

Everyone agrees that a new IAM program is needed. But, what should it include?

Do the Deep Dig

What?

To create an IAM program that is truly aligned with enterprise needs, the organization must set goals and then establish a roadmap for fulfillment. Such a process begins with an in-depth analysis. CA Technologies advises contracting an external team in order to take advantage of the opportunity to replace “the way we’ve always done things” thinking with fresh insights and perspectives.

To start, organizations should focus on identifying and prioritizing business drivers, such as:
- Business enablement
- Security enablement
- Efficient operations
- Audit compliance
- Enhanced user experience
- Technology standardization

Next, they should identify the data and processes that are most critical to addressing the enterprise’s high-level requirements and expected functionality. Finally, they should map organizational priorities against existing technology to pinpoint areas in need of improvement. For instance:
- Single sign-on vs. access certification
- Availability of identification data
- Internal vs. external compliance regulations

Once all the data has been collected, an organization should create a multi-year roadmap—a series of small projects, in priority order—that helps attain the final state the business is demanding. Plot the roadmap against a maturity model to determine which projects the organization possesses the capabilities to execute immediately and which will need to wait. It’s also useful to compare the existing situation and roadmap against comparable competitors to see how the roadmap matches up against industry best practices. Points of comparison include:
- Web access management and access management enforcement
- Access requests: granting, provisioning and de-provisioning
- Access reporting and certification
- Identity data availability
To succeed, a strategic assessment requires broad participation throughout the organization. Experience shows that essential participants include HR, Legal and Audit, as well as all of the largest application communities in the enterprise (e.g., sales, partner networks, engineers, etc.).

The fundamental reasons for conducting a detailed strategic assessment are to:

- Identify and prioritize areas in need of improvement
- Develop a program based around organizational needs and priorities
- Align activity to strategic demand
- Establish the path from the present situation to the ideal end state for the business

An effective strategic assessment determines how to align IAM policies with organizational imperatives.
Step 3 – Recruit a Team

The strategic assessment is complete. The findings are in. Now, who’s going to turn strategy into reality?

**Distribute Ownership**

**What?**
As with any business initiative, the success of an enterprise-wide IAM program requires widespread participation and commitment. The enterprise must create a task force to review the findings of the strategic assessment, prioritize projects, assign tasks and oversee implementation.

**Who?**
This task force should not be comprised of new hires brought in specifically to manage the IAM program. Rather, it should include individuals throughout the organization who will be impacted by the program and responsible for its execution.

**Why?**
Ownership of the program translates directly into investment in the outcome. To build and maintain support, it is essential that areas of the business most likely affected by the new processes and procedures have a stake in their development and implementation.
Step 4 – Execute Projects

The roadmap is written. The team is in place. Now what?

Implement the Strategy

What?
Using the roadmap objectives, the IAM team should prioritize elements of the program. Meanwhile, the team should evaluate and select vendors and solutions to address specific needs. Finally, it should establish a communications cadence for reporting back to stakeholders on milestones—both achieved and planned.

Who?
IT and procurement specialists should take the lead in the evaluation, negotiation and purchasing process. A subset of the team should be tasked with communicating updates to those with a vested interest in the program.

Why?
This is where the entire exercise begins to pay dividends in the form of a more strategically coherent and robust IAM program—one that facilitates business activities while mitigating risk. In addition, an effective IAM program decreases resource requirements and their associated expenses, ultimately enhancing ROI. Regular progress reports to stakeholders throughout the enterprise validates the program and helps to sustain support and participation.
Step 5 – Repeat Strategic Assessment

The new IAM program is in place. So, it’s safe to sit back and let it work, right?

Assess, Address, Improve

What?
To remain sustainable, a strategic IAM program must be assessed and modified on a regular basis. A formal state-of-the-program review to reevaluate security performance against present and emerging needs should be conducted at least every one to two years. The program and resources should then be revised as necessary.

Who?
While it may be possible to reduce the size of the team once the IAM program is implemented, it’s important to retain representation from all affected sectors of the enterprise. At this juncture, it is appropriate for IT to take the lead because it is the day-to-day facilitator of the program and its supporting processes.

Why?
Sustainable IAM isn’t a finite effort—a box that can be checked. It requires consistent and continual commitment and vigilance due to a constant state of change. Routine portfolio rationalization helps keep the focus on current priorities and challenges. In addition, regular quantitative status reviews provide the validation necessary to justify the program and calculate ROI.
How CA Technologies Can Help Facilitate IAM Excellence

Experts from the CA Identity and Access Management Assessment Services group are available for strategic assessment engagements to help organizations measure maturity, identify gaps and develop an actionable, proactive IAM program.

CA professionals possess diverse and extensive industry experience that makes them more technically knowledgeable and astute than business-oriented consultants. Most importantly, they have a vested interest in delivering the best program and exceptional value to their clients.

While technology independence is often viewed as an advantage, at the implementation and operation stages, it is far less important than a practical understanding of how the technology actually works. Deep knowledge of CA products give our Identity and Access Management assessment services consultants a solid grounding and the practical experience needed to succeed. And for added peace-of-mind, they can implement and support the products they recommend.

For more information about how Identity and Access Management Assessment Services from CA Technologies can help develop a better performing, more efficient IAM program, visit http://www.ca.com/us/security-and-compliance-services.aspx.

CA is the only vendor named a “Leader” in The Forrester WaveTM: Privileged Identity Management, Q1 2014,* as well as the top scorer in all three of the report’s overall criteria categories.

About the Solutions from CA Technologies

CA Technologies’ Identity and Access Management platform provides a modular solution for multi-channel business enablement and security. The solution is optimized to help organizations improve engagement with their internal customers, accelerate delivery of new services and externalize their core business to capture new markets and revenue. It can be customized to include the appropriate components from among the following:

**CA Single Sign-On**
- Provides single sign-on, federation, authorization and session management

**CA API Security & Management**
- Provides the ability to quickly develop manage and secure APIs to safely expose web services and help leverage cloud and mobile

**CA Advanced Authentication**
- Delivers strong authentication capabilities, including unique two-factor credentials and adaptive authentication

**CA Identity Manager**
- Offers identity management, provisioning, governance and entitlement certification capabilities

**CA Secure Cloud**
- Delivers a set of identity management, single sign-on and strong authentication capabilities as a service

**CA Application Delivery**
- Addresses DevOps challenges by optimizing application development and testing through service virtualization, release automation and data mining

**CA Application Performance Management**
- Ensures quality of service and experience for organizations’ critical business applications
For more information about how IAM solutions from CA Technologies can help you deliver secure, new business services and improve the customer experience, visit ca.com/us/application-security.aspx