Build Your Identity And Access Management Strategy

Strategic Plan: The Identity And Access Management Playbook

by Andras Cser and Merritt Maxim

April 3, 2017

Why Read This Report

Your strategic plan for identity and access management (IAM) must establish and explain the business need and value of IAM to both technology management and business leaders. It must also describe the current state, define the future state, and make defensible recommendations for the sequence of projects needed to make the strategy a reality. In this report, we provide security and risk (S&R) leaders with systematic guidance for the development of a compelling IAM strategic plan.

This report was originally published on January 7, 2015; Forrester reviews and updates it periodically for continued relevance and accuracy.

Key Takeaways

IAM Projects Require A Defined Strategy For Success

IAM projects are complex. They: 1) usually fail without adequate analysis and planning; 2) require executive attention and buy-in; and 3) cannot disrupt existing services. A good IAM strategy balances security requirements with employee and customer experience and communicates these goals effectively to executives.

People Are Central To Any IAM Project

Successful IAM projects involve a manageable number of cross-functional stakeholders throughout the process. These include security pros, business leaders, technology leaders, HR, call center pros, and application developers, whose functions range from operation, process, and audit to budget and support.

Compelling IAM Strategies Must Evolve To The Changing Business Environment

Successful IAM projects go through an iterative process, which includes confirming scope, defining success metrics, reaffirming requirements, assessing current state, and defining the future state and road map.

Build Your Identity And Access Management Strategy

Strategic Plan: The Identity And Access Management Playbook

by Andras Cser and Merritt Maxim
with Stephanie Balaouras, Salvatore Schiano, and Peggy Dostie

April 3, 2017

Table Of Contents

Related Research Documents

Forrester's Customer IAM Security Maturity Assessment Model

Making The Business Case For Identity And Access Management

The Top IAM Trends From The RSA Conference 2017

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

An Effective IAM Strategy Boosts Employee And Customer Experience

Most S&R professionals understand that they need to manage identities in an automated fashion in order to achieve regulatory compliance, reduce costs, dramatically increase security, and improve both employee and customer experience. Customer experience across multiple delivery channels has become particularly important because today's empowered customers are less and less likely to tolerate cumbersome registration, login, and password reset processes. And if customers won't tolerate it, you can be sure that your business leaders won't tolerate it. Consequently, S&R pros must constantly balance security with seamless access.[1]

A Well-Defined IAM Strategy Is The Difference Between IAM Project Success And Failure

Forrester regularly interviews and performs maturity and strategy assessments for companies embarking on new IAM projects or after their IAM projects have failed or when their S&R professionals have had to backpedal on requirements to meet deadlines or budgetary restrictions. Although overscoping and a lack of executive attention are probably the leading factors in missed deadlines or project delay, lack of strategy is a major contributor as well. You need an IAM strategy because it will help you:

- **Maintain or improve customer experience (CX) across channels.** Having an easy-to-use customer-facing website or mobile app that does not frustrate users during enrollment, login, password reset, and other self-service processes is a must. Otherwise, customers will defect to your competition.[2] A solid IAM strategy will force you to consider the CX across not only online channels, such as web, mobile app, email, and kiosk, but phone, branch, and snail-mail channels as well.[3] It will also force you to carefully plan transitioning customers from the old to the IAM experience by avoiding big-bang go-live events and sticking to a gradual implementation plan for specific customer segments.
- **Identify interdependencies and other risks.** S&R pros who begin IAM projects spurred by executive enthusiasm but without a well-defined strategy often fail to consider interdependencies. For instance, user repository consolidation should precede a provisioning project or mapping, and re-engineering identity life-cycle management processes should happen before vendor selection. Without a well-defined strategy, S&R pros easily overlook hidden interdependencies or duplication between IAM activities, which results in changing requirements, budget overruns, missed deadlines, and IAM implementation fatigue.
- **Win and maintain executive support with compelling benefits and good governance.** S&R pros often think of buy-in as a meaningless platitude. In the case of IAM, it's a real requirement. In almost all of our recent assessments, Forrester identified lack of technology management executive buy-in and attention, such as from CIO, CISO, CRO, or vice president of IT operations, as a chronic symptom of failure. IAM projects are not bottom-up, grassroots movements: Much of the change management and championing needs to come top-down from senior management.[4] Without a strategy that outlines a detailed two-year road map, and hard monetary benefits of IAM, execs are

not likely to fully fund your IAM projects or encourage your technology management colleagues to collaborate with you. And buy-in needs to be continuous; we increasingly see companies creating IAM governance committees to reassess and reevaluate progress on a quarterly basis to ensure that execs remain informed and engaged.

› **Avoid disrupting existing employee services.** Older IAM infrastructure components are reaching the end of their useful lives, and technology management must replace them. However, you have to do this while providing the necessary IAM services that keep employees connected to technology systems with the appropriate level of access. Pulling this off is akin to building Boston's "Big Dig" Central Artery/Tunnel Project. Before digging the tunnels, construction crews had to move the existing utilities (gas, electric, etc.) out of the way, and throughout the construction, state and local leaders prohibited any disruption of traffic. The project came in 10 years behind schedule and $12 billion over budget.[5] S&R pros often overlook the cost of reshuffling and preparation for IAM projects. A good strategy forces you to consider those concerns.

Developing A Successful IAM Strategy Requires Multiple Stakeholders

Identities represent applications and other technology objects, but mostly, they represent people — your business users, your partners and contractors, and your customers that need access to your technology services to conduct business or purchase your goods and services. People are an integral part of any IAM project. For IAM projects to be successful, S&R pros must involve a cross-functional team of relevant stakeholders from across the business throughout the process.

IAM Requires Cooperation From Several Technology Management Teams

Security teams take a lead in the development of IAM strategy and the execution of IAM-related projects, but they are not the only technology management team that plays a key role and carry out responsibilities. In particular:

› **IT operations performs essential identity administration.** Security teams usually own IAM, but they rely heavily on IT operations for day-to-day administration and to help deliver IAM projects. Most IT operations teams are also heavily involved in access recertification and identity administration activities — they feel the pain and know the ins and outs of all manual processes that good IAM projects aim to automate.

› **App developers adhere to secure IAM practices in code development.** Historically, app developers had to deal with user administration and authentication in their applications — a responsibility they sometimes have a hard time abdicating. Proving to developers how a centralized IAM platform can actually accelerate and simplify app development is vital to their buy-in for any IAM projects. IAM subject matter experts on the security team should work on internal guidelines, code samples, and checklists that enable and enforce secure IAM practices in mobile, web, and other apps. Also, it's very helpful if security pros can show developers how to externalize access

controls (authentication and authorization) and identity administration from applications. Such efforts can accelerate application development while also mitigating risks by delivering consistent security policy management.

- **Compliance managers drive audit requirements.** Complying with regulations such as FERC/NERC, HIPAA, PCI DSS, and SOX is often a main driver for IAM projects, so the ability to obtain appropriate identity information out of any IAM system is critical. Compliance and audit managers will establish the requirements for what data they require to verify compliance. Among many other needs, auditors will want to see who granted a user a read/write access entitlement to the general ledger, who approved a user having toxic combinations of entitlements, and when a particular user last accessed a system and how.
- **CIOs and CISOs provide budget and support.** No IAM project can be successful without executive sponsorship and adequate funding. In addition, Forrester interviews reveal that forward-thinking senior technology management leaders, such as CISOs and CIOs, often look to IAM as a career promoter. To this end, many IAM project teams implement an internal end user satisfaction survey that allows them to measure the value of IAM. Measuring definitive value from IAM helps sustain an IAM road map and allows CIOs and CISOs to broaden their organization's IAM capabilities. Grassroots movements are nonstarters and usually fail, given the cultural change IAM needs in the organization.

IAM Requires Business Leaders To Define Requirements And Promote IAM

It's not just technology management teams that play a vital role in the success of IAM; it's also teams from across the firm. In particular:

- **Marketing and line-of-business (LOB) owners guard customer experience.** Forrester's interviewees indicate that marketing and LOB stakeholders represent a growing force around the security and IAM table when it comes to customer-facing websites. If S&R pros can implement customer-facing IAM nicely and support their progress with metrics on reducing new user enrollment abandonment rates, help desk calls for locked-out accounts, and number of unsuccessful password resets, they will quickly gain respect from marketing and LOB stakeholders.[6]
- **Business leaders define usability and process requirements.** Good IAM systems provide the appropriate level of access and security without hurting productivity or forcing employees to understand and use technology lingo. Business owners want to quickly onboard new employees and contractors to support business growth. To do this, business owners want S&R pros to provide transparent, business-user-friendly, delegated administration, user provisioning, and access recertification processes. Failing to involve business users causes many IAM projects to lose momentum.
- **HR provides quality identity data from talent management systems.** Since most IAM systems use a talent management database as the largest system of record for employee identity management and provisioning, S&R pros need to collaborate intensively with HR when building the

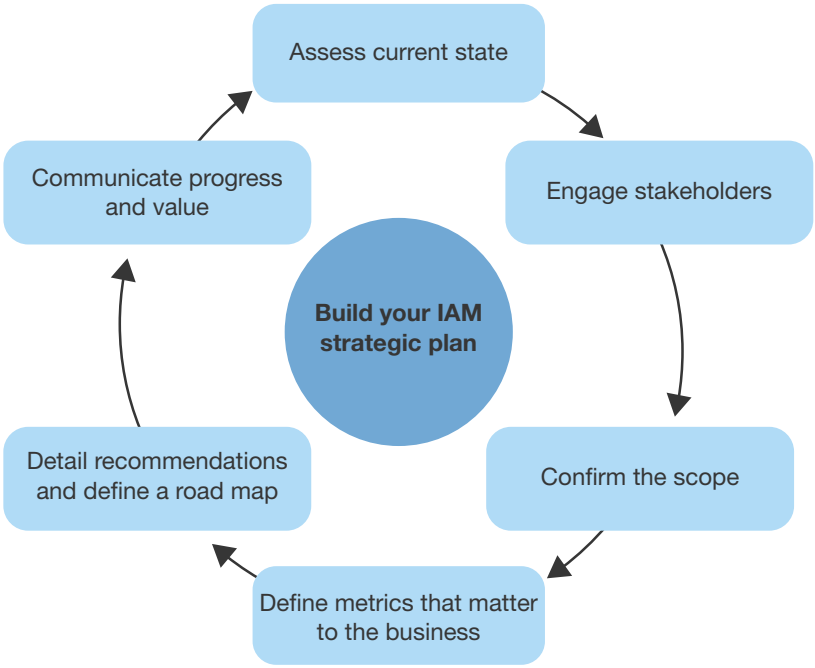
IAM environment. Squeezing data cleansing into HR's responsibilities is no easy task, so in return for HR collaboration, many security teams provide a vantage-point view into the provisioning data. This feedback allows HR to have a much better and deeper understanding of what a person does and improves data quality in talent management databases.

- **Call center professionals provide customer-facing identity support.** Call center professionals often take all the heat when customers can't use online self-services to manage their access or get things done online. If things don't work as expected, customers will call the help desk and ask call center representatives to reset passwords and provision access for them. Call center personnel need to be at least aware of all IAM projects and be enabled with a big green button to reset profiles and password data and fix entitlements in applications that were erroneously changed by a half-baked IAM implementation.
- **Procurement must be on board with your selection of IAM system integrators.** Given the size and complexity of IAM projects, firms rarely undertake them without the help of system integrators (SIs). IAM SIs (e.g., Accenture, EY, KPMG, Infosys, PwC, Tech Mahindra, and Wipro) provide services for: 1) business mapping; 2) design breakdown; 3) business requirement mapping; 4) development and customization; 5) policy design; and 6) ongoing maintenance of IAM solutions. While their expertise has traditionally been with on-premises IAM solutions (e.g., CA Technologies, IBM, NetIQ, Oracle, etc.), they are now starting to develop competencies for customer-facing IAM implementations (using solutions from the above vendors as well as from ForgeRock, Gigya, Janrain, and Ping). During the past 24 to 36 months, they have been embracing implementing and integrating IDaaS services into the enterprise.

A Good IAM Strategy Requires Iterative Processes

Security teams that create IAM strategies that lead to successful projects often go through an iterative process to refine and further build out their strategy. The process includes six steps: 1) assess the current state; 2) engage stakeholders; 3) confirm the scope; 4) define metrics that matter to the business; 5) detail recommendations and define the future state road map; and 6) communicate progress and value (see Figure 1).

FIGURE 1 The Annual IAM Strategy Life Cycle



Step 1: Assess Current State To Make Sure Everyone Agrees On Current Problems

You can't solve IAM problems until you fully understand your current situation and architecture. In assessments, Forrester runs into many security teams that claim they have a full understanding and documentation of business processes, relevant IAM architecture, and coding practices, only to conduct interviews and find out that reality is vastly different. Therefore, we recommend that S&R pros:

- **Conduct a systematic and comprehensive maturity assessment.** For employee-facing IAM, you can use Forrester's Identity And Access Management Cost Model as a basis for the areas you assess (see Figure 2).[7] For customer-facing IAM, you can use Forrester's Customer IAM Maturity Model.[8] It is also helpful to evaluate the company's stature in identity management and governance, and Active Directory.[9]
- **Summarize your IAM observations and current state for key stakeholders.** Documenting the current state and identifying prioritized observations (or findings, depending on your corporate culture) is key to making solid and realistic recommendations. In Forrester's experience, skipping this step leads to failure of IAM projects. We've created an example summary to help you get started (see Figure 3).

FIGURE 2 Provide Recommendations And Rationale Tied To The Forrester IAM Maturity Model

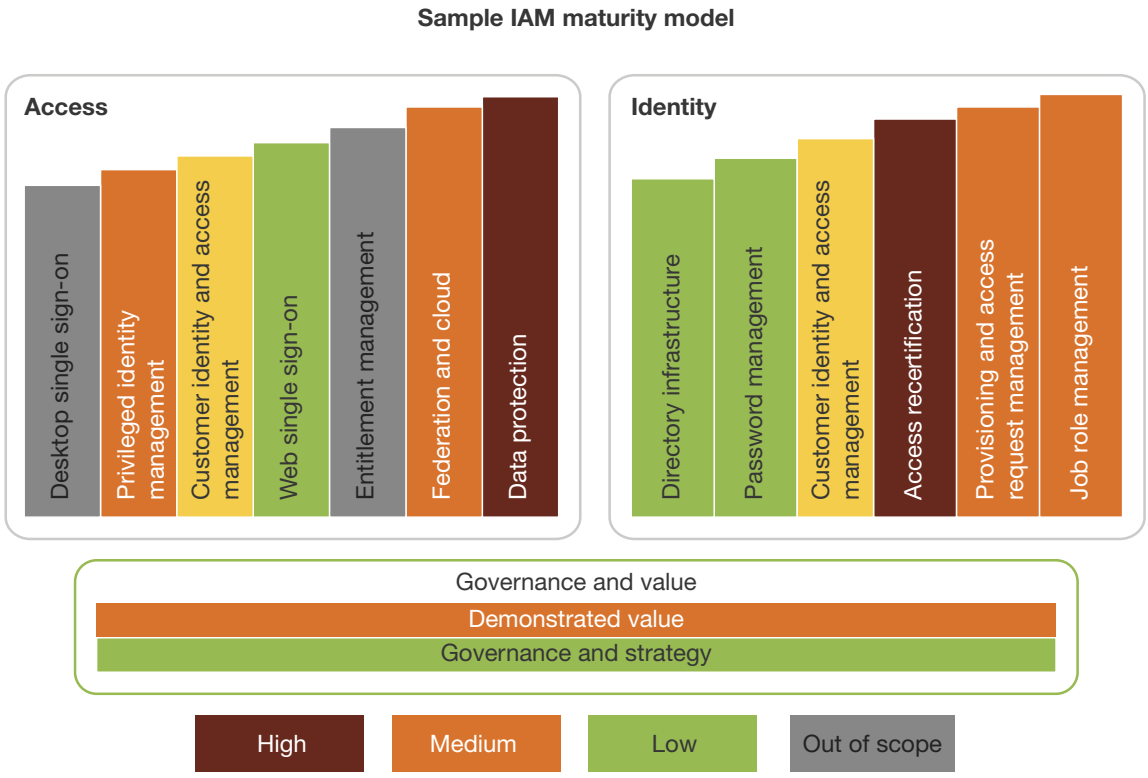


FIGURE 3 Example Summary Of IAM Observations And Supporting Facts

Area	Status	Our company compared with peers	Supporting facts
Data protection	Red	Behind	No comprehensive mapping of file shares to AD, no DLP/ERM, no data content tagging
Access recertification	Red	Behind	Manual processes for access recertification, no data assets access recertified, no preventive or detective SoD checks
Provisioning and request management	Yellow	On par	Continuous update of identity management and governance solutions for employees and business partners
Federation and cloud	Yellow	On par	Web services protection is nonstandard, it is difficult to map internal to external roles' translations, can't support SaaS applications adequately today
Privileged identity management	Yellow	On par	No registry of privileged systems, embedded credentials in property and configuration files for API calls and database access
Governance and value	Green	Ahead	Planning of IAM strategy systematic, HR is involved in IAM, our company is conscious about the business value-add of IAM
Web single sign-on	Green	Ahead	A web single sign-on product is implemented for a large number of applications, for password resets, and to lock out accounts not used for 60 days
Directory infrastructure	Green	Ahead	Two main AD domains exist: DOM1 and DOM2. Most authentication (from web SSO applications) happens against these AD domains
User password management	Green	Ahead	Centralized user identification provided by custom down-stream system, web SSO provides SSPR, most authentication is against AD so there is no major need for password sync

Step 2: Engage Stakeholders To Pique Their Interest And Build Cross-Functional Support

Many security teams believe they know everything about pain points of business stakeholders — this is simply not true. When interviewing business and other stakeholders, not only do you establish rapport and raise visibility, but you also discover new requirements and ways to optimize existing business processes. Therefore, we recommend that S&R pros:

› **Ask for and listen to the opinion of business users — even if you feel you know it.** Business users can respond to technical challenges provided the security team does a good job of explaining process, architectural and implementation options, and design decision factors in nontechnical terms. Spending time here will improve rapport and yield better business processes with better mapping of tools. Make sure interviewees can prepare for their interviews by providing them with a set of interview questions. Reducing the number of interview participants in individual meetings greatly increases candor. Business users will often have marketing and business goals (e.g., increasing conversion rates, lowering registration and log-in abandonment rates, or improving customer service times). You will have to work with your business users to connect their metrics to IAM metrics.

› **Demonstrate your ongoing commitment to solving business challenges.** If you have succeeded in addressing business pain identified during stakeholder interviews, be sure to highlight this fact in milestone presentations. This demonstrates to business leaders that you've taken the time to really understand their challenges and you've devised IAM approaches that alleviate them. This is even more important with nontechnical folks: Marketing and LOB stakeholders will always be very receptive to simplified security experiences that are communicated well to customers.

Step 3: Confirm A Tight Scope So That You Can Keep Your Job

In terms of complexity, effort, and collaboration required, IAM projects bear a resemblance to small ERP implementations and total website redesigns. Therefore, we recommend that S&R pros:

› **Cut 70% from the IAM scope by default.** Executive enthusiasm has forced many S&R pros to overscope IAM projects that eventually succumb to failure. Resist the temptation, and cut the initially planned scope in half, then cut an additional 20% from it. The resulting scope will be something that's more manageable to implement and will experience only slight delays. A reduced scope also increases the likelihood of success and can generate meaningful metrics that can prove business value and justify additional IAM investments.

› **Go live or die — go live with something useful and visible every three months.** We often hear S&R pros tell us they keep IAM projects on track by adhering to the "go live with something every three months" rule. Create an inventory and a priority chart of user groups or organizations and applications and prioritize them before casting the scope in stone. For customer-facing websites, this very often means trying to persuade the business to reduce the number of places where customers can enroll across all of the websites of the company.

Step 4: Define Metrics That Matter To The Business

At the end of the day, IAM is not different from any other project — it needs to have a return on investment. If you don't track metrics of how much you spend, and on what, and what benefits the IAM project brings in terms of administrative efficiency, cost reduction, better access and data security, employee satisfaction, and customer satisfaction, you won't be able to defend the project. Therefore, S&R pros should:

- **Track employee metrics that measure cost reductions, productivity, and security.** Typical metrics we have seen are: 1) number of help desk calls related to login and profile management; 2) time spent creating, modifying, and disabling/deleting accounts throughout the user's life cycle; 3) duration users wait before they have all their access; 4) time and cost to remediate compliance audit findings; and 5) cost of a security breach per record.[10]
- **Track customer metrics that zero in on experience.** For customer IAM, you should track: 1) how much time customers spend on enrollment and resetting passwords after failed login attempts and 2) what percentage of customers go to your competitors. This will also boost priority of the project.
- **Blend in IoT and operational technology metrics as appropriate.** Success in the world of connected IoT devices and operational technology (OT) requires that you examine the operational efficiencies of managing IoT devices and OT. Forrester expects that IoT devices will outnumber mobile and in-data center device numbers by 100 to 1 in the next two to three years. Typical metrics in this space include: 1) how many new devices are provisioned and deprovisioned in a day and what the cycle time is for provisioning each of these devices, and 2) time spent authenticating users and other devices to IoT and OT components.

Step 5: Detail Recommendations And Define A Future State Road Map

You need to visually represent your IAM recommendations to senior stakeholders. In addition, recommendations must be concrete and measureable. We recommend that S&R pros:

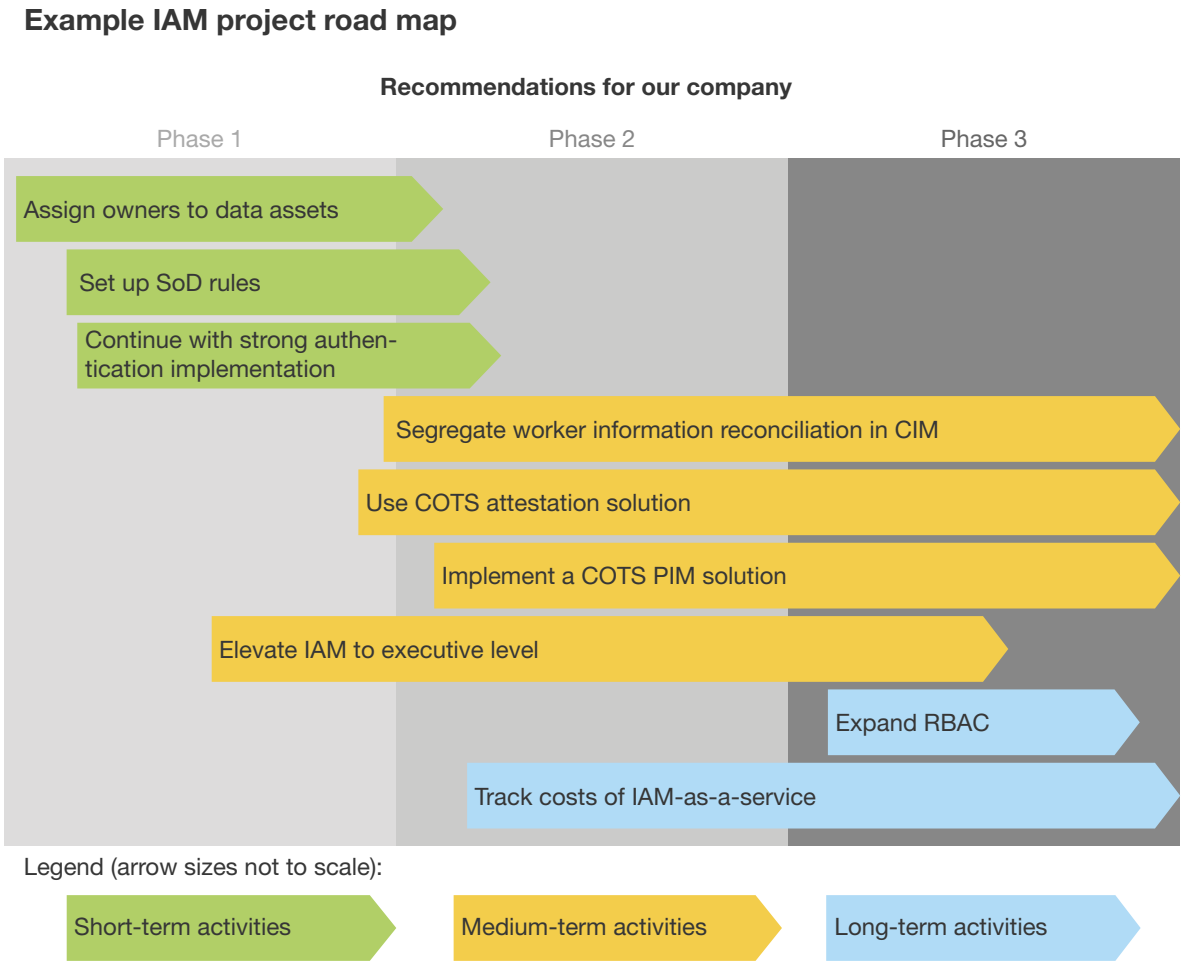
- **Align detailed recommendations with self-assessments.** Tying recommendations to observations helps justify why you're making the recommendation and helps overcome resistance (see Figure 4). Tying IAM changes to business transformation and external-facing website overhaul and redesign plans is a natural way to enhance the likelihood of successful completion of these projects.
- **Develop a detailed road map of your recommendations.** Once you have the tie-backs for recommendations established, you need to define a road map to detail when you will implement recommendations. A road map doesn't need to be a full-blown project plan; instead, it's a visual tool to understand interdependencies and rough project durations (see Figure 5). Having a technology road map comparing various technologies and their ease of use, cost, and potential user acceptance is also very useful.[11]

FIGURE 4 Linking Recommendations To Observations And Road Mapping Is Critical

Sample detailed recommendations

Observations/ recommendations	Data protection	Access recertification	Provisioning and request management	Federation and cloud	Privileged identity management	Governance and value	Web single sign-on	Directory infrastructure	User password management
Assign default owners to data assets	●	●				●			
Set up broad SoD detection and prevention rules	●	●	●	●	●				
Use COTS access recertification solution	●	●		●				●	●
Expand RBAC	●	●	●		●				
Continue with strong authentication implementation	●				●				
Implement a COTS PIM solution	●	●			●				
Track cost of IAM-as-a-service	●	●	●	●	●	●	●	●	●
Elevate IAM coordination to executive level	●	●	●	●	●	●	●	●	

FIGURE 5 Expand Linked Recommendations Into A High-Level IAM Road Map



Step 6: Communicate Progress And Value

The next step is transforming the road map into a concrete project schedule. Again, scoping is key. At this point, you may want to further reduce the scope to ensure that you have manageable projects. Tracking metrics is a great way of defending your project, proving that the project took off, and establishing a solid ROI; it's difficult for naysayers to argue with substantiated and quantified process improvements.[12] In addition to tracking customer-facing metrics for marketing, LOB, and executive stakeholders, Forrester's interviewees have also conducted qualitative interviews with their customer base to see how the redesigned IAM and security features of customer-facing websites have contributed to changed and improved customer perceptions of the company.

What It Means

Remember, IAM Strategy Is Only 30% Technology

Jumping to vendor selection prematurely is by far the biggest mistake we see in the field. IAM projects involve a fair amount of business re-engineering. Focusing on vendor selection too early distracts from core activities. Fully understanding requirements and business processes ahead of time, and making recommendations about how to make them simpler, dramatically reduces the cost of IAM product customizations and operational costs. When you've done all the appropriate due diligence and you're ready to select a vendor technology, we recommend that you:

- **Tie your proof of concept (POC) and vendor selection to the IAM strategy road map.** Carefully craft POC sessions with vendors. Your POC session should reflect your already well-understood requirements. Evaluating vendors along the same dimension and scoring them consistently is especially hard in IAM as tools have subtle and sometimes big differences in approach to the onboarding and offboarding and access recertification. Mapping the POC to the RFP is a must: Requirements must cascade from the IAM strategy road map to the RFP to the POC.
- **Look for packaged and well-integrated offerings.** Today's IAM tools and identity-as-a-service offerings increasingly provide out-of-the box support for basic IAM functions: registration; routine and step-up, two-factor authentication; URL-level authorization; user name and password recovery and management; provisioning; access request submission; and access request approval. Instead of spending time on customizing IAM for brick-and-mortar processes, accept what IAM solutions provide, and negotiate with business stakeholders to change processes. Find out from SIs their track record integrating your IAM solution selections in your vertical.
- **Aim for standards support, and avoid vendor lock-in.** Enterprises sink so much money and effort into implementing IAM that they're too reluctant to walk away from an obsoleted IAM solution, even if it's no longer working for what they need. Being ruthless about weeding out vendors that are not standards-compliant, and ensuring that a solution modularly fits into the firm's environment and can be swapped out in case it turns out to be a flop, reduces costs and helps avoid later frustrations.[13]

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester's research apps for iPhone® and iPad®
Stay ahead of your competition no matter where you are.

Endnotes

[1] See the Forrester report "Applying Technology, Systems, And Processes To Win, Serve, And Retain Customers" and see the Forrester report "Mobile Application Authentication Trends And Best Practices."

[2] See the Forrester report "The Best Of Website Experiences And Security Strength: US Online Retail Banks 2017."

[3] See the Forrester report "Forrester's Customer IAM Security Maturity Assessment Model."

[4] See the Forrester report "Optimize Your Identity And Access Management Program For Success."

[5] IT must replace older IAM infrastructure components, but must do this while providing necessary IAM services that keep end users connected to the IT system with the appropriate level of access. Pulling this off is akin to building Boston's "Big Dig" Central Artery/Tunnel Project, a project that was ultimately at least 10 years behind schedule and $12 billion over budget. Source: "Road to Tragedy: A history of Big Dig problems," Boston.com (http://www.boston.com/news/specials/big_dig_problems/).

[6] See the Forrester report "Identity And Access Management Metrics For Business Value."

[7] Security and risk (S&R) executives must manage identities and control access to sensitive applications and data because of security and compliance requirements — and they need to do so as effectively as possible. S&R pros can carry out identity and access management (IAM) processes using a combination of the following approaches: 1) a manual IAM process; 2) a "build your own" on-premises IAM system; 3) a commercial off-the-shelf (COTS) on-premises IAM solution; and 4) an IDaaS. This tool helps S&R executives quantify the cost and benefits for each of the above scenarios to determine which one provides the best return on investment (ROI). See the Forrester report "Forrester's Identity And Access Management Cost Model."

[8] See the Forrester report "Forrester's Customer IAM Security Maturity Assessment Model."

[9] See the Forrester report "The Forrester Identity Management And Governance Maturity Model" and see the Forrester report "Assess Your Active Directory Security."

[10] See the Forrester report "Identity And Access Management Metrics For Business Value."

[11] Strong authentication technologies vary and represent a very fragmented market. In a critical time when user authentication directly impacts the overall business, S&R leaders need to take a hard look at the current authentication solutions landscape and find the best solution for their business needs. See the Forrester report "Market Overview: Employee And Customer Authentication Solutions In 2013, Part 1 Of 2."

[12] See the Forrester report "Making The Business Case For Identity And Access Management" and see the Forrester report "Don't Bore Your Executives — Speak To Them In A Language That They Understand."

[13] See the Forrester report "TechRadar™: Zero Trust Identity Standards, Q1 2016."

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.