protiviti®
Face the Future with Confidence

Top 10 pitfalls of an IAM program

In spite of over 20 years of experience as an industry, Identity & Access Management (IAM) programs continue to struggle — and with good reason. There is a lot that can go wrong with an IAM program.

Lack of funding, treating IAM like a project and not a program, not having business buy-in, and trying to overly customize packaged software are all examples of significant challenges that can impact the ability for an IAM program to be successful. That's where this e-book comes in. The team at Protiviti has decades of real world, hands-on experience not only doing IAM, but doing IAM well. As a team, we collectively work with dozens of clients per year and have seen some commonalities for struggling IAM programs. In putting together this top ten list, you may recognize some that apply to you and some that you may want to keep an eye out for so you can proactively plan against those risks.

The top 10 common pitfalls of an IAM initiative:

01	Treating IAM like a project, not a program.
02	Lack of strong executive sponsorship.
03	Not having an IAM roadmap.
04	Not having the right team of engaged stakeholders.
05	Not treating IAM like a process (re)engineering exercise.
06	Letting the 20% (customization) ruin the 80% (out of the box functionality).
07	Too much, too soon.
08	Ignoring the end user.
09	Ignoring the cloud.
10	Not heeding the future.

01 Treating IAM like a project, not a program

Identity and access management

Identity and Access Management is core to many of an organization's most fundamental business processes. It ties into how employees are onboarded, how their relationship with the organization evolves through promotions, role changes, and geographic relocations, and ultimately how their separation from the organization is handled. It also is intricately involved with which privileges and access rights a user should have based on the nature of that evolving relationship with the business. Other constituencies, including contractors, partners, suppliers, and customers, further compound IAM complexity.

To tackle this effectively, IAM needs to be recognized for what it is, a multi-phased and frequently multi-year program that is composed of a series of projects with some running sequentially and others overlapping and in parallel. It needs one or more program managers that bring continuity and context for the duration of the program, spanning the various projects. Organizations that try to treat IAM as a singleton product implementation exercise are almost guaranteed to fail due to a combination of reasons: dissatisfied stakeholders, resource depletion, scope creep, and ultimately, inability to prove ROI or return the business case.

The pitfall

- Is the single biggest cause of failure of IAM programs
- Requires Ownership, Stewardship, Continuity, and Context
- Stakeholders that aren't getting their priorities addressed in the near-term will disengage
- Initiative will stall/fail

The remedy

- Set expectations that this is a multi-phase, multi-year initiative
- Establish the role of an IAM Program Manager, or equivalent
- Routinely communicate the IAM Program vision and resulting efforts

02 Lack of strong executive sponsorship

Mandate, authority, and internal respect

Per the previous point, IAM is a program and as such spans numerous departments in an organization. The budget is frequently created as a composite with a chunk coming from IT and/or Information Security, but with contributions also coming from stakeholder organizations including Operations, Human Resources, and others. Just as importantly, the program requires negotiation and priority-based tradeoffs for requirements across these various stakeholder organizations. Also, an IAM program almost always drives process changes in an organization (more on this in a bit) which can clash with cultural inertia and cause intra-department conflict. In addition to one or more program managers that are responsible for the day-to-day execution, without strong and steady executive leadership, the IAM program will not get off the ground.

An IAM program needs a strong executive sponsor that has the mandate, authority, and internal respect to shepherd it through the inevitable rocky times that will arise. This sponsor needs to be a respected leader within the organization and needs to be vested in and motivated by the success of the program. The sponsor will need to broker discussions and negotiations regarding prioritization across different stakeholders, communicate up and across the organization, and use a diverse set of interpersonal skills to build rapport and maintain consensus with the senior leadership of the organization to keep the program on track.

The pitfall

- IAM is a cross-functional initiative requiring budget and alignment across multiple stakeholders and departments
- If the Sponsor is disengaged or doesn't deem IAM as a priority, it will be undervalued
- Stakeholders will not engage when needed
- Initiative will stall/fail

The remedy

- Ensure that the Executive Sponsor is engaged and willing to be a "change agent" for the organization
- Empower the sponsor with business justification to market the IAM program to their peers

03 Not having an IAM roadmap

Tackle specific areas of capability

Due to its multi-phased approach, an IAM program will not deliver immediate benefits to all stakeholders. Many items will need to be deferred, not only out of the early phases, but may in fact be tabled until Year 2 or even Year 3 of the program. Without clear communication of how prioritization is taking place and what capabilities are planned for which phases and associated timeframes, stakeholder support will begin to fragment. Those that aren't clear on when their needs will be met or why they're being deferred in the first place may implement point solutions to tackle their immediate needs, leading to a reactionary organization and redundant and unnecessarily complex IT infrastructure. This in turn will expose the organization to additional cost due to software and hardware expenditures, and the need for additional skillsets, operational support, and additional upgrade cycles.

The Roadmap is a codification of how and when the IAM Program will tackle specific areas of capability. It needs to be defined and agreed upon during program inception and there needs to be clear consensus that all parties are "bought in." This consensus can only be achieved by having detailed discussions with all stakeholders regarding the cost and complexity of each phase as well as the business benefits that can be quantified for that phase. This allows dispassionate prioritization that will return value to the organization in an optimized manner. Periodically revisiting the roadmap also allows everyone to reassess those priorities based on changes in organizational strategy and needs.

The pitfall

- IAM is multi-faceted program
- Different phases will bring benefits to different stakeholders/organizations
- Without a defined roadmap, people that aren't getting what they need right away will implement redundant/point solutions for tactical needs
- Organization becomes reactionary instead of strategic
- Leads to technology redundancy, higher exposure to painful upgrade cycles, and ultimately rip-and-replace projects downstream

The remedy

- Define a clear, phased roadmap upon commencing the program
- Prioritize phases based on organizational urgency, technical complexity, and business benefit
- Tie each phase to a quantifiable business justification
- Get stakeholder buy-in from all parties, particularly those whose requirements will be addressed in downstream phases
- Assess the roadmap periodically as well as at the end of each phase of the program

04 Not having the right team of engaged stakeholders

IAM is a team sport

The multi-faceted nature of an IAM program requires the involvement of a diverse set of stakeholders and team members including those from Compliance, Finance, and Human Resources. If the program is treated just as an IT or Security project without involvement from the other stakeholders, the team will not have sufficient context or organizational knowledge to properly understand and decode the requirements and satisfy them appropriately. At the same time, getting too many people signed on for the team when their involvement is not consistently needed will create frustration and cause disengagement.

The ideal way to structure an IAM program team is by differentiating between a "core" team and an "extended" team. The Core team should be 100% dedicated to the program and include IT, Security, and Operations personnel. The extended team will be larger, perhaps significantly larger, and will include people that bring specific technical skills to bear or represent stakeholder organizations. It is critical to set expectations regarding when and how much time will be needed from extended team members (the Roadmap is a great tool for this!!). For instance, HR will be critical to have at the table when dealing with employee onboarding or termination use cases but shouldn't be needed for Compliance-oriented use cases such as periodic access reviews or reporting.

Similarly, enterprise architects may be needed during the initial technical architecture phase, but likely only need to be brought in for key checkpoints during subsequent use-case-driven phases.

The pitfall

- This is not just an IT or InfoSec project
- Has far-reaching impact across the entirety of the organization including HR, Finance, Compliance, and of course, IT
- Team members lack the skill set, or the organizational experience and knowledge
- Team members not available/engaged when needed due to overallocation

The remedy

- Structure the team as a Core team (~100% dedicated to Program) and an Extended team (as needed based on phase and stage)
- Set expectations and get management buy-in on when resources will be needed
- Involve the right stakeholders/team members at the right time
  - **Example:** In an "Onboarding" or "Termination" phase, HR will be a crucial participant, particularly during requirements analysis and design
  - **Example:** During a "Recertification/Access Review" phase, Compliance and Finance will be needed to understand the impacted systems (Finance) and the governance requirements (Compliance)

05 Not treating IAM like a process (re)engineering exercise

Put your management consulting hat on

An IAM Program is fundamentally a business process engineering and automation effort, and organizations ignore that maxim at their own peril. At a minimum, you are trying to automate some fairly core and critical business processes as they're defined in your organization. Far more likely, you've been chartered with identifying inefficiencies and functional coverage gaps in existing process, and to automate a set of refined processes to make the organization more secure, more compliant, and more efficient. If you don't keep this in mind, you will suffer from a combination of automating bad processes (put more colorfully, you will help do bad things much more quickly) and breaking things due to insufficient understanding of poorly documented existing processes.

Tackle your IAM program with the same rigor you would apply to business process re-engineering because that's what you're undertaking. Make sure you invest in building a deep understanding of the process you're trying to automate or refine. Any process or policy documentation is certainly important to digest but supplement it with detailed discussions with the appropriate stakeholders that are close to that process and take time to understand the intent of the process and any informal steps that occur to expedite it. Based on that knowledge, refine the process if needed, and from there automate what makes sense.

The pitfall

- IAM is a business process exercise
- Automate Bad Processes
  - Leads to doing the wrong things faster and at more scale
  - **Example:** Undocumented Recruiter-to-Payroll manual steps/handshakes are omitted during automation, resulting in creation and then cleanup of duplicate accounts

The remedy

- Make sure you deeply understand existing processes, including manual steps and inefficiencies.
- Work with your stakeholders to define a practical process
- Only automate what makes sense

06 Letting the 20% (customization) ruin the 80% (out of the box functionality)

There's a reason it's called the 80/20 rule

Another common pitfall we see is organizations that try to perfectly model their existing processes and workflows. Sometimes this is driven to harness the purported flexibility of an underlying tool or platform. It can also be the result of organizational rigidity and a desire to preserve what is perceived to be the best way to do something. Unfortunately, our experience with most tools is that there is an exponential cost in time and effort the further "offroad" clients try

to get from standard functionality. Ultimately, even after the extra time and expense, the end result still doesn't end up being perfect, resulting in unmet expectations and frustration with the program.

Instead, use the analysis stage of each phase to dig deep into the "why" of each requirement. Much as with the previous pitfall regarding business process, try to tease out the intent and see if there is any opportunity for optimization. Bear in mind that most modern tools are based on years of knowledge of IAM and often have best practices "baked in" to their baseline functionality (think SalesForce.com or Workday). Ultimately, if modeling the existing process is the correct thing to do, understand the cost/benefit of automating that aspect of the process (will automation be worth the cost of customization, support, maintenance, and so on) and if it isn't, consider leaving that manual instead of investing in automation.

The pitfall

- Try to mirror your existing processes and workflows perfectly
- Spend excessive time on the wrong side of the 80/20 divide
- Leads to budget/schedule overruns and the end result is still unsatisfactory

The remedy

- Most modern tools have best practices/processes built in; leverage them
- For complex workflows that require extensive customization
  - Work with stakeholders to understand the process and see if there's room to optimize
  - Consider leaving complex processes manual

07 Too much, too soon

Patience is a virtue

As with any program, the initial kickoff phase for IAM is frequently a time of excitement. The company has probably been through an IAM strategy session/workshop and has looked at tools and architectures to tackle their pain points around user administration, governance, compliance, and risk management. This is when organizational appetite for investment and risk will be at its highest and the program runs the risk of biting off more than it can chew. By trying to tackle big ticket items too early in the program lifecycle, organizations run the risk of creating expensive, complex, and long-lived early phases that don't deliver results fast enough and create disenchantment with the IAM program as a whole. Pitfall #3 was not having a roadmap at all — this one teaches us that a bad roadmap is (almost) as bad as no roadmap.

Instead, be judicious in how you phase out the early stages of your program. Get buy-in from all appropriate stakeholders because it is important for all that the program start by achieving some quick wins to demonstrate success to the business atlarge, and to build up momentum for more substantial phases. Early phases should be scoped so that they're strongly aligned with key organizational priorities and can be tackled quickly and with low technical risk. And as always, be sure to tie each phase to a clear business case based on fully loaded TCO (product licenses, hardware if needed, services, operations costs, etc.) and expected business benefit.

The pitfall

- Ambitious Phase I takes too long to deliver any tangible value
- Costs become harder to justify
- Organization loses faith in the initiative

The remedy

- Prioritize quick wins in the early phases of a project
  - Strong organizational alignment, low technical complexity, high business benefit
- Early phases should be 3-6 months — the shorter the better
- No phase should exceed 6 months
- Each phase should be tied to a clear business justification/business case that takes the entire TCO into account (license, maintenance, services, operational costs, etc.)

08 Ignoring the end user

Respect the consumerization of IT

This is a recent entrant into our pantheon of IAM pitfalls. The consumerization of IT over the past several years has created an irreversible expectation of elegant and user-friendly user experiences (UX), even for enterprise apps. Even in the largest and most

conservative of organizations, the use of SaaS and mobile apps for enterprise functions is commonplace (leading to a different issue — shadow IT). This trend is accelerating with the integration of the millennial generation into the mainstream workforce as they have even higher expectations regarding mobility and easy-to-use apps that allow them to execute their tasks efficiently and with a pleasing UX. IAM programs that don't take UX into consideration will be faced with abandonment and nonuse at best, which will significantly and negatively impact the ROI of the program. At worst, users will find workarounds, typically using shadow IT, that can expose the enterprise to security breaches.

A good IAM program will tackle UX head on by having end-users represented at the stakeholder table. Additional end-user representatives should be involved early in each phase to understand their usage patterns and common task flows. User Acceptance Testing (UAT) should be a crucial part of the QA cycle for each phase, and UAT testers should be empowered to create "blockers" if they believe that a particular deliverable is not sufficiently usable. Foundational to all of this is that the core set of technologies chosen for your IAM program should be modern and elegant with their web UI and ideally also offer mobile choices for end users.

The pitfall

- Consumerization of IT has led to high expectations for usability, even for enterprise apps
  - SaaS apps are increasingly seeing enterprise use ratcheting this bar higher
  - Further compounded by millennials entering the mainstream workforce
- Poor UX will cause non-adoption, and business benefit will not be realized
- Will create perception leading to a self-fulfilling prophecy of IAM program failure

The remedy

- Select modern tools with user-friendly UI and mobile apps
- Make sure that end-users are included as stakeholders and are involved in requirements analysis for each phase
- UAT should be a critical step in each phase, and should be empowered to block deployment if UX requirements aren't met

09 Ignoring the cloud

Utility computing is here to stay

Ignoring the impact that Cloud and SaaS will have on your company's IT infrastructure and on your IAM program is a sure-fire way to launch a program that's going to hit a wall in short order. It's an absolute given that at a minimum there are some SaaS/mobile apps being used in your organization. Most likely, you also have some flavor of IaaS cloud usage — Amazon AWS, Microsoft Azure, and the like — either as part of sanctioned work or through shadow IT. If your IAM program doesn't account for these scenarios, it will leave your organization without coverage for these elements of your IT infrastructure and leave you exposed to attack.

Factor "cloud awareness" into your thinking as it relates to your IAM program and roadmap along two dimensions. First, consider what SaaS/Cloud assets you need to secure and protect with your IAM program by performing a SaaS inventory and using CASB tools. Second, for your IAM toolset itself, make sure you consider SaaS-based IDaaS (Identity-as-a-Service) tools which can significantly reduce cost, effort, and time-to-market. Given the nascent nature of the IDaaS market, if those tools don't meet your requirements, strongly consider deploying an on-prem solution as a managed service to gain some of the same "SaaS-y" benefits.

The pitfall

- SaaS and IaaS are already being used in your organization
- This is not an "if" and it's no longer a "when," it's happening now, with or without your knowledge/consent
- At a minimum, there are probably employees using SaaS apps for departmental use and file sharing — guaranteed
- Pretending it's not happening will expose you to insufficient coverage of your infrastructure with your IAM program, and even worse, expose you to a breach

The remedy

- Be "Cloud Aware" in your roadmap
- Inventory your SaaS apps
- Understand where your organization is using IaaS platforms such as AWS and Azure and how that usage impacts your compliance, governance, and security requirements
- Consider using SaaS solutions where appropriate, or at least cloud-hosted solutions to reduce your data center footprint

10 Not heeding the future

Stay aware of where you're going

Change is the only constant in modern organizations. This is true for the organization itself and is even more true for the underlying IT infrastructure that serves as the fabric of its core business systems. Businesses are becoming increasingly agile in strategy and in their adoption of rapidly evolving technologies to enable that strategy. If an IAM program and underlying architecture is designed without sufficient foresight as to where the organization is going in the foreseeable future, it will not be able to adapt and evolve in an agile manner to support those changes. The end result is either a terminus for the IAM program or an expensive and time-consuming "rip and replace" process to accommodate a new platform that can meet those requirements.

As you instantiate your program (and on an ongoing basis), keep your finger on the pulse of how your organization is evolving. Begin by exploring how it has changed in the past five or ten years in terms of business strategy, M&A, technology strategy, and geographic footprint — this is frequently a strong indicator of what you can expect in the next five or ten years. Engage with the executive sponsor to understand the kinds of strategic directions that are being contemplated at leadership levels. At the same time, understand the trends that are occurring in technology and cybersecurity that may have an impact on your IAM roadmap. Use these all as inputs, always balancing them against the "here and now," to shape the fundamentals of your IAM program and technical architecture. Things like Customer IAM (CIAM), DevOps, the decomposition of monolithic apps into micro-services architectures, and the increased adoption of SaaS/Cloud/Mobile are all things that are at a minimum worth factoring into your medium- to long-range roadmap if they're not short-term needs for your organization yet.

The pitfall

- Every organization evolves, both as a business and in its technology platforms
- If you don't anticipate what kinds of requirements to expect in subsequent years of your IAM program, you will get locked into an unsustainable architecture
- The IAM platform will need to be replaced before it has returned the business case

The remedy

- Ask yourself and your team about how your organization has changed in the last decade, and will change in the next decade
  - Geographic expansion
  - M&A
- New strategic directions
- Be cognizant of secular trends (macro- trends) in technology and cyber security that could impact your IAM initiatives in Year 2 and beyond
  - DevOps
  - Micro-Services
  - B2C scenarios/Customer IAM
