CYBERWARRIOR
CONSULTING

10 STEPS TO A SUCCESSFUL IAM PROGRAM

ABSTRACT

The task of implementing an Identity & Access Management program can seem daunting, but it is not impossible. The goal of this document is to provide the reader with best practices for a successful AIM program.

These best practices are presented in the form of a high-level roadmap that goes from consensus building across the organization, project planning to get a solution implemented, and ultimately maintaining an up-to-date program that aligns with your regulatory compliance and audit needs.

TABLE OF CONTENTS

CYBERWARRIOR

STEP I: STARTING AT THE END... FIND YOUR PAIN POINTS

Begin the journey to governance by looking at the pain points you face today and defining goals: required versus important. A small core team led by the CISO/CIO (executive sponsor) should do this. The goal is not to develop solutions but to get an inventory of audit needs, business processes, and existing infrastructure.

As the team reaches out to stakeholders for initial data gathering, no promises should be made. In fact, the process should be explained to stakeholders as a discovery so that everyone feels at liberty to provide feedback on the proposed initiative.

Ensure that your team gathers facts, not solutions. Do not allow yourself to be pulled into a rabbit hole driven by someone's perspective or departmental agenda. When you have all the information, you can make decisions based on what is best for all involved instead of the specific needs/wants of a person/department.

The following is a generic list of assets that must be documented as we develop the IAM program. None of these belong to a single person, yet they impact the entire organization. You must capture everyone's perspective, as it will ensure collective buy-in as we move further into the process.

- Enterprise security program review.
- Enterprise Directory model.
- Enterprise Single Sign-On.
- Existing access control & user management procedures.
- HR procedures for onboarding, transferring, termination.
- Audit requirements & existing audit findings.
- Staff dedicated to access control & user management.
- Documentation on past attempts at automating IAM (just facts).
- Existing governance for IAM.
- List of stakeholders & their respective level of buy-in/interest for an IAM initiative.

DELIVERABLE

The delivery of this phase needs to be a report of the existing procedures & requirements that are currently outstanding or can be improved; in short, what the pain points are.

The report will be presented to the executive sponsor for direction on setting priorities.

The executive sponsor & the team will develop the goals of the project as well as the high level phases.

The team can now prepare an initial presentation for the future stakeholders (the folks which were initially interviewed). The presentation should outline the collective benefits of an IAM program and propose the creation of a Program Management team in which all stakeholders have an active participation.

STEP 2: DEVELOPING A SALES PITCH

The IAM project team & the project sponsor should now begin to research the types of identity management solutions in the market that appear to meet your requirements and industry reports on these vendors.

The team should develop a Q&A document on the types of constructive & negative criticisms they will face as they engage stakeholders across the organization. The goal of this exercise is to be prepared for the "reasons this project will fail." This can then be added to your proposal "pitch" to implement an IAM solution. This exercise will ensure that stakeholders become aware of your research & willing to work with them to meet the enterprises' requirements. The goal is to be perceived as "cool-tempered" and with a realistic strategic proposal.

The following is a suggested list of stakeholders whom to engage:

- Head of the HR Department.
- Head of the HRIS Department.
- CISO and or CIO (if these are not your executive sponsors).
- Head of the audit department (IT audit).
- Head of the department handling access requests.
- Head of the department handling access recertification.
- Head of the help desk department.
- Head of IT Infrastructure.
- Head of application support.
- Head of user experience.

DELIVERABLE

The deliverable of this phase will be a presentation with your initial data & general proposal. In this second presentation, you are connecting the dots. Phase 1 identified a problem. Phase 2 provides detail on what those issues are and aims to build consensus with the various stakeholders that something must be done.

This presentation should then be shared with the stakeholders in individual meetings to inform them of the "proposed" initiative to gather their feedback.

While developing your "pitch" presentation & Q&A documentation, it is important to note all concerns gathered and provide market options or best practice business process realignment. The presentation should be informational and provide a general direction to resolve the issue.

During the meeting with the stakeholder, provide an informational update and avoid engaging the stakeholder and/or his team in endless solution development sessions. The goal for each meeting is to present your research & high-level plan to the stakeholder. The team needs to make an effort to note & not judge the requirements presented by the stakeholder. The meeting should end on a positive note, with the team taking away the action to inventory the needs of all stakeholders. As well as an action to have a stakeholders' meeting to review the updated findings and the existing plans.

STEP 3: MEETING REGULATIONS AND SETTING PRIORITIES... GETTING FUNDING

The previous two phases were concentrated on data gathering as well as creating a stakeholder list. As painstaking as it may seem, it will now begin to pay off. As with any IT security project, requesting funding can be an uphill battle but, with your new arsenal of data and loosely assembled supporters, you will be able to draft an ROI statement that meets the requirements of various department needs.

Let's begin by listing out generic reasons why your stakeholders would back your proposal:

- Head of the HR Department – Alignment to existing procedures.
- Head of the HRIS Department – Enforcement of existing procedures.
- CISO and or CIO – Meets Audit requirements & cost reduction by automation.
- Head of the audit department (IT audit) – Aids in the enforcement of audit requirements.
- Head of the department handling access requests – Frees up staff for other duties.
- Head of the department handling access recertification – Aids in meeting audit requirements.
- Head of the help desk department – Frees up staff for other duties.
- Head of IT Infrastructure – Reduces IT infrastructure complexity by standardization.
- Head of application support – Reduces application support complexity by standardization.
- Head of user experience – Centralizes experience for access & recertification.

DELIVERABLE

This phase aims to customize your funding request proposal with your environment's specific requirements & pain points. The document needs to showcase an enterprise "must-have," not an IT security initiative.

The proposal document you develop in this phase will need to align your requirements to audit findings not being met and dollar figures that could be reduced by introducing a centralized identity & access management solution.

These "pain points" can be aligned to available vendor solutions in the marketplace. The vendor solutions should have an estimated cost (including disclaimers that a proof of concept will be required) and the costs associated
with IAM implementation (requires customer data to properly price). Do not forget about the cost for staff to maintain the solution; this is not just headcount cost but also training & shadowing time of the selected implementer. Vendors can guide the skillset required to support their tools. However, it is important to check with existing vendor customers and hear straight from them about what skills were required in their implementations. Talk to people that have deployed that specific technology.

Be sure to be open-minded as funding for various phases can be split by the various stakeholders or an agreement reached for a single budget that all the stakeholders support.

STEP 4: DON'T BLAME YOUR IAM VENDOR OR YOUR IMPLEMENTER

As you work through researching the IAM market, you will find a downright bloodcurdling truth: most IAM implementations FAIL. Now, before you call a team meeting to return the funding you had approved, let's work through a "gut check" of why they fail. It is imperative to note that at this point, you don't have a vendor or services implementer to blame as you have not spent any money.

We can begin by listing the pre-requisites for any IAM implementation:

- HR feed for employee data.
- Feed for non-employee data.
- User store feed for all applications being included in your project.
- Inventory of the procedures for hiring, transferring & terminating employees.
- Use cases for application provisioning for each of the applications in your scope.
- Use cases for access requests that your auditors approve.
- Use cases for access recertification that your auditors approve.
- Requirements for the user interface of your new IAM tool.
- Do you have a unique user identifier across applications?
- List of official IT policies to be met by this implementation (I.E., enterprise password policy).
- Staffing plan for your IAM implementation (internal staff & professional services budget).
- Server environments to host proof of concepts using your data, not the sales demo.

At this point, you may be panicking, calling your "preferred" vendor, and being told that these are not "required" to sign the contract and begin the work. There is a level of truth in that statement, but the risk is that you will be paying a professional services team to attend business analysis meetings to gather this data. A better approach is to gather the requirements and present these to the professional services team. Adjustments can be made at a lower cost.

DELIVERABLE

The goal of this phase is to deliver business analysis documents for the pre-requisites listed above. This is the perfect time for your internal IAM team to become fully engaged in the needs of your environments. It is strongly recommended that a PM be assigned to the project to develop a timeline based on the status of the pre-requisites.

To be fair to the vendor, you do not need to resolve all the issues, but you must document them & have a crystal clear view of the timeline to deliver them. The professional services team will thank you for your hard work, and your chances of delivering within budget will increase. This exercise will enable you to judge what solutions to buy what year. You may require one or two fiscal years to deliver all the phases due to your own internal requirements not being ready.

PS- The weird feeling you have in your stomach is your “gut check.” Don’t’ despair. It will pay off in the long run.

STEP 5: THE CHECKLIST FOR VENDOR SELECTION

Now that you understand the current status of your internal pre-requisites, it is time to develop a checklist that can be presented to the IAM vendors. We can begin by developing a use case list of all the functionality your team requires as part of the program and a list of applications to be provisioned.

The list below can be used as a foundation:

WORKFLOW NAME	FUNCTION
New hire employee	On-boards employees when they come in through the HR feed.
New hire non-employee	On-boards non-employees when they come in through the HR feed.
Employee disable	Disables employee accounts when accounts match given criteria.
Non-employee disable	Disables non-employee accounts when accounts match given criteria.
Non-employee profile creation	Allows authorized users to create a profile for a Non-Employee not created by the user feeds.
Ad-hoc change employee/non-employee	Change account level entitlements by request.
Non-employee extension	Extend the access of a Non-Employee per the given audit controls.
Termination employee/non-employee	Terminate users in the system and remove associated accounts when marked terminated.
Employee/non -employee transfers	Via a data flag in the HR feed a recertification workflow is initiated & assigned to the new manager. Provisioning actions can be assigned via a ticket or an automated connector process.
Employee's leave or absence	Temporarily mark a user's inactive until the time comes when the enable workflow runs.
Emergency termination	Terminate users in the system and immediately remove associated accounts from the target systems upon request from a manager, HR, or helpdesk user.
Role management	Create roles and map them to a user to add a set of entitlements without having to individually select them.
Recertification	Leverage the new certification tools to periodically review the access that each user has in the organization to ensure that everyone has the correct access to the various target systems.

DELIVERABLE

Remember that we are developing a phased program that sets realistic goals based on the current status of your internal data, procedures and your audit pre-requisites. The deliverable for this phase is a document that provides vendors with your requirements. A high-level program/project plan will need to be part of the documentation delivered. As part of this step your team should inventory the applications to be provisioned by an IAM solution. This will later help you to develop an identity management program that allows for the various workflows and target systems to be implemented over various project phases. Understanding your desired scope will ensure that you manage your budget wisely and will aid you and your vendor to properly work with you to plan out your various implementation phases.

STEP 6: VENDOR SELECTION

Present all prospective vendors with your requirements from the previous sections. Encourage vendors to suggest additional functionality and services that they feel were missed in your requirements document. Also, request to speak to a member of the vendor's implementation team (professional services) to make sure you are getting realistic project delivery timelines. You may also want to consider a vendor and a separate implementation team. Some vendors will have the right tool but the wrong approach to implementation. A strong consulting partner can be a valuable resource and an independent sounding board.

Ask vendors to package formal training classes into their proposal. As part of the review of the training programs, do not assume that your team meets the technical requirements to support the tool. Consider staff augmentation to get you started.

On the technical side, you are looking to meet the following basic IAM functionality as well as internal requirements:

Identity & Access Intelligence – This module will allow you to scan your existing infrastructure (AD is a good first step) and provide you with baseline reports that allow you to see what access has been granted to users and the reverse, who is a member of a given group or any other resource in your directory. You should be able to identify un-managed (orphan accounts). The tool has dual-use; it provides a snapshot of your existing directory and will later allow your team to monitor the performance of your operational IAM tools. This tool will not provide solutions but will aid in setting the priority and structure of your development phases. If your project budget has not been secured, this tool can help create a budget.

Access Request Management & Provisioning – This module will provide end-users with a centralized location for access requests. This will help develop an audit trail for management or application owner approval and the delegation of those approvals. This module will need to provide the data & reporting to meet audit requirements.

The module is the foundation from which you will eventually provide role-based provisioning. It will need to give you the flexibility to provide "role-based" access requests that "kick-off" a process for a manual request to fulfill the access request. For applications like Active Directory, the module should provide a "connector" for automated provisioning. We recommend that the vendor support team for the given application reviews any automated provisioning connectors before purchase. Connectors are a common "gotcha."

Compliance/Recertification Management – This is a simple but invaluable module. It should provide the ability to leverage an existing manager to report hierarchy to ensure accurate recertification. The module will need to extract or receive data from the applications being recertified and provide a "friendly" display of that data to the recertification manager. The ability to track the data and provide audit reports is a key factor when choosing a vendor in this area. Also, consider an add-on tool such as CyberWarrior's Intelligent Aqcess, which can automate recertification using Artificial Intelligence.

Password Management – This module will need to provide a very friendly/simple user interface to allow for self-service password reset and a workflow to allow your support team to reset passwords using the IAM tools. This module will aid in reducing the users that have privileged access to your various applications. This module is recommended as an "easy win" as it can help your team get familiar with the vendor tool.

Role mining & Role-based provisioning – This module may be part of your vendor's provisioning modules, or it may be separate. The decision to buy this product should be based on your internal team's ability to develop roles fully. Most teams will not be ready for roles in the first year of their IAM program. Many tools in the market today function with Machine Learning algorithms.

Single Sign-on tools/Management - This module is necessary for a full IAM implementation but does not need to be purchased until your team is ready to deploy it. Be sure to review how the vendor integrates with applications and verify that your application teams can meet the requirements.

DELIVERABLE

The deliverable in this phase is a comparison chart of vendor proposals including software pricing (licensing & maintance), professional services, and training costs. Please include a travel budget to attend the training. We encourage you to also include the cost of attending your vendor’s yearly conference as these can provide valuable partnerships with other customers going through similar implementations.

STEP 7: IMPLEMENTATION PLANNING

Prior to kicking off your implementation, your team should develop documentation to not only run the project but to also communicate to your various stakeholders the progress at the various levels. A key piece of a successful implementation is your IAM core support team.

This is made up of:

- Business Analyst.
- Project Manager.
- Application and Database support tech.
- Infrastructure Architect (someone that understands all the pieces across the company).

This is your core support team.

You will want to re-engage your stakeholders to ensure they are providing resources to make up your extended support team. Below is a sample of what your will need:

- Head of the HR Department – An analyst that is familiar with HR. procedures and the HR system.
- CISO and or CIO – A security analyst.
- Head of the audit department (IT audit) - Internal Auditor.
- Head of the department handling access requests – Manager of the group.
- Head of the department handling access recertification – Manager of the group.
- Head of the help desk department – Manager of the group Head of IT Infrastructure – Infrastructure Architect.
- Head of application support – Manager of the group per target system in scope.
- Department in charge of user experience – Manager of the group.

DELIVERABLE

This section will be focused on delivering the fully vetted PMO documents based on your requirements and the statement of work from your selected vendor. The required documents for this phase are:

- IAM program charter
- IAM phase one charter
- IAM phase one schedule
- Weekly status update
- Stake holder bi-weekly report
- Requirements document for phase one
- Use cases for the phase one implementation
- Test cases for the phase one implementation

These documents will be used to manage resources, communicate issues, and to progress update stakeholders. Communication and relationship management will be the key in the next phase.

STEP 8: IMPLEMENTATION EXECUTION

Providing immediate value to stakeholders will lock in continued support. Using PMO standards will be key to a successful project. An experienced implementation partner will have pre-built templates that may be customized, saving you time.

Below are proven approaches and checkpoints to delivering on this initial roll-out:

The core team “kick-off”

This meeting should be limited to the core team, vendor, and implementation team. The goal is to review how to complete the base installation and to discuss a project delivery timeline.

Your vendor should now provide the latest version and documentation of the purchased IAM solution as well as the technical requirements to build out the development environment. Your technical support team should attend training prior to this meeting to ensure a basic understanding of the product.

The team will now become a key part of your success. In this meeting, you should have a frank discussion on resource allocation with your implementer to ensure they are able to support the timelines you will be communicating to your stakeholders. A good starting point is a review of the statement of work with your implementation team with a deliverable of a technical requirements list for building the development environment, a resource requirements list, and a delivery timeline.

A commitment should be made by the core team to deliver a baseline demo of the IAM solution prior to scheduling the extended team “kick off”. Lots of people fail because they spend a year white boarding. They are trying to create a perfect system that requires for all data and business process issues to be resolved, however, that’s not the reality of where they are. Install the vendor solution as is and use it to clarify what’s wrong with the data and business processes so that you find yourself dealing with an action-oriented issues list and not just a whiteboard.

The extended team "kick-off."

This meeting aims to have an official kick-off with your stakeholders, an executive sponsor from your vendor, and an executive sponsor from the implementation team. The secondary goal is to have a strong "performance" by your core team to convey confidence amongst the extended group. The presentation should include the following:

- A demo of the base functionality of the solution by the implementation team
- A review by the Business Analyst's findings of the current state of data and business procedures and how they compare to the desired business solution – what are the gaps identified by the baseline demo?
- A review of the scope and the delivery timeline
- A next steps review as well as clear direction on what the team needs from the stakeholders

Bi-weekly Executive Meetings

As the team works to deliver the User Acceptance Testing phase, you should ensure that the project gets executive attention from your stakeholders and your vendor and implementation team. This ongoing communication will ensure resource allocation and focus on your effort. Communication should include positive progress reports, but most importantly, candid discussions about the items that are not going well.

Go Live Review

As your team works on finalizing the first phase of your program, the extended team should meet to review the functionality being delivered and the rollout and communication plans.

STEP 9: TRANSITION TO SUPPORT & FUTURE PLANNING

Prior to the official go-live date, your core team and the implementation team will need to meet with your vendor's support team. Usually, the implementer will be your go-to partner on product questions and issues and they receive support from the product vendor. However, it is strongly suggested that you require the product vendor to have someone from their organization be an active participant during meetings for the first 30 days post go-live (they should have been involved in implementation planning as well). That level of vendor engagement must be negotiated during vendor selection.

It is imperative that an as-built is document is not only delivered by the implementation team but also fully reviewed and validated by your core team. The recommended way to review it is an onsite knowledge transfer prior to the go-live.

A post go-live meeting is a good starting point for planning for your next phase. This should be a candid discussion about what was successful during Phase 1 and what can be improved upon. You also want to review what was delivered and how your changing environment will require that you re-align the delivered solution to new/changing business process, changing audit requirements, and data repositories that require upkeep. This meeting will ensure that your stakeholders and your vendor continue to support the IAM's program vision for the upcoming phases.

STEP 10: ACCESS RECERTIFICATION / ENTITLEMENT REVIEW

Now that your IAM platform is in place, you'll find the biggest challenges are still ahead. Not talking about technology, but rather that the processes to support the program are followed. Identity and Access Management is tedious and downright boring. It can also be time-consuming and often depends on managers that are already overworked to review entitlements (access privileges) of people they trust and have worked with for years… just another unnecessary bureaucratic process, they may think. This is where "rubber-stamping" is introduced and the foundation for many breaches. Forrester Research estimates that 80% of hacks involve compromised credentials. We recommend that entitlement review be done in real-time.

To solve this common problem, CyberWarrior developed Aqcess. Aqcess is a next-generation Identity Analytics Engine that makes it easy to enhance your existing governance program and maximize prior investments into Identity Management software. Our open API makes it easy to integrate. The tool can be deployed within a day as part of an auditing program, and the analysis takes seconds. It can also be configured in-line as part of the user provisioning process to prevent errors.

Aqcess leverages data classification algorithms to analyze entitlements and automatically identify users provisioned for rights they should not have. It tells you why the entitlement was flagged and provides a risk score. You then decide to approve or deny. The software learns from your decisions and continuously improves accuracy — eventually, it's able to take over low-risk approval workflows end-to-end.