Avoid failure and disappointment: essential items for your PAM checklist.

Written by Barry Scott, Customer Service Director, Osirium

Barry Scott,
Customer Services Director

Barry's career in IT infrastructure and operations spans more than 30 years, across a wide range of verticals and many different technologies. For the last 16 years, Barry has worked for startup software vendors in the Identity and Access Management (IAM), Privileged Access Management (PAM) and Identity as a Service (IDaaS) fields.

Barry helped to grow those companies across EMEA by building technical teams to fulfil customer pre- and post-sales needs, speaking at events across the region and blogging on topics such as GDPR.

Why a PAM project checklist?

It relates to a critical element in your security strategy. It addresses factors involved in over 80% of security breaches. And it's consistently identified by analysts as essential for organisations' security. But I've noticed over the years that projects to implement Privileged Access Management (PAM) too often end in disappointment and failure.

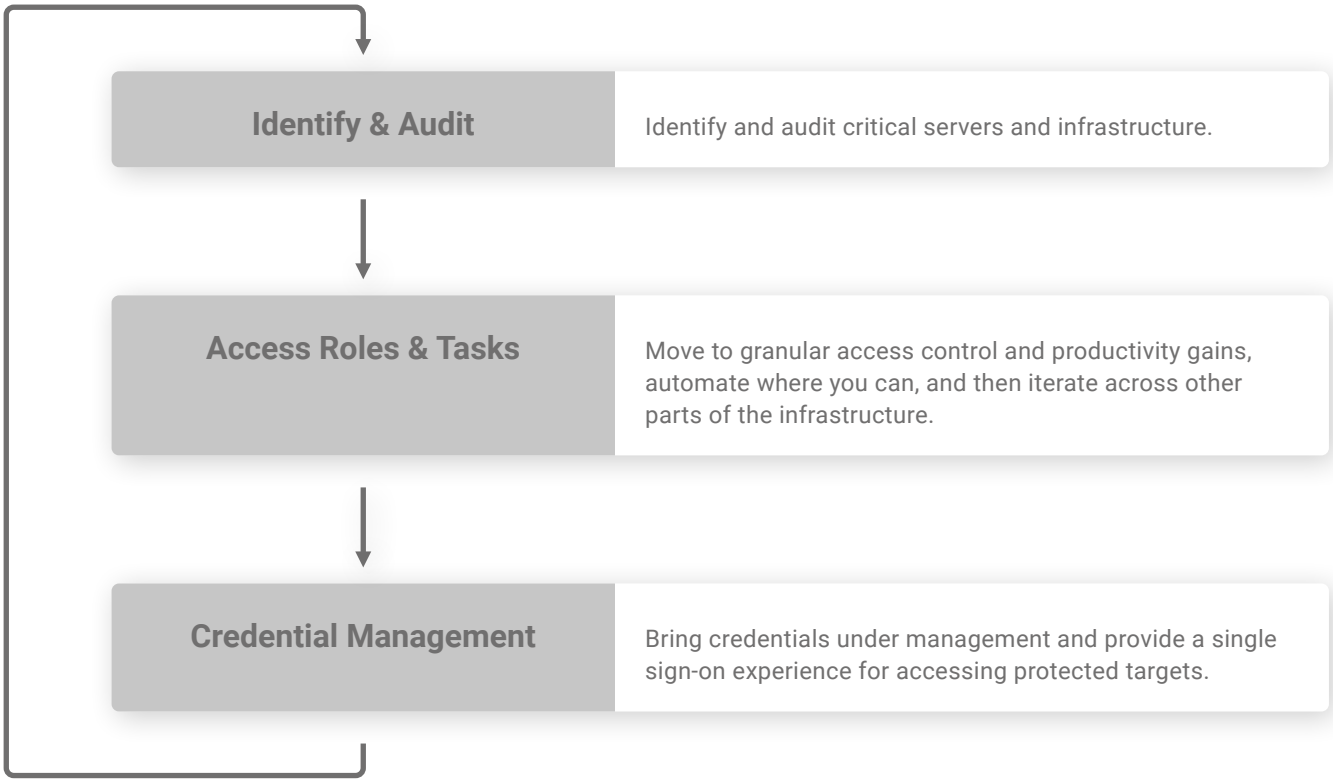
So, for people planning PAM projects, I thought it would be useful to understand and learn how to avoid factors that have at times given PAM a bad reputation. Too often we hear customers telling us of projects blighted by mismatched expectations, impenetrable complexity, rising costs, bus loads of vendor consultants, or implementations that drift to an eventual standstill with a wearying sense of nothing achieved.

Privileged Access is central to what we do at Osirium. In their current roles and previous lives our consultants and engineers have either worked on PAM projects themselves, or with partners and customers on their PAM implementations. Sometimes we're parachuted in to help sort out implementations that have drifted away from their original purpose. We're not infallible, but we have acquired considerable experience and insights into challenges that can arise with PAM, and this is what I'll be sharing here.

That's why we see merit in this PAM project checklist. It's not about teaching experienced and capable project managers how to do their jobs. It's about drawing on the wide range of PAM experiences shared by the Osirium team to help you supplement good programme skills with checks that apply consistently and uniquely to PAM, and avoid failure and disappointment.

A Staged Implementation Model

In this document we'll look at actions we recommend you take as part of a mental or process check to avoid the pitfalls that have contributed to many failed PAM projects. The checklist items we'll explore complement the three stage iterative Osirium implementation model we consistently and successfully apply with our customers.



Checklist Item 1. Identify the Key Drivers

Define the fundamental purpose for your PAM project, as this is where the greatest value is likely to be found. Very frequently it's variations on classic use cases:

- **Securing remote access, both for internal and external users.**
- **Getting oversight for privileged sessions.**
- **Controlling 3rd party or vendor access.**
- **Managing insider threats, either with the often cited 'disgruntled employee' or the well-meaning staff member with over-privileged access to excessive numbers of privileged accounts.**
- **Implementing Just in Time PAM, perhaps as part of a Zero Trust initiative.**
- **Demonstrating compliance and auditing, such as for GDPR, ISO 27001, Cyber Essentials, NIST, PCI.**

Identifying the driver with the greatest security benefit is key. Just 'Doing PAM' will soon lose direction.

Checklist Item 2. Set the Scope

This point follows on closely from the first, and will also affect how you demonstrate success as you roll out your project. Stay focused and concentrate on a limited number of use cases or organisational areas. Valuable lessons are learned in the early days of the planning and implementation and these can be applied to subsequent phases. Juggling multiple drivers across an entire infrastructure can easily become bogged down.

In addition, there's a disconcerting trend for analysts and vendors to keep redefining the boundaries of PAM. Some of them offer potential real value e.g. PAM for DevOps, PAM for Endpoints. However, on a PAM project the risk occurs when its scope is expanded. That's when clarity is lost and complexity sets in.

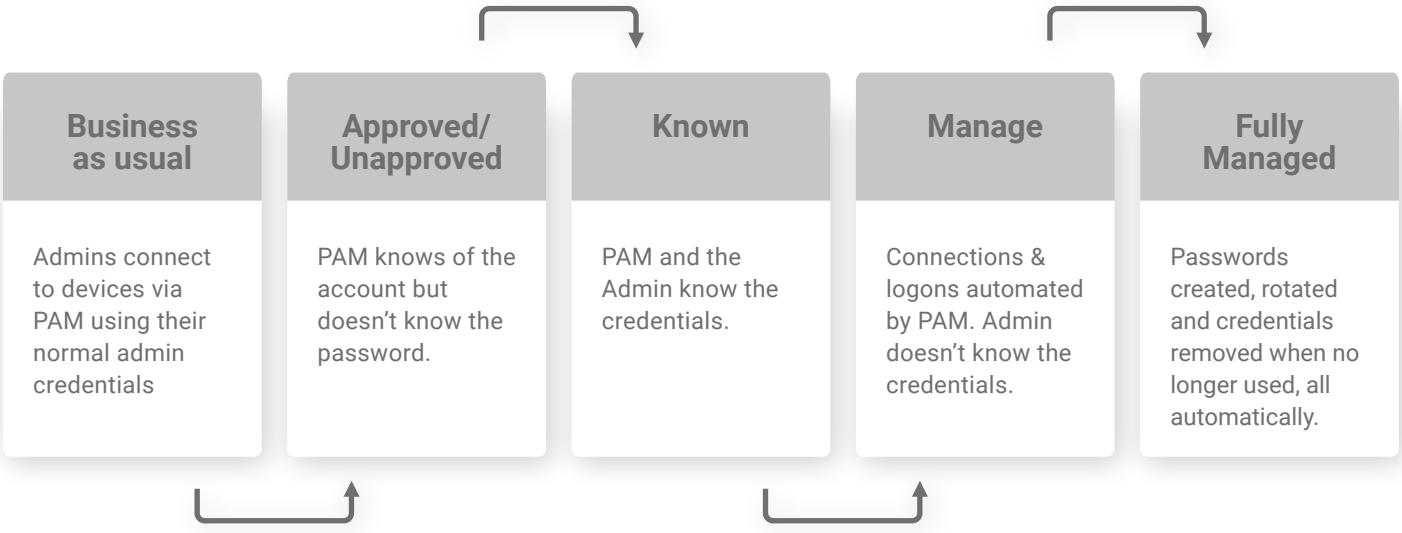
Ultimately the priority is to be sure you know why the project is happening. Clarity of who really needs privilege to access what and when will help you understand what success will look like.

Checklist Item 3. Secure Quick Wins

It's an uncomfortable truth, but unfortunately the very nature of PAM - limiting privileged access, authorisation, recording of sessions - means many project managers are likely to encounter resistance from PAM naysayers. Therefore it's important the project achieves some quick and visible wins to help get friends and allies in place.

Rather than attacking the entire infrastructure in a single hit, plan to have small subsets of devices to secure. Don't aim to bring in every Windows server and every Windows privileged user in one go. Depending on the infrastructure, look for discrete groups – possibly comprising database servers or network management devices or routers. To show progress, use PAM reporting to show how many targets and privileged accounts are being protected, and how usage over time is increasing.

For an illustration of how you might win the hearts and minds of stakeholders, the following sequence shows the steps we might encourage an Osirium customer to use. In this example we progress through non-intrusive phases of privileged account "states" to reach the nirvana of automatic password creation and rotation, as well as automatic removal of credentials when they're no longer used.



Above: Outlines the path through non-intrusive phases of privileged account "states" to reach full automation.

Checklist Item 4. Get Buy-in

It's an unfortunate truth, but without getting early buy-in from key stakeholders, including senior management, your PAM project will fail. As it progresses, you need to make sure the people who will be affected by the PAM project are on board, and keep them happy. For each phase of the project you'll need to explain how it affects them, what is being done, and why it is a good thing for both them and the organisation.

SysAdmins are a key target for bringing onside for several reasons.

You may well be changing the way they work, and most people don't like change on principle.

They've always had exclusive knowledge of passwords for this server or that router, so you'll need to explain why that needs to change.

If the project involves advanced PAM rather than a simple check-out/check-in password vault process, they might no longer know the passwords or be able to find them out.

Initially SysAdmins may well baulk at the idea of Session Recording. With explanation however they will realise that Session Recording is as much about proving innocence as highlighting fault if something goes wrong, and the resistance will lessen.

Be aware of possible changes to working practices. Jumping laterally from system to system may have previously been allowed as part of troubleshooting, but may be banned in a PAM environment as it can resemble hacker behaviour.

Checklist Item 5. Plan for Production and Integration

The PAM service you deploy is a critically important production system and needs to be treated and respected as such. Nothing will jeopardise the success of your project as much as your PAM system being unavailable when people need it. Checklist items for your rollout will therefore need to include:

- **Where you want to deploy PAM - on premises? Or in Azure, AWS or another Cloud environment?**
- **High availability and clustering. If applicable, will your PAM supplier require extra licences for PAM or elements such as database clustering that weren't mentioned in the original purchase (this is not an issue with Osirium licensing, which is simply based on the numbers of targets protected)?**
- **Backups need to be taken regularly and checked periodically to be sure you can restore from them.**
- **Document your disaster recovery processes, including your Break-Glass scenarios.**
- **Document the procedures for operations and maintenance.**
- **24/7 cover? If you need it, check your Support Contract includes it.**

The value of your PAM implementation will also be maximised with a well thought-through integration plan.

Your SIEM solution could be a good starting point. Make sure anything that goes on in PAM, such as adding targets, adding or deleting users, or user connections to a specific device, will be made available for your SIEM solution to perform any event correlation and / or reporting

Other tools, such as a scanning tool, will become more secure if it's PAM they get their credentials from, rather than having them hard-coded.

Look for PAM to add value to other tools and processes, such as increasing the use of automation.

Checklist Item 6. Looking to the Positives

It's almost certainly security or governance that were the initial drivers for PAM, but look early on in your project to build in measures that add value to the overall business.

This isn't 'scope creep' as warned against earlier, but a case of being mindful of the ROI and operational benefits that help sell the system against competing 'other projects'. For example, Osirium customers often look to our Privileged Process Automation technology to automate and delegate tasks and processes that would otherwise involve privileged accounts and (expensive) IT specialists. It bolsters the security of the implementation through a least privilege approach, as it only gives users access to carry out specific tasks. At the same time, it enables greater "shift left" from 3rd line to helpdesk and even end user resources.

A word of caution though: be careful of PAM solutions that claim to offer automation. In reality many only address specific PAM tasks like rotating passwords on a schedule, as opposed to automation of complex processes that rely on privileged skills.

Wrapping Up

As stated at the beginning of this document, its purpose is not to teach you how to run a project. It's goal is to draw your attention to those PAM-specific pitfalls that can dog even the best planned implementations. We hope you can bear these in mind in preparing for and executing your PAM project, and bring about success, satisfaction and security.

Identify the Key Drivers | **Setting the Scope** | **Securing the Quick Wins** | **Getting Buy-in** | **Plan for Production & Integration** | **Looking to the Positives**

About Osirium

Osirium is a leading innovator in Privileged Access Management. Founded in 2008 and with its HQ in the UK, near Reading, Osirium's management team has been helping thousands of organisations over the past 25 years protect and transform their IT security services.

The Osirium team have intelligently combined the latest generation of Cyber-Security and automation technology to create the world's first built-for-purpose Privileged Protection and Task Automation solution.

Tried and tested by some of the world's biggest brands and public-sector bodies, Osirium helps organisations drive down business risks, operational costs and meet IT compliance.

For more information, please contact us at info@osirium.com