SECURITY RESOURCE

Identity & PAM Quick-Wins Checklist

Most serious intrusions begin with a valid login, not an exploit. These focused steps reduce identity risk without a single large project.

For security and IT teams in Ireland and the UK
Prepared by the Edge7 Networks Security Practice

The control hiding in plain sight

Ask where the security budget goes and the answer is usually endpoints, firewalls, and monitoring. All necessary. But the control attackers most reliably exploit, and organisations most reliably under-invest in, is identity. Compromise a valid account, especially a privileged one, and much of the rest of the stack is looking the other way, because the activity appears legitimate.

> **Why break in when you can log in**
>
> Most serious intrusions do not begin with an exploit. They begin with a valid login. Credential theft, phishing, and session hijacking are attractive precisely because a working credential is quieter and more reliable than exploiting a vulnerability.

The privileged access problem

Ordinary accounts are a risk. Privileged accounts are the prize. Domain admins, cloud root accounts, service accounts, and local administrator rights scattered across endpoints let an attacker move laterally, disable defences, and reach the data that matters. In most organisations privilege is sprawling and poorly mapped.

- [ ] Administrator rights granted for a one-off task and never revoked
- [ ] Service accounts with high privilege, shared passwords, and no clear owner
- [ ] Former staff or projects whose access was never cleaned up
- [ ] No single view of who holds privileged access to what

Quick wins that move the needle

Improving identity posture does not require a single large project. This sequence delivers real reduction in risk, and the first move is always visibility.

1

1 · Inventory privileged access

You cannot control what you cannot see. A clear map of privileged accounts, human and service, is the starting point.

2

2 · Enforce phishing-resistant MFA

Everywhere it can be applied, and especially on privileged and remote access.

3

3 · Remove standing privilege

Withdraw rights that are not justified and move toward just-in-time elevation for a defined task and window.

4

4 · Bring service accounts under management

Clear ownership, secure storage, and rotated credentials, instead of shared passwords in plain sight.

5

5 · Review access regularly

Rights granted for a reason are removed when the reason ends.

What PAM delivers when done well

Capability	What it means
Least privilege	People and systems hold only the access they need, for as long as they need it.
Just-in-time access	Elevated rights are granted for a defined task and window, then withdrawn, rather than standing permanently.
Credential vaulting & rotation	Privileged credentials are stored securely, rotated regularly, and not shared in plain sight.
Session control & audit	Privileged sessions are monitored and recorded, so there is a clear account of what was done with elevated rights.

Identity is the foundation of Zero Trust

Strong identity and privileged access control are the base layer of a Zero Trust architecture. Every access decision starts with verifying who is asking. If the identity estate is weak, the controls layered above it inherit that weakness, which is why identity is usually the first serious workstream.

Want a clear view of your identity estate? Let’s talk.

Edge7 Networks helps IT teams across Ireland and the UK map privileged access, enforce phishing-resistant MFA, and bring service accounts and standing privilege under control.

Web edge7networks.com **Dublin +353 1 969 4001** **London +44 20 8176 0150**

This checklist is a practical planning aid produced by Edge7 Networks. Edge7 Networks holds ISO 27001:2022, ISO 9001:2015, and Cyber Essentials certifications.