Measuring Your Identity & Access Management (IAM) Maturity

A Step-by-Step Checklist for Gaining Visibility into Your Existing Security Posture

MANGANO IT
www.manganoit.com.au

16 Edmondstone St, Newmarket
QLD 4051, Australia
Phone: 07 3151 9000 | Email: sales@manganoit.com.au

Microsoft Partner
Microsoft

Gold Security
Gold Small and Midmarket Cloud Solutions
Gold Cloud Productivity
Gold Cloud Platform

With Microsoft reporting a 300% increase in identity attacks over the past year alone, the potential ramifications of IAM shortcomings must be taken seriously.

Modern organisations have no shortage of responsibilities when it comes to information technology and digital assets – especially as threats including bushfires and COVID-19 have driven faster adoption of remote work and digital transformation than ever before. Yet, when it comes to identity and access management (IAM), it's not uncommon for businesses to fall behind.

That's a problem, as companies with weak IAM policies put themselves at risk of identity attacks, may face penalties for failing to meet modern compliance standards surrounding data privacy and security, and can struggle to keep up with the growing demands of remote productivity and IT modernisation. With Microsoft reporting a 300% increase in identity attacks over the past year alone, the potential ramifications of IAM shortcomings must be taken seriously.

A comprehensive analysis of your IAM policies and security posture is important, but before taking that step, use this audit checklist to understand your organisation's IAM maturity. While this checklist shouldn't replace a full IAM assessment down the road, it'll give you a starting point towards understanding your program's strengths and weaknesses – ultimately preparing you to make meaningful changes to your IT landscape and IAM protocols.

16 Edmondstone St, Newmarket QLD 4051, Australia | Phone: 07 3151 9000 | Email: sales@manganoit.com.au

IAM Requirements and Audit Checklist

Use the following sections to reflect on your current cybersecurity and digital setups to see what you have in place already – and what you're missing.

Your Organisation's Current IAM Policy

To begin, do you have a current IAM policy in place? While it's in every company's best interest to have an IAM policy, not all companies do.

Ideally, your policy should outline the current steps taken to manage identity and access across all levels of the business, from clients and entry-level employees through to the board of directors. Understanding your current policies, if they exist, will help you establish key areas for improvement going forward.

- ☐ Do you have an existing IAM policy that employees must agree to, sign and follow?
- ☐ What are your organisation's main compliance requirements? Are they addressed by the IAM policy?
- ☐ Have you mapped out who in your organisation needs access to what, as part of the IAM policy planning process?
- ☐ Have you identified the stakeholders involved in IAM decision-making at your organisation? Are they aware of – and able to execute – their roles and responsibilities?
- ☐ Have you established a cadence for reviewing and updating your IAM policy?
- ☐ Do your disaster recovery (DR) or incident response plans include actions to address any related IAM issues?
- ☐ Is the IAM policy enforced at your organisation, or is lacklustre adoption allowed to persist?

> "Modern technology presents a decentralised network of applications and platforms that users require access to from multiple devices. Identity and Access Management reduces complexity at the organisational level using a single, holistic solution that presents simplified user access and increased security and agility."
>
> **- Craig Smith, Enterprise Architect, Mangano IT**

MANGANO IT
www.manganoit.com.au

As the way we work has changed, the way we think about IAM must change as well.

IAM Documentation

Documentation is the foundation of proper IAM programming. Companies that focus on creating and maintaining appropriate documentation benefit from higher levels of security and a greater understanding of their IT systems (including its advantages and limitations) than those without this core element in place.

- Do you maintain a central database or other directory infrastructure with details of all users, including roles and access levels?
- Are IAM processes and procedures codified within a single document (or set of documents)?
- Is your policy documentation stored in a central location that's easy to access by relevant parties?
- How do you communicate with relevant team members that documentation has been updated?
- Have you established the length of time for which you'll keep past IAM documentation for reference?

Modern Workforce

When it comes to measuring your IAM maturity, many companies limit their thinking to office firewalls or on-prem systems. But all of that becomes irrelevant once employees get home and log on to their home networks. As the way we work has changed, we have to think about IAM differently.

- Do you have policies in place controlling the access users have to sensitive information while working remotely from personal devices?
- Have you educated team members on proper security protocols for remote networks and remote network usage?
- Have you implemented a policy around printing documents on home networks?
- How have you addressed social media usage within your IAM policies?
- If employees are working remotely, does your IAM policy address risks associated with other devices sharing their home networks?

> Business needs to consider the implications of Identity and Access Management (IAM) holistically across an organisation. A successful implementation of IAM requires a cohesive approach from all departments ensuring business policy and process leads to the right people having access to the right data from the right locations.
>
> **- Paul Mangano, Managing Director, Mangano IT**

Device Management

Although IT infrastructures vary from business to business, appropriate device management is crucial to organisations both big and small. Strengthening your IAM policies requires a comprehensive understanding of what devices exist in your organisation, how they're used and how access is provisioned.

- Are you utilising a service like Azure AD to facilitate multi-factor authentication (MFA) and single sign-on (SSO)?
- Do you use a 'zero-trust' approach when managing device access and usage?
- How often do you update device security software? If employees use their own devices, how do you ensure they're updated?
- What measures do you have in place to protect sensitive data in the event of device theft (or misplaced devices)?

If your device management policies haven't been updated recently, commit to a review in the near future. Advances such as conditional access policy enforcement and AI-assisted authentication can make device management easier and less painful – and more likely to be adopted – than ever before.

User Roles and Access

Teams change, projects finish and new programs are regularly introduced. These and other updates must be accounted for in routine audits of user role and access security.

- Have you captured a list of all the systems in which you manage user roles, including any Software-as-a-Service (SaaS) or on-prem resources?
- Do you follow a 'least-privileged' approach when provisioning new accounts?
- How often do you check your user access documentation to update roles and privileges?
- In the case of critical functions, do you use a 'Segregation of Duties' (SoD) approach to share control over core systems or processes?
- What security measures control how and when user roles or access levels can be changed?

MANGANO IT
www.manganoit.com.au

16 Edmondstone St, Newmarket QLD 4051, Australia | Phone: 07 3151 9000 | Email: sales@manganoit.com.au

81 per cent of breaches leverage **stolen or weak passwords**, which makes proper user management and training essential for IAM.

User Privileges

Professional, timely communications and collaboration requires appropriate access to devices and data. However, keeping stakeholders connected also introduces security risk. User privileges cover who has access to what information and software, as well as what the conditions of their access are.

Setting the right user privileges is crucial to both protecting sensitive information and maintaining an efficient team workflow.

- ☐ Do you have an up-to-date list of users and their privileges across various programs and devices?
- ☐ Is the ability to change individual users' privileges appropriately secured?
- ☐ Do you have a process in place for allowing and revoking temporary privileges?
- ☐ If you use generic accounts, have you ensured they haven't been granted Admin rights?
- ☐ Are you satisfied with your current delegation of user privileges? Do you feel you need more or fewer privileges?

Hiring Workflow

Bringing on new workers is a key part of managing growth and turnover, but granting new users access to your systems also introduces risk. Businesses across aged care, manufacturing, financial services, government organisations and other sectors must have a proper onboarding process in place to protect the organisation from unanticipated security threats.

- ☐ Does your onboarding process include a review of your organisation's IAM policy?
- ☐ Are new employees required to sign a confidentiality agreement or other policies controlling data collection and usage?
- ☐ Do you provide new users with security training for your various systems and devices?
- ☐ Do you update existing users when changes are made to security or IAM policies?
- ☐ Do you have generic accounts for training and testing purposes? If so, how is access to these accounts limited after training or testing is complete?
- ☐ How often are employees required to change their passwords and security settings?
- ☐ Do you review user access and privileges following internal promotions or department changes?

16 Edmondstone St, Newmarket QLD 4051, Australia | Phone: 07 3151 9000 | Email: sales@manganoit.com.au

> It is critical that cybersecurity foundational services, such as identity and access management, be effectively implemented and maintained. If these core services are in poor condition, building additional layers of security on this will likely suffer greatly or even become nullified.
>
> **- Ben McLeod, Security Lead, Mangano IT**

Termination Workflow

When turnover occurs, it must be handled strategically to minimise security risks. Once an employee leaves your business, there is no reason for them to have access to any of your sensitive business data. Maintaining an IAM termination workflow ensures access is discontinued in a timely manner and that their devices or data can be transferred over to their replacement.

- ☐ Does your IAM policy encompass employee termination procedures?
- ☐ Do you take steps to identify where terminated employees may have stored company data (including downloaded data or files kept at home by remote workers) to ensure it can be protected?
- ☐ Do you have a timeline for removing and/or switching over user access and privileges when an employee leaves the company?
- ☐ Do you have a record of previous employees and their devices and access levels for reference?
- ☐ What system do you use to maintain records of onboarded and terminated employees?
- ☐ How often do you delete or disable inactive or dormant accounts?

Customised IT Solutions Focused on Identity and Access Management

Going through this identity and access management audit checklist gives you the visibility needed to reflect on your current IT systems, as well as where upgraded security and preventive measures may be appropriate.

However, if you've identified issues – or if you're ready to implement any necessary changes you've uncovered – Mangano IT, a Microsoft Gold Certified Security Partner, can help you establish and enhance your IAM practise so that you can focus on what you do best, without compromising digital safety and security.

Contact our team of trusted IT specialists today for a personal review of your IAM audit results or to explore next steps for your company's IT solutions.

MANGANO IT
www.manganoit.com.au

Contact Us

Mangano IT
16 Edmondstone St, Newmarket QLD
4051, Australia
Phone: 07 3151 9000
Email: sales@manganoit.com.au