Barracuda
Your business, secured.

IDENTITY ACCESS AND MANAGEMENT CHECKLIST

Identity and access management (IAM) is a set of protocols, frameworks and policies that organisations use to control who has access to digital assets and resources. IAM is an important aspect of cybersecurity, ensuring that only the right individuals are given access, and then only to what they need, and that unauthorised users don't gain access. It's particularly important now because many companies have hybrid working policies, allowing users access to the network from outside of the traditional perimeter.

□ Establish a user lifecycle management process

A user lifecycle management process is a repeatable list of steps that are taken across the duration of users' time with an organisation. This includes setting up the account, making tweaks to permissions and removing access when they are no longer with the company. These steps might be different for different types of users, such as in-office staff, external contractors and remote workers.

What's important is that there is a defined process and regular reviews so that companies can be sure that all users have the correct access rights — nothing more and nothing less.

□ Set up authentication controls

Giving access permissions to users isn't enough to guarantee that your IAM stays secure. It's also important to set up methods to continuously verify each user at a regular cadence. You should have clear, enforced password policies with a regular reset schedule, and strong login monitoring and lockout procedures.

You should also implement multi-factor authentication, using an authenticator app or biometric identification, for an extra layer of security. Single sign-on is another method that both streamlines the user authentication experience and helps your organisation stay secure.

□ Implement robust access management

It's important that you have a thorough access management framework and make sure that you adhere to it with all user accounts. Create a role-based access framework, which grants people in specific roles the access they need for that role, rather than assigning access for each individual. This simplifies admin and makes sure they only have necessary permissions. Underpinning this framework, the principle of least privilege helps you limit users' access to the minimum required to perform their roles effectively.

You should also consider using Zero Trust Network Access, which is an approach to cybersecurity that operates with a 'never trust, always verify' philosophy. It assumes that no one should be automatically given access to any of your organisation's resources — all access should be granted on a case-by-case basis.

It's also important to define third-party access controls. Third-party access controls let external partners, such as vendors or service providers, gain access to your data. Effectively managing third-party access is crucial for your security posture, because opening up access to external users comes with potential risk.

□ Continuously monitor access

You should never 'set and forget' your identity and access management policies. It's not enough to just grant the necessary permissions, because the process doesn't end there. Organisations must ensure that they are continuously logging and reviewing access activity to identify any potential threats or issues. Implement suspicious behaviour detection tools that use AI to identify anomalous user behaviour that might indicate a threat.

A strict incident response policy is also part of your IAM protocol. This is the process that you follow if you identify a problem with a bad actor — a malicious insider, for example — gaining access to assets or resources by exploiting your IAM approach. This incident response policy should include remediation and reporting.

Lastly, it's important to consider how your IAM framework helps you maintain compliance with regulations such as GDPR, by cross-referencing your IAM protocols with sensitive data policies and directives.

By making sure that your organisation can tick every box on this checklist, you are setting up your users and business for cybersecurity success. But don't stop your learning here. Discover how Barracuda can help you boost your IAM framework.

Barracuda®
Your business, secured.