Identefi

SELF-ASSESSMENT

Identity Risk Self-Assessment

Ten minutes, twelve questions, one score. See where your Microsoft 365 identity setup is exposed.

How to use this

Answer each question for your organization as it works today, not as it should work. Score **2** for Yes, **1** for Partly, and **0** for No or Don't know.

> **If you can't say, score 0.** Not knowing is itself a finding.

The questions

#	Question	Your score	Why it matters
1	**Is multifactor authentication (MFA) required for every user, not just administrators?**	☐ 2 ☐ 1 ☐ 0	Stolen passwords are the most common way into Microsoft 365 accounts. MFA stops most of those attempts.
2	**Do you have a written offboarding process, and is IT told on or before a person's last day?**	☐ 2 ☐ 1 ☐ 0	Accounts that stay active after someone leaves are open doors that no one is watching.
3	**Can you confirm that no former employee, volunteer or contractor from the past 12 months still has an active account?**	☐ 2 ☐ 1 ☐ 0	Most organizations find leftover accounts the first time they check.
4	**Is your number of Global Administrators small (five or fewer), with each one a named person?**	☐ 2 ☐ 1 ☐ 0	Every extra administrator is another account that could give an attacker full control.
5	**Do administrators use a separate account for admin work, one that is not used for email and browsing?**	☐ 2 ☐ 1 ☐ 0	An admin who reads email with an admin account is one phishing message from a full compromise.
6	**In the past 12 months, has someone reviewed who can reach your most sensitive data (donor, client, case or financial records)?**	☐ 2 ☐ 1 ☐ 0	Access accumulates over time. Without a review, people keep access to things they no longer need.
7	**Do you know every guest or external account in your tenant, and are they reviewed regularly?**	☐ 2 ☐ 1 ☐ 0	Guests are easy to add and easy to forget.
8	**Do volunteers, contractors and board members have accounts with an end date or a named owner?**	☐ 2 ☐ 1 ☐ 0	These groups turn over often and are the accounts most often left behind.
9	**Is legacy authentication (older sign-in methods that cannot use MFA) blocked?**	☐ 2 ☐ 1 ☐ 0	Legacy sign-in lets attackers bypass MFA entirely.

#	Question	Your score	Why it matters
10	**Can you see which third-party apps users have allowed to access company data, and are users prevented from approving new ones without review?**	☐ 2 ☐ 1 ☐ 0	Malicious apps that request permission to read mail and files are a common attack.
11	**Are shared or generic logins (for example info@ or admin used as a sign-in) avoided or tightly controlled?**	☐ 2 ☐ 1 ☐ 0	A shared login means you cannot tell who did what, or remove one person's access.
12	**Are automatic mail forwarding to outside addresses and unusual inbox rules blocked or monitored?**	☐ 2 ☐ 1 ☐ 0	Hidden forwarding rules are a standard method for stealing mail after a compromise and often go unnoticed for months.

Your total (max 24): ☐

Your score

0–8
High exposure

Basic identity controls are missing or unconfirmed. One compromised or forgotten account could cause a serious incident. Fix the items you scored 0 first.

9–16
Moderate exposure

Some controls are in place, with gaps that attackers look for. The gaps are usually in processes (offboarding, reviews), not technology.

17–24
Stronger position

Good foundation. The risk now is drift: controls that were set up once and not reviewed.

What to do first

Whatever your score, start with these in order:

1. **Enforce MFA for everyone** (question 1)
2. **Find and disable accounts that should no longer exist** (questions 2, 3, 8)
3. **Reduce and separate administrator access** (questions 4, 5)
4. **Put a recurring review on the calendar** (questions 6, 7)

Limits of this self-assessment

This is a quick screening based on your own answers. It does not test your configuration, and a high score does not mean your environment is secure. A technical review of your Microsoft Entra ID settings will show the real picture.

Want the real picture? Identefi can review your Microsoft 365 / Entra ID identity setup and tell you what to fix first. **hello@identefi.com** · identefi.com

© Voss Technology Group LLC dba Identefi.