SCALLEX

TORONTO / GTA PROFESSIONAL FIRMS

# Microsoft 365 & Cyber Risk Scorecard for Professional Firms

A leadership self-review for Toronto and GTA professional firms to identify what is verified, partly verified or still unknown.

- Review identity, administrator access, onboarding/offboarding, sharing, email, devices, backup and recovery ownership.
- Record evidence states instead of relying on an unsupported numeric risk score.
- Turn unknowns into practical questions for your current IT provider or internal team.

This resource is not a compliance audit, security certification, penetration test or guarantee of security. Do not enter passwords, recovery codes, secret keys or other credentials in this worksheet.

# How to use this scorecard

The purpose is to separate what your firm can actually verify from what is assumed. Work through the questions with the person responsible for Microsoft 365, security and IT support. Ask for evidence when a control or process is described as complete.

Use the scorecard as a discussion and evidence-gathering tool. It intentionally does not calculate a percentage, letter grade or compliance score.

| Verified | Partly verified | Unknown | N/A |
|---|---|---|---|
| You can point to current configuration, documentation, logs, reports or a repeatable process. | Some evidence exists, but scope, ownership or consistency is incomplete. | The firm cannot currently confirm the answer or identify reliable evidence. | The question genuinely does not apply to the current environment. |

**Suggested starting point: unknown privileged access, departed-user access, external sharing, backup/recovery responsibility and unclear administrative ownership deserve prompt clarification because they affect core access and recovery decisions.**

## Scorecard boundary

A completed worksheet describes the state of your evidence, not the probability of a cyber incident. A deeper technical review may be needed to validate configuration, licensing, recovery capability or implementation details.

# 1. Identity and sign-in evidence

Mark one evidence state for each prompt. Use the notes area on the next page or your own working paper to record the evidence location, owner and follow-up.

| Review question / evidence prompt | Verified | Partial | Unknown | N/A |
|---|---|---|---|---|
| 01 Can the firm identify which user accounts are active and who owns them? | ☐ | ☐ | ☐ | ☐ |
| 02 Can the firm show how multifactor authentication is applied to users and administrators where appropriate? | ☐ | ☐ | ☐ | ☐ |
| 03 Are inactive, stale or unnecessary accounts reviewed and addressed through a repeatable process? | ☐ | ☐ | ☐ | ☐ |
| 04 Can the firm identify guest or external identities that still have access to business resources? | ☐ | ☐ | ☐ | ☐ |
| 05 Is there a documented process for urgent access revocation when an account is compromised or a person leaves? | ☐ | ☐ | ☐ | ☐ |
| 06 Can the firm identify how access decisions are documented when a person changes role or responsibilities? | ☐ | ☐ | ☐ | ☐ |

# 2. Administrator access and privileged roles

Mark one evidence state for each prompt. Use the notes area on the next page or your own working paper to record the evidence location, owner and follow-up.

| Review question / evidence prompt | Verified | Partial | Unknown | N/A |
|---|---|---|---|---|
| 01 Can the firm identify every account with privileged Microsoft 365 or Microsoft Entra administrator access? | ☐ | ☐ | ☐ | ☐ |
| 02 Is each privileged role assigned for a clear business or administrative reason rather than convenience? | ☐ | ☐ | ☐ | ☐ |
| 03 Can the firm show that broad administrator access is limited when a narrower role can perform the task? | ☐ | ☐ | ☐ | ☐ |
| 04 Are privileged accounts reviewed periodically so old assignments do not remain indefinitely? | ☐ | ☐ | ☐ | ☐ |
| 05 Is responsibility for emergency administrative access documented and controlled? | ☐ | ☐ | ☐ | ☐ |
| 06 Can the firm identify who reviews administrator sign-in or audit activity when investigation is required? | ☐ | ☐ | ☐ | ☐ |

# 3. Onboarding, role changes and offboarding

Mark one evidence state for each prompt. Use the notes area on the next page or your own working paper to record the evidence location, owner and follow-up.

| Review question / evidence prompt | Verified | Partial | Unknown | N/A |
|---|---|---|---|---|
| 01 Is there a repeatable onboarding checklist covering account creation, access, devices and required applications? | ☐ | ☐ | ☐ | ☐ |
| 02 When a person changes role, is old access reviewed instead of only adding new access? | ☐ | ☐ | ☐ | ☐ |
| 03 Is there a repeatable departure process with a named owner and timing expectations? | ☐ | ☐ | ☐ | ☐ |
| 04 Can the firm show that departed-user sign-in access is disabled and sessions/access are addressed as appropriate? | ☐ | ☐ | ☐ | ☐ |
| 05 Are group, application, shared-mailbox and external-service permissions reviewed during offboarding? | ☐ | ☐ | ☐ | ☐ |
| 06 Is ownership of the departed person’s business data, mailbox or shared files reassigned when needed? | ☐ | ☐ | ☐ | ☐ |

# 4. Sharing, collaboration and email

Mark one evidence state for each prompt. Use the notes area on the next page or your own working paper to record the evidence location, owner and follow-up.

| Review question / evidence prompt | Verified | Partial | Unknown | N/A |
|---|---|---|---|---|
| 01 Can the firm identify where external sharing is allowed across Microsoft 365 collaboration services? | ☐ | ☐ | ☐ | ☐ |
| 02 Are guest and external sharing settings reviewed against how the firm actually collaborates with clients and third parties? | ☐ | ☐ | ☐ | ☐ |
| 03 Can the firm identify unusually broad links, sharing permissions or guest access that should be reviewed? | ☐ | ☐ | ☐ | ☐ |
| 04 Is there a process for reviewing mailbox forwarding or other email configuration when misuse is suspected? | ☐ | ☐ | ☐ | ☐ |
| 05 Can the firm identify who owns email-security configuration and incident escalation? | ☐ | ☐ | ☐ | ☐ |
| 06 Are staff told how to report suspicious sign-ins, phishing or unusual access requests? | ☐ | ☐ | ☐ | ☐ |

# 5. Devices, backup and recovery responsibility

Mark one evidence state for each prompt. Use the notes area on the next page or your own working paper to record the evidence location, owner and follow-up.

| Review question / evidence prompt | Verified | Partial | Unknown | N/A |
|---|---|---|---|---|
| 01 Can the firm identify which business devices are managed and who is responsible for their security configuration? | ☐ | ☐ | ☐ | ☐ |
| 02 Is there a clear process for removing or securing access when a device is lost, replaced or reassigned? | ☐ | ☐ | ☐ | ☐ |
| 03 Can the firm state which Microsoft 365 data is covered by its backup/recovery approach and which data is not? | ☐ | ☐ | ☐ | ☐ |
| 04 Can the firm identify who monitors backup jobs or recovery readiness? | ☐ | ☐ | ☐ | ☐ |
| 05 Has the firm seen recent evidence that important data can be restored using its current recovery approach? | ☐ | ☐ | ☐ | ☐ |
| 06 Are recovery responsibilities documented for Microsoft 365, local systems and third-party services rather than assumed? | ☐ | ☐ | ☐ | ☐ |

# 6. Ownership, documentation and incident readiness

Mark one evidence state for each prompt. Use the notes area on the next page or your own working paper to record the evidence location, owner and follow-up.

| Review question / evidence prompt | Verified | Partial | Unknown | N/A |
|---|---|---|---|---|
| 01 Is there a current list of the people or providers responsible for Microsoft 365 administration, security and recovery? | ☐ | ☐ | ☐ | ☐ |
| 02 Can leadership identify where important IT documentation is stored and who can access it during an incident? | ☐ | ☐ | ☐ | ☐ |
| 03 Are changes to critical access or security settings traceable through appropriate administrative records? | ☐ | ☐ | ☐ | ☐ |
| 04 Does the firm know who to contact first for a suspected account compromise, data-loss event or service outage? | ☐ | ☐ | ☐ | ☐ |
| 05 Can leadership distinguish what the internal team owns from what the IT provider, Microsoft or another vendor owns? | ☐ | ☐ | ☐ | ☐ |
| 06 Are unresolved security or recovery questions tracked to a named owner and next action? | ☐ | ☐ | ☐ | ☐ |

# Questions to ask your current IT provider or internal team

Use these questions to turn an “Unknown” into a verifiable next step. Ask for the evidence that supports the answer; avoid requesting passwords or secrets.

| Question | Evidence / owner / follow-up |
|---|---|
| Who has privileged Microsoft 365 or Microsoft Entra access today? | |
| What happens to access when an employee or contractor leaves? | |
| How do we review external sharing and guest access? | |
| What evidence can you show that our recovery process works for the data we consider critical? | |
| Where is our current Microsoft 365 / IT administration documentation stored? | |
| Who owns incident escalation if we suspect account compromise or data loss? | |

## Priority action worksheet

| Priority | What needs evidence or change? | Owner | Target date |
|---|---|---|---|
| Now | | | |
| Now | | | |
| Next | | | |
| Next | | | |
| Later | | | |

# What this scorecard does - and does not - tell you

It helps you: organize leadership questions, identify missing evidence, clarify ownership and prepare for a more detailed Microsoft 365 or IT review.

It does not: certify compliance, prove that an environment is secure, replace a technical security assessment, determine whether a particular Microsoft license includes a feature, or guarantee recovery.

## Reference notes reviewed August 17, 2026

Microsoft documents least-privilege principles for administrator roles, guidance for revoking user access, and the settings that influence Microsoft 365 guest sharing. These sources are useful technical references; this Scallex scorecard remains a business self-review rather than a substitute for Microsoft documentation.

Microsoft Learn - Best practices for Microsoft Entra roles
Microsoft Learn - Revoke user access in Microsoft Entra ID
Microsoft Learn - Microsoft 365 guest sharing settings reference

## Turn the unknowns into a practical IT review

If this worksheet reveals unclear access, recovery or ownership questions, the canonical next step is the Scallex Free IT Assessment. The assessment is separate from this worksheet and is intended to review the broader business IT context behind the unknowns you identified.

Start the Free IT Assessment at scallex.ca