WESTERN EDGE
TECHNOLOGIES

12 MICROSOFT 365 AND ENTRA EXPOSURES ORGANIZATIONS MISS

A practical field guide for leaders who need clear priorities - not another scanner export.

FIELD GUIDE 01

Identity | Email | Privilege | Evidence | Recovery

READ THIS FIRST

Configuration is not the same as assurance.

Microsoft 365 and Entra provide strong controls, but the practical outcome depends on licensing, scope, exclusions, operating discipline, and whether anyone reviews the evidence. This guide helps leaders ask better questions before a configuration gap becomes an incident lesson.

IDENTITY	EMAIL	EVIDENCE
MFA coverage	Authentication	Audit retention
Conditional Access	Forwarding	Alerts
Emergency access	Anti-phishing	Guest reviews
Privilege	OAuth access	Recovery tests

Use the guide as a discussion tool, not a compliance attestation. Each exposure should be verified in the tenant and interpreted in the context of business operations, licensing, regulatory requirements, and risk tolerance.

No configuration should be changed without an approved plan, tested exclusions, rollback steps, and an understanding of user impact.

EXPOSURE MAP

Twelve questions worth asking now.

A red flag is not proof of compromise. It is a reason to verify scope, evidence, and ownership.

#	AREA	LEADERSHIP QUESTION
01	MFA coverage	Are all users and privileged identities protected by appropriate authentication strengths?
02	Conditional Access	Do policies cover every relevant user, workload, app, and authentication path?
03	Emergency access	Can the organization regain control without creating a permanent bypass?
04	Privileged roles	Are standing privileges minimized, reviewed, and separately administered?
05	Legacy authentication	Are older protocols and clients creating alternate sign-in paths?
06	OAuth consent	Which applications can access tenant data, and who approved them?
07	Guest lifecycle	Do external identities still have a legitimate business need?
08	Email authentication	Do SPF, DKIM, and DMARC work together for every sending domain?
09	External forwarding	Can mailbox rules silently move business data outside the tenant?
10	Audit evidence	Is auditing enabled, retained long enough, and actually reviewed?
11	Alert ownership	Who receives identity, email, endpoint, and data protection alerts?
12	Recovery proof	Can identity, data, and administrative access be restored under pressure?

IDENTITY

Strong authentication fails when coverage has holes.

01

MFA coverage is assumed, not proven

Enrollment is not enforcement - and not every MFA method offers the same resistance to phishing.

Administrative roles, service identities, guests, legacy clients, and excluded groups can leave gaps that dashboards obscure.

Verify: Review authentication methods, Conditional Access coverage, sign-in logs, exclusions, and workload identities.

First move: Prioritize phishing-resistant methods for privileged and high-risk use cases; phase changes with user readiness.

Source: Microsoft Learn: Phishing-resistant MFA [1]

02

Conditional Access scope drifts

A policy can exist, look sensible, and still miss a user, application, platform, client, or emergency scenario.

Overlapping policies and broad exclusions often create behavior no single policy owner intended.

Verify: Use report-only analysis, What If testing, sign-in logs, policy coverage, exclusions, and change history.

First move: Document the intended control model before editing individual policies.

Source: Microsoft Learn: Conditional Access overview and deployment plan [2-3]

ADMINISTRATIVE RESILIENCE

The accounts that save the tenant can also sink it.

03

Emergency access is missing or unusable

Break-glass access should survive federation, device, policy, and personnel failures without becoming an everyday bypass.

An account that is untested, dependent on the failed system, or caught by the wrong policy is not emergency access.

Verify: Confirm at least two cloud-only accounts, protected credentials, alerting, exclusions, storage, and quarterly validation.

First move: Test with an approved procedure and record evidence without weakening the control.

Source: Microsoft Learn: Manage emergency access admin accounts [4]

04

Privilege becomes permanent

Standing Global Administrator access expands both attack surface and blast radius.

Role accumulation, shared admin identities, and daily productivity from privileged accounts make compromise more consequential.

Verify: Inventory role assignments, eligible versus active access, admin workstations, separate identities, and review cadence.

First move: Reduce standing access and establish role-specific, time-bound administration where licensing and operations support it.

Source: Microsoft Learn: Plan access reviews and PIM deployment [5]

ALTERNATE PATHS

Attackers use the path your standard did not cover.

05

Legacy authentication remains reachable

Older authentication protocols can bypass controls designed for modern sign-in flows.

One forgotten client, device, or exception can preserve an alternate path after the main user population is protected.

Verify: Review sign-in logs for legacy client types, service dependencies, exclusions, and blocked attempts.

First move: Identify dependencies, replace them, then block legacy authentication with staged validation.

Source: Microsoft Learn: Conditional Access deployment guidance [3]

06

OAuth consent is treated as harmless

A user can authorize an application to access data even when the application never receives the user's password.

Consent phishing and excessive permissions can create durable access that survives password changes.

Verify: Review enterprise applications, consent grants, publishers, permissions, sign-in activity, owners, and unused apps.

First move: Restrict user consent appropriately and establish an admin consent and app-review workflow.

Source: Microsoft Learn: Manage app consent and protect against consent phishing [6-7]

COLLABORATION AND EMAIL

Convenience controls deserve the same scrutiny as identity.

07

Guest access has no end date

External collaboration often outlives the project, vendor, or employee who created it.

Guests can remain in groups, Teams, applications, and SharePoint sites after business ownership disappears.

Verify: Review guest age, sponsors, group and app assignments, last activity, sensitive sites, and recurring access reviews.

First move: Assign accountable owners and remove access that no longer has a documented business purpose.

Source: Microsoft Learn: Guest access reviews [8]

08

SPF is mistaken for complete email authentication

SPF, DKIM, and DMARC work together; one record alone does not protect the visible From domain.

Unaligned domains, forgotten senders, and weak DMARC policy can leave the brand open to spoofing or disrupt legitimate mail when tightened carelessly.

Verify: Inventory every authorized sender and validate SPF, DKIM signing, DMARC alignment, reports, and unused domains.

First move: Move toward enforcement only after legitimate senders and failure patterns are understood.

Source: Microsoft Learn: Email authentication in Microsoft 365 [9]

EXFILTRATION AND EVIDENCE

A control you cannot observe is difficult to trust.

09

External forwarding becomes a quiet exit

Inbox rules and mailbox forwarding can move sensitive messages outside the organization.

Forwarding may be intentional, inherited, or created after account compromise.

Verify: Review outbound spam policy, remote domains, mailbox forwarding, inbox rules, forwarded-message reports, and exceptions.

First move: Disable external forwarding by default and document narrow, monitored exceptions.

Source: Microsoft Learn: Control automatic external forwarding [10]

10

Audit logging is present but not operational

Logs help only when ingestion is enabled, retention matches the need, permissions work, and someone knows how to search them.

SMB licensing, retention assumptions, and missing procedures can reduce evidence exactly when the organization needs it.

Verify: Verify audit status, retention, licensing, alert integrations, search permissions, test events, and export requirements.

First move: Run a test investigation and record the time required to answer basic identity, mailbox, file, and admin questions.

Source: Microsoft Learn: Audit search and enablement [11-12]

OPERATIONS AND RECOVERY

Licenses do not assign ownership or prove recovery.

11

Alerts do not have an accountable owner

Identity, email, endpoint, and data alerts can exist without a person responsible for triage and escalation.

Default recipients, departed administrators, noisy queues, and unclear severity rules turn detection into decoration.

Verify: Map each alert source to recipients, response expectations, escalation paths, after-hours limits, and evidence of closure.

First move: Test one alert from each critical control family and measure whether it reaches the right person with enough context.

Source: CISA and Microsoft 365 security guidance [13]

12

Recovery is described, not demonstrated

Retention, recycle bins, platform availability, and backup are different capabilities with different failure boundaries.

Organizations often discover identity, encryption key, SaaS data, device, or administrative dependencies only during an incident.

Verify: Document recovery objectives, protected data, administrative access, identity dependencies, restore authority, test results, and vendor responsibilities.

First move: Run a tabletop and a limited restore test; record gaps, owners, and target dates.

Source: NIST Cybersecurity Framework 2.0 - Recover function [14]

A PRACTICAL REVIEW

Turn twelve questions into a thirty-day plan.

DAYS 1-5	**Establish facts**	Read-only discovery, licensing, tenant structure, admin roles, policy inventory, mail flow, audit status, and recovery ownership.
DAYS 6-12	**Test coverage**	Sign-in analysis, Conditional Access What If tests, emergency account validation, guest and app review, forwarding and sender inventory.
DAYS 13-20	**Prioritize risk**	Rank findings by likelihood, impact, effort, user disruption, dependencies, and regulatory or insurer relevance.
DAYS 21-30	**Change safely**	Approve owners, communications, pilot groups, rollback steps, monitoring, and evidence before enforcement.

A useful finding states the observed condition, supporting evidence, affected scope, plausible business impact, recommended action, dependency, owner, and verification method.

Avoid the two common extremes: changing controls immediately without understanding operations, or producing a long report with no accountable next step.

A SENSIBLE FIRST ENGAGEMENT

Get an experienced second opinion before the next major change.

SECURITY ARCHITECTURE SECOND OPINION	MICROSOFT 365 / ENTRA EXPOSURE REVIEW
A focused 90-minute working session for one design, migration, vendor proposal, incident lesson, or architecture decision. Suggested starting fee: $750	A fixed-scope review of identity, privilege, email, external access, evidence, and recovery, followed by an executive summary and prioritized roadmap. Suggested starting fee: $2,500

Western Edge brings deep Microsoft experience and broader security architecture judgment. The goal is not to sell a platform or replace your IT provider. It is to establish facts, explain risk in business terms, and produce a usable plan.

Start at westernedgetech.com or email sales@westernedgetech.com

REFERENCES

Primary guidance used in this field guide.

[1] Phishing-resistant MFA
https://learn.microsoft.com/en-us/security/zero-trust/sfi/phishing-resistant-mfa

[2] Conditional Access overview
https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview

[3] Plan a Conditional Access deployment
https://learn.microsoft.com/en-us/entra/identity/conditional-access/plan-conditional-access

[4] Manage emergency access admin accounts
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-emergency-access

[5] Plan access reviews
https://learn.microsoft.com/en-us/entra/id-governance/deploy-access-reviews

[6] Manage app consent policies
https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/manage-app-consent-policies

[7] Protect against consent phishing
https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/protect-against-consent-phishing

[8] Manage guest access with access reviews
https://learn.microsoft.com/en-us/entra/id-governance/manage-guest-access-with-access-reviews

[9] Email authentication in Microsoft 365
https://learn.microsoft.com/en-us/defender-office-365/email-authentication-about

[10] Control automatic external forwarding
https://learn.microsoft.com/en-us/defender-office-365/outbound-spam-policies-external-email-forwarding

[11] Search the Microsoft Purview audit log
https://learn.microsoft.com/en-us/purview/audit-search

[12] Turn auditing on or off
https://learn.microsoft.com/en-us/purview/audit-log-enable-disable

[13] CISA Microsoft 365 minimum viable secure configuration baselines
https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project

[14] NIST Cybersecurity Framework 2.0
https://www.nist.gov/cyberframework