M365 Instant Audit

Cloud audit report for **Sample Organization**

Audit ID: cs_sample_showcase_001 · 2026-06-14 15:22 UTC · v1.0

by WINTIVE LLC
Microsoft Verified Publisher
nicolas@wintive.com
https://www.wintive.com

Executive summary

36/100

At risk

14 passed · **35** to fix · **49** live checks of 50 declared

At risk	Needs work	Fair	Good	Excellent
0–39	40–59	60–74	75–89	90–100

Security score 0–100, weighted by finding severity — your **36** is in the **At risk** band.

Cost savings opportunity

$2,358 **estimated annual license waste identified** — $2,358 potential after review. Full breakdown in License cost control below.

Findings by severity

SEVERITY	FAILURES	RECOMMENDED ACTION
CRITICAL	4	Address within 24 hours
HIGH	15	Address within 1 week
MEDIUM	11	Address within 1 month
LOW	5	Backlog / next review

What each status means

Every check in the detailed sections below carries one of these verdicts:

PASS FAIL WARNING N/A ERROR

Top 5 findings to fix this week

1. CRITICAL #01 **Security Defaults OR Conditional Access enabled**
2. CRITICAL #02 **Legacy authentication blocked**
3. CRITICAL #36 **Device compliance enforced via Conditional Access**
4. CRITICAL #37 **Disk encryption required (BitLocker / FileVault)**
5. HIGH #03 **Break-glass (emergency) account exists**

Licensing posture

Your tenant currently holds:

- **Microsoft 365 Business Premium (EU, no Teams)** — 15 seats
- **Microsoft Teams (EEA add-on)** — 15 seats
- **FLOW_FREE (unmapped)** — 4 seats

Licensing coverage of the findings to fix:

27 ✅ fixable immediately with current licensing

2 🚫 require a licensing upgrade

Recommended upgrade path: adding **Microsoft 365 E5** would unlock 2 of the 2 licensing-blocked findings.

Estimated annual savings (realizable at renewal — or mid-term on a flexible agreement)

60% of your current Microsoft 365 licence spend ($3,960/yr) is recoverable — **$2,358/yr identified**

None

Immediate — cancellable at renewal (unassigned + redundant)

$2,358

Potential after review (inactive, downgrades, bundling)

Line	SKU	Seats	Annual subtotal
Over-licensed right-sizing	Microsoft 365 Business Premium (EU, no Teams)	10	$1,830
Inactive accounts	Microsoft 365 Business Premium (EU, no Teams)	2	$528
Total identified annual waste			**$2,358**

Realizing these savings. When you can act depends on your purchase agreement. Under a flexible vehicle (MOSA) you can downgrade or cancel mid-term with a prorated refund from Microsoft; under MCA or CSP-NCE annual you are committed until renewal (a 7-day window aside). To keep the ability to right-size and be refunded mid-term, consider purchasing via MOSA rather than MCA — subject to current Microsoft availability.

From 2026-07-01, Microsoft's new list prices narrow the right-sizing gap — your identified waste becomes $2,292/yr (Business Premium holds while the lower tiers move).

Estimates based on current Microsoft 365 US list prices (annual commitment), as of 2026-06-09. Actual savings depend on your agreement, commitment type and CSP discounts. These are advisory findings, not instructions: validate every change with your IT provider or MSP before acting. The recommended actions (convert to a shared mailbox, right-size, disable) are reversible and preserve data — do NOT delete accounts to capture savings, as that can permanently lose mailboxes/files and stop mail.

Contents

1. Entra ID & Identity

Checks #01–#16 · 16 total

#01 Security Defaults OR Conditional Access enabled

CRITICAL FAIL

Neither Security Defaults nor any active Conditional Access policy is in place. The tenant has NO baseline protection — credential-stuffing, password spraying, and legacy-protocol attacks are unimpeded.

```
Entra admin center → Identity → Overview → Properties → Manage security defaults
→ enable. For E3/Business Premium, prefer a Conditional Access policy requiring
MFA for all users on all cloud apps.
```

✅ **Licensing:** Security Defaults free for any tenant; Conditional Access requires Entra ID P1 (included in Business Premium / E3+).

[See evidence]

#02 Legacy authentication blocked

CRITICAL FAIL

No Conditional Access policy blocks legacy authentication protocols (POP, IMAP, SMTP AUTH, ActiveSync basic auth). Legacy auth bypasses MFA and accounts for the vast majority of password-spray compromises.

```
Entra admin center → Protection → Conditional Access → New policy. Users: All.
Cloud apps: All. Conditions → Client apps: tick 'Other clients'. Grant: Block.
Legacy protocols (SMTP AUTH, IMAP, POP3) bypass MFA entirely without this gate.
```

POWERSHELL ALTERNATIVE

```
# Audit existing CA policies that target legacy clients (Connect-MgGraph -Scopes
Policy.Read.All):
Get-MgIdentityConditionalAccessPolicy | Where { $_.Conditions.ClientAppTypes -contains
'other' } | Select DisplayName, State
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#03 Break-glass (emergency) account exists

HIGH FAIL

No Global Admin account matches a break-glass naming convention (breakglass / emergency / bg-* / ba-*). If your only admin loses MFA or is locked out, you have NO recovery path.

```
Create 1-2 cloud-only Global Admin accounts (breakglass-1, breakglass-2) with 64+
char passwords stored in a physical safe. Exclude from all Conditional Access
policies. Without break-glass, an MFA outage locks you out of your own tenant.
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#04 MFA enforced for all administrators

CRITICAL PASS

Configuration valid — no action required.

#05 Self-service password reset enabled

MEDIUM PASS

Configuration valid — no action required.

#06 Risky sign-in & risky user policies enabled

HIGH FAIL

No Conditional Access policy reacts to Identity Protection sign-in or user risk signals. Risky sign-ins (impossible travel, leaked credentials, anonymous IP) are detected but trigger nothing.

```
Entra admin center → Protection → Conditional Access → Templates: enable 'Require MFA for high sign-in risk' AND 'Require password change for high user risk'. Identity Protection signals (impossible travel, leaked credentials) trigger nothing without these policies.
```

🚫 **Licensing:** Requires Entra ID P2 (in Microsoft 365 E5 or Entra ID P2 add-on).

[See evidence]

#07 Privileged Identity Management configured

HIGH N/A

Just-in-time admin access (Privileged Identity Management) requires Microsoft Entra ID P2. Note: Microsoft 365 Business Premium includes Entra ID P1, NOT P2 — they're different tiers — so PIM isn't available on this licence (Graph confirms: AadPremiumLicenseRequired). Without it, every admin role is a permanent standing assignment, so a single compromised admin credential is privileged 100% of the time.

```
P2 (and PIM) ship with Microsoft 365 E5, or as a standalone Entra ID P2 add-on
(~$9/user/month — admin seats only). Until then, keep standing admins to the
strict minimum: 2 break-glass Global Admins, least-privilege roles for everyone
else, MFA enforced on all of them.
```

🚫 **Licensing:** Requires Entra ID P2 (in Microsoft 365 E5 or as standalone add-on).

[See evidence]

#08 Guest user settings locked down

MEDIUM FAIL

Anyone in the directory (including guests) can invite further guests. This is the default tenant setting and the most permissive option — a single compromised guest account can fan out unchecked.

```
Entra admin center → External Identities → External collaboration settings: set
'Guest user access' to 'limited access' and require admin approval for invites.
Default settings let any user invite externals who can then read directory
metadata.
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#09 Admin consent workflow enabled

MEDIUM FAIL

Admin consent workflow is disabled. Users hitting an app that requires admin consent get a dead-end error and have no in-product way to request approval — they typically end up emailing IT or, worse, abandoning legitimate apps.

```
Entra admin center → Roles & admins → Global administrator: audit assignments and remove any not actively needed. Aim for ≤5 standing Global Admins; more = wider blast radius on a single compromise.
```

POWERSHELL ALTERNATIVE

```
# Count Global Admin assignments (Connect-MgGraph -Scopes RoleManagement.Read.Directory):
$ga = Get-MgDirectoryRole -Filter "displayName eq 'Global Administrator'"
(Get-MgDirectoryRoleMember -DirectoryRoleId $ga.Id).Count
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#10 Password protection (banned words list)

LOW FAIL

No custom 'Password Rule Settings' is configured. Microsoft's default global banned-passwords list applies but you cannot ban your own brand names or local-language guesses (e.g. '[client]2025!').

```
Entra admin center → Conditional Access → Policies: review every active policy for stale user exclusions, overlapping rules, and 'report-only' modes never promoted. Each unused exclusion is a permanent bypass; consolidate or retire policies quarterly.
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#11 Global Administrator count within 2-4

HIGH PASS

Configuration valid — no action required.

#12 MFA registration coverage across all users

HIGH FAIL

Only 44% of users are MFA-capable (7/16) — most accounts are password-only and trivially phishable.

```
Run an MFA registration campaign and enforce MFA for all users via a Conditional Access policy.
```

✅ **Licensing:** No licensing requirement defined for this check.

[See evidence]

#13 Guest invitations restricted to admins

MEDIUM FAIL

Any member can invite external guests (allowInvitesFrom = 'everyone') — uncontrolled external access to Teams, SharePoint and files.

```
Entra → External collaboration settings → restrict guest invites to administrators and designated guest inviters.
```

✅ **Licensing:** No licensing requirement defined for this check.

[See evidence]

#14 User app registration and consent restricted

MEDIUM FAIL

Standard (non-admin) users can register applications, widening the consent-phishing and rogue-app surface.

```
Entra → Users → User settings → set 'Users can register applications' to No;
review app-consent settings so users can't consent to risky scopes.
```

✅ **Licensing:** No licensing requirement defined for this check.

[See evidence]

#15 No over-privileged OAuth consent grants

HIGH FAIL

14 OAuth grant(s) carry high-impact scopes (mailbox/file/directory write); 11 are consented tenant-wide. A compromised or rogue app with these scopes can read/exfiltrate broadly.

```
Entra → Enterprise applications → Permissions → review each grant; revoke unused
broad scopes and restrict user consent to verified publishers + low-impact scopes
only.
```

✅ **Licensing:** No licensing requirement defined for this check.

[See evidence]

#16 Phishable authentication methods (SMS/Voice) disabled

MEDIUM PASS

Configuration valid — no action required.

2. Exchange Online & Mail Flow

Checks #17–#24 · 8 total

#17 SPF record present and strict

HIGH PASS

Configuration valid — no action required.

#18 DKIM signing enabled per accepted domain

HIGH FAIL

13 domain(s) have NO DKIM selector published ([client].com, client-64fd.example, client-e610.example). Outbound mail from these domains is unsigned, making spoofing trivial and reducing inbox delivery rates.

```
Defender → Email & collaboration → Threat policies → DKIM: enable signing for each accepted domain, then publish the two selector1/selector2 CNAME records at your DNS. Validate: dig +short CNAME selector1._domainkey.yourdomain.com.
```

POWERSHELL ALTERNATIVE

```
# Connect-ExchangeOnline first. Run per verified sending domain:
Set-DkimSigningConfig -Identity yourdomain.com -Enabled $true
Get-DkimSigningConfig | Select Domain, Enabled, Selector1CNAME, Selector2CNAME
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#19 DMARC record published (p=quarantine or p=reject)

HIGH WARNING

DMARC is in monitoring mode (p=none). Receivers will not reject spoofed mail; you only get aggregate reports.

Improvement: Add a TXT record at _dmarc.yourdomain.com: v=DMARC1; p=quarantine; rua=mailto:dmarc@yourdomain.com; pct=100. Start with quarantine, monitor rua reports 2-4 weeks, then tighten to p=reject. Validate: dig +short TXT _dmarc.yourdomain.com.

POWERSHELL ALTERNATIVE

```
# Validate DMARC TXT after publishing (no Connect-* required, native PS):
Resolve-DnsName -Type TXT -Name "_dmarc.yourdomain.com" | Select Strings
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#20 Anti-phishing policy with impersonation protection

HIGH PASS

Configuration valid — no action required.

#21 Safe Attachments and Safe Links enabled

HIGH PASS

Configuration valid — no action required.

#22 Outbound spam policy limits configured

MEDIUM PASS

Configuration valid — no action required.

#23 Mailbox auditing enabled

MEDIUM PASS

Configuration valid — no action required.

#24 Auto-forwarding to external blocked

HIGH FAIL

External auto-forwarding is allowed — a common data-exfiltration path after account compromise.

```
Exchange admin center → Mail flow → Remote domains → Default: set 'Allow
automatic forwarding' to false. Validate via PowerShell (alternative below).
Compromised mailboxes routinely set forwarding rules to exfiltrate mail.
```

POWERSHELL ALTERNATIVE

```
# Block external auto-forwarding tenant-wide (Connect-ExchangeOnline first):
Set-RemoteDomain -Identity Default -AutoForwardEnabled $false
Get-RemoteDomain Default | Select Name, AutoForwardEnabled
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

3. SharePoint & OneDrive

Checks #25–#29 · 5 total

#25 External sharing restricted at tenant level

HIGH FAIL

Tenant allows ANYONE links (anonymous, no sign-in). Any leaked URL exposes the file to the internet.

```
SharePoint admin center → Policies → Sharing. Under 'External sharing — SharePoint', move the slider to 'New and existing guests' (default safe) or stricter. Anyone-with-the-link surfaces tenant content to crawlers and ex-employees.
```

POWERSHELL ALTERNATIVE

```
# Tighten tenant-wide sharing in one line (Connect-SPOService -Url https://-admin.sharepoint.com first):
Set-SPOTenant -SharingCapability ExistingExternalUserSharingOnly
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#26 Anonymous link expiration enforced

MEDIUM FAIL

Anonymous links never expire. A URL leaked once stays live forever; rotation of access is impossible without revoking each link manually.

```
SharePoint admin center → Policies → Sharing: enable 'Notify owners when files / folders are shared'. Plus enable tenant-wide audit log. Without alerts, a phished user inviting an attacker as a guest goes unnoticed for weeks.
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#27 Sensitivity labels deployed

LOW FAIL

No sensitivity labels are published. Files cannot be auto-classified or encrypted at the data layer; access enforcement falls entirely on permissions. (Note: authoring/publishing labels requires Microsoft 365 E5 or the Compliance E5 add-on.)

```
Microsoft Purview → Information protection → Labels: publish a 'Public / Internal / Confidential' label set with auto-labelling on sensitive patterns (credit cards, NHS numbers). Without labels, DLP and encryption are blind to data classification.
```

🚫 **Licensing:** Requires Microsoft 365 E5 or AIP P1 (in EMS E3+) / P2 (in EMS E5).

[See evidence]

#28 OneDrive retention for ex-employees

HIGH FAIL

Ex-employee OneDrives are kept for only 30 day(s) (Microsoft default = 30). If a manager realises a departing employee owned key files later, recovery may already be impossible.

```
SharePoint admin center → Policies → Sharing → Anyone-link defaults: expiration 30 days max, permissions View only. Permanent Anyone-links are a slow-motion data leak as documents drift via forwards.
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#29 Site creation restricted to admins

LOW FAIL

Any user can create SharePoint sites. Tenants with ≥50 users typically grow to hundreds of orphaned sites within 12 months, each with its own permissions to audit.

```
Purview → Data lifecycle management → Retention policies → New: scope OneDrive, retain 7 years (or per legal). Without retention, ex-employee OneDrives are wiped 30 days post-licence-removal — common cause of lost compliance evidence.
```

POWERSHELL ALTERNATIVE

```
# Create a 7-year OneDrive retention policy (Connect-IPPSSession first):
New-RetentionCompliancePolicy -Name "OneDrive 7y retention" -OneDriveLocation All
New-RetentionComplianceRule -Policy "OneDrive 7y retention" -RetentionDuration 2555 -RetentionComplianceAction Keep
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

4. Microsoft Teams

Checks #30–#35 · 6 total

#30 Guest access in Teams reviewed

MEDIUM WARNING

Guest access in Teams is enabled. Legitimate for external collaboration, but every guest is a standing access path that needs governance.

Improvement: Teams admin center → Users → External access: shift 'Choose which external domains your users have access to' to 'Allow only specific external domains' and explicitly allow only known partners. Default is open to every M365 tenant globally.

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#31 External communications policy configured

MEDIUM WARNING

External communication is open via: federation with external domains, personal (consumer) Teams accounts. Open federation widens the phishing/impersonation surface.

Improvement: Teams admin center → Meetings → Meeting policies → Global → 'Anonymous users can join a meeting': set to Off (or 'Anyone in your org and trusted orgs'). Anonymous join with no PIN is a vector for meeting-bombing and credential phishing.

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#32 Meeting lobby for external participants

HIGH FAIL

Anyone can bypass the lobby (AutoAdmittedUsers='Everyone') — external and anonymous participants join meetings unannounced.

```
Teams admin center → Teams apps → Permission policies → Global: block third-party and custom apps tenant-wide; allow Microsoft only. Add per-group exceptions where needed. Default open exposes your tenant to supply-chain attacks via Teams app store.
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#33 Recording policies restricted

MEDIUM WARNING

Cloud recording is enabled tenant-wide. Best practice is off by default; confirm recordings are governed (retention, access, consent).

Improvement: Teams admin center → Org-wide settings → Files: align with the SharePoint external sharing policy from #21. Teams files inherit SharePoint policies — mismatch creates a silent leakage path no one audits.

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#34 Third-party application registrations reviewed

HIGH FAIL

19 application(s) registered in this tenant — well past the 5-app threshold for casual review. Each is a potential consent-phishing target.

```
Teams admin center → Meetings → Meeting policies: under 'Recording & transcription', set 'Cloud recording' to On and 'Transcription' to On. Define retention via Purview retention policy (e.g. 90 days). Recordings are evidence in HR / IP disputes.
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#35 Anonymous join disabled for confidential meetings

LOW WARNING

Anonymous users can join meetings. Acceptable for public webinars but a leak risk for confidential meetings.

Improvement: Teams admin center → Live events policies → Global: set 'Allow scheduling' to specific groups only. Set 'Recording for attendees' to 'Disabled'. Live events broadcast to thousands; a misconfigured one leaks broadcasts publicly.

✅ **Licensing:** Covered by your current licensing.

[See evidence]

5. Intune & Device Management

Checks #36–#43 · 8 total

#36 Device compliance enforced via Conditional Access

CRITICAL FAIL

No Conditional Access policy enforces device compliance. Compliance policies configured in Intune have no teeth — non-compliant devices can still access company resources.

```
Pair an Intune compliance policy (Endpoint Manager → Devices → Compliance policies) defining 'compliant' (encryption, OS version, threat level) with a Conditional Access policy: Users All / Cloud apps All / Grant: Require device to be marked as compliant.
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#37 Disk encryption required (BitLocker / FileVault)

CRITICAL FAIL

No Windows or macOS device compliance policies are defined. Intune is licensed but the encryption baseline is not enforced — non-encrypted laptops can enrol and stay 'compliant'.

```
Endpoint Manager → Devices → Compliance policies: create per-platform policy requiring BitLocker (Windows) / FileVault (macOS) + minimum OS version. Pair with #32 CA. Unencrypted stolen laptops = full data breach + GDPR notification.
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#38 Minimum OS version enforced

HIGH FAIL

1 of 1 compliance policy/policies do not enforce a minimum OS version. Devices on EOL operating systems can enrol and stay 'compliant'.

```
Endpoint Manager → Devices → Compliance policies: ensure one per supported
platform (Windows, macOS, iOS, Android). Without per-platform policy,
compliant=true is granted by default for that platform — Conditional Access #32
has no teeth there.
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#39 Microsoft Defender for Endpoint deployed

HIGH FAIL

No device configuration profile references Microsoft Defender or Endpoint Protection. EDR coverage is unconfirmed — devices may be relying on built-in Defender AV without the cloud-attached protection layer.

```
Endpoint Manager → Endpoint security → Antivirus: create a 'Microsoft Defender
Antivirus' profile assigned to all devices. Plus 'Endpoint detection and
response' with cloud-attached protection on. Built-in Defender is base AV; EDR
adds the cloud signal layer.
```

✅ **Licensing:** Either MDE_SMB (in Microsoft 365 Business Premium) OR WINDEFATP (in M365 E5 / Defender for Endpoint P1+) satisfies; pick whichever your tenant has.

[See evidence]

#40 Windows Autopilot deployment profiles configured

MEDIUM FAIL

No Windows Autopilot deployment profile is configured. New laptops require manual IT provisioning — slower onboarding + higher chance of misconfiguration.

```
Endpoint Manager → Devices → Windows enrollment: import OEM device hashes (CSV)
into Autopilot, then assign a deployment profile (user-driven, hybrid AD join, or
AAD join). Manual provisioning is error-prone and slows on/offboarding.
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#41 App Protection Policies (MAM) deployed

HIGH FAIL

No App Protection Policies are defined. On personal devices (BYOD), corporate data in Outlook mobile / Office apps can be copy-pasted, screenshotted, or saved locally without restriction.

```
Endpoint Manager → Devices → Enrollment → Device platform restrictions: block
personal-owned iOS/Android unless approved. Set per-user enrolment limit to 5.
Without limits, an attacker with creds can flood Intune with rogue devices.
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#42 Stale managed devices cleaned up (>180 days)

LOW PASS

Configuration valid — no action required.

#43 Device enrollment restrictions configured

MEDIUM FAIL

Only the built-in default enrollment configurations exist — no platform restrictions or device limits have been set. Any supported personal device can enroll and reach company data.

```
Intune admin center → Devices → Enrollment → Enrollment restrictions: set platform restrictions (block unmanaged/personal platforms) and a per-user device limit.
```

✅ **Licensing:** No licensing requirement defined for this check.

[See evidence]

6. License Waste & Cost Control

Checks #44–#48 · 5 total

#44 Unassigned licenses reviewed

LOW PASS

Configuration valid — no action required.

#45 Inactive accounts (no sign-in or send for 6 months)

MEDIUM WARNING

2 of 16 enabled account(s) show no activity of any kind in 180+ days — no interactive sign-in AND no non-interactive sign-in (which covers SMTP mail-send, app/service and token auth). So these are genuinely dormant, not just 'didn't open the portal': a still-sending service mailbox would have non-interactive activity and is excluded. Each is paying for a license nobody uses and is a dormant attack surface.

Improvement: Two steps, in order: 1) convert each mailbox to a shared mailbox (free ≤50 GB — keeps all data, mail still arrives); 2) then remove the paid licence. WARNING: removing the licence BEFORE converting deletes the mailbox/OneDrive after ~30 days (data loss). Confirm with your IT/MSP.

POWERSHELL ALTERNATIVE

```
# List licensed users with no sign-in for 180+ days (Connect-MgGraph -Scopes
AuditLog.Read.All,User.Read.All):
$cutoff = (Get-Date).AddDays(-180)
Get-MgUser -Filter "assignedLicenses/`$count ne 0" -ConsistencyLevel eventual -CountVariable
c -Property UserPrincipalName,SignInActivity -All | Where
{ $_.SignInActivity.LastSignInDateTime -lt $cutoff } | Select UserPrincipalName,
@{n='LastSignIn';e={$_.SignInActivity.LastSignInDateTime}}
```

Inactive account	Current licence	Last sign-in	Reclaim $/yr
[person-24e415]@[client].net	Business Premium (EU)	2025-11-05	$264
[person-576473]@[client].net	Business Premium (EU)	2025-06-18	$264
Total licence cost reclaimable (annual)			**$528/yr**

If an account must stay active, its right-size target is shown under the over-licensed right-sizing finding instead.

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#46 Mailbox size vs license tier mismatch

LOW PASS

Configuration valid — no action required.

#47 Duplicate or redundant license SKUs

LOW PASS

Configuration valid — no action required.

#48 Over-licensed users right-sizing

LOW WARNING

10 active users are paying for more than they use and could move to a cheaper plan — about $1,830/year. 2 inactive account(s) can also be right-sized if kept active rather than converted to a shared mailbox (see the inactive-accounts finding). Review before action. Each move rests on a fact, not a guess. Premium→Standard: the account has no Intune-managed device, so the security tier (what Premium adds over Standard) isn't in use — Standard keeps Office and collaboration, so nothing used is removed. Dropping further (Basic / Exchange Online) is claimed only on PROVEN web-only usage — from...

Improvement: For each user below, confirm they don't need their plan's extras (Intune/security, desktop Office, Teams/SharePoint), then move them down the ladder (Premium→Standard→Basic→Exchange Online P1) in M365 admin → Active users → Licenses, at renewal or on a flexible MOSA agreement.

Over-licensed user	Current licence	Recommended	$/yr
user-c59a53@client-64fd.example	Business Premium (EU)	Exchange Online Plan 1	$216
alert@[client].net	Business Premium (EU)	Exchange Online Plan 1	$216
bitwarden@[client].net	Business Premium (EU)	Exchange Online Plan 1	$216
user-3f1db5@client-2055.example	Business Premium (EU)	Business Standard	$114
user-adde82@client-64fd.example	Business Premium (EU)	Business Standard	$114
user-6cb756@client-2055.example	Business Premium (EU)	Exchange Online Plan 1	$216
user-f00967@client-e610.example	Business Premium (EU)	Business Standard	$114
user-8cdba8@client-2055.example	Business Premium (EU)	Exchange Online Plan 1	$216
user-597494@client-7d45.example	Business Premium (EU)	Exchange Online Plan 1	$216
user-423138@client-f971.example	Business Premium (EU)	Business Basic	$192
Dormant accounts — already counted under inactive accounts (right-size these only if you keep them active rather than convert to a shared mailbox)			
[person-24e415]@[client].net	Business Premium (EU)	Exchange Online Plan 1	$216

Over-licensed user	Current licence	Recommended	$/yr
[person-576473]@[client].net	Business Premium (EU)	Exchange Online Plan 1	$216
Active accounts (annual)			**$1,830/yr**
Dormant accounts — if kept active & right-sized			**$432/yr**
Total right-sizing — active + dormant kept (annual)			**$2,262/yr**

✅ **Licensing:** Covered by your current licensing.

[See evidence]

7. Security Posture & Audit Logs

Checks #49–#50 · 2 total

#49 Unified audit log enabled

CRITICAL PASS

Configuration valid — no action required.

#50 Microsoft Secure Score posture

HIGH FAIL

Microsoft Secure Score is only 44% (122/278) — 37 recommended controls earn zero points today.

```
Microsoft Defender portal → Secure Score → work the highest-impact
recommendations first (the unimplemented controls are listed in the evidence).
```

✅ **Licensing:** No licensing requirement defined for this check.

[See evidence]

Evidence appendix

Raw API response excerpts captured during the audit, for review by your IT team. Only checks that returned data are listed; manual-review placeholders are documented inline in their section.

#01 Security Defaults OR Conditional Access enabled [Back to summary]


```
{
  "ca_policies_enabled_count": 0,
  "ca_policies_total": 0,
  "security_defaults_enabled": false
}
```


#02 Legacy authentication blocked [Back to summary]


```
{
  "blocking_policies": []
}
```


#03 Break-glass (emergency) account exists [Back to summary]


```
{
  "break_glass_count": 0,
  "global_admin_count": 3,
  "matched": []
}
```


#04 MFA enforced for all administrators [Back to summary]


```
{
  "admin_mfa_capable": 3,
  "admin_mfa_registered": 3,
  "admin_total": 3,
  "admins_without_mfa": []
}
```

#05 Self-service password reset enabled [Back to summary]


```
{
  "configured_methods": [
    "Fido2",
    "MicrosoftAuthenticator",
    "Sms",
    "TemporaryAccessPass",
    "SoftwareOath",
    "Voice",
    "Email",
    "X509Certificate",
    "VerifiableCredentials",
    "QRCodePin"
  ],
  "enabled_non_password_methods": [
    "Fido2",
    "MicrosoftAuthenticator",
    "SoftwareOath",
    "Email"
  ]
}
```


#06 Risky sign-in & risky user policies enabled [Back to summary]


```
{
  "sign_in_risk_policies": [],
  "user_risk_policies": []
}
```


#07 Privileged Identity Management configured [Back to summary]


```
{
  "entra_p2": false,
  "http_status": 400
}
```


#08 Guest user settings locked down [Back to summary]


```
{
  "allowInvitesFrom": "everyone",
  "guestUserRoleId": "2af84b1e-32c8-42b7-82bc-daa82404023b"
}
```


#09 Admin consent workflow enabled [Back to summary]


```
{
  "isEnabled": false,
  "reviewer_count": 0
}
```

#10 Password protection (banned words list) [Back to summary]


```
{
  "setting_present": false
}
```


#11 Global Administrator count within 2-4 [Back to summary]


```
{
  "global_admin_count": 3,
  "recommended_max": 4,
  "recommended_min": 2,
  "sample": [
    {
      "displayName": "Nicolas",
      "upn": "nicolas@[client].com"
    },
    {
      "displayName": "Admin",
      "upn": "user-4248eb@client-9544.example"
    },
    {
      "displayName": "[person-5a6952]",
      "upn": "user-3f1db5@client-2055.example"
    }
  ]
}
```


#12 MFA registration coverage across all users [Back to summary]


```
{
  "admins_without_mfa": [],
  "coverage_pct": 44,
  "mfa_capable": 7,
  "users": 16
}
```


#13 Guest invitations restricted to admins [Back to summary]


```
{
  "allow_invites_from": "everyone"
}
```


#14 User app registration and consent restricted [Back to summary]


```
{
  "allowed_to_create_apps": true
}
```

#15 No over-privileged OAuth consent grants [Back to summary]


```
{
  "risky_grants": 14,
  "sample": [
    {
      "clientId": "cfc8d6ab-2e94-4bea-94a0-d55851ad61e2",
      "risky_scopes": [
        "Mail.ReadWrite"
      ],
      "tenant_wide": true
    },
    {
      "clientId": "72f14bff-bad4-4f33-b8b4-7c5204f4be5a",
      "risky_scopes": [
        "Files.ReadWrite.All",
        "Sites.FullControl.All",
        "Sites.ReadWrite.All"
      ],
      "tenant_wide": true
    },
    {
      "clientId": "72f14bff-bad4-4f33-b8b4-7c5204f4be5a",
     ...
```


#16 Phishable authentication methods (SMS/Voice) disabled [Back to summary]


```
{
  "states": {
    "Email": "enabled",
    "Fido2": "enabled",
    "MicrosoftAuthenticator": "enabled",
    "QRCodePin": "disabled",
    "Sms": "disabled",
    "SoftwareOath": "enabled",
    "TemporaryAccessPass": "disabled",
    "VerifiableCredentials": "disabled",
    "Voice": "disabled",
    "X509Certificate": "disabled"
  },
  "strong_enabled": [
    "Fido2",
    "MicrosoftAuthenticator"
  ],
  "weak_enabled": []
}
```

#17 SPF record present and strict [Back to summary]


```
{
  "domains_checked": [
    "[client].com",
    "client-64fd.example",
    "client-e610.example",
    "client-2055.example",
    "client-c14a.example",
    "client-7d45.example",
    "client-b280.example",
    "client-839d.example",
    "client-eb38.example",
    "[client].net",
    "client-d5da.example",
    "client-f971.example",
    "client-9a89.example"
  ],
  "per_domain": {
    "[client].com": {
      "spf": "v=spf1 include:spf.protection.outlook.com include:spf.hornetsecurity.com...
```


#18 DKIM signing enabled per accepted domain [Back to summary]


```
{
  "domains_checked": [
    "[client].com",
    "client-64fd.example",
    "client-e610.example",
    "client-2055.example",
    "client-c14a.example",
    "client-7d45.example",
    "client-b280.example",
    "client-839d.example",
    "client-eb38.example",
    "[client].net",
    "client-d5da.example",
    "client-f971.example",
    "client-9a89.example"
  ],
  "per_domain": {
    "[client].com": {
      "selectors_published": []
    },
    "[client].net": {
      "selectors_published":...
```

#19 DMARC record published (p=quarantine or p=reject) [Back to summary]


```
{
  "domains_checked": [
    "[client].com",
    "client-64fd.example",
    "client-e610.example",
    "client-2055.example",
    "client-c14a.example",
    "client-7d45.example",
    "client-b280.example",
    "client-839d.example",
    "client-eb38.example",
    "[client].net",
    "client-d5da.example",
    "client-f971.example",
    "client-9a89.example"
  ],
  "per_domain": {
    "[client].com": {
      "dmarc": "v=DMARC1; p=none; rua=mailto:user-bc55f4@client-591b.example;...
```


#20 Anti-phishing policy with impersonation protection [Back to summary]


```
{
  "enabled_count": 1,
  "policy_count": 1
}
```


#21 Safe Attachments and Safe Links enabled [Back to summary]


```
{
  "safe_attachments": true,
  "safe_links_email": true
}
```


#22 Outbound spam policy limits configured [Back to summary]


```
{
  "actions": [
    "BlockUserForToday"
  ],
  "policy_count": 1
}
```


#23 Mailbox auditing enabled [Back to summary]


```
{
  "audit_disabled": false
}
```

#24 Auto-forwarding to external blocked [Back to summary]


```
{
  "outbound_autoforwarding_modes": [
    "Automatic"
  ],
  "remote_domain_autoforward": true
}
```


#25 External sharing restricted at tenant level [Back to summary]


```
{
  "sharingCapability": "externalUserAndGuestSharing"
}
```


#26 Anonymous link expiration enforced [Back to summary]


```
{
  "requireAnonymousLinksExpireInDays": null,
  "sharingCapability": "externalUserAndGuestSharing"
}
```


#27 Sensitivity labels deployed [Back to summary]


```
{
  "label_count": 0,
  "label_names": []
}
```


#28 OneDrive retention for ex-employees [Back to summary]


```
{
  "deletedUserPersonalSiteRetentionPeriodInDays": 30
}
```


#29 Site creation restricted to admins [Back to summary]


```
{
  "isSiteCreationEnabled": true,
  "isSiteCreationUIEnabled": true
}
```


#30 Guest access in Teams reviewed [Back to summary]


```
{
  "allow_guest_user": true
}
```

#31 External communications policy configured [Back to summary]


```
{
  "allow_federated_users": true,
  "allow_public_users": false,
  "allow_teams_consumer": true
}
```


#32 Meeting lobby for external participants [Back to summary]


```
{
  "auto_admitted_users": "Everyone"
}
```


#33 Recording policies restricted [Back to summary]


```
{
  "allow_cloud_recording": true
}
```


#34 Third-party application registrations reviewed [Back to summary]


```
{
  "app_count": 19,
  "sample": [
    {
      "appId": "a709d7da-a8ce-4e54-a2c6-b9f34cca2412",
      "displayName": "Powershell"
    },
    {
      "appId": "e1dfa8be-0a7b-4086-a112-de1fcade73a2",
      "displayName": "[person-1b9b95]"
    },
    {
      "appId": "323282fc-7200-40b5-8ba1-4fadddd57b59",
      "displayName": "SMTP"
    },
    {
      "appId": "a0fa6085-cf67-4888-8df0-c85519d9431c",
      "displayName": "[person-9b0f17]"
    },
    {
      "appId":...
```


#35 Anonymous join disabled for confidential meetings [Back to summary]


```
{
  "allow_anonymous_join_policy": true,
  "disable_anonymous_join_config": false
}
```

#36 Device compliance enforced via Conditional Access [Back to summary]


```
{
  "enforcing_policies": []
}
```


#37 Disk encryption required (BitLocker / FileVault) [Back to summary]


```
{
  "macos_policies_requiring_filevault": 0,
  "macos_policies_total": 0,
  "windows_policies_requiring_bitlocker": 0,
  "windows_policies_total": 0
}
```


#38 Minimum OS version enforced [Back to summary]


```
{
  "policies_total": 1,
  "policies_without_min_version": [
    "Default compliance policy for Android (androidCompliancePolicy)"
  ]
}
```


#39 Microsoft Defender for Endpoint deployed [Back to summary]


```
{
  "defender_related_configs": [],
  "device_configurations_total": 2
}
```


#40 Windows Autopilot deployment profiles configured [Back to summary]


```
{
  "profile_count": 0,
  "profile_names": []
}
```


#41 App Protection Policies (MAM) deployed [Back to summary]


```
{
  "policy_count": 0,
  "policy_names": []
}
```

#42 Stale managed devices cleaned up (>180 days) [Back to summary]


```
{
  "device_total": 5,
  "stale_count": 0,
  "stale_sample": []
}
```


#43 Device enrollment restrictions configured [Back to summary]


```
{
  "admin_defined_count": 0,
  "config_count": 5,
  "types": [
    "",
    "deviceEnrollmentLimitConfiguration",
    "deviceEnrollmentPlatformRestrictionsConfiguration",
    "deviceEnrollmentWindowsHelloForBusinessConfiguration",
    "windows10EnrollmentCompletionPageConfiguration"
  ]
}
```


#44 Unassigned licenses reviewed [Back to summary]


```
{
  "billable_sku_total": 2,
  "sku_total": 7,
  "total_unused": 0,
  "trial_free_excluded": 5,
  "unused_licenses": []
}
```


#45 Inactive accounts (no sign-in or send for 6 months) [Back to summary]


```
{
  "inactive_count": 2,
  "sample": [
    {
      "displayName": "[person-24e415]",
      "lastSignInDateTime": "2025-11-05T07:39:40Z",
      "userPrincipalName": "[person-24e415]@[client].net"
    },
    {
      "displayName": "[person-576473]",
      "lastSignInDateTime": "2025-06-18T21:15:51Z",
      "userPrincipalName": "[person-576473]@[client].net"
    }
  ],
  "users_enabled": 16,
  "users_total": 16,
  "users_without_signin_data": 0
}
```

#46 Mailbox size vs license tier mismatch [Back to summary]


```
{
  "auto_expand_detection": "manual_verification_required",
  "current_sku_distribution": {
    "Microsoft 365 Business Premium (EU, no Teams)": 15
  },
  "mailbox_total": 16,
  "recommended_actions": [],
  "resource_excluded": 0,
  "sample_per_tier": {
    "tier_1": [],
    "tier_2": [],
    "tier_3": []
  },
  "shared_excluded": 1,
  "tier_1_count": 0,
  "tier_2_count": 0,
  "tier_3_count": 0
}
```


#47 Duplicate or redundant license SKUs [Back to summary]


```
{
  "overlaps": [],
  "sku_count": 7
}
```


#48 Over-licensed users right-sizing [Back to summary]


```
{
  "annual_saving": 1830.0,
  "candidates": [
    {
      "action": "downgrade_license",
      "annual_saving": 216.0,
      "current": "Office_365_w/o_Teams_Bundle_Business_Premium",
      "current_name": "Microsoft 365 Business Premium (EU, no Teams)",
      "target": "EXCHANGESTANDARD",
      "target_name": "Exchange Online Plan 1",
      "upn": "user-c59a53@client-64fd.example"
    },
    {
      "action": "downgrade_license",
      "annual_saving": 216.0,
      "current":...
```


#49 Unified audit log enabled [Back to summary]


```
{
  "sample_recent_events": 1
}
```

#50 Microsoft Secure Score posture [Back to summary]


```
{
  "controls_evaluated": 72,
  "current_score": 121.9,
  "max_score": 278.0,
  "percent": 44,
  "top_gaps": [
    "McasFirewallLogUpload",
    "mdo_commonattachmentsfilter",
    "dlp_datalossprevention",
    "exo_individualsharing",
    "meeting_restrictanonymousjoin_v1",
    "meeting_pstnusersbypasslobby_v1",
    "meeting_autoadmitusers_v1",
    "meeting_designatedpresenter_v1",
    "CustomerLockBoxEnabled",
    "mip_autosensitivitylabelspolicies",
    "mdo_allowedsenderscombined",
   ...
```


All data was read via the Microsoft Graph API using read-only Application permissions. No tenant data is retained after this report is generated. This report is informational and is not a substitute for a full security audit by a qualified consultant. Re-running this audit periodically is recommended; recommended cadence is monthly.