CHECKLIST

Microsoft 365 Conditional Access Review Checklist

A practical checklist for auditing and hardening your Conditional Access policies

Walk through your Conditional Access configuration systematically. This checklist covers policy inventory, baseline controls, identity protection, device compliance, application access, session management, and monitoring — helping you find gaps and strengthen your posture.

For	M365 Admin
Stage	Any
Topic	Microsoft 365 Conditional Access Policy Review And Hardening

Conditional Access is the policy engine that enforces how users reach your Microsoft 365 environment. A strong configuration blocks risky sign-ins, enforces MFA where it matters, and limits access from unmanaged devices. A weak one leaves gaps that phishing and credential theft walk straight through. This checklist helps you audit what you have, find what is missing, and prioritise the fixes that reduce real risk. Work through it in order or jump to the section that matches your current concern.

> *Print this or keep it open in a second window while you work in the Entra admin centre. Tick off each item as you verify it. Where you find a gap, note it and decide whether to fix it now or add it to your backlog. If a control does not apply to your environment, mark it not applicable and move on.*

Policy Inventory and Baseline

Start by understanding what policies you have and whether the fundamentals are in place.

- [ ] List all active Conditional Access policies and their assigned users or groups
  You cannot audit what you do not know exists. Policies targeting all users or nested groups can surprise you.
- [ ] Check for policies in report-only mode that should be enforced
  Report-only is useful for testing, but leaving a policy there indefinitely means it is not protecting anything.
- [ ] Verify that at least one policy requires MFA for all users
  Exclude break-glass accounts only.
- [ ] Confirm that administrator roles are covered by a separate, stricter MFA policy
  Admin accounts are high-value targets. They need stronger controls than standard users.
- [ ] Check whether legacy authentication is blocked for all users
  Legacy protocols bypass MFA and modern security controls entirely.
- [ ] Verify that break-glass accounts are excluded from all Conditional Access policies
  Document the exclusion and test the accounts regularly.

Identity Protection and Risk-Based Controls

Use the signals Microsoft collects to block risky sign-ins and force remediation automatically.

- Enable a policy that blocks sign-ins flagged as high risk
  High-risk sign-ins indicate credential theft or compromise. Blocking them stops the attacker at the door.
- Require MFA or password change for medium-risk sign-ins
  Medium risk is not certain compromise, but it is enough to demand stronger proof before granting access.
- Require password change for users flagged as high risk
  A high-risk user signal means the account is likely compromised. Forcing a password reset cuts off the attacker.
- Review risky users and risky sign-ins reports weekly
  Automated policies catch most problems, but manual review finds patterns and persistent threats the automation misses.
- Confirm that risk-based policies apply to all users, not just a pilot group
  Attackers do not limit themselves to pilot groups.

Device Compliance and Trusted Locations

Control access based on device state and network location to limit exposure from unmanaged endpoints.

- Require compliant or Entra hybrid joined devices for access to sensitive applications
  Define which applications are sensitive: email, file storage, finance systems.
- Block access from untrusted locations for administrator accounts
  Admin access from unexpected countries or anonymous proxies is almost always an attack.
- Define trusted IP ranges and exclude them from MFA only where justified
  Be conservative. Office IPs are not inherently safe if an attacker is already inside.
- Review the list of compliant devices and remove stale or decommissioned entries
  Old device records can be re-registered by an attacker who finds the hardware or spoofs the identity.
- Verify that non-compliant devices are blocked, not just warned
  Warnings are ignored. Blocking forces remediation.

Application Access Controls

Not every application needs the same level of protection. Apply controls that match the risk.

- [ ] Identify which cloud applications are covered by Conditional Access policies
  Check for gaps: third-party SaaS, custom apps, legacy integrations.
- [ ] Require MFA for access to all Microsoft 365 applications
  Email, SharePoint, and Teams contain the data attackers want. Protect them all.
- [ ] Block or restrict access to high-risk applications from unmanaged devices
  If the device is not yours, you cannot control what happens to the data after the user downloads it.
- [ ] Review application consent policies and block risky app permissions
  Users granting broad permissions to third-party apps bypass your access controls entirely.
- [ ] Verify that guest and external users have separate, more restrictive policies
  Guests do not belong to your organisation. Treat them as higher risk by default.

Session Controls and Continuous Monitoring

Access decisions are not one-time events. Use session controls to limit what users can do after they sign in.

- [ ] Enable Conditional Access App Control for sensitive applications
  Requires Microsoft Defender for Cloud Apps.
- [ ] Set sign-in frequency to require re-authentication for high-risk scenarios
  For example, every 4 hours for admin roles or every 1 hour for unmanaged devices.
- [ ] Use persistent browser sessions only where necessary and document the justification
  Persistent sessions are convenient but weaken security. Apply them narrowly.
- [ ] Review sign-in logs for Conditional Access failures and investigate anomalies
  Repeated failures from the same user or location indicate an attack in progress or a misconfigured policy blocking legitimate access.
- [ ] Check for users bypassing Conditional Access through legacy protocols or unsupported clients
  If legacy authentication is not fully blocked, attackers will find and exploit it.

Exclusions, Exceptions, and Policy Conflicts

Exclusions are necessary but dangerous. Audit them carefully and remove any that are no longer justified.

- [ ] List all user and group exclusions across all policies
  Exclusions are the first place attackers look for a way around your controls.
- [ ] Verify that exclusions are documented with a business justification and review date
  Undocumented exclusions accumulate over time and are rarely removed even after the reason disappears.
- [ ] Remove service accounts and shared mailboxes from user-targeted policies
  Create separate policies for non-human identities if needed.
- [ ] Check for conflicting policies that might block legitimate access
  Use the What If tool in Entra to simulate sign-ins and see which policies apply.
- [ ] Review policies targeting all users and confirm they do not accidentally include break-glass accounts
  If your emergency accounts are blocked, you have no way to recover from a misconfiguration.

Monitoring, Alerts, and Continuous Improvement

Conditional Access is not a one-time setup. Monitor it, measure it, and adjust it as your environment changes.

- [ ] Set up alerts for Conditional Access policy changes
  Unauthorised changes to policies can disable your security controls without anyone noticing.
- [ ] Review Conditional Access insights and recommendations in the Entra admin centre monthly
  Microsoft surfaces unused policies, risky configurations, and coverage gaps automatically.
- [ ] Run a What If analysis for common user scenarios and verify the expected policies apply
  Test: standard user from office, admin from home, guest from mobile device.
- [ ] Document your Conditional Access design and keep it updated as policies change
  When someone leaves or you need to troubleshoot at 2am, documentation is the only thing that saves you.
- [ ] Schedule a full Conditional Access review every six months
  Your environment changes. New applications, new users, new threats. Policies that worked six months ago may not work now.

Next steps

→ Work through each section and mark items complete, not applicable, or requiring action.

→ For items requiring action, decide whether to fix them immediately or add them to your security backlog with a priority.

→ Use the What If tool in Entra to test policy behaviour before making changes that affect all users.

→ Document any exclusions you keep and set a calendar reminder to review them in three months.

→ Run a Conditional Access insights report and compare it against this checklist to find additional gaps.

→ If you found significant gaps, schedule a follow-up review in one month to verify fixes are working as intended.

> *Conditional Access is the foundation of Zero Trust in Microsoft 365. A strong configuration stops most attacks before they reach your data. A weak one is the gap attackers exploit first. Work through this checklist, fix what you find, and review it regularly.*

More free resources and training at nandycybersuccess.com