

UK Cyber Essentials v3.3 ("Danzell") Practitioner Implementation Handbook

Complete Technical Runbook for NCSC / IASME Question Set v3.3 (Mandatory from 27 April 2026) • Microsoft Entra ID & Intune

Section 1: What Changed in NCSC / IASME v3.3 ("Danzell" – 27 April 2026)

On 27 April 2026, the UK National Cyber Security Centre (NCSC) and IASME replaced v3.2 ("Willow") with the **Cyber Essentials v3.3 ("Danzell")** question set. Assessors are instructed to issue an immediate **Automatic Certification Fail** if any of the five core technical controls below are non-compliant across your in-scope estate.

IASME CLAUSE	CONTROL AREA	LEGACY V3.2 ("WILLOW") RULE	NEW V3.3 ("DANZELL" APR 2026) RULE
Sec A1.1 & A1.4	Cloud Services & Home-Worker VPN Boundary	Cloud services often poorly documented; split-tunnel VPNs ambiguously treated.	Cannot-Be-Excluded Cloud Scope: Every SaaS/PaaS/IaaS app storing org data is in-scope. Home workers must use locked host firewalls OR full-tunnel VPN.
Sec A4.5	Cloud Multi-Factor Authentication (MFA)	MFA mandatory for Admins and certain cloud users; standard user carve-outs common.	Zero-Exception Cloud MFA: Where a cloud service offers MFA, it MUST be enforced for 100% of Admins AND Standard Users .
Sec A4.5 (b)	Passwordless, Biometrics & PIN Throttling	Passwordless guidance split across annex notes.	Anti-Hammering & Backup Auth: FIDO2/WHfB PINs (≥ 6 chars) and biometrics require hardware brute-force throttling (≤ 10 attempts) + secure backup auth.
Sec A3.1	14-Day High/Critical Patching & OS EoL	Windows 10 22H2 still supported prior to Oct 2025.	Win 10 22H2 Unlicensed = Auto-Fail: All OS/apps must be supported and patched within 14 days for CVSS v3 ≥ 7.0 / CISA KEV.
Sec A4.2	Leaver Deprovisioning & Guest Dormancy	Informal offboarding timelines tolerated.	1 Working Day Offboarding: Leavers disabled within 24h; accounts (including B2B Guests) inactive >30 days suspended automatically.

Assessor Alert – Conditional Access "Report-Only" Trap: Policies left in `enabledForReportingButNotEnforced` state do NOT satisfy IASME Section A4.5. You must transition ``CA01``, ``CA02``, and ``CA03`` to `enabled` prior to signing your self-assessment declaration.

Section 2: Cloud Service Scope & Home-Worker / BYOD VPN Rules (Sec A1.1 & A1.4)

Under v3.3 ("Danzell"), any cloud platform hosting organisational email, files, finance records, CRM data, or identity planes cannot be carved out of scope. Furthermore, home workers and BYOD devices operating on residential ISP routers do not have a trusted hardware boundary firewall.

2.1 Mandatory Boundary Controls for Remote & Home Workers

- **Option A – MDM-Locked Host Software Firewall (Recommended for Cloud-Native SMEs):** Enable `Windows Defender Firewall` or `macOS Application Firewall` across Domain, Private, and Public profiles via Microsoft Intune, blocking all unsolicited inbound connections and preventing standard users from disabling the firewall.
- **Option B – Full-Tunnel (Split-Tunnel Disabled) Corporate VPN:** Route 100% of remote endpoint traffic (`0.0.0.0/0`) through an Always-On VPN terminating at a managed corporate firewall that meets NCSC password/patching standards.

Section 3: Entra ID Zero-Exception MFA & Passwordless Throttling (Sec A4.5)

Deploy the four Conditional Access policies provided in `templates/Entra-Conditional-Access-CEv33-Baselines.json`:

POLICY ID	TARGET POPULATION	GRANT CONTROL / TECHNICAL REQUIREMENT
CA01	14 Privileged Entra Directory Roles	Require Phishing-Resistant MFA Strength (FIDO2 Security Key / Windows Hello for Business / Passkey) + 12-hour sign-in frequency.
CA02	100% Internal Users & B2B Guests	Require Multi-Factor Authentication across all cloud apps. Zero contractor or executive exemptions permitted.
CA03	All Users & Service Accounts	Block Legacy Authentication (<code>`exchangeActiveSync`</code> , <code>`other`</code> – IMAP, POP3, SMTP Basic Auth).
CA04	All Corporate Endpoints	Require Intune Compliant Device or Hybrid Entra Joined status before accessing Office 365 data.

3.1 Passwordless PIN & Biometric Brute-Force Throttling (Intune Windows Hello Baseline)

Intune Portal > Endpoint Security > Account Protection > Windows Hello for Business:

- Minimum PIN Length: 6 characters (8 recommended for Admins)
- Require TPM 2.0 Security Processor: Enabled (Blocks software-only fallback)
- Maximum PIN Failed Sign-In Attempts Before Lockout: 5 attempts (TPM anti-hammering active)
- Recovery / Backup Authentication: Require Entra MFA challenge or secondary FIDO2 key

Section 4: Intune 14-Day CVSS ≥ 7.0 Patching SLA & End-of-Life OS Removal (Sec A3.1)

IASME v3.3 requires all operating systems, browsers, firmware, and third-party applications to receive high/critical security updates (CVSS v3 ≥ 7.0 or CISA Known Exploited Vulnerabilities) within **14 calendar days** of vendor release.

4.1 Intune Windows Update for Business Ring Configuration

INTUNE UPDATE RING SETTING	CE V3.3 COMPLIANT VALUE	WHY ASSESSORS CHECK THIS
Quality Update Deferral Period	3 Days (Must be ≤ 7 Days)	Deferrals >7 days leave insufficient time to complete installation + reboot inside 14 days.
Deadline for Quality Updates	5 Days	Forces background installation within 3 + 5 = 8 days of patch release.
Grace Period Before Forced Reboot	2 Days	Guarantees reboot completion within 3 + 5 + 2 = 10 days (4 days inside the 14-day SLA).
Feature Update Minimum OS	Windows 11 23H2 / 24H2	Windows 10 22H2 reached End-of-Life in Oct 2025; unpatched Win 10 causes automatic fail.

Section 5: 1-Day Leaver Offboarding & 30-Day Dormancy Governance (Sec A4.2)

Run this PowerShell remediation snippet immediately when HR notifies IT of a leaver (must execute within **1 working day**) and monthly to suspend accounts inactive >30 days:

```
# 1. Immediate Same-Day Leaver Lockout & Token Revocation
$LeaverUPN = "former.employee@yourcompany.co.uk"
Update-MgUser -UserId $LeaverUPN -AccountEnabled:$false
Revoke-MgUserSignInSession -UserId $LeaverUPN

# 2. Automated Suspension of Internal/Guest Accounts Inactive > 30 Days
Import-Csv ./ce33-evidence/01-Entra-Identity-MFA-And-Dormancy.csv |
  Where-Object { $_.AccountEnabled -eq "True" -and [int]$_DaysInactive -gt 30 } |
  ForEach-Object {
    Write-Host "Suspending dormant account (>30d): $($_.UserPrincipalName)" -ForegroundColor
    Yellow
    Update-MgUser -UserId $_.UserPrincipalName -AccountEnabled:$false
  }
```

Section 6: Final Pre-Submission IASME v3.3 Assessor Sign-Off Checklist

Complete every row below and attach the output of `evaluate_ce_v33_posture.py` to your internal compliance ticket before submitting your IASME portal declaration.

CHECK	IASME V3.3 CLAUSE	VERIFICATION REQUIREMENT	EVIDENCE FILE IN PACK
☐ 01	Sec A1.1 / A1.4	All SaaS, PaaS, and IaaS services hosting org data are listed in the Cloud Asset Register.	Cloud-Asset-And-Shadow-IT-Register.csv
☐ 02	Sec A1.3	Home workers have MDM-locked host firewall enabled OR use a full-tunnel corporate VPN.	03-Intune-Endpoint-OS-Compliance.csv
☐ 03	Sec A4.5	100% of enabled Admin, Standard User, and Guest accounts have MFA enforced ('CA01' & 'CA02' = enabled).	01-Entra-Identity-MFA-And-Dormancy.csv
☐ 04	Sec A4.5 (b)	Passwordless WHfB PINs (≥6 digits) and biometrics enforce TPM brute-force throttling (≤10 attempts).	Model-Answer-Bank-IASME-v33.md
☐ 05	Sec A4.3	Legacy authentication protocols blocked tenant-wide ('CA03' = enabled) and Service Principals IP-locked.	04-Service-Principals-And-Workload-Scope.csv
☐ 06	Sec A4.2	Zero enabled user or guest accounts exceed 30 days of sign-in inactivity; leavers disabled in ≤1 working day.	01-Entra-Identity-MFA-And-Dormancy.csv
☐ 07	Sec A3.1	Zero Windows 10 22H2 (unlicensed ESU) or unsupported macOS devices; Update Ring deferral ≤7 days.	03-Intune-Endpoint-OS-Compliance.csv
☐ 08	Sec A5.1	100% of endpoints report active Defender antimalware, Tamper Protection, and BitLocker/FileVault.	CE-v33-Executive-Readiness-Report.html

Need Cyber Essentials Plus Hands-On Verification? Run our free live DNS/DMARC/SPF Scanner and NIS2/DORA 5-Domain Batch Auditor anytime at <https://faultypacket.co.uk> or email security@faultypacket.co.uk.