

Identification and Implementation of Security Baselines Aligned to Cyber Essentials v3.3

Tom Walters



Research Context

- Creditsafe: global credit referencing & financial intelligence agency
 - HQ Dublin; engineering centres in Cardiff and India; Cardiff Engineering = sole IT provider
- Existing certifications: ISO 27001, PCI-DSS, SOC 2 Type 2, DORA/GDPR/NIS2 — CE v3.3 not yet held
- Commercial driver: CE v3.3 unlocks ~£14M in new UK contracts + public sector eligibility via G-Cloud
- Researcher positionality: Security Engineer, 4 yrs + 3.5 yrs SOC/service desk
 - Embedded access to 2 representative Windows 11 devices

Research Problem

- Approximately 1,500 Windows 11 devices, hybrid Intune + on-prem Active Directory
 - Intune policy takes precedence where the two conflict
- No single source reconciles CE v3.3, CIS Benchmarks, MS Security Baseline & NCSC guidance
- Prior CIS compliance: 72% (2024 baseline) — no formal re-assessment since
- **Core problem: Which controls are equivalently enforceable via Intune vs. GPO, and where do parity gaps exist?**

Research Aim & Objectives

- **Aim: a viable, culturally acceptable hardening baseline aligned to CE v3.3**
 - Reconciling CE, CIS Benchmarks & MS Security Baseline into one Intune-deployable strategy
- Obj 1 — Identify current compliance state (baseline scans, 2 devices)
- Obj 2 — Reconcile framework requirements (CE ↔ CIS ↔ MS ↔ NCSC mapping tool)
- Obj 3 — Design & export a unified baseline (GPO + Intune dual output)
- Obj 4 — Validate the hardened baseline (re-scan, gap documentation)

Success Criteria & Scope

- **Success across 5 dimensions:**
 - Control coverage $\geq 90\%$ of CE controls mapped to CIS/MS/NCSC
 - Compliance improvement: baseline ~32–38% $\rightarrow$ target 58–62%
 - Artefact delivery: mapping tool + dual-export baseline + lab validation report
 - Artefact traceability to CE's 5 pillars
 - Timeline achievement against module deadlines
- In scope: Windows 11 endpoints (1,500 devices), hybrid Intune+AD, lab/pilot validation (2 devices)
- Out of scope: org-wide rollout, macOS, production deployment/change management

Literature Review

- CE v3.3: 5 pillars — Firewalls, Secure Configuration, Security Update Management, User Access Control, Malware Protection
- CIS Windows 11 Benchmarks: 250+ controls across Level 1 (foundational) / Level 2 (advanced)
- MS Security Baseline & NCSC Device Guidance: vendor/government approaches — none reconcile all four
- Academic literature: SMEs struggle to translate abstract requirements into technical controls
 - Policy-to-practice gaps emerge specifically in hybrid cloud/on-prem environments

Literature Review (continued)

- Vendor: Intune baselines align partially with CIS L1; CIS 8.1 ↔ CE v3.2 crosswalk exists
 - ...but doesn't address Intune vs. GPO enforcement parity
- Practitioner: CE+ audits test ~418 granular controls; IASME's April 2026 update signals continued evolution
- **The gap: no study reconciles CE v3.3 + CIS + MS + NCSC into one conflict-annotated baseline for hybrid Intune+GPO environments**
- This project's contribution: a normalised mapping tool, validated in a real organisational context

Research Methodology: Philosophy & Approach



A documented conflict between CIS guidance and CE requirements is risk-accepted or remediated in consultation with Security & Corporate Solutions.

Research Strategies

- Literature review: multivocal (MLR) approach across 4 source tiers
 - Primary standards, academic literature, vendor/practitioner, grey literature
- Gap analysis: HardeningKitty scans (418 L1/L2 controls) mapped to CE pillars, not raw % scores
- Design & validation: Intune Settings Catalogue + Graph API export
 - Lab PoC validation, then monthly production tracking on a second device

Risk, Ethics & Rigour

- Primary risk: adoption resistance (UAC / AppLocker / Credential Guard conflicts)
 - Mitigated via staged deployment + close liaison with security/infra teams
- Secondary risk: tool unavailability — CIS-CAT Pro fallback pending 2027 budget
- Ethics: no human subjects; device anonymisation; scope fixed at 2 pilot devices; reversible within 90 min
- Rigor: HardeningKitty is reproducible; manual verification of High/Medium items
 - Comparable to similar hybrid Intune/AD UK orgs — not cloud-native or on-prem-only estates

Data Collection & Evaluation

- HardeningKitty scans: monthly, CSV output, pass/fail across 418 controls
- Intune configuration exports via Graph API: before/after JSON snapshots
- Manual verification of High/Medium severity flagged items
- Evaluation: HardeningKitty → CE pillar mapping + CIS → CE parallel mapping
 - Presented as a narrative before/after improvement story, with comparison matrices as applicable

Development Methodology

- Not a software build — implementation governed by ITIL-aligned change control
- PoC phase (2 devices): minor non-production change, peer reviewed
 - Each submission includes rollback plan, monitoring & success criteria, escalation points
- Scaled Technical Readiness Review: 5-user cohort → 25-user cohort
- ‘Target Week’: last week of each month frozen — no changes, protects Sales Office stability

Resources & Materials

- Hardware: 2 representative Windows 11 laptops (production + minimal-permission test device)
- Software: HardeningKitty, MS Graph PowerShell SDK, Intune Admin Centre, Settings Catalogue, GPO Editor
- Information: NCSC CE v3.3, CIS Benchmarks, CIS↔CE mapping, MS Security Baselines, UWTSD library access
- Human: internal test groups via approved change process; CIS-CAT Pro pending 2027 budget

Project Plan



Implementation phase (Feb–Aug 2027) hands off to the final-year individual project.

References

- [1] UK National Cyber Security Centre, “Cyber Essentials: Requirements for IT Infrastructure v3.3,” NCSC, 2023. [Accessed 01 Sept. 2026].
- [2] Center for Internet Security, “CIS Benchmark for Microsoft Windows Desktop,” CIS, 2026. Available: cisecurity.org/benchmark/microsoft_windows_desktop. [Accessed 26 Aug. 2026].
- [3] D. J. Button, J. Ophoff, A. Irons and S. McDonald, “Mind the gap: exploring perceptions of cyber security in the SME context,” *Information and Computer Security*, vol. 34, no. 2, pp. 231-245, 2025.
- [4] M. Wilson and S. McDonald, “One size does not fit all: cybersecurity perspectives of UK-based small businesses,” *Information Security Journal*, vol. 34, no. 1, pp. 15-49, 2025.
- [5] M. F. Arroyabe et al., “Exploring the economic role of cybersecurity in SMEs: a case study of the UK,” 2024. Available: doi.org/10.1016/j.techsoc.2024.102670.
- [6] S. Chaudhary, V. Gkioulos and S. K. Katsikas, “A quest for research and knowledge gaps in cybersecurity awareness for SMEs,” *Computer Science Review*, p. 100592, Sept. 2023.
- [7] A. H. Juma, A. A. Arman and F. Hidayat, “Cybersecurity Assessment Framework: A Systematic Review,” *Int. Conf. on ICT for Smart Society*, 2023.
- [8] Microsoft Learn, “Microsoft Intune Security Baselines Overview,” Microsoft, 2024. [Accessed Aug. 2026].
- [9] Center for Internet Security, “CIS Controls v8.1 Mapping to NCSC Cyber Essentials v3.2,” CIS, 2024. [Accessed Aug. 2026].
- [10] National Cyber Security Centre, “NCSC Device Security Guidance,” NCSC, 2024. [Accessed 02 Sept. 2026].
- [11] CyPro, “Cyber Essentials Plus – What the Audit Tests,” CyPro Ltd, 2024. [Accessed 28 Aug. 2026].
- [12] IASME, “Upcoming changes to Cyber Essentials scheme: April 2026 Update,” IASME, 3 Nov. 2025. [Accessed 02 Sept. 2026].
- [13] Microsoft, “Security Compliance Toolkit v1.0,” Microsoft, 2024. Available: github.com/microsoftgraph/powershell-intune-samples. [Accessed 02 Sept. 2026].