Securing the NHS Endpoint for the **CAF-aligned Data Security and Protection Toolkit**

An endpoint assurance mapping with IGEL - primary framework: DSPT (CAF) v8 · with a Cyber Essentials v3.3 control mapping

June 2026

Table of Contents

Executive summary

The way the NHS evidences data security has fundamentally changed. The Data Security and Protection Toolkit (DSPT) is no longer a checklist of yes/no assertions; it is now aligned to the National Cyber Security Centre's (NCSC) Cyber Assessment Framework (CAF). Organizations must now demonstrate that controls work in practice and achieve defined outcomes - and, in many cases, prove it through an independent audit.

This shift raises the bar for endpoint security. Outcome-based assessment rewards architectures that reduce attack surface, remove local data, enforce consistent configuration and recover quickly - precisely the properties of the IGEL endpoint operating model.

IGEL's Adaptive Secure Endpoint Platform enforces a Preventative Security Model™ to deliver an immutable, modular operating system with no persistent local data, centrally managed configuration, application allow-listing and rapid re-provisioning. These characteristics map directly onto the most security-relevant CAF outcomes within the DSPT - in particular Secure by design (B4.a), Identity and access control (B2.a), Resilience preparation (B5.a), Vulnerability management (B4.d) and Data security (Objective B3).

This white paper does three things:

- Explains what changed when the DSPT moved to a CAF-aligned, outcome-based model, and what that means for endpoint strategy.
- Maps IGEL's capabilities to the relevant CAF objectives and contributing outcomes used by the DSPT - honestly framed as a contribution to outcomes an organisation owns end-to-end.
- Provides, in Appendix A, a clean mapping to the five NCSC Cyber Essentials v3.3 technical controls, which remain a common NHS procurement requirement.

Key dates and facts

- DSPT 2025/26 is version 8 - the most significant change since the toolkit launched in 2018.
- **Submission deadline:** 30 June 2026. Category 1 organisations require an independent CAF-aligned audit.
- **Assessment is outcome-based:** evidence must show effectiveness, not just existence.
- Cyber Essentials Plus and ISO 27001 no longer auto-satisfy DSPT outcomes - each outcome must be evidenced directly (and independently audited for Category 1 and 2)

The NHS endpoint challenge: Now and Next

The NHS faces a unique set of pressures in managing and securing its clinical and administrative endpoints. The same challenges that make care delivery hard also make cyber assurance hard:

- Fast, simple, secure access to patient information. Clinicians need instant access to the latest patient record - often while managing multiple critical situations, such as in an A&E setting. Technology must be supportive, not a source of friction.
- Data security and privacy. Protecting sensitive patient information demands robust technical measures to prevent breaches and unauthorised access - and, under CAF, evidence that those measures are effective.
- Endpoint diversity. The NHS operates a wide range of device types and ages, creating real complexity in standardisation, configuration and patching.
- Budget. As a publicly funded institution, IT budgets are constrained and frequently consumed by "keeping the lights on" rather than transformation.

IGEL's healthcare endpoint strategy, helps organisations to deliver secure, cloud-ready digital workspaces that support patient care, reduce endpoint risk, and optimise IT spend. By replacing the general-purpose local OS with IGEL Secure Endpoint OS Platform - an immutable endpoint OS with no local data storage - IGEL reduces the attack surface and supports the security, governance, and evidence requirements expected across NHS environments.

What's changed: the DSPT is now CAF-aligned

The DSPT changed in September 2024 for NHS trusts and foundation trusts, ICBs, Commissioning Support Units (CSUs) and DHSC arm's length bodies (ALBs), and again in September 2025 for designated Operators of Essential Services (OES) and genomics organisations. The driver is the Department of Health and Social Care (DHSC) cyber security strategy for health and social care to 2030, which seeks to harmonise healthcare cyber standards with other critical national sectors.

In practical terms, the toolkit moved away from a checklist of discrete evidence items (the old 1.1.4, 4.5.3, 6.2.1 references) towards principle-led, outcome-based assurance built on the NCSC CAF. **There are 47 contributing outcomes in total, grouped under five objectives:**

Objective	Focus
A	Managing security risk - governance, risk management, asset management and supply chain.
B	Protecting against cyber attack - policies and processes, identity and access control, data security, system security, resilient networks and systems, and staff awareness.
C	Detecting cyber security events - security monitoring and proactive event discovery.
D	Minimising the impact of incidents - response and recovery planning, and lessons learned.
E	Using and sharing information (NHS-specific) - lawful use and sharing of patient data, data subject rights, consent and the national data opt-out.

Old model vs CAF-aligned model

Legacy DSPT (to v5/v7)	CAF-aligned DSPT (v8, 2025/26)
Numbered evidence items answered yes/no.	Contributing outcomes rated Achieved / Partially achieved / Not achieved.
Compliance demonstrated by presence of a control.	Assurance demonstrated by effectiveness of a control in practice.
Largely a self-assessment exercise.	Independent CAF-aligned audit required for Category 1 organisations.
Cyber Essentials Plus / ISO 27001 could offset elements.	No exemptions - outcomes must be evidenced directly.
Endpoint treated as one of many checkboxes.	Endpoint architecture is judged on the outcomes it actually delivers.

This table describes the CAF-aligned track that applies to NHS trusts, ICBs, CSUs, ALBs, OES and genomics organisations. IT suppliers remain on the non-CAF DSPT for 2025/26 - though they too now face mandatory independent audit, and the same shift toward evidence-based assurance is visible there, most clearly in the withdrawal of Cyber Essentials Plus equivalence for the DSPT's MFA evidence item (4.5.3). See Appendix A, Control 4.

Why this favours the IGEL model

Outcome-based assessment rewards designs that reduce risk by construction. An immutable OS with no local data, a single approved image, centrally enforced configuration, application allow-listing and minutes-to-rebuild recovery are easy to evidence as effective - because the desirable outcome is a property of the architecture, not a process layered on top of it.

IGEL's Preventative Security Model™ and Zero Trust

IGEL's Preventative Security Model™ is designed to eliminate vulnerable endpoint attack vectors rather than detect and remediate them after the fact.

Four principles do most of the work:

- Reduced attack surface. A purpose-built, minimal operating system runs only the services required for the workspace, removing the broad attack surface of a general-purpose OS.
- Immutable operating system. The OS image is immutable, so unauthorised or malicious changes cannot persist across a reboot.
- No local data. Patient and corporate data are not stored on the device; the endpoint is an access layer to centrally hosted applications and desktops.
- Modular, centrally managed design. Configuration, applications and updates are delivered and enforced centrally, giving a consistent, known-good state across the estate.

Together these remove the need for costly, complex agent stacks on the device and reduce reliance on user vigilance. They also align naturally with Zero Trust: the NCSC's CAF guidance is explicit that its technical controls do not prevent the adoption of a Zero Trust architecture, in which the network is assumed hostile and each access request is verified. A stateless, centrally governed endpoint is a strong foundation for that model - the device holds nothing of value and asserts nothing the management plane has not authorised.

IGEL also partners with essential care-delivery peripheral manufacturers and platform providers to support microphones, signature pads, badge-tap technologies, EMR workflows and other critical clinical and administrative functions - so security gains do not come at the cost of clinical usability.

How IGEL supports CAF-aligned DSPT outcomes

The tables below map IGEL's capabilities to the CAF objectives and contributing outcomes that underpin the DSPT. Outcomes marked ★ are among those mandated for independent audit for NHS Trusts, ICBs, ALBs and CSUs in 2025/26.

Important framing: the DSPT outcomes are owned end-to-end by the NHS organisation. IGEL is a contributing component of the endpoint layer; achieving an outcome also depends on the organisation's wider processes, governance and evidence. The "How IGEL contributes" column describes the part of the outcome IGEL helps deliver - not a claim to satisfy it in full.

Objective A: Managing security risk

Outcome	What the outcome looks for	How IGEL contributes
A1.a ★ Board direction	Security is directed and owned at board level, with assurance flowing up to the board.	Central management and estate-wide reporting give the board clear, current visibility of endpoint state, versions and configuration compliance - supporting (not replacing) board-level oversight.
A3.a Asset management	The organisation maintains authoritative, accurate information about its assets to support decision-making.	The IGEL Universal Management Suite controls, configures and orchestrates policies centrally. It maintains an authoritative inventory of every IGEL endpoint - hardware, firmware, OS and application versions - exportable to a CMDB or asset tool. The Asset Inventory Tracker can also record connected peripherals.
A4.a Supply chain	Risks from suppliers and third parties are understood and managed.	IGEL is an in-scope supplier and completes the DSPT IT-supplier assertions. IGEL Technology GmbH is certified to ISO/IEC 27001:2022 covering the development, maintenance and support of IGEL products and services. By removing the local OS and data, IGEL also shrinks the endpoint footprint that other suppliers and managed-service accounts can reach.

Objective B: Protecting against cyber attack

Outcome	What the outcome looks for	How IGEL contributes
B1.a ★ Policy, process & procedure development	Security policies and processes are defined, applied and kept current.	Configuration policy is defined once and enforced consistently across the whole estate from the management platform, so the documented standard and the deployed reality stay aligned - a key evidence point under outcome-based audit.
B2.a Identity, authentication & authorisation	Users, devices and systems are verified and granted only the access they need.	Single sign-on and MFA via Microsoft Entra ID, Okta, Imprivata and Ping; MFA built into Citrix, Omnissa and Microsoft AVD/365; role-based access control in the management platform; least privilege via application entitlement (users only see apps they are authorised for); device/network authentication via NLA (SCEP/NDES).
B3.a Data security (at rest & in transit)	Data is protected against unauthorised access, including at rest and in transit.	No patient or corporate data is stored on the endpoint. The OS is immutable; relevant configuration/data partitions are encrypted; all traffic between the management platform and the device is encrypted; devices can be remotely reset to factory defaults, revoking access.

Objective B: Protecting against cyber attack (cont.)

Outcome	What the outcome looks for	How IGEL Contributes
B4.a ★ Secure by design	Systems are designed and built to be secure, minimising avoidable vulnerability.	The IGEL endpoint is secure by construction: a minimal, modular, immutable OS with autorun disabled, unnecessary services absent, a single approved base image and unapproved ports denied by default. Security is a property of the design rather than a bolt-on.
B4.d Vulnerability management	Vulnerabilities are found and fixed within appropriate timescales.	A minimal OS exposes fewer components and therefore fewer CVEs. The management platform centrally patches the estate; IGEL OS receives updates roughly every 1-2 months, with out-of-band releases for critical issues, supporting the 14-day critical-patch expectation. Active maintenance entitles devices to the latest supported OS.
B5.a ★ Resilience preparation	Systems are prepared to withstand and recover from disruption.	Endpoints are stateless. A compromised, failed or replaced device re-provisions to a known-good image in minutes from the management platform, with no local data to reconstruct - a directly verifiable recovery capability.
B5.c ★ Backups	Essential data is backed up and recoverable.	Because endpoints hold no unique data, there is nothing to back up at the device layer; management-platform configuration is itself backed up centrally. This narrows backup scope and removes the endpoint as a recovery dependency. (Backup of hosted apps/desktops remains the organisation's responsibility.)
B6.a Staff awareness & training	People are supported to work securely; reliance on user vigilance is reduced.	Application allow-listing and the immutable OS prevent users from installing or running unsanctioned software, reducing the impact of a user mistake. (Awareness and training programmes themselves remain the organisation's responsibility.)

Objective C: Detecting cyber security events

Outcome	What the outcome looks for	How IGEL Contributes
C1.a Monitoring coverage	Monitoring covers the assets and activity needed to detect events.	The management platform logs administrative actions; the IGEL Insight Service provides analytical and usage telemetry; partner integrations (e.g. ControlUp, SysTrack) add endpoint and session telemetry that can feed a SIEM. IGEL contributes endpoint signal - it is not itself the monitoring solution.
C1.b ★ Securing logs	Logs are captured, retained securely and protected from tampering.	Administrative management logs can be exported to third-party analysis/SIEM tooling and incorporated into the organisation's retention and protection policies. The immutable OS limits local tampering with device state.

Objective D: Minimising the impact of incidents

Outcome	What the outcome looks for	How IGEL Contributes
D1.a Response & recovery planning	The organisation can respond to and recover from incidents effectively.	Remote reset and rapid re-provisioning give responders a fast, reliable containment and recovery action for affected endpoints, returning them to a known-good state without rebuild effort.
D2.a Incident root cause analysis	Incidents are analysed so root causes are understood and addressed.	Management-platform and partner telemetry provide endpoint data to support root cause analysis. Note the immutable design limits on-device persistence, so endpoint forensics differ from a traditional fat client; IGEL contributes inputs to RCA rather than performing it.

Objective D: Minimising the impact of incidents

Outcome	What the outcome looks for	How IGEL Contributes
D1.a Response & recovery planning	The organisation can respond to and recover from incidents effectively.	Remote reset and rapid re-provisioning give responders a fast, reliable containment and recovery action for affected endpoints, returning them to a known-good state without rebuild effort.
D2.a ★ Incident root cause analysis	Incidents are analysed so root causes are understood and addressed.	Management-platform and partner telemetry provide endpoint data to support root cause analysis. Note the immutable design limits on-device persistence, so endpoint forensics differ from a traditional fat client; IGEL contributes inputs to RCA rather than performing it.

Objective E - Using and sharing information (NHS-specific)

Objective E concerns the lawful use and sharing of patient information - data subject rights (E2.a), the national data opt-out (E2.c), consent (E2.b) and information sharing for direct care (E3.a). IGEL does not process, store or share patient data; it is the secure, access-controlled layer through which authorised staff reach the systems that do. IGEL's contribution to Objective E is therefore indirect but real: it ensures access happens only through authenticated, authorised, centrally governed endpoints, and that no patient data persists on the device after use. The lawful-basis, consent and opt-out obligations themselves remain wholly the organisation's responsibility.

IGEL in the supply chain

The earlier white paper noted simply that "IGEL does not handle or process patient or staff information." That remains true - but under the CAF-aligned DSPT it is no longer the whole story. Supply-chain assurance (A4) explicitly brings suppliers and the accounts they use into scope, and there are no longer exemptions based on a supplier's own certifications.

IGEL supports NHS supply-chain outcomes in two ways. First, as a supplier, IGEL completes the DSPT IT-supplier assertions and can provide the assurance documentation an organisation needs for its A4 evidence - including IGEL's ISO/IEC 27001:2022 certification, which covers the development, maintenance and support of IGEL products and services. Second, as an architecture, IGEL reduces supply-chain risk at the endpoint: with no local OS to manage and no local data to expose, the surface that third-party administrators, managed-service accounts and other suppliers can touch on the device is minimal, and privileged access can be constrained and monitored through the management platform and partner tooling.

Summary

The move to a CAF-aligned, outcome-based DSPT is the most significant change to NHS data-security assurance since 2018, and it raises the bar for endpoints. Organisations now have to show that their controls work - and, increasingly, prove it to an independent auditor by 30 June 2026.

That is good news for the IGEL model. An immutable OS with no local data, a single approved image, centrally enforced configuration, application allow-listing, MFA-backed access and minutes-to-rebuild recovery are not just controls that exist - they are outcomes that are easy to evidence as effective. IGEL helps NHS organisations strengthen their position against the most security-relevant CAF outcomes while reducing cost and keeping clinical workflows fast and simple.

Appendix A - Cyber Essentials v3.3 control mapping

Cyber Essentials no longer grants a DSPT exemption, but Cyber Essentials (and Cyber Essentials Plus) remains a common condition in NHS procurement and a useful, concrete baseline. The table below maps IGEL to the five technical controls in the NCSC's Cyber Essentials: Requirements for IT Infrastructure v3.3 (April 2026).

Control	v3.3 requirement (summary)	How IGEL helps
1. Firewalls	Every in-scope device protected by a correctly configured firewall; block unauthenticated inbound by default; no default admin passwords; software firewall on untrusted networks.	IGEL OS denies unapproved port connections by default and acts as a per-device software firewall wherever the endpoint is used. Configuration is enforced centrally; there are no exposed default endpoint admin credentials.
2. Secure Configuration	Remove unnecessary accounts/software, change default passwords, disable autorun, authenticate users, apply device-locking and credential quality.	A hardened, immutable OS built from a single approved image; unnecessary services and software absent; autorun disabled; users authenticated before access; device locking and credential controls enforced centrally.
3. Security Update Management	All software licensed and supported; auto-update where possible; critical/high-risk fixes (CVSS ≥7) applied within 14 days; remove unsupported software.	Central, scheduled updates via the management platform; IGEL OS updates every 1–2 months with out-of-band critical releases; the App Portal manages application updates; active maintenance keeps devices on a supported OS version, supporting the 14-day rule.
4. User Access Control	Unique-credential authentication before access; MFA where available (always for cloud services); least privilege; separate admin accounts; remove accounts no longer needed.	SSO and MFA via Entra ID, Okta, Imprivata and Ping (and within Citrix/Omnissa /AVD); role-based access control; least privilege via application entitlement; integration with the directory for joiners/movers/leavers so unnecessary access is removed.
5. Malware Protection	Anti-malware active and updated, or application allow-listing restricted by code signing so only approved apps run.	IGEL is a secure by design immutable endpoint operating system. Due to its design it does not require anti-Malware software simplifying management and reducing TCO. IGEL aligns with the application allow-listing route: only sanctioned applications, deployed via the App Portal, can run, and the immutable OS prevents execution of unapproved code. Users cannot install software. Anti-malware can be added for tracking/reporting if required.

> **Note on scope**
>
> Cyber Essentials v3.3 confirms that cloud services and end-user devices cannot be excluded from scope, and that thin clients are explicitly in scope as end-user devices. IGEL endpoints, which can include thin clients, and the cloud/virtual desktops they access, therefore form part of any Cyber Essentials assessment and should be represented in scope documentation.

References

The framework facts in this paper are drawn from the following primary sources (verify the latest versions before publication):

- NCSC - Cyber Essentials: Requirements for IT Infrastructure v3.3 (April 2026)
- NHS England - CAF-aligned Data Security and Protection Toolkit guidance
- DSPT - Independent assessment guides (2025/26, v8)

Related IGEL resources:

- IGEL - NIS2 Directive: Endpoint Security Quick Guide
- IGEL - From Prevention to Governance: NIST CSF 2.0 and SOC 2

Talk to us

Questions about IGEL and the DSPT? Contact NHS@IGEL.com.

To register for trial access, visit igel.com/get-started/try-for-free.