ALLIED ESM

HALO WHITE PAPER

DEFENCE DIGITAL · ITSM SECURITY

Halo ITSM and MOD Secure by Design

An independent assessment of how Halo ITSM aligns to the Ministry of Defence's Secure by Design framework, and what it means for defence procurement teams evaluating ITSM suppliers.

PUBLISHED BY
Allied ESM Ltd

DATE
June 2026

CLASSIFICATION
Public

VERSION
1.0

EXECUTIVE SUMMARY

Halo ITSM and MOD Secure by Design

The Ministry of Defence's Secure by Design (SbD) framework is now a mandatory delivery requirement for all MOD capability teams. It demands that cyber security is embedded throughout a capability's lifecycle, from procurement through to decommission, and that every component in the supply chain can demonstrate appropriate security controls.

As organisations in the defence sector evaluate ITSM platforms, the question of SbD alignment is increasingly central to procurement decisions. This paper provides a structured, evidence-based assessment of how Halo ITSM aligns to each of the seven SbD principles.

> **Key finding:** Halo ITSM holds Cyber Essentials Plus, ISO 27001:2022, SOC 2 Type 2, FedRAMP 20x, and DSPT certification. It is hosted on UK-region AWS infrastructure, commissions independent penetration testing, and has a demonstrable vulnerability management programme. It presents a strong, multi-framework security posture for OFFICIAL-tier MOD use cases and can meaningfully support a capability team's SbD compliance obligations. Allied ESM's delivery consultants hold SC and DV clearances, enabling end-to-end engagement on classified programmes.

5+	7	6 of 7
ACTIVE SECURITY CERTIFICATIONS	SBD PRINCIPLES ASSESSED	PRINCIPLES: STRONG ALIGNMENT

About this paper

This assessment was produced by Allied ESM, a pure-play Halo partner specialising in Halo ITSM implementation and managed services for UK organisations. It draws on Halo's published security documentation, the MOD's Secure by Design guidance at digital.mod.uk, and Allied ESM's implementation experience across regulated sectors.

It is intended to support procurement teams, Senior Responsible Owners (SROs), and security architects who are evaluating Halo ITSM as a defence capability component. It is not a formal security accreditation and does not replace the organisation's own supply chain risk assessment.

Scope

This paper focuses on **HaloITSM** delivered as a cloud-hosted SaaS solution on AWS. Where relevant, notes on Halo's on-premise deployment option are included. The assessment addresses OFFICIAL-classification use cases. Customers processing OFFICIAL SENSITIVE or above should request supplementary documentation from Halo directly via trust.usehalo.com.

BACKGROUND

What is MOD Secure by Design?

Secure by Design is the Ministry of Defence's mandatory cyber security framework for all defence capabilities. Published and maintained by the Defence Digital directorate, it requires that cyber security is designed into a capability from the outset, not bolted on at the end of a programme.

It applies to the full CADMID/T lifecycle (Concept, Assessment, Demonstration, Manufacture, In-Service, and Disposal) and to all defence capabilities, including networks, applications, platforms, and third-party services that handle or transmit Defence data.

MOD policy requirement

"Cyber security must be embedded throughout the lifecycle of every capability. Secure by Design should be used at all stages, to understand cyber risks and implement appropriate mitigations."

Source: digital.mod.uk/policy-rules-standards-and-guidance/secure-by-design

The Seven Principles

SbD is structured around seven principles that capability teams, and their supply chains, are expected to address and evidence throughout the lifecycle:

1 Understand and define context

Know what your capability does, what data it processes, and who it interacts with.

2 Plan the security activities

Define the right security activities for your capability's size, complexity, and risk profile.

3 Implement continuous risk management

Make cyber security risk management an ongoing process throughout the lifecycle.

4 Define security controls

Identify and implement proportionate controls, or use existing approved patterns.

5 Engage and manage the supply chain

Understand supply chain risks. Ensure suppliers can evidence appropriate security.

6 Assure, verify and test

Gain security assurance, testing, and validation throughout the capability's lifecycle.

7 Plan the through-life approach

Continuously monitor and improve security from deployment through to decommission.

The following section assesses Halo ITSM's alignment to each of these principles.

SUPPLIER PROFILE

Halo's Security Posture

Before assessing alignment to the SbD principles, it is useful to understand Halo's baseline security posture. Halo Service Solutions publishes its security position at usehalo.com/security and maintains a trust portal at trust.usehalo.com.

Certifications and Compliance

Cyber Essentials Plus (certified 2025 and 2026)

The independently verified, hands-on-tested tier of the UK government's cyber security standard. An external assessor verifies controls through technical testing, making it significantly more rigorous than self-assessment. Certificates for 2025 and 2026 are available from the trust portal.

ISO 27001:2022 (certified)

Current edition of the international information security management standard, covering annual risk assessment, information classification, supplier management, and continual improvement. The 2025 certificate is downloadable from the trust portal.

SOC 2 Type 2 and SOC 3 (2024 and 2025)

Independently audited assurance covering security, availability, and confidentiality over a sustained period. Halo holds 2024 and 2025 SOC 2 Type 2 reports, a Bridge Letter for continuity, and a SOC 3 available without NDA.

FedRAMP 20x (Authorization Letter)

US federal cloud security framework rooted in NIST SP 800-53 Rev 5. Halo holds a FedRAMP 20x Authorization Letter. NIST 800-53 controls map closely to the NCSC's 14 Cloud Security Principles, providing strong additional assurance for defence procurement teams.

DSPT Certificate 2026-2027

UK NHS and health sector mandatory data security standard, assessed by NHS England. Confirms alignment with UK government data security requirements across health and public sector use cases.

AWS Infrastructure (London region)

All instances hosted on AWS (ISO 27001, SOC 2, and PCI DSS certified). Six global regions including London (eu-west-2). UK data residency is available and should be confirmed contractually for MOD deployments.

Penetration Testing

Halo commissions independent penetration testing of both its web application and mobile application. Web Application and Mobile Application pen test reports are available on request via the trust portal at trust.usehalo.com. This addresses one of the most common evidence gaps raised during supply chain assurance for defence deployments.

Vulnerability Management

Halo operates a published Vulnerability Disclosure Statement and demonstrated active CVE response in 2025, including coordinated disclosure and customer notification within 48 hours for critical/high severity findings. Patches are delivered on a fortnightly release cycle, with emergency patching available for critical vulnerabilities.

> Halo's security posture is materially stronger than many ITSM vendors of equivalent scale. Cyber Essentials Plus, ISO 27001:2022, SOC 2 Type 2, FedRAMP 20x, and DSPT together represent a multi-framework security posture that significantly exceeds the baseline expected for a supply chain component in an MOD OFFICIAL-tier capability. The next section maps this posture to the seven SbD principles.

ASSESSMENT

Alignment to Secure by Design Principles

1 · Understand and define context

● STRONG ALIGNMENT

This principle requires capability teams to understand what their system does, what data it processes, and how it connects to other systems. Halo ITSM directly supports this through its Asset Management module, Service Catalogue, and integration with Virima for IT asset discovery and CMDB mapping. Teams can use Halo to document their capability context, map data flows through service records, and maintain a current picture of their IT estate, all of which feed into a SbD context definition.

As a *supplier*, Halo publishes clear documentation of its own data handling, infrastructure, and integration points, enabling the deploying team to incorporate Halo accurately into their context definition.

2 · Plan the security activities

◐ MODERATE ALIGNMENT

SbD requires capability teams to plan proportionate security activities (threat assessments, risk reviews, security testing schedules) and track them through the lifecycle. Halo's Project Management and Change Management modules provide a structured way to plan and track activities, including security tasks. However, Halo does not provide defence-specific security planning templates or SbD-specific workflow automation out of the box. Allied ESM's implementation service includes configuration of Halo's project and change modules to align with the organisation's SbD activity plan.

3 · Implement continuous risk management

● STRONG ALIGNMENT

This is one of the clearest areas of alignment. Continuous risk management is exactly the operational mode that ITSM platforms are designed to support. Halo's Incident Management, Problem Management, and Change Management modules, used together, provide a structured, auditable way to identify, log, prioritise, escalate, and close cyber security risks. Risks can be raised as incidents or problems, linked to change records, and tracked through to resolution with full audit trails.

Halo also applies continuous risk management to its own platform through its ISMS, which includes an annual risk assessment and treatment plan, and a continuous improvement programme. This provides assurance that the platform itself is being managed to a known risk posture.

4 · Define security controls

● STRONG ALIGNMENT

Halo supports a comprehensive set of security controls at the platform level. All communications are encrypted via HTTPS/TLS 1.2 or higher with HSTS active. Role-based access control is enforced across all modules. Native integrations with Microsoft Entra ID and Okta enable SSO, MFA enforcement, and conditional access policies, bringing Halo into alignment with an organisation's wider identity and access management architecture.

Data is encrypted in transit and at rest. AWS infrastructure provides additional controls including network isolation, DDoS protection, and physical security. Halo's role-based code repository access and QA process for every release also constitute controls on the software supply chain itself.

5 · Engage and manage the supply chain

● STRONG ALIGNMENT

This principle is most directly relevant when evaluating Halo as a supply chain component. The SbD framework requires capability teams to understand and evidence the security posture of their suppliers. Halo's certification stack (Cyber Essentials Plus, ISO 27001:2022, SOC 2 Type 2, FedRAMP 20x, and DSPT) substantially exceeds the evidence that a standard MOD supply chain risk assessment would require for a commercial SaaS ITSM platform at OFFICIAL classification.

The breadth of certification is particularly notable. Cyber Essentials Plus is the externally tested tier of the UK government's own standard. SOC 2 Type 2 provides sustained independent assurance. FedRAMP 20x (rooted in NIST SP 800-53 Rev 5) demonstrates alignment with US federal security requirements, a framework that maps closely to NCSC's 14 Cloud Security Principles. Together, these certifications provide multi-framework, independently verified assurance across the key control domains a defence capability team would need to evidence.

Halo's published Vulnerability Disclosure Statement, active CVE response programme, independently commissioned penetration testing, and trust portal (trust.usehalo.com) provide the transparency and evidence access expected of a responsible defence supply chain component. Halo also maintains awareness of its own sub-supplier security (AWS, third-party integrations) through its ISMS supplier management process.

6 · Assure, verify and test

● STRONG ALIGNMENT

Every Halo release passes a structured QA process covering functionality, performance, configuration, and stability before deployment. SOC 2 Type 2 compliance involves sustained, independent third-party auditing, with both 2024 and 2025 reports available via the trust portal. ISO 27001:2022 requires regular internal audits of the ISMS.

Halo commissions independent penetration testing of both its web application and mobile application. Reports are available on request via trust.usehalo.com. This, combined with the continuous monitoring model embedded in FedRAMP 20x and the external technical verification required for Cyber Essentials Plus, means Halo's assurance posture spans automated controls monitoring, independent audit, and hands-on technical testing.

7 · Plan the through-life approach

● STRONG ALIGNMENT

Halo's fortnightly release cycle, delivering security patches, platform updates, and new capabilities on a predictable cadence, demonstrates a mature through-life security management approach. Customers always run the latest version; there is no version fragmentation and no forklift upgrade risk.

Halo's active CVE monitoring, coordinated disclosure programme, and published security news page (updated in 2025 with responses to three separate CVEs) show that the through-life security process is operational, not just documented. The ISMS includes annual review cycles aligned to the ISO 27001 continual improvement model.

Summary Assessment

6 of 7 principles: strong alignment

Principles 1, 3, 4, 5, 6, and 7: Halo's platform capabilities and multi-framework security posture directly support compliance.

1 of 7 principles: moderate alignment

Principle 2: Halo provides the building blocks for security activity planning but defence-specific workflow configuration is recommended.

FOR PROCUREMENT TEAMS

Key Considerations for Defence Deployments

Halo's security posture is credible for OFFICIAL-tier MOD use cases. The following table identifies the specific considerations procurement teams should address during supplier assurance and contract negotiation.

CONSIDERATION	DETAIL	RECOMMENDED ACTION
UK data residency	Halo operates a London AWS region but also has five other global regions. Data residency is not enforced by default.	Confirm UK data residency contractually. Specify eu-west-2 (London) as the required hosting region.
Penetration testing	Halo commissions independent web application and mobile application penetration tests. Reports are available via the trust portal (trust.usehalo.com) under NDA.	Request the most recent Web Application and Mobile Application pen test reports via the trust portal ahead of supply chain assurance sign-off.
HMG data classification	Halo does not explicitly reference HMG Government Security Classifications (OFFICIAL / OFFICIAL SENSITIVE).	Request a written statement from Halo confirming the highest classification of data their platform can handle under current controls.
NCSC Cloud Security Principles	Halo does not publish a mapping to the NCSC's 14 Cloud Security Principles.	Request or commission a mapping from Halo as part of the supply chain assurance process. Allied ESM can produce this mapping on behalf of the deploying organisation where required.
G-Cloud listing	Halo is listed on the Crown Commercial Service G-Cloud framework. This gives MOD and public sector organisations a streamlined, pre-approved procurement route with reduced commercial due diligence requirements.	Procure Halo through G-Cloud to take advantage of the pre-agreed framework terms and accelerate the procurement timeline.
On-premise option	Halo offers an on-premise deployment option for customers who cannot use cloud hosting.	For higher-classification requirements, evaluate on-premise deployment. Allied ESM can advise on the security controls applicable to on-premise instances.

Allied ESM: Defence-Ready Delivery

Selecting a capable ITSM platform is only part of the equation. Successful delivery in a defence environment requires consultants who understand both the platform and the operating context. Allied ESM's Halo-certified delivery team includes personnel holding SC (Security Check) and DV (Developed Vetting) clearances, enabling engagement across the full range of classified programme environments without the delay of sourcing separately vetted resource.

Allied ESM also holds Cyber Essentials certification, meaning that as your implementation partner, Allied ESM itself satisfies the supply chain security requirements that the SbD framework places on your organisation.

PURE-PLAY HALO PARTNER

Allied ESM is 100% focused on Halo.

We are one of a small number of pure-play Halo ITSM partners globally. Every consultant, every project, every support call is built exclusively around Halo, no competing platforms, no divided loyalties.

Allied ESM holds Cyber Essentials certification and our Halo-certified delivery consultants include personnel with SC (Security Check) and DV (Developed Vetting) clearances. For defence sector clients, this means you can engage Allied ESM across the full spectrum of classified programme environments without needing to separately source cleared ITSM resource.

WEBSITE
alliedesm.com

EMAIL
info@alliedesm.com

REGISTERED IN ENGLAND
Company No. 16274973

ADDRESS
3rd Floor, 86-90 Paul Street, London
EC2A 4NE