ARMIS®

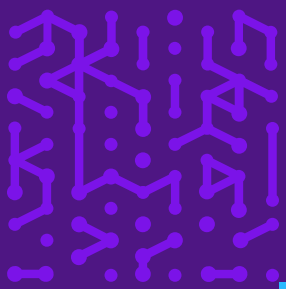
WHITE PAPER

How Comprehensive Cybersecurity Simplifies Compliance with the Cyber Assessment Framework (CAF)-aligned Data Security and Protection Toolkit (DSPT)

Overview

In the NHS, a cyber attack could lead to compromised medical records or personal information, disruptions of essential medical equipment or technology, and even delay life-saving procedures and treatments. Information security is critical to maintaining essential services and upholding the trust and safety of patient care. The UK National Cyber Security Centre (NCSC) has developed the Cyber Assessment Framework (CAF) to support organizations responsible for critical services—including healthcare— in evaluating and enhancing cybersecurity resilience. NHS England and the National Data Guardian have released a joint statement describing changes to the Data Security and Protection Toolkit (DSPT) to be phased out and replaced by the National Cyber Security Centre's Cyber Assessment Framework (CAF).

As cyber threats to healthcare systems continue to evolve, CAF-aligned DSPT offers NHS Trusts, Integrated care boards, and healthcare providers a structured approach to understanding, assessing, and improving their cyber defense posture. This white paper outlines the core principles of the CAF and demonstrates how Armis Centrix™ enables healthcare organizations to align with CAF's requirements, safeguarding critical healthcare infrastructure from an expanding range of attack surfaces and cyber threats.



Introduction to the UK National Cybersecurity Center (NCSC) Cyber Assessment Framework (CAF)

The Cyber Assessment Framework (CAF) by the NCSC is a standardized, risk-based approach designed to help organizations delivering essential services—including healthcare, utilities, and telecommunications—establish and maintain robust cybersecurity practices. In September 2024, the Data Security and Protection Toolkit (DSPT) adopted CAF as its basis for cyber security and information governance assurance. According to the NHS, this is driven by a desire for good decision-making, not just box-ticking compliance, a culture of evaluation and improvement, and enabling organizations to remain current with new security measures to manage new threats and risks. CAF-aligned DSPT covers essential cybersecurity principles across governance, risk management, and protective measures, enabling organizations to assess and enhance resilience against cyber threats.

Objectives of the Cyber Assessment Framework

The CAF is structured to support organizations in:

Understanding their cybersecurity maturity levels by assessing risks to critical operations.

Improving resilience through structured control areas and best practices.

Complying with the NIS (Network and Information Systems) Directive, a requirement for organizations providing critical services in the UK.

The framework also aligns with international standards, such as ISO/IEC 27001, providing healthcare organizations with a scalable method for ensuring regulatory and operational compliance.

Core Principles of CAF

CAF outlines four main objectives with fourteen principles (or outcomes) that provide a comprehensive framework for securing critical services. The CAF-aligned DSPT extends the four objectives and includes an additional information governance-focused section: Objective E: Using and Sharing Information Appropriately. Each principle covers specific areas that organizations must assess, such as governance, risk management, and system security.

Objectives and Principles Overview

01 Managing Security Risk (Objective A)

- **A1 Governance:** Establish clear roles and responsibilities for cybersecurity
- **A2 Risk Management:** Identify, assess, and manage risks to critical services
- **A3 Asset Management:** Maintain accurate inventory and manage assets effectively

02 Protecting Against Cyber Attacks (Objective B)

- **B1 Service Protection Policies:** Implement and enforce cybersecurity policies
- **B2 Identity and Access Control:** Manage access to systems and data
- **B3 Data Security:** Secure sensitive data through protection controls
- **B4 System Security:** Protect systems through security configurations and controls
- **B5 Resilience:** Ensure operational continuity through resilience measures

03 Detecting Cyber Security Events (Objective C)

- **C1 Security Monitoring:** Monitor systems for anomalous activity and threats
- **C2 Proactive Security Event Detection:** Implement tools to quickly detect cybersecurity events

04 Minimizing the Impact of Cyber Security Incidents (Objective D)

- **D1 Response and Recovery Planning:** Establish and test incident response plans
- **D2 Lessons Learned:** Develop feedback loops to continuously improve cybersecurity

05 Using and Sharing Information Appropriately (Objective E)

- **E1 Transparency:** Be transparent about how information is used and stored
- **E2 Upholding the Rights of Individuals:** Manage data subject rights, consent, and adhere to regulatory frameworks
- **E3 Using and Sharing Information:** Lawfully and appropriately use and share information for direct care
- **E4 Records Management:** Manage records in accordance with your organization's professional responsibilities and the law

Challenges in Coordinating CAF-Aligned DSPT Adoption for Healthcare

The transition to adopting the Cyber Assessment Framework as the guiding framework for cyber security brings with it additional compliance requirements and the obligation for self-assessment. These new requirements pose an administrative challenge, layered on top of the already lengthy list of regulatory requirements in healthcare. The CAF requires organizations to adopt stringent measures for maintaining cyber resilience, covering aspects such as managing security risks, defending against cyber threats, and recovering from potential attacks.

Healthcare organizations face unique challenges when aligning with the CAF framework:

- **Complexity of Environments:** Healthcare facilities contain a diverse array of medical devices and IoT equipment, creating a broad and complex attack surface.
- **Regulatory Compliance:** Healthcare providers must comply with strict regulations (e.g., GDPR) on top of CAF.
- **Resource Constraints:** Many healthcare organizations lack dedicated cybersecurity teams and resources, making CAF implementation difficult without automation and visibility

How Armis Supports Healthcare Organizations in DSPT-CAF Alignment

Armis Centrix™ is a comprehensive cybersecurity platform that addresses the specific needs of healthcare organizations in aligning with CAF and other frameworks and guidelines. Armis offers real-time visibility, continuous monitoring, and proactive security measures tailored to protect medical and IoT assets, ensuring healthcare organizations can effectively meet CAF requirements.

Supporting CAF's Core Principles with Armis

A1 & A3: Governance & Asset Management

> **Complete Asset Visibility:** Armis provides an up-to-date, real-time, and in-depth inventory of all connected devices, from IT and IoT to medical devices, across the healthcare environment.

> **Detailed Device Profiles:** Each device is profiled based on behavior, manufacturer, and firmware details, allowing healthcare providers to identify and manage assets efficiently.

A2: Risk Management

> **Risk Assessment and Prioritization:** Armis identifies and prioritizes risks across connected devices, enabling healthcare organizations to assess and address threats and risk efficiently.

> **Automated Threat Intelligence:** Leveraging threat intelligence, Armis enables proactive risk management by identifying known vulnerabilities while also connecting the finding to the fix.

B1, B3 & B4: Policy, Data, and System Security

> **Comprehensive Security Policies:** Armis helps enforce security policies across device types and protocols, including medical devices that often lack in-built security controls.

> **Data and System Protection:** Armis protects sensitive data by monitoring device behaviors for anomalies, preventing unauthorized access or data exfiltration.

> **Automated System Hardening:** Through continuous vulnerability monitoring, Armis ensures that medical devices are configured securely and up-to-date with the latest patches.

B2: Identity and Access Management

Access Control: Armis monitors access points across devices and systems, identifying unauthorized access attempts and securing privileged access pathways.

C1 & C2: Security Monitoring and Event Detection

Continuous Monitoring: Armis continuously monitors device activity, providing real-time visibility into anomalies and potential threats.

Behavioral Analytics: By learning normal device behaviors, Armis quickly identifies anomalies that may indicate cyber threats, facilitating rapid event detection and response.

D1 & D2: Incident Response and Improvement

Incident Response Playbooks: Armis assists in developing and automating incident response playbooks tailored to healthcare, reducing response times and mitigating potential impact.

Post-Incident Analysis: After an incident, Armis helps healthcare providers conduct root-cause analysis, providing data to inform and enhance future responses.

Armis and Compliance with the NIS Directive

As the CAF is closely tied to the NIS Directive, healthcare organizations can leverage Armis to ensure compliance with NIS requirements by:

Providing Real-Time Reporting: Armis' reporting features simplify compliance audits, enabling organizations to demonstrate continuous security monitoring and event detection.

Risk-Based Prioritization: Armis ranks threats by risk level, allowing healthcare providers to allocate resources efficiently and prioritize compliance initiatives.

CAF Objective	CAF Principle	Armis Capability	Description
Objective A: Managing Security Risk	A1 Governance	Comprehensive Asset Visibility	Armis provides real-time visibility across all connected assets, including medical, IoT, IT, and OT devices, ensuring governance over all digital assets.
	A2 Risk Management	Continuous Risk Assessment	Armis assesses and prioritizes risks by identifying vulnerabilities and abnormal behaviors, helping organizations manage risk effectively across the device landscape.
	A3 Asset Management	Automated Device Inventory	Armis maintains a real-time, up-to-date inventory of all connected devices, providing accurate asset records for effective asset management.
Objective B: Protecting Against Cyber Attacks	B1 Service Protection Policies	Policy Enforcement	Armis allows healthcare organizations to enforce customized security policies across all devices, including non-traditional devices like medical and IoT assets.
	B2 Identity and Access Control	Access Monitoring	Armis monitors and manages device access controls, identifying unauthorized access attempts and safeguarding against unauthorized access.
	B3 Data Security	Data Protection	Armis protects data in transit and monitors for unauthorized data access or exfiltration from connected devices, enhancing data security across the network.
	B4 System Security	Vulnerability Management	Armis continuously scans for vulnerabilities and alerts on outdated configurations, ensuring devices meet security baselines and are properly hardened.
	B5 Resilience	Device Behavioral Analytics	Armis' behavioral analytics detect and mitigate suspicious activities in real time, bolstering resilience against cyber threats and minimizing operational disruptions.

CAF Objective	CAF Principle	Armis Capability	Description
Objective C: Detecting Cyber Security Events	C1 Security Monitoring	Real-Time Monitoring	Armis continuously monitors connected devices, detecting anomalies or indicators of compromise, providing proactive threat detection across the environment.
	C2 Proactive Security Event Detection	Anomaly Detection	Armis uses machine learning to establish behavioral baselines for each device, identifying deviations and potential threats as soon as they occur.
Objective D: Minimizing the Impact of Cyber Security Incidents	D1 Response and Recovery Planning	Automated Incident Response	Armis enables automated incident response workflows, isolating compromised devices and providing rapid remediation options tailored for healthcare environments.
	D2 Lessons Learned	Post-Incident Analysis	Armis provides forensic insights and analysis after an incident, allowing organizations to continuously improve their security posture and incident response strategies.
Objective E: Using and Sharing Information Correctly	E1 Transparency	Data Protection	Armis supports compliance with data privacy and transparency guidelines, such as the EU General Data Protection Regulation (GDPR).
	E2 Upholding the Rights of Individuals	Internal and External Compliance Reporting	Armis automatically tracks compliance in a single source of truth, demonstrates status in accordance with various frameworks in visual dashboards.
	E3 Using and Sharing Information	Data Protection	Armis manages third-party risk and monitors for patient data or other sensitive personally identifiable information being transmitted, if it is unencrypted, or being shared externally.
	E4 Records Management	Policy Enforcement	Armis manages medical device security and reduces unencrypted PHI transmission to unsanctioned destinations, with automated alerts and policies to contain and manage any anomalies.

Conclusion

Achieving DSPT-CAF Compliance in Healthcare with Armis

Healthcare organizations in the UK face increasing cybersecurity threats, with cybercriminals targeting critical medical infrastructure and patient data. By aligning with DSPT-CAF, healthcare providers can establish a resilient cybersecurity posture.

Armis supports DSPT-CAF alignment across the following areas:

- **Enhanced Security Posture:** Comprehensive visibility and control over all connected devices, ensuring robust protection across the entire attack surface of every asset.
- **Compliance and Standards:** Simplified compliance with detailed reporting and continuous monitoring, making it easier to meet, maintain, and demonstrate adherence to these standards.
- **Improved Cyber Resilience:** Real-time threat detection and response capabilities ensure critical health services remain operational even during cyber incidents.
- **Risk Management:** Prioritize cybersecurity efforts based on risk assessment. Armis provides contextual risk assessment and management, helping allocate resources efficiently to protect the most critical assets.
- **Continuous Improvement:** Armis delivers ongoing updates and intelligence to keep security measures in line with, and ahead of, evolving threats.

Demonstrating adherence to the CAF-aligned DSPT is crucial for the NHS to protect sensitive patient data, ensure the continuity of vital health services, and maintain public trust in its cybersecurity capabilities. Armis delivers the visibility, monitoring, and risk management capabilities needed to achieve CAF compliance, helping healthcare agencies secure critical systems and protect patient safety. With Armis, healthcare providers can not only meet DSPT-CAF requirements but also build a proactive, resilient cybersecurity foundation that enhances patient care and operational integrity.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial