



Supporting NHS CAF Alignment Through **Thales** **Solutions and Expertise**

How Thales Supports the NHS to Implement the Cybersecurity Assessment Framework

What is the Cybersecurity Assessment Framework (CAF)?

The Cybersecurity Assessment Framework (CAF) is the UK National Cyber Security Centre's (NCSC) comprehensive, outcome-based tool for evaluating how effectively organisations – especially those running critical infrastructure or essential services – manage cyber risk. As of 2025, the Data Security and Protection Toolkit (DSPT) is aligned with the Cybersecurity Assessment Framework (CAF). DSPT continues to exist but has evolved to reflect CAF principles, ensuring stronger, outcome-based assessment while retaining familiar NHS processes.

The CAF is structured to guide both self-assessment and independent assurance reviews, helping organisations systematically strengthen their cyber resilience. **Thales offers solutions designed to fill capability gaps and support CAF alignment in ways that complement NHS internal DSPT services.**

The CAF is built around four overarching objectives:

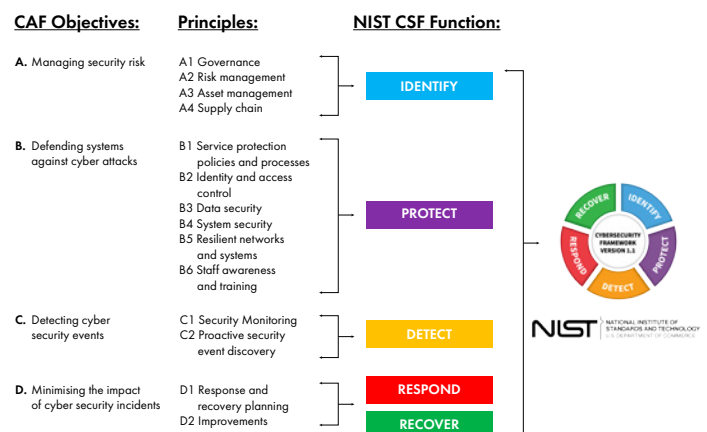
- A - Managing Security Risk
- B - Protecting Against Cyber Attack
- C - Detecting Cyber Security Events
- D - Minimising the Impact of Cybersecurity Incidents

And 14 security principles, including Governance, Risk Management, Asset Management, Incident Response, and Lessons Learned, each

of which is broken down into more specific contributing outcomes and detailed Indicators of Good Practice (IGPs). Each contributing outcome is rated: Not Achieved, Partially Achieved, or Achieved.

How Does the CAF Map to Broader Cybersecurity Frameworks?

The CAF is based on the NIST Cyber Security Framework (CSF) and tailored for UK regulatory regimes, including NIS, GovAssure, and NHS DSPT. Here's how they align:



Why Does the NHS Need to Align with the CAF?

NHS bodies’ primary responsibility is delivering healthcare. Cybersecurity exists to support this mission. Information systems, networks, and data are the foundation of NHS services; failing to protect them can mean failure to deliver essential services and functions.

Ultimately, achieving compliance with the CAF isn’t a burden; it is a way to protect the critical systems that enable patient care.

How Does Thales Help?

Thales can help NHS organisations align with the CAF by addressing cybersecurity requirements and automating security, reducing the burden on security and compliance teams. This is achieved through our three key product arms:



Application Security

Protect applications and APIs at scale in the cloud, on premises, or in hybrid model.



Data Security

Identify, protect, monitor, report, and govern sensitive data across hybrid IT.



Identity & Access Management

Provide seamless, secure and trusted access to applications and digital services

We help NHS organisations cut through the complexity of the CAF so they can focus on delivering patient care, not deciphering compliance documents. We provide the tools, expertise, and support NHS bodies need to meet CAF requirements confidently and efficiently. Our solutions map directly to CAF principles, helping organisations:

- **Monitor activity and audit access** across sensitive data and clinical systems
- **Identify risks and prevent threats** that disrupt healthcare delivery
- **Simplify compliance** through clear frameworks and digestible roadmaps

Function	Category	Thales Capabilities
Govern (GV)	Organizational Context Risk Management Cybersecurity Supply Chain Risk Management Roles, Responsibilities and Authorities Oversight	Data Discovery, Activity Monitoring, Threat Detection

Function	Category	Thales Capabilities
Identity (ID)	Asset Management Risk Management Improvement	Application Network inspection Threat Detection
Protect (PR)	Identity Management, Authentication and Access Awareness and Training Data Security Platform Security Technology Infrastructure Resilience	IdIAM, MFA, Encryption, Tokenisation, Keys Security FIPS 140-3 DDoS, Bad Bot Prevention
Detect (DE)	Continuous Monitoring Adverse Event Analysis	Data and API Activity Monitoring Risk Intelligence
Respond (RS)	Incident Management Incident Analysis Incident Response Reports and Communication Incident Mitigation	DDoS Mitigation, Ransomware Protection Abnormally Behaviour Detection Automation
Recover (RC)	Incident Recovery Plan Incident Recovery Management	Auditing and Automation

Thales can accelerate your progress to full CAF alignment with:

- Ready-made solutions that bridge capability gaps
- Expert integration guidance for Thales products to support CAF alignment
- Reduced workload for stretched IT and security teams
- Seamless integration with NHS frameworks, including ISO 27001, NIST CSF, and Cyber Essentials

Thales brings clarity, structure, and scale to your CAF journey, ensuring your systems stay secure and your services stay operational.

About Thales

Thales is a global leader in cybersecurity, helping the most trusted organizations protect critical applications, data, identities, and software anywhere, at scale. Through Thales’ integrated platforms, customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.



Contact us

For contact information, please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com

