NCSC's Cyber Assessment Framework (CAF): How to comply with Specops

CAF: Quick summary

What's CAF? The NCSC's Cyber Assessment Framework (CAF) helps UK organizations assess and improve cyber resilience.

What does CAF cover? It focuses on identity and access control, protective technology, asset management, and overall risk management.

Is it the same as NCSC's Cyber Essentials? No, Cyber Essentials offers more basic, general guidance. CAF is a more detailed framework.

Who does CAF apply to? UK public sector (e.g. NHS) and critical national infrastructure (CNI) typically need to demonstrate CAF alignment.

Are there fines for non-compliance? No, but non-compliance can lead to situations where organizations are unable to meet the requirements of other regulatory frameworks or contractual obligations, which may have associated penalties.

Why Specops for CAF?

CAF requires broad, phishing-resistant authentication, strong password hygiene, secure recovery, and auditable evidence — Specops delivers all four with AD-native tooling. We typically help organizations who need support with the following:

- Enforcing MFA across all systems and users – not just admins and essential systems
- Moving away from SMS-verification to phishing-resistant MFA factors
- Reviewing active & stale privileged accounts and their access rights
- Blocking weak passwords and scanning for compromised passwords
- Setting up secure, self-service password recovery
- Demonstrating password and MFA compliance to auditors

CAF requirement	Specops solution	How compliance is supported
MFA must be deployed broadly	Specops Secure Access enforces MFA at Windows logon, RDP and VPN, so every user is covered.	CAF expects MFA for all users and applications, including legacy ones. If you have some apps that only rely on AD authentication, then adding MFA to the logon process is vital.
Organizations should move to phishingresistant MFA methods	Specops Secure Access supports stronger, phishing-resistant factors like authenticator apps.	This helps phase out SMS-based MFA, which is vulnerable to exploitation by hackers via SIM-swap attacks and SMS prompt bombing.

CAF requirement	Specops solution	How compliance is supported
Update and strengthen existing password policies	Specops Password Policy continuously scans for breached/weak passwords and blocks them. Makes it simple to enforce length/complexity in line with NCSC guidance.	Passwords policies are key for CAF compliance. Blocking breached passwords and enforcing length are low-cost, high-impact wins — often reducing breach risk faster than big infrastructure projects. If you've followed CAF/NCSC guidance and removed password expiry, it's critical to continuously scan them for breaches.
Control privileged accounts	Specops Password Policy combined with Specops Secure Access lets you enforce stronger MFA policies for admins/privileged accounts and ensure unique, complex admin passwords. Specops Password Auditor can give you a snapshot view of your active (and stale) admin accounts and their passwords.	CAF expects not just limited access, but also strong authentication for privileged accounts, unique complex passwords, and regular review. We can help you demonstrate control to auditors.
Secure recovery methods	Specops uReset offers MFAprotected self-service resets with secure verification flows.	Specops' AD-native controls cut deployment time and avoid the cost of replacing your identity stack while still meeting CAF outcomes. We also support admin and auto enrollments for many strong ID services. Our self-service resets are MFA-gated and logged, so this won't become a CAF failure point.
Document and authentication access policies clearly	All Specops tools have an AD-native approach gives auditors the direct evidence they ask for, where they'd expect to find it.	CAF requires demonstrable controls and audit trails. If the auditor asks for proof of password hygiene, you don't want to be building exports on the spot — Specops gives you that view instantly.