

Ensure UK Cyber Assessment Framework (CAF) Compliance

The UK Cyber Assessment Framework (CAF) is a high-level cybersecurity framework developed by the UK's National Cyber Security Centre (NCSC) to help organizations assess and improve their cybersecurity posture. The CAF is structured around four overall security objectives and 14 cyber security principles or outcomes:

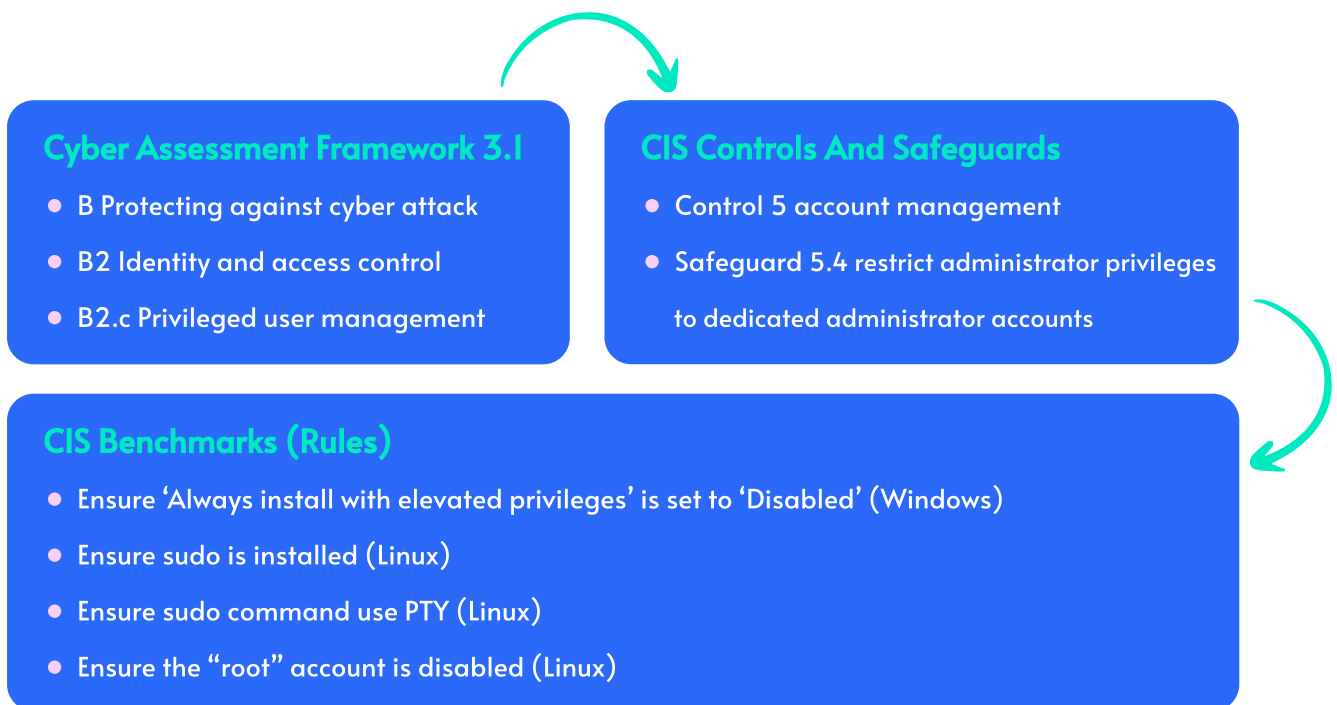
Objectives			
A Managing security risk	B Protecting against cyber attack	C Detecting cyber security events	D Minimising the impact of cyber security incidents
Principles and Outcomes			
A1 Governance	B1 Services protection policies and processes	C1 Security monitoring	D1 Response and recovery planning
A2 Risk management	B2 Identity and access control	C2 Proactive security event discovery	D2 Lessons learned
A3 Asset management	B3 Data security		
A4 Supply chain	B4 System security		
	B5 Resilient networks and systems		
	B6 Staff awareness		

However, CAF does not provide direct implementation details or guidelines, requiring organizations to define specific metrics and actionable remediations on their own in order to ensure compliance. Monitoring CAF compliance can be complex, as organizations need to translate high-level guidelines into actionable security measures. This involves defining the exact parameters to be measured, evaluating configurations, as well as identifying and enacting security upgrades across systems.

On the other side, Remedio, a SaaS leader in configuration security, already provides tools to continuously detect and remediate misconfigurations and deviations from various cyber security frameworks, including CIS Benchmarks, HIPAA, Cyber Essentials, MITRE, NIST 800-53, NIST CSF, PCI, and more.

Remedio now maps CAF outcomes to CIS Benchmark rules, giving users a direct path to translate principles into real-world practices. Since GYTPOL already converts CIS Benchmarks to specific controls (checks and action paths) that can be automated from within the platform, this new mapping extends that same functionality to the Cyber Assessment Framework.

The following diagram illustrates mapping a high-level CAF control to well defined, measurable and fixable CIS Benchmark rules.



This functionality is especially useful on account of Remedio's ability to remediate non-compliant configurations without disrupting operational systems. By checking dependencies, Remedio ensures that remediation actions won't cause downtime or break workflows anywhere downstream. Additionally, Remedio allows organizations to easily revert changes if necessary, providing flexibility and control.

With Remedio's help, organizations can now ensure they meet CAF's high-level objectives across the very granular day-to-day realities of their network and endpoint operations. All with the push of a button and without ever endangering system stability or business continuity.



The screenshot displays the Remedio web interface. On the left is a navigation sidebar with sections for 'Manage' (Misconfiguration, Security Compliance, Compliance Mapper, CIS Compliance, AD GPO, Microsoft Intune, Devices, Action Center, Executive Summary) and 'Settings'. The main content area is titled 'CIS Controls Mapped to Other Compliance Systems' and prompts the user to 'Choose a compliance profile to explore relevant CIS issues'. A 'Filter' panel on the left allows selection of various frameworks like NIST CSF, HIPAA, Cyber Essentials, Cyber Assessment Framework 3.1, and ASD Essential Eight. The main area shows a grid of control cards for 'CIS Controls mapped to Cyber Assessment Framework:3.1'. Each card includes a title, description, progress bar, and a list of affected mapped controls such as 'B2.c - Privileged User Management'.



Key Benefits:

- **Fast Deployment**
Quick Visibility into CAF Compliance.
- **Seamless CAF Implementation**
Direct mapping of CAF principles to specific checks and actions.
- **Proven Security Practices**
Adherence to globally recognized CIS Benchmarks.
- **Automated Monitoring & Remediation**
Instant detection and remediation of misconfigurations and vulnerabilities.
- **Non-Disruptive Remediation**
Ensure fixes never compromise system integrity or business continuity.
- **Reversible Changes**
Remediations can be easily reverted if needed.

About Remedio

Remedio is a first-of-its-kind solution focused on the configuration side of endpoint security. Predicated on principles of automation and prevention, Remedio continuously monitors your devices and systems, detecting unpatched vulnerabilities and insecure configurations. The platform enables proactive and non-disruptive remediation (or reversion) at the push of a button – ensuring safe and strict policy adherence while bolstering operational resilience and business continuity.

With Remedio, it's easy to bring any device or group in line with the standards of your choosing (e.g. CIS, MITRE, HIPAA, NIST, PCI, etc.). Additionally, Remedio helps organizations create and enforce golden image configurations – assuring consistent and secure baselines across all devices.