Ensure UK Cyber Assessment Framework (CAF) Compliance

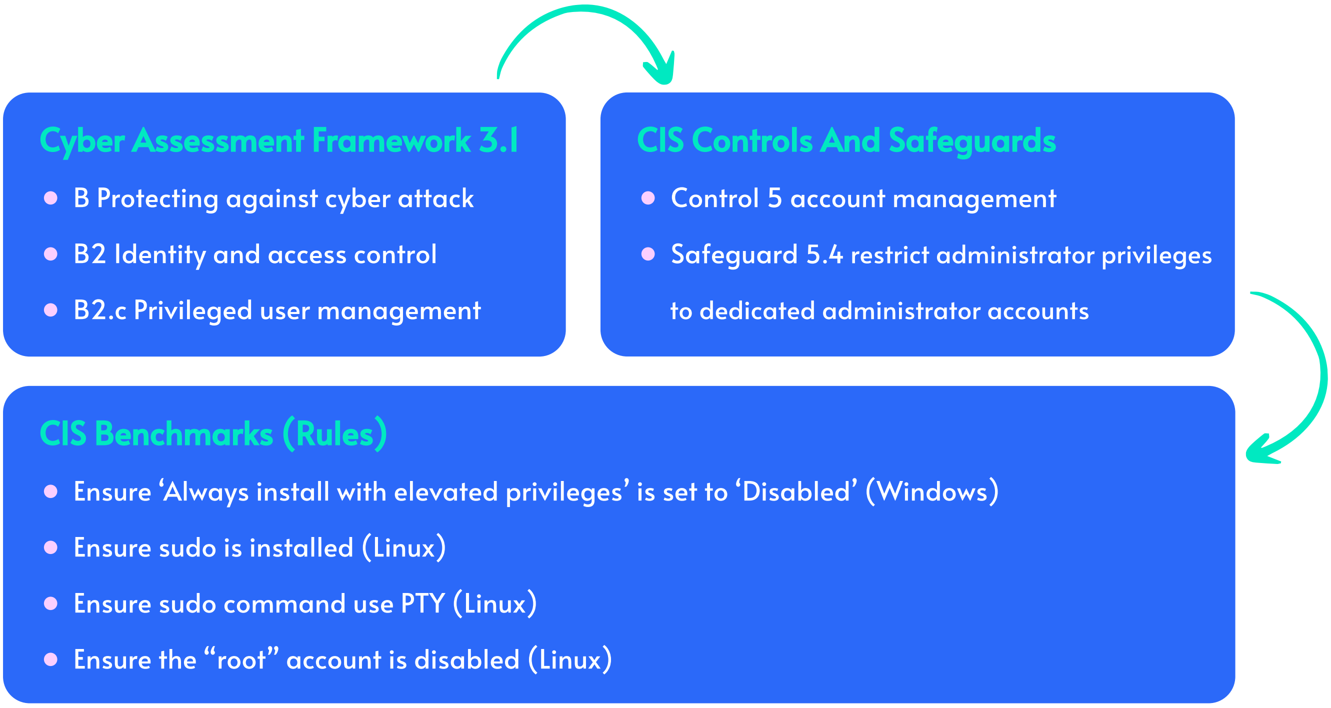
The UK Cyber Assessment Framework (CAF) is a high-level cybersecurity framework developed by the UK's National Cyber Security Centre (NCSC) to help organizations assess and improve their cybersecurity posture. The CAF is structured around four overall security objectives and 14 cyber security principles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

GYTPOL 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.



Cyber Assessment Framework 3.1

- B Protecting against cyber attack
- B2 Identity and access control
- B2.c Privileged user management

CIS Controls And Safeguards

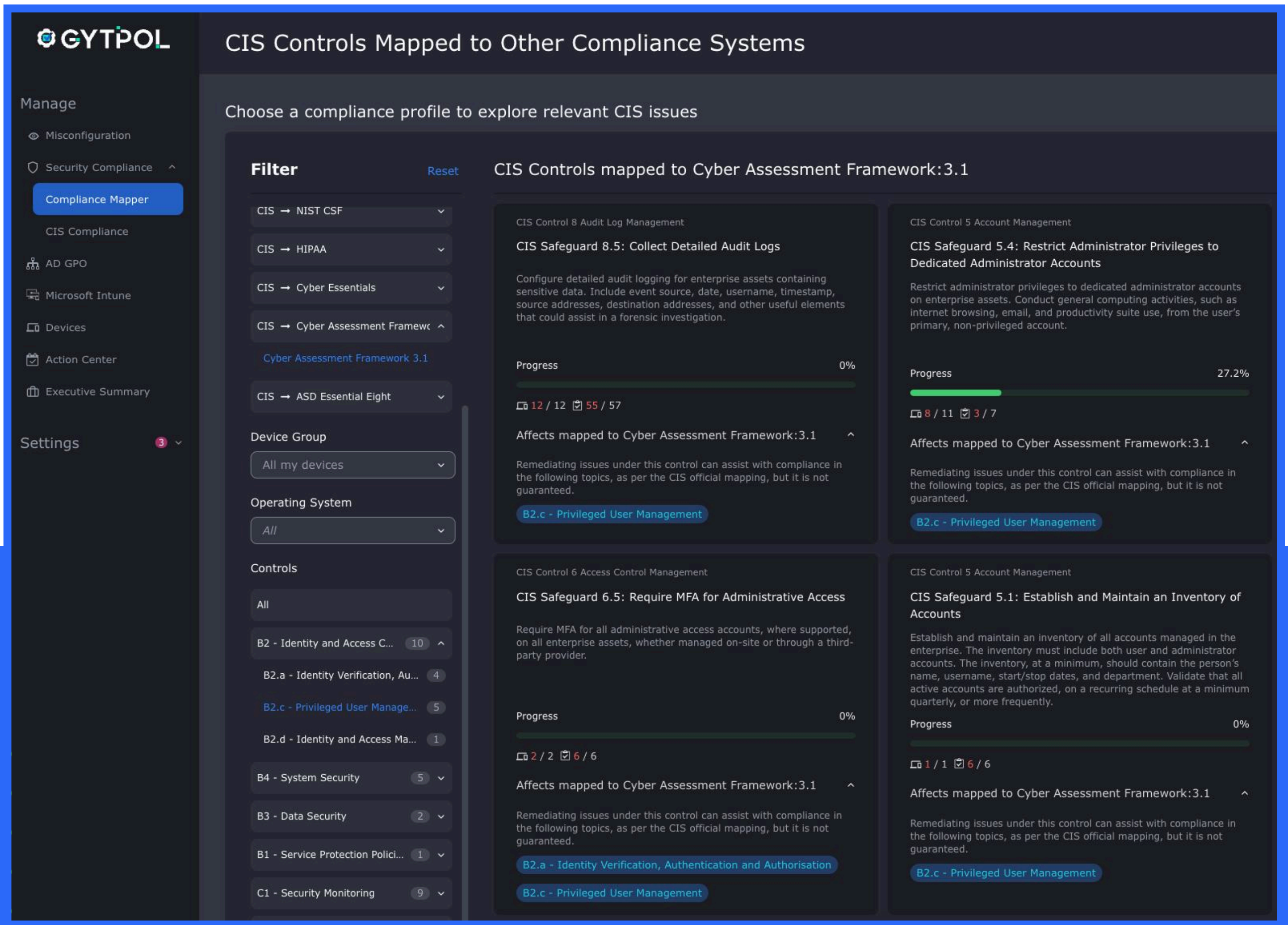
- Control 5 account management
- Safeguard 5.4 restrict administrator privileges to dedicated administrator accounts

CIS Benchmarks (Rules)

- Ensure 'Always install with elevated privileges' is set to 'Disabled' (Windows)
- Ensure sudo is installed (Linux)
- Ensure sudo command use PTY (Linux)
- Ensure the "root" account is disabled (Linux)

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

With GYTPOL'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.



CIS Controls Mapped to Other Compliance Systems

Choose a compliance profile to explore relevant CIS issues

Filter
Reset

CIS → NIST CSF
CIS → HIPAA
CIS → Cyber Essentials
CIS → Cyber Assessment Framewc
Cyber Assessment Framework 3.1
CIS → ASD Essential Eight

Device Group: All my devices

Operating System: All

Controls
All
B2 - Identity and Access C... 10
B2.a - Identity Verification, Au... 4
B2.c - Privileged User Manage... 5
B2.d - Identity and Access Ma... 1
B4 - System Security 5
B3 - Data Security 2
B1 - Service Protection Polici... 1
C1 - Security Monitoring 9

CIS Controls mapped to Cyber Assessment Framework:3.1

CIS Control 8 Audit Log Management

CIS Safeguard 8.5: Collect Detailed Audit Logs

Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.

Progress 0%

12 / 12 55 / 57

Affects mapped to Cyber Assessment Framework:3.1

Remediating issues under this control can assist with compliance in the following topics, as per the CIS official mapping, but it is not guaranteed.

B2.c - Privileged User Management

CIS Control 5 Account Management

CIS Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts

Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

Progress 27.2%

8 / 11 3 / 7

Affects mapped to Cyber Assessment Framework:3.1

Remediating issues under this control can assist with compliance in the following topics, as per the CIS official mapping, but it is not guaranteed.

B2.c - Privileged User Management

CIS Control 6 Access Control Management

CIS Safeguard 6.5: Require MFA for Administrative Access

Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.

Progress 0%

2 / 2 6 / 6

Affects mapped to Cyber Assessment Framework:3.1

Remediating issues under this control can assist with compliance in the following topics, as per the CIS official mapping, but it is not guaranteed.

B2.a - Identity Verification, Authentication and Authorisation

B2.c - Privileged User Management

CIS Control 5 Account Management

CIS Safeguard 5.1: Establish and Maintain an Inventory of Accounts

Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

Progress 0%

1 / 1 6 / 6

Affects mapped to Cyber Assessment Framework:3.1

Remediating issues under this control can assist with compliance in the following topics, as per the CIS official mapping, but it is not guaranteed.

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 GYTPOL

GYTPOL is a first-of-its-kind solution focused on the configuration side of endpoint security. Predicated on principles of automation and prevention, GYTPOL 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 GYTPOL, 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, GYTPOL helps organizations create and enforce golden image configurations — assuring consistent and secure baselines across all devices.