How Cyolo Helps You Achieve Compliance: Cyber Assessment Framework (CAF)

Use this guide to discover how Cyolo can help you comply with the Cyber Assessment Framework (CAF).

INTRODUCTION TO THE CAF

The CAF is a framework created by the National Cyber Security Center (NCSC), the United Kingdom's technical authority on cybersecurity. While specific to the UK, the CAF aligns with other international frameworks such as the NIST Cyber Security Framework (CSF), ISO27001, and the EU's Network and Information Systems Regulations (NIS) Directive.

The CAF was created to help uphold the security and resiliency of organizations within the UK Critical National Infrastructure (CNI), those managing cyber-related risks to public safety, and public sector organizations that support core government functions. However, due to its adaptability and outcome-focused design, the CAF provides useful guidance for organizations across industries and sectors.

OVERVIEW OF CYOLO PRO

Cyolo PRO (Privileged Remote Operations) is an advanced, infrastructure-agnostic secure access solution built to mitigate the risks of remote access to mission-critical assets. Cyolo PRO's decentralized architecture provides exceptional flexibility and can seamlessly adapt to all environments (cloud-connected, on-premise, and offline) without change management.

The CAF is divided into 4 objectives:

Objective A:
Managing security risk

Objective B:
Protecting against cyberattack

Objective C:
Detecting cybersecurity events

Objective D:
Minimising the impact of cybersecurity events

Common challenges Cyolo PRO solves include:

- Ensuring rapid, secure, and safe support and maintenance for the factory floor and OT environments
- Safely connecting third parties to OT environments with no agents or end-user downloads required
- Adding multi-factor authentication (MFA) to legacy systems that do not natively support modern identity authentication
- Securing all access points to mission-critical assets, whether remote or on-premises
  Implementing segmentation, supervision, session recording, and other requirements of industry and regional compliance mandates

CYOLO PRO/CAF ALIGNMENT

See how the capabilities of the Cyolo PRO advanced secure remote access solution align to the objectives and principles of the CAF:

Objective	Principle	Assessment	Indicator of Good Practice	Cyolo Alignment
A	4	a – Supply Chain	All network connections and data sharing with third parties are managed effectively and proportionately.	Cyolo PRO offers capabilities to secure network connections with third parties, providing several simple to implement and proportional controls. These include multi-factor authentication (MFA), session approval, session supervision, and session recording.
B	2	a – Identity Verification, Authentication and Authorisation	Only authorised and individually authenticated users can physically access and logically connect to the networks or information systems on which your essential function depends. The number of authorised users and systems that have access to all your networks and information systems supporting the essential function is limited to the minimum necessary. You use additional authentication mechanisms, such as multi-factor (MFA), for privileged access to all systems that operate or support your essential function. You use additional authentication mechanisms,such as multi-factor (MFA), when you individually authenticate and authorise all remote user access to all your networks and information systems that support your essential function. The list of users and systems with access to networks and systems supporting and delivering the essential function is reviewed on a regular basis, at least every six months.	Cyolo PRO controls all logical connections to essential functions, permitting only strongly authenticated and specifically approved users access to systems. Once access has been granted, sessions can be supervised, observed, and recorded. Cyolo limits access to essential functions to authorised users only (either registered or supervised unregistered users). Cyolo PRO provides a choice of MFA methods to match the needs of the user base. This includes TOTP (time-based one-time passcode), SMS and email. Through integration with external Identity Providers (IdPs), many other MFA mechanisms are supported, including but not limited to passkeys, FIDO2 security keys, biometrics etc. Access to networks and systems supporting essential functions can be easily reviewed in the Cyolo PRO platform, through a combination of policy and identity management controls.

Objective	Principle	Assessment	Indicator of Good Practice	Cyolo Alignment
B	2	b – Device Management	Dedicated devices are used for privileged actions (such as administration or accessing the essential function's network and information systems). These devices are not used for directly browsing the web or accessing email. You either obtain independent and professional assurance of the security of third-party devices or networks before they connect to your systems, or you only allow third-party devices or networks dedicated to supporting your systems to connect. You perform certificate-based device identity management and only allow known devices to access systems necessary for the operation of your essential function.	Cyolo PRO supports the assurance of dedicated devices connecting to your systems through a combination of methods, including but not limited to source IP checks, device certificate checks and posture management. Cyolo PRO supports the application of device certificates to authenticate devices connecting to systems supporting essential functions. This is typically combined with strong user authentication and posture checking, to give the upmost confidence in the user and devices accessing systems supporting essential functions.
B	2	c – Privileged User Management	The issuing of temporary, time-bound rights for privileged user access and / or external third- party support access is in place. Privileged user access rights are regularly reviewed and always updated as part of your joiners, movers and leavers process. All privileged user access to your networks and information systems requires strong authentication, such as multi- factor (MFA) or additional real- time security monitoring. All privileged user activity is routinely reviewed, validated and recorded for offline analysis and investigation.	Cyolo PRO supports time-based and temporary access policies for both internal and third-party privileged users access to systems supporting essential functions. Access requests can be made at the time of connection or in advance and then authorised by appropriately provisioned and authenticated supervisor users. User access rights within the Cyolo PRO platform can be easily reviewed through a comparison of the active policies and group memberships. Cyolo PRO provides a choice of MFA methods to match the needs of the user base. This includes TOTP (time-based one-time passcode), SMS and email. Through integration with external Identity Providers (IdPs), many other MFA mechanisms are supported, including but not limited to passkeys, FIDO2 security keys, biometrics etc. Cyolo PRO enables all privileged activity to be explicitly authorised, observed, recorded, and logged for offline analysis. Recordings of sessions can be exported to external storage devices (e.g. NAS) for long term retention.

Objective	Principle	Assessment	Indicator of Good Practice	Cyolo Alignment
B	2	d – Identity and Access Management	You follow a robust procedure to verify each user and issue the minimum required access rights, and the application of the procedure is regularly audited. All user, device and systems access to the systems supporting the essential function is logged and monitored. You regularly review access logs and correlate this data with other access records and expected activity. Attempts by unauthorised users, devices or systems to connect to the systems supporting the essential function are alerted, promptly assessed and investigated.	Cyolo PRO makes it simple to limit access to specific applications after identity verification has taken place. Each session is also strongly authenticated through a choice of MFA mechanisms, and detailed logging aids with regular system auditing. Cyolo PRO provides detailed logging or all essential function system access, which can be exported or streamed to a log management or SIEM platform. Alternatively, the logs can be analysed within the Cyolo platform. Cyolo PRO access logs are easy to review through manual or automated approaches. Export to a SIEM or Log Management system allows correlation of Cyolo logs with additional system telemetry. Cyolo PRO provides detailed logging of access attempted by unauthorised users, devices and systems connecting to the essential functions. When logs are streamed real-time to a SIEM platform, alerts can be generated to be assessed and investigated.
B	3	a – Understanding Data	You have identified and catalogued who has access to the data important to the operation of the essential function. You maintain a current understanding of the data links used to transmit data that is important to your essential function.	Cyolo PRO simplifies the process of identifying who has access to important operational data by providing a single auditable point through which all access to essential functions must flow. Cyolo PRO provides a single point of access to all systems supporting essential functions for both internal and external users. Cyolo also provides detailed audit logs and options for session recording and supervision. This unified data access makes building an understanding of data links used to transmit data a simple process.

Objective	Principle	Assessment	Indicator of Good Practice	Cyolo Alignment
B	3	d – Data in Transit	You have identified and protected (effectively and proportionately) all the data links that carry data important to the operation of your essential function. You apply appropriate physical and / or technical means to protect data that travels over non-trusted or openly accessible carriers, with justified confidence in the robustness of the protection applied.	Cyolo PRO provides a single point of access to all Essential Functions for both internal and external users. Additionally providing detailed audit logs and options for session recording and supervision. This unified data access makes building an understanding of data links used to transmit data a simple process. Cyolo PRO utilises TLS encryption to protect all data passing over untrusted and openly accessible carriers. In addition, all users connecting via Cyolo will be strongly authenticated with optional additional policy controls (E.g. Posture checking, Geo Location restrictions, IP Source restrictions). For Identity Access Controller (IDAC) to EDGE and EDGE to EDGE connectivity these sessions are further secured via TLS mutual authentication.
B	4	a – Secure by Design	Your networks and information systems are segregated into appropriate security zones, e.g. operational systems for the essential function are segregated in a highly trusted, more secure zone. The networks and information systems supporting your essential function are designed to have simple data flows between components to support effective security monitoring.	Cyolo PRO makes it simple to separate operational systems from other systems into highly secure zones, without impacting usability or serviceability. Cyolo PRO enables simplification and centralisation of data flows between essential functions and other zones. This further enables detailed and timely security monitoring (logging) which can be analysed in a SIEM or log management system.
B	4	b – Secure Configuration	You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented. Only permitted software can be installed and standard users cannot change settings that would impact security or the business operation.	Cyolo PRO allows for all administration changes and configurations to be closely monitored and reported. This includes, but is not limited to session recording, session supervision and observation, and detailed session logging. All changes within the Cyolo platform are logged and recorded for later auditing. Utilizing Cyolo PRO enables supervisors to monitor all changes made to the systems supporting essential functions and confirm no system settings are changed or unauthorised software is installed. Additionally, all software uploaded or downloaded from the systems supporting essential functions can be scanned using leading malware detection engines.

Objective	Principle	Assessment	Indicator of Good Practice	Cyolo Alignment
B	4	c – Secure Management	Your systems and devices supporting the operation of the essential function are only administered or maintained by authorised privileged users from dedicated devices that are technically segregated and secured to the same level as the networks and systems being maintained. You prevent, detect and remove malware or unauthorised software. You use technical, procedural and physical measures as necessary.	Cyolo PRO supports the user of dedicated devices to access systems supporting essential functions. These devices can be strongly authenticated through a combination of methods, including but not limited to source IP, device certificate, and posture checks. Cyolo PRO provides integration with leading malware scanning engines to secure all files uploaded or downloaded from the systems supporting essential functions.
B	5	b – Design for Resilience	Operational systems that support the operation of the essential function are segregated from other business and external systems by appropriate technical and physical means, e.g. separate network and system infrastructure with independent user administration. Internet services are not accessible from operational systems.	Cyolo PRO provides a secure gateway between enterprise systems and systems and networks supporting essential functions, permitting only strongly authenticated users to access permitted applications, optionally enhancing connections with supervision, observation and recording.
B	5	b – Design for Resilience	Extensive monitoring of user activity in relation to the operation of essential functions enables you to detect policy violations and an agreed list of suspicious or undesirable behaviour.	Cyolo PRO provides extensive logging of user activity, specifically in relation to privileged remote operations of systems supporting essential functions. This logging data can be used directly or exported to a SIEM or log management system for further analysis. In addition to this, Cyolo provides live session monitoring and recording capability, allowing for real-time and retrospective detection of suspicious or undesirable behaviour.

ABOUT CYOLO

Cyolo, the access company for the digital enterprise, takes a holistic approach to cybersecurity that aligns closely with the ethos of the CAF. The adaptable, infrastructure-agnostic Cyolo solution is purpose-built to secure, monitor and audit privileged remote connections to critical infrastructure and OT systems.

With Cyolo, organizations like yours can proactively implement the steps highlighted here with no operational disruptions and no changes needed to your existing infrastructure.

Schedule a demo and begin your path to CAF compliance today.

cyolo.io