WHITE PAPER

Ensuring Comprehensive and Proactive Cybersecurity by Aligning with the Cyber Assessment Framework (CAF)

Executive Summary

Balancing the need to manage evolving cyber threats and demonstrating adequate protection and resilience as prescribed in frameworks and guidelines is no easy task. It is particularly important for public sector entities tasked with delivering critical services to strike this delicate balance in order to prevent large-scale disruptions.

The Cyber Assessment Framework (CAF), developed by the UK National Cyber Security Centre (NCSC), provides a standardized method for appraising cyber resilience and enhancing a proactive defense against evolving threats. The CAF emphasizes an outcomes-based approach, pushing beyond mere compliance towards constant improvement. This white paper provides an in-depth analysis of how CAF can serve as a toolkit for organizations aiming to assess cybersecurity maturity, comply with regulatory obligations like the Network and Information Systems (NIS) Directive, and reinforce their defenses.

This document further outlines the main objectives and principles of the CAF, its significance in the public sector, and how technologies like Armis can play a significant role in achieving compliance and enhancing cyber resilience. It also details how each principle can offer a clear, actionable roadmap for handling cyber issues effectively.

How can Armis support alignment to the Cyber Assessment Framework?

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time. Armis secures Fortune 100, 200, and 500 companies as well as national governments, state and local entities to keep critical infrastructure, economies, and society safe and secure 24/7. Armis is deployed at scale in verticals and industries including manufacturing, transportation, health and medical, federal, national, state and local governments, critical infrastructure, higher education, financial services, retail, telecommunications and media, information technology, and many more.

Our platform, Armis Centrix™, is powered by our AI-driven asset intelligence engine that monitors billions of assets world-wide in order to identify cyber risk patterns and behaviors. Armis Centrix™ provides organizations with the ability to build a comprehensive cybersecurity program focused on: asset management and security, vulnerability and security finding prioritization and remediation, OT/ICS security, medical device security, and exposure early warnings.

Overview of the Cyber Assessment Framework (CAF)

Cybersecurity is a critical priority for public sector organizations entrusted with delivering essential services. A cyberattack in the public sector could compromise sensitive data, disrupt critical infrastructure, and erode public trust. That's why the UK National Cyber Security Centre (NCSC) developed the **Cyber Assessment Framework (CAF)** — a standardized, risk-based approach to evaluating and improving resilience against evolving cyber threats.

Core Objectives and Principles of CAF

The **Cyber Assessment Framework** is underpinned by clear objectives that help organizations assess risks, implement best practices, and manage cyber resilience effectively. Its structure is both sector-agnostic and extensible, making it suitable for diverse public sector entities involved in delivering essential services like utilities, transportation, and local government functions.

Main Objectives of the CAF

Understanding Cybersecurity Maturity: Assess risks specific to critical operations and infrastructure.

Improving Resilience: Establish a framework for adopting structured controls and resilience-focused best practices.

Complying with Standards: Ensure alignment with the **NIS Directive** and internationally accepted standards such as **ISO/IEC 27001**.

Avoiding Tick-Box Compliance: Shift from meeting minimum standards to fostering a culture of ongoing improvement in cybersecurity.

Key Principles of CAF

The CAF is organized into four main objectives, each embodying several principles. These principles enable organizations to assess their resilience against cyber risks and gauge the maturity of their cybersecurity practices.

01 Managing Security Risk (Objective A)

- **Governance** (A1): Establish accountable roles and responsibilities for cybersecurity within your organization.
- **Risk Management** (A2): Identify, evaluate, and manage cybersecurity risks to critical operations.
- **Asset Management** (A3): Maintain an accurate inventory of your IT, IoT, and OT assets.

02 Protecting Against Cyber Attacks (Objective B)

- **Service Protection Policies** (B1): Implement enforceable cybersecurity policies.
- **Identity and Access Control** (B2): Safeguard sensitive systems and data with robust authentication measures.
- **Data Security** (B3): Protect sensitive information through encryption and data access controls.
- **System Security** (B4): Secure systems through configurations, patching, and protective measures.
- **Resilience** (B5): Prepare for the worst with operational continuity plans.

03 Detecting Cyber Security Events (Objective C)

- **Security Monitoring** (C1): Continuously monitor for unusual activity or threats.
- **Proactive Event Detection** (C2): Use tools and technologies to rapidly identify cybersecurity incidents.

04 Minimizing Incident Impact (Objective D)

Response and Recovery Planning (D1): Create and test incident response plans tailored to organizational needs.

Lessons Learned (D2): Conduct post-incident analysis to inform future improvements and reduce vulnerabilities.

These principles provide public sector organizations with a clear, actionable framework for managing cyber resilience.

Why CAF Matters for the Public Sector

Public sector organizations often handle vast amounts of sensitive data and operate vital services where disruptions can have cascading effects on citizens' daily lives. The CAF is critical for ensuring such organizations can identify and manage risks proactively.

While the CAF is a useful benchmark, every environment is different and assessments against the CAF need to be conducted intelligently. For example, it may be impossible to apply multi-factor authentication to some Operational Technology, but other compensating controls (such as physical access controls, secure remote access mechanisms, security monitoring, network segmentation etc.) might achieve a similar impact and meet the overall spirit of the Contributing Outcome.

Although the CAF is a valuable guideline, it's critical to remember that every environment has its unique characteristics and requires a mindful evaluation against the CAF. In certain cases, multi-factor authentication for some Operational Technology or medical devices may not be feasible. However, using the guidelines set out by the framework, you can still leverage alternative controls like fortified remote access methods, vigilant security supervision, and network segmentation. The benefit of a framework, rather than strict regulatory requirements, is to leverage the goals and ideals to suit your specific environment and technology infrastructure in the most effective way to achieve the outcomes.

Benefits of Implementing CAF

- **Proactive Risk Reduction:** Helps uncover vulnerabilities before they become threats.
- **Regulatory Preparedness:** Positions organizations to comply with the NIS Directive and other regulatory requirements.
- **Operational Continuity:** Enhances the capacity to respond to and recover from disruptions.
- **Improved Public Confidence:** Demonstrates commitment to data security and safeguarding critical services.

ⓘ By adopting the CAF principles now, public sector organizations can implement robust cybersecurity defenses before regulations mandate adherence, thereby avoiding costly penalties, reputational damage, or service outages.

Addressing CAF Objectives with Armis

Armis provides a cutting-edge cybersecurity platform that helps public sector organizations align with the CAF, ensuring both compliance and enhanced cyber resilience. Below, we outline how Armis supports key CAF principles:

A1 & A3: Governance & Asset Management

- **Complete Asset Visibility:** Gain real-time, up-to-date inventory of all devices across IT, IoT, and OT environments.
- **Comprehensive Device Profiles:** Understand each device's behavior, firmware version, and configuration for effective management.

A2: Risk Management

- **Threat Prioritization:** Identify vulnerabilities and related risks across all connected devices.
- **Proactive Threat Intel:** Stay ahead of emerging threats with automated intelligence integration.

B1, B3 & B4: Cybersecurity Policies, Data & System Security

Policy Enforcement: Implement and enforce consistent security policies across diverse devices and ecosystems.

Data Protection: Secure sensitive data by detecting anomalies in device behavior.

System Hardening: Monitor vulnerabilities in real time and ensure your systems are always up-to-date.

B2: Identity and Access Management

Access Control: Identify unauthorized access and secure privileged pathways across connected devices.

C1 & C2: Security Monitoring and Detection

Constant Monitoring: Monitor all device activity continuously to detect and mitigate threats in real time.

Behavioral Analytics: Identify suspicious activity through machine-learning-based behavior models.

D1 & D2: Incident Response and Continuous Improvement

Automated Playbooks: Customize and automate incident response plans to reduce reaction time and improve containment.

Post-Incident Analysis: Facilitate root-cause analysis to refine cyber defense strategies.

By leveraging Armis, public sector organizations can ensure robust security across all connected infrastructure and meet CAF requirements efficiently.

Proactive Compliance Without the Threat of Regulation

Waiting for mandated cybersecurity regulations is a reactive approach that leaves organizations vulnerable to attacks and penalties. By proactively adopting CAF principles now, public sector organizations can:

- **Establish a Strong Security Foundation** aligned with international and national standards.
- **Ensure Operational Resilience** keeping services running even during incidents.
- **Save Costs and Resources** by mitigating risks before they escalate into larger problems.

CAF isn't just a compliance framework—it's a roadmap to cybersecurity excellence that all public sector organizations should prioritize.

CAF Objective	CAF Principle	Armis Capability	Description
Objective A: Managing Security Risk	A1 Governance	Comprehensive Asset Visibility	Armis provides real-time visibility across all connected assets, including medical, IoT, IT, and OT devices, ensuring governance over all digital assets.
	A2 Risk Management	Continuous Risk Assessment	Armis assesses and prioritizes risks by identifying vulnerabilities and abnormal behaviors, helping organizations manage risk effectively across the device landscape.
	A3 Asset Management	Automated Device Inventory	Armis maintains a real-time, up-to-date inventory of all connected devices, providing accurate asset records for effective asset management.

CAF Objective	CAF Principle	Armis Capability	Description
Objective B: Protecting Against Cyber Attacks	B1 Service Protection Policies	Policy Enforcement	Armis allows organizations to enforce customized security policies across all devices, including non-traditional devices like medical and IoT assets.
	B2 Identity and Access Control	Access Monitoring	Armis monitors and manages device access controls, identifying unauthorized access attempts and safeguarding against unauthorized access.
	B3 Data Security	Data Protection	Armis protects data in transit and monitors for unauthorized data access or exfiltration from connected devices, enhancing data security across the network.
	B4 System Security	Vulnerability Management	Armis continuously scans for vulnerabilities and alerts on outdated configurations, ensuring devices meet security baselines and are properly hardened.
	B5 Resilience	Device Behavioral Analytics	Armis' behavioral analytics detect and mitigate suspicious activities in real time, bolstering resilience against cyber threats and minimizing operational disruptions.
Objective C: Detecting Cyber Security Events	C1 Security Monitoring	Real-Time Monitoring	Armis continuously monitors connected devices, detecting anomalies or indicators of compromise, providing proactive threat detection across the environment.
	C2 Proactive Security Event Detection	Anomaly Detection	Armis uses machine learning to establish behavioral baselines for each device, identifying deviations and potential threats as soon as they occur.
Objective D: Minimizing the Impact of Cyber Security Incidents	D1 Response and Recovery Planning	Automated Incident Response	Armis enables automated incident response workflows, isolating compromised devices and providing rapid remediation options tailored for environments.
	D2 Lessons Learned	Post-Incident Analysis	Armis provides forensic insights and analysis after an incident, allowing organizations to continuously improve their security posture and incident response strategies.

Start Building a Resilient Cybersecurity Future

Meeting the challenges of today's cyber risks requires more than compliance; it demands a proactive, outcomes-based approach. The Cyber Assessment Framework provides public sector organizations with the guidance they need to protect essential services and sensitive data.

Armis complements the CAF principles by providing unparalleled visibility, security monitoring, and incident response capabilities for connected devices across IT, IoT, and OT environments. It empowers public sector organizations to align with the CAF, safeguard critical infrastructure, and build the trust of the communities they serve.

Learn how Armis can help your organization align with CAF and strengthen your cybersecurity resilience. Contact us today for a demo!

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial