

The UK National Cyber Security Centre Cyber Assessment Framework:

An approach to a successful implementation

1. The UK National Cyber Security Centre Cyber Assessment Framework 4.0

Since the UK National Cyber Security Centre (NCSC) introduced the Cyber Assessment Framework (CAF) in 2018, critical national infrastructure (CNI) operators and essential service providers have used it to better understand and manage cyber risk. Subsequently, the UK's approach to cyber security has matured, with greater emphasis on resilience across critical sectors. In response, the NCSC has updated the framework through CAF 4.0.

1.1 The evolving regulatory and threat landscape

The need for stronger cyber resilience is increasingly reflected in UK policy, regulation and proposed legislation. The Cyber Security and Resilience Bill is expected to broaden the scope beyond traditional critical national infrastructure, bringing a wider range of digital service providers and other organisations that are vital to the UK economy. These organisations are likely to be expected to use the NCSC CAF to demonstrate stronger security and resilience outcomes.

Meeting these expectations will require more than a compliance-led approach. Organisations will need to show a higher level of cyber security maturity, supported by stronger governance, clearer accountability and a more proactive approach to managing cyber risk.

At the same time, sophisticated threat actors, including state-sponsored groups, continue to increase the scale and sophistication of their operations by targeting supply chains for systemic compromise and launching ransomware campaigns across sectors and their suppliers. These attacks affect critical infrastructure and the wider technology ecosystem, reinforcing the need for a more preventive and resilient approach.

1.2 NCSC CAF 4.0 raises the bar for resilience

The CAF 4.0 raises the bar for cyber security maturity by emphasising informed risk management and continuous assessment of the evolving threat landscape. It requires organisations to understand their core services and supply chain dependencies, while also strengthening third-party oversight, adopting a whole-system and Zero Trust approach, and improving their ability to detect and respond to threats proactively.

Palo Alto Networks supports these goals by helping organisations manage security risks and protect against, detect and minimise the impact of cyber incidents. Our integrated visibility across network, endpoint, identity and cloud environments helps security teams reduce residual cybersecurity risk and strengthen resilience across critical services.

This white paper explores the benefits of the CAF and shows how Palo Alto Networks capabilities and products align with and support CAF guidance.

NCSC CAF 4.0

Objective	Principle
A. Managing Security Risk	A1 - Governance A2 - Risk Management A3 - Asset Management A4 - Supply Chain
B. Protecting against cyber attack	B1 - Service Protection Policies, Processes & Procedures B2 - Identity & Access Control B3 - Data Security B4 - System Security B5 - Resilient Networks & Systems B6 - Staff Awareness & Training
C. Detect Cyber Security Events	C1 - Security Monitoring C2 - Threat Hunting (new)
D. Minimising the impact of a cyber security incident	D1 - Response & Recovery Planning D2 - Lessons Learnt

Figure 1: [NCSC CAF 4.0](#)

The following section explores the practical considerations involved in delivering the CAF principles, highlighting key outcomes and additional guidance from the NCSC to support successful adoption and maximise return on investment in people, processes and technology.

1.4 Objective A: Managing Security Risk

Effective risk management requires a dynamic approach that extends beyond the physical perimeter to include the digital supply chain and hosting agreements, supported by clear shared-responsibility models.

Assessment starts with establishing a strong baseline grounded in the organisation's mission and objectives. A clear understanding of normal operations helps organisations identify anomalies, protect critical services and respond more effectively when conditions change. A critical step in achieving this outcome is identifying the organisation's digital estate, including an inventory of its assets - hardware, software, virtual assets and services - their locations, connectivity and interactions. This asset inventory and service topology provide the foundation for CAF-aligned transformation.

Establishing this baseline is not a one-time activity. Ongoing maintenance and validation through a managed change process are essential to sustaining it over time.

1.5 Objective B: Protecting Against Cyberattack

Following the identification and classification of the cyber estate into sanctioned, tolerated and unsanctioned categories, the focus should shift to delivering an effective Zero Trust implementation. This phase requires segmenting applications, workflows, services, users and privileges, then applying actionable policies consistently across the organisation, together with the processes required to enforce them.

By integrating the NCSC's secure-by-design and Zero Trust principles, organisations can systematically reduce their exposed attack surface without disrupting essential business operations.

1.6 Objective C: Detecting Cyber Security Events

Building a resilient digital infrastructure requires more than prevention alone. It also calls for automated response capabilities that help minimise impact when incidents occur.

As adversaries continue to refine their tactics, techniques and procedures, often using AI to increase the speed and scale of their campaigns, organisations need detection and response models that operate at machine speed. By using highly integrated security orchestration and automation, organisations can improve their ability to contain suspected breaches before they escalate into business-critical events.

1.7 Objective D: Minimising the Impact of Cyber Security Incidents

When a cybersecurity incident occurs, swift and decisive action is essential to minimise disruption, preserve operational effectiveness and reduce business losses.

Effective cyber incident response plans are critical to reducing impact and shortening recovery time. To support prompt detection, containment and response during a crisis, these plans must be developed, rehearsed and ready for immediate execution. Key elements of this preparation include:

1. establishing a clear chain of command and aligning decision-making authority with the recovery strategy
2. designing a digital architecture that enables rapid containment of business-critical services through segmentation, while preserving unaffected areas of business operations

Taken together, these measures help organisations limit the impact of incidents, accelerate coordinated response and minimise business disruption. Incident response planning and exercises, such as NCSC Exercise in a Box and other cyber range exercises, are important control measures that help staff practise response procedures under realistic conditions.

1.8 Key enablers for success

Cyber adversaries continuously adapt their tactics, techniques and procedures, and organisations need to keep pace by updating the processes they use to detect, respond to and protect their digital environments. This creates additional pressure as they work to maintain the required security posture, particularly when resources and processes alone are not agile or scalable enough to meet the challenge.

To address this, organisations need automated, integrated, prevention-first capabilities that protect systems, users and devices regardless of location. Palo Alto Networks supports successful implementation through six enablers aligned with the CAF's four overarching objectives. These are mapped below.

Objective	Principles	Network & Access Security	Cloud & AI Security	Endpoint & Security Operations	Identity Security	Incident Response & Threat Intelligence
A. Managing security risk	A1. Governance	✓	✓	✓	✓	✓
	A2. Risk management	✓	✓	✓	✓	✓
	A3. Asset Management	✓	✓	✓		
	A4. Supply chain	✓	✓		✓	✓
B. Protecting against cyber attack	B1. Service Protection Policies and Processes	✓	✓	✓		
	B2. Identity and access control	✓	✓	✓	✓	
	B3. Data security	✓			✓	
	B4. System security	✓	✓	✓	✓	
	B5. Resilient networks and systems	✓	✓	✓	✓	
	B6. Staff awareness and training	✓				✓
C. Detecting cyber security events	C1. Security Monitoring	✓	✓	✓	✓	✓
	C2. Proactive security event discovery	✓	✓	✓	✓	✓
D. Minimising the impact of cyber security incidents	D1. Response and recovery planning					✓
	D2. Lessons learned					✓

2. How Palo Alto Networks support these six enablers

2.1 Build full visibility across the environment

Successful implementation of the CAF depends on full visibility across the environment, including workflows, locations, services, custom applications and supply chain dependencies. Palo Alto Networks capabilities help organisations visualise and apply policies consistently across the full estate, including network, cloud, third-party services and endpoint data flows. They identify thousands of applications, services and behaviours, with options for tailored definitions. This supports accurate traffic mapping and a clearer definition of sanctioned, tolerated and unsanctioned activity.

It is also important to understand the impact of a breach from both technical and business perspectives. Palo Alto Networks Unit 42 services help organisations develop and exercise incident response plans that align with business continuity plans, strengthening cyber resilience. A tested incident response plan helps minimise the business impact of a cyber incident.

2.2 Reduce exposure across the attack surface

Discovering the organisation's digital ecosystem and applying the right policies helps identify residual risk. The same technologies can then be used to enforce cyber risk management policies across a broad attack surface.

Effective policy enforcement requires centralised, end-to-end management and reporting. This helps organisations monitor and harden their environment proactively, reduce the operational burden of maintaining security posture, and support real-time action to prevent incidents.

2.3 Reduce known and unknown exploits earlier

Implementing robust controls after minimising the attack surface significantly reduces the likelihood that threats will escalate into full-scale security incidents. By applying Zero Trust principles, broader cyber security controls and robust detection capabilities can identify the bypass of controls with automated responses to help block known exploits and identify anomalies that may indicate unknown attacks or emerging threats.

Palo Alto Networks use a multilayered approach to automated prevention across the digital environment, extending beyond the network. Our detection engines combine signature-based methods with behavioural analytics, machine learning and AI to deliver strong protection across critical points in an organisation's environment.

2.4 Turn intelligence into practical action

Palo Alto Networks products and consulting services provide specialist resources that support ongoing analysis, security posture reporting and strategic guidance. They help organisations monitor third-party capabilities and present compliance views dynamically through dashboards that can be used at different levels of the organisation.

Several Unit 42 services can be combined to support these objectives, including Managed Detection and Response (MDR) and Threat Analyst Services. Together, they enable organisations to apply global threat intelligence in ways that are relevant to their environment and priorities.

2.5 Strengthen vulnerability management across operations and development

In the context of vulnerability management, Palo Alto Networks helps organisations address two key areas:

- **Operational vulnerabilities** – vulnerabilities an organisation inherits through the use of services and software, including the configuration of commercial off-the-shelf (COTS) services and solutions
- **Development vulnerabilities** – vulnerabilities introduced during internal development cycles for specific capabilities and workflows

The NCSC also provides guidance in this area through its Secure Design Principles and Secure Development and Deployment Principles.

2.6 Sustain readiness through operations, training and response

An organisation can deploy highly capable technologies and services, but they must be configured, optimised and maintained to continue delivering the protections. This also includes ensuring staff are trained to make full use of these preventive capabilities.

Palo Alto Networks Unit 42 offers proactive services ranging from strategic advisory to cloud security and AI security assessments, Zero Trust advisory, incident response planning, tabletop exercises and vulnerability analysis. In addition, Unit 42 has been assured by the NCSC to the Enhanced Level of the Cyber Incident Response (CIR) Scheme and provides CREST cyber incident response and digital forensics services to support organisations if an incident occurs. Follow-on transition services can also help organisations strengthen resilience, improve recovery outcomes and reduce the likelihood of repeat incidents.

2.7 How can the Palo Alto Networks platform help?

Palo Alto Networks helps organisations move from framework alignment to operational resilience. By bringing together integrated platforms, threat intelligence and expert services, we help security teams reduce complexity, strengthen protection and respond with greater speed and confidence.

Aligned to the CAF, our solutions support organisations across the full lifecycle of cyber resilience—from understanding risk and reducing exposure to improving detection, accelerating response and strengthening recovery. The table below maps the Palo Alto Networks solutions and services that can help organisations put CAF principles into practice while reducing current and future risk.

Key Enablers	Network & Access Security	Cloud & AI Security	Endpoint & Security Operations	Identity Security	Incident Response & Threat Intelligence
Visibility	✓	✓	✓	✓	✓
Reduce the Attack Surface	✓	✓	✓	✓	✓
Prevent Known & Unknown Exploits	✓	✓	✓	✓	
Threat Intelligence	✓	✓	✓	✓	✓
Vulnerability Management	✓	✓	✓	✓	
Configuration Management, Operations & Training		✓	✓		✓

Further information on how Palo Alto Networks' capabilities can assist an organisation's CAF implementation, as identified in the table above, is below:

Or contact us today or take our Cloud security assessment

Cloud security assessment



22 Bishopsgate
London
EC2N 4BQ

www.paloaltonetworks.com

© 2026 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.