InfoBrief sponsored by Akamai | October 2024

NCSC Cyber Assessment Framework (CAF)

Achieving CAF Outcomes in the UK Public Sector with Akamai Security

Ralf Helkenberg
Senior Research Manager,
European Privacy and Data Security

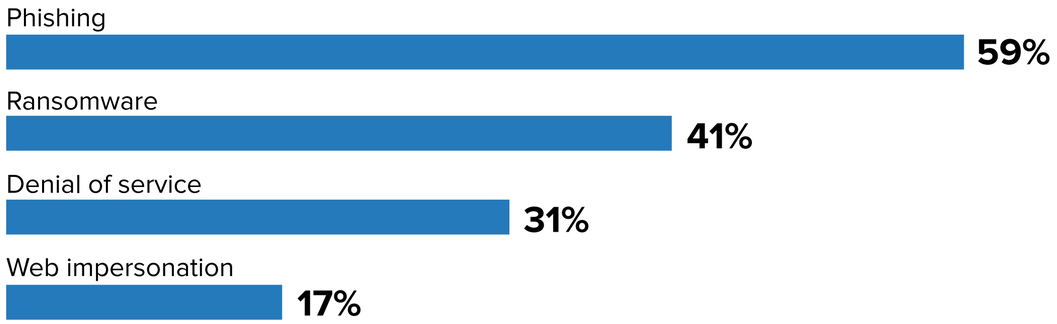
Table of Contents

United Kingdom Public Sector Cybersecurity

What are your organisation's top business priorities for the next 12 months?

Given its critical function in safeguarding critical infrastructure, delivering essential services, and holding sensitive data, the public sector is a prime target for cyberthreats and attacks. Geopolitical conflicts have further influenced this, with nation-state and state-affiliated threat actors intensifying their cyber activities against public entities.

Top security threats UK public sector

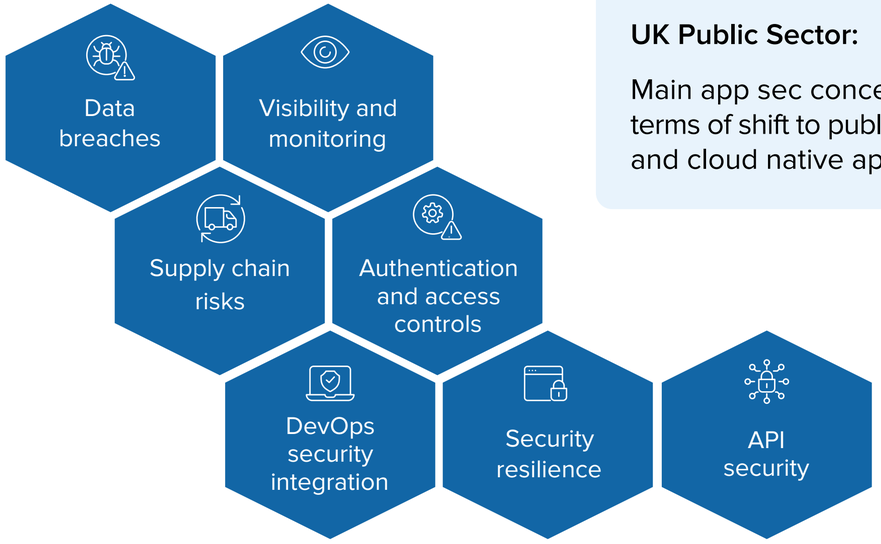


There were more than 1,420 reported incidents of malware, ransomware, and phishing that targeted public bodies in the first half of 2023, according to the Information Commissioner's Office. This was an increase of 855 incidents over the same period in 2022. Councils, NHS hospitals, Manchester Police, and the British Library have all fallen victim to ransomware attacks since September 2023. And DDoS attacks continue to grow, amplified through DDoS-for-hire services and virtual machine bots.

Application security and hybrid cloud ops

Today's public sector IT leaders have numerous options for delivering and managing their applications to create superior digital experiences and unlocking innovative opportunities or public service models. Hybrid, multicloud deployments are becoming the go-to choice for application and API deployment due to their flexibility and scalability.

As application deployment becomes more distributed, so do the security risks that need to be addressed:



UK Public Sector:

Main app sec concerns in terms of shift to public cloud and cloud native apps

Source: IDC EMEA, Digital Transformation and Security, Akamai, September 2023

The State of Cyber Resilience and Zero Trust

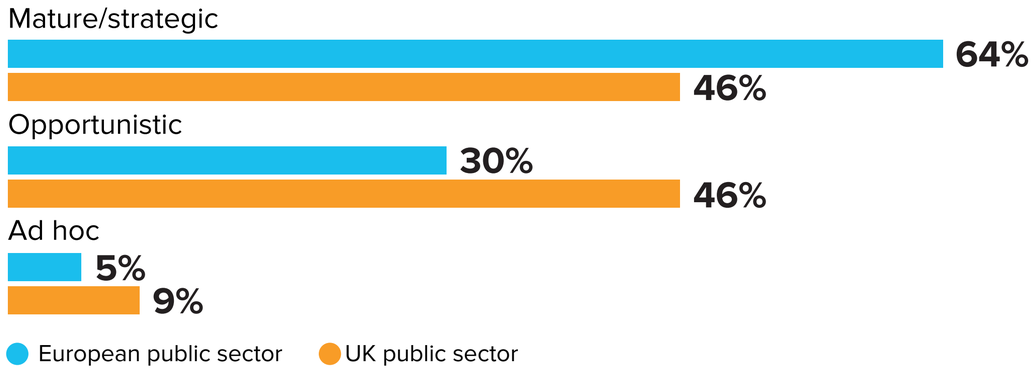
The cyber resilience imperative

Given the increasingly disruptive nature of cyber incidents, there is a heightened focus on resiliency of business IT infrastructure and critical national infrastructure. The UK public sector is behind its European counterparts in prioritizing cyber resilience as a strategic concern, with a defined strategy, goals, and support from senior management.

Zero Trust

Zero Trust principles provide an agile and dynamic security foundation that's resilient to organisational change and provides the flexibility to meet the challenges posed by modern business, workforce, and technology trends. Forty-five percent of public sector organisations have adopted a strategic approach to Zero Trust.

Public sector approach to cyber resilience



Public sector approach to Zero Trust

Top 3 factors driving cyber resilience

- Supporting secure digital transformation
- Reputational impact of security incidents
- Cyberattack caused operational downtime

Top 3 factors driving Zero Trust adoption

- Shift to more proactive security
- Secure hybrid work models
- Security best practice

Source: IDC Security Technologies and Strategies Survey 2024, Europe, May 2024

Source: IDC EMEA, Digital Transformation and Security, Akamai, September 2023

Cyber Assessment Framework — a Tool for Assessing Cyber Resilience

The National Cyber Security Centre (NCSC) developed the Cyber Assessment Framework (CAF) to be sector-agnostic and future-proof.

The CAF provides organisations with a structured approach to assess, achieve, and demonstrate an appropriate level of cyber resilience, especially those:

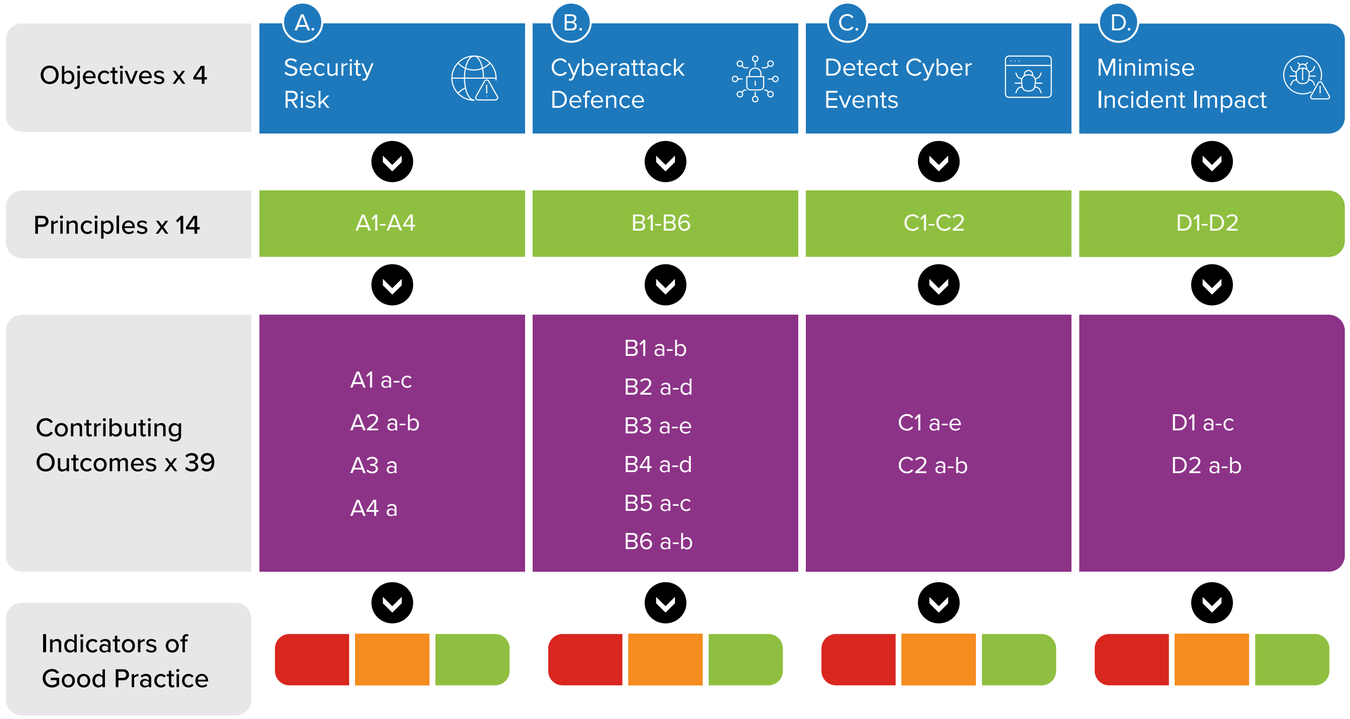
- Subject to the Network and Information Systems (NIS) Regulation
- Within the Critical National Infrastructure (CNI)
- Managing cyber-related risks to public safety
- Public sector organisations that support core government functions

It is applicable to both information technology (IT) and operational technology (OT) environments.

Cyber Assessment Framework in the Public Sector

Adoption was broadened under the UK Government Cyber Security Strategy 2022-2030. With GovAssure introduced in 2023, public sector organisations must undergo an annual security assessment based on the CAF.

The Cyber Assessment Framework is written primarily in terms of outcomes to be achieved rather than a compliance checklist of what needs to be done.



The CAF is built upon a set of 4 objectives and 14 principles, and supported by a series of 39 contributing outcomes, with indicators of good practice (IGPs) utilised to measure success, i.e., whether the contributing outcome is judged achieved, partially, or not achieved.

NCSC Cyber Assessment Framework

CAF Objectives and Principles

- A1. Governance
- A2. Risk management
- A3. Asset management
- A4. Supply chain

- 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

- C1. Security monitoring
- C2. Proactive security event discovery

- D1. Response and recovery planning
- D2. Lessons learned

Benefits of Cyber Assessment Framework

Enhanced Cybersecurity Posture

CAF helps identify gaps in existing security measures and provides recommendations for mitigating risks, thereby bolstering overall cyber resilience.

Standardised Approach

CAF offers a standardised approach to assessing cybersecurity capabilities. This consistency allows organisations to benchmark their security posture against industry best practices.

Measurable Progress

Contributing outcomes with indicators of good practice enables organisations to set realistic goals and track their improvement efforts. It also helps with prioritizing cybersecurity investments and resource allocation.

Regulatory Compliance

CAF aligns with compliance standards, making it a valuable tool for organisations striving to meet legal requirements.

CAF Objective A: Managing Security Risk

Objective A: Appropriate organisational structures, policies and processes are in place to understand, assess, and manage security risks to network and information systems supporting essential functions.

A1 Governance
Principle: The organisation has appropriate management policies processes for the security of network and information systems.

A2 Risk Management
Principle: The organisation identifies, assesses, and understands security risks to networks supporting essential functions, establishing an overall approach to risk management.

A3 Asset Management
Principle: Determination and comprehension of all assets necessary for the operation of essential functions, including data, people, systems, and supporting infrastructure.

A4 Supply Chain
Principle: The organisation understands and manages security risks to networks and information systems arising from dependencies on external suppliers, ensuring implementation of appropriate measures.

Security Measures

While some of the security outcomes within this objective cannot solely be achieved through technology (A1, A2), certain control areas can be supported by security solutions.

Akamai solutions across application, API, infrastructure, and Zero Trust security that can contribute to achieving the following CAF outcomes:

A3 Asset Management

Zero Trust Network Segmentation

Microsegmentation enhances visibility by providing detailed insights into network traffic and asset interactions, while also improving the management and security of network assets through targeted controls and policies.

A4 Supply Chain

Complete API Security

Continuous discovery and visibility into all APIs across applications and endpoints, their risk posture, and with behavioural analysis uncover potential threats and misuse.

JavaScript Supply Chain

Shield websites in real time from JavaScript threats and mitigate client-side script executions with actionable alerts. And enable meeting PCI DSS v4.0 script security compliance requirements.

CAF Objective B: Protecting Against Cyberattacks

Objective B: Proportionate security measures are in place to protect the networks and information systems supporting essential functions from cyberattack.

B1 Service Protection Policies and Processes

B2 Identity and Access Control

Principle: Organisations should have a clear understanding of who or what has authorisation to interact with essential networks and information systems. Users, devices, and systems must undergo appropriate verification, authentication, and authorisation before accessing data or services.

B3 Data Security

B4 System Security

B5 Resilient Networks and Systems

B6 Staff Awareness and Training

Security Measures

Akamai solutions across application, API, infrastructure, and Zero Trust security that can contribute to achieving the following CAF outcomes:

B2 Identity and Access Control

Zero Trust Network Access

Deliver Zero Trust user and device application access with granular and scalable access controls based on real-time signals of threat intelligence, device posture, and user information.

Public Sector Use

Already using

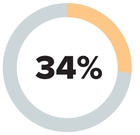
Plan to use

Multifactor Authentication

Extend Zero Trust security for workforce logins to cloud and web applications by leveraging FIDO2-supported multi-factor authentication.

Public Sector Use

Already using



Plan to use

Source: IDC EMEA, Digital Transformation and Security, Akamai, September 2023

CAF Objective B: Protecting Against Cyberattacks

Objective B: Proportionate security measures are in place to protect the networks and information systems supporting essential functions from cyberattack.

B1 Service Protection Policies and Processes

B2 Identity and Access Control

B3 Data Security

B4 System Security
Principle: Protect critical network and information systems and technology from cyberattack. A secure-by-default design approach is crucial. This includes:
- Visibility of cyber risk
- Effective detection of unauthorised attempts to bypass security measures
- Segmentation of network and information systems into appropriate security zones

B5 Resilient Networks and Systems

B6 Staff Awareness and Training

Security Measures

Akamai solutions across application, API, infrastructure, and Zero Trust security that can contribute to achieving the following CAF outcomes:

B4 System Security

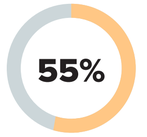
Dynamic DDOS Protection and Network Cloud Firewall
Proactive protection of applications, data centres, and cloud and internet-facing infrastructure from DDoS attacks and malicious traffic.

API Security/Web App Protection
Continuous discovery and visibility into all web applications and APIs, their risk posture, and with behavioural analysis to uncover threats and misuse.

Zero Trust Network Segmentation and DNS Firewall
Protect critical assets by stopping malicious lateral network movement with a granular software-based microsegmentation approach. Protect your network from phishing and malware. A DNS firewall filter and traffic monitor block user and device access to malicious domains.

Public Sector Use

Already using



Plan to use

Source: IDC EMEA, Digital Transformation and Security, Akamai, September 2023

CAF Objective C: Detecting Cybersecurity Events

Objective C: Capabilities exist to ensure security defences remain effective and to detect cybersecurity events affecting, or with the potential to affect, essential functions.

Principle C1: Security Monitoring
Monitor the security status of networks and systems to detect potential security problems and track the ongoing effectiveness of protective security measures.

Principle C2: Proactive Security Event Discovery
Detect anomalous events in relevant network and information systems.

Security Measures

Akamai solutions across application, API, infrastructure, and Zero Trust security that can contribute to achieving the following CAF outcomes:

C1 Security Monitoring

Complete API Security / Web App Protection
Observability with integrated WAF, bot, API, and DDoS security controls to protect web applications against data exfiltration and account takeover, and avoid application downtime.

C2: Proactive Security Event Discovery

Cyberthreat Hunting
Proactive and systematic search for anomalous behaviour and unknown, undetected threats that may have evaded a network's automated defence systems.

Public Sector Cyberthreat Hunting

The government cybersecurity strategy for the public sector emphasises operating a threat hunting capability. Twenty-four percent of public sector respondents have identified this as a top operational security priority.

Source: IDC Security Technologies and Strategies Survey 2024, Europe, May 2024

Guidance on Conforming to the Cyber Assessment Framework

#1

Understanding your needs:

- **Identify essential functions:** Determine the essential functions of your organisation that rely on critical IT systems and data.
- **Prioritise risks:** Evaluate the potential cyberthreats and vulnerabilities associated with these essential functions. This helps prioritise your focus during the assessment.

#2

Self-assessment:

- **CAF:** Use the CAF as a guide to conduct a self-assessment of your organisation's cybersecurity posture. Review each objective, principle, contributing outcome, and IGP.
- **Gather evidence:** Collect evidence to support your assessment. This includes existing policies, procedures, security controls, and incident response plans.

#3

Addressing gaps:

- **Identify areas for improvement:** Based on your self-assessment, identify areas where your organisation fails to meet the CAF objectives and outcomes.
- **Develop action plans:** Create action plans to address the identified gaps and improve your overall cyber resilience. This might involve implementing new security controls, revising policies, or conducting staff training.

#4

Continuous improvement:

- **Regular review and updates:** Continually review your organisation's cybersecurity posture and update your self-assessment as required.
- **Consider external assessment:** While self-assessment is a valuable starting point, consider seeking an external assessment from a qualified security professional for a more comprehensive evaluation.

About the Analyst

Ralf Helkenberg
Senior Research Manager, European Privacy and Data Security

Ralf Helkenberg is a senior research manager with the European security research team, responsible for leading IDC's European Privacy and Data Security research practice. His core research coverage includes the impacts of data protection regulation, such as the GDPR on the technology sector, with key insight into market dynamics, vendor activities in privacy workflow management and data security (including data discovery, DLP, and encryption), end-user trends, and the future of digital trust.

More about Ralf Helkenberg

Message from the Sponsor

Power and protect critical public sector online services

Everything the public sector does online is mission-critical, whether it's national security or securing a database. Akamai works with many of Europe's largest public agencies and has proven security, content delivery, and cloud computing solutions for central citizens; defence and intelligence; regional, local, and education; or critical national infrastructure needs. We back them up with public sector experts and 24/7/365 support.

Build citizen trust through cyber resilience.

Akamai Security for Public Sector

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets.

With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight help IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.), the world's leading tech media, data, and marketing services company.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell, and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC UK
5th Floor, Ealing Cross, 85 Uxbridge Road, London, W5 5TH, United Kingdom
T 44.208.987.7100

@idc | @idc | idc.com