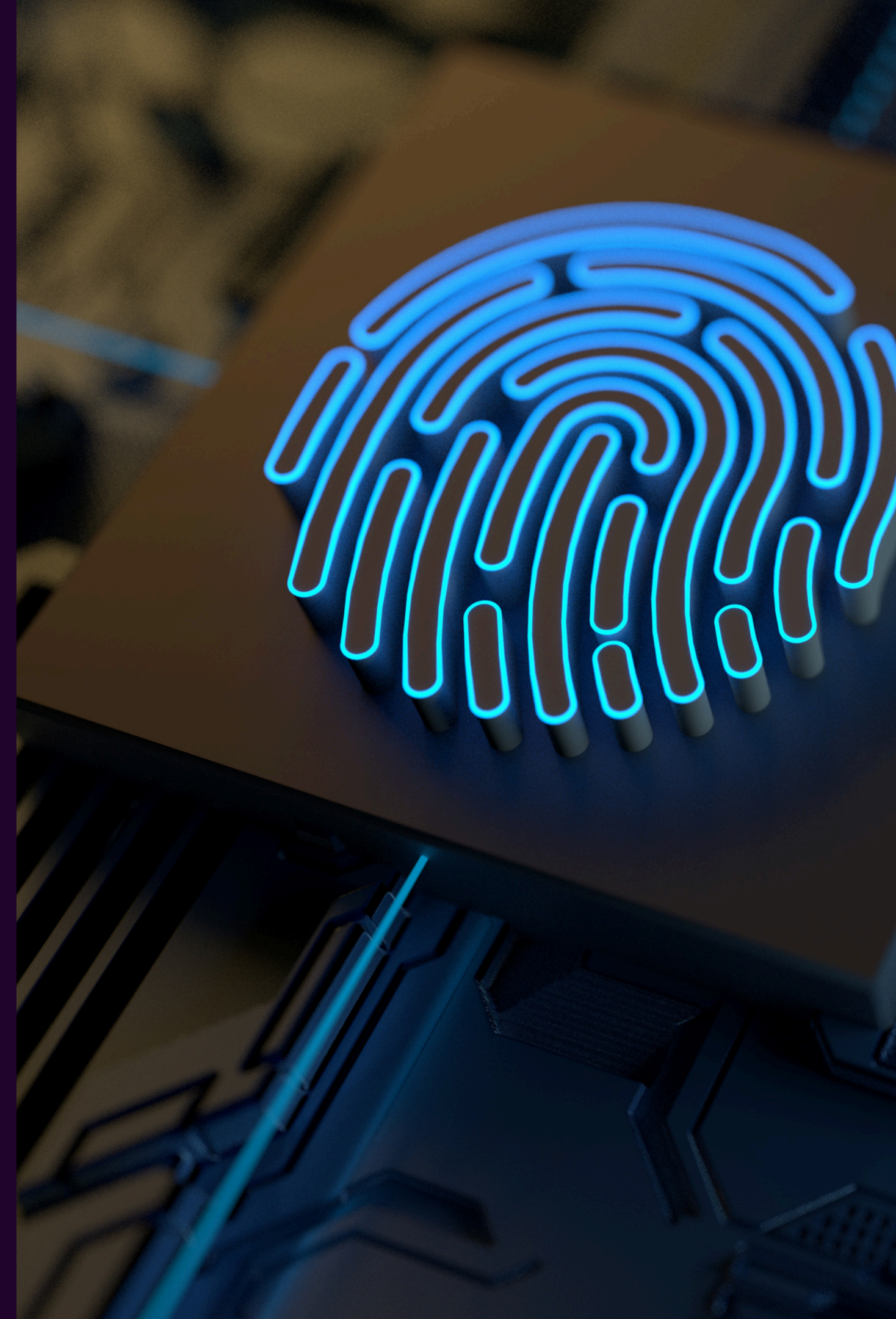




Understanding Cybersecurity Requirements for CNI and Public Sector

Adopting the Cyber Assessment Framework (CAF)





The Cybersecurity Landscape

Cybersecurity is now a central pillar of operational resilience for public sector organisations, as the risks associated with cyber threats continue to escalate. To address these risks, the UK government has laid out specific requirements for cybersecurity, particularly through guidelines established by the National Cyber Security Centre (NCSC).

One key tool is the Cyber Assessment Framework (CAF), designed to help public sector bodies assess and improve their cybersecurity posture. Here, we explore the fundamental cybersecurity requirements and directives issued by the government, focusing on the CAF's structure and significance.

The Role of the NCSC and Cybersecurity in the Public Sector

The NCSC operates as the UK's leading authority on cybersecurity, providing expert guidance, response, and support to mitigate cyber risks across critical sectors. In the public sector, which is a prime target for malicious actors, the NCSC's frameworks help ensure that governmental and public service organisations have robust protection against potential breaches. By adhering to these frameworks, organisations can protect sensitive information, maintain public trust, and ensure continuity of essential services.



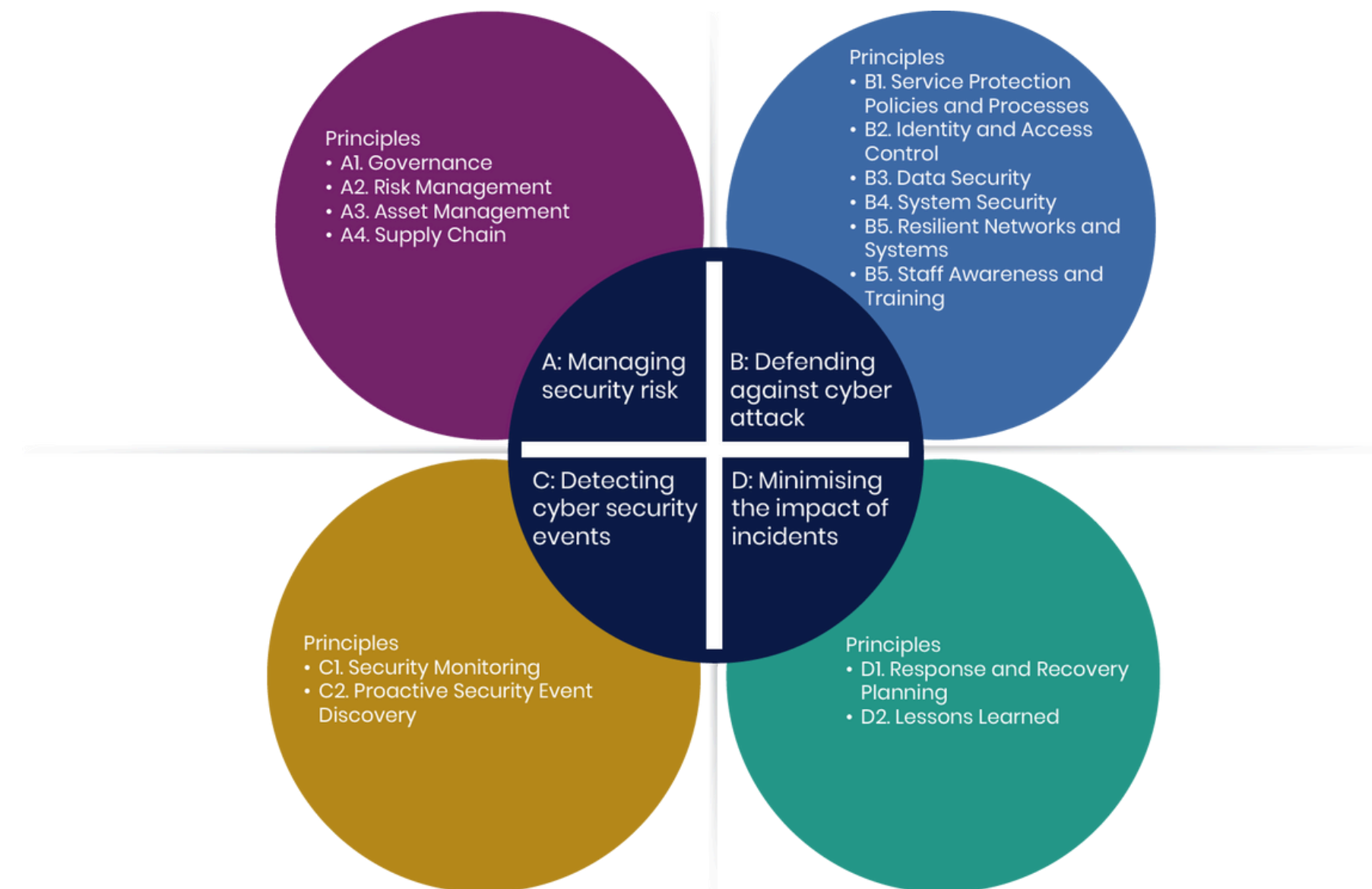
National Cyber
Security Centre

a part of GCHQ



What is the Cyber Assessment Framework (CAF)?

The CAF, developed by the NCSC, offers a structured approach to assessing cybersecurity within organisations that play a critical role in the nation's infrastructure. It is tailored to fit the unique demands of the public sector, covering areas from data protection to resilience and risk management. Its objective is to help organisations identify vulnerabilities, assess risk exposure, and implement effective controls.





Key Objectives of CAF

CAF is centred around four key objectives



1 Managing Security Risk



2 Protecting Against Cyber Attack



3 Detecting Cybersecurity Events



4 Minimising the Impact of Incidents



Key Objectives of the CAF

Managing Security Risk

Effective cybersecurity begins with understanding and managing risk. Public sector organisations are required to have clear policies and procedures for identifying, assessing, and mitigating cybersecurity risks. This includes regular audits, the establishment of risk ownership, and the implementation of risk management practices throughout the organisation

Detecting Cybersecurity Events

Detection is equally vital in cybersecurity. The CAF highlights the need for systems that can effectively identify and log unusual or suspicious activities. These measures ensure that breaches or attempted breaches are recognised quickly, minimising potential damage. Public sector bodies are encouraged to adopt monitoring tools and procedures that can help detect any threat activity within their digital infrastructure.

Protecting Against Cyber Attack

The scope of NIS2 is broader, covering a wider range of sectors and organisations. Entities providing digital services, managed service providers, and critical infrastructure operators are now subject to the regulations. This shift means that even organisations indirectly involved in essential sectors must adhere to NIS2's guidelines, extending protection across the supply chain.

Minimising the Impact of Incidents

No cybersecurity measure is entirely infallible, so the CAF requires that public sector organisations have response plans ready in case of an incident. This objective stresses the importance of effective recovery strategies to minimise service disruptions, manage communications, and ensure data recovery if necessary. Having a well-practised incident response plan reduces the potential long-term impact of a cyberattack.



Cybersecurity Directives for Public Sector and CNI Compliance

Alongside the CAF, several government directives shape the cybersecurity landscape for CNI and the public sector. These are aimed at helping organisations meet their security obligations in line with national security standards:

Mandatory Security Controls

Public sector organisations are required to follow baseline security controls, which include implementing encryption, two-factor authentication, and secure data storage measures.

Data Protection Regulations

Compliance with data protection regulations, such as the General Data Protection Regulation (GDPR), is essential to safeguard citizen data and ensure privacy. The CAF helps align organisations' cybersecurity practices with these regulations,

Incident Reporting and Response

Public sector organisations must have a defined process for incident reporting and response. This includes notifying the relevant authorities, stakeholders, and affected individuals in the event of a data breach or cyber incident

Regular Audits and Assessments

To maintain compliance, public sector entities are expected to undergo regular cybersecurity assessments, using the CAF as a benchmark. These assessments help identify areas for improvement and ensure that organisations remain aligned with evolving cyber threats.



Government's critical functions to be significantly hardened to cyber attack by 2025, with all government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030



The Benefits of CAF for CNI and Public Sector

Using the CAF as a guide, public sector organisations can build a robust cybersecurity framework that offers multiple benefits:

Enhanced Resilience

Public sector organisations are required to follow baseline security controls, which include implementing encryption, two-factor authentication, and secure data storage measures. The scope of this also needs to be extended across all touch points including networking Infrastructure as well as supply chain that can pose a risk to resilience.

Improved Stakeholder Confidence

Compliance with data protection regulations, such as the General Data Protection Regulation (GDPR), is essential to safeguard citizen data and ensure privacy. The CAF helps align organisations' cybersecurity practices with these regulations,

Strategic Risk Management

Public sector and Critical National Infrastructure organisations must have a defined process for incident reporting and response. This includes notifying the relevant authorities, stakeholders, and affected individuals in the event of a data breach or cyber incident.

Risk management is not a one off exercise and needs regular review and assessment as well as included on report and discussions at board level.



The Adoption of digital security measures, is now a key consideration for BEIS and Ofgem given the joint competent authority role as defined in the NIS Regulations.

ofgem



Practical Steps for Improving Cyber Resilience



CAF - Managing Security Risk

Organisations need to understand cyber risks and their ability to handle and manage a cyber attack. Our consultative approach creates a benchmark of your current security strengths and weaknesses. This allows us to prioritise areas for attention in line with organisational goals and priorities overlayed with risk analysis. Approaching cybersecurity is not just a technical issue, our methodology revolves around three key elements, people, process and technology.

A1 - Governance

Having visibility into security posture, data, and processes helps meet governance goals. You cannot achieve governance if you don't have a holistic view of IT, Data, Processes, etc. Add to this the complexity of managing the risks posed by services and applications outside of normal IT boundaries and this can become very challenging. FourNet Assess can help you, providing the insight and intelligence needed to ensure ongoing governance and compliance

A2 - Risk Management

Fournet Assess provides vulnerability scanning on all external systems protected by your firewall as well as vulnerability testing from inside the network. This report highlights vulnerabilities and areas of risk, benchmarking security posture and allowing for organisations to plan investment and adopt appropriate and proportional security controls.

A3 - Asset Management

Organisations must review security Infrastructure and the wider network, identifying assets that could pose a risk to security, for example, unpatched devices and those accessing the network that may pose a risk. FourNet Assess does just this, providing a simple-to-understand report detailing strengths and opportunities for improvement and prioritises the most pressing actions first with a traffic light scoring system.

A4 - Supply Chain

By understanding your internal and external network and controls you will have greater visibility of where the organisation interconnects with your supply chain, allowing you to take proactive steps to mitigate risks from these areas.

Principles

- A1. Governance
- A2. Risk Management
- A3. Asset Management
- A4. Supply Chain

A: Managing security risk



CAF - Defending against Cyber Attack

B1 - Service Protection Policies and Process

Having visibility into security posture, data, and processes helps meet governance goals. You cannot achieve governance if you don't have a holistic view of IT, Data, Processes, etc. Assess helps provide the insight and intelligence needed to ensure ongoing governance and compliance.

B2 - Identity and Access Control

For many organisations visibility is a key challenge, we can help get full visibility of the network and organisation and help to implement proportional controls for verification and access to systems and applications. We offer a range of services including Zero Trust Network Access (ZTNA) and well as Zero Trust Application Access (ZTAA) fully supported by our 24/7 Security Operations Centre.

B3 - Data Security

We can help protect your data where it resides and whilst in transit as well as implementing access control and backup functionality to protect and restore your data, should the worst happen.

B4 - System Security

From Endpoint to Core, our proactive Security Services will be constantly providing proactive support to protect your network and systems. quickly identifying, remediating and protecting you against threats as they emerge. Our solutions can help detect cyber incidents earlier allowing rapid remediation and reducing impact and further risk.

B5 - Resilient Networks and Systems

Assess provides a review of your security Infrastructure and network identifying assets that could pose a risk to your security, for example, unpatched devices and those accessing the network that may pose a risk. With a Cloud First approach for many organisations, additional security challenges can arise across cloud environment, commonly misconfigurations or failed patches than can expose an organisation. These services require continuous review, refinement and control. Proactive threat hunting is also a recommendation, providing additional defence and security, especially against emerging next generation attacks.

B6 - Staff Awareness training

Your security services are only as strong as your weakest link and humans often fall foul creating serious security incidents. With threats changing your people must be a key focus of any security initiative. Its is recommended that organisations not only have a measure of technological risks, but create a human risk register identifying weak areas allowing remedial action and control. We offer a range of services to not only train staff to identify and repel threats, but more importantly to change behaviours to create a culture of security.

Principles

- B1. Service Protection Policies and Processes
- B2. Identity and Access Control
- B3. Data Security
- B4. System Security
- B5. Resilient Networks and Systems
- B5. Staff Awareness and Training



CAF - Detecting Cyber security Events

C1 - Security Monitoring & C2 - Proactive Security Event Discovery

Security monitoring is a vital aspect of the Cyber Assessment Framework (CAF), as it underpins an organisation's ability to detect, respond to, and recover from cyber threats. Continuous monitoring provides visibility into the security posture of systems and networks, enabling early identification of anomalies and potential breaches. This proactive approach reduces the risk of harm to critical assets and supports compliance with regulatory and organisational requirements. To meet CAF principles, organisations should implement robust logging mechanisms, deploy Security Information and Event Management (SIEM) tools, and establish real-time alerting systems to track and analyse security events. Regularly reviewing and updating monitoring processes, conducting threat intelligence analysis, and ensuring that staff are trained to interpret and act on security data are also essential practices for maintaining a resilient cybersecurity environment.

In addition, implementing Zero Trust Network Access (ZTNA) and Zero Trust Application Access (ZTAA) can enhance security monitoring and access controls.

ZTNA enforces strict identity verification for every user and device attempting to access resources, regardless of whether they are inside or outside the network perimeter. This approach limits access to only authorised individuals and devices, reducing the attack surface and mitigating the risk of unauthorised access. Similarly, ZTAA extends these principles to application-level controls, ensuring that users can only access the specific applications and data they are authorised to use. Both ZTNA and ZTAA provide granular visibility into user activity and access patterns, enabling organisations to monitor, detect, and respond to potential threats in real-time.

C: Detecting
cyber security
events

Principles

- C1. Security Monitoring
- C2. Proactive Security Event Discovery



Minimising the Impact of Incidents

Principles

- D1. Response and Recovery Planning
- D2. Lessons Learned

D1 - Response and Recovery Planning

Response and recovery planning is a cornerstone of the Cyber Assessment Framework (CAF), ensuring organisations can effectively manage and recover from cyber incidents while minimising disruption. A well-structured response plan provides clear protocols for detecting, containing, and mitigating threats, while recovery planning ensures business continuity and restoration of normal operations. Organisations can benefit from an internal or external Security Operations Centre (SOC) to monitor threats in real-time and coordinate incident response.

Also Integrating a Security Information and Event Management (SIEM) solution can provide additional support enabling the collection, correlation, and analysis of security data to identify and prioritise threats. Leveraging Security Orchestration, Automation, and Response (SOAR) tools can further enhance incident management by automating routine tasks, streamlining workflows, and facilitating faster, more effective responses. Regularly testing and updating response and recovery plans through simulated exercises ensures that teams remain prepared and processes remain aligned with evolving threats.

However, unless you have undertaken a thorough risk assessment and created and tested a robust Business Continuity plan, the best tools in the industry won't be able to help you recover as quickly as you would like.

D2 - Lessons Learned

Recording lessons learned is a crucial practice under the Cyber Assessment Framework (CAF) as it enables organisations to continuously improve their cybersecurity resilience. By analysing past incidents, organisations can identify weaknesses in their defences, response processes, and recovery strategies, ensuring that similar vulnerabilities are mitigated in the future. This reflective approach fosters a culture of learning and adaptation, essential in the face of evolving cyber threats.

To meet CAF principles, organisations should document key insights from every incident, including root cause analysis, the effectiveness of response measures, and areas for improvement. These findings should be shared with relevant stakeholders, used to update policies, and incorporated into training programmes. Additionally, conducting regular reviews of lessons learned ensures that they remain actionable and relevant, contributing to the organisation's ongoing cybersecurity maturity.



Getting Help With Cybersecurity



Achieving CAF Compliance with FourNet Managed Security

Our managed Security Services, called **Assess**, **Protect** and **Defend** have been built to offer an end to end cyber security solution. Underpinned by our security experts and our staff with the highest levels of security clearance we can help organisations meet the demands of the digital age and CAF requirements.

Below is an overview of how our services map to the principles of the Cyber Assessment Framework

FourNet **Assess**

Managing Security Risk

A1 Governance
A2 Risk Management
A3 Asset Management
A4 Supply Chain

Minimising the Impact of Incidents

D1 Response and Recovery Planning

FourNet **Protect**

Managing Security Risk

A1 Governance
A4 Supply Chain

Defending Against Cyber Attack

B1 Service protection, Policies & Process
B2 Identity & Access Control
B3 Data Security
B4 System Security
B5 Resilient Networks & System
B6 Staff Awareness and Training

Detecting Cyber Security Events

C1 Security Monitoring
C2 Proactive Event Discovery

FourNet **Defend**

Managing Security Risk

A4 Supply Chain

Defending Against Cyber Attack

B2 Identity & Access Control
B3 Data Security
B4 System Security
B5 Resilient Networks & System

Detecting Cyber Security Events

C1 Security Monitoring
C2 Proactive Event Discovery

Minimising the Impact of Incidents

D1 Response and Recovery Planning
D2 Lessons Learned

How we can Help



FourNet Assess

Organisations need to understand cyber risks and their ability to handle and manage a cyber attack. Our consultative approach creates a benchmark of your current security strengths and weaknesses. This allows us to prioritise areas for attention in line with organisational goals and priorities overlaid with risk analysis. Approaching cybersecurity not just as technical issue, our methodology revolves around three key elements, people, process and technology.

FourNet Protect

FourNet Protect provides next generation security services including mail protection, advanced Endpoint Detection and Response (EDR) and Security Access Service Edge (SASE) to protect applications and services. Wherever the network is accessed, and however the perimeter moves, FourNet Protect ensures users are safe and secure.

FourNet Defend

No matter what technology solutions are in place an attacker only needs to be successful once to compromise the network and organisation. With FourNet Defend our team of experienced cybersecurity professionals work in unison with internal teams, utilising advanced tools and methodologies to swiftly detect, analyse, and mitigate threats. With years of experience and fifteen languages, our team of industry award-winning experts are by your side.

Defence in Depth

Defence in depth is essential in cybersecurity as it provides multiple layers of protection, reducing the risk of breaches if one layer is compromised. In the UK, where cyber threats are constantly evolving, this layered approach helps organisations detect and respond to attacks more effectively, minimising the impact on business continuity and national security. By combining controls like firewalls, encryption, and access management, defence in depth strengthens overall resilience, fostering greater trust in systems and services.

Delivering a Zero Trust Strategy

In today's threat landscape, traditional perimeter-based security is no longer sufficient. Zero Trust is a security model that assumes no trust and requires continuous verification of all entities. This approach significantly reduces the risk of breaches, ensuring robust protection for your sensitive data and systems.

Discover more about ZTNA in our quick guide to Zero Trust

Learn More





About **FourNet**


FourNet works with some of the most secure, critical and commercially driven organisations in the UK.

Our expertise is in transitioning and integrating complex, legacy systems to deliver the latest communication, collaboration, and contact centre capabilities.

We provide the knowledge and technical expertise to help our customers achieve their digital transformation and customer experience goals. FourNet's Intelligent Managed Service frees up time for our customers to focus on running their business, without having to worry about their communications infrastructure.

Our Infrastructure Partners





Easy To Procure











Discover



ANTENNA is designed and built to support all UK Critical National Infrastructure (CNI) providers.

Designated itself as Critical National Infrastructure, ANTENNA is a highly secure, reliable, resilient service which enables organisations delivering critical services to UK citizens to achieve digital advantage through innovative and agile digital transformation.

Secure by design, ANTENNA offers CNI providers a trusted, reliable, highly secure service which helps deliver the UK government cyber security, digital and data, and national resilience strategies.



The ANTENNA programme was formed because we wanted to share our ICT infrastructure with other Departments in a way that's not been achieved before. The approach taken by the Cabinet Office meant that by utilising existing equipment, we could reduce costs, improve service and provide expert support to Departments in a way that they've not experienced previously.

Malcolm Coates MBE
Director of ICT, Cabinet Office





Further Reading

FourNet

Navigating NIS and NIS2 Regulations: What Businesses Need to Know

5 - Getting it Wrong - Sanctions

Sanctions for Violations of NIS 2

The NIS 2 Directive requires E.U. member states to establish provisions for imposing fines on entities that breach Article 21 concerning risk management measures and Article 23 relating to reporting obligations for major security incidents. Additionally, the directive outlines maximum benchmarks for the maximum range of these fines:

Essential Entities Administrative fines of up to 10 million EUR or 2% of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher	Important Entities Administrative fines of up to 7 million EUR or 1.4% of the total worldwide annual turnover in the preceding financial year of the undertaking to which the important entity belongs, whichever is higher
--	---

“ The NIS 2 Directive requires essential and important entities to take appropriate and proportionate technical, operational and organisational action to manage the risks posed to the security of the network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimize the impact of incidents on the recipients of their services and on other services. **(Article 21(7) NIS 2 Directive)** ”



FourNet

Quick Guide to Zero Trust Network Access (ZTNA)

Considerations When Looking to Implement ZTNA

When considering the implementation of ZTNA, organisations should evaluate the following:

01 Overview of ZTNA	04 Assessment of Current Infrastructure	05 Cloud and Hybrid Environment Compatibility	06 User Experience	Scalability
02 Benefits of ZTNA	03 How ZTNA fits into your environment	04 Policy Management	05 Vendor Evaluation	





Thank you

Discover how we can help you achieve secure outcome and Compliance

[Get in touch](#)

0845 055 6366

hello@fournet.co.uk