NCSC CAF Compliance with Microsoft and Bridewell

National Cyber Security Centre

Achieve and demonstrate compliance with the NCSC's Cyber Assessment Framework (CAF) when using Microsoft security with the guidance, support and services of a leading cyber security services provider. With the Government Cyber Security Strategy making it clear that the CAF is foundational, this framework is only becoming more critical for more organisations.

Member of Microsoft Intelligent Security Association

Microsoft Security

Microsoft Verified Managed XDR Solution

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Threat Protection

Understanding the CAF

The CAF was introduced in 2018, primarily to help meet the needs of the UK's Network and Information Security regulations, and initially covered Critical National Infrastructure organisations. Its use has since expanded and it is now recommended for any organisation as a 'systematic and comprehensive approach for assessing which cyber risks to essential functions are being managed by the organisation responsible for them'.

It is structured around objectives and principles, and is outcome-focused rather than prescriptive. The four objectives are:

- **A Managing security risk**
- **B Protecting against cyber attack**
- **C Detecting cyber security events**
- **D Minimising the impact of cyber security incidents.**

14 Principles are spread across the four objectives, supported by a further 39 contributing outcomes that support achievement of the outcomes.

Furthermore, there are two profiles - baseline and enhanced – which define a status for each outcome. The CAF collection also includes Indicators of Good Practice (IGPs) to help assess practices against contributing outcomes for the appropriate profile, and it's important to note that assessing all IGPs as 'achieved' does not mean that you are compliant with the CAF, but it is instead a good starting point for discussions.

The CAF, MHCLG and Local Government

Local Government organisations are also being further driven to adopt the CAF, with the MHCLG further refining the CAF for Local Government, and CAF is in use across multiple other departments such as emergency services.

Microsoft has worked with various parts of the UK Government, including NCSC and GDS, to provide guidance for Microsoft 365 around configuration, collaboration and information protection, and blueprints and assessments for Microsoft Azure services. These can help work towards CAF compliance but in themselves do not achieve it.

Challenges with the CAF

With so much latitude for interpretation, and so much guidance, many organisations are unclear on what areas within the CAF they need to focus on and what steps they must take to achieve and demonstrate compliance. Those working with the CAF for the first time – and even those with experience – frequently need external support to identify which Objectives and Principles they are falling short of and what controls and capabilities they must implement.

Competent Authorities - the industry bodies which regulate and enforce the CAF – also have different expectations and requirements depending on your sector, which requires further expertise in the framework. This can be especially challenging if your organisation relies on Operational Technology (OT) and/ or Industrial Control Systems (ICS).

Why Bridewell for CAF?

Expertise Across All Four Objectives – Whether you need help at a point in time to assess or address findings, or you need continuous services to help meet Objectives B and C in particular, Bridewell has experience in delivering across all aspects of the CAF for both basic and enhanced profiles.

Regulatory and Sector Experience – Bridewell has worked with governments and Competent Authorities to implement their overall oversight and enforcement approach, including the development of specific versions of the CAF for different CNI industries. This provides our consultants with an unmatched understanding of the CAF across sectors and allows them to operate as an authority on the framework.

Cloud and OT Expertise – Bridewell's consultants have extensive experience applying the CAF across IT, cloud, and OT environments. We also have a dedicated team of OT cyber security experts who have previously operated as engineers within CNI sectors, enabling us to understand the complexities and nuances of implementing the CAF in industrial environments.

NCSC Assured – Bridewell is one of the few companies assured by the NCSC to provide all of their services, including Consultancy, Cyber Incident Response (CIR), Cyber Incident Exercising (CIE), and Penetration Testing. This level of assurance validates the quality and reliability of our services, especially those relating to the NCSC's proprietary framework – the CAF.

Microsoft Security Partnership and Expertise – Bridewell is a Microsoft Security Solution partner, an Expert partner, a member of the Microsoft Intelligent Security Association, and holds multiple security specialisations. We participate in many exclusive invite-only events and programs, giving feedback and learning from product experts around the globe.

Benefits of Working with Bridewell for CAF

Improved Cyber Resilience - Meeting the outcomes of the CAF provides a strong baseline for cyber security. When combined with ongoing risk management, this allows organisations to continuously improve their cyber security and defend against threats.

Access to Technical Expertise and Resources – Working with Bridewell to implement the CAF provides you with access to our consultant's extensive knowledge on the framework and additional resource to support in meeting IGPs.

Customised Approaches – Our consultants will take a tailored approach to implementing the CAF that helps you achieve compliance while considering your specific goals, challenges, and business processes. This includes the support of our security development and software teams who can develop innovative approaches to address specific problems.

How it Works

1. **Gap Analysis – Our consultants assess your current level of maturity against the framework, identifying where improvements are needed.**
2. **Planning – We will assist you in performing CAF self-assessments and developing remediation programs.**
3. **Implementation – Our team will support you in implementing the remediation program so you can meet the requirements of the CAF.**
4. **Management - We will fully manage the requirements of the CAF across your organisation and work with Competent Authorities.**

About Bridewell

Bridewell is the trusted cyber security partner for organisations operating within Critical National Infrastructure (CNI), as well as companies who want the highest standard of cyber security. Our team are highly accredited by major industry bodies and have extensive experience of delivering cyber consulting and managed security services across highly regulated sectors. As a long-standing Microsoft partner, our team are experts in maximising the effectiveness of Microsoft Security technology to deliver robust and effective solutions.

We have a deep understanding of the challenges faced by CNI organisations and how to resolve them. We work in continuous partnership with our clients to implement the right security solutions to defend and protect them against threats and attacks, allowing them to continue operating safely and securely.

Get in Touch

+44 (0)3303 110 940

hello@bridewell.com

bridewell.com