



# SAPPHIRE™

## Building Your Organisation's Cyber Resilience

Society's reliance on information technology has never been greater. An organisation's increasing dependence on digital technologies that are at risk of disruption or compromise by cyber-attacks, has meant that cyber security has never been a more critical component to an organisation's strategy.

With cyber crime predicted to cost the world \$9.5 trillion by the end of 2024, we are increasingly hearing about the importance of cyber resilience. The UK Government has highlighted that maintaining robust cyber resilience is key to maintaining operational resilience and business continuity. However, this isn't nor should it be the exclusive focus of the public sector.

The ability of an organisation to prepare for, respond to, and recover from, cyber attacks and security breaches is at the very heart of the security and prosperity of the UK as a whole.

The Cyber Assessment Framework (CAF) supports organisations to building their cyber resilience.

### What is the Cyber Assessment Framework?

CAF was developed by the UK's National Cyber Security Centre (NCSC) to provide a systematic and comprehensive approach to assessing the extent of an organisations ability to maintain cyber resilience.

Whilst it was developed for all organisations that are responsible for securing critical network and information systems that keep our businesses, citizens and public services protected, its principles are applicable to any organisation that understands the importance of cyber security and resilience.

### Benefits of CAF

- **Risk Assessment:** CAF helps organisations assess and manage cyber risks effectively.
- **Compliance:** CAF aligns with regulatory requirements, such as the Network and Information Systems (NIS) regulations.
- **Resilience:** Organisations gain insights into their cyber resilience capabilities.
- **Prioritisation:** CAF assists in prioritising security measures based on critical functions.
- **Best Practices:** Following CAF guidelines promotes the adoption of best practices, improving an organisation's overall cyber security posture



To find out more or to speak to an expert contact us today

[CONTACT US TO FIND OUT MORE](#)

Or call: 0845 58 27001

## How Can Sapphire Help?

Whether aligning to the CAF principles or transitioning from Cyber Essentials to the CAF, Sapphire can help.

### CAF Gap Analysis

Before you can get somewhere, you must first know where you are. Conducting a CAF Gap Analysis is the first step.

A CAF gap analysis will provide a thorough assessment of your organisation's current cyber security posture against the core principles of CAF:

- Managing Security Risk
- Defending systems against cyber attack
- Detecting cyber security events
- Minimising the impact of cyber security incidents

This analysis will identify areas where existing controls meet the CAF standards and highlights gaps that need to be addressed. By systematically evaluating these gaps, you can prioritise your cyber security efforts, ensuring a focused and efficient approach to achieving alignment with the CAF.

### CAF Compliance Report

On completion of the Gap Analysis, you will be provided with a CAF Compliance Report, which will detail the core findings of the analysis presented at both an executive-level and a technical-level, as well as providing a roadmap to achieving full compliance with the CAF

### CAF-Relevant Sapphire Services

If the Compliance Report identifies areas that need improvement, Sapphire offers a range of relevant services to meet your needs and support your security transformation.

## Who is Sapphire?

Sapphire is a 100% UK owned and operated IT/OT security provider, and we bring 25 years of dedicated security expertise; cyber security is our only focus.

We have extensive experience in successfully helping organisations meet regulatory compliance such as ISO 27001 and Cyber Essentials, and in improving their all-round cyber security posture.



To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001

## Managing security risk

### Governance

- CISO as a Service
- ISM as a Service
- Compliance to Legislation and Regulation

### Risk Management

- CAF Gap Analysis
- Threat Assessments
- Open-Source Threat Intelligence
- Risk Management of IT/OT
- Penetration Testing
- Vulnerability Management
- Breach Attack Simulations
- Ransomware Simulation

### Asset Management

- IT/OT Asset Discovery
- IT/OT Asset Management
- Endpoint Management

### Supply Chain

- Business Impact Assessments
- Third-Party Risk Management

## Protecting against cyber attacks

### Policies & Procedures

- Policy Development
- ISMS Development
- Compliance Audits

### Identity & Access Control

- IT/OT Consultancy
- Identity & Access Management
- SOC Services

### Data & System Security

- Threat Intelligence & Assessments
- Open-Source Intelligence
- Penetration Testing
- Breach Attack Simulations
- Endpoint Management (EDR/XDR)

### Resilience Network & Systems

- Business Continuity
- Incident Response
- Managed Firewall

### Training & Awareness

- Security Awareness Training

## Detecting cyber security events

### Security Monitoring

- SOC Services
- Threat Intelligence
- SIEM
- EDR/XDR
- IT/OT Discovery
- Managed Firewall

### Proactive Security Event Discovery

- Incident Response
- SOC Services

## Minimising impact of cyber security incidents

### Response & Recovery Planning

- Incident Response Readiness
- Incident Response Management
- Business Continuity Planning
- Disaster Recovery Planning

### Response & Recovery Planning

- Debrief Sessions
- Improvement and Remediation Planning
- Security Improvement Plannin

To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001