SAPPHIRE™

Navigating the NCSC's Cyber Assessment Framework

Key Benefits:

- Reduced cyber security incident impact
- Improves board-level understanding and governance
- Identifies and prioritises security investments
- Strengthens software supply chain resilience
- Reduces third-party vendor risks
- Accelerates transition from CAF 3.2 to 4.0
- Achieves regulatory compliance
- Demonstrates due diligence to key stakeholders

Understanding and adapting to an updated requirement such as the Cyber Assessment Framework 4.0 can seem daunting. Whilst the intent behind the changes to the Cyber Assessment Framework (CAF) is clear, the requirement can leave some organisations unsure how best to navigate the task in front of them amongst the other competing demands of their operations and cyber security strategy.

Sapphire is here to support you and to plan your approach within the CAF requirements.

How Sapphire helps you

In approaching the CAF, Sapphire recommends a staged and methodical approach to avoid making any unnecessary investment and to ensure enhanced cyber resilience and a maturing security posture that scales with an evolving threat landscape.

Engaging in this process will provide a consistent understanding of your environment and a roadmap to address technical debt whilst building a secure foundation for the future. It underpins informed decision making and improving overall cybersecurity posture and how this can relate to your current cyber security and Indicators of Good Practice (IGPs).

Sapphire's services ensure alignment with the NCSC Cyber Assessment Framework (CAF) and any sector-specific security requirements. The review will identify vulnerabilities, assess cyber resilience, and provide recommendations for improving security maturity in line with CAF's four key objectives.

Objective A: **Managing Security Risk**

Objective B: **Protecting against cyber-attack and data breaches**

Objective C: **Detecting Cyber Security Events**

Objective D: **Minimising the Impact of Cyber**

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

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001

CAF Gap Analysis and Technical Discovery

Before you can get somewhere, you must first know where you are. Conducting a CAF Gap Analysis and Technical Discovery is the first stage.

A CAF gap analysis from Sapphire provides a thorough assessment of your organisation's current cyber security posture against the core principles of CAF and any sector-specific overlays.

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

Additionally, the Technical Discovery will review actual technical controls in place against these core principals, primarily looking at the following areas:

- Asset management
- Access control
- Secure configuration
- Patch management
- Endpoint protection
- Backup and recovery
- Resilience measures

This discovery stage will identify any significant technical debt, which regulators will require a clear plan for addressing this, including prioritising actions to reduce risk and improve security resilience. This plan will be communicated upfront to avoid any uncertainty about the next steps.

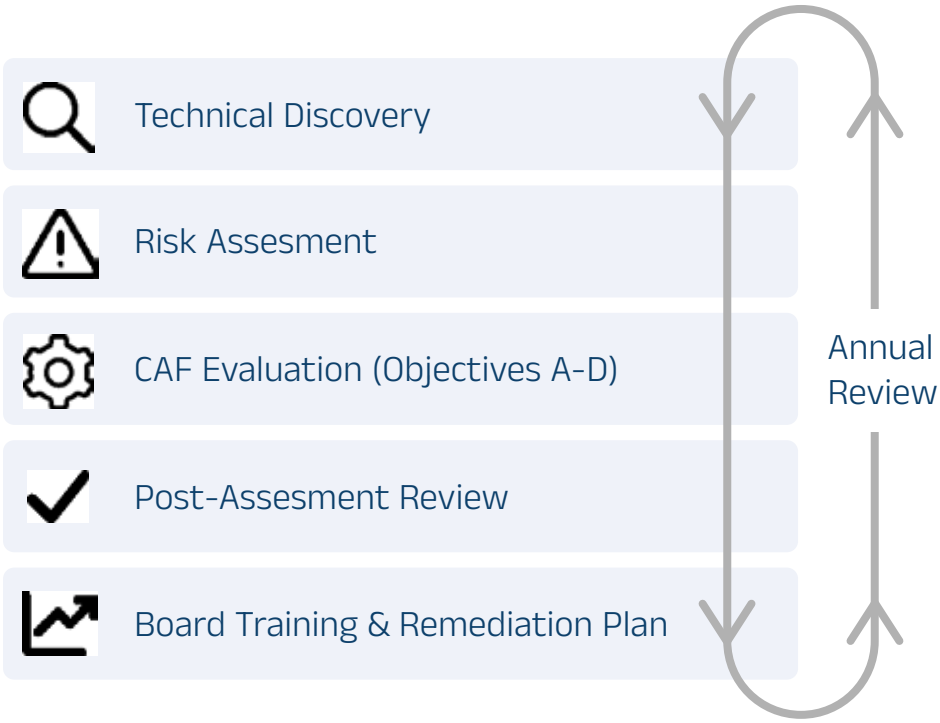
To help achieve the desired outcomes within your budget cycle, we will scope out the necessary work, identify priority actions to reduce risk, and enable you to demonstrate measured and appropriately paced resolutions to your oversight committee and leadership. This approach ensures that you can achieve your security goals within the available budget.

Security Improvement Plan (SIP)

A Security Improvement Plan (SIP) is a structured roadmap designed to enhance your cybersecurity posture in line with the CAF. It identifies weaknesses, outlines corrective actions, and sets clear objectives for improving security resilience.

- Defined Objectives
- Actionable Security Measures
- Implementation Roadmap
- Monitoring and Continuous Improvement

Service Overview



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

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001

Sapphire Services to Support CAF

If the Compliance Report identifies areas that need improvement, Sapphire provides a range of relevant services to meet your needs, assist your security transformation and increase operational resilience through a focussed security improvement program. They include:

- CAF Submission
- Executive / Board Presentation – development and in-person presentation
- Security Improvement and Remediation activities linked to maturity gaps in the CAF

The CAF gap 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.

Deliverables

On completion of the Gap Analysis and Technical Discovery, 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 CAF with actionable recommendations.

Why Sapphire

With three decades of hands-on experience, Sapphire has been working with and delivering cyber security solutions and services for a wide array of organisations. We understand the challenges you are facing.

A significant portion of the Cyber Assessment Framework (CAF) requirements centres on Governance, Risk, and Compliance (GRC). Our consultancy spans a range of services, including policy development, business continuity testing, and full-scale certification projects and have a proven track record in delivering robust, effective, and tailored security solutions that meet the highest international standards. From Cyber Essentials to NIS2, ISO 27001 to DORA, Sapphire has consistently and successfully guided our clients to achieve compliance.

Crown Commercial Service Supplier

HM Government G-Cloud Supplier

Assured Service Provider in association with National Cyber Security Centre CHECK Penetration Testing

CREST SECURITY OPERATIONS Security Operations Centre

CREST SECURITY TESTING Penetration Testing

CISM CERTIFIED INFORMATION SECURITY MANAGER

CYBER ESSENTIALS CERTIFIED PLUS

CYBER ESSENTIALS

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

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001