Cyberfort

G-Cloud 15

Service Definition

NCSC Cyber Resilience Audit (CRA)

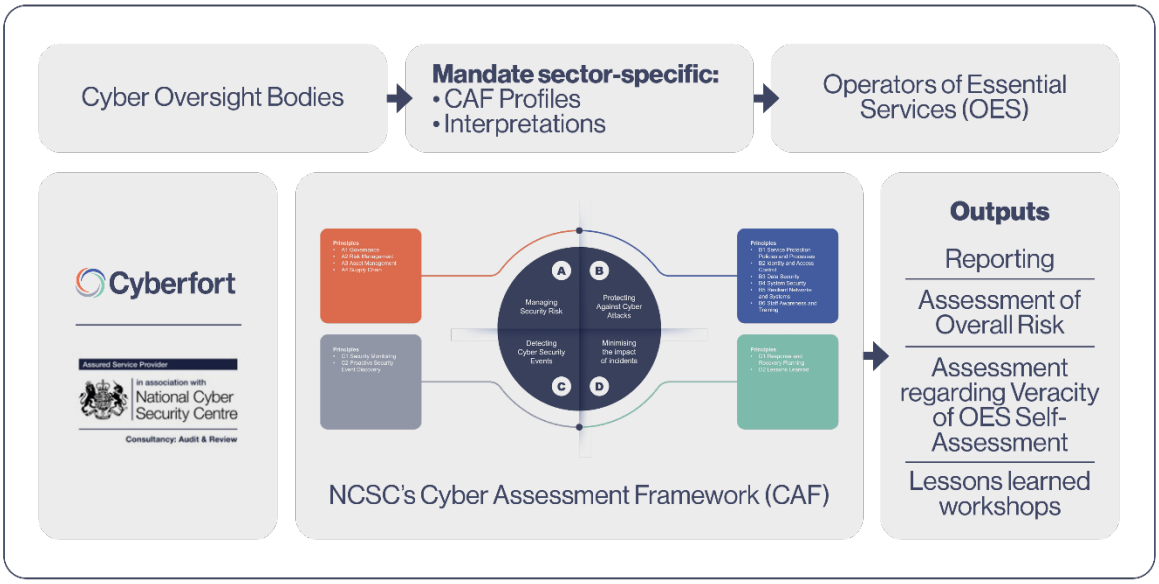
Table of Contents

1. Service Overview

1.1 Summary of Service

NCSC's Cyber Resilience Audit (CRA) scheme provides a single 'Core' Resilient Audit scheme to support a broad selection of Cyber Oversight Bodies and sectors including HMG, Healthcare, Civil Aviation and Energy. Cyberfort's Service supports Operators of Essential Services (OES) undertaking and passing the required assessments, so you successfully comply with the CRA scheme.

Fig.1: Cyberfort's Cyber Resilience Audit Service



Cyberfort are one of the few companies that are part of NCSC's Cyber Resilience Audit scheme and comply with the bespoke GovAssure requirements. As per NCSC's CRA Assurance Reviewer training, Cyberfort follows the approach and process outlined below to present and agree the final IARR (Independent Assurance Review Report) and resolve areas of arbitration:

1.1.1 Plan

During the planning meeting with clients, we:

- Agree assessment scope,
- Identify key Authority individuals involved in preparing CAF assessments, also those who can provide evidence to support assertions,
- Review WebCAF return and evidence,
- Agree how final IARR will be presented and agreed.

1.1.2 Assurance Review

Initial high-level desk-based review:

We review the self-assessment submission and WebCAF entries, considering:

- Overall quality,
- Confirm contributing outcomes and IGPs are fully answered,

- Evidence is supportive,
- Approach to complete CAF objectives.

In-depth assessment of Contributing Outcomes:

We will review contributing outcomes, their assessed state compared to target GovCAF Baseline and Government Enhanced profile, considering:

- Achievement against target CAF profile and Government Cyber Security Policy Handbook,
- IGP statements supporting overall contributing outcome,
- Evidence,
- Deliver narrative at the contributing outcome level.

Update WebCAF for each system in scope.

Submit draft IARR for review by client.

Workshop:

To finalise the IARR, identify lessons learned and resolve areas of arbitration, we will initiate a workshop to consider:

- Contributing outcomes, then assess underlying IGPs', resolving any assessor arbitrations at IGP level,
- Achievement against target CAF profile,
- Identify any IGP outliers,
- Agree consistent level of evidence for IGPs that require justification or that do not fit with CO's assessment,
- Resolve queries relating to evidence and completeness.

Develop list of control gaps/observations:

Summarising findings of any control gaps at a CO level, providing an overall achievement level and justification.

Submit final IARR for review by client and Government Security Group.

1.1.3 Reporting & Presentation

Once the Assurance Review is complete Cyberfort will produce the Independent Assurance Review Report (IARR) as follows:

- CRA Independent Assurance Review Report: Using a combination of output from WebCAF and findings recorded during the Assurance Review, we will complete the CRA IARR template to include the following:
  - Summary radargram graphics for each CAF objective showing the underlying contributing outcomes of the assessor results for the system vs the target government CAF profile (Baseline or Enhanced).
  - A summary table comparing the assessor achievement results of each contributing outcome vs the Government CAF profiles.

  - A list of the contributing outcomes under each objective that assessor ratings have highlighted did not meet the required rating under the target government CAF profile (Baseline or Enhanced).
  - A table of the IGP comments and achievement levels as determined by the assessor clearly referencing any IGPs that are causing the contributing outcome to not meet the target Government CAF profile for the system.

- The final objective of the Independent Assurance Review Report is to provide recommendations to inform a targeted improvement plan allowing key decisions relating to controls and investment, and, if implemented, will reduce the overall Cyber Risk for client.

Following full completion of the Independent Assurance Review, Cyberfort's Head Consultant and assessors will attend a Lessons Learned workshop with client to discuss the final report.

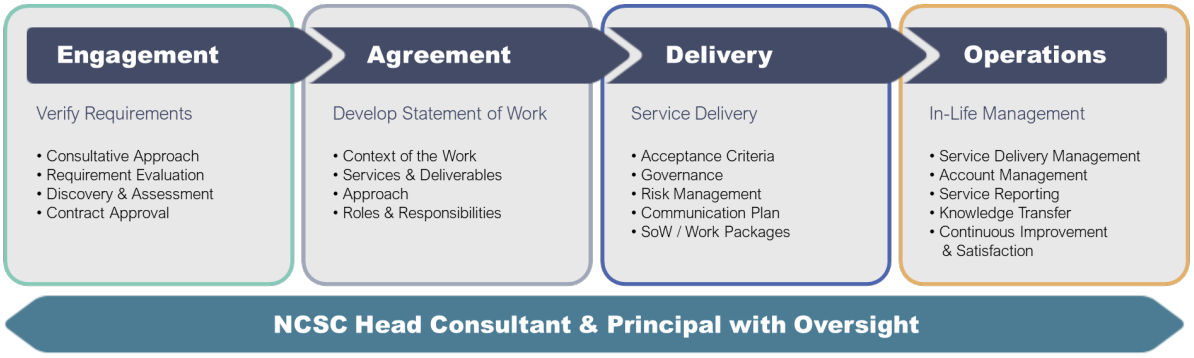
2. Delivery Approach

2.1 Our delivery approach

Cyberfort deploy an auditable and assured approach to the design and delivery of services. We have a 'one team' approach when working with our clients, engaging stakeholders to focus on business objectives and build collaborative, effective relationships that support the agile delivery of project outcomes. We take ownership of activities within our specialist areas, ensuring outcomes are delivered within required deadlines

Underpinning our delivery approach, we align our services with the NCSC Assured Cyber Consultancy Standard, particularly the Consultancy Lifecycle, and adhere to the Consultancy Competency Requirements and Code of Ethics. We layer NCSC delivery lifecycle best practices into our clients' existing workflows and operating models, minimising disruption whilst providing an assured, high-quality service.

Fig.1: Cyberfort Lifecycle Journey



2.1.1 Engagement – Verification Requirements

Our Lead Consultants will work collaboratively with client key stakeholders to evaluate, scope, and refine all Statement of Work (SoW) requirements. We assess how the SoW supports client's overall business vision and objectives. Through a combination of workshops and meetings, we conduct detailed discovery and assessment activities to confirm all SoW elements and required deliverables. Investing the appropriate time and approach during this phase is critical and enables a comprehensive understanding of requirements to ensure they are effectively applied to the target environment or service, delivery plan, and future operations.

2.1.2 Agreement – Develop Statements of Work

Upon receipt of draft Statement of Work (SoW), we will review the scope, context, and deliverables, and return a fully costed final draft for approval within five days. We will recommend the most appropriate delivery approach for each SoW, define roles, and assign responsibilities to Suitably Qualified and Experienced Personnel (SQEP). Draft SoWs will be shared with all relevant stakeholders, with scheduled meetings or calls to discuss, agree, and finalise each SoW in line with the agreed five-day turnaround period.

2.1.3 Delivery – Service Delivery

Based on the finalised SoWs, we will develop a comprehensive Service Delivery Plan and hold a project kick-off meeting with your team to review and agree all aspects of the plan, including deliverable acceptance criteria.

2.1.4 Operation – In-Life Management

A monthly Service Review Report will be produced and presented at a Service Review Meeting. The review will cover previous actions and the action log, invoicing and forecasts for each SoW, performance against defined Key Performance Indicators, reporting on added value, risks, issues and mitigation measures, service improvements, and compliance with contractual obligations.

2.2 Managing the work and maintaining quality

As part of our service, we will keep relevant stakeholders informed of work status throughout the project and ensure that the quality of deliverables is maintained and aligns with requirements by:

- **Deliverables Management:** For each cyber security area, SoWs will define and summarise deliverables along with relevant KPIs and SLAs.
- **Quality Assurance (QA):** We will establish a QA matrix to ensure service deliverables are reviewed and approved by senior personnel from both organisations.
- **Daily Reviews:** We will monitor progress across all SoWs, review action logs, and address any resource constraints, challenges, or blockers with the delivery teams.
- **Service Delivery Meetings:** Attend regular meetings or calls with the client to ensure delivery remains aligned with strategic objectives.

These commitments will enable us to identify any unexpected emerging priorities promptly and engage with the appropriate stakeholders to understand the context and required milestones for new activities.

2.3 Our Teams

We will establish the appropriate strategic team structure, governance, and engagement processes to maintain and strengthen our successful working relationship. Our team is designed to provide strategic leadership, expert consultancy, and hands-on subject-matter expertise, ensuring seamless service delivery. This structure also clearly demonstrates the chain of communication for client engagements, facilitating effective collaboration and accountability throughout the project.

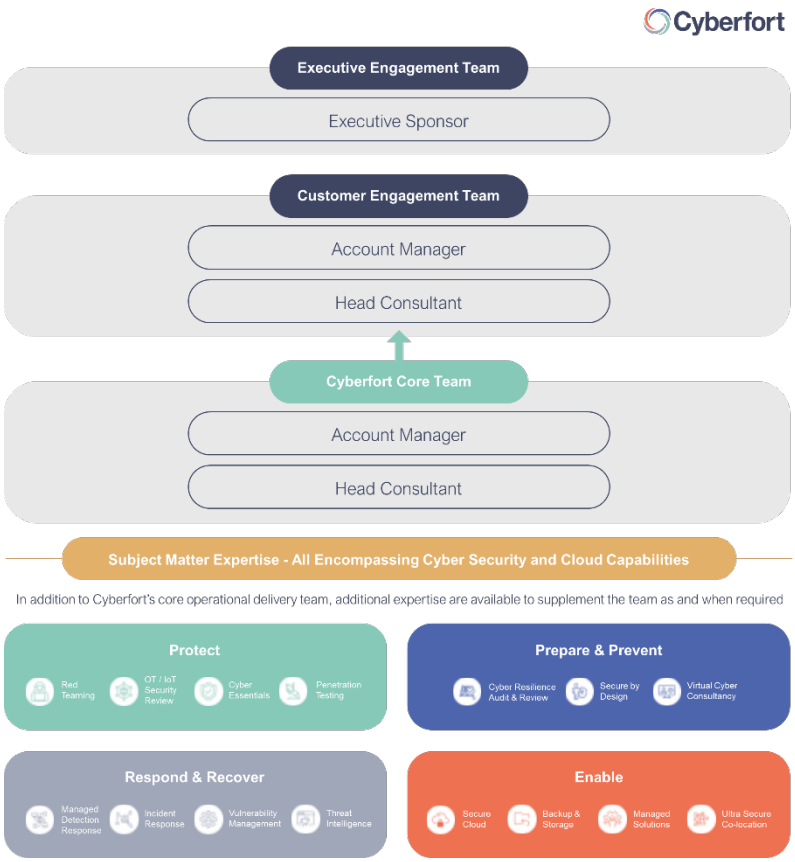


Fig.2: Cyberfort's Team Structure

2.4 Delivering High-Quality Outputs

To ensure all services are delivered to the highest standards, Cyberfort has implemented a Quality Management System (QMS) in line with ISO:9001 International Standards. We adopt a customer-centric approach, aiming to build long-lasting, trusted relationships with all our clients.

Our QMS manages and maintains several international and industry-specific standards, enhancing customer satisfaction by consistently delivering products and services that meet regulatory and statutory requirements. We also invest in our people and uphold our commitments to information security, quality, and environmental responsibility.

Cyberfort prioritises the implementation of consistent processes and policies to support our certifications, providing confidence to clients, suppliers, and stakeholders that we deliver safe, reliable, and high-quality services. A fully implemented internal audit process is conducted annually for all certifications to verify that policies and procedures are followed consistently and effectively, ensuring compliance to standards and regulations and improve the effectiveness of our operations.

2.4.1 Regulatory Compliance

Our consultants are obligated under the NCSC Assured Consultancy Scheme to maintain up-to-date knowledge of relevant regulations, standards, policies, and guidance, supported by evidence. We submit an annual Obligations Report to the NCSC to demonstrate compliance with this requirement.

Additionally, our consultants hold memberships with CIISEC, which require the submission of Continual Professional Development (CPD) evidence to maintain membership standards.

To ensure our team's skills remain current, we have recently trained a group of consultants in the NIST Cyber Security Framework and NIST 800-53. We have also updated the qualifications of our ISO 27001-certified consultants to align with the new 2022 standard.

3. Commercials & Pricing

3.1 Ordering & Invoicing Process

Please contact us for a quote via email at bidmanagement@cyberfortgroup.com

Orders are processed on receipt of a purchase order.

Prior to commencement of any work ordered via the G-Cloud framework, Cyberfort requires client acceptance of the order and also completion of a Call-Off Contract.

Clients are invoiced on a monthly basis or according to agreed milestones.

3.2 Service pricing model

Cyberfort's services are priced based on scoped client requirements, documented in a Schedule of Work (SOW), with the following options:

- **Time & Materials**: Agreed day-rate for Cyberfort resources will apply; services are invoiced monthly in arrears.
- **Outcome Based:** Cyberfort will quote for defined service outcomes, with milestone-payments agreed as appropriate.

Cyberfort's pricing for Consulting Services links clearly to Resources Based Pricing aligned to our SFIA rate card. Please refer to our Pricing document for more details.

3.3 Minimum contract period

Contract terms will be provided at the time of quotation, based on specification. These will not exceed the maximum contract constraints of the G-Cloud framework.

4. Governance Compliance

Cyberfort confirm that we will deliver our services to clients in line with all industry and Government recognised standards, best practice and legal regulations, including but not limited to the following:

4.1 GDPR

We adhere to the legal and statutory requirements outlined in the UK Data Protection Act 2018 and the General Data Protection Regulations (GDPR). Our organisation has a current registered Information Commissioners Office (ICO) certificate for Data Protection.

4.2 Government and industry standards

Throughout the life of any contract, our consultants will ensure that all service standard principles are adhered to so that clients can be assured that all delivered outcomes conform with Government and industry standards and expectations. Our teams are deeply experienced in operating services, to deliver outcomes and outputs that fully comply with:

- The principles defined in the Government's Service Standard and Technology Code of Practice (TCoP).
- The Government Functional Standard (GovS 007: Security), ensuring that the stated principles (for example security objectives are aligned to government policy and organisational objectives) are applied to all projects.
- Open standards supported include TOGAF, NIST-CSF, ISO/IEC27000, SANS and OWASP.
- Regulation frameworks including, Cyber Security and Resilience Bill, Digital Operational Resilience Act (DORA), and NIS2 Directive.
- Government Cyber Security Strategy, including National Cyber Security Centre (NCSC).
- As an NCSC assured Cyber Security Consultancy, we are members of the NCSC Assured Consultancy Scheme Community Network and leverage the CiSP (Cyber Information Sharing) platform.

4.3 Quality Management

Further, we have a fully implemented Quality Management System (QMS) and are certified to ISO 9001:2015 International Standard, which details our policy, objectives and processes, as well as demonstrating how our QMS framework enhances client satisfaction whilst ensuring consistent delivery of product and services is maintained to meet client, statutory and regulatory requirements.

Our delivery is underpinned by certifications and associated management systems including:

- ISO:27001
- ISO:14001
- ISO:9001
- ISO:45001
- Cyber Essentials Plus
- CREST Certified Body CE
- CREST Penetration testing
- NHS Digital Toolbox
- PCI DSS
- DSPT
- NCSC Cyber Security Consultancy
- NCSC CHECK ITHC

About Cyberfort

Cyberfort's all-encompassing Cyber Security Services

At Cyberfort we provide a range of customers with all-encompassing Cyber Security Services. We are passionate about the cyber security services we deliver for our customers which keeps their people, data, systems and technology infrastructure secure, resilient and compliant.

Our business offers National Cyber Security Centre assured Consultancy services, Identification and Protection against cyber-attacks, proactive Detection and Response to security incidents through our security operations centre and a Secure and Recover set of Cloud solutions which keeps data safely stored, managed and available 24/7/365.

Over the past 20 years we have combined our market leading accreditations, peerless cyber security expertise, strong technology partnerships, investment in our future cyber professionals and secure locations to deliver a cyber security experience for customers which enables them to achieve their business and technology goals in an ever-changing digital world.

Cyberfort

Care about the impacts we make on the Environment, Social and Governance.

We are passionate about empowering our employees, suppliers, customers, and the cyber security ecosystem to create a better world for our business and the communities we participate in, for example:

As a member of Neurodiversity in Business (NiB) and Disability Confident Employer

Cyberfort are supporting those with physical and neurodiverse disabilities, by disarming barriers for people with disabilities and ensuring equal opportunities for all.

Cyberfort are inspiring and attracting young people to the world of cybersecurity.

We support the development of their passion for technology through Apprenticeships, Graduate Schemes, CyberFirst and school education/awareness.

We are committed to achieving net zero carbon emissions by 2050.

Cyberfort have clear plans and activities that deliver environmental benefits by increasing the energy efficiency of our operations, reduce our waste, and protect our communities.

Our Values

Teamwork | Curiosity

Ownership | Agile | Innovative

Cyberfort

Accreditations

We are proud of the extensive list of industry and government accreditations we hold. We understand the need for independent validation when entrusting the security of valuable or sensitive data to a third party.

Our Vision

To be an integral part of the cyber security ecosystem, providing assured, highly skilled and reliable security services to businesses and government departments. Embodying the UK Cyber Security Strategy, through trusted partnerships we aim to empower businesses and government departments with confidence, making the world a safe and secure place to conduct business.

Our Mission

To provide our customers with an agile and innovative approach to help them overcome their cyber security challenges. Through a collaborative approach with our customers we design, build and operate their cyber security environments resulting in a secure and resilient infrastructure, providing a safe environment for employees, service users and stakeholders to conduct their business in the knowledge that their critical data remains safe in an ever-changing digital world.

www.cyberfortgroup.com

For more information, please contact us on:

01304 814800

info@cyberfortgroup.com