



Cyberfort

G-Cloud 15

Service Definition

Secure by Design (SbD)



Table of Contents

1. Service Overview	1
1.1 Summary of Service	1
2. Delivery Approach	4
2.1 Our delivery approach	4
2.2 Managing the work and maintaining quality	5
2.3 Our Teams	5
2.4 Delivering High-Quality Outputs	6
3. Commercials & Pricing	7
3.1 Ordering & Invoicing Process	7
3.2 Service pricing model	7
3.3 Minimum contract period	7
4. Governance Compliance	8
4.1 GDPR	8
4.2 Government and industry standards	8
4.3 Quality Management	8
5. About Cyberfort	9



1. Service Overview

1.1 Summary of Service

Our Secure by Design (SbD) service is aligned with UK Government Security 10 SbD Principles. Cyberfort blends Cyber security skills and experience of Security Architecture, Governance, Risk, and Compliance (GRC), Security Operations and Testing to help organisations implement these Secure by Design principles effectively - balancing security, functionality, risk appetite, and regulatory obligations with Business needs. Together, these specialists provide the expertise, oversight, and governance required to embed security into business operations and technology estates

This approach ensures the integration of security practices and considerations required to deliver programmes in line with a Secure Development Life Cycle (SDLC) and a Continuous Implementation/Continuous Development (CICD) pipeline. With focus on building secure software and systems from the ground up, considering security requirements and designing out potential risk throughout the entire development life cycle. Cyberfort's team of Security Architects and Risk Managers will embed with clients' project delivery teams, ensuring that from the very first design session all the way to delivery, threats are understood and risk is designed out where possible. This approach offers material benefits which are shown in Table 1 below:

Table 1: Cyberfort's Secure by Design Approach

The material benefits delivered to clients from the SbD service approach.

Activity	Cyberfort's Approach	Benefit to clients
Prioritise cybersecurity efforts	Risk assessments reviewed, matured where necessary, newly identified risks assessed and progress through established risk management structures.	By understanding risk priorities, resource can be directed at specific risk mitigating activities.
Defence In Depth	Apply a combination of technical, physical, and administrative measures.	Failure of individual controls less likely to result in significant impact.
Frameworks and Standards	Leverage established cyber security frameworks & standards such as the NIST Cybersecurity Framework, ISO27001, NIST RMF, CIS Controls benchmarks, NCSC Cyber Assessment Framework (CAF)	Provides structured approaches to cybersecurity, help establish comprehensive security practices.
Secure Development Lifecycle	Implement secure software development practices across entire development lifecycle in line with business security requirements, threat modelling, secure coding practices.	Vulnerabilities and risks are identified early in the lifecycle.
Threat Modelling	We apply threat modelling as a core Secure by Design activity aligned to NCSC guidance. By systematically analysing service architecture, data flows, trust boundaries, and attacker behaviours early in the lifecycle, we identify and prioritise security risks before implementation. Threats are addressed primarily through design-led controls such as secure defaults, least privilege, and reduced	Improves risk analysis process through continual threat modelling.

	attack surface. The threat model is maintained as a living artefact and updated as the service evolves, providing ongoing assurance and transparency for public sector customers.	
Continuous Monitoring and Response	Utilise intrusion detection systems, log analysis, and SIEM solutions to continuously monitor, alert, and respond to threats, adhering to clients' Incident Management Processes.	Proactive identification of threats, weaknesses, and the ability to counter them. Specialist resource to respond to security incidents.
Security Assessments	Conduct security assessments, including penetration testing and vulnerability scanning.	Identification of vulnerabilities and weaknesses, and prompt remediation or risk management.
Review and Improvement	Continual Service Improvement (CSI) approaches will review and regularly update process and procedures. E.g. risk management tooling, maturity of the threat modelling methods, removing limitations from Supplier Assurance Processes.	The capability and supporting processes remain resilient, and conformant to the regulatory and legislative landscape.
Secure Configuration Management	Establish strict configuration management practices to ensure systems are configured securely.	Resilience to attack and effective recovery from incidents
Data Protection	Implement strong data protection measures following the clients' Data Protection processes, and by working with Information Asset Owners and Data Protection Office.	The effective use of data and supporting governance processes remain resilient, and conformant to the regulatory and legislative landscape.

1.1.1 Leveraging SbD approach to redefine agile delivery of assurance

Working with our clients, Cyberfort implements an assurance approach that brings Risk and Security Architects together to investigate and agree a risk position, which repeatedly results in risk-based acceptance into service. This approach fosters an increased willingness to take informed decisions and a more open and effective relationship between SbD functions and the programme risk and project teams.

This approach used in our delivery to clients has been evolved alongside the development and project acceptance into service, to adapt the assurance processes through functionally aligned sequential process flows.

Outputs of design activity, design review (High Level Solution Architecture (HLSA), Digital Solution Vision (DSV), HLD and LLDs), ITHCs, DPIA reviews or other vulnerability identification, informs the service's risk profile, allowing risks to be assessed according to clients' Risk Methodology.

Consistently adopting this end-to-end approach, allows for a better understanding of what can flexibly change, where critical timings of service releases require. Cyberfort Technical Delivery Managers working with clients' Product/Service Delivery Team(s) have visibility of upcoming sprint release content and release plans and can effectively manage and assign the appropriate resources.

This is not just a sequential series of activities, but the collaboration of multiple functions across departmental teams striving to achieve a risk managed outcome. Risk Management does not end at



the point a service goes live. Through life assurance activities are carried out and Risk Assessment and Risk Management are the functions that provide confidence to stakeholders that exposure of risk to their services and information is understood and managed.

Fig.1: Cyberfort Secure by Design Approach

Our agile delivery approach within a risk management lens ensures that all assurance functions and roles are used efficiently to inform client stakeholders' decision making.



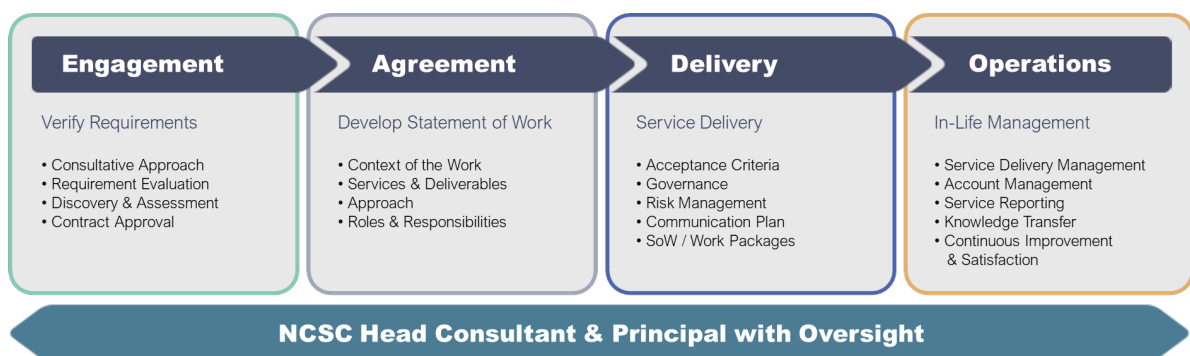
2. Delivery Approach

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.

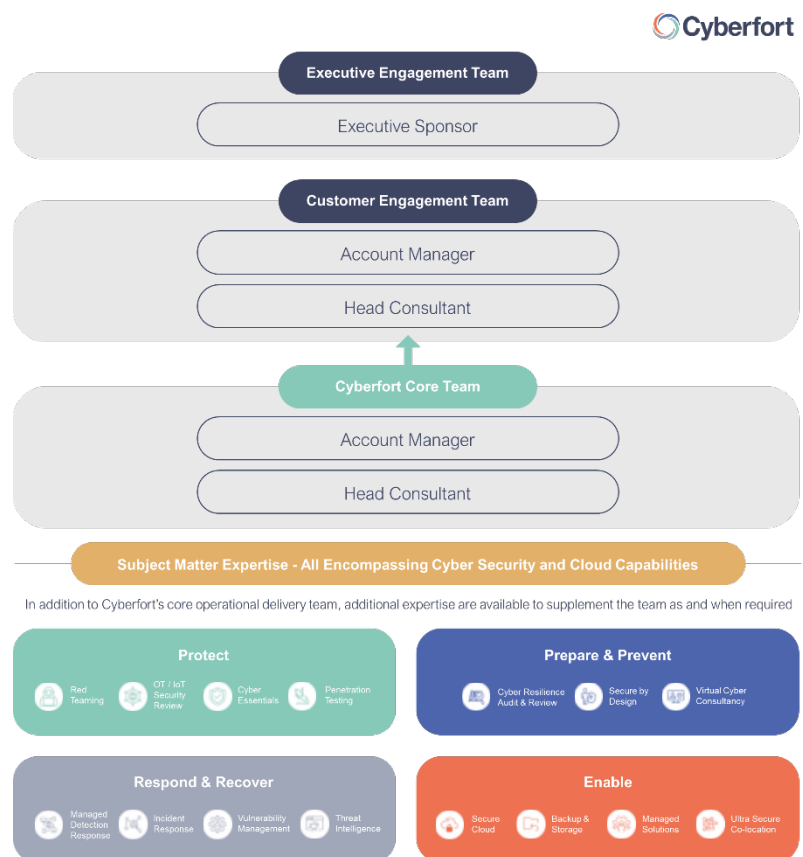


Fig.2: Cyberfort's Team Structure



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 | • Cyber Essentials Plus | • PCI DSS |
| • ISO:14001 | • CREST Certified Body CE | • DSPT |
| • ISO:9001 | • CREST Penetration testing | • NCSC Cyber Security Consultancy |
| • ISO:45001 | • NHS Digital Toolbox | • 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.



Cyberfort

www.cyberfortgroup.com

For more information, please contact us on:

01304 814800

info@cyberfortgroup.com