CYBERFORT

G-Cloud 14
Service Description
Secure by Design

Table of Contents

1. Service Overview

1.1 Summary of Service

Cyberfort's suitability to deliver Secure by Design services comes from our deep on the ground experience of delivering complex cyber security services to HMG clients by deploying and managing large teams of expert consultants. In a fast-digitising environment with a constantly evolving threat landscape, Cyberfort leads from the front, developing new techniques, constantly upskilling our staff and clients, and actively involved in key UK cyber security institutions, contributing to the latest cyber security thinking through various ways, as described below that we will feed into your day-to-day security.

- **NCSC assured consultancy community network:** As an NCSC assured cybersecurity consultancy, we are members of the NCSC Assured Consultancy Scheme Community Network and leverage the CiSP (Cyber Information Sharing Platform). We regularly attend the quarterly Assured Consultancy Community Events.
- **British Computer Society (BCS) Information Security Specialist Group (ISSG):** We meet regularly to discuss latest threats, innovations, and advancements.
- **Chartered Institute of Information Security (CIISec):** As members, we support and attend Cyber Security events for example CIISec Live to engage with world-leading cyber security experts.
- **UK Cyber Security Council's (UKCSC) Professional Standard Programme:** We focus on leadership, outreach, and diversity to develop our services.
- **Information Systems Audit and Control Association (ISACA):** We are actively involved in several areas including Special Interest Groups (SIG's), Risk, Cloud & Training.

To stay up to date and adapt our services and approach, we partner with:

- **TechUK:** Our Founder, is Vice-Chair for the Cyber Security SME Forum (CSSMEF), which provides a conduit for TechUK's SME members to engage with stakeholders in HMG, and closely related Security Agencies.
- **Eastern Cyber Resilience Centre (ECRC):** Our Chief Operating Officer (COO), is Vice-Chair of the board and we attend regular networking sessions with public and private sector organisations.

1.2 Service Detail

1.2.1 Service Description

Our Secure by Design (SbD) service is aligned with UK Government Security 10 SbD Principles. Applying these Principles, we deliver:

- Programmes in-line with a Secure Development Life Cycle (SDLC)
- Implementation of secure systems from the ground-up, considering security requirements and mitigating risks throughout the entire development life cycle

Cyberfort will build in the NCSC SbD principles (on which the UK Government Security - 10 Secure by Design Principles are based) to its whole service approach for Secure Design. 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 entrench 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. The approach has 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	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 HMCTS's security requirements, threat modelling, secure coding practices.	Vulnerabilities and risks are identified early in the lifecycle.
Threat Modelling	Review of and contribution to the HLD, LLDs, HLSAs and DSV allows Security Architects to efficiently use the STRIDE(LM) threat modelling methods to model threats of associated system developments and changes.	Improves risk analysis process through continual threat modelling.
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.

1.2.1.1 Leveraging SbD approach to redefine agile delivery of Authority to Operate

Working with our clients, Cyberfort redefines the Authority to Operate (AtO) approach, bringing 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.

The AtO process 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.

The output of the design activity, design review (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.

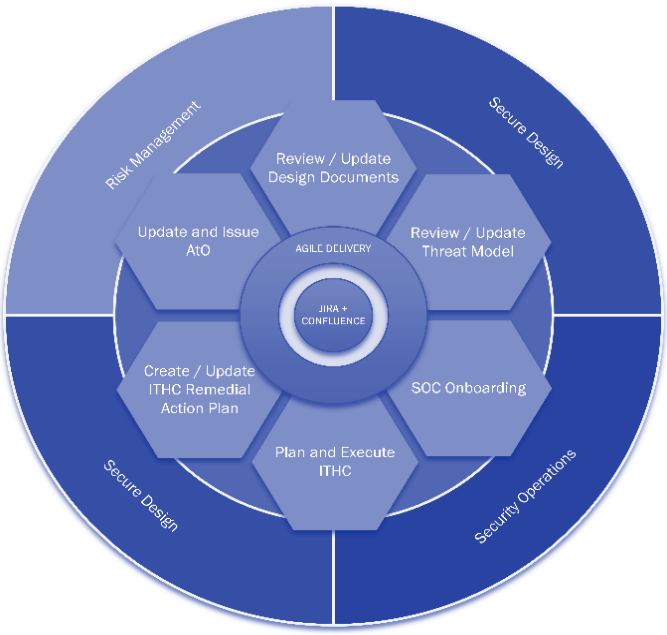


Figure 1: Our agile delivery approach within a risk management lens ensures that all assurance functions and roles are used efficiently to inform client stakeholders' decision making.

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 Enhancement Team(s) (PET) have visibility of upcoming release sprint content and release plans and can effectively manage and assign the appropriate resources.

The AtO Process 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 and AtO issued. 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.

1.2.2 Features

- Complies with UK MOD and Government Security SbD principles.
- SbD Service includes Security Architecture, 1st/2nd line Risk.
- SbD Service includes Vulnerability Management, Supplier Assurance, Controls Testing.
- Enables implementation of secure architectural patterns and design principles.
- Enables adoption of the three lines of defence model.
- SbD approach can be tailored to fit the agility required.
- SbD with timely ITHC checks to validate design findings.
- SbD principles promote continuous improvement.

1.2.3 Benefits

- Assurance Service delivery aligns with UK Government SbD principles.
- SbD principles define approach to other core Security capabilities.

- Minimise potential vulnerabilities and address common security risks.
- Supports systematic approach of identifying, assessing and managing security risks.
- SbD approach supports the agile scrum style of collaboration.
- ITHC checks will confirm remediation of previously identified vulnerabilities.
- Leverage lessons learned to enhance security and influence future changes.

1.2.4 NCSC Assured

Cyberfort is an NCSC Assured Cyber Security Consultancy, and to ensure that we remain fully aligned to the NCSC Assured Consultancy Lifecycle, Cyberfort's NCSC Head Consultant will oversee the end-to-end service delivery. They will continue to certify that NCSC Cyber Security Consultancy Standards & Code of Ethics, GovAssure, together with CAF principles, are adhered to at each stage.

2. Delivery Approach

2.1 Maximum results, minimal risk

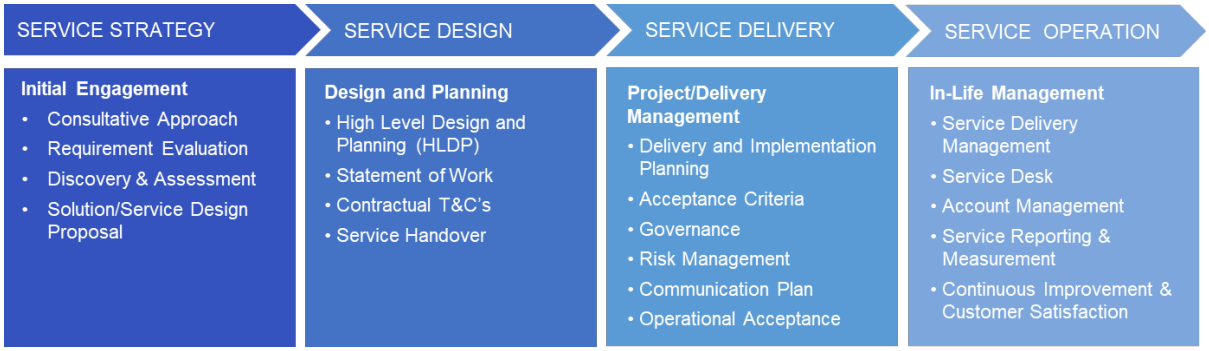
Our working practices to ensure delivery of services meet our clients' requirements.

Cyberfort works with the core principle of providing you with an auditable and assured approach to the design and delivery of services. We take a "one team" approach to working with clients, engaging with stakeholders to focus on business objectives and build working relationships that are conducive to the agile delivery of project outcomes. We'll take ownership for activities within our specialist areas, ensuring that outcomes are delivered within required deadlines. Through applying our accredited standards, predefined check point stages are built into our delivery processes, from initial conception through delivery and into lifecycle management, as follows:

2.2 Client Lifecycle Journey

Our delivery and service approach will be fully aligned to best practices, recommendations and guidance. The below Lifecyle Journey forms the foundation of everything we do in the delivery our service to our clients. We work closely with our clients to integrate our delivery and service methods to align with any existing processes, operating models and associated tooling in place within the department.

Cyberfort Lifecycle Journey



2.2.1 Service Strategy: Initial Engagement

- **Consultative Approach:** Our approach is to engage and work collaboratively and in partnership with our clients to ensure delivery of the specific requirements.
- **Requirement Evaluation:** We will initially conduct a stakeholder engagement meeting, or a series of meetings/workshops, to better understand the specific aspects of the clients business challenges and requirements.
- **Discovery & Assessment (DA):** This initial phase of DA is critical to providing the foundation for successful outcomes, by building a comprehensive understanding of the requirements, and applying this knowledge to the target environment/service, delivery plan and future operations.
- **Solution/Service Design Proposal:** Based upon the DA by our specialists, we will translate the specific aspects of the clients security, technology and business needs to develop and deliver a proposal that meets all your requirements.

2.2.2 Service Design: Design and Planning

- **High Level Design and Planning (HLDP):** Upon completion of the initial DA and Solution/Service Design Proposal phase, we'll engage our Subject Matter Experts to develop the HLDP from an informed position.

- **Statement of Work (SOW):** Upon acceptance of the HLDP with the client, we will draft a SOW, that provides a high-level narrative description of the solution/service to be delivered.
- **Contractual T&C's:** In line with the SOW, a Call-Off Contract relevant to the goods and/or services will be prepared and agreed with the client, as per the framework.
- **Service Handover:** Following contract signature, we will complete a formal handover from the Sales team to the Project /Delivery team.

2.2.3 Service Delivery: Project/Delivery Management

- **Delivery and Implementation Planning:** The assigned Project/Delivery Manager will lead a Project-Kick Off meeting with the client. To ensure the scoped success factors are delivered they will build a Delivery and Implementation plan to define project specific deliverables, dependencies, resource requirements and timeframes for each deliverable.
- **Acceptance Criteria:** Agreement and acceptance with the client for all project deliverables.
- **Governance:** We recommend following a governance framework to ensure regular updates (on a daily, weekly, monthly and quarterly basis), which we'll agree with the client to ensure we are providing enough information at the correct frequency.
- **Risk Management:** We will ensure that a full and thorough risk assessment is conducted across all aspects of the project. This will highlight any potential problems from the outset, which are recorded and tracked within the Project RAID Log.
- **Communication Plan:** The Project/Delivery Manager will agree with the client the frequency, format and parties to be communicated to throughout the project lifecycle.
- **Operational Acceptance (OA):** The OA records the process that the Project, Technical Delivery, Facilities and Service Support Teams (as required) will follow to ensure the services are introduced consistently and efficiently and that associated documentation, configurations and processes/service boundaries are defined. The OA Process is the final sign-off stage recording completion of a project and delivery into Service.

2.2.4 Service Operation: In-Life Management

- **Service Delivery Management:** The Service Delivery Manager (SDM) will work closely with the client to ensure that a close relationship is reached, and frequent communication is maintained to ensure a high level of client service can be maintained.
- **Service Desk:** Cyberfort's 24x7x365 Service Desk will manage all communications in relation to incident or request management.
- **Account Management:** Your account manager will be your Cyberfort internal ambassador, taking leadership of delivery and management of all commercial matters. Account managers will facilitate regular touch points across all areas of Cyberfort's client success framework and have accountability of all services provided to the client.
- **Service Reporting & Measurement:** The SDM will perform regular service reviews and provide a service management report based on availability metrics whilst also including service operation metrics and KPIs for support tickets and tasks, and any other information agreed.
- **Continuous Improvement & Client Satisfaction:** Enhancing Client satisfaction is a key part of our success and how Continual Improvement is achieved. There are several mechanisms in place such as Net Promoter Score (NPS), Service Delivery Management and Key performance Indicators that we'll use to ensure the services we offer our clients are the best possible.

3. Service Management Approach

3.1 Your satisfaction is the heart of our service

We have a proactive, consultative approach that allows us to gain a better understanding of our clients' needs, requirements, objectives and measures of success in order to help you meet your strategic objectives. Ongoing support and management of services under this framework will be based on this approach. From the Service Desk to your dedicated Account Manager, all are in place to manage the relationship across your business and ensure that you receive the right engagement to help drive and deliver a great service.

3.2 Service Delivery Management

Cyberfort's service management model is designed to meet ISO 9001 and ISO 27001 guidelines and has been established in alignment with ITILv3 service management processes. Clients will have a combination of the best people, using the best tools, delivering a 'best-in-class service management' experience. We recognise that to support your business operational requirements we need to have in place the right team structure, governance and engagement processes.

The ultimate responsibility for the achievement and validation of services delivered will be the Service Delivery Management function, which will be led by a dedicated Account Manager and supported by the Service Delivery Manager (SDM). The SDM will be responsible for the delivery of services, ensuring end-to-end service accountability, responsibility and effectiveness. The service structure is ultimately scalable and will be monitored through the Service Governance processes to ensure Cyberfort deliver all in-scope supported services against agreements, expectations, and commitments with the client.

3.3 Service Satisfaction and Improvement

Key to ensuring Client Satisfaction, is the Continuous Improvement of our services. Measurement and validation of service outcomes is therefore a critically important part of the delivery of services. Cyberfort will provide a comprehensive Service Report, tailored to the specifics of each service/project. This report is provided by the SDM to identified client stakeholders who are then invited to a Service Review meeting where the details are discussed, and any follow-on actions are agreed and documented.

3.4 Service Desk Information and Processes

3.4.1 Service Desk Information

Cyberfort's Service Desk operates 24 hours a day 365 days a year and is the primary point of contact for all service requests, incidents, events, or support escalations.

Cyberfort Service Desk can be contacted via:

- Telephone 01304 814890
- Email service@cyberfortgroup.com

The Service Desk will undertake initial triaging of any service requests, incidents, or events directly with the client.

The Service Desk will manage all communications in relation to service requests, incidents, or events for IT infrastructure or managed services hosted within Cyberfort.

For security purposes, client validation will be required by contacts recorded in the Authorised Contacts Form prior to any work being undertaken.

Each inbound query made by the client will be captured by Cyberfort's ticketing system and assigned a unique reference number with an appropriate severity level. This severity level will be calculated using an impact, urgency, and priority matrix.

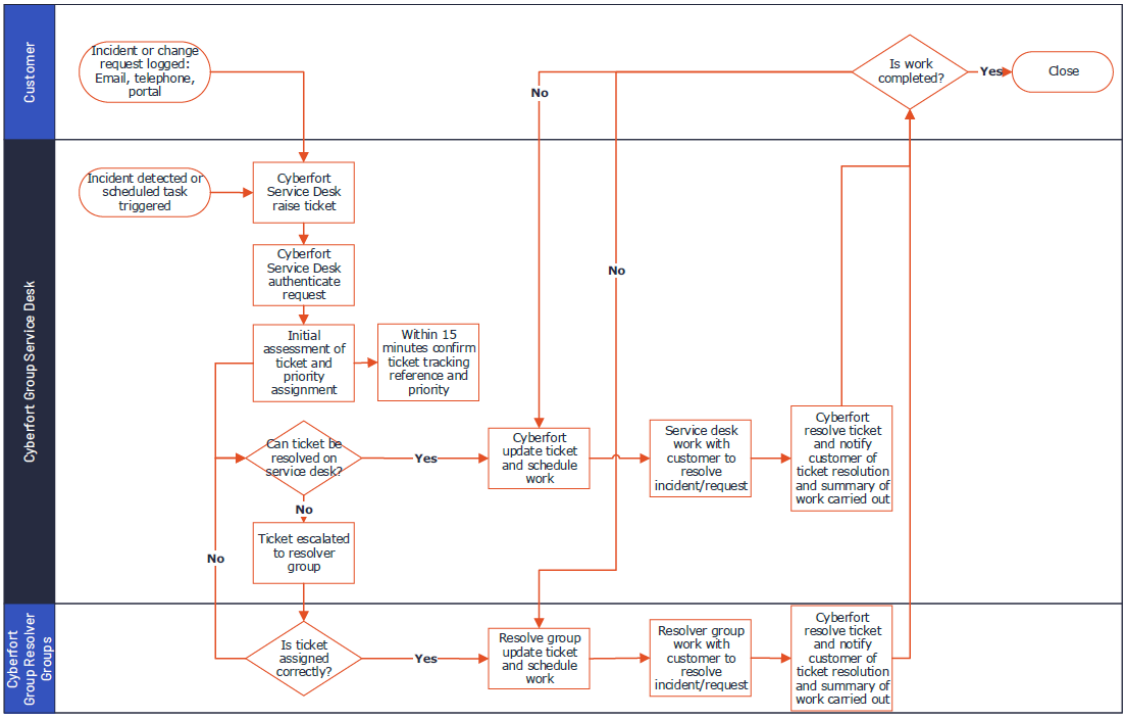
A ticket number will be issued with an initial response within the first fifteen minutes of logging a query. Resolution time goals will be calculated in accordance with a priority matrix. If a client would like to discuss assigned resolution times, they should contact the Service Desk.

Throughout the ticket lifecycle the Service Desk or technical owners will:

- Function as the first point of contact for tickets relating to the provisioned service.
- Ensure tickets are correctly logged, categorised, and prioritised.
- Conduct investigation and diagnosis where appropriate.
- Ensure that all tickets are assigned to the correct analyst or support partners for investigation.
- Manage tickets throughout their lifecycle, escalating where appropriate.
- Keep the client informed of the status of tickets, using ticket updates, telephone communication or emails as appropriate.

3.4.2 Call Handling Process Flow

All tickets logged through the Service Desk will be processed as shown in the figure below.



3.4.3 Client Escalations

In the event that a client is dissatisfied with the progress of their support ticket, they are entitled to request its escalation. Upon such a request, our Service Desk will promptly elevate the matter through our specialised service support engineering team for in-depth analysis and potential solutions. Should the situation necessitate further expertise, it will be advanced to our technical consultancy team to ensure a comprehensive approach to resolution. Recognising the importance of timely and effective responses, escalation to the client's account manager, and depending on the severity, to senior management, will be undertaken to guarantee that all necessary resources are mobilised to meet resolution targets and uphold the highest level of client satisfaction.

4. Commercials & Pricing

4.1 Ordering & Invoicing Process

Please contact us for a quote via email (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.

4.2 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 SFIA 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 detailed in our SFIA rate card framework. Please refer to our Pricing document for more details.

4.3 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.

5. About Cyberfort

As one of the leading cyber security organisations in the UK, Cyberfort is an SME with over thirty years' experience in the market, offering end-to-end cyber security solutions from Consulting to Secure Cloud and Data Centre Services. Security is in the DNA of Cyberfort and our company culture and it's this culture that shapes our approach to ensuring we continue to innovate, improve, develop, and share in the ever-changing world of security.

5.1 Our Values

One Team

We put ourselves in our client's shoes and work together to deliver the best solution. This symbiotic relationship leads to successful outcomes. We are on the same team, our diversity makes us strong; when we collaborate and play to these strengths, we become even more formidable. We respect each other's differences, we give honest feedback and by being accountable for our actions, we act positively to grow and develop.

Transparent

We are responsible for ensuring strong and clear communication with our client; Our bedrocks of trust and professionalism are demonstrated in all that we do. As colleagues, we are open and honest with each other, we share opinions, ideas are sought and given due consideration; we act upon decisions and feedback on outcomes. We trust each other to do the right thing, take pride in our actions and celebrate our successes.

Curious

We are inquisitive and looking to find the best solution, technology and approach for our clients' requirements. Our approach allows us to unpick and probe every avenue with a focus on successful outcomes. Striving for knowledge and driving our own development with energy and enthusiasm, we are constantly questioning how to improve and innovate; by learning from others we will thrive and grown.

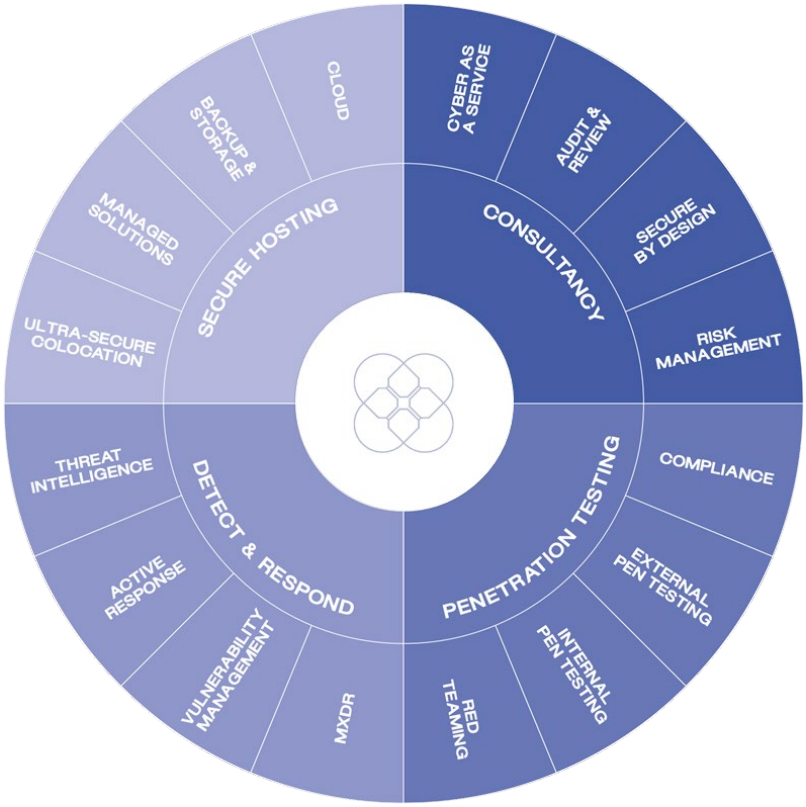
Owners

Providing the best solution and support is not always the easiest path; we proactively support our clients, are empowered to make a difference and take accountability to ensure we do what is right. We step up and do not wait for
others to act, we care about the outcome and showing others that they can trust us to do the right thing.

5.2 Our Accreditations

We're 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.

5.3 Our Services



Consultancy

Cyberfort understands risk and our consultancy services provide you with a realistic view of the risks your business faces and we do this in quantifiable and objective terms. Managing risk is a balancing act between avoiding threats and missing out on positive opportunities; and our consultants are experts in helping organisations achieve this. Our consultants will work closely with you to help you understand your business, cyber and data related risks and where you should focus your available resources. We provide practical advice, helping you implement pragmatic solutions that will help your organisation run smoothly, while keeping risk at a level you're comfortable with.

Detect & Respond

Cyberfort's MXDR services defends clients and pervasively monitors your network. We combine organisational context with security expertise to detect, correlate analyse and respond across the multiple sites, devices and environments that you and your clients depends on. We understand the criticality of the services provided to often vulnerable individuals, and as such our service defends you with a focus on availability, and effective and appropriate defences.

Cyberfort's SOC operates as an extension of your own team, monitoring your environments 24x7x365, detecting, correlating and analysing events, and providing both guided response and active defences for your environment under your predefined governance.

Penetration Testing

Cyberfort's Penetration Testing and Offensive Security will give you the confidence that the technology you are using or developing is as secure as it possibly can be, and if it isn't - what you need to do. Whether you are developing internal software solutions, or you want to ensure your own infrastructure is secure, you need to test your technology for vulnerabilities. This is done by carrying out a penetration or 'pen test' of your IT infrastructure. Cyberfort pen testers are renowned for finding system vulnerabilities other pen testers just haven't dug deep enough to uncover. We tell you what you don't know, not what you know already, allowing you to make informed decisions about where best to invest your resources and budget.

Secure Hosting

Our cloud services are designed to enable your organisation to deliver hosted cloud services in a secure way. We ensure your mission-critical data is always secure and available within our ultra-secure, UK-based data centres. We partnerwith you, becoming a trusted extension of your team and designing bespoke solutions that enable you to grow and meet your business objectives. Our cloud services include public cloud and bespoke technical solution architecture, managed public and private clouds, hosting, colocation services includingsecure and managed suites.

6. Our Experience

Our clients range from the largest of HMG departments, to non-departmental public bodies including projects of critical national infrastructure status. Our private sector work is equally wide-ranging, including blue-chip and FTSE companies, SMEs and agile technology start-ups.

6.1 Case Study Example

UK HMG DEPARTMENT

The Challenge

Clients required to comply with MoD and Cabinet Office SbD Principles and Process.

Using SbD approach, client needed holistic management of security requirements including Security Architecture, 1st Line and 2nd Line Risk and Governance, Vulnerability Management, Controls Testing and Supplier Assurance.

The Solution

Working with the client to migrate their legacy estate into cloud infrastructure, we embedded Secure by Design (SbD) within the Cyber Team's agile processes and wider governance authorities (Technical Design Authorities, Technical Assurance Board, and Product Design Governance). Supporting, influencing and assuring every stage of design from Digital Solution Vision, High Level Design, Low Level Design through to delivery. This has fostered an increased willingness to take decisions and a more open and effective relationship between SbD functions and the programme risk and project teams.

We embedded the SbD principles to our service delivery, ensuring that the client has a high level of confidence in the SbD process. This approach has ensured the integration of security practices and considerations required to deliver the programme 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 mitigating potential risks throughout the entire development life cycle all framed by NCSC SbD Principles on which the UK Government Security 10 SbD Principles are based. By driving key activities that support these principles, ensuring clients risk management is centric to the assurance landscape, our client better understand the risk they are exposed to and proactively respond to and manage the vulnerability landscape.

The Outcomes

Cyberfort delivers a complete cradle-to-grave security risk and governance management function. The introduction of clients' Cyberfort Security approach is enabling the opportunity to remediate or reduce vulnerabilities and associated new and legacy risks at an early stage by implementing a SbD analysis and guidance approach with appropriate, independent architectural governance, facilitated with timely ITHC checks to validate design findings, and confirm remediation of previously identified vulnerabilities as they have been implemented in the design and build sprints. Cyberfort follows the risk assessment process aligning to the NCSC Risk Management framework, industry best practice and continual security governance aligned to the HMG Orange Book. The colocation of live proactive Security Operations monitoring, and central Management Information Systems collation allows the use of automated analysis and identification of new vulnerabilities, changes in behaviour and active monitoring from a central point, where previously, individual vendors and 3rd parties were responsible for monitoring the assets they were contracted to supply. As a result, the client has eliminated the vulnerability of not being in possession of a complete threat picture, where now they can manage their IT estate from an informed real-time view of risk, ensuring compliance to all legislation, HMG guidance and industry best practice within the timescale set by clients.

7. 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:

7.1 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.

7.2 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.
- 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.

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

CYBERFORT

www.cyberfortgroup.com

For more information, please contact us on:

01304 814800

info@cyberfortgroup.com