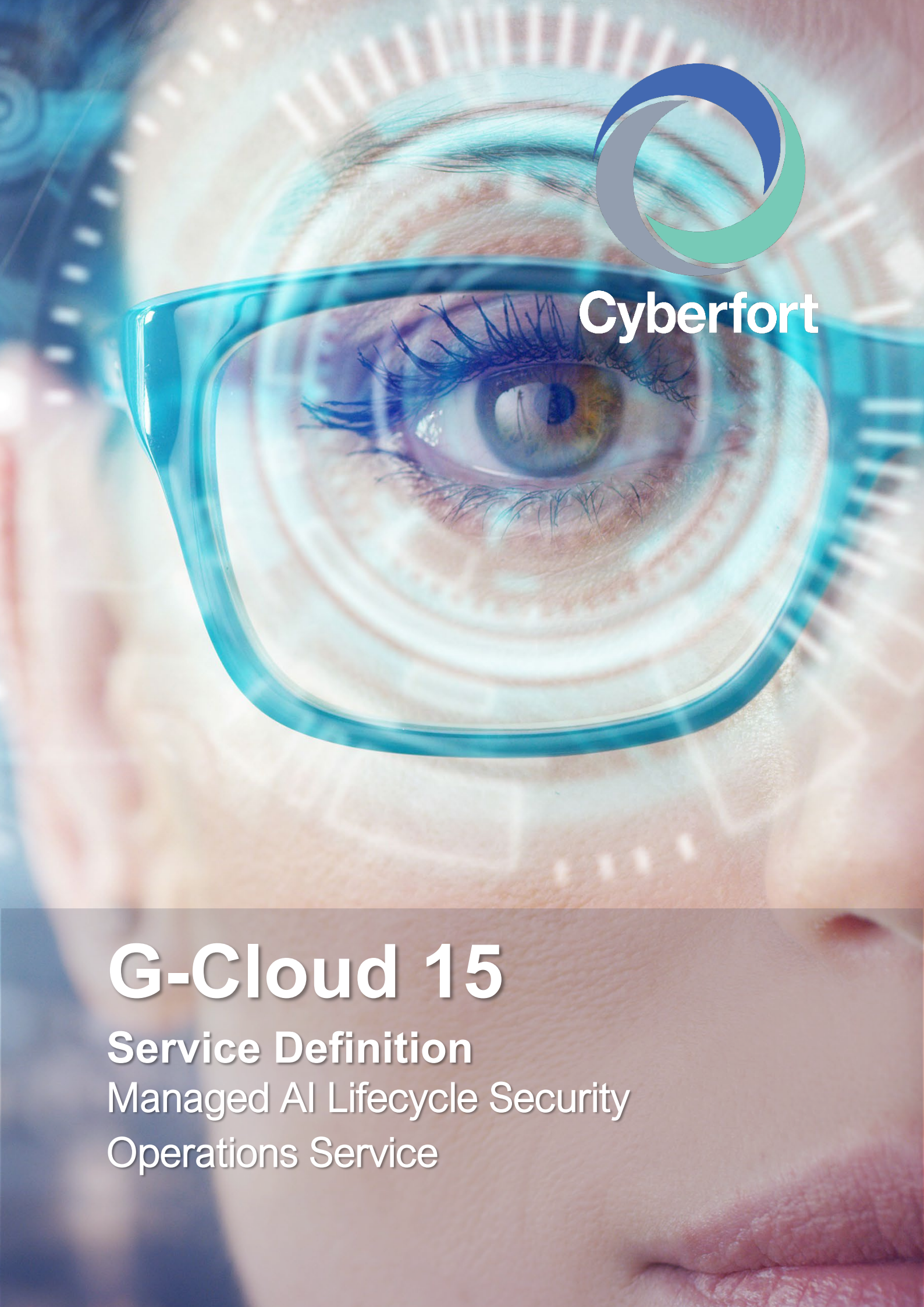


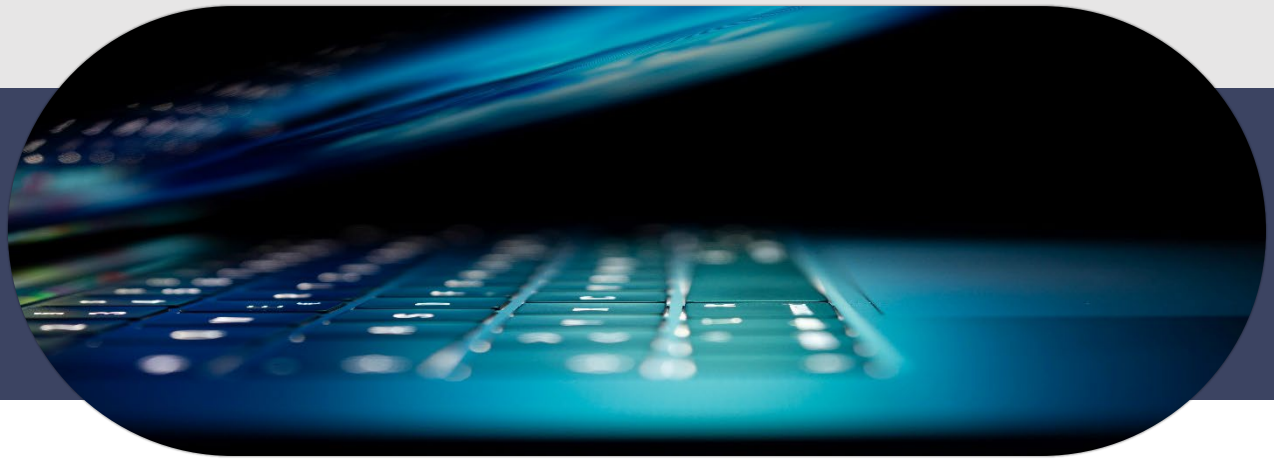
Cyberfort

G-Cloud 15

Service Definition

Managed AI Lifecycle Security Operations Service

Table of Contents



1. Service Overview

Cyberfort's Managed AI Lifecycle Security Operations Service delivers peace of mind by helping organisations securely design, build, deploy, and operate AI systems across their full lifecycle. Our service provides deep visibility into AI-related security risks, misuse, and threats — supported by specialist security consultants and analysts who apply proven cybersecurity best practices and AI-specific security expertise.

We deliver an innovative service underpinned by robust methodologies aligned to recognised security frameworks, integrating up-to-date threat intelligence, attacker tactics and techniques, and emerging AI threat patterns. Service management works alongside our cybersecurity specialists from day one, ensuring you benefit from a consistent, secure, and commercially accountable experience.

We pride ourselves on delivering a holistic approach to AI security. By considering the organisation as a complete system — including people, process, data, platforms, models, and supply chain dependencies — we enable organisations to adopt AI confidently without compromising safety, compliance, or operational resilience.

Cyberfort's Managed AI Lifecycle Security Operations Service includes the following key elements:

- **AI Security Awareness and Training:** Reduces human-driven AI risk and unsafe usage behaviours across business and technical teams.
- **AI Developer best practise and training:** Assures any challenges shift left into the development lifecycle promoting security as BAU and reducing both risk and cost.
- **AI Governance and Secure-by-Design Engineering:** Establishes policies, guardrails, design principles, and secure implementation patterns.
- **AI Security Testing:** Specialist testing for GenAI and ML solutions, including prompt injection, data leakage, insecure integrations, and agent abuse.
- **Continuous Monitoring:** Detection and oversight for AI environments, AI usage patterns, anomalous behaviour, and risk indicators.
- **Incident Support and Response Guidance:** Enables rapid triage and remediation when AI-related security incidents occur.

Utilising proven security practices and evolving AI security risk intelligence, our service supports secure delivery of innovation — from experimentation through production and ongoing operation.

1.1 Service Detail

Cyberfort's Managed AI Lifecycle Security Operations Service includes the following capabilities and services:

1.1.1 Lifecycle Security Coverage (End-to-End AI Protection)

We provide security assurance throughout the AI lifecycle, including:

- AI strategy and use-case risk assessment
- Data sourcing and preparation controls
- Secure model development and tuning
- AI application build (including RAG and agentic workflows)
- Deployment into production environments

- Ongoing monitoring and continuous security improvement

This ensures AI systems are protected as they evolve, and that security remains consistent as AI capabilities scale across the business.

1.1.2 Alignment to your organisation's risk, governance, and AI adoption roadmap

We align the service to your organisation's risk appetite, threat landscape, and AI maturity. This includes establishing contextual awareness of:

- AI use-case sensitivity and impact
- Data classifications and privacy requirements
- Model and vendor dependency risk
- Integration points (APIs, plug-ins, tools, agents)
- Operational environments and user groups

This approach maximises security ROI while supporting business enablement rather than security delay.

1.1.3 Single point of commercial and technical expertise

Cyberfort provides clear ownership and accountability through:

- A dedicated, named Commercial Account Manager acting as your representative within Cyberfort, providing a single point of escalation and commercial alignment.
- A dedicated, named Technical Account Manager (TAM) acting as a first point of contact for operational matters, service optimisation, and proactive improvement.

The TAM provides continuous guidance and recommendations to improve AI security posture based on service insight and evolving AI risks.

1.1.4 AI Risk Profiling, Assurance and Control Validation

Our service is not based on generic advice or "tick-box" assessments. We apply a structured approach to identify:

- What AI systems are in use
- What data they access
- How they integrate with other services
- How they could be attacked, misused, or manipulated
- What immediate improvements reduce risk fastest

We deliver prioritised recommendations and practical remediation guidance aligned to business value and threat likelihood.

1.1.5 Active and passive security responses

Cyberfort provides response support for AI-related incidents and identified risks.

Passive responses include:

- Guided recommendations on containment, remediation, secure design improvements and governance reinforcement.

Active responses (where tools/integration permit, and under client governance) include:

- Applying agreed controls, disabling exposed access paths, and supporting implementation of mitigation actions via defined playbooks.

1.1.6 AI Security Testing and Validation

Our service includes AI security testing aligned to real-world threats, including:

- Prompt injection and jailbreak testing
- Data leakage testing (sensitive data extraction and inference risk)
- Model misuse and unsafe output testing
- Insecure integration testing (APIs, tools, plug-ins, third-party services)
- Agent workflow abuse and unintended behaviour testing
- Weak access control and identity enforcement review

Testing can be performed periodically and aligned to change events, such as new releases, model updates, or new integrations.

1.1.7 Continuous Monitoring

Cyberfort delivers continuous monitoring of AI system security signals and risk indicators, aligned to your environment.

Monitoring typically includes:

- Identity and access behaviours related to AI tooling
- Indicators of misuse or abnormal usage patterns
- Data egress indicators and sensitive prompt exposure risk
- Application logs and AI workflow events
- Alerts linked to high-risk user activity or suspicious automation
- AI pipeline and deployment observability

Where applicable, we help integrate monitoring signals into your security operations workflow for correlation and escalation.

1.1.8 Threat Intelligence for AI Risk

We use actionable threat intelligence to inform:

- AI-specific detection patterns
- Testing and red-team priorities
- Threat modelling and risk control recommendations
- Horizon scanning of emerging AI attacker techniques

This ensures your AI security controls remain aligned to emerging threats rather than only historic attacks.

1.1.9 Evidence and Reporting

Our service includes:

- Regular service reporting
- Risk and maturity insight

- Evidence of control adoption and improvements
- Action plans and prioritised remediation recommendations

Reporting cadences can be agreed, but are typically:

- Monthly service reporting
- Quarterly service review (QSR) sessions
- Annual strategic assurance review aligned to the AI roadmap

1.1.10 Continuous Improvement & Efficiency

AI risk changes rapidly as AI systems evolve. Cyberfort continuously improves:

- Risk controls and guardrails
- Testing methods and scenarios
- Detection logic and monitoring signals
- Playbooks and incident workflows

This ensures long-term resilience rather than a one-off point-in-time assessment.

1.1.11 Technical Requirements

Technical requirements are defined during onboarding and typically include:

- Identification of AI services in scope (e.g., LLM platforms, AI products, internally hosted models, copilots, assistants, agent frameworks)
- Access to appropriate system logs, configuration data, and security telemetry
- Agreement on escalation routes and incident handling expectations
- Integration to existing security tooling where available (e.g., SIEM, identity platforms, endpoint tooling, CASB/DLP)
- Ability to validate AI control implementation (policy, access controls, data flows, and deployment pipelines)

Where required, Cyberfort can provide guidance on enabling improved logging and monitoring coverage for AI services.

1.1.12 Outage and Maintenance Management

The platforms and environments that underpin AI delivery are often cloud-hosted and managed by the client or third-party providers. Cyberfort provides service management support to:

- Maintain monitoring and assurance coverage
- Identify control drift and configuration change risk
- Support secure updates and release cadence changes
- Manage change and risk review against AI system updates

1.1.13 Hosting Options and Locations

Cyberfort's service supports cloud-hosted, hybrid, and multi-environment AI deployments. Cyberfort resources and service delivery teams operate from the UK. Service delivery models may include:

- Client-hosted AI systems (in your cloud tenant / environment)
- Third-party AI service providers (with integration and policy governance)

- Cyberfort-managed monitoring and assurance processes (as agreed)

1.1.14 Access to Data (Upon Exit)

All client data remains the property of the client.

Upon exit, Cyberfort will support:

- Knowledge transfer and transition support
- Provision of service artefacts (reports, control recommendations, risk registers where agreed)
- Agreement-led handling of monitoring data and incident records, aligned to your governance and contractual requirements

1.1.15 Security

Cyberfort services are governed by stringent security policies, procedures, and controls aligned to cybersecurity best practices. Key security control principles include:

- Least privilege access and governed escalation
- Modern authentication (MFA) and conditional access guidance
- Secure handling of service data and client-provided information
- Encryption in transit and at rest (where applicable)
- Staff training, governance alignment, and auditable service processes
- Secure operating procedures aligned to continuous monitoring and incident support

2. Onboarding and Offboarding Support

2.1 Deployment and phasing

To simplify delivery, Cyberfort adopts a structured and repeatable approach to ensure rapid and consistent onboarding.

Our onboarding approach provides:

- Reduced onboarding time through structured workshops and defined outputs
- Reduced internal client effort by maximising Cyberfort-led implementation
- A flexible deployment approach aligned to client governance and regulatory requirements
- A phased onboarding approach aligned to AI risk priorities (e.g., high sensitivity systems first)

2.1.1 Onboarding process

The onboarding process typically includes:

- Initial stakeholder discovery and scope definition
- AI service and system mapping
- Data and integration understanding
- Security governance and role mapping
- AI lifecycle risk assessment and prioritisation
- Monitoring and testing plan design
- Operationalisation into service cadence and reporting

Workshops may be repeated for different AI systems or service lines depending on complexity and scale.

2.1.2 Offboarding

Offboarding plans are developed consultatively with the client and may include:

- Final reporting and transition documentation
- Handover of ongoing improvement backlog
- Support for alternative provider transition (if required)

2.1.3 Service Constraints and Customisation

Cyberfort's managed AI service is designed to be adaptable across AI adoption patterns, including:

- AI-enabled applications
- LLM-powered assistants and copilots
- Retrieval Augmented Generation (RAG) systems
- Agentic workflows and tool-enabled AI services
- Machine learning models and pipelines

Customisation is achieved through scoping, risk prioritisation, and jointly agreed service outputs.

3. Service Management Approach

3.1 Service Delivery Teams

Cyberfort provides a cross-discipline service team to deliver the Managed AI Lifecycle Security Operations Service, including:

- **Principal Security Consultant (AI Security Lead):** Oversees overall delivery quality, methodology, and escalation leadership.
- **Senior Security Analysts / Consultants:** Conduct AI security assessments, testing, assurance, and incident support.
- **Security Architect:** Supports secure design patterns, governance controls, and engineering assurance guidance.
- **Security Engineer:** Supports integration, telemetry, and monitoring enablement where required.
- **Technical Account Manager (TAM):** Owns client service delivery experience, reporting cadence, and continuous improvement.
- **Commercial Account Manager:** Supports commercial governance, escalations, and stakeholder alignment.

3.1.1 Service Cadence and Communications

Cyberfort provides structured service communications aligned to client requirements, typically including:

- Regular service reporting
- Scheduled operational touchpoints
- Quarterly strategic review sessions
- Incident escalation communications as required
- Continuous improvement planning and prioritisation

4. Commercials & Pricing

4.1 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.

4.2 Service pricing model

Cyberfort's AI Security service pricing consists of a number of optional components to create the service charge.

- An onboarding charge which covers the discovery, design and preparation for the service elements selected.
- The ongoing service charge covers the delivery of the services selected, including user and developer awareness, design assistance, security assurance and monitoring.

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. 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:

5.1 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.

5.2 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.

5.3 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

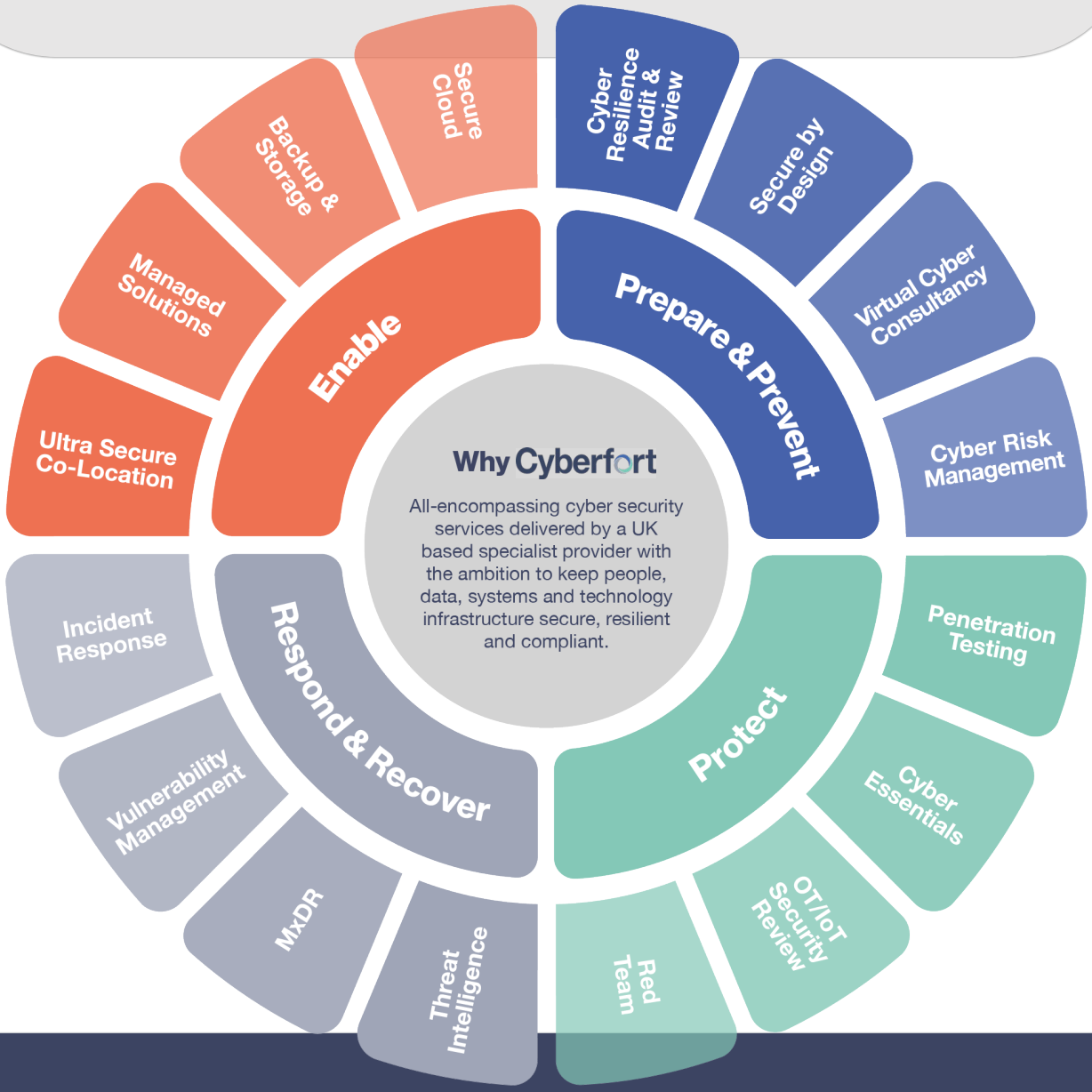
About Cyberfort

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