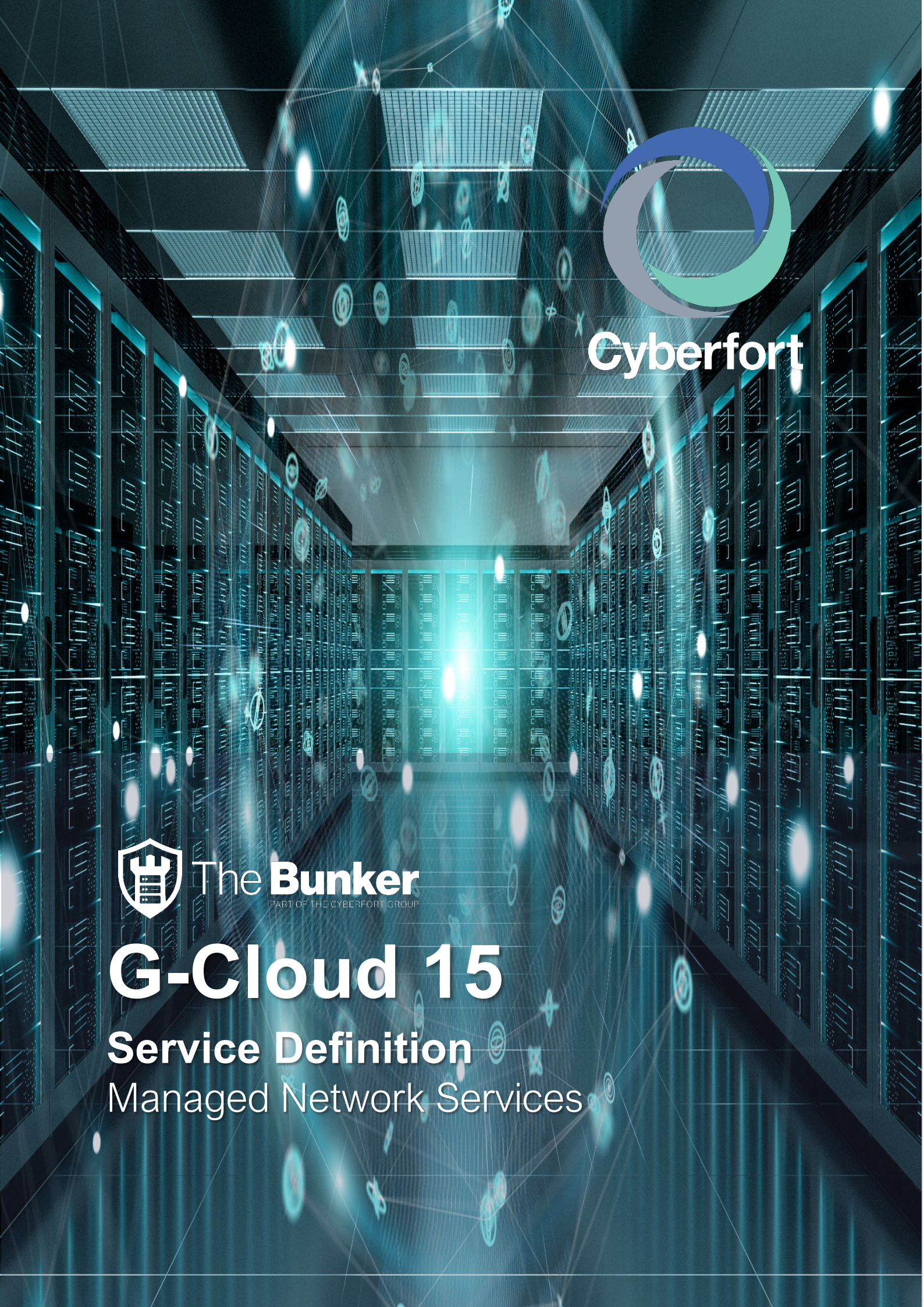
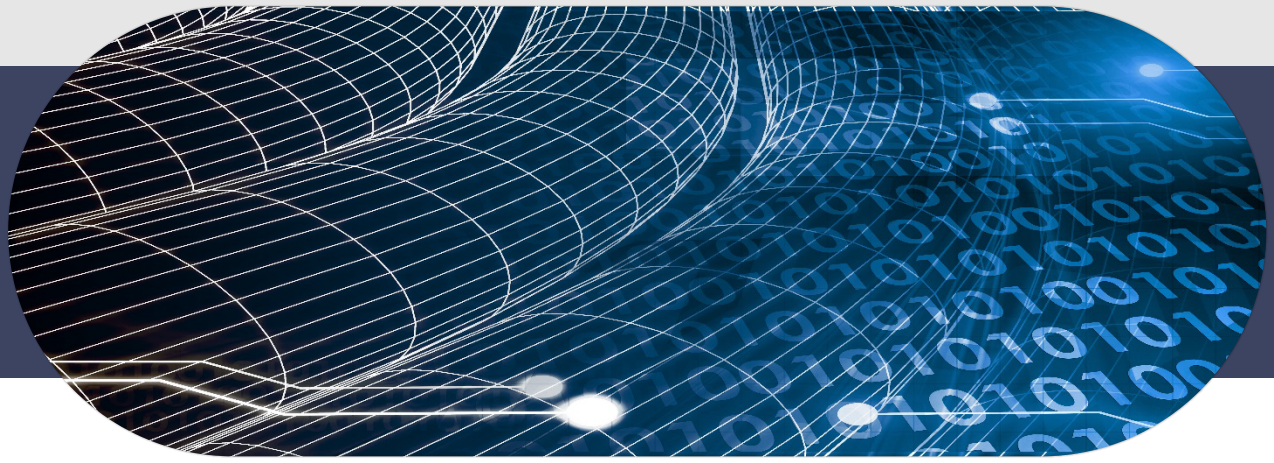


G-Cloud 15

Service Definition

Managed Network Services

Table of Contents



1. Service Overview

Cyberfort's Managed Network Services offer customisable connectivity solutions tailored to your requirements. Whether it's managed networks, firewalls, private MPLS links, DDoS protection, or load balancing, we collaborate to design and construct a secure, interconnected network, empowering your business with reliability and flexibility.

1.1 Service Detail

1.1.1 Firewalls

Cyberfort's Managed Firewall Service draws on our experience and depth of knowledge in protecting data through design and management. We will ensure best practices are employed at the edge of your network zones – building and taking care of the on-going configuration of firewall rules and policies. We will also layer additional next-generation features that will further increase security as an in-depth defence method, limiting the attack surface of your internet-facing systems and reducing the risk of cybercrime through breaches in perimeter security.

Our firewalls go beyond traditional access control lists, using advanced methods of protection based on Application Control, User and Role-based policies, Intrusion Detection and Prevention, and SSL and Deep Packet Inspection.

Cyberfort's Web Application Firewall (WAF) capability, adds additional layers to your firewall, sitting at the application layer inspecting every request against your application, reporting or blocking, suspicious and malicious connections against a tailored ruleset for your application requirements. WAF's are a critical part of compliance standards, assisting to ensure standards like PCI DSS are met with the highest levels of security, protecting critical information to provide the level of security you need.

The frequency and severity of data breaches are increasing at an alarming rate and the financial and reputational damage a breach can inflict on an organisation is escalating to unprecedented levels. Protecting the confidentiality and integrity of business and personal data needs to take precedence on every Board-level agenda so that every measure can be taken to avoid such a breach.

1.1.1.1 Client Challenges

- The staffing and training expenses of maintaining a dedicated network security team available 24/7/365.
- Not possessing the specialist knowledge required to build and maintain hardened firewalls to protect internet applications/services.
- The need to deploy firewall-based perimeter defences to preserve the confidentiality, integrity and availability of critical IT systems.
- Requirements beyond traditional firewalls – Web Application Firewall (WAF) / Secure Sockets Layer (SSL) inspection / Intrusion Detection and Prevention System (IDS/IPS).

1.1.2 Managed WAN

By utilising our MPLS services and managed firewall options, we can connect your remote locations together through secure and dedicated connections. This solution protects your traffic against prying eyes and provides predictable latency backed up by SLA's.

Our managed firewall offering, combined with private MPLS links, provides a fully encrypted end-to-end tunnel for your traffic. These can range from simple point-to-point tunnels, or more complex meshed topologies using Group VPNs.

1.1.2.1 Client Challenges

- When you send traffic across the Internet, you really have no control over how it will reach its destination. This could lead to your traffic being maliciously intercepted, or even just taking an extra-long route.
- With a Managed WAN network, you get a dedicated pipe for your traffic between locations. This pipe will be bound by contractual SLAs and will guarantee delivery. A managed firewall will ensure that all of your traffic is encrypted and the pipe is secured, while multiple pipes from multiple providers can also be utilised to provide a fully redundant service.

1.1.3 Load Balancers

Load balancing distributes load across multiple servers. It enables you to carry out scheduled maintenance work and, should a server fail, there's one ready to take over. With this increased level of redundancy, having a load balancing solution in place allows your end-users to have a seamless, uninterrupted and unaffected experience in any situation.

Both layer 4 and 7 load balancing options are available , improving the availability, performance and end-user experience of your business critical applications and websites.

At Layer 4, a load balancer has visibility on network information such as application ports and protocol (TCP/UDP). The load balancer delivers traffic by combining this limited network information with a load balancing algorithm, such as round-robin, and by calculating the best destination server based on least connections or server response times.

At Layer 7, a load balancer has application awareness and can use this additional application information to make more complex and informed load balancing decisions. With a protocol such as HTTP, a load balancer can uniquely identify client sessions based on cookies and use this information to deliver all a client's requests to the same server. This server persistence using cookies can be based on the server's cookie or by active cookie injection where a load balancer cookie is inserted into the connection.

1.1.3.1 Client Challenges

- Load balancing gives you the ability to removes single points of failure from an infrastructure, whilst facilitating simple horizontal expansion to optimise infrastructure for performance.
- Scalability and future proofing are added benefits, allowing you to scale horizontally in a seamless fashion.
- Additional functionality can be delivered including Encryption offloading and basic DDoS protection.

1.1.4 GSLB

Global Server Load Balancing (GSLB) is a technology which directs network traffic to a group of data centres in various geographical locations. Each data centre provides similar application services, and client traffic is directed to the optimal site with the best performance for each client. GSLB monitors the health and responsiveness of each site, and like Server Load Balancing, directs traffic to the site with the best response times.

Services, or groups of services, can be defined as virtual pools with sites across multiple geographically diverse locations. End-users connect to a Virtual IP (VIP) address that lives on or within the GSLB infrastructure.

When a connection arrives on the GLSB infrastructure a decision is made on the optimal location to send the traffic. Defined rules and health checks allow highly granular choices to be made.

These check the health of both site and services, based on customised monitoring points that examine facets of the infrastructure and applications (from Layer 4 through to Layer7).

1.1.4.1 Client Challenges

GSLB can help you if you require any of the following services:

- Traffic routing of client traffic to most appropriate data centre site.
- Monitoring of the health, availability and loading for each data centre.
- Redirecting client traffic away from a failed or unhealthy site.
- Calculating client geographical locations to direct traffic for optimal site selection.
- Controlling and optimising multi-site data centre deployments with management policies.
- Delivering SLA expectations to clients.
- Meeting regulatory requirements for countries with specific, in-country restrictions.

Provide customized content specific for countries, regions or languages.

1.1.5 Switches

Whether you have servers in a rack or users in an office, everything needs to be connected together.

A managed switched network from Cyberfort provides you with a safe and secure network for your devices. Deployment topologies can be best designed to meet your business and security requirements.

Cyberfort will take all the complication out of the process for you. We buy the hardware, configure the devices as per your requirements, deploy the devices and then monitor and manage the switches.

1.1.5.1 Client Challenges

All switches should be locked down and secured to protect their integrity, especially those located in remote locations, outside of Cyberfort's strict physical security. All switching architectures should also be implemented in a way that protects their availability. By implementing fast and resilient architectures, we can minimise your office or data centre downtime.

1.1.6 Unique Service Points

- As a security-focused company, Cyberfort has decades of experience protecting the confidentiality, integrity and availability of our clients' critical IT systems.
- We pride ourselves on working with clients to deliver successful outcomes. This means providing a clear portfolio of services, a consultative approach and always being flexible to our clients' needs.
- Cyberfort operates from two geographically separate, ex-MoD decommissioned nuclear bunkers, protected by the best physical security available. Our service is protected within ultra-secure fortresses of three-metre-thick reinforced concrete, built to withstand a nuclear strike.

- Our service desk is entirely UK-based, vigilant and available 24x7x365 PRINCE2 qualified project management teams.
- We can provide 100 percent uptime with auto failover to secondary sites.
- Fully redundant, multi-homed, 10 gigabit network between data centres and to metropolitan PoPs.
- Physical security – including 3m thick reinforced concrete walls, solid steel doors, CCTV system with 24-hour video recording.
- Visual verification of all persons entering the data floors, no unescorted access.
- Electro Magnetic Pulse (EMP) protection, Tempest RFI intrusion protection, shared or dedicated partitioned areas redundant power, cooling and Carrier Neutral connectivity..

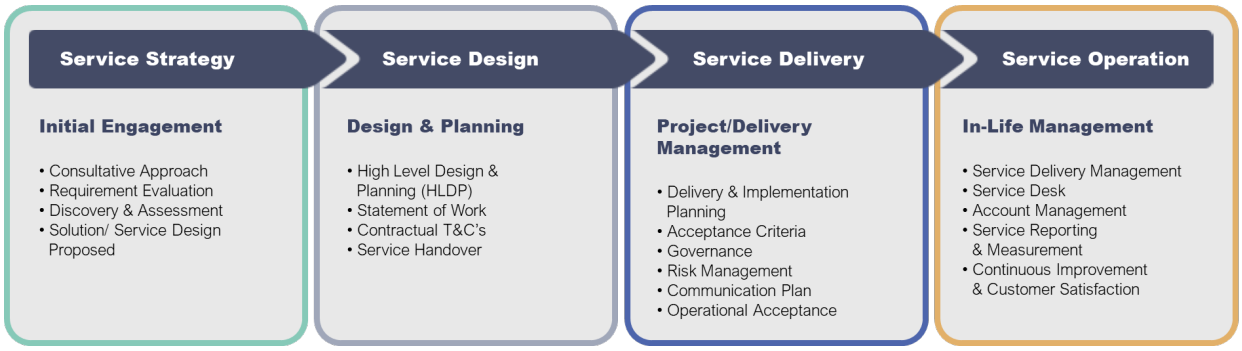
2. Delivery Approach

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:

2.1 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.

Fig.1: Cyberfort Lifecycle Journey



2.1.1 Service Strategy: Initial Engagement

- Consultative Approach: We will engage and work collaboratively and in partnership with our clients to ensure delivery of the specific requirements.
- Requirement Evaluation: We conduct a stakeholder engagement meeting, or a series of meetings/workshops, to understand specific aspects of business challenges and requirements.
- Discovery & Assessment (DA): The DA phase is critical to providing the foundation for successful outcomes, 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.

2.1.2 Service Design: Design and Planning

- High Level Design and Planning (HLDP): Upon completion of the initial engagement 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.

2.1.3 Service Delivery: Project/Delivery Management

- Delivery and Implementation Planning: The assigned Project/Delivery Manager will lead a Project-Kick Off meeting with the client. A Delivery and Implementation plan is created to define project specific deliverables, dependencies, resource requirements and timeframes.
- 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.

2.1.4 Service Operation: In-Life Management

- Service Delivery Management (SDM): The SDM will work closely with the client building strong relationships and maintain regular communication ensuring a high level of service.
- Service Desk: Cyberfort's 24x7x365 Service Desk will manage all communications in relation to incident or request management.
- Account Management: Your Account Manager acts as your internal Cyberfort ambassador, leading the delivery and management of all commercial matters. They facilitate regular engagement and are accountable for all services provided.
- 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

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.

3.1 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.

3.2 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.

3.3 Service Desk Information and Processes

3.3.1 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.

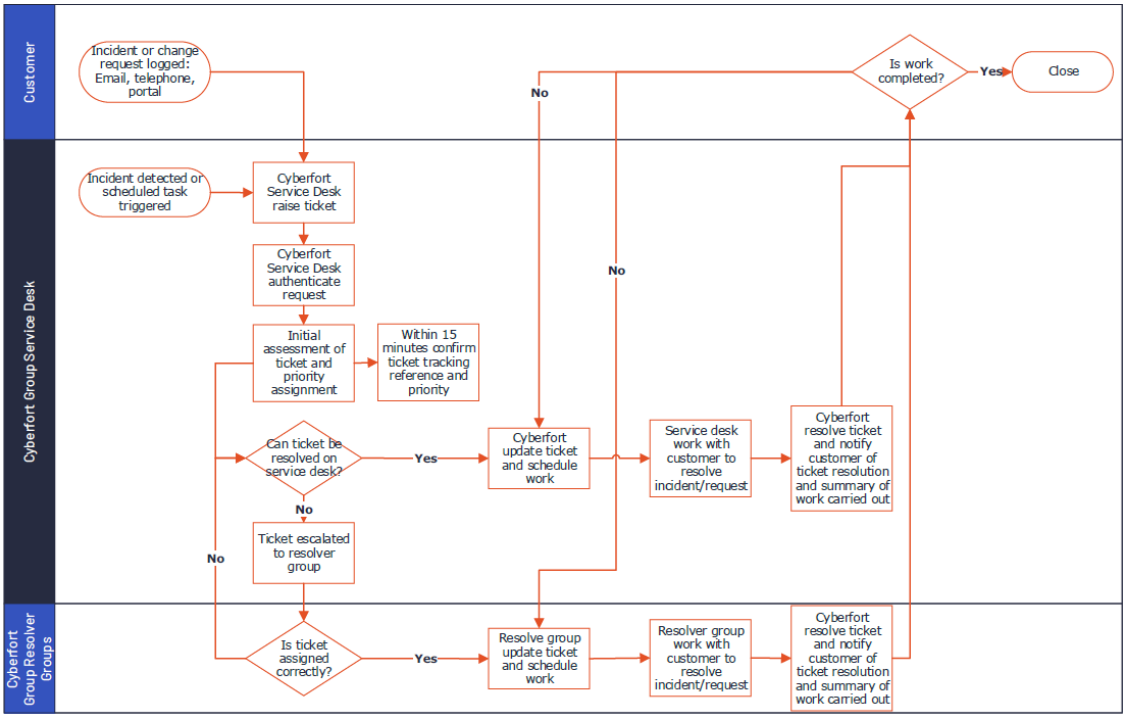
A ticket number will be issued with an initial response within the first fifteen minutes of logging a query. Resolution time goals will be calculated in accordance with a priority matrix. If a client would like to discuss assigned resolution times, they should contact the Service Desk.

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.

3.3.2 Call Handling Process Flow

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



3.3.3 Client Escalations

If a client is dissatisfied with the progress of a support ticket, they may request an escalation. The Service Desk will escalate the issue to the service support engineering team for further analysis and resolution. If additional expertise is required, the matter will be referred to the technical consultancy team. Where necessary, the issue will also be escalated to the client's account manager and, depending on severity, to senior management to ensure timely resolution and maintain client satisfaction.

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 services are priced on your committed resource total (compute and storage) per month. Additional units of work are charged on a day rate depending on the services required. Service provisioning charges will be required depending on the service requirements set out at the scoping/advisory stage.

4.3 Hosting options

Cyberfort MCX is hosted on Cyberfort's multi-tenant platform, available in either of our Data Centres. Configuration is designed based on customer requirements and Disaster Recovery solutions can be provided across our geographically diverse, isolated platforms.

Pricing for the install will depend on integration costs, and these differ for each customer. These costs will be provided in each customer's quotation.

4.4 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.
- Government Cyber Security Strategy, including National Cyber Security Centre (NCSC).

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