

Managed Cyber Security Operation Centre (CSOC)

GCloud 11 Service Definition document

Lot 3 - Support

Crown
Commercial
Service
Supplier

RM1045, RM3804
& RM1557

 **HEALTH &
SOCIAL CARE
NETWORK**

RM3825 ACCESS SERVICE FRAMEWORK



HM Government | G-Cloud



Table of Contents

Introduction.....	3
Features	3
Benefits.....	3
Service Planning, Transition & Onboarding	3
Overview	3
Customer Pre-Requisites	4
Understanding Customer Infrastructure	4
Planning & Designing the CSOC Service	4
Transition / Onboarding	4
Training.....	4
Go-Live.....	4
Off boarding.....	4
Exponential-e CSOC Mission Statement & Goals	5
CSOC Goals	5
Working with Exponential-e.....	5
Introduction.....	5
Our Network.....	5
Our Accreditations.....	6
Our Promise.....	7
Exponential-e's Approach.....	7
Thought Leadership and Applied Innovation	8
Meeting our Brand Promise	8
Our Security Capabilities	9
Security assurance.....	9
Connectivity.....	9

Introduction

The Exponential-e Cyber Security Operations Centre (CSOC) is a specialised unit to help your organisation prevent, detect and respond to a range of threats.

Exponential-e's CSOC (Cyber Security Operations Centre) provides customers with best-in-breed real-time security services. Detecting and reacting to threats while protecting customer's assets.

We enable you to reduce risk and increase your IT resilience.

Features

- ✓ 24x7x365 real-time monitoring, analysis, alerting and reporting
- ✓ Manual evaluation and investigation by certified security experts
- ✓ Easy integration with existing solutions
- ✓ Purpose-built system provides full and flexible security management
- ✓ Categorise devices and assets with advanced business logic
- ✓ Powerful processing of high volumes of data
- ✓ Simple management platform presents reports and ticket investigation
- ✓ Generate insight through analytics

Benefits

- ✓ Monitor your whole security estate
- ✓ Fast incidence response
- ✓ Reduced risk and increased cyber security
- ✓ Integrate advanced technology and multi-layered solutions.
- ✓ Reduced capital expenditure
- ✓ Simplified operating model with increased automation.
- ✓ Accountability and support from certified cyber security analysts.
- ✓ Analytics and full visibility
- ✓ Manage and report on compliance

Service Planning, Transition & Onboarding

Overview

The Exponential-e Cyber Security Operations centre (CSOC) is a specialised unit to help organisations prevent, detect and respond to a range of threats. The CSOC provides monitoring and alerting for all of your systems and infrastructure – regardless of size, geography and manufacturer, enabling reduced risk and increased IT resilience.

Customer Pre-Requisites

Customers are asked to complete a Solutions Viability questionnaire to get a clear overview of the organisation infrastructure and gather information for the onboarding of the CSOC. If possible a topology will need to be completed.

Understanding Customer Infrastructure

We will use a topology (network architecture) for designing the solution and understanding how the customers network looks and create a Statement of Works (SoW) which will define the deliverables, the design, the resources, the deployment model as well as the monitoring and alerting parameters for the CSOC service.

Planning & Designing the CSOC Service

The planning and designing of the CSOC is implemented by completing a solutions viability questionnaire and a statement of work which will define the deliverables, the design, the resources, the deployment model as well as the monitoring and alerting parameters for the Cyber Security Operations Centre (CSOC) services.

Transition / Onboarding

- ✓ Configuration of the intrusion detection system
- ✓ Customisation of security rules to be tailored to the customer
- ✓ Silencing of “noisy” logs and false positives
- ✓ Agreement of pin number to be used during call with customer
- ✓ Will take period of 6-9 weeks for the transition phase to be completed

Training

During the transition period the customer will have weekly calls to explain how to use the system and discuss any possible alarms generated that week and customers may ask any questions to have a better understanding before CSOC goes live.

Go-Live

After the transition and onboarding stage is completed, there will be a week to handover the system to the 24/7 analysts called the staging period.

Off boarding

The off boarding is simply removing the server from the customer’s site (if physical) or deleting the server (virtual). The logs will be handed back to the customer and they are kept for 365 days.

Exponential-e CSOC Mission Statement & Goals

CSOC Goals

- ✓ Rapid onboarding of new detective, reactive and/or protective technologies to each client's unique service stack.
- ✓ Data analysis capability for real-time threat detection, general threat landscape analysis and customer threat trending.
- ✓ A 'no incident' service to our customers, in the context of our services.
- ✓ Incident Alerting and Notification to minimise incident impact.
- ✓ Complete UK data Sovereignty of service. No data off-shoring.
- ✓ Compliance to Major Standards.
- ✓ Service delivery across Exponential-e's core network and any public Internet services.
- ✓ Service quality, technical excellence and Exponential-e's endless dedication to good service.

Working with Exponential-e

Introduction

Founded in 2002, we are an award-winning, privately owned British Cloud and Connectivity provider. The majority owner, CEO and founder of the company - Lee Wade - is still at the helm of Exponential-e and demonstrates the same passion for our customers, service innovation and business as he did at our inception. We pride ourselves on delivering super-fast, low latency Connectivity, flexible and resilient Cloud solutions Unified Communications, Cyber Security and world-class IT Services. Organisations from all sectors of the economy run critical services underpinned by our technological innovations. We deliver leading-edge solutions to over 2,200 customers in every vertical sector.

Our Network

Exponential-e's own Cloud infrastructure is fully integrated with our 100 Gigabit Carrier-Class Ethernet Network, utilising premium grade enterprise compute, and is supported by our UK based 24x7x365 Customer Service Desk to deliver a non-stop compute platform to you and your end users.

What differentiates us from the competition is how we utilise our own network to deliver multiple services over one connection, with 100% Network visibility and control, and the cost efficiencies this provides our customers. Our fusion of complementary technologies, a carrier-class network and Cloud infrastructure, means we can deliver enterprise applications at super-fast, low latency, with an end-to-end SLA, for a superior end-user experience.



17 year pedigree of delivering enterprise-grade solutions for our customers



Over 3,300 customers across SME, Enterprise and Public Sector organisations



Fully owned Network, Data Centres, Cloud, UCC Platform and Security services



Dun & Bradstreet rating 1
Privately owned and Financially stable



Turnover up 16% to £115m
EBITDA up 81% to £36.2m



Average 25% compound Annual Growth Rate

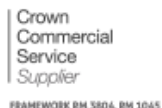
Our Accreditations

We support the security and compliance standards of the Public Sector by embedding our compliance certifications into our Business Management Systems. These include:

- ✓ **ISO27001** - Information Security
- ✓ **CSA Star** - Cloud Security
- ✓ **Cyber Essentials Plus**
- ✓ **PCI-DSS**
- ✓ **(HSCN)** Health Social & Care Network Stage 2 Compliance
- ✓ **CAS(T)** accreditation
- ✓ **ISO9001** - Quality Management
- ✓ **ISO20000-1** - Service Management
- ✓ **BS10012** – Personal Information (GDPR)
- ✓ **ISO22301** - Business Continuity
- ✓ **ISO50001** - Energy Management
- ✓ **ISO14001** - Environmental Management

Our certifications are fully audited every three years by BSI, NCC Group & NHS Digital, supplemented by six monthly continuing assessment audits to ensure continuing compliance. The following preventive are undertaken actions to ensure we maintain our certifications & accreditations;

- ✓ 12 month Audit Schedule
- ✓ Monthly Internal Audits in line with our audit schedule
- ✓ Six monthly external Audits
- ✓ Live Net Promoter Score on our Website
- ✓ All Engineers undertake BPSS vetting by a government approved vendor
- ✓ Corrective and Preventive Actions – CAPA
- ✓ Control of Documents and Records
- ✓ Companywide Risk Assessment
- ✓ Annual review of policies, procedures and documents
- ✓ Internal & External PEN (ITHC) Network Test by a 'Check' or "Crest" approved vendor
- ✓ Annual off site Business Continuity Test
- ✓ Management reviews (Management Meeting, Service Review, Quality Review, Business Continuity, Security Review and Operation Review)



Our Promise

Our brand promise is to 'Constantly exceed expectations with innovation and service'. In order to achieve this, we promise to deliver the following:

- ✓ **Customer Service Excellence:** Our first priority we never compromise on, this culture spans across every department and is championed by every board member
- ✓ **Trusted Supplier:** A reliable and fully owned carrier-class network, with pro-active support from our 24x7x365, fault find and fix Service Desk, and verified financial stability inspire customers' confidence in us
- ✓ **Technical Capability:** Working within eight international ISO and British Standards, we design, manage and support customers' complex, bespoke network, Cloud and Voice requirements
- ✓ **Applied Innovation:** Ensuring customers' businesses remain at the leading edge with a dynamic approach to investment, R&D and innovation, and consistently delivering industry firsts.

Our network has undergone a rigorous security assessment and has achieved PCI-DSS compliance to ensure top security standards. We design, deliver, manage and support communications solutions, both simple and complex, to international ISO management standards: 9001, 22301, 14001, 5001, 27001, 20000 and BS 10012.

By the start of FY2018, our turnover had reached approximately £115 million and ongoing recruitment activity meant that we had over 500 employees. Our success is driven by the quality of service we provide and is underpinned by investments in people and infrastructure that enable us to deliver on our brand promise.

Exponential-e's Approach

Our approach is based on a partnership philosophy, ensuring we deliver high quality, competitive services. In keeping with this, our technology solutions provide cost-effective connectivity, future-proof networking and uncompromising customer support. Our approach is designed so that there are no hidden extras from you. From the initial point of contact, including technical consultancy, project management and on-going customer support, we are entirely transparent about our work and the costs involved. To maximise the value for money customers receive, we constantly challenge the performance of the service through 24x7x365 monitoring and management via the Exponential-e Service Desk, feeding back at monthly service reviews that constantly benchmark your

expectations. During these reviews, we propose and implement continuous improvement targets for service levels and cost efficiency. On award of any contract, we analyse the service required and explore how we will improve the services year-on-year.

Thought Leadership and Applied Innovation

We have an entire team devoted to seeking out new products, features and enhancements. We pride ourselves on our ability to generate, identify, and deploy the latest technologies. Our commitment to innovation has seen us develop pioneering new products and services for our customers and deliver all manner of industry firsts.. We will constantly keep you informed of new technologies that ensure you remain current and knowledgeable as to innovative solutions and best practices. The most effective means of doing that is during our regular Service Management review meetings; the reviews will take place on a monthly or quarterly basis, or upon request. These sessions are used to understand your requirements, address any current service issues, and for our team to update you on new market trends or technologies our researchers have identified.

You will have the opportunity to attend regular events that provide an opportunity to speak with our subject matter specialists and to exchange ideas and experiences with other Exponential-e customers. We are firmly committed to listening and collaborating with our customers, and partners, in order to deliver innovative technical solutions that drive tangible business benefits.

We organise industry focused and private seminar events at exclusive venues, such as the Ritz and Emirates Stadium. We invite key speakers to present, as well as our in-house technical experts and evangelists, and look at topics including 'Demystifying SD-WAN' These events are excellent networking opportunities which present you with a chance to speak with like-minded individuals in an informal environment and gain real technical knowledge and insight from our team of experts.

Details of our events can be found on our website, <http://www.exponential-e.com/about/events>, where you can register.

You will also be sent updates from our marketing department, highlighting new features or services available in the market. New products, features or services that we feel are well suited to our customer's infrastructure, or will benefit their IT environment, will be brought to their attention. Initially, many of our customers adopt our WAN solution and are often keen to complement this service with our Cloud, IT and Voice services.

Meeting our Brand Promise

For over 17 years we have focused on building trusting relationships with our customers by placing service excellence at the heart of our operations. Key to our success is the development and sustainment of effective working partnerships through regular service review meetings, proactive management and - most importantly - continually seeking to improve the services which will be delivered.

In order to ensure that we are continuously improving, we benchmark customer satisfaction which provides us with the analysis to improve. Measuring our customer satisfaction is achieved through our Net Promoter Score and our Voice of the Customer Programme.



Rolling 3 month average. Industry average 17

<https://www.exponential-e.com/about/customer-service-promise>

Our current 3 monthly rolling NPS score is more than double the UK Industry average.

Our Voice of the Customer Programme gives you the opportunity to provide real-time feedback by simply clicking on one of four icons on each Exponential-e employee's email-signature (Gold- Excellent,

Green- Good, Amber- Could have been better, Red- Poor).

These awards are all testament to our solutions and achievements in innovation. Details of our other awards can be found on our website:

<https://www.exponential-e.com/about/our-accreditations-awards>

Meeting our brand promise through customer service excellence is embedded into our culture; anytime our customers recognise our people doing well, we reward this throughout the business. At Exponential-e, we're committed to service excellence and are empowering our people to deliver it.

Our Security Capabilities

Security assurance

Our services are designed, built and optimised with clear alignment to the 14 CESG Cloud Security Principles that UK Public Sector organisations use when assessing cloud hosted solutions for information assurance compliance.

The Exponential-e cloud benefits from extensive independent validation via certifications ranging from international standards e.g. ISO9001, ISO27001 and ISO20000 to UK public sector specific standards such as CAS(T) and HSCN Stage 2 certification.

The Exponential-e Cloud Platforms are subject to regular, extensive IT Security Health Check (ITSHC) CHECK Tests by independent, CESG-approved assessors to ensure that our customers have confidence in the physical and technical security controls which have been implemented to protect their valuable data assets. Platforms are suitable for all data classified at OFFICIAL under the Government Security Classification Policy (GSCP)

All customer data is stored in Exponential-e's two secure UK data centres with SC-cleared UK staff. Customer identifiable data does not leave the UK.

Connectivity

Our UK Data Centres have resilient connections to secure UK government networks such as HSCN Assured as well as large scale, DDoS protected internet connectivity. We also offer the ability for customers to present their own connections (such as direct connectivity into your MPLS, or inexpensive point to point connections via leased lines) and the Secure Remote Access solution to allow security assured VPN access to the Elevated OFFICIAL platform.