Crown Commercial Service

G Cloud 14

BT Cyber Security Strategy & Transformation Advisory Services

May 2024

Crown Commercial Service

BT

British Telecommunications Plc
1 Braham Street
London
E1 8EE
United Kingdom

www.bt.com

Copyright

Contents

1. Services Overview 1
BT Cyber Security Advisory Services 1
1.1. Security Strategy & Transformation Advisory 1
2. Why work with the Supplier? 4
2.1. The Supplier's connections are the Buyer's connections 4
2.2. The Supplier's Global Experience 4
2.3. A Trusted Partner and Risk-based Approach 4
2.4. The Supplier's Technical Expertise 4
2.5. The Supplier is Recommended 4
3. Pricing 6
4. Ordering and Invoicing Process 7
5. Data 8
5.1. Sub-processing 8
6. Other Service Considerations 9
6.1. Security 9
6.2. Business Continuity/Disaster recovery 9
6.3. Exit Management 9
6.4. Cyber Essentials 9
6.5. Personnel Security 9
6.6. Recruitment Screening – Non-Supplier People 10
6.7. Suppliers 10
6.8. Security Education and Training 10
6.9. Government Security Vetting 11
6.10. Anti-Virus Definitions 11

1. Services Overview

BT Cyber Security Advisory Services

Today's cyber security landscape is complex. The Supplier offers strategic security guidance and solutions to organisations across the globe, to help navigate this complexity.

The Supplier helps the Buyer secure their business from network to cloud, keep up with the changing threat landscape, protect critical data and ensure compliance, and optimise your security estate and future roadmap.

At every stage of the Buyer's security journey, the Supplier helps the Buyer to assess and test their defences and select the solutions that match their security needs - whether that requires building an entirely new security strategy or upgrading their protections to combat the latest threats and trends.

As trusted advisors, the Supplier can help the Buyer:

- Define a **security strategy and transformation roadmap** to help the Buyer on their journey to:
    - Securing their SD WAN
    - Securing their hybrid cloud
    - Take a zero-trust approach to security
    - Protecting their end users and securing their data
    - Accelerating their threat detection and response

Across all the Supplier's engagements they will work with the Buyer to clearly identify, evaluate, assess their security position, issues, vulnerabilities, and challenges, and will provide clear recommendations and improvement plans to deliver desired outcomes.

Why work with the Supplier?

- Strategic partner - the Supplier work with the Buyer long-term, supporting them on their digital transformation journey.
- Vast experience – the Supplier's consultants have vast experience navigating the wide range of challenges involved when their clients are undergoing digital transformation.
- Shared expertise - the Supplier uses the same processes and frameworks to protect itself and the Supplier's customers which means the Buyer gets the best of what the Supplier has.
- Integrated approach - the Supplier's built-in network security and expert management services mean that any security gaps are plugged.
- Risk based approach - the Supplier's recommendations will be tailored to the Buyer's individual risk appetite and budget.

1.1. Security Strategy & Transformation Advisory

Cyber Security is a journey, every organisation starts from a different point with a different set of existing security solutions. Point solutions from different vendors often don't work together, creating blind spots in the Buyer's view of security. Cloud migration and remote working have punctured the perimeter making it harder to get complete visibility of the Buyer's estate. A lack of situational awareness of the cyber threat landscape means

attacks go unnoticed, or reactions are inappropriate. Staying on top of vulnerabilities, managing user access, and educating employees is a complex process. Compliance requirements and regulations continue to increase, with heavier workloads to stay compliant. Finding, recruiting, and retaining skilled resources is costly and time-consuming.

We recognise the complexity of these challenges that organisations are facing. The Buyer's experienced security advisors can partner with the Buyer to help the Buyer evaluate their current position, define their next steps, navigate through the uncertainty and abundance of choice, and create a transformation roadmap to help them achieve the business outcomes they're aiming for.

The Supplier will give the Buyer the expert advice they need to define, manage, and guide their information security, compliance, governance, and regulatory programmes. The Supplier can leverage its extensive expertise to help guide the Buyer for example to:

- Secure the Buyer's SD WAN
    - Increase the Buyer's network flexibility with SD-WAN but protect them from increased risks
- Take a Zero Trust approach to security
    - Step up and create a flexible and dynamic security policy to control the Buyer's borderless estate
- Protect the Buyer's end users and secure their data
    - Let the Buyer's employees work from anywhere and on any device but protect them from identity misuse, endpoint threats and data loss
- Secure the Buyer's hybrid cloud
    - Avoid data loss and remain compliant as the Buyer migrates services to the cloud
- Accelerate threat detection and response
    - Continuously monitor the Buyer's estate to spot security breaches and quickly respond to any alerts

The Supplier's advisors have a wealth of security experience and expertise, combined with best practices learned from working with nation states and multinationals around the world. The Supplier can help the Buyer balance their need for security with their strategic business vision. This means the Buyer can optimise the overall value of their existing investment, regardless of where their organisation is in their security maturity journey.

The benefits of the Supplier's Security Strategy and Transformation Advisory Services include:

- **Capability** – With a global client base of hundreds of clients across all sectors, the Supplier has experience of the challenges that the Buyer is facing and can leverage previous learning as well as insight and research on what may be important next.
- **Flexibility** – the Supplier's advisors are available remote or onsite for stand-alone projects or regular activity. Pay only for what the Buyer needs.
- **Agility** – the Supplier's advisors are proven experts in their field. They don't need training and they can get started straightaway.
- **Low risk** – the Supplier's advisors can help the Buyer meet their security needs whilst allowing them the time to build their security programme; digitally transform; or protect their assets whist building their own capability.
- **Integrity** – the Supplier's advisors will work with the Buyer's team to create a solid

framework they can build on for now with the future in mind.

- **Return on Investment** – meet the Buyer's security needs without a large, committed investment in a function that the Buyer may have under development or be looking to evolve and expand.

2. Why work with the Supplier?

2.1. The Supplier's connections are the Buyer's connections

Because of the Supplier's position in the industry, the Supplier has a ringside seat on security. The Supplier is connected to some of the biggest names in cyber security – giving the Buyer access to industry leading insights and analysis. The Supplier's combined knowledge will help identify threats based on adversary, industry, and vertical analysis – and their relevance to the Buyer.

2.2. The Supplier's Global Experience

The Supplier has 70 years of experience managing the threat environment. With the Supplier as a partner, the Buyer gets the expertise and professionalism of a protector of nation-states, with the experience and know-how of a multinational securing many different business units.

The Supplier uses the same processes and frameworks to protect itself and its customers which means the Buyer gets the best of what the Supplier has.

2.3. A Trusted Partner and Risk-based Approach

The Supplier is a trusted advisor, working with the Buyer long-term as a strategic partner, supporting the Buyer on their digital transformation journey as it evolves. The Supplier's recommendations will be tailored to the Buyer's individual risk appetite and budget.

An effective end-to-end data security strategy requires a joint effort from many different business areas including operations, legal and compliance, security, and IT departments. The Supplier's security consultants provide the link between different departments and help the Buyer to secure stakeholder contribution.

Beyond organisational security measures, the Supplier's expertise covers the most detailed architectural knowledge about security technologies available on the market.

2.4. The Supplier's Technical Expertise

The Supplier's Security Advisory team are experts across the cyber security landscape, holding over 500 certifications including CISSP, CISA, CISM, CGEIT, QSA, CCEP, CCEP-I, CIPP, CIPT and ITIL. Plus, the Supplier has been accredited by Lloyd's Register Quality Assurance for the ISO9001:2008 quality management system since 2003. So the Supplier's consulting services have been around for a while, improving year on year to bring its customers the best quality of service possible.

2.5. The Supplier is Recommended

The Supplier has been named a Leader in both IDC Marketscape: Worldwide Managed Security Services 2020 Vendor Assessment, and IDC MarketScape: European Managed Security Services (MSS) 2022 Vendor Assessment report.

The Supplier has also been recognised as 'Very Strong' overall in the 2021 GlobalData (formerly Current Analysis) Managed Security Product Assessment Report (Global), when assessed against Portfolio, Service, Security Assessment, Authentication and Encryption, Threat Management and Monitoring and Cloud Security. The analyst quotes "BT's capabilities in the UK and Europe place it among the leading MSSPs in the region."

3. Pricing

All BT Cyber Security Advisory Services are delivered on a Time and Materials basis according to the day rates detailed in the SFIA. In addition, where licencing costs are required, (e.g. software, servers, analytical tools) these will be based on the applicable fee for the volume and timeframe that the licences are required.

Where an assessment is focussed on virtual machines the appropriate licence fees will apply. There may be instances where the Buyer requires an application to be hosted/managed. In such situations the appropriate hosting and management costs will be applied subject to the Buyer's specific needs/requirements.

All prices will be exclusive of V.A.T. and expenses.

4. Ordering and Invoicing Process

These are specialist security support and advisory services charged for on a Time and Materials basis: orders should be placed following agreement on the requirements and scope of the engagement. The services can be ordered through The Supplier's standard sales channels. The Supplier's salesperson will work closely with the Buyer to capture requirements in a statement of work and will then provide a firm price and indicative service commencement date for the service requested. Once the G Cloud order form is completed and signed by the Buyer, the Supplier will initiate the engagement. The billing schedule is agreed with the Buyer in the statement of work.

5. Data

This Service requires the Processing and Sub-processing of Buyer Data and Buyer Personal Data outside of the EEA.

Please note that given the standard nature of the Service, the Supplier, and its suppliers, including any Sub-processors of the Supplier and its suppliers, may from time to time use back-office support and system functions which are located or can be accessed by users from outside of the European Economic Area. The Buyer consents to the disclosure and transfer of Buyer Personal Data as required in order to provide the Service and the Parties will give effect to that consent as necessary in accordance with paragraph 5(d) of the Framework Agreement Schedule 7.

The Buyer shall ensure that it discloses to the Supplier only the Buyer Personal Data that the Supplier requires in order to perform the Service.

Where for the provision of the Service, the Supplier is required to Process Buyer Personal Data on behalf of the Buyer, the Supplier will Process that Buyer Personal Data to the extent necessary for the performance of the Call-Off Contract.

In accordance with paragraph 2 of the Framework Agreement Schedule 7, this schedule 7 of the Call-Off Contract lists the processing of Buyer Contact Data that the Supplier is entitled to do.

5.1. Sub-processing

The Buyer consents to the Supplier's use of Sub-processors in accordance with paragraph 12(b) of the Framework Agreement Schedule 7. The Supplier will ensure that data protection obligations in respect of Processing Buyer Personal Data that are broadly comparable to those set out in paragraphs 1 to 15 inclusive of the Framework Agreement Schedule 7 will be agreed with any Sub-processors.

The Supplier will inform the Buyer of intended changes to its Sub-processors from time to time, either by providing the Buyer with online access to intended changes or by such other means as the Supplier may determine. If the Buyer does not object to the proposed change within 30 days of this notice, the Buyer will be deemed to have authorised the use of the new Sub-processors.

The Buyer may object to the use of a new Sub-processor by formally notifying the Supplier, documenting its material and substantiated concerns that the new Sub-processor will not be able to comply with the Data Protection Legislation. The Parties will discuss and agree how to address the Buyer's objection and the Supplier may use the relevant Sub-processor to provide the Service until such objection is resolved, or if not resolved then the matter will be referred to the Dispute Resolution Procedure.

6. Other Service Considerations

The service described in this Service description is based on the Supplier's standard offering for a commodity cloud service. It should be noted G Cloud 14 mandates that specific consideration be given to Security Plans, Business Continuity, Exit Management, Cyber Essentials, Personnel Security and Anti-Virus definitions. This section clarifies the scope of such support in the context of this commodity service.

6.1. Security

The production of an ISMS and security plan is dependent on the specific policies of the Customer procuring such service, and as such it is highly variable and cannot be included as a standard item within the commodity Cloud offering. In the event that a Buyer does wish Supplier to develop such security documentation then Supplier, working with the Buyer, will determine the number of additional professional service days required to produce the required artefacts. Such requirements shall be identified in writing at least 20 working days prior to contract agreement, and this requirement is in addition to the obligations detailed in the Framework Agreement. The security (ISMS/plan) requirements, and any associated costs, shall be included within the call off contract prior to signature. No work can be undertaken on these security documents without agreement within the call off contract.

6.2. Business Continuity/Disaster recovery

Due to the commodity nature of the service, the only data storage, business continuity and disaster recovery services provided are those included in the above service description and associated terms. For the avoidance of doubt, no other business continuity plans, or recovery services are provided within the Supplier's standard offer of service.

6.3. Exit Management

The support provided to users when services come to the end of their contract period, or are terminated in advance, will be in accordance with the Supplier standard terms and conditions associated with this catalogue offering, to the extent such services are included. Due to the commodity nature of the service, no additional exit management services (exit plans/additional exit plans) can be provided at this time.

6.4. Cyber Essentials

The Supplier (BT) holds a Cyber Essential Plus certificate for its Enterprise Sales and Bid environments enabling it to bid for and administer this framework.

6.5. Personnel Security

Our recruitment process includes pre-employment screening and vetting prior to placement to ensure adequate levels of confidentiality are maintained, screening includes:

- Application for a criminal record check

- Giving us contact details for reference checks
- Health declaration
- CIFAS- Staff Fraud Database check.

Additional checks are made when dealing with particularly sensitive positions (such as people handling cash or valuable items, or those involved with sensitive contracts). The normal undertakings signed by individuals at recruitment include non-disclosure provisions and it is a disciplinary offence to misuse any information obtained from Supplier systems. Offenders are subject to disciplinary action up to and including dismissal and may be subject to prosecution, while ensuring compliance with local legislation.

6.6. Recruitment Screening – Non-Supplier People

The Supplier only uses agency or contract personnel from approved agencies with the Supplier has established a contract that requires them to meet our standards for recruitment, vetting and verification. Furthermore, managers must assess the risks of taking on any agency person before they begin working for the Supplier, and, if they proceed, ensure that a copy of a signed non-disclosure agreement is obtained before they are allowed access to any Supplier systems or information.

6.7. Suppliers

The Supplier is committed to ensuring that all third-party people supplied to undertake work for the Supplier or who require access to Supplier's property and/or systems to deliver contracted goods or services have appropriate pre-employment checks in advance of any interaction with the Supplier. There are different levels of checks depending on the type of work, the level of contact with Supplier employees, customers and information, and the requirement for systems and physical access to Supplier property.

6.8. Security Education and Training

As part of the induction training for all staff, Supplier or non-Supplier, managers are required to ensure that their people receive adequate security training and instruction before using the Supplier systems. Areas of training include:

- Security policy and data protection – with particular emphasis on information security, access rights, misuse of information and privacy-markings and their use
- Non-disclosure agreement and the individual's responsibility to comply
- Disciplinary and legal consequences associated with unauthorised use and abuse of resources and position of trust
- Local security measures, emergency procedures, backup processes, contingency plans, and incident reporting.

The Supplier runs an extensive security awareness and culture-change programme. The security culture of the company is measured by conducting online surveys and the results are assessed to determine how to prioritise appropriate action. Supplier then designs action plans to address these key areas. This material is then delivered through information programmes that include webinars, roadshows, regular reminder briefings, websites, articles in internal magazines, computer-based training packages, videos, focus groups and feedback channels.

6.9. Government Security Vetting

Additionally the Supplier requests Government Security Vetting when this is required under sponsorship from the relevant [HMG] customer. Supplier will ensure that individual roles meet the specified criteria as set out within the contractual obligations.

6.10. Anti-Virus Definitions

The Supplier uses/applies anti-virus definitions provided by industry accepted sellers to minimize the impact of Malicious Software. The Supplier cannot warrant that we apply the most up to date anti-virus definitions at any single point in time however, we have robust processes in place to update all anti-virus definitions on the Supplier estate in a timely manner.