



G Cloud 15

BT Service Definition for BT Ethical Hacking

Contents

Page

1	Services Overview	3
2	Why Work With Us?	5
3	Pricing	7
4	Ordering and Invoicing Process	8
5	Security Requirements	9
6	Personal Data	11
7	Other Service Considerations	12



1 Services Overview

1.1 BT Cyber Security Advisory Services (Ethical Hacking)

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:

- Evaluate the weak spots the Supplier has in their policies, procedures, and estate through the Supplier's Offensive Security services.

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.

1.2 Offensive Security (Penetration Testing)

As the global threat landscape constantly evolves, the Buyer's risk exposure needs to be continually reviewed, considering the requirements of their evolving organisation. The Supplier's ethical hackers can identify weak spots, and work with the Buyer to fix them. The Supplier will pinpoint the vulnerabilities in the Buyer's people behaviours, procedures, policies, applications, and networks before the cyber criminals do.

The Supplier has more than 60 highly skilled consultants all over the globe which will help the Buyer ensure proactive protection of their brand, reputation, and valuable electronic assets – and gain a clear view of their overall risk profile. Over the past 25 years, the Supplier has worked with a huge range of organisations ranging from financial institutions to the public sector, evaluating systems like internet banking infrastructures and electronic payment transactions environments.

The Supplier's global coverage and international customer base across several industries gives the Supplier a unique view on the security of systems, web and mobile applications, mobile devices, and both wired and wireless network infrastructures.

Using the Supplier's structured testing methodologies, their consultants will identify vulnerabilities in the Buyer's web and thick client applications, mobile devices, systems, network infrastructure, Active Directories, and behaviour of the Buyer's people that are supporting their business strategy. The Supplier will work with the Buyer to review their current risks against their desired risk profile, and then provide a reliable, flexible road map that will help the Buyer manage their vulnerabilities. Through extensive research and experience, the Supplier's consultants continually develop new intrusion testing techniques and add to their proprietary library of manual tests and custom developed tools.

As a network operator, the Supplier has specific and in-depth knowledge of network infrastructure devices. The Supplier's own systems and services are thoroughly tested by their own ethical hackers before being deployed on their network infrastructure, on which many international customers rely.

Both the Supplier's professional and security services are backed by accreditations for both ISO 9001 and ISO 27001 quality management systems. The Supplier has been globally accredited by Lloyd's Register Quality Assurance Ltd. since 2000 (ISO 27001) and 2003 (ISO 9001), showing their long-term commitment to continuously improving the quality of their services.

The Supplier's consultants are highly skilled and have passed several industry-related certifications such as CISSP, CISA, OSCP, OSCE, GWAPT or GPEN.

2 Why Work With Us?

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 Security Requirements

Due to the nature of the service within scope of this service offer, optional Call-Off Schedules 9A (Security: Short Form), 9B (Security: Consultancy), 9C (Security: Development), 9D (Security: Supplier-led Assurance) and 9E (Security: Buyer-led Assurance) are excluded and the **Suppliers standard Security Management Plan applies only**.

Additionally, BUYER'S SECURITY REQUIREMENTS AND ICT POLICY SECURITY REQUIREMENTS within the Call-Off Order Form will be marked with the option **There are no Security Requirements for the purposes of this Call-Off Contract** and SECURITY ASPECTS LETTER will be marked as **not applicable**.

5.1 The Security Management Plan

The Security Management Plan (SMP) defines the security measures that are implemented, and maintained, by BT. BT will maintain the adherence to the contracted security measures.

The plan supports the provision of the services in scope of this service offer and covers the following:

- Our approach to security
- Our information security policy
- External parties
- Human resource security
- Physical and environment security
- Asset management
- Operation of the plan
- The security lifecycle

5.2 Security Accreditation and Governance Standards

Security accreditation and governance standards will be in line with the details defined within the Suppliers Digital Marketplace submission and where applicable, additional information will be detailed within this Service Definition document.

5.3 Operational Security

Operational security will be in line with the details defined within the Suppliers Digital Marketplace submission and where applicable, additional information will be detailed within this Service Definition document.

5.4 Asset Protection

Operational security will be in line with the details defined within the Suppliers Digital Marketplace submission and where applicable, additional information will be detailed within this Service Definition document.

5.5 Cyber Essentials Certification

Cyber essentials certification was a mandatory requirement to secure a place on the framework as a Supplier and to maintain our place on the agreement, all Suppliers must present evidence to Crown Commercial Service (CCS) of their continued certification.

Therefor the option under CYBER ESSENTIALS CERTIFICATION within the Call-Off Order Form under is marked as not applicable and for the purposes of Call-Off Schedule 27 (Cyber Essentials Scheme), clauses 2.1 to 2.4 are not used.

5.6 Staff Vetting Requirements and Background Checks

Staff vetting requirements will be in line with the details defined within the Suppliers Digital Marketplace submission and this Service Definition document and STAFF VETTING REQUIREMENTS within the Call-Off Order Form will be marked accordingly.

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 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.

Due to the nature of the service within scope of this service offer, optional Call-Off Schedule 18 (Background Checks) is excluded and in the event that Supplier Staff do not have the necessary clearance required, the Parties will agree an acceptable alternative such as escorted access.

6 Personal Data

Personal data in relation to services in scope of this service offer is divided into 2 areas:

- Managing the contract
- Managing the services

Personal data, where required to be managed, complies with the requirements of clause 17 Data protection and security, within the Framework Core Terms including new Clause 17.7 included via Framework Special Term 13

6.1 Managing the Contract

Joint Schedule 10 (Processing Data) will be completed to define what types of personal data in relation to managing the contract may be held, the nature and purposes of the processing and will confirm The Parties are Independent Controllers of Personal Data.

6.2 Managing the Service

Where personal data is held as part of delivering the service, how this will be managed will be defined, where applicable, within the Suppliers product specific Terms and Conditions that are attached to the Suppliers Digital Marketplace entry for this service offer. The Suppliers Digital Marketplace entry also confirms details of data storage and processing locations specific to this service.

The Supplier, including any Sub-processors of the Supplier, 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 UK and/or the European Economic Area. Any such processing will be in accordance with Joint Schedule 10 Paragraph 5.5.2, and for the purpose of clause 5.5.2 (a), the Buyer consents to the disclosure and transfer of Data, including Personal Data, as required in order to provide the Service.

6.3 Sub-processing

The Buyer consents to the Supplier's use of Sub-processors in accordance with the Framework Agreement. The Supplier will ensure that data protection obligations in respect of Processing Buyer Personal Data that are broadly comparable to those set out in the Framework Agreement and 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.

7 Other Service Considerations

The service described in this Service Definition is based on the Supplier's standard offering for this cloud service and the contract is not defined as a Critical Service Contract. It should be noted that the G Cloud 15 Call-Off Order Form has a number of mandatory schedules, optional schedules and Call-Off Order Form options, and this section clarifies the position of these options for this service as provided by the Supplier. The service will additionally be delivered in line with the Supplier Terms and Conditions included within the Suppliers Digital Marketplace submission.

7.1 Modern Slavery, Environmental Requirements and Sustainability

To comply with the reporting requirements to the Buyer as defined within Joint Schedule 5 (Sustainability) the Buyers can access the Suppliers annual Modern Slavery Report, and where required (for lots 1a and 1b only) its Carbon Reduction Plan here [Our reports & policies - Responsible business | BT Plc](#)

Optional Call-Off Schedule 25 (Additional Sustainability Requirements) is excluded. The Suppliers approach to sustainability, managing our environment, and our modern slavery policies can be found here [Our reports & policies - Responsible business | BT Plc](#)

Optional Call-Off Schedule 26 (Carbon Reduction) is excluded. The Suppliers approach to carbon reduction and our carbon reduction plans can be found here [Our reports & policies - Responsible business | BT Plc](#)

7.2 Financial Difficulties

For the purpose of Joint Schedule 7 (Financial Difficulties), the Ratings Agencies listed within Annex 1 (Rating Agencies and their standard Rating System) will be Standard & Poor and Moody's and for Annex 2 (Credit Rating Thresholds) these will be BB+ for Standard and Poor and Ba1 for Moody's.

BT's published ratings are available [here](#)

7.3 Guarantee

For the purpose of Joint Schedule 8 (Guarantee), the Buyer does not require a Guarantee from the Supplier to award the contract.

7.4 IPR

For the purpose of Call-Off Schedule 1 (Intellectual Property Rights) **Part A Option A3: Supplier ownership of all New IPR with Buyer rights for the current contract only;** applies and is not further amended on the Call-Off Order Form under INTELLECTUAL PROPERTY RIGHTS.

7.5 Staff Transfer

No staff transfer is required and for the purposes of Call-Off Schedule 2 (Staff Transfer) **Part C: No Staff Transfer on the Start Date** only applies.

7.6 ICT Services

ICT services, where applicable, will be managed in line with the details defined within the Suppliers Digital Marketplace submission and supporting Supplier Terms, and where applicable within this Service Definition document and optional Call-Off Schedule 6 (ICT Services) is excluded, and the option under ICT POLICY within the order form will be marked as not applicable. Any maintenance of the ICT environment, where applicable, will be defined within this Service Definition document and the option under MAINTENANCE OF THE ICT ENVIRONMENT within the Call-Off Order Form will be marked as not applicable.

7.7 Business Continuity and Disaster Recovery

Due to the nature of the services within scope of this service offer, optional Call-Off Schedule 8 (Business Continuity and Disaster Recovery) is excluded.

7.8 Corporate Resolution Planning

Due to the nature of the services within scope of this service offer, , which is available only when the Call-Off Contract is not a Critical Service Contract, optional Call-Off Schedule 24 (Corporate Resolution Planning) is excluded.

7.9 Exit Management

Optional Call-Off Schedule 10 (Exit Management) is excluded and at the end of the Call Off Contract Period, the offboarding process will be managed in line with the details defined within the Suppliers Digital Marketplace submission and where applicable within this Service Definition document. The Call-Off Order Form SPECIFIC EXIT MANAGEMENT ASSISTANCE (LOT 1A AND LOT 1B ONLY) and VIRTUAL LIBRARY will both also marked as not applicable.

7.10 Clustering and Leasing

Services will be contracted and invoiced to the Buyers detailed within Framework Schedule 6 (Order Form Template) and as such optional Call-Off Schedule 12 (Clustering) is excluded.

Due to the nature of the services within scope of this service offer, leasing of services is not applicable and as such, optional Call-Off Schedule 22 (Lease Terms) is also excluded.

7.11 Implementation Plan and Testing

Due to the nature of the services within scope of this service offer, optional Call-Off Schedule 13 (Implementation Plan and Testing) is excluded and the services in scope will be implemented and tested in line with the details defined within the Suppliers Digital Marketplace submission and this Service Definition document.

7.12 Performance Levels

Due to the nature of the service within scope of this service offer, optional Call-Off Schedule 14 (Performance Levels) is excluded and the service levels provided are as defined within the Suppliers Digital Marketplace submission and this Service Definition document.

7.13 Service Credits

Any service credits for the services within scope of this service offer will be as detailed, where applicable, within this Service Definition document and SERVICE CREDITS within the Call-Off Order Form will be marked accordingly.

7.14 Call Off Schedule 17 (MOD Terms)

Where optional Call-Off Schedule 17 (MOD Terms) is required, this will be based on no additional DEFCONS or DEFFORMS being added within Annex 1 which incurs additional costs to the Supplier.

7.15 Call Off Specification and Deliverables

The services will be delivered in line with the Suppliers Digital Marketplace submission and this Service Definition document and as such, optional Call-Off Schedule 20 (Call-Off Specification) is excluded.

7.16 Call Off Special Terms

Due to the nature of the services within scope of this service offer based on the Supplier's standard offering for this cloud service, no additional call off special terms are introduced into the Call-Off Order Form under CALL OFF SPECIAL TERMS

7.17 Service Request Process

The service request process will be as defined within the Suppliers Digital Marketplace submission and this Service Definition document and SERVICE REQUEST PROCESS within the Call-Off Order Form will be marked accordingly.

7.18 Minimum Commitments

Any MINIMUM COMMITMENT(S) where applicable noted within Call-Off Order Form will be aligned to those as defined within the Suppliers Digital Marketplace submission and Suppliers Price Card where applicable and MINIMUM COMMITMENT(S) within the Call-Off Order Form will be marked accordingly.

7.19 Maximum Liability

The limitation of liability for this Call-Off Contract remains as stated in Clause 14.2 of the General Terms (as that Clause 14.2 has been amended pursuant to Framework Special Term 12 as set out in the Framework Award Form) and is not further amended on the Call-Off Order Form under MAXIMUM LIABILITY.

7.20 Additional Insurances

There is no requirement for additional insurances which will remain as defined within Joint Schedule 3 (Insurance Requirements) and ADDITIONAL INSURANCES on the Call-Off Order Form will be marked as not applicable.

7.21 Product Roadmaps

Any defined product roadmaps, where applicable, will be defined within this Service Definition document and PRODUCT ROADMAP (IF APPLICABLE) within the Call-Off Order Form will be marked as not used.

7.22 Quality Plans

Any defined quality maps, where applicable, will be defined within this Service Definition document and the option under QUALITY PLANS within the Call-Off Order Form will be marked as not applicable.

7.23 Social Value Commitment

Social value is at the heart of our purpose, driving impactful initiatives that address the needs of diverse communities across the UK. Our dedicated Social Value team have a focus on sustainability, community, sponsorship, charity, and the environment.

We're increasing digital inclusion and giving back to local communities through on-the-ground initiatives that make real-world positive changes.

The five pillars of social value at BT are:

- Outreach: no one is forgotten in our social value delivery.
- Improvement: continuous improvement in our delivery.
- Sustainability: our incentives are built to last.
- Engagement: user voice at the forefront and not an afterthought.
- Equity: leveraging our power to mobilise individuals, institutions, and communities

Details and reporting on what we are doing around social value can be found here [Social Value At BT | About Us](#) and SOCIAL VALUE COMMITMENT within the Call-Off Order Form will be marked accordingly and no additional bespoke commitments or reporting will be included.



Copyright

© British Telecommunications plc 2026

Registered office: One Braham, Braham Street, London, E1 8EE

Registered in England no. 1800000

BT is an ISO 9001 Registered Company

Company information

Parent Company: BT Group plc

Company Legal Entity Name: British Telecommunications plc

Company Trading Name: BT

Address: One Braham, Braham Street, London, E1 8EE

Web Address: <https://business.bt.com/>