G Cloud 15
BT Service Definition for BT Cyber Security Advisory Services

Contents

1 Services Overview

1.1 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 the Buyer's 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:

- **Assess their security governance, risk, and compliance posture**
    - The Supplier can help benchmark the Buyer's security strategy and defences against established frameworks to evaluate what the Buyer has in place and identify any weak spots through a **Security Health Check.**
    - Review the Buyer's level of compliance against the requirements of **ISO27001** and other frameworks as directed and assist in the development of any supporting processes or policies to meet the standard.
    - Assess the current status and security maturity of the Buyer's OT environment.
- **Understand the most prevalent threats to their organisation**
    - Gain insight to the tactics, techniques and procedures that cyber criminals are using in the Buyer's industry sector using the Supplier's **Threat Modelling and Prioritisation Advisory Service.**
    - Gain insight into the most valuable mitigations and CIS Controls to help mitigate the identified threats.
- Define a **security strategy and transformation roadmap** to help the Buyer on their journey to:
    - Securing their SD WAN
    - Take a zero-trust approach to security
    - Protecting their end users and securing their data
    - Accelerating their threat detection and response

- **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 works with the Buyer long-term, supporting them on their digital transformation journey.
- Wide range of experience – the Supplier's consultants have extensive 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.

1.2 Security Governance, Risk and Compliance

1.2.1 Security Health Check and Cyber Assessment

With the Buyer's security constantly evolving to meet new threats, it can be easy to lose track of what's in place, or where any weak spots are. The Buyer's business could be open to serious risk and they might not even know it. Even when the Buyer is aware of the risks, they may not have the right solution. While the Buyer can never remove risk completely, they can manage it, get the measure of it and spot what's coming next.

Through the Supplier's Security Health Check, the Supplier will conduct analysis to identify the level of security relevant to the Buyer's organisation and assess the effectiveness of their security measures. The Supplier will draw on established frameworks e.g. CIS (Centre for Internet Security) Top 18 Critical Security Controls or NCSC (National Cyber Security Centre) CAF (Cyber Assessment Framework) as reference standards and complete a gap analysis.

The Supplier will identify the most vital information coming in and out of the Buyer's business to understand what the risks and threats are to that data. The Supplier will give the Buyer a clear prioritised plan of what the Buyer can do to improve the effectiveness of their existing controls, plus the Supplier will identify where the Buyer needs further controls.

With the Supplier's Security Health Check, the Supplier gets into the detail of the Buyer's cyber security. And this includes using industry-leading knowledge including:

- Reports based on the chosen security control framework or standard, such as Centre for Internet Security Critical Security Controls, National Cyber Security Centre Cyber Assessment Framework, National Institute for Standards and Technology Cyber Security Framework, and others.
- A tailored report from the Supplier with a prioritised list of recommendations and an overall maturity level assessment of the Buyer's business. The Supplier can then create a plan to address any gaps with a high-level roadmap.
- The Buyer's security report is written so it's easy to present to the board as to why changes and improvements need to be made. Plus, it identifies good practice that's already in place.

1.2.2 OT Cybersecurity Maturity Assessment

As organisations digitally transform, they expose their OT environment to IT, cloud, and suppliers. This enlarged attack surface, and the ever-increasing threat landscape pose a severe risk to the business. A holistic security strategy is key and converging Information Technology (IT) and Operational Technology (OT) essential to create synergies and avoid costly double structures.

A major challenge CISOs facing today is that OT is an area over which they have little to no visibility and control. This is aggravated by the fact that leveraging IT tools and concepts will fail in OT environments due to peculiarities such as legacy equipment or real-time network requirements.

The essential first step to overcome these challenges is to gather information about the existing OT estate. The Supplier's OT Cybersecurity Maturity Assessment creates visibility by systematically checking the current OT security maturity. This enables a prioritised action plan to strengthen the organisation's security posture and prepares for compliance with cybersecurity regulations such as NIS2.

The Cybersecurity Maturity Assessment is a high-level assessment designed to quickly get visibility into the current status and security maturity of the Buyer's OT environment. The CMA is an interview-based pen and paper assessment that can be conducted both remotely and on-site. It is based on the Cybersecurity Capability Maturity Model (C2M2) and covers the following ten security domains of which two focus on corporate-level capabilities (*) while all other domains are site-specific:

- Asset, Change, and Config Management
- Incident Response and Continuity of Operations
- Threat and Vulnerability Management
- Cybersecurity Architecture
- Workforce Management
- Third-Party Risk Management

- Identity and Access Management
- Risk Management (*)
- Situational Awareness
- Cybersecurity Program Management (*)

Three progressive maturity levels exist and are reported separately per domain. This helps to quickly identify any gaps and weak spots that should be prioritised in the security roadmap.

It starts with a preparation meeting to identify the key stakeholders within the Buyer's organisation that can answer the domain-specific questions. The CMA will then typically take between 3-5 days depending on the availability of the stakeholders. The Supplier will then prepare the report and recommendations that can be used to discuss next steps to increase your cybersecurity maturity.

What you will get:

- Preparation / Kick-off meeting (2-3 weeks in advance)
- Remote or on-site CMA (3-5 days)
- Report delivery & final presentation (2-3 weeks after the CMA)

Outputs include:

- CMA Report - summary report with bespoke recommendations
- OT Cyber Security Roadmap including prioritisation and potential quick wins

With this documentation you are able to strengthen your organisation's security posture and be prepared for compliance with cybersecurity regulations in an efficient manner.

1.2.3 ISO27001 / ISMS Review

ISO27001 is a technology neutral specification for an Information Security Management System (ISMS). An ISMS is a framework of policies and procedures, including legal, physical, and technical controls for an organisation's information risk management processes. It provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an effective ISMS.

The Supplier offers a full range of specialist support and advisory services, to support the ISO27001 certification lifecycle; understanding the scope of the service, analysing security controls, and assessing compliance, through to fully documented improvement plans. Please note – the Supplier cannot provide ISO27001 certification.

If the Buyer requires a security audit, the Supplier will scope, schedule, and independently audit the service against an agreed reference standard and will work with the Buyer to identify corrective actions and improvements. The Supplier uses experienced ISO27001 Security Auditors supported by security specialists.

1.2.4 Threat Modelling & Prioritisation Advisory Service

The Supplier can help design and tailor the Buyer's cyber defence capabilities for the threats that affect the Buyer.

Building upon MITRE ATT&CK®, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations, The supplier's Threat Modelling and Priority Reporting service gives the Buyer the insight to understand the most prevalent threats to the Buyer's organisation.

Then the Supplier's Threat Modelling and Prioritisation Framework comes into play. The Supplier will use it to create a custom threat model that highlights and describes the tactics, techniques, and procedures that cyber criminals are using in the Buyer's industry sector.

The Buyer will also be able to:

- Recognise the threat surface of the Buyer's organisation, align their security controls, and identify where gaps exist.
- Gain insight into the most valuable mitigations and CIS Controls to help mitigate the identified threats.
- Take immediate and effective action against threats as the Buyer discovers them.
- Focus investment on the Buyer's key threats to deliver maximum value.
- Start to change from reactive to proactive defence.

The Supplier's Threat Prioritisation Advisory Service is delivered as a report, which includes:

- A threat model, featuring top techniques contextualised with intelligence reporting.
- The Supplier's expert analysis, and the relevance of specific threats to the Buyer's business.
- MITRE ATTACK Navigator Layer File(s), which allows the Buyer to continue developing the model.

1.3 Security Strategy and 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
- vCISO support
    - Gain access to an experienced security specialist resource as and when you need it

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 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.
- **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.

1.4 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 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

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 needs 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 multiple certifications including CISSP, CISM, CRISC, CCSP, GICSP, and ITIL. 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.

2.5 The Supplier is Recommended

The Supplier is recognised as a Leader in ISG Provider Lens™ – Cyber Security – Solutions and Services 2024 in the UK. The report highlighted the Supplier's strengths in managed security services, strategic security services, and technical security services in the UK.

The Supplier has been named a Leader for the 20th consecutive year* in the 2024 in the Gartner Magic Quadrant™ for Global WAN Services based on its "Ability to Execute and Completeness of Vision".

*Magic Quadrant for Global WAN Services was previously named Magic Quadrant for Network Services, Global

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 date 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 with 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

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/