G Cloud 15: VBSE Vulnerability Scanning Service

Cyber Enhanced Vulnerability Scanning
Service Terms

Contents

Cyber Enhanced Vulnerability Scanning
Service Terms

1. The Service - Overview

1.1 The Vodafone Business Security Enhanced (VBSE) Vulnerability Scanning Service (the "VBSE Vulnerability Scanning Service") provides a means to scan assets in scope for CVEs (Common Vulnerabilities & Exposures). Supplier provides the VBSE Vulnerability Scanning Services by combining different Service Elements to create a solution for the Buyer (the "Buyer Solution"). Supplier will describe the Buyer Solution in a Buyer Solution Design and that Buyer Solution Design forms part of the Agreement. The term "Service" or "Services" in these Service Terms means the VBSE Vulnerability Scanning Service.

1.2 The term "**Service**" or "**Services**" in these Service Specific Terms means the VBSE Vulnerability Scanning Service.

2. Service Term Structure

2.1 These Service Terms form part of the Call-Off Contract entered into under the G Cloud 15 Framework.

2.2 The Call-Off Contract comprises the Call-Off Order Form, the Supplier's Service Terms, Service Definition and Pricing Document, and the applicable Call-Off Terms and Conditions.

2.3 These Service Terms describe how the Service operates and apply in conjunction with the Call-Off Contract.

2.4 In the event of any conflict or inconsistency between these Service Terms and the Call-Off Contract, the Call-Off Contract shall prevail.

3. General Conditions on the Buyer

The Service is available to Buyers that meet and agree the following criteria:

3.1 Additional Service Recipient:

3.1.1. If Buyer wishes to add an Additional Service Recipient, then Buyer shall:

(a) provide the full corporate details of the Additional Service Recipient;

(b) seek approval in writing from Supplier;

(c) inform the Additional Service Recipient of the contractual arrangements; and

(d) agree to pay such additional Charges as Supplier may reasonably request in relation to the approval of such requests.

3.2 Authorised Users: Access by Buyer to the Services and Equipment is limited to authorised Users. Buyer is responsible for ensuring Users' compliance with this Agreement.

3.2.1. If Supplier provides each authorised User with User Details, Buyer is responsible for:

(a) the security of User Details; and

(b) providing Supplier with the identity of the authorised Users and keeping that information current.

3.2.2. Supplier accepts no liability for any unauthorised or improper use or disclosure of any User Details. Buyer is liable for all acts and omissions relating to the User Details up until the time that it informs Supplier that they are being used without authority or may be compromised.

3.3 AUP: Buyer shall comply with the AUP in using the Services.

3.4 Third Parties: Buyer shall ensure that the Users and all Additional Service Recipients (if any) comply with this Agreement in relation to their use of the Services and Equipment and shall be liable to Supplier for the acts and omissions of the Users and all Additional Service Recipients (if any) in relation to this Agreement. Save as expressly permitted under this Agreement, Buyer shall not resell, distribute, provide or sub-licence the Services or Equipment (except Buyer Equipment) to any third party.

3.5 Terms of Use: Buyer shall not:

(a) make unauthorised modifications to the Services;

(b) use the Services as a means to establish permanent servers, relay connections or interconnection services or any similar commercial activities;

(c) do anything that causes the Network to be impaired;

(d) use automated means to make calls and/or texts or to send data (including via a GSM Gateway), unless expressly authorised in this Agreement;

(e) use the Services in a way that:

(i) may reasonably be considered to be a nuisance, defamatory, offensive, abusive, obscene or in violation of any person's rights; or

(ii) is illegal, fraudulent or contrary to good faith or commercial practice to Supplier's detriment; or

(f) use the Supplier's SMS service to send mass notification messages, or mass marketing messages, whether or not the messages are unsolicited unless expressly authorised in this Agreement.

3.6 **Service Monitoring:** Buyer gives express consent for Supplier to monitor Buyer's use of the Service (and disclosing and otherwise using the information obtained) to the extent allowed by Applicable Law to:

(a) comply with Applicable Law;

(b) protect the Network from misuse;

(c) protect the integrity of the public internet and/or Supplier's systems and Networks;

(d) determine if Buyer has breached any conditions or restrictions on use of the Service;

(e) provide the Service; and/or

(f) take any other actions agreed or requested by Buyer.

3.7 **Compatibility:** Buyer shall ensure its systems, equipment and processes satisfy any Technical Prerequisites and if required to be used in conjunction with the Equipment and/or the Services, are in good working order (if applicable) and are compatible for use with the Equipment and/or the Services. Supplier shall use reasonable endeavours to advise Buyer of relevant requirements on request, but in no event shall Supplier be responsible for any performance or non-performance issues with the Equipment and/or the Services, or liable to support the Equipment and/or the Services, if Buyer's systems, equipment, or processes fail to satisfy the Technical Prerequisites or are otherwise incompatible with the Equipment and/or the Services. Supplier may suspend the provision of any Service for which Technical Prerequisites have not been procured within the specified period and charge Buyer any applicable Recovery Charge.

3.8 **Security and Misuse:** Buyer shall take reasonable steps in line with commercial good practice with entities it controls to limit misuse of or threat to the Service or Network; and address any misuse or threat identified by Supplier through the implementation of appropriate security or user controls. Buyer shall not run any security tests, vulnerability scans or penetration tests on Supplier Equipment or Services without Supplier's prior written approval.

3.9 **Unauthorised Equipment or Repairs:** Buyer acknowledges that:

(a) Equipment or Buyer Equipment not authorised for use on the Network; or

(b) any unauthorised attempt to repair or tamper with the Equipment,

may result in an impaired User experience and/or invalidate the manufacturer's warranty.

3.10 **End of Life**

3.10.1. **Notification:** Where Equipment is End of Life, Supplier may, on provision of reasonable notice:

(a) retire the Equipment; and/or

(b) provide the Buyer with an option of replacement Equipment which provides equivalent or improved functionality to the extent that alternatives are available.

3.10.2. **Replacement:** Where End of Life Equipment is replaced in accordance with clause 3.10.3 (Notification), the costs of such replacement shall be charged to Buyer a One-Off Charge and invoiced accordingly.

3.10.3. **Continued Use:** Where, following receipt of an End of Life notification in accordance with this clause, Buyer continues to use End of Life Equipment, or does not use its best endeavours to allow Supplier to replace the End Of Life Equipment, Supplier:

(a) shall have no maintenance obligations for the End of Life Equipment;

(b) shall not be liable for Buyer's use of the End of Life Equipment;

(c) shall not be liable for any service levels relating to the Equipment; and

(d) reserves the right to suspend all or part of the affected service.

3.11 **Buyer Equipment:** Where Buyer provides Buyer Equipment for use with a Service, Buyer shall (and Buyer acknowledges that failure to do so will excuse Supplier from liability for failure to deliver the Service):

(a) install and configure the Buyer Equipment at Buyer Sites by the date necessary to allow Supplier to perform its obligations;

(b) maintain the Buyer Equipment to Supplier's satisfaction, including prompt installation of security patches and updates;

(c) immediately replace any Buyer Equipment which is declared by its manufacturer as end-of-life (or otherwise stops marketing, selling or supporting it) and notify Supplier of any such replacement;

(d) promptly after the Service terminates, give Supplier access to and reasonable help with disconnecting Buyer Equipment from the Service; and

(e) warrant and undertake that Buyer has full authority to permit Supplier to perform the Service using the Buyer Equipment.

3.12 **Exclusions:**

3.12.1. Supplier does not guarantee that the Services will be continuously available and/or fault-free and Buyer acknowledges that faults may occur from time to time. This acknowledgement is without prejudice to any specific service levels agreed between the Parties in this Agreement.

3.12.2. Buyer is responsible for satisfying itself that the Services and any Equipment are suitable for its intended purpose and requirements (including but not limited to any resiliency and/or business continuity requirements). Supplier does not warrant or represent that the Services and Equipment are or will be fit for Buyer's intended purpose and requirements. Supplier recommends that Buyer obtains business continuity (or other) insurance that is appropriate for the nature of its business.

3.12.3. Supplier is not responsible for any content, goods or services which are accessed, downloaded or transmitted by Buyer through use of the Services. Supplier accepts no responsibility for any such content, goods or services. Buyer shall take appropriate measures to back up data and otherwise protect against loss of data under this Agreement.

3.12.4. Buyer acknowledges that the Service is not intended for use by Consumers in the European Union. Without prejudice to the foregoing, the Buyer shall immediately notify Supplier if it becomes aware that anyone other than Supplier has made available, or intends to make available, the Service to a Consumer in the European Union.

3.13 **Termination:** Where Buyer terminates the Call-Off Contract during the Call-Off Contract Period, the Buyer agrees to pay Supplier's reasonable, committed and unavoidable losses resulting from the termination of the Call-Off Contract.

3.14 Network Sunset

3.14.1. Buyer hereby acknowledges and accepts that:

(a) certain Network technologies used to provide the Service on Supplier Equipment or Buyer Equipment may retire prior to the expiry of the contract; and/or

(b) current Networks may be replaced by further advanced Network technologies during the term of the Call-Off Contract.

3.14.2. As a result, Buyer agrees that maintaining compatibility of its devices with the available Networks from time to time shall be its responsibility.

3.15 **Planned Service Changes by Third-Party Providers:** Supplier has been informed that BT Openreach (the "Third-Party Provider") for legacy PSTN is withdrawing the service, with full switch off expected to be complete by 31 January 2027. Supplier is entitled to move the Buyer from legacy PSTN to Ethernet Access Method as and when required. Buyer will be advised of an alternative Service Element and the associated Charges, as set out in these Service Terms below. Buyer will have the option to either order an alternative Service Element or to cancel the affected Service Element only in accordance with the terms of these Service Terms and Call-Off Contract.

3.16 **Interpretation:** In this Agreement, unless the context otherwise requires, words in the singular include the plural and vice versa.

3.17 **Format:** If Buyer requires this Agreement (or any bills, communications or a document referred to in this Agreement) in a different format, call 03333 043 222 or email disability.access@vodafone.co.uk for a large print, braille version, dyslexia-friendly or audio CD version. These contact details are for accessibility ***help*** only.

4. Fixed Services Conditions on the Buyer

4.1 **Service Commencement Date:** Buyer shall notify Supplier within 5 Working Days of the Service Commencement Date if, in the Buyer's reasonable opinion, the Services do not conform to the standard testing criteria and provide sufficient supporting details. Upon receipt of Buyer's notification, Supplier shall take reasonable action to meet the standard testing criteria.

4.2 **Supplier-Owned Equipment:** The following will apply where Supplier provides Fixed Equipment for Buyer's use with a Service:

4.2.1. **Title:** Title to the Fixed Equipment at all times belongs to Supplier, its suppliers or subcontractors (subject only to any rights which may be granted to Buyer in respect of Supplier Software, as set out in these Service Terms).

4.2.2. **Buyer Obligations:**

4.2.3.1 Buyer agrees to:

(a) provide secure storage for Fixed Equipment that is sent to Buyer Sites prior to installation;

(b) use the Fixed Equipment only for the purpose of using the Services, in accordance with Supplier's instructions and Applicable Law;

(c) allow only Supplier's authorised representatives to add to, move, modify, inspect, test or alter the Fixed Equipment (either on Buyer Site or remotely);

(d) adequately insure for, and notify Supplier immediately of loss, breach or suspected breach or damage to the Fixed Equipment;

(e) only connect the Fixed Equipment to the Network using a network termination point that has been approved in advance by Supplier;

(f) provide Supplier with:

(i) adequate power supply, connection, and space for the operation of the Fixed Equipment at Buyer Sites; and

(ii) in the case of BPE patch cords and cabling; and

(iii) 10 Supplier Working Days' notice of any known disruptive event (such as power disconnection).

4.2.3.2 Additionally, specifically in relation to BPE, Buyer shall:

(g) appoint a local security representative to ensure the physical security of the BPE who will grant access by approved authorised personnel only and conduct routine physical checks, including ensuring tamper evident labels remain intact; and

(h) ensure that the physical environment in which the BPE is housed is appropriate for the protective marking of the data being transmitted through such Fixed Equipment. In particular:

(i) BPE must be located in a communications room or other isolated area that is suitable to limit the occurrence of accidental or malicious damage to the BPE; and

(ii) if the BPE is located in a shared environment, then it must be kept in a dedicated locked cabinet or rack. If that is not possible, robust access control mechanisms must be implemented by Buyer, with access only available with prior approval from Buyer's local security representative.

4.2.3. **Buyer Equipment:** Where Buyer provides Buyer Equipment for use with a Service Buyer shall (and Buyer acknowledges that failure to do so will excuse Supplier from liability for failure to deliver the Service

4.2.4. install and configure the Buyer Equipment at the Buyer Sites by the date necessary to allow Supplier to perform its obligations;

(i) Maintain the Buyer Equipment including prompt installation of security patches and updates;

(ii) Promptly after the Service terminates, give Supplier access to, and reasonable help with, disconnecting Buyer Equipment from the Service; and

(iii) Warrant and undertake that Buyer has full authority to permit Supplier to perform the Services using the Buyer Equipment.

4.3 Buyer Sites: For the purposes of preparing for and delivery of the Services, Buyer shall:

(a) carry out, or permit Supplier or its subcontractors to conduct, a Site Survey;

(b) prepare the Buyer Site for the Services in accordance with Supplier's instructions;

(c) allow and/or have in place (or assist Supplier to do so at Buyer's cost) all third-party consents necessary to allow Supplier or its subcontractors and agents (and obtain consents from third parties to allow) to:

(i) access the Buyer Sites, and any Buyer Equipment, Fixed Equipment or Equipment, and third-party property located there, as Supplier reasonably requires to perform its obligations under this Agreement (including for the purposes of installing and uninstalling Equipment (whether in the Buyer Sites or outside) and providing and preparing for the provision of, the Services) and including access outside Working Hours; and

(ii) ensure that Buyer Sites are safe and have a suitable working environment.

4.4 Emergency Services:

4.4.1. **General**: In the event of a power cut or failure affecting Buyer's fixed line and/or broadband Service, and/or a failure of the internet connection on which the Service relies, Buyer may not be able to make calls including calls to emergency services. This may also affect any calls using the internet including calls to emergency services.

4.4.2. **Buyer Obligations**: Buyer shall:

(a) provide Supplier with complete and accurate Buyer Site address information; and

(b) give Supplier at least 30 days' written notice of any change to the location of any Fixed Equipment and to any change to the relevant Buyer Site address information.

4.4.2.1 Buyer acknowledges that any failure to provide the information required in 4.4.2 may render emergency services unable to identify User's location.

4.5 Calls Using the Internet: Where a Service places calls using the internet, Buyer shall:

4.5.1. Make Users accessing the Service via a soft client aware that Supplier may be unable to automatically determine their location if they make an emergency services call using the Services.

4.5.2. Ensure that such Users provide their location details in the event that they make an emergency services call using the Services. In the event of a power failure, the emergency call placed will be routed over the Network and not through the Service.

4.5.3. Provide a registered address where a Buyer or User will make calls over the internet including if there are multiple addresses where such calls will be made and keep information on all such locations up to date.

4.6 Survey: These Service Terms and each Service Element are subject to survey. In the event a Site Survey output results in an increased price from the Call-Off Contract, the Buyer has the right to cancel the affected Service Element only in accordance with the terms of this Service Offer and the Call-Off Contract.

4.7 Third-Party Costs: Unless otherwise agreed and stated in the Buyer's Call-Off Contract, the Buyer will be liable for any additional costs charged to Supplier by third parties in connection with the provision of the Services. Such Charges (often referred to as Excess Construction Charges) are detailed in the Professional Services section of these Service Terms. These Charges will be notified to the Buyer before any construction works take place. In the event this results an increased price from the Call-Off Contract, the Buyer has the right to cancel the affected Service Element only in accordance with the terms of these Service Terms and Call-Off Contract.

5. Service Specific Conditions of Use

5.1 Buyer Obligations:

(a) **Compliance with AUP:** Buyer must ensure that any person who uses the VBSE Vulnerability Scanning Services shall comply with Supplier's acceptable use policy (as amended from time to time), which can be found at www.vodafone.com/business/AcceptableUsePolicy;

(b) **Buyer Representative:** Buyer must nominate a representative (the **"Buyer Representative"**) who must be able to make financial and contractual decisions relating to the user requirements;

(C) **Project Plan:** Buyer must carry out the tasks allocated to the Buyer under the project plan agreed with the Buyer Representative;

(d) **Access to In-scope Assets:** Buyer shall be responsible for providing Supplier with access at all times to the Buyer's environment (including, but not limited to, In-scope Assets, Buyer Sites, and Buyer's network) to enable Supplier to provide support and/or carry out replacements or repairs in the event of any system failure;

(e) **Compliance with Terms:** Buyer must comply with any other obligations ascribed to the Buyer as set out in these Service Terms, or elsewhere in the Agreement or as reasonably notified to Buyer by Supplier from time to time;

(f) **Provision of technical data and other information:** Buyer must provide to Supplier all technical data and other information Supplier may reasonably request to enable Supplier to supply the Service;

(g) **Compliance with technical pre-requisites:** Buyer must ensure that the Buyer's systems comply with all pre-requisites for supply of the Services reasonably notified to the Buyer in advance by Supplier;

(h) **Security Scans:** Buyer shall notify Supplier in writing, and obtain the agreement in writing of Supplier, prior to carrying out any security scans;

(i) **No re-selling**: Buyer shall not re-sell, sub-lease, sub-rent or sub-license part or all of the Services;

(j) **Indemnification:** Buyer shall indemnify Supplier against any liability to any third party arising out of any use of information sent or received by the Buyer by way of Supplier system or a system of a supplier to Supplier;

(k) **Further Buyer Obligations:** Buyer must comply with the further Buyer Obligations set out in paragraph 8 (Buyer Obligations) of Annex 1 to these Service Terms;

5.2 Limitations:

(a) **Excluded Events:** Supplier shall have no responsibility or liability for any breach of the Agreement, or for failure or delay in performing its obligations, and shall have no obligation to pay Service Credits, where the breach, delay, or failure to meet a Service Level occurs as a result of or in connection with an Excluded Event.

(b) **Data Security and Internet Transmission:** Buyer acknowledges that the public internet is an inherently insecure environment. The use of the public internet is at the sole risk of Buyer and its Users. Supplier is relieved from all liability in connection with Buyer's and its Users' use of the public internet including liability for any disclosure of Confidential Information transmitted over the public internet.

5.3 Changes

General

5.3.1. Buyer is responsible for all Buyers costs, migration of Buyer data and updating of Buyer systems as a result of any changes made under this clause 5.

5.3.2. Supplier may make changes to the Buyer Solution in accordance with the Framework Agreement.

Operational Change

5.3.3 A change constitutes an "Operational Change" if:

(a) it is a technical or operational change which does not impact the Buyer Solution Design or the agreed timescales for the provision of the Buyer Solution; and

(b) it applies to Services that are already delivered and in service.

5.3.3. Operational Changes (as categorised by Supplier in Supplier's discretion) include changes such as modifications to scanning scope and changes to tuneable parameters such as frequency.

5.3.4. Operational Changes may be requested and implemented by way of the "**Operational Change Management Procedure**", which is set out in paragraph 5.10 below.

5.3.5. The Operational Change Management Procedure is not intended to be used:

(a) to resolve any loss of Service performance; or

(b) to deliver new Services.

5.3.6. Supplier will categorise a requested change as an Operational Change at Supplier's absolute discretion. Examples of changes that Supplier may (in its absolute discretion) categorise as Operational Changes include modifications to the Solution configuration. Supplier will categorise Operational Changes into the following categories and types at Supplier's absolute discretion:

(a) **Emergency Change:** an Operational Change:

(i) which is required to prevent the occurrence of a Severity 1 or Severity 2 Service Incident;

(ii) where the failure to implement the requested Operational Change would have a material and detrimental impact on Supplier's ability to provide the Services to Buyer; or

(iii) where the circumstances of the Operational Change necessitate Supplier providing an expedited response.

(b) **Routine Change:** an unplanned Operational Change which is not an emergency change.

5.3.7. Supplier will respond to Emergency Changes in priority to Routine Changes.

5.3.8. **Operational Change Management Procedure**: The procedure for reviewing, processing and recording requested Operational Changes is as follows:

(a) in the case of an Emergency Change:

(i) Emergency Changes must be raised with Supplier via telephone and electronically;

(ii) Buyer must only declare genuine Emergency Changes and Supplier reserves the right to downgrade an Emergency Change if, in Supplier's reasonable opinion, it is not a genuine emergency or Buyer makes excessive use of this facility;

(iii) Supplier will record and review the request for the Emergency Change and contact Buyer with a committed action in respect of the Emergency Change;

(b) In the case of a Routine Change:

(i) Routine Changes must be raised with Supplier electronically;

(ii) Supplier will record and review the request for the Routine Change and contact Buyer with a committed action in respect of the Routine Change.

Planned Works

5.3.9. Supplier will use reasonable endeavours to provide Buyer with at least 10 Working Days' notice of any Planned Works affecting Buyer.

5.3.10. Buyer may not refuse Planned Works that Supplier requires to ensure the integrity, supportability, security, performance or availability of any infrastructure for Buyer or Supplier's other customers.

5.3.11. Supplier will use reasonable endeavours to ensure that the Planned Works are not carried out in a way that affects the Services provided to Buyer in a materially detrimental way.

6. Data Protection

Supplier as a Data Controller

6.1 **Supplier as a Data Controller:** Supplier acts as an independent Data Controller for the Processing activities in these clauses 6.1 to 6.5 (Data Controller role and processing activities) and any additional activities listed in the Service Terms.

6.2 **Buyer as a Data Controller:** The Parties acknowledge that Buyer will also act as an independent Data Controller for any Personal Data relating to Supplier employees or representatives, for example business contact information.

6.3 **Processing Activities:** Supplier may process:

6.3.1. Personal Data to:

(a) manage account relationships;

(b) send bills;

(c) fulfil an Order or delivery;

(d) provide customer service; and

(e) control access to Supplier's systems that support the Services.

6.3.2. As an electronic communications service's provider, Traffic Data in accordance with Applicable Laws to:

(a) deliver User communications;

(b) calculate Charges for each User;

(c) identify threats to the Network or Services and protect against them; and

(d) internally develop and improve the Network or Services.

6.4 **Data Disclosures:** Supplier may disclose Personal Data and Traffic Data:

(a) to Vodafone Group or third parties for the purpose of supporting the Processing activities described in this clause 6 (Data Protection) or as permitted under Applicable Privacy Law; and

(b) as required by Applicable Law, court order, or any Authority (including Privacy).

6.5 **Privacy Notice:** Supplier's privacy notice can be accessed at: www.vodafone.co.uk/privacy.

Supplier as a Data Processor

6.6 **Supplier as a Data Processor:** Supplier acts as a Data Processor for the specific processing as set out in the relevant Service Terms.

6.7 **Processing Personal Data:** Supplier may only Process Personal Data on behalf of the Buyer:

(a) to provide and monitor a Service as outlined in the Service Terms; or

(b) for any other purpose agreed in writing between the Parties. Additional instructions from Buyer require prior written agreement and may be subject to Charges.

6.8 **Changes to Sub-Processors:** If Supplier adds or replaces a Sub-Processor, Supplier shall inform the Buyer of changes to Sub-Processors where Supplier is required by Applicable Privacy Law by:

(a) providing at least 10 Working Days' prior notice; or

(b) listing the new or replacement Sub-Processor on www.vodafone.co.uk at least 10 Working Days before Supplier authorises and permits the new or replacement Sub-Processor access to Personal Data in order to give the Buyer the opportunity to reasonably object to such changes.

6.9 **Sub-Processor Obligations:** Supplier will enter into binding agreements with its Sub-Processors, who will have substantially the same legal obligations for Processing activities as Supplier under these clauses 6.6 to 6.17 (Data Processor role and related requirements). Supplier will be liable to Buyer for the performance of that Sub-Processor's obligations.

6.10 **Data Retention:** Supplier may keep Personal Data for as long as required to deliver the Service. After this Agreement is terminated, and unless Applicable Law requires otherwise, Supplier will:

(a) delete the data within a reasonable time frame;

(b) return the data if the Buyer provides notification before termination of the Agreement.

6.11 **Data Access:** Supplier may give access to Personal Data only if necessary to meet its obligations in relation to the Service and will take reasonable steps to ensure that whoever accesses the data:

(a) is under a statutory or contractual obligation of confidentiality;

(b) is trained in Supplier's policies for handling Personal Data; and

(c) does not Process Personal Data except as instructed by Buyer, unless Applicable Law requires otherwise.

6.12 **Data Security:**

6.12.1. As required by Applicable Privacy Law, Supplier will:

(a) provide technical and organisational measures for a level of security appropriate to the risk presented by Processing taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing;

(b) comply with Supplier information security policies based on ISO / IEC 27001:2013;

(c) give Buyer all information, assistance, and co-operation it may reasonably require to comply with Applicable Privacy Law;

(d) notify Buyer without undue delay of any unauthorised access to Personal Data that results in loss or unauthorised disclosure of, or alteration to, Personal Data;

(e) provide reasonable assistance to Buyer in relation to any Personal Data breach notification that Buyer is required to make under Applicable Privacy Law; and

(f) when requested by Buyer and before any Processing, provide reasonable assistance with:

(i) carrying out a privacy impact assessment of the Services; and

(ii) consulting the relevant Privacy Authority regarding Processing activities related to the Services.

6.12.2. Further information on data security measures can be found at www.vodafone.com/business/customer-security.

6.13 **Audits and Inspections:** If Buyer has a right of audit and inspection under Applicable Privacy Law, it agrees to act as follows:

(a) Buyer may ask to review Supplier's security organisation, and the good practice and industry standards contained in Supplier's information security policies no more than once each calendar year, and any such review shall relate only to data protection compliance of the Services; and

(b) ensure its instructions comply with Applicable Privacy Law. Supplier will inform Buyer if it believes any Buyer instruction infringes Applicable Privacy Law or any confidentiality obligations.

6.14 **Buyer Responsibilities:** Buyer accepts and agrees that they are responsible for:

(a) reviewing the information Supplier makes available; and

(b) determining if the Services meet Buyer's requirements and legal obligations.

6.15 **Onward Transfers out of the EEA and UK:** Supplier may onward transfer Personal Data to a country outside the European Economic Area, the UK or a country that has not been designated by the European Commission or Secretary of State in the UK as ensuring an adequate level of protection under Applicable Privacy Law, only if:

(a) the data is transferred in line with the requirements under Applicable Privacy Law;

(b) the Processing or transfer does not put any Buyer in breach of Applicable Privacy Law; or

(c) Applicable Law requires it. In this case, Supplier will inform Buyer of that legal requirement before Processing, unless prohibited by Applicable Law.

6.16 **Law Enforcement:** Supplier:

(a) may receive legally binding demands from a law enforcement authority for the disclosure of, or assistance with Personal Data, or be required by Applicable Law to disclose Personal Data to persons other than Buyer ("Demand");

(b) is not in breach of any obligation to Buyer in complying with the Demand; and

(c) will notify Buyer of the Demand as soon as possible, unless prohibited by Applicable Law.

6.17 **Data Subject Enquiries:** Taking into consideration the nature of the data processing conducted by Supplier on behalf of the Buyer, Supplier shall assist the Buyer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Buyer's obligation to respond to requests for exercising the data subjects' rights laid down in Applicable Privacy Law.

7. Service Elements

7.1 **Service Elements:** The Service shall comprise:

(a) Core Service Elements; and

(b) Optional Service Elements, where selected.

7.1.2. The Core Service Elements and Optional Service Elements are set out at paragraphs 2 and 3 of Annex 1.

7.2 Each Service Element may have a different Service Commencement Date and Initial Term as detailed in these Service Terms and the relevant Order.

7.3 The Service provides for:

(a) Vulnerability scanning of assets in scope for CVEs (Common Vulnerabilities & Exposures) as specified in the Buyer Solution Design.

(b) Vulnerability monthly report of CVEs ranked by severity from the Common Vulnerability Scoring System (CVSS), as specified in the Buyer Solution Design.

7.4 The resilience of the Service will be described in the Buyer Solution Design.

7.5 Adding Assets to the Buyer Solution may incur additional charges.

7.6 Key performance indicators are specified at paragraph 5 of Annex 2.

7.7 Supplier's engineers or engineers of Supplier's sub-contractors are responsible, on Supplier's behalf, for installation and maintenance of the equipment delivered and managed as part of the Services.

7.8 Where agreed, Supplier will carry out procurement and arrange for appropriate equipment to be shipped to Buyer provided locations as defined in the Buyer Solution Design or relevant Order. Supplier will ensure the equipment is fitted, racked, powered and connected to the Buyer's LAN, all of which the Buyer must ensure is provided and ready in advance. Supplier reserves the right to charge the Buyer for costs incurred in respect of the engineers attending any Site at which agreed prerequisites (as set out in these Service Terms and/or the Buyer Solution Design) are not provisioned. Once evidence of connectivity has been ascertained, Supplier engineers will then remotely configure and manage the device.

7.9 Supplier shall have no responsibility for any failure to meet Service Levels if Engineers cannot gain access to a location with on-site equipment for any reason.

7.10 The Services require appropriate connectivity in place to enable Supplier's remote management. The required connectivity will be specified in the Buyer Solution Design.

8. Service Level Agreement

8.1 The Service benefits from the Service Levels and Service Credits set out in Annex 2.

9. General Definitions

9.1 The following definitions apply to the **section 3 - General Conditions on the Buyer** of these Service Terms:

Additional Service Recipient	a Buyer Group entity which is not a direct party to this Agreement, but which is named in this Agreement as a beneficiary of the Services or otherwise approved to receive the Services in accordance with clause 3.1 (Additional Service Recipient).

Cyber Enhanced Vulnerability Scanning Service Terms

Agreement	this agreement, consisting of the documents set out in clause 2 (Service Terms Structure).
Applicable Law	law, regulation, binding code of practice, rule or requirement of any relevant government or governmental agency, regulatory Authority, each as relevant to (i) Supplier in the provision of the Services and/or (ii) Buyer in the receipt of the Services or the carrying out of its business.
AUP	Supplier's acceptable use policy set out at http://www.vodafone.co.uk/Acceptable-Use-Policy-Business, as updated by Supplier from time to time.
Buyer	the entity identified in the Call-Off Order Form as such.
Buyer Equipment	hardware, software or any other tangible material not supplied by Supplier that is used with or to access the Service. Any Equipment Buyer purchases from Supplier shall be considered to be Buyer Equipment once title has passed to the Buyer.
Buyer Group	Buyer and any company in which Buyer has the beneficial ownership of more than 50% of the issued share capital, or the legal power to direct the general management of the company in question, either at or after the date of this Agreement.
Buyer Site	as the context permits a Buyer's premises (either owned by Buyer or a third party) which Supplier needs to access in order to deliver or install Equipment and/or to provide the Services or the location where the Services are to be provided, as set out in the Call-Off Order Form.
Charges	the charges or fees specified in this Agreement as payable by Buyer.
Consumer	means any natural person acting for purposes that are outside the person's trade, business, craft or profession.
End Of Life	where Supplier or a manufacturer of Equipment declares that the type of Equipment is end-of-life (or otherwise stops marketing, selling or supporting it).
Equipment	hardware, Supplier Software, and any other tangible equipment (other than SIMs) supplied by, or on behalf of, Supplier to Buyer for use in receiving the Services. Equipment excludes Buyer Equipment.
European Union (EU)	an economic and political union of 27 countries, as may be updated from time to time. A full list of countries can be found here https://www.gov.uk/eu-eea.
GSM Gateway	any equipment containing a SIM which enables calls from a fixed network (landline) to be routed via a GSM link to a mobile network establishing a mobile-to-mobile ('on-net') call.
Incumbent Provider	a regulated operator who is authorised to provide a Service in a given country.
Intellectual Property Rights	(a) rights in, and in relation to, any patents, registered designs, design rights, trade marks, trade and business names (including all goodwill associated with any trade marks or trade and business names), copyright, moral rights, databases, domain names, topography rights and utility models, and includes the benefit of all registrations of, applications to register and the right to apply for registration of any of the foregoing items and all rights in the nature of any of the foregoing items, each for their full term (including any extensions or renewals) and wherever in the world enforceable; (b) rights in the nature of unfair competition rights and rights to sue for passing off; and (c) trade secrets, confidentiality know how, technical information and other proprietary rights.
Network	the communications network together with the equipment and premises that are connected to such network and which are used by Supplier to perform the Services.
Non-Recurring Charges	means One-Off Charges.

One-Off Charges	the Non-Recurring Charges payable by Buyer in relation to the Service and/or Equipment as described in the Commercial Terms and/or in Buyer's Call-Off Order Form, and may include installation Charges for ports, access circuits and routers, charges for set up of Service Elements and configuration changes.
Party or Parties	Buyer and/or Supplier, as relevant.
Recovery Charge	any amount payable by Buyer for early termination or failure to meet commercial commitments as set out in this Agreement.
Service Element	the individual components of a Service (including optional service elements if applicable).
Service Specific Terms	the document(s) identified in this Agreement as the "Service Specific Terms" that set out information such as terms and conditions, specifications and technical information specific to a Service.
Service(s)	the services to be provided by Supplier or a Third Party Provider under this Agreement and as specified in this Agreement. Any reference to Service within this Agreement may be an individual Service or collectively all Services, as appropriate.
SIM	a "subscriber identity module" card is an integrated circuit, whether physical or embedded in a device (and then known as an eSIM Card), storing user specific data and provided by Supplier to allow use of equipment on the Network by Buyer.
Supplier	where used in these Service Terms or the Call-Off Contract means Vodafone Limited.
Supplier Software	any Software supplied by Supplier or its licensors to Buyer (including Software embedded in any Equipment).
Technical Prerequisites	any requirements detailed in the Service Specific Terms or otherwise provided to Buyer in writing relating to a Service or Equipment including notification to upgrade.
Third Party Provider	a third party contracted directly or indirectly by either Supplier (including Vodafone Group) or Buyer that provides a Service, a Third Party Service or that provides a service that connects to a Service. Third Party Providers may include Incumbent Providers.
User	an individual end user of the Services who is approved by Buyer and who must be a permanent or temporary employee or sub-contractor of Buyer or an Additional Service Recipient unless otherwise specified in this Agreement.
User Details	a user name, password, or other access information used by a User to access the Service and/or Equipment.
UK	England, Wales, Scotland, Northern Ireland and adjacent islands (e.g. Isle of Wight) but excluding the Channel Islands and the Isle of Man.
Vodafone	Vodafone Limited, registered number 01471587, and registered office Vodafone House, The Connection, Newbury, Berkshire RG14 2FN.
Vodafone Group	(a) Vodafone Group Plc, Vodafone Limited and any company in which Vodafone Group Plc owns (directly or indirectly) 15% or more of the issued share capital; and (b) any partner market listed on the "Where we are" page at http://www.vodafone.com/.
Working Days	Monday to Friday inclusive, other than public holidays in the UK.
Working Hours	9.00am to 5.00pm on a Working Day.

9.2 The following definitions apply to the Fixed Services Conditions on the Buyer set out in section 4 of these Service Terms:

BPE (Buyer premises equipment)	Fixed Equipment on Buyer Site.
Fixed Equipment	hardware, Supplier Software, BPE and any other tangible equipment (other than SIMs and mobility equipment) supplied by or on behalf of, Supplier to Buyer for use in receiving the Services.
Service Commencement Date	the date of completion of Supplier's testing when the Service is ready for use.
Site Survey	a survey of a Buyer's Site to assess whether (in Supplier's opinion) the existing infrastructure is sufficient for providing the Services and detailing what the Buyer needs to do to receive the Service.

9.3 The following definitions apply to the Service Specific Conditions on the Buyer and Service Elements set out in **sections 5, 7 and 8** of these Service Terms:

Buyer Solution	a set of Services comprising specified Service Elements, to scan customer Assets, which Services may also utilise Equipment and Supplier Software, all of which are more specifically defined in the Buyer Solution Design.
Excluded Event	any of the following: (a) any fault in, or any other problem associated with, Buyer-supplied; electricity or other Buyer-supplied power source, hardware, software, non-maintained structured cabling or other telecommunications network or systems not provided by Supplier; (b) any fault, or negligent act or omission on the part of: (i) any third party that is not within Supplier's direct control; or (ii) Buyer (c) any suspension of the Service in accordance with the provisions of the Agreement, or otherwise agreed between the Parties; (d) any other circumstances caused by events for which Supplier has expressly excluded liability in accordance with the provisions of the Agreement (including these Service Terms); (e) any delay or failure of the Buyer to fulfil or perform its obligations under the Agreement (including, but not limited to, the obligations set out in paragraph 4.1 of these Service Terms and in paragraph 8 of Annex 1 to these Service Terms); (f) a fault or incident with another Supplier service purchased under a separate agreement; (g) a Service Incident, delay, or breach of the Agreement resulting from a request by Buyer for expedited delivery of the Service; (h) Buyer's request to modify or test a Service Element; (i) a Force Majeure Event; (j) a Service Request during implementation of the Solution;

	(k) a Service Incident caused by service failure at any other Buyer Site; (l) Planned Works; (m) any breach of the Agreement, failure, or delay to performance in relation to Equipment and/or Supplier Software which has been modified or changed on the Buyer's behalf and where Supplier has not agreed that such modification or change will not affect Supplier's liability to pay Service Credits; (n) a breach of the Agreement, failure or delay in performance, or Service Incident which arises as a result of the Buyer failing to agree to the installation of an upgrade, patch or change recommended by Supplier, such as security or other fixes; and/or (o) any circumstances where engineers cannot for any reason gain access to a location with on-site hardware required for provision of the Service.
In-scope Asset	The equipment, device or application to which the Service is provided, as set out and delineated within the Buyer Solution Design, subject to any subsequent amendments or changes to the Buyer Solution Design, or to the delineation of the In-scope Assets, which is agreed and documented in writing.
NOC	Supplier's Network Operations Centre.
Operational Change	has the meaning set out in 5.3.4 – 5.3.10 of these Service Terms.
Planned Works	planned Supplier-initiated changes to the Service or equipment (including, for example, activities undertaken to carry out routine or essential maintenance or upgrades, or to take preventative actions to support the running of Supplier's infrastructure).
Professional Services	the optional services from Supplier in order to customise the Buyer Solution, obtain additional services based on the Buyer's individual requirements, or obtain project management in respect of the Buyer Solution.
Quarterly Measurement Period	means the period from the Service Level Commencement Date up to the end of the calendar quarter and then each calendar quarter thereafter (save for the last quarter that will end upon the termination date of the Service).
SOC	Supplier's Security Operation Centre.
Services	the services (which consist of Fixed Services and/or Mobility Services, and which include any applicable Service Elements) to be provided by Supplier or a Third Party Provider under this Agreement and as specified in this Agreement. Any reference to Service within this Agreement may be an individual Service or collectively all Services, as appropriate.
Service Availability	the percentage of time the Buyer Solution or Service Element as applicable is available for use in a Quarterly Measurement Period.

Service Credit(s)	the service credit payable by Supplier to Buyer in accordance with these Service Terms, in particular Annex 2 (Service Levels).
Service Incident	an unplanned interruption to the Service, a reduction in the quality of a Service, or a failure of a Service configuration item.
Service Level(s)	the service levels that apply to the provision of the Service as set out in Annex 2 to these Service Terms.
Service Level Commencement Date	in respect of the Buyer Solution, or an individual Service Element (if applicable) the later to occur of: (i) the end of the Service Baselining Period; or (ii) the Service Commencement Date for such Buyer Solution or individual Service Element as applicable.
Service Request	a minor customer request for a standard or catalogue pre-approved change that is low risk, relatively common and follows a standard procedure (for example, a password reset), and excluding an Operational Change.
Solution	a combination of customer Assets and Service Elements specified in the Buyer Solution Design, as may be supplemented or amended in accordance with these Service Terms.
Buyer Solution Design	the document prepared by Supplier to describe, the technical aspects of the Buyer Solution including the Service Level details.
Trouble Ticket	a record of a Service Incident with a unique reference allocated to it that is used for all subsequent updates and communications.

The following definitions apply to **section 6 - Data Protection** of these Service Terms:

Applicable Privacy Law	the relevant data protection and privacy law, regulations (including UK GDPR and the Data Protection Act 2018) and other regulatory requirements to which Supplier Limited is subject.
"Fixed Authority	means those governments, agencies, courts of law, and professional and regulatory authorities including NRAs that supervise, regulate, investigate, or enforce Applicable Law.
Data Controller	the person that determines the purposes and means for which Personal Data is Processed, as defined under Applicable Privacy Law.
Data Privacy Obligations	in respect of each Party, that Party's obligations relating to the Processing or control of Personal Data as a Data Controller or Data Processor, as expressly set out in clause **Error! Reference source not found.** (Data Protection) of this Agreement.
Data Processor	the person that Processes Personal Data on behalf of the Data Controller as defined under Applicable Privacy Law.

European Economic Area (EEA)	means the Member States of the European Union together with Iceland, Liechtenstein, and Norway, as may be updated from time to time. A full list of countries can be found here https://www.gov.uk/eu-eea.
GDPR	General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data.
Personal Data	shall mean any information relating to an identified or identifiable natural person as defined by the Applicable Privacy Law.
Privacy Authority	the relevant statutory or supervisory authority with responsibility for the Applicable Privacy Law in the jurisdiction of the Data Controller.
Process/Processed/ Processing/ Processes	obtaining, recording or holding information or data or carrying out any operation or set of operations on it.
Sub-Processor	a sub-contractor who is processing Personal Data on behalf of Supplier.
Traffic Data	any data processed for the purpose of the conveyance of a communication on an electronic communications network and for billing.
UK GDPR	means GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

ANNEX 1

KEY TECHNICAL FEATURES

1. Overview

1.1 Supplier is an established provider of industry leading security services to organisations and institutions in the UK. VBSE is a division of Supplier dedicated to protecting critical national services, based in secure locations, and staffed by UK security cleared personnel, from the account management team through to personnel working on design, installation and operations. The Vulnerability Scanning Service is a part of a portfolio of security products offered by VBSE.

1.2 The Service examines the software version, patches and configuration of In-scope Assets for potential security vulnerabilities and supplies regular reports detailing potential Security Vulnerabilities on the In-scope Assets.

1.3 The Service analyses In-scope Assets against known vulnerabilities. Where a Security Vulnerability is found by the software used in the service, that will be reported.

1.4 VBSE delivers services entirely using UK-based VBSE staff. VBSE staff, including all field engineers, are security cleared. VBSE are responsible for all aspects of the Services, including account management, design, operation and service management. All core VBSE equipment is housed in secure facilities.

2. Core Service Elements

2.1 VBSE Vulnerability Scanning Service includes the following Core Service Elements:

(a) Vulnerability Scanning Platform: Security Vulnerability scanning services supplied by Supplier. The platform will connect to In-scope customer assets using credentials provided by the customer to perform the scan. No agent software is required on the customer assets;

(b) Vulnerability Information: Supplier will collect vulnerability information from In-scope customer assets and present that in reports to the customer;

(c) Management: Central management by VBSE including maintenance, configuration and fault fixing backed up with SLAs;

(d) Proactive Monitoring: Standard proactive monitoring and 24x7x365 fault management; and

(e) Service Levels: for Availability and Service Incident Resolution (further details of which are provided in Annex 2 below).

3. Optional Service Elements

3.1 The Buyer Solution Design will specify whether the VBSE Vulnerability Scanning Services include any of the following:

(a) **Secure communications network:** Support for a range of secure communications to connect the Vulnerability Scanning Service in the VBSE Datacentres with the In-scope Assets.

(b) **Resilience options:** Single and resilient solutions are available for deployment in Supplier Datacentres and Buyer premises.

(c) **Service Level Management:** Options including regular service reviews, performance reporting and dedicated service management (see paragraph 6 below);

(d) **Monthly review meeting:** Remotely held review meeting of the vulnerability scan reports.

4. Features

4.1 **Service Configurations**

(a) Supplier configures the Service to support agreed In-scope Assets. This is a chargeable service included within the Buyer Solution Design that has the following deliverables:

(i) creation of a configuration for the In-scope Asset requested by the Buyer;

(ii) testing of the configuration to ensure it correctly connects to the In-scope Asset and can retrieve required information;

(iii) configuration of template reports;

(b) If the underlying In-scope Asset changes over time (e.g. a new version of software or configuration on an In-scope Asset), then the Buyer may need additional Professional Services to modify the configuration. Supplier will not be liable where changes to the underlying In-scope Asset mean that the specific element of the VBSE Vulnerability Scanning Service cannot continue to function as intended.

4.2 **Secure Communications Network**

The Buyer Solution Design will confirm how In-scope Assets will be scanned by scanners within the Supplier Data Centre(s).

4.3 **Service Setup**

(a) The Service includes equipment, licences, design and implementation of the Vulnerability Scanning Service. This includes:

(i) Implementation;

(ii) Supplier Data Centre space (with suitable power and cooling);

(iii) Connectivity between the In-scope Assets and the Vulnerability Scanning Platform;

(iv) 24x7x365 support

(v) Critical Security upgrades;

(vi) Monthly Reporting; and

(vii) Lead times quoted by Supplier for delivery of the service will be based on Supplier acceptance of order and completion of the approved design.

4.4 **Buyer Project Management**

(a) A Project Manager will usually be assigned to manage complex implementations to ensure that the solution is implemented in a timely and effective manner. Project Management is a chargeable service and the number of days required depends on the complexity of the Solution and Buyer requirements. The Project Manager will be responsible for:

(i) co-ordinating the delivery of required hardware, software and service integration;

(ii) agreeing with the Buyer any specific requirements and required delivery timescales; and

(iii) acting as the single liaison point for all Buyer contact until the Buyer Solution is live.

4.5 **Testing and acceptance**

Upon completion of the build phase, Supplier will perform a standard set of tests to confirm that all the components are working correctly and vulnerability information is collected from the In-scope Assets by the Service as expected. Additionally, the initial scan report(s) generated will form part of the testing. At the point that all tests have been performed successfully, the solution will be considered live.

4.6 **Reporting**

(a) The Service includes monthly reporting. Reports will be provided to the Buyer within an agreed week of the month following the final date to which the report relates. The report will typically comprise:

(b) High-Level data summary of top vulnerabilities and patching history from previous month;

(c) Low-level .CSV format file with full list of CVEs discovered from the scans.

5. Facility & Network Services

5.1 Each of the VBSE Data Centres applies an integrated approach to physical security in which a range of protective security measures deliver a “defence in depth” capability. These measures include:

(a) Manned Guarding – this includes 24x7 support for each site and each Security Officer is cleared to Security Check (SC) level and is Security Industry Authority (SIA) registered;

(b) External and Internal CCTV;

(c) Perimeter Intruder Detection;

(d) Lighting;

(e) Access Control Systems;

(f) CPNI (Centre for the Protection of National Infrastructure) Rated Rooms, Cabinets and Locks;

(g) Caging;

(h) Internal Intruder Alarms;

(i) Fire detection and suppression systems; and

(j) Redundant power, cooling and network architectures with generator backup.

6. Service Support

6.1 The Supplier Support model is an IT Infrastructure Library (ITIL) aligned support structure built to meet the needs of our customers integrating standard support agencies and key ITIL functions such as Incident, Problem and Change Management.

6.2 The VBSE Vulnerability Scanning Service is a fully monitored, managed and maintained service supported 24x7 by VBSE.

6.3 **Proactive Monitoring:** VBSE undertakes proactive monitoring of the Vulnerability Scanning service for a range of fault conditions. VBSE use a range of monitoring and alarm tools to detect events on the application and infrastructure and provide the required expertise to ensure that the application and infrastructure are maintained according to VBSE and Industry standards.

6.4 **Service Levels:** The Service benefits from the Service Levels and Service Credits set out in Annex 2.

7. Service Management

7.1 VBSE offers a chargeable option for Service Level Management ("SLM").

7.2 SLM is a fundamental part of our Services Support Model providing specialised additional services to our customers alongside our standard business support functions.

7.3 Supplier SLM aims to meet and exceed agreed service delivery and performance targets and ensure future services are also delivered in the same way; constantly striving to exceed expectations and drive continual service improvement.

7.4 **Service Level Management (SLM) Key features**

Deliverables	Detail / Frequency
Service Manager resource	VF Office Based
Buyer Satisfaction Surveys; regular surveys to collate Buyer feedback. Linked to service improvement and development plans.	Quarterly
Monthly Service Reports; detailing performance against service level targets and proactively identifying performance trends requiring improvement or development	Mid-Level
Service Level Performance Analysis; Improvement actions tracked with clear deadlines for progress and resolution.	10 Days Post Reporting Period
Service Reviews; monthly joint business review to drive service quality and efficiency in line with Buyer goals and priorities.	By Phone (Monthly)
Service Improvement Plans; Improvement actions tracked with clear deadlines for progress and resolution.	Yes
Knowledge Management; Buyer specific document production, storage and inventory management.	Bi-annual
Contact Model - Specialist to Specialist, e.g. security specialists, technical analysts etc.	Yes

8. Escalation Procedures

8.1 VBSE has established Operational and Hierarchical escalation processes in place to ensure we are proactive in escalating issues that are not being resolved within SLA and to address non-operational issues quickly.

8.2 **Operational Escalations**

(a) These can be initiated at any point in the lifecycle of an incident, change or new provisioning activity if the customer feels that the service level target is in danger of not being met or the support mechanisms in place to manage and resolve an issue are not working.

(b) Operational escalations should in all cases be made by telephone, whereas hierarchical escalations can be made by telephone or email.

(c) Operational escalations table (incidents & change):

Level	Title	Criteria	% of Target Time to Restore (depending on Severity Level) elapsed since the beginning of the Incident
1	NOC Analyst	SLA at risk of not being met No action plan or path to resolution within SLA Lack of response or co-operation	75%
2	NOC Manager & Service Manager (if assigned)	SLA at risk of not being met No action plan or path to resolution within SLA Previous action plan failed Lack of response or co-operation	90%
3	Sector Service Lead & Head of Sales	SLA missed No action plan or path to resolution within SLA Previous action plan failed Lack of response or co-operation	100%
4	Head of Business Security Enhanced	No action plan or path to resolution. Missed 2 x SLA or agreed action plan failed Lack of response or co-operation Breach	Breach

(d) Operational Escalations table (New orders/provisioning):

Level	Title	Criteria	% of Target Time to Restore (depending on Severity Level) elapsed since the beginning of the Incident
1	Project Manager or Implementation Manager	Agreed Delivery Date at risk of not being met No action plan or path to resolution Lack of response or co-operation	50%
2	Programme Manager	Agreed Delivery Date at risk of not being met No action plan or path to resolution Previous action plan failed Lack of response or co-operation	75%
3	Sector Service Lead &/or Head of Sales	Agreed Delivery Date at risk of not being met No action plan or path to resolution Previous action plan failed Lack of response or co-operation	90%
4	Head of Vodafone Business Security Enhanced	No action plan or path to resolution. Agreed Delivery Date and action plan failed Lack of response or co-operation	Breach

8.3 **Hierarchical Escalations:** These can take place at any time to resolve issues that relate to a dispute with the contract, persistent breach of service levels, service performance calculations or if the customer is unsatisfied with how operational escalations are being handled.

Level	Account/Contract related	Support/Performance related	Timescale
1	Account Manager	Service Manager (if assigned)	To be agreed with the customer at each level and dependant on the nature of the escalation
2	Account Sector lead	Sector Service lead	
3	Head of Vodafone Business Security Enhanced		
4	Senior Manager Vodafone Business		

9. Buyer Obligations

9.1 The following are the responsibilities the Buyer must fulfil in order for Supplier to be able to deliver the Service in accordance with the Service Levels defined for the service. To the extent these are not fulfilled, Supplier will not be liable for failure to comply with an affected Service Level.

9.2 **Project lead**

Buyer must provide a project lead that will be the single point of contact and escalation route for the duration of the service setup.

9.3 **Asset credentials**

Provide expiry-free credentials for assets in scope for scanning.

9.4 **Contextual Information**

(a) Buyer must identify, keep up to date and provide VBSE with full and accurate information about the In-scope Assets. This is known as 'Contextual Information'.

(b) The effectiveness of the Service relies on Supplier having accurate and up to date Contextual Information about the Buyer environment. Contextual Information is used to assess CVEs seen to determine whether they require further investigation. The list below indicates the types of information that MUST be provided to Supplier in a timely manner to ensure the correct operation of the Service (including, but not limited to):

(i) Network Architecture Diagrams;

(ii) IP address subnets in use across the estate;

(iii) Server and Network Asset Data (IP addresses, patch levels, back profiles etc);

(iv) Summary of any SOC & SIEM solution in place and contact points;

(v) Changes to software releases, patches or new application code introduction;

(c) Where Supplier is operating the underlying service, much of this information will be collated and managed by Supplier. It is the Buyer's responsibility to ensure that any relevant information under Buyer's control is passed to Supplier in a timely fashion to allow the information to be included in the contextual information set for the solution.

9.5 **Authorised contacts**

(a) A list of authorised Buyer contacts must be provided and maintained. Buyers are responsible for notifying Supplier of any changes to this list of authorised contacts e.g. new staff. As a minimum one central administrative / technical contact will be required who will act as the Buyer Representative with regard to queries.

(b) All change requests must come from an authorised contact. Buyers should ensure that all necessary personnel are informed of the need to follow the agreed request procedure.

(c) Buyer agrees to keep the list of contacts up to date. Should, for any reason, it become necessary to notify Supplier of the removal of a named contact then that request should be forwarded immediately to the Supplier SOC.

9.6 **Configuration**

(a) The Buyer is responsible for ensuring that the necessary communication protocols can traverse Buyer's networks, and for making any necessary changes to enable delivery of the Service.

9.7 **Third parties**

Buyer must engage and manage its third-parties as required to support delivery of the Service.

9.8 **Notification of Buyer Change**

(a) Buyer will notify VBSE at least 5 working days in advance of any operational or business changes that may impact the Service (e.g. maintenance, upgrades, penetration testing). If the planned change is expected to be temporary, Buyer will provide the following information:

(i) Anticipated Start Date / Time of Change Window;

(ii) Anticipated End Date / Time of Change Window;

(iii) Nature of the Change and likely impact on the Service; and

(iv) Point of Contact.

(b) Buyer will notify VBSE to confirm that the planned change has been completed or if the Change Window has been extended. Any affected components and/or functionality will not be subject to Service Levels during the Buyer Change.

(c) Any change requests must be made using the methods shown in paragraph 5 of the Service Terms above.

Annex 2:

SERVICE LEVELS

1. GENERAL SUPPORT SERVICES TERMS

1.1 Supplier will provide Buyer with Support Service for the Service Elements ordered by Buyer.

1.2 Support Service is available in English only.

1.3 Support Service is available as shown below:

Support Service	Service Cover Period
Service Incident Management for Severity Level 1 & 2 Service Incidents	24/7
Service Incident Management for Severity Level 3 & 4 Service Incidents	Working Hours
Service Request Fulfilment	Working Hours

1.4 Service Incidents may be reported at any time during the Service Cover Period, however, Service Incident resolution will only occur during Working Hours for Severity Level 3 and 4 Service Incidents.

1.5 The Buyer must appoint primary and secondary central points of contact responsible for accessing the Support Service and communicating with Supplier during the relevant Service Cover Period. Buyer will inform Supplier, and keep Supplier up-to-date with the appointed individuals' identity and level of access.

1.6 Buyer will:

(a) reimburse Supplier for reasonable expenses associated with actions taken when Buyer has reported a Service Incident caused by an Excluded Event; and

(b) permit Supplier to interrupt the Service to resolve a Severity Level 1 or 2 Service Incident (and if no permission is granted then the relevant Service Incident will be downgraded to a Severity Level 3 Service Incident).

1.7 Supplier may temporarily interrupt the Service to carry out Planned Works. Supplier will endeavour to notify Buyer in advance of any Planned Works.

1.8 **Service Incident Commencement and Resolution Rules:**

(a) A Service Incident:

(i) commences when Supplier creates a Service Incident report (being no later than 60 minutes after the Service Incident has been reported to Supplier); and

(ii) ends on the earlier of when Supplier advises Buyer of Service Incident resolution or when the Service Incident affecting the Service has ceased.

(b) At Supplier's discretion or at Buyer's reasonable request, Supplier may continue to investigate using Supplier's internal problem management procedures, however, this shall not affect the resolved status of the Service Incident. Buyer is deemed to have been advised of Service Incident resolution if Supplier has made reasonable attempts to contact Buyer and Buyer has not notified Supplier within 24 hours from Supplier's last attempt to contact the Buyer that the Service Incident resolution is unsuccessful. Supplier's method of Service Incident resolution is at Supplier sole discretion.

2. AVAILABILITY SERVICE LEVEL

2.1 **Calculation:**

(a) Service Availability is expressed as a percentage ("P"), and calculated as: P= ((A-B))/A x 100, where:

(i) "A" equals the number of minutes in the Quarterly Measurement Period; and

(ii) "B" equals the number of whole minutes when the relevant Buyer Solution or Service Element is unavailable in the Quarterly Measurement Period.

2.2 **Availability Service Level**

(a) The Service Level for Service Availability of the Solution ("**Availability Service Level**") is 99.7%.

(b) The Availability Target excludes scheduled outages for maintenance, configuration changes that require re-boot and changes that have been approved in accordance with paragraph 5 of the Service Terms. Availability calculations exclude any interruption to service due to fault in, or any other problem associated with, customer-supplied WAN, electricity, hardware, software, non-maintained structured cabling or other network or systems not provided by Supplier;

Cyber Enhanced Vulnerability Scanning
Service Terms
3. SEVERITY OF INCIDENTS

3.1 The following Severity Levels apply to the Service:

Severity Level	Severity Level definitions
1 - Critical	A total loss of the Service. E.g. The Supplier SOC is unable to process or receive Security Event Logs.
2 - Significant	Partial loss of the Service which has a significant detrimental effect on Supplier's ability to perform normal operations but which does not represent a total loss of the service. Eg. SIEM persistently fails to connect to a Software Agent or does not receive Security Events from a Software Agent within the expected period.
3 - Minor	Degradation of service, such as loss of resilience, including a Severity Level 1 or 2 Service Incident where Supplier has been denied access to the Buyer Site or Equipment or where Supplier has been unable to agree a period of maintenance activity (for reasons outside Supplier's reasonable control) to restore normal service.
4 - No service impact	Any Service Incident not classified as severity level 1, 2 or 3 Service Incident.

4. RESTORATION TIMES SERVICE LEVEL

4.1 The target time to resolve a Service Incident (the "**Target Time to Restore**") is dependent on the Severity Level of the Service Incident as set out in paragraph 3.1 of Annex 2 to these Service Terms.

4.2 The elapsed time from the point at which Supplier raises a Trouble Ticket for the Service Incident to the point at which Supplier declares that, in Supplier's reasonable opinion, the Service or relevant Service Element has been restored, shall be known as the "**Actual Time to Restore**".

4.3 The Target Time to Restore for each Severity Level is as follows:

Severity Level	Target Time to Restore
1	4 Hours
2	8 Hours
3	24 Hours
4	72 Hours

5. Vulnerability Scanning Service report delivery

5.1 Vulnerability Scanning reports will be provided to the Buyer and remote review meeting scheduled within a week of the month following the agreed final date to which the report relates.

6. Service Credits

6.1 **General Service Credit Terms**

(a) Service Levels and Service Credit terms for the Buyer Solution or applicable Service Element commence on the Service Level Commencement Date.

(b) Service Credits are calculated as follows:

(i) Service Credits for Service Incident Resolution are calculated and reported monthly;

(ii) Service Credits for Availability are calculated and reported quarterly;

(iii) Service Credits are expressed as a percentage of the monthly recurring charge ("MRC") for the Buyer Solution.

(c) Service Credits do not apply for any failure or delay in performing the Service that arises out of, or in connection with, an Excluded Event.

(d) Where the failure to meet a Service Level impacts another Supplier service, the Buyer shall be entitled only to Service Credits relating to the primary service.

(e) If one Service Incident causes a failure of two or more Service Levels, only the greater Service Credit amount of the two (or more) Service Levels shall be payable.

(f) Service Credits as set out in this Annex 2 shall be the Buyer's sole and exclusive remedy against Supplier in respect of any failure in Service performance. Service Credits have been calculated as, and are, a genuine pre-estimate of the loss likely to be suffered by the Buyer for failure in Service performance. Service Credits may only be applied to Charges for the Service and have no cash value.

(g) Any Service Credits will be applied to your next bill after such Service Credits become due. All Service Credits will only be payable if:

(i) we proactively notify you that a Service Credit is payable; or

(ii) you notify your Supplier representative that you believe a Service Credit is payable, such notification to be made in writing within 30 calendar days of the date of the relevant service failure which you believe gives rise to a Service Credit. We will then investigate the claim for a Service Credit and confirm whether the Service Credit is payable.

(h) The following financial limits apply to Service Credits:

(i) in no event will Service Credits due for any accounting period exceed the associated recurring charge payable by the Buyer for that period; and

(ii) aggregate Service Credits (whether for breach of the Availability Service Level and/or the Restoration Times Service Level) in a measurement period will be capped at 40% of the aggregate MRC for the Solution.

6.2 **Service Credits for failure to meet the Availability Service Level**

Where the Service Availability in a Quarterly Measurement Period falls below the Availability Service Level, Buyer shall be entitled to a Service Credit. The Service Credit available is dependent on the value of 'X' in the table below, where X is a positive number expressed as a percentage figure and calculated as (X = percentage Availability Service Level minus percentage Actual Service Availability).

X (= % Availability Service Level minus % Service Availability)	Service Credit (% of MRC)	
	Non-Resilient Solution	Resilient Solution
X is between 0.01% and 0.99% inclusive	None	2.5%
X is between 1.00% and 1.99% inclusive	2.5%	5.0%
X is between 2.00% and 2.99% inclusive	5.0%	10.0%
X is equal to or greater than 3.0%	10%	20.0%

6.3 **Service Credits for failure to meet the Service Incident Resolution Target**

(a) The "Service Incident Resolution Target" is the percentage of Service Incidents, in each calendar month following the Service Commencement Date, which are resolved within the Target Time to Restore (i.e. where the Actual Time to Restore is equivalent to or less than the Target Time to Restore).

(b) Buyer is entitled to the following Service Credits where the Service Incident Resolution Target for Service Incidents of the relevant Severity Level is not achieved within a given calendar month.

(c) Buyer is entitled to Service Credits for failure to meet Service Incident Resolution Targets only in relation to resolution of Service Incidents relating to Equipment supplied and maintained by Supplier and used within the environment.

(d) The time taken by Buyer to resolve any Service Incident raised by Supplier will be excluded from the calculation of the Actual Time to Restore for the purposes of the Service Credit.

(e) Achievement of, or failure to achieve, the Service Incident Resolution Targets, is measured, reported and calculated each calendar month.

Severity level	Service Incident Resolution Target	Service Credit for failure to meet the Service Incident Resolution Target (% of monthly recurring charge)
1	100% of Service Incidents resolved within the Target Time to Restore	2.5.%

2	< 95% of Service Incidents resolved within the Target Time to Restore	2.5%
3	< 95% of Service Incidents resolved within the Target Time to Restore	2.5%
4	N/A	N/A