Service Specific Terms

Penetration Testing Service

Vodafone Business Customers

THE PARTIES AGREE:

1. Structure of contractual relationship

1.1 This Professional Services Agreement (this **"Agreement"**) incorporates the following terms and conditions:

1.1.1. The agreed statement of work (the **"SOW");**

1.1.2. The Professional Services General Terms, which can be found at www.vodafone.co.uk/terms, govern the relationship of the Parties in relation to any Service provided by Vodafone to the Customer under the SOW; and

1.1.3. The Vodafone Business Marketplace Service Specific Terms (the **"VBM Service Terms"**), which can be found at www.vodafone.co.uk/cloudservices/.

1.2 Precedence: In the event of any conflict between the provisions of (a) the SOW; (b) the VBM Service Terms; and (c) the Professional Services General Terms, this decreasing order of precedence shall apply.

2. Vodafone Business Marketplace (the "Marketplace")

2.1 The Service is made available to purchase through the Marketplace.

2.2 The Marketplace Service Specific Terms apply to the extent of the Customer's use of the Marketplace website.

2.3 The Customer accepts that certain features and functionality detailed in the Marketplace Service Terms may be limited or not apply to the Service, including but not limited to the applicability of Charges and Subscription periods.

Service Specific Terms

Penetration Testing Service

Vodafone Business Customers

STATEMENT OF WORK

STATEMENT OF WORK ("**SOW**"): **Vodafone Managed Security Services: Penetration Testing Service (the "Service")**

1. Project and Services – Penetration Testing Service (the "Service")

<table>
<tr>
<td>Service Summary</td>
<td>
The aim of the Service is to simulate a Cyber Attack on the Customer's Environment, in order to test the Customer's cyber defence capabilities and allow Vodafone to identify any vulnerabilities. The objective of the Service is not to list all vulnerabilities discovered in the Customer's Environment, but instead to gain unauthorized access to system features and data, escalate user privileges or compromise data integrity.

The findings of the Cyber Attack will be documented and prioritized, by level of risk, in the Penetration Test Report detailing any recommendations and Vodafone shall also remotely provide the 60-minute Explanatory Presentation.

There are three editions of the Service to meet different sized Customer Environments:

External Infrastructure Penetration Test (Black-Box Testing)
<table>
<tr><th>Edition</th><th>No. of Target IP Addresses</th></tr>
<tr><td>Small</td><td><25 IPs</td></tr>
<tr><td>Medium</td><td><100 IPs</td></tr>
<tr><td>Large</td><td>< 256 IPs</td></tr>
</table>
Internal Infrastructure Penetration Test (Black-Box Testing or Grey-Box Testing)
<table>
<tr><th>Edition</th><th>No. of Target IP Addresses</th></tr>
<tr><td>Small</td><td><50 IPs</td></tr>
<tr><td>Medium</td><td><256 IPs</td></tr>
<tr><td>Large</td><td>< 400 IPs</td></tr>
</table>
The Service shall comprise of the following deliverables:

Deliverable 1: Simulation of the Cyber Attack

Deliverable 2: Provision of the Penetration Test Report

Deliverable 3: Provision of the Explanatory Presentation
</td>
</tr>
</table>

Customer Prerequisites	**External Infrastructure Penetration Test** Where Customer selects an External Infrastructure Penetration Test edition of the Service, the Customer shall complete the External Infrastructure Penetration Test Questionnaire prior to the Service Commencement Date. No connectivity pre-requisites are required as testing is performed against Customer's external public facing Environment. **Internal Infrastructure Penetration Test** Where Customer selects an Internal Infrastructure Penetration Test edition of the Service, the Customer shall complete the Internal Infrastructure Penetration Test Questionnaire prior to the Service Commencement Date. The Internal Infrastructure Penetration Test requires remote network connectivity into the Customer's Environment. The Customer has the following two options available to provide Vodafone with the remote network connectivity: 1. the Customer must (a) deploy Vodafone's custom Kali Linux image on a Virtual Machine provided by the Customer; and (b) provide Vodafone with access to the Virtual Machine (e.g. via a client virtual private network (**"VPN"**), Citrix or any other remote access solution). The Customer's Virtual Machine must be deployed in an internal network so the access to all of the Target IP Addresses is not blocked by any network device. Hardware requirements for the Customer's Virtual Machine are as follows: 2x CPU, 4 GB RAM and 20 GB HDD space; or 2. Customer must provide Vodafone with a VPN which is terminated within the Customer's Environment and has access to all Target IP Addresses.
Service Methodology	Vodafone shall deliver the Service remotely from Prague, Czech Republic. Where Customers selects an External Infrastructure Penetration Test edition of the Service, the Black-Box Testing approach shall be used. Where Customer selects an Internal Infrastructure Penetration Test edition of the Service, by default, the Service shall be performed using the Black-Box Testing approach. However, Customer may choose for the Service to be performed using the Grey-Box approach, by confirming this in the Internal Infrastructure Penetration Test Questionnaire. Vodafone will perform the Service in accordance with the phases set out below in order to identify and exploit vulnerabilities that may impact confidentiality, integrity or availability of the Customer's Environment and data contained within it. Phases 1 to 3 below shall together constitute the Cyber Attack. **Phase 1: Reconnaissance:** Vodafone shall gather additional information on the Customer's Environment by: • performing cyber security scans on the Target IP Addresses; • identifying running services, open ports, technologies in use and understanding targeted network architecture and controls in place; and/or • using publicly available sources to identify additional information about the Customer's Environment. **Phase 2: Identify Vulnerabilities & Misconfigurations:** Vodafone shall attempt to identify vulnerabilities and misconfigurations within the Customer's Environment by deploying a range of manual and automated techniques. Vodafone shall also develop the attack vectors to be used for the Cyber Attack. **Phase 3: Exploit Vulnerabilities & Misconfigurations:** Vodafone shall exploit any vulnerabilities and misconfigurations found in the Customer's Environment by: • Attempting to gain access to the Customer's Environment; • identifying additional details and vulnerabilities about the relevant part of the Customer's Environment that has been compromised; • escalating privileges in order to obtain high-privileged user access to the Customer's Environment;

<table>
<tr>
<td></td>
<td>

obtaining and/or cracking passwords when found in hashed format;
identifying new targets in consultation with Customer (testing of which would not form a part of the scope of the Service); and/or
attempting to attack integrity of the Customer's Environment.

Vodafone shall not exploit any vulnerabilities or misconfigurations affecting the availability of the Customer's Environment, without having first obtained the Customer's agreement.
Phase 4: Reporting:
Following completion of the Cyber Attack, Vodafone shall prepare the Penetration Test Report, in accordance with the Customer Deliverables section below.
</td>
</tr>
<tr>
<td>Customer Deliverables</td>
<td>
The following deliverables shall be securely provided to Customer:
<table>
<tr><th>Deliverable</th><th>Description</th><th>Expected Timeframe (Business Days)</th></tr>
<tr><td>Execution of the Cyber Attack</td><td>Vodafone shall carry out the 3 Phases detailed in the Service Methodology section above.</td><td>Within the following Business Days from the Service Commencement Date:

Small edition – 3

Medium edition – 7

Large edition - 12</td></tr>
<tr><td>Provision of the Penetration Test Report</td><td>On completion of the Cyber Attack, Vodafone shall securely provide to the Customer the Penetration Test Report which may contain, without limitation, the following:

• an introductory section detailing the scope of the Service, the Target IP Addresses and any relevant limitations;
• an executive summary detailing the activities performed by Vodafone, any issues identified and any general recommended actions;
• a technical findings matrix detailing any identified risks and vulnerabilities, ranked in risk priority order, and any suggested remediation activities; and
• proof of concept evidences of identified and exploited vulnerabilities which may include, without limitation, escalated access to system or domain, cracked or found passwords and access to other sensitive information.

Vodafone will only capture, retrieve, or exfiltrate an amount of targeted data records reasonably necessary to demonstrate Vodafone's successful penetration of the customer systems. Vodafone may include proof of vulnerability screen captures of targeted data to evidence such exposure</td><td>Within 3 Business Days from completion of the execution of the Cyber Attack.</td></tr>
<tr><td>Provision of the Explanatory Presentation</td><td>Vodafone shall deliver the Explanatory Presentation remotely to Customer.</td><td>Within 3 Business Days of providing the Penetration Test Report.</td></tr>
</table>
Any targeted data that contains Personal Data will be redacted prior to its inclusion in the Penetration Test Report or Explanatory Presentation. The targeted data will either be returned or destroyed upon request by the Customer, except as retained in accordance with this Agreement.
</td>
</tr>
</table>

2. Project Terms

Customer Dependencies	In addition to any other responsibilities or assumptions described in this Agreement, the Customer Dependencies are as follows and the Customer recognises that if it fails to comply with the following dependencies, Vodafone is relieved from performing or delivering the Service and may choose to suspend or terminate this Agreement:
	
	• Customer shall perform and complete the responsibilities and assumptions set out in the Customer Prerequisites section prior to the Service Commencement Date;
	• the Customer will consent to and authorize Vodafone to access the Customer Property and perform the Service;
	• Customer is solely responsible for:
	  ○ defining the verified Target IP Addresses;
	  ○ any legal consequences that can occur from providing Target IP Addresses that the Customer is not authorized to perform the Service on;
	  ○ determining what third-party property, information, data or other assets is included within the Customer Property;
	  ○ determining whether any third-party consent, notices, permissions or licenses are required for Vodafone to perform the Service;
	  ○ obtaining any such consents, permissions or licenses or providing such notices (including from third-parties and Customer employees) necessary for Vodafone to perform its obligations under this Agreement;
	  ○ ensuring the availability of the Customer personnel and resources for the duration of the Service as necessary for the performance of the Service, or as otherwise agreed upon by Vodafone and Customer. Customer will commit the necessary resources and management involvement to support the Service. Customer acknowledges that material impacts to the Service including the schedule, scope and estimated or agreed upon costs may result from Customer resources being unavailable; and
	  ○ implementing a process to ensure that if Customer's information security team detects Vodafone's activities under the Service, such detection will be escalated to Customer's senior management, or such other knowledgeable Customer personnel, who can intervene prior to such activity being reported outside of Customer's organisation (e.g. to law enforcement) or, if such activity is reported outside of Customer's organisation, Customer will promptly clarify that Vodafone was acting with Customer's full knowledge and consent;
	• decisions to be made by the Customer will be made promptly and without delay;
	• Customer must provide necessary support for Vodafone obtaining any required visas and/or travel authorisations;
	• Customer will perform any remediation activities required to reinstate its systems and data after completion of the Service. Vodafone will have no liability for any losses arising out of Customer's failure to do so;
	• any other Customer responsibility that Vodafone and Customer mutually agree upon in writing;
	• Customer shall be responsible for delivering all communications internal to Customer regarding the Service, including communications intended to inform Customer staff about the Service, any impact it may have on Customer employees and personnel, and any training necessary to impacted Customer employees and personnel;
	• Customer must be aware of the risks associated with the Service and must have taken the necessary pre-testing steps (e.g. data backup, internal communications etc.) to help minimize these risks. These can include:
	  ○ careful selection of in-scope targets, for example, avoiding business critical systems in production environment, old/unstable systems, Operational Technology (OT) systems;
	  ○ communicate timelines and scope of activities with involved staff/departments, such as, a Security Operation Centre, network administrators, system owners; and

	○ ensure disaster recovery procedures are in place; • Customer shall use its commercially reasonable efforts to provide accurate and complete information, data and documentation in a timely manner, as required by Vodafone, and shall promptly notify Vodafone if it learns that any information, data or documentation previously provided to Vodafone is materially inaccurate or incomplete. • In the event of penetration testing that includes Customer cloud Infrastructure, the Customer will be responsible for getting the necessary approvals from the Cloud Service Provider and clarify the rules of engagement with Vodafone before the execution of the tests; • Customer acknowledges that Vodafone uses, among others, the following techniques, and that Customer does not object to this: ○ Technical operations, false signals, keys or identity to gain access to Customer's automated systems; ○ Techniques that may copy and store data encountered on Customer's automated systems; ○ A public telecommunication infrastructure or system to use computing capacity of Customer's automated systems; and ○ Techniques that may process or transfer the data encountered on Customer's automated systems, or append data to it; • Customer shall notify Vodafone directly if the Customer requires Vodafone to cease accessing the Customer's Environment. Vodafone shall cease accessing the Customer's Environment as soon as practicable upon receipt of such request; and • If Customer decides to remediate an exploited vulnerability that allowed Vodafone to gain an elevated level of access prior to the end of the engagement with Vodafone, Customer agrees to provide Vodafone with the same level of access obtained in a controlled secured manner so that Vodafone's testing can continue.
General Assumptions & Dependencies	The general assumptions & dependencies applicable for this Service are: • All work is carried out on a fixed fee basis. • There will be no changes to the scope of the Service, as set out in this Agreement. • The Service is not warranted to: • detect or identify all security or network threats to, or vulnerabilities of Customer's networks or other facilities, assets, or operations; • prevent intrusions into or any damage to Customer's networks or other facilities, assets, or operations; • return control of a Customer or third party system where unauthorized access or control has occurred; or • meet or help Customer meet any Applicable Law, industry standard or any other requirements including the Payment Card Industry Data Security Standard. It is Customer's sole responsibility to provide appropriate and adequate security for its company, its assets, systems and employees. • Customer must promptly notify Vodafone of any changes to information provided in either the External Infrastructure Penetration Test Questionnaire or the Internal Infrastructure Penetration Test Questionnaire (as relevant). • Vodafone may provide reasonable recommendations, advice or instructions on a particular course of action in the course of performing or as a result of the Service or in the Deliverables to be provided to Customer and if Customer chooses not to follow such reasonable recommendations, advice or instructions, Customer acknowledges that Vodafone shall not be responsible for any losses or claims made by the Customer that arise from Customer's failure to follow such recommendations, advice or instructions. • While Vodafone will use reasonable care to carry out the Service in line with Good Industry Practice and in a manner designed to mitigate and reduce the risk of damage to Customer Property, Customer acknowledges that there is inherent risk in the provision of the security Service in accordance with this Agreement which may lead to operational degradation, performance impact,

	breach of Customer policies or industry standards, or otherwise impair Customer Property (each a **"Customer Damage"** and together the **"Customer Damages"**) and, Vodafone will not be liable to the Customer or its respective employees or any third parties of the Customer for Customer Damages arising from the foregoing. To the extent possible, prior to commencing any provisioning of the Service, Vodafone shall identify and inform the Customer of any Customer Damage associated with the Service. • Customer agrees that Vodafone has the right to anonymise and aggregate Customer Data that will not in any way reveal the Customer Data as being attributable to the Customer with other data and leverage anonymous learnings and insights regarding use of the Service (the anonymised data, **"Vodafone Insights Data"**), and that Vodafone owns Vodafone Insights Data and may use Vodafone Insights Data during and after the term of this Agreement solely to develop, provide, and improve Vodafone products and services. • Customer agrees that Vodafone is not liable to Customer for Customer Damages provided that Vodafone will use reasonable care to carry out the Service in line with Good Industry Practice and in accordance with the terms of this Agreement. • The Customer agrees that, to the extent permitted by Applicable Law, it shall not bring any claim against Vodafone or any Group Company, whether in tort or otherwise, in connection with the Service or otherwise in relation to the subject matter of this Agreement. • Customer acknowledges that, in providing the Service, Vodafone will access Customer Systems and data. Customer agrees that, in advance of the Agreement Start Date, it shall provide and maintain all necessary consents, permissions, notices and authorisations as that are necessary for Vodafone to perform the Service, including any of the foregoing from employees or third parties; valid consents from or notices to applicable data subjects; and authorisations from regulatory authorities, employee representative bodies or other applicable third parties (**"Customer Consent"**) in a timely manner as necessary for Vodafone to access and use such System and data to perform the Service under this Agreement, and/or to use any third-party System(s) or data that Vodafone may use or require access to in performing the Service. For purposes of this Clause, **"System"** means, as applicable, Customer's or a third party's computer environment, network, equipment, software and related services. • Customer agrees to provide and maintain the Customer Consents. • Vodafone shall perform the Service in line with the scope of the Service as set out in this Agreement, in accordance with Good Industry Practice, and in reliance on, and in line with, the Customer Consent. • Customer agrees to indemnify Vodafone on an unlimited basis to the extent the Customer fails to provide and maintain the Customer Consents. • Vodafone is not responsible for remedying any security issues, vulnerabilities or other problems discovered in the course of performing or as a result of the Service (where such Service is provided in accordance with the terms of this Agreement). • In providing the Service, Vodafone has no intention of committing any civil or criminal offences. • Customer acknowledges and agrees that, no act or omission of Vodafone arising out of or related to Vodafone's provision of the Services will be deemed to exceed the authorisation as set out in this Agreement, provided that Vodafone has provided the Services in accordance with this Agreement and in line with the relevant agreed scope of services with the Customer and/or the applicable Order. • Customer must promptly notify Vodafone of any changes to Validation Information. • Customer agrees and authorises Vodafone, to retain any indicators of compromise, malware, anomalies, or other metadata found as part of, or related to the performance of the Service (**"Metadata"**) only for the purposes

	of gathering and compiling security event log data to look at trends, and real or potential security threats and improving Vodafone's security services. Vodafone may analyse, copy, store, and use such Metadata provided that such Metadata is compiled or combined in an aggregated, anonymised or pseudonymised, de-identified manner that will not in any way reveal the Metadata as being attributable to the Customer. • To the extent permitted by Applicable Law, the Customer agrees that it shall not bring any claim against Accenture or any Accenture Group Company (or any other third party acting on behalf of Vodafone in providing the Service), whether in tort or otherwise, in connection with the Service or otherwise in relation to the subject matter of this Agreement. • The Customer is responsible for: (i) ensuring that the Customers' use of the Service and associated Deliverables is in accordance with the terms of this Agreement; (ii) ensuring that the scope of the Service to be provided to the Customer meets the Customer's requirements; and (iii) Customer's compliance with all Applicable Laws and regulations applicable to Customer in connection with the use of the Service and/or Deliverables. • The Customer agrees to and authorises that Vodafone may, as necessary in performance of the Service: (i) access Customer Property and physically connect, disconnect, install, update, upgrade, manage and operate equipment, tools and software on Customer Property; and (ii) to the extent required to comply with Applicable Laws, take such actions with respect to Customer Property required by law enforcement authorities or regulatory authorities.
Materials and Software	• Vodafone may use certain third-party software products ("**Third-Party Software**") in its provision of the Service. The Customer agrees and acknowledges that Customer will not be provided access to these products. Any output directly from the Third-Party Software that is used by Vodafone in connection with the provision of the Service to the Customer without further input from Vodafone is being provided on an "as-is" basis and is excluded from any warranties set out in this Agreement. • Vodafone reserves the right to: (i) change the hosting provider used to host any proprietary or Third-Party Software used for the provision of the Service; and (ii) change any Third-Party Software it uses to provide the Service to Customer, provided that such changes do not materially impact the Service. • With regard to any Third-Party Software provided as part of the Service, the Customer agrees not to, directly or indirectly do any of the following: (i) reverse engineer, decompile, disassemble or otherwise attempt to discover the source code or underlying ideas or algorithms of the Third-Party Software; (ii) modify, translate, or create derivative works based on any element of the Third-Party Software or any related documentation; (iii) rent, lease, distribute, sell, resell, assign, or otherwise transfer its rights to use the Third-Party Software; (iv) use the Third-Party Software for any purpose other than the performance of the Service in accordance with this Agreement; (v) remove any proprietary notices from Third-Party Software or related materials furnished or made available to Customer; and/or (vi) permit any third party to access the Third-Party Software. • Vodafone may additionally utilize custom-developed software, scripts, exploits, and other technologies ("**Custom Products**") in its provision of the Service. Such technologies may be deployed on Customer systems during the provision of the Service. Any such technologies remain Vodafone intellectual property, and Vodafone retains all corresponding rights to these technologies. Vodafone shall not be obligated to provide Customer with copies of, access to, or a license for such technologies.

Acceptance Testing	There is no acceptance testing applicable to this SOW unless specifically mentioned in the "Project and Services" section.
Out of scope statement	The following are not in scope for the Service: • any Penetration Testing of applications; • any assessment of any systems outside of Customer's networks (with the exception of any such system that is: (i) within Customer facilities; and (ii) managed directly by Customer; and (iii) communicated with by Customer-owned assets; is considered in-scope for the purposes of the Penetration Testing Services). Vodafone and Customer further agree that any interaction with Customer's third-party cloud services providers will be done in a manner consistent with the Customer's normal interaction with those third-parties; • any remediation of identified vulnerabilities or other security issues; • any review and analysis of any data or equipment: (i) belonging to an individual outside of their employment with the Customer, without appropriate consent; or (ii) belonging to a third-party where Customer does not have control, custody and/or authorization to possess such data or equipment, or all necessary consents/authorization for Vodafone to access such data or equipment in order to perform the Service set out in this SoW; • any provision of services involving the collection of physical evidence, collection of evidence for admission in court including for criminal or civil litigation purposes, provision of evidence lockers, or 'chain of custody' collection of evidence; • any provision of expert testimony or litigation assistance or support services; • any provision of services involving retaliatory actions, hacking back or attribution that would breach applicable laws; • any installation of software, unless agreed by Vodafone and expressly consented to and authorized by Customer and Vodafone in writing, and which may require additional terms and conditions to be agreed; • any intentional interception of communications between Customer and a third-party, or between two or more third-parties, which is not authorized or directed by Customer as part of the Service. For the purposes of this paragraph, interception means intentionally modifying or interfering with Customer's systems or the operation of such systems, or intentionally monitoring transmissions made by means of Customer's system, such that some or all of the contents of the communications are made available to Vodafone while such contents are being transmitted. If unintentional interception does occur, Vodafone shall promptly after becoming aware inform Customer; • any provision of a regulated service. Vodafone is not licensed or certified in any country, state, or province as a public accountant, auditor, legal advisor, or private investigator, and is not being retained to provide any accounting services, accounting guidance, audit or internal control advisory services, tax or legal advice or investigatory services that would require a license; • any targeted investigation of any individuals. For the purposes of clarity, Vodafone may in the course of providing the Service, identify the internet profile (IP address, geographic location, potential aliases/usernames) of potential threat actor(s) or individual(s) involved in a perceived security threat, but the Service does not include any targeted investigation into such individual(s); • any incident response services/activities; and • at no point will Vodafone perform deliberate denial of service testing or excessive brute force attacks. The services detailed in this SOW shall be provided remotely and constitute Vodafone's complete scope of work and all other services (and the provision of services onsite) are out of scope.
Data Protection	1. Where Vodafone processes Personal Data, the relevant section of the clause headed "Data" of the Professional Services General Terms shall apply.

	2. Vodafone shall only act as Data Processor in respect of any Personal Data processed on behalf of Customer for the performance of the following deliverables: 1. Deliverable 1: Simulation of Cyber Attack; 2. Deliverable 2: provision of Penetration Test Report; 3. Deliverable 3: Explanatory Presentation, (the "**Processor Services**"). Where Customer shares Personal Data with Vodafone for the Processor Services, the Customer warrants and undertakes that it has complied with all necessary obligations imposed on it under Applicable Law including ensuring that it has either (i) obtained all necessary consents to transfer the Personal Data to Vodafone; or (ii) secured another lawful basis, in accordance with Applicable Privacy Law, to share such Personal Data with Vodafone for the processing envisaged by this Agreement and has provided appropriate privacy notices to the relevant data subjects (as required by Applicable Privacy Law) to enable it to share the Personal Data with Vodafone for the purposes envisaged by this Agreement
Payment Card Industry	Vodafone does not warrant that the Service will be payment card industry (**"PCI"**) requirements Compliant or that the Service will enable Customer to be compliant with Applicable Privacy Law.

3. Standard Information

Contractual Terms	The Professional Services General Terms govern the relationship of the Parties in respect of the Service provided by Vodafone to the Customer under this SOW.
Minimum Term	Commencing on the Agreement Start Date and ending when the final Deliverable is provided by Vodafone to Customer. There shall be no Renewal Term.
Agreement Start Date	The date of the Customer's acceptance of the terms of this Agreement.

4. Charges

Charges	The Charges shall be set out in the Order and shall be exclusive of VAT at the prevailing rate.
Invoice	Charges shall be invoiced upon completion of the Service.

Definitions

Penetration Testing Service

Vodafone Business Customers

The following definitions are applicable to the Service, and are in addition to the definitions detailed in the Professional Services General Terms:

Accenture	means Accenture (UK) Limited, a company incorporated in England with registration number 4757301, whose registered office is at 30 Fenchurch Street, London, EC3M 3BD.
Accenture Group Company	means Accenture or any entity, whether incorporated or not, that controls, is controlled by, or is under common control with Accenture.
Black-Box Testing	means the default penetration testing approach taken by Vodafone, where Vodafone only has limited information about the Customer's target IP addresses in-scope with no additional user access details regarding any Customer Property.
Customer Data	means all data, documents or records of whatever nature and in whatever form relating to the business of the Customer, the Customers' employees or otherwise, whether subsisting before or after the date of this Agreement and whether created or processed as part of, or in connection with, the Services.
Customer Property	means Endpoints, computer systems; servers; technology infrastructures; telecommunications or electronic communications systems and associated communications; confidential information; data (including Personal Data, employee identification, authentication or credential data user details and other sensitive information); assets; devices; intellectual property; and/or physical premises, that are used by Customer, or its respective employees, customers, or suppliers, whether owned or otherwise controlled by the Customer or owned by a third party.
Cyber Attack	means an attempt to expose, alter, disable, destroy, steal or gain information through unauthorized access to computer information systems, infrastructures, computer networks, or personal computer devices.
Environment	means network connected devices such as servers, workstations, printers, scanners, phones, routers, switches, hypervisors, wireless devices and others. Environment does not include software applications.
Explanatory Presentation	means the one-off sixty (60) minute presentation provided by Vodafone to Customer, explaining the findings of the Penetration Test Report, and as further detailed in the Customer Deliverables section above.
External Infrastructure Penetration Test	means non-authenticated penetration testing which is performed against public facing infrastructure.
External Infrastructure Penetration Test Questionnaire	means the questionnaire which Customer must complete where Customer has selected an External Infrastructure Penetration Test edition of the Service, prior to the Service Commencement Date, in order to enable Vodafone's provision of the Service. A copy of the External Infrastructure Penetration Test Questionnaire can be found at www.vodafone.co.uk/cloudservices/.
Good Industry Practice	means, in respect of any activity, performing that activity effectively, reliably and professionally in good faith and in a prompt and timely manner using the degree of skill, care, diligence, prudence, foresight and judgement which would reasonably be expected from a skilled, experienced and market leading operator engaged in the provision of the Service or such activity (as applicable) on a commercial basis.
Grey-Box Testing	means testing which is performed where the tester knows only a limited amount of information about the Customer's Environment.
Group Company	means an Vodafone Group Company or a company or corporation within Vodafone Group (as the case may be).
Internal Infrastructure Penetration Test	means penetration testing which is performed within the Customer's internal network and for which requires remote connectivity provided to Vodafone in order to perform.
Internal Infrastructure Penetration Test Questionnaire	means the questionnaire which Customer must complete where Customer has selected an Internal Infrastructure Penetration Test edition of the Service, prior to the Service Commencement Date, in order to enable Vodafone's provision of the Service. A copy of the Internal Infrastructure Penetration Test Questionnaire can be found at www.vodafone.co.uk/cloudservices/.
Marketplace	means the platform set out at https://marketplace.vodafone.co.uk/home.
Penetration Test Report	means the final report provided by Vodafone to Customer at the conclusion of the Service and as further detailed in the Customer Deliverables section above.
Service Commencement Date	the date as agreed between the parties for the Service to commence.
Target IP Addresses	means the Customer's IP addresses to be targeted by the Cyber Attack, and as confirmed by the Customer in either the Internal Infrastructure Penetration Test Questionnaire or the External Infrastructure Penetration Test Questionnaire.

Validation Information	means the information provided by Customer to Vodafone, prior to the Agreement Start Date, which was used by Vodafone to determine whether or not the Service could be provided to Customer. The Validation Information may include, but is not limited to, (i) the countries the Customer will receive the Service; (ii) the core business of the Customer; (iii) the systems Customer will be using the Service for; and (iv) whether the Customer has any existing conflicts with Vodafone.
Virtual Machine	means the virtualisation/emulation of a computer system which is based on computer architectures and provides functionality of a physical computer.
Vodafone	means (a) Vodafone Limited, a company incorporated in England with registration number 1471587, whose registered office is at Vodafone House, The Connection, Newbury, Berkshire, RG14 2FN, England; and/or (b) a third party acting on behalf of Vodafone, which includes Accenture.
Vodafone Group	means Vodafone Group plc and each body corporate, partnership, or unincorporated association, in respect of which Vodafone Group plc owns (directly or indirectly) at least 15 per cent. of: (a) the issued share capital; or (b) the ownership interests or units issued by such partnership or unincorporated association