Service Terms

Professional Security Services

Vodafone Business Customers

1. The Service - Overview

1.1 The Vodafone Professional Security Services service (the "**Professional Security Services**") provides technical and business consultants with practical technical and business experience to produce Deliverables specific to Customer's requirements. Within these Service Terms, the term '**Service**' means the Professional Security Services.

2. Service Term Structure

2.1 These Service Specific Terms include:

(a) the service specification which sets out a description of the Service, including optional Service Elements and complementary Services (where applicable) and may be updated from time to time (the "Service Specification"). The specific Service Elements selected by Customer will be set out in the Commercial Terms and/or Order;

2.2 The following documents further govern Vodafone's supply of the Service and form part of the Agreement, applying in the order of precedence set out in the General Terms:

(a) the Commercial Terms;

(b) the General Terms;

(c) the Fixed Service Terms;

(d) the Statement of Work or the Order, which confirms the Service Elements selected by/for Customer;

(e) the Service Specification;

(f) any other documents referenced as incorporated in these Service Terms; and

(g) any applicable policies and guidelines, as provided from time to time by Vodafone.

2.3 Notwithstanding any terms in any framework agreement between the Parties, if there are any conflicting terms in these Service Terms, the following order of precedence applies (highest level of precedence first): (a) the Commercial Terms; (b) the Service Terms; and (c) the General Terms or other framework agreement.

3. The Service

3.1 As part of the Professional Services, Customer may purchase the following optional Service Elements.:

(i) X-Force Application Penetration Testing

(ii) X-Force DevSecOps Assessment

(iii) X-Force Incident Response and Intelligence Service

(iv) Cloud Security Strategy Assessment Service

3.2 The term "Service" or "Services" in these Service Specific Terms includes each Service Element.

(a) The Service shall comprise of;

(i) Core Service Elements; and

(ii) Additional Optional Service Elements (where selected)

Both Core Service Elements and Optional Service Elements select by the Customer shall be set out in the Commercial Terms and/or Order. The Service Specification summarises the Core Service Elements that are included in the base Charges, and the Optional Service Elements available for an extra charge.

4. Service Specific Conditions of Use

4.1 **Third Party Providers**: Service Elements are provided by a Third Party Provider. Third Party Provider reserves the right to modify these Service Terms at any time by providing thirty (30) days' notice. Any further terms and conditions relevant to those Service Elements are set out in the Extra Service Terms.

C2 General

4.2 **On Premises Testing**: Customer is required to accept a Third Party Provider end user licence agreement(s) ("EULA") for on premises testing. Customer must agree to be bound by the terms and conditions set forth in following EULA(s) as they pertain to the security technology agent(s) included as part of the on-premises testing. The applicable EULA(s) are available for review at: http://www.ibm.com/services/iss/wwcontracts under the Third-Party End User Licence Agreements section for the applicable country.

4.3 **Systems Owned by Customer Third Party:** For systems (which for purposes of the provision of the Service includes but is not limited to applications, internet service providers, content-hosting firms and IP addresses) owned by a third party and that will be the subject of testing hereunder, Customer will: (a) prior to the commencement of the Service, have appropriate consents in place from all third party system owners; (b) be responsible for any risks to, or impact on, any third party systems which arise from Vodafone's performance of the Service;(c) be solely responsible for communicating any risks, exposures, and vulnerabilities identified on these systems by Vodafone's remote testing to the system owner or any other relevant third party; (d) arrange for and facilitate the exchange of information between the system owner and Vodafone as deemed necessary by Vodafone; (e) inform Vodafone as soon as possible whenever there is a change in ownership of any system that is the subject of the testing hereunder; and (f) not to disclose the Deliverables to a third party system owner unless to the extent relevant, to remediate the issues identified as part of the testing.

3.3.1 **Third Party Claims**: Customer agrees to reimburse Vodafone for all liabilities, costs, expenses, damages and losses incurred by Vodafone arising out of or in connection with any claim made against Vodafone by a third party arising out of or in connection with Customer's failure to obtain third party licences or approvals for Third Party Provider facilities, software, hardware or resource used in connection with provision of the Service. This provision is not subject to the liability cap in the General Terms.

4.4 **IP Addresses**: Customer acknowledges and agrees that it is Customer's responsibility to add the IP addresses associated with the testers (as provided by Vodafone ahead of the Service Commencement Date) to any filtering devices, thereby permitting unfiltered network access to the target systems and Customer agrees not to modify the configurations of any in-scope systems and infrastructure devices during the period of testing.

4.5 **Designated Point of Contact**: prior to the commencement of the Services, Customer will authorise Vodafone designated point of contact to act on Customer's behalf in all matters regarding the Services.

4.6 **Permission to Perform Testing**: Customer authorises Vodafone to perform the Service as described herein and acknowledges that the Service constitutes authorised access to Customer's computer systems. Vodafone may disclose this grant of authority to a third party if Vodafone deem necessary to perform the Service.

4.7 Customer agrees and accepts that the Service entails certain risks. Customer acknowledges and agrees that the following may occur as a result of the service delivery: (a) generation of log messages may increase resulting in excessive log file disk space consumption; (b) temporary degradation of the performance and throughput of Customer's systems and associated routers and firewalls; (c) temporary changes to some data as a result of probing vulnerabilities; (d) Customer's computer systems may hang or crash, resulting in system failure or temporary system unavailability; (e) any third party service level agreement rights or remedies will be waived during any testing activity; (f) a scan may trigger alarms by intrusion detection systems; (g) traffic interception of the monitored network for the purpose of looking for events.

4.8 **Procedures:** Customer agrees that Vodafone may establish new procedures for Customer's use of the Services, including as Vodafone deems necessary, for the optimal performance of the Services.

4.9 **Disclaimer**: Customer acknowledges and agrees:

(i) that the Service is not warranted to operate uninterrupted or error free;

(ii) that Service is not fault tolerant and is not designed or intended for use in hazardous environments requiring fail-safe operation, including without limitation aircraft navigation, air traffic control systems, weapon systems, life support systems, nuclear facilities, or any other applications in which Service failure could lead to death, personal injury, or property damage;

(iii) that it is solely within Customer's discretion to use or not use any of the information provided pursuant to the Service;

(iv) that it is Customer's sole responsibility to provide appropriate and adequate security for Customer's organisation, its assets, systems and employees;

C2 General

(v) that new technology, configuration changes, software upgrades and routine maintenance, among other items, can create new and unknown security exposures. Moreover, computer "hackers" and other third parties continue to employ increasingly sophisticated techniques and tools, resulting in ever-growing challenges to individual computer system security. Vodafone's performance of the Services does not constitute any representation or warranty by Vodafone about the security of Customer's computer systems including, but not limited to, any representation that Customer's computer systems are safe from intrusions, viruses, or any other security exposures. Vodafone do not make any warranty, express or implied, or assume any legal liability or responsibility for the usefulness of any information provided as part of the Service.

5. X-Force Red Portal

5.1 When Customer has selected one of the X-Forces Services, Customer will be provided with access to the X-Force Red Portal (the "**Red Portal**"). Vodafone will provide Customer with a username, password, URL and appropriate permissions to access the Red Portal ("**User Details**"). Customer is responsible for: (a) the security of the User Details; (b) providing Vodafone with the identity of the authorised Users and keeping that information current; and (c) authorised Users' compliance with the terms of use. Vodafone accepts no liability for any unauthorised or improper use or disclosure of any User Details. Customer is liable for all acts and omissions conducted using the User Details.

6. Data Protection

6.1 Vodafone shall act as Data Controller save:

(a) in respect of any Customer Data processed by Vodafone on behalf of Customer;

(the "Processor Services").

6.2 Vodafone shall act as Data Processor in respect of the Processor Services. The remainder of this clause 6 shall apply only in respect of the Processor Services.

6.3 Customer shall ensure that it has all necessary authorisations and consents from individual data subjects, work councils and relevant authorities as required under Applicable Law in relation to that Processing before Vodafone commences the Processing.

6.4 Vodafone (and their subcontractors):

(a) may Process Customer Data for: (i) provision and monitoring of the Service; or (ii) any other purpose agreed between the parties subject to Customer's prior written consent. Additional instructions require prior written agreement and may be subject to Charges. Customer shall ensure that its instructions comply with Applicable Laws. As between the parties, the Customer is responsible for the lawfulness of its instructions to Vodafone concerning the Processing of Personal Data. Vodafone will not comply with Customer's instructions until Customer has modified or confirmed the lawfulness of the instruction, or the instruction has, in writing, been amended to make it lawful or possible for Vodafone to comply. The parties acknowledge and agree that Vodafone shall be entitled to a reasonable reimbursement of any proper costs, which Vodafone may incur in excess of those accounted for as part of the Services, Vodafone's standard compliance with Data Protection Legislation or what has already been accounted for in accordance with Customer's Service related instructions, such charges to be set forth in a quote and agreed in writing by the parties, or set forth in an applicable amendment agreement.

(b) may use Customer Data to create statistical data and information about service usage and devices that does not identify a User.

(c) may engage another processor (a "Sub-Processor") to carry out processing activities in the provision of the Services or to fulfil certain obligations of Vodafone under the Agreement. Vodafone shall inform the Customer of changes to Sub-Processors where Vodafone is required by Applicable Privacy Law by (i) providing at least ten (10) Working Days' prior notice, or (ii) listing the new or replacement Sub-Processor on https://www.vodafone.co.uk/terms-and-conditions/ at least ten (10) Working Days before Vodafone authorises and permits the new or replacement Sub-Processor access to Customer Data in order to give the Customer the opportunity to reasonably object to such changes. Vodafone will enter into a contract or other legal act with the Sub-Processor and will impose upon the Sub-Processor substantially the same legal

C2 General

obligations as under this clause to the extent required by Applicable Privacy Law and that the Sub-Processor is carrying out the relevant processing activities. Vodafone shall remain liable to the Customer for the performance of that Sub-Processor's obligations.

(d) may retain the Customer Data for as long as is required to deliver the Service and shall destroy or return (at Customer's option) Customer Data in its possession upon termination of the Agreement, save where Customer opts for Vodafone to retain Customer Data subject to a new hosting agreement.

(e) shall limit access to Customer Data to those necessary to meet Vodafone's obligations in relation to the Service and take reasonable steps to ensure that they: (i) are under an appropriate statutory obligation of confidentiality; (ii) are trained in Vodafone's policies relating to handling Customer Data; and (iii) do not process Customer Data except in accordance with the Customer's instructions unless required to do so by Applicable Law.

(f) shall (i) provide appropriate technical and organizational measures for a level of security appropriate to the risks that are presented by Processing; and (ii) comply with the security requirements contained in the Vodafone information security policies based on ISO 27001;

(g) shall (i) provide Customer with such information, assistance and co-operation as Customer may reasonably require to establish compliance with Applicable Privacy Law including any personal data breach notification; (ii) without undue delay, notify Customer of any unauthorised access to Customer Data of which Vodafone becomes aware, which results in loss, unauthorised disclosure or alteration to the Customer Data; and (iii) where required by Applicable Privacy Law and requested by the Customer (prior to the processing), provide the Customer reasonable assistance to carry out a privacy impact assessment of the Services and any prior consultation of the relevant supervisory authority.

6.5 **Audit:** Customer shall with respect to any right of audit, including inspections, which they may have under Applicable Privacy Law relating to data protection, agree to exercise such right as follows: (a) no more than once per annum following the Agreement Start Date, request to meet (on a mutually acceptable date) with one or more senior representatives of Vodafone's security and/or audit department to review Vodafone's security organization and the best practice and industry standards which Vodafone meets or to which it aspires, including, without limitation, ISO 27001 (or equivalent), provided that such audit shall relate to the Services only. If the Transfer Contract Clauses apply (the model contract clauses set out in the European Commission's Decision of 5 February 2010 on standard contractual clauses for the transfer of Personal Data to data-processors established in third countries, under the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data as may be amended or replaced by the European Commission from time to time), nothing in this clause 6.5 6.5amends or varies those standard clauses nor affects any data subject or supervisory authority's rights under those clauses; and (b) be responsible for reviewing the information made available by Vodafone and making an independent determination if the Services meet the Customer's requirements and legal obligations as well as its obligations under this clause.

6.6 **Transfer of Customer Data out of the EEA:** Vodafone may transfer Customer Data to countries outside the European Economic Area only to the extent that (i) Customer Data is transferred on terms substantially in accordance with the Transfer Contract Clauses for the transfer of Personal Data to processors established in third countries; (ii) that the transfer of Customer Data does not put any member of Customer Group in breach of its obligations under Applicable Privacy Law; or (iii) it is required to do so by Union or Member State law to which it is subject; in such a case, Vodafone shall inform the Customer of that legal requirement before processing, unless that law prohibits such information.

6.7 **Law enforcement authorities:** Vodafone: (i) may receive legally binding demands from a law enforcement authority for the disclosure of, or other assistance in respect of, Customer Data, or be required by Applicable Law to disclose Customer Data to persons other than Customer; (ii) will not be in breach of its obligation to Customer in complying with such obligations to the extent legally bound; (iii) may provide Customer's basic contact information to a law enforcement agency in an attempt to redirect the law enforcement agency to request that data directly from Customer and (iv) shall give Customer reasonable notice of the demand unless otherwise prohibited.

6.8 **Enquiries from Users:** Vodafone shall, where the Customer is required under Applicable Privacy Law to respond to enquiries or communications (including subject access requests) from Users and taking into account the nature of the processing (i) without undue delay (at Vodafone's discretion) redirect the data subject to make its request

C2 General

directly to the Customer or pass on to Customer any enquiries or communications (including subject access requests) that Vodafone receives from Users relating to their Customer Data or its Processing; and (ii) assist the Customer by appropriate technical and organizational measures, insofar as this is possible in the Customer's fulfilment of those obligations under Applicable Privacy Law.

6.9 **Independent Determination:** Customer is solely responsible for reviewing the information made available by Vodafone relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations as well as Customer's obligations under this Agreement. Customer confirms that the technical and organisational measures provide an appropriate level of protection for the Personal Data taking into account the risks associated with the Processing of Personal Data.

6.10 **Details of Data Processing:** Customer shall maintain a record of processing detailing the following: list of categories of Data Subjects, types of Personal Data (including any special or sensitive categories of Personal Data), security categories for all data being processed and the processing activities of Customer. Customer shall make the record of processing available to Vodafone without undue delay upon Vodafone's written request.

6.11 **Interpretation and Definitions:** in this clause 6, any reference to "Vodafone may" is deemed to constitute: (a) a specific acknowledgement and authorisation on the part of Customer as required by Applicable Privacy Law; and (b) permission for Vodafone's lawfully appointed sub-processors to do likewise (for whose acts and omissions Vodafone remains responsible).

7. Decommission or Turn-Down of Service

7.1 If the Service is terminated, Customer may request receipt of archived data by providing Vodafone with written notice within 90 days from the date of termination or expiry of the Initial Term (or Renewal Term, if applicable), whichever first occurs.

7.2 Vodafone will charge Customer for all time and materials, and shipping charges (if applicable) utilised to restore and make the archived data available via download from a secured server. In cases where the amount of archived data is too excessive to make available via download, data will be stored on encrypted media and shipped to a location specified by Customer.

7.3 If a request is not received within the 90-day period described above, all archived data will be permanently destroyed.

8. Delivery Services

8.1 Delivery Date: Save where specified in a Statement of Work or Order, dates for delivery of any Deliverables are reasonable estimates only and are not guaranteed.

8.2 Time shall not be of the essence for the performance of the Services.

8.3 Acceptance**:** Customer will be deemed to have accepted the Deliverables, unless Customer notifies Vodafone within 5 Working Days of receiving the Deliverables, if such Deliverables do not materially comply with the Statement of Work and provide sufficient supporting details. Upon receipt of notification, Vodafone will take reasonable action to rectify such non-compliance and re-submit the Deliverables in accordance with the Statement of Work.

9. Disposition of Agents

9.1 Where a physical security technology agent has been provided to Customer pursuant to a Service Request, then upon termination or expiry of the X-Force Services or upon completion of the relevant security test, Customer agrees: (a) to work with Vodafone regarding the return of the security technology agent(s); (b) to return all security technology agent(s) to a shipping location agreed with Vodafone; (c) to ensure the security technology agent(s) is returned in the same condition (excepting reasonable wear and tear) as delivered to Customer; and (d) to be responsible for reasonable and demonstrable costs incurred by Vodafone as a result of misuse or damage of the security technology agent(s).

9.2 If Customer does not return the security technology agent(s) within a reasonable time after termination of the Service, Vodafone shall notify the Customer. If Customer fails to return the security technology agent(s) within

C2 General

twenty-five (25) days from the date of notification to Customer, then Customer shall pay Vodafone for their reasonable and demonstrable residual value as invoiced by Vodafone.

10. X-Force Application Testing

10.1 **Service Summary:** X-Force Application Penetration Testing provides a human tester who will manually discover and exploit vulnerabilities in an application to simulate a real-world attack. Testing is performed against both authenticated and public areas of the target.

10.2 **Penetration Levels**: Customer will purchase the X-Force Application Penetration Testing under one of the levels below as set out in the Customer Agreement or Order:

(a) **Entry-level penetration tests** require up to 10 days of testing. Customer is provided a report documenting the application's overall security posture and all test findings. Each finding will include an explanation of risk and recommendations. Entry-level penetration tests focus on high-priority application components and simpler vulnerabilities. For example, authentication and session tracking mechanisms, interfaces that handle sensitive data, and workflows that could allow fraud.

(b) **Standard-level penetration tests** require up to 18 days of testing. Customer is provided a report documenting the application's overall security posture and all test findings. Each finding will include an explanation of risk and recommendations. Standard-level tests also provide the testers with the time to use more complex techniques and look for more complex vulnerabilities. Examples include multi-step logic flaws, insecure file uploads, advanced injection flaws, and basic encryption flaws.

(c) **Advanced penetration tests** offer the highest level of dynamic application testing. All aspects of standard and entry-level tests are included. Testers will use more complex techniques such as reverse engineering of compiled files, dissection of custom binary protocols and objects, custom memory corruption exploits, and in-depth analysis of publicly available libraries and frameworks. Vulnerabilities typical of advanced penetration tests include serialization/marshalling flaws, padding oracle attacks, and improper block modes. Advanced penetration tests require up to 25 days of testing. Customer is provided a report documenting the application's overall security posture and all test findings. Each finding will include an explanation of risk and recommendations.

10.3 **Conditions of Use:** Customer will ensure that the in-scope systems and infrastructure remain in a static state throughout the testing period as configuration or infrastructure modifications made during the testing may cause inconsistencies in the results.

10.4 **Delivery:** Vodafone will facilitate a project initiation call for up to one (1) hour to review Customer's environment and organisation, including application platform, architecture, frameworks, supporting infrastructure, known security problems or concerns associated with the application, preliminary testing schedule and emergency contact plan. After testing is completed, Vodafone will conduct report briefing call for up to one (1) hour to explain the findings and associated risks. Customer has two (2) weeks or as otherwise agreed in the Service Request, after receiving the report to request a report briefing. Vodafone will consider this activity as completed on the expiry of the two (2) week period.

11. X-Force DevsSecOps Assessment

11.1 **Service Summary:** X-Force DevSecOps Assessment includes dynamic tool-based unvaldiated raw application scanning on internal and external web, mobile, terminal, Customer-server, mainframe and middleware platforms. Upon completion of the assessment, Vodafone will produce a vulnerability scan report.

11.2 **Conditions of Use**

(a) Customer agrees to install a testing device on Customer's network.

(b) Customer will ensure that the in-scope systems and infrastructure remain in a static state throughout the testing period as configuration or infrastructure modifications made during the testing may cause inconsistencies in the results.

C2 General

12. X-Force Incident Response and Intelligence Service

12.1 **Service Summary**: X-Force Incident Response and Intelligence Service ("**IRIS**") provide resources to assist Customer with computer security incidents or assist with emergency response preparation. Vodafone will provide resources to assist Customer in preparing for, managing and responding to computer security incidents, including steps for analysis, intelligence gathering, containment, eradication, recovery and prevention.

(a) The Service: The X-Force Incident Response and Intelligence Service includes a subscription for sixty (60) hours per annum of Project Initiation and Emergency Incident Support. Customer may also purchase the following optional service elements: (a) Incident Program Assessment; (b) Incident Response (IR) Playbook Customisation; (c) IR Tabletop Exercise and (d) Quarterly IR Related Support and Status Update.

12.2 **Project Initiation and Emergency Incident Support**

12.2.1 As part of the Project Initiation, Vodafone will review the processes for making declaration for a computer security incident that presents a real or a possible threat to Customer's computer system and network environment (the "Emergency Incident Declaration"), and to validate the schedule.

12.2.2 As part of the Emergency Incident Support, Vodafone will provide emergency response for each Emergency Incident Declaration, subject always to there being a limit on the amount of incidents that can be declared in any given time period. Customer is responsible for all reasonable and demonstrable charges of Vodafone associated with any additional Emergency Incident Declarations Customer makes during the term of the Service Request.

12.2.3 Vodafone will prepare an analysis (the "Incident Analysis Report") describing the computer security incident, causes and effects, actions taken by Vodafone, and recommended future actions to mitigate risk.

12.3 **Conditions of Use**: (a) Customer may not make an Emergency Incident Declaration until after the project kick-off session has been conducted; (b) Customer's additional locations, or locations not specified in the Service Request, must be contracted for separately; (c) one Vodafone consultant will be assigned for remote and/or on-site Emergency Incident Declaration response to the declared physical location. Additional consultants must be agreed in the Service Request; and (d) if Vodafone discovers what it considers, in its sole discretion acting reasonably, to be illegal content during the performance of Emergency Incident Support, Vodafone has the authority to report such information to law enforcement Authorities.

12.4 **Incident Program Assessment**: Upon completion of the Incident Program Assessment, Vodafone will provide a final presentation.

12.5 **IR Tabletop Exercise**: Upon completion of the IR Tabletop Exercise, Vodafone will deliver a report and discuss findings, for up to two (2) hours, via conference call with Customer's computer security incident response team.

12.6 **Quarterly IR Related Support and Status Update**: Vodafone will deliver a quarterly status update and report.

12.7 **Service Limitations**: Customer acknowledges and agrees that the following are not included in the X-Force Incident Response and Intelligence Service: (a) services involving incidents of violence, injury to persons, or damage to or theft of tangible personal property; (b) services to identify a perpetrator; however, determining the source of network traffic or specific digital activity may be included in IRIS; (c) investigatory interrogation; (d) testifying in judicial or administrative proceedings; (e) communication on Customer's behalf with any entity, such as law enforcement Authorities, the news media, or its customers; (f) any services requiring professional licensing of the service provider; (g) evidentiary chain of custody control or management, but Vodafone may adhere to Customer's chain of custody procedures if Vodafone has reviewed and agreed with them prior to starting work; (h) legal counsel of any kind; and (i) opinions as to the credibility of any person.

13. Cloud Security Strategy Assessment Service

13.1 **Service Summary:** Cloud Security Strategy Assessment Service ("**CSSA**") is designed to assist Customer with gaining visibility into Customer's current state of cloud security maturity and provide advice on required organisational, process, and technological transformations necessary to support the desire state of maturity.

C2 General

13.2 **Delivery:** CSSA comprises of a single assessment of one business unit/site only. Vodafone will deliver the CSSA with up to two (2) cloud security consultants. The cloud security consultants will provide up to fifty (50) days of remote support. Vodafone will deliver CSSA in the following four phases:

13.2.1 **Phase One - Project Initiation** includes finalisation of the project team members, development of a common understanding of the project scope, objectives, roles and responsibilities, and conducting preliminary data collection for analysis by Vodafone;

13.2.2 **Phase Two - Current State Assessment** includes identifying Customer's current IT security posture, catalogue Customer's enterprise cloud usage (if necessary) and finalise a Report;

13.2.3 **Phase Three - Target State Analysis** includes identifying Customer's current IT security posture, catalogue Customer's enterprise cloud usage (if necessary) and finalise a Report; and

13.2.4 **Phase Four - Recommendations** includes identifying Customer's current IT security posture, catalogue Customer's enterprise cloud usage (if necessary) and finalise a current state assessment report.

14. Completion

14.1 Completion of the Service shall take place upon the latter of the following: (a) expiry of the duration defined in the Order; and (b) delivery of the Deliverables to the Customer.

C2 General

Service Specification

Professional Security Services

Vodafone Business Customers

1. Introduction

1.1 The Vodafone Professional Security Services service (the "**Professional Security Services**") service provides technical and business consultants with practical technical and business experience to produce Deliverables specific to Customer's requirements.

2. Service Elements

The service offers four optional Service Elements as set out in Figure 1.

Figure 1.

Application Penetration Testing	This service is a suite of security testing solutions designed to meet an organisation's need to validate their environment for security vulnerabilities. The service is available in two forms: Application Penetration testing and Dev Sec Ops testing
DevSecOps Testing	
Incident Response and Intelligence Services	This is a subscription service that can be used to either pro-actively prepare for security incidents or seek recommendations on restoring service during a major security incident
Cloud Security Strategy Assessment	To assist the customer with gaining visibility into their current state of cloud security maturity and advise on required organisational, process, and technological transformations necessary to support the Customer's business initiatives and achieve the desired state of maturity

2.1 Application Penetration Testing is an attack and exploitation exercise designed to evaluate the effectiveness of a target's security controls. While tools may be used in the course of a penetration test, manual testing and exploitation are key components of the testing methodology offered in this service.

2.2 DevSecOps Testing is a dynamic tool-based, unvalidated raw application scanning service available on internal and external web, mobile, terminal, on-premises server, mainframe and middleware platforms. The targeted applications are scanned with an automated suite of tools to identify potential security vulnerabilities.

Figure 2. sets out the deliverables that can be derived from the above:

Output	Notes

C2 General

Application Penetration Test Report	Following testing will be conducted for the corresponding level of security testing Entry level: Mis-configured web servers, Proper network encryption (SSL / TLS), Single-step logic flaws, Basic injection vulnerabilities (basic SQL injection, cross-site scripting, etc.), Simple session management flaws, Authentication / authorisation functionality. Standard level: All vulnerabilities from Entry-Level Application Penetration Tests, Logic flaws in multi-step work flows, Insecure file uploads, Advanced versions of injection flaws (blind / timing-based SQL injection, OS command injection, XPath, etc.),Basic data encryption flaws (reused keys, encryption / decryption oracles, etc.) Advanced level: All vulnerabilities from Standard Application Penetration Tests, Serialisation / marshalling flaws, Advanced encryption attacks (padding oracle attacks, improper block modes, etc.)
Vulnerability Scan Report	A dynamic unvalidated raw vulnerability automated scanning of Customer identified targeted application(s) will be performed to identify common vulnerabilities (web server configuration flaws, insecure network communication, SQL injection, or cross-site scripting, etc.) the finding of which will be identified in a report (titled "**Vulnerability Scan Report**") that reflects the identified vulnerabilities.

2.3 Incident Response and Intelligence Services is a subscription service that provides access to highly skilled security consultants. These consultants conduct pre-emptive incident preparation, data preservation, in-depth data analysis and response and management functions in the event of an incident. The service is designed to provide a preventive and proactive approach to security for an organisation and facilitate greater visibility into threats to enable a more rapid remediation while supporting complex infrastructures and industry-specific operations. The service provides up to 60 hours per annum of support based on a minimum 12-month subscription period. It's main deliverables are:

(a) Project Initiation

(i) Facilitate an on-site or remote project initiation workshop, for up to one day
(ii) Introduce the IRIS management personnel that will be providing the service
(iii) Define the process for making an emergency incident declaration, including establishing the designated telephone number(s) and e-mail address(es);
(iv) Review processes for responding to an emergency incidents and for exchanging security incident data in a secure manner;

(b) Emergency Incident Support

Provide emergency response for emergency incidents and assistance and advice if possible for handling the emergency including:

(i) analysis of computer security incident data to determine the source of the incident, its cause, and its effects;
(ii) stopping the computer security incident at its source and/or protecting computer systems and networks from the effects of the computer security incident;
(iii) recommendations for restoration of the affected computer systems and networks to normal operation;
(iv) Prepare an analysis report describing the computer security incident, causes and effects, actions taken, and recommended future actions to mitigate risk.

Additional services can be purchased in addition to those listed above. These include;

(c) Incident Program Assessment

(i) Conduct a review of existing incident response ("IR") program documentation to deliver a one-year roadmap to support developing the maturity of the program by identifying milestones to serve as future goals.

(d) Incident Response (IR) Playbook Customisation

(i) Provide the business with a number of IR Playbook Customisations following a review that targets the top five highest priority incidents that could potentially occur.

(e) Incident Response Tabletop Exercise

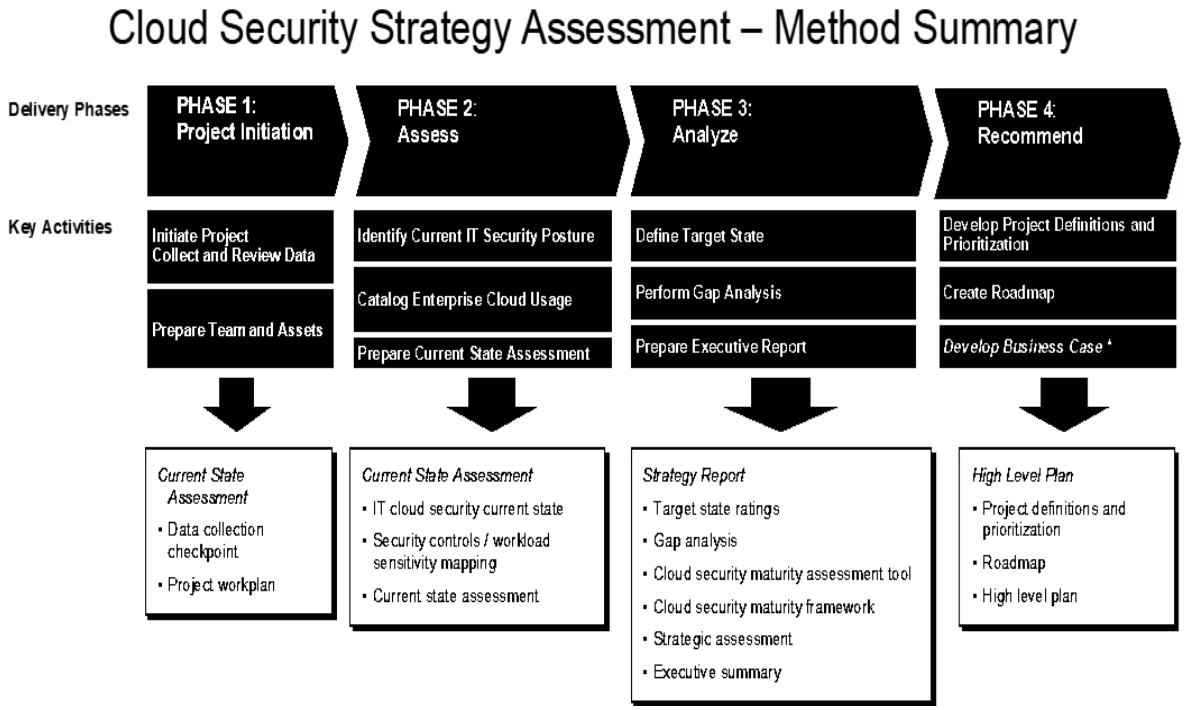
(i) Working with the customer's security team to conduct a simulated exercise to determine how their team will respond to a security incident.

(f) Quarterly IR Related Support and Status Update

(i) This provides a check-up to review quarterly status, relevant events, provide update on threat trends, ensure IR readiness, and provide recommendations if appropriate; supported with a written status report.

2.4 Cloud Security Strategy Assessment offers actionable results in four key phases: initiate, analyse, assess and recommend. Within each phase, Vodafone prioritizes cloud security scenarios for business- specific security requirements and helps improve security controls and mechanisms to support better management of regulatory and industry requirements.

Figure 3:



C2 General

Figure 4. sets out the deliverables for the Cloud Security Strategy Assessment.

Output	Description
Current state assessment	This document will set out the Customer's current IT security posture, catalogue Customer's enterprise cloud usage (if necessary)
Gap Analysis Findings	The document will define the target state of maturity and develop a gap analysis against the Current State Assessment.
Project Roadmap	The purpose of this activity is to develop a roadmap of recommendations given all of the analysis done in the previous phases.

© Vodafone Limited 2019

C2 General

Definitions

Professional Security Services

Vodafone Business Customers

The following definitions are applicable to the Services:

Authority	those governments, agencies, and professional and regulatory authorities that supervise, regulate, investigate, or enforce Applicable Law.
Commercial Agreement	an agreement for purchase of Services signed by both Parties.
Customer Data	means the Personal Data that is processed by Vodafone on behalf of Customer in connection with the Services.
Deliverables	any deliverable, process or document to be provided by Vodafone in accordance with the Extra Service Terms and as set out in the Statement of Work.
Extra Service Terms	the additional terms that apply to relevant optional Service Elements ordered by Customer
Quarterly Status Report	the document result of each telephone support and discussion of the check-up teleconference in a quarterly report.
Service Request	a formal communication from Customer for the provision of a Service change, information, advice or access to the Service.
Statement of Work	the document prepared for Customer by Vodafone providing details of the Service Element, if applicable
Third Party Resources	Third Party Provider facilities, software, hardware or other resource.
X-Force Services	means: (i) X-Force Application Penetration Testing (ii) X-Force DevSecOps Assessment (iii) X-Force Incident Response and Intelligence Service