G-Cloud 15

Penetration Testing

Service Offerings

Secure, Integrated Cloud Services

This document includes the following Service Descriptions:

- Internal Penetration Testing.
- External Penetration Testing.
- Web Application Testing.
- Web Service and API Penetration Testing.
- Vulnerability Scanning.
- Cloud Platform Build Review.
- Build Review.
- Mobile Application Penetration Testing Service.
- PCI ASV Scanning.
- Phishing - Penetration Testing Service.
- Scenario Testing.
- System Configuration Review.

Six Degrees

For more information

Tel – 0207 858 4935

Email – info@6dg.co.uk

www.6dg.co.uk

Secure, Integrated Cloud Services

1. Service Overview

Six Degrees provides an internal penetration test service to help you understand the level of risk that you are exposed to from an attacker placed within your internal network. This attacker could be a rogue employee, guest, or an intruder within the environment. An internal attack could also result from the compromise of a wireless network, or from an internet-based attacker who has breached external perimeter defences to gain access to the internal network. The assessment is designed to identify internal points of entry within your environment, identify areas of weakness and investigate each of these weaknesses to understand how vulnerabilities can be mitigated.

Additional information may be included in your Order Form or Terms of Reference (ToR).

2. Service Deliverables

The scope of testing specific to your environment will be documented in the ToR and agreed with you in writing before work commences.

We will provide the necessary resources and technical tools to perform the internal penetration testing according to your requirements as stated in your ToR.

If you require assistance with any prerequisite or supporting element, our offensive security team can provide additional pre-test support, including the provision of IP information, credentials, system configurations and other information using secure channels. Additionally, we can assist you to prepare for the Service and to meet the dependencies listed in Section 5. Such additional support will be delivered as part of a separate professional services engagement which will be subject to a separate Fee as indicated on your Order Form.

The Internal Penetration Testing process will be as follows:

(a) Port Scanning (Phase 1) - We will scan your target hosts via an automated scanner and will enumerate all available ports and services that are exposed to the internet. We will inspect these open ports and services to determine the purpose and the version details of any running software. We will assess whether the web server software is out of date, whether default or weak credentials can be used to authenticate to the site and whether the SSL/TLS configuration can be improved. Please note that this is not an exhaustive list of checks that we will perform as part of Phase 1, and the specific checks performed as part of your Service will ultimately depend on your environment.

(b) Vulnerability Scanning (Phase 2) - We will scan each open port and service via an automated scanner to identify potential vulnerabilities. We will analyse the open ports and services information obtained through the scanning to check whether they match any profile of known vulnerabilities. Probes designed to elicit responses which can indicate the presence or absence of relevant vulnerabilities are sent to the target hosts and their open services.

We will exploit the vulnerabilities identified during the scanning and testing process to rule out false positives. Where multiple vulnerabilities are identified, we will exploit them in conjunction to build an attack chain.

(c) Penetration Testing (Phase 3) - We will probe each open port and service manually to rule out any false positives and put together a potential attack tree. We will prioritise any vulnerability identified during the vulnerability scanning and we will manually examine the ports and services to identify other potential vulnerabilities.

(d) Segregation Testing (Phase 4) - We will ensure that a destination network (A) which should be segregated from a source network (B), is in fact segregated and that a host in network (B) cannot access services which are in network (A). This phase is essentially a repeat of Phase 1, but our testers will be connected to each source network in turn and given a specific set of destinations to target from each source network.

The report will include:

(a) Categorisation of each vulnerability;

(b) Threat exposure;

(c) Root cause of the issue;

(d) Testing technique used to find/reproduce the issue;

(e) Remediation advice;

(f) Severity ratings.

We will perform the test service using one or more of the following tools (as we determine to be the most appropriate):

(a) Port scanners (e.g. nmap);

(b) Vulnerability scanners (e.g. Nessus);

(c) SSL/TLS scanner (testssl.sh);

(d) Text-based SSL/TLS clients (e.g. openssl);

(e) Text-based network socket clients (e.g. netcat);

(f) Service clients (e.g. telnet, ftp); and/or

(g) Exploit code and exploitation frameworks selected based on your environment (e.g. Metasploit).

The choice of tools will vary according to your requirements and your host environment. If we agree with you to use specific tools not listed in this Section 2, we will include details of such tools in your ToR.

3. Service Delivery

After order acceptance, we will deliver the Service as follows:

Service Delivery	Us	You
We will discuss with you the Service and your environment to ensure accurate scoping for the penetration test.	•	•
You will provide us details of any required limitation around the scope of the penetration test.		•
You will provide us all the information necessary to conduct the penetration test.		•
You will approve and sign-off the project.		•
We will provide you with a ToR confirming the scope and the schedule of the penetration test prior to commencement.	•	
You will accept and sign the ToR.		•

All service delivery work will be carried out during Business Hours. We will invoice additional charges for any work undertaken out of hours. We reserve the right to charge additional fees for any change in your requirements occurring after completion of the activities listed in the table above and outside the scope of the contract (as described in the MSA).

3.1 Ready for Service

The Ready for Service Date for this Service is the date on which we agree and sign an Order Form with you, unless otherwise specified in your ToR.

(a) Test Date

You can request to postpone the test up to eleven (11) Business Days before the agreed test date indicated in your ToR, in which event we will reschedule the test and agree a new date with you for no additional charge. Please note that this will not change your Ready for Service Date.

In the event that you are not ready for the test on the agreed date, and you fail to submit a request to postpone the test date with at least eleven (11) Business Days' prior notice, you will be able to cancel the test subject to a cancellation fee calculated as follows:

(i) A charge equal to 50% of the Non-Recurring Fee if you submit a cancellation request between eleven (11) and six (6) Business Days before the agreed test date; or

(ii) A charge equal to 100% of the Non-Recurring Fee if you submit a cancellation request less than (6) Business Days before the agreed test date.

For the avoidance of doubt, any test that you wish to reschedule after cancellation shall be deemed a new order subject to a separate Fee.

4. Billing

The Service will be billed as a professional service Non-Recurring Fee on or shortly after signature of the Order Form, as described in the Billing Guide.

4.1 Additional Charges

We reserve the right to charge additional Fees in the following situations:

(a) Any work carried out outside Business Hours; and

(b) Any change in your requirements occurring after completion of the Service Delivery activities listed in Section 3 and outside the scope of the contract (as described in the MSA).

5. Dependencies

We will provide the Internal Penetration Testing Service subject to the following dependencies:

5.1 Client Obligations

(a) You will provide us details of your target hosts and any required information around scope (e.g. list of IPs or ports on which we will be performing the testing);

(b) You will provide us your source IP address, network mask, gateway and any relevant VLAN details for the network segments from which the tests should be conducted from; and

(c) You will ensure that the source IP addresses you provide us are applied to any firewall, router/switch access controls list or other whitelists as required to facilitate access to the target subnets.

5.2 Prerequisites

(a) You will provide written approval and sign-off the project before we commence any work pursuant to this Service Description.

5.3 Dependencies

(a) If Web Applications are present, you will provide us the relevant host name to allow access;

(b) If applicable, you will provide us details and/or firewall rules set to allow bypass of any intrusion prevention or other network filtering systems; and

(c) To allow the performance of segregation testing, you will provide us a list of source networks which the tester will be placed in, and a list of destination networks or hosts which the tester should target from each source network.

6. Exclusions

Please note that verification of vulnerabilities is not always possible, and we will not attempt exploitation where this would pose any undue risk to the availability or integrity of your production systems and/or data.

The excluded items described below are outside the scope of this Service Description:

(a) Performance of additional tests outside the agreed scope and schedule, unless otherwise specified in your ToR;

(b) Completion of any remediation actions;

(c) Creation of risk treatment plans;

(d) Denial of service;

(e) Data deletion;

(f) Data alteration;

(g) Power cycling of the host;

(h) Any activity that would compromise the BAU use of the host; and

(i) Full Web Application assessment.

7. Definitions and Acronyms

7.1 Definitions

In this document “we” or “us” refers to the Supplier, and “you” refers to the Client.

The terms listed have the following meanings:

Term	Meaning
Terms of Reference	A document which specifically sets out the detail of the testing engagement, how and when we will carry out that test and any dependencies or requirements needed for us to perform that activity.
Web Application	A piece of computer software which allows users to interact with servers on the internet or other network (e.g. a corporate internal network) using a web browser.

7.2 Acronyms

Acronym	Meaning
BAU	Business as Usual
DoS	Denial of Service
IP	Internet Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security protocol
ToR	Terms of Reference

8. Operational Targets

N/A

1. Service Overview

The External Penetration Testing service is designed to assess the level of risk that you are exposed to over the internet. The scope of the assessment is to identify external points of entry to your environment and areas of weakness, and to investigate each of these weaknesses to understand how vulnerabilities can be mitigated.

We will scan your target hosts to determine which ports and services within your environment are exposed to the internet. Each open port will then be scanned for potential vulnerabilities, such as outdated software, using an automated scanner. Once a list of potential security issues has been compiled, we will probe each port and service exposed to the internet manually to rule out any false positives and understand how an attack could potentially be carried out. We will then document each vulnerability identified within a report, which will include supporting evidence and recommendations on how the vulnerabilities could be mitigated.

Additional information may be included in your Order Form or Terms of Reference (ToR).

2. Service Deliverables

The scope of testing specific to your environment will be documented in the ToR and agreed with you in writing before work commences.

We will provide the necessary technical tools to perform the test in accordance with your requirements as stated in your ToR.

If you require assistance with any prerequisite or supporting element, our offensive security team can provide additional pre-test support, including the provision of IP information, credentials, system configurations and other information using secure channels. Additionally, we can assist you to prepare for the Service and to meet the dependencies listed in Section 5. Such additional support will be delivered as part of a separate professional services engagement which will be subject to a separate Fee as indicated on your Order Form.

The External Penetration Testing process is as follows:

(a) Port Scanning (Phase 1) – We will scan your target hosts via an automated scanner and will enumerate all available ports and services that are exposed to the internet. We will inspect these open ports and services to determine the purpose and the version details of any running software. We will assess whether the web server software is out of date, whether default or weak credentials can be used to authenticate to the site and whether the SSL/TLS configuration can be improved. Please note that this is not an exhaustive list of checks that we will perform as part of Phase 1, and the specific checks performed as part of your Service will ultimately depend on your environment.

(b) Vulnerability Scanning (Phase 2) – We will scan each open port and service via an automated scanner to identify potential vulnerabilities. We will analyse the open ports and services information obtained through the scanning to check whether they match

any profile of known vulnerabilities. Probes designed to elicit responses which can indicate the presence or absence of relevant vulnerabilities are sent to the target hosts and their open services.

We will exploit the vulnerabilities identified during the scanning and testing process to rule out false positives. Where multiple vulnerabilities are identified, we will exploit them in conjunction to build an attack chain.

(c) Penetration Testing (Phase 3) - We will probe each open port and service manually to rule out any false positives and put together a potential attack tree. We will prioritise any vulnerability identified during Phase 2 and we will manually examine the ports and services to identify other potential vulnerabilities.

We will determine the exploitability of each vulnerability identified during the penetration testing to provide you with an indication of what an attacker could achieve and help you to determine the extent of the risk to your organisation.

Please note that verification of vulnerabilities is not always possible, and we will not attempt exploitation where this would pose an undue risk to the availability or integrity of your production systems and/or data. In these cases, we will categorise the severity of vulnerabilities according to the information available to our offensive security team during the engagement and, therefore, there will be a higher chance of vulnerabilities being false positives.

The report will include:

(d) Categorisation of each vulnerability;

(e) Threat exposure;

(f) Root cause of the issue;

(g) Testing technique used to find/reproduce the issue;

(h) Remediation advice; and

(i) Severity ratings.

We will perform the test using one or more of the following tools (as we determine to be the most appropriate):

(a) Port scanners (e.g. nmap);

(b) Vulnerability scanners (e.g. Nessus);

(c) SSL/TLS scanner (testssl.sh);

(d) Text-based SSL/TLS clients (e.g. openssl);

(e) Text-based network socket clients (e.g. netcat);

(f) Service clients (e.g. telnet, ftp); and/or

(g) Exploit code and exploitation frameworks selected based on your environment (e.g. Metasploit).

The choice of tools will vary according to your requirements and your host environment. If we agree with you to use specific tools not listed in this Section 2, we will include details of such tools in your ToR.

3. Service Delivery

After order acceptance, we will deliver the Service as follows:

Service Delivery	Us	You
We will discuss with you the Service and your environment to ensure accurate scoping for the penetration test.	•	•
You will provide us details of any required limitation around the scope of the penetration test.		•
You will provide us all the information necessary to conduct the penetration test.		•
You will approve and sign-off the project.		•
We will provide you with a ToR confirming the scope and the schedule of the penetration test prior to commencement.	•	
You will accept and sign the ToR.		•

All service delivery work will be carried out during Business Hours. We will invoice additional charges for any work undertaken out of hours. We reserve the right to charge additional fees for any change in your requirements occurring after completion of the activities listed in the table above and outside the scope of the contract (as described in the MSA).

3.1 Ready for Service

The Ready for Service Date for this Service is the date on which we agree and sign an Order Form with you, unless otherwise specified in your ToR.

(a) Test Date

You can request to postpone the test up to eleven (11) Business Days before the agreed test date indicated in your ToR, in which event we will reschedule the test and agree a new date with you for no additional charge. Please note that this will not change your Ready for Service Date.

In the event that you are not ready for the test on the agreed date, and you fail to submit a request to postpone the test date with at least eleven (11) Business Days' prior notice, you will be able to cancel the test subject to a cancellation fee calculated as follows:

(i) A charge equal to 50% of the Non-Recurring Fee if you submit a cancellation request between eleven (11) and six (6) Business Days before the agreed test date; or

(ii) A charge equal to 100% of the Non-Recurring Fee if you submit a cancellation request less than (6) Business Days before the agreed test date.

For the avoidance of doubt, any test that you wish to reschedule after cancellation shall be deemed a new order subject to a separate Fee.

4. Billing

The Service will be billed as a professional service Non-Recurring Fee on or shortly after signature of the Order Form, as described in the Billing Guide.

4.1 Additional Charges

We reserve the right to charge additional Fees in the following situations:

(a) Any work carried out outside Business Hours; and

(b) Any change in your requirements occurring after completion of the Service Delivery activities listed in Section 3 and outside the scope of the contract (as described in the MSA).

5. Dependencies

We will provide the External Penetration Testing Service subject to the following dependencies:

5.1 Client Obligations

(a) You will provide us details of your target hosts and any required information around scope (e.g. list of IPs or ports on which we will be performing the testing);

(b) You will obtain authorisation to perform the test from network/hosting providers, or written confirmation that such authorisation is not required in the case of providers such as Microsoft Azure; and

(c) You will ensure that the source IP addresses you provide us are applied to any border firewalls or other whitelists as required.

5.2 Prerequisites

(a) You will provide written approval and sign-off the project before we commence any work pursuant to this Service Description.

5.3 Dependencies

(a) Before commencing the service, we will provide you with our source IP addresses and you will disable any DDoS protection or other network controls that could hinder testing for our source IP;

(b) If Web Applications are present, you will provide us the relevant host name to allow access; and

(c) If applicable, you will provide us details and/or firewall rules set to allow bypass of third-party DDoS/WAF protection.

6. Exclusions

Please note that verification of vulnerabilities is not always possible, and we will not attempt exploitation where this would pose any undue risk to the availability or integrity of your production systems and/or data.

The excluded items described below are outside the scope of this Service Description:

(a) Performance of additional tests outside the agreed scope and schedule, unless otherwise specified in your ToR;

(b) Completion of remediation actions;

(c) Creation of risk treatment plans;

(d) Denial of service;

(e) Testing that may affect the availability or integrity of production systems or data; and

(f) Full web application assessment.

7. Definitions and Acronyms

7.1 Definitions

In this document “we” or “us” refers to the Supplier, and “you” refers to the Client.

The terms listed have the following meanings:

Term	Meaning
Terms of Reference	A document which specifically sets out the detail of the testing engagement, how and when we will carry out that test and any dependencies or requirements needed for us to perform that activity.
Web Application	A piece of computer software which allows users to interact with servers on the internet or other network (e.g. a corporate internal network) using a web browser.

7.2 Acronyms

Acronym	Meaning
DDoS	Distributed Denial of Service
DoS	Denial of Service
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security protocol

ToR	Terms of Reference
WAF	Web Application Firewall

8. Operational Targets

N/A

1. Service Overview

The Web Application Testing is designed to assess the level of risk that you and your users are exposed to from an internet-based attacker who is using your Web Applications as well as system users or a rogue employee. the Service provides a security assessment of Web Applications based on OWASP principles and guidelines. This test focuses on the applications and their bespoke set of interactions with the web browser.

Additional information will be included in your Order Form or Terms of Reference (ToR).

2. Service Deliverables

If you require assistance with any prerequisite or supporting element, our offensive security team can provide additional pre-test support, including the provision of IP information, credentials, system configurations and other information using secure channels. Additionally, we can assist you to prepare for the Service and to meet the dependencies listed in Section 5. Such additional support will be delivered as part of a separate professional services engagement which will be subject to a separate Fee as indicated on your Order Form.

The Web Application Testing process is as follows:

(a) Application Mapping (Phase 1) – We will examine the applications in scope to determine the extent of the standard features and functionalities. One of our testers will map the applications as an unauthenticated user and as each user role. The objective of this Phase 1 is to gain an understanding of the application prior to the main testing.

(b) Security Testing (Phase 2) – We will perform bespoke testing on each page, form, workflows and all of their individual parameters mapped during Phase 1. Where applicable, we will conduct the test from all user roles, including unauthenticated. We will test the categories listed in the OWASP Mobile Application methodology:

(i) Information gathering;

(ii) Service configuration;

(iii) Cryptography (Transport);

(iv) Identity and authentication;

(v) Authorisation and session management;

(vi) Input validation;

(vii) Error handling;

(viii) Cryptography (Application);

(ix) Application and business logic; and

(x) Client-side controls.

The report will include:

(a) Categorisation of each vulnerability;

(b) Threat exposure;

(c) Root cause of the issue;

(d) Testing technique used to find/reproduce the issue;

(e) Remediation advice; and

(f) Severity ratings.

We will perform the Web Application Testing service using one or more of the following tools (as we determine to be the most appropriate):

(a) Web browser (Chromium/Firefox);

(b) Intercepting proxy (Burp);

(c) Web application vulnerability scanner (Burp and plugins);

(d) Vulnerability-specific scanner (sqlmap);

(e) SSL/TLS scanner (testssl.sh);

(f) Text-based SSL/TLS client (openssl);

(g) Text-based network socket client (netcat);

(h) File metadata extractor (exiftool);

(i) Web application framework scanner (wpscan); and/or

(j) Exploits and exploitation frameworks (selected based on your applications).

The choice of tools will vary according to your requirements and your host environment. If we agree with you to use specific tools not listed in this Section 2, we will include details of such tools in your ToR.

3. Service Delivery

After order acceptance, we will deliver the Service as follows:

Service Delivery	Us	You
We will discuss with you the Service and your environment to ensure accurate scoping for the penetration test.	•	•

You will provide us details of any required limitation around the scope of the penetration test.		•
You will provide us all the information necessary to conduct the penetration test.		•
You will approve and sign-off the project.		•
We will provide you with a ToR confirming the scope and the schedule of the penetration test prior to commencement.	•	
You will accept and sign the ToR.		•

All service delivery work will be carried out during Business Hours. We will invoice additional charges for any work undertaken out of hours. We reserve the right to charge additional fees for any change in your requirements occurring after completion of the activities listed in the table above and outside the scope of the contract (as described in the MSA).

3.1 Ready for Service

The Ready for Service Date for this Service is the date on which we agree and sign an Order Form with you, unless otherwise specified in your ToR.

(a) Test Date

You can request to postpone the test up to eleven (11) Business Days before the agreed test date indicated in your ToR, in which event we will reschedule the test and agree a new date with you for no additional charge.

In the event that you are not ready for the test on the agreed date, and you fail to submit a request to postpone the test date with at least eleven (11) Business Days' prior notice, you will be able to cancel the test subject to a cancellation fee calculated as follows:

(i) A charge equal to 50% of the Non-Recurring Fee if you submit a cancellation request between eleven (11) and six (6) Business Days before the agreed test date; or

(ii) A charge equal to 100% of the Non-Recurring Fee if you submit a cancellation request less than (6) Business Days before the agreed test date.

For the avoidance of doubt, any test that you wish to reschedule after cancellation shall be deemed a new order subject to a separate Fee.

4. Billing

The Service will be billed as a professional service Non-Recurring Fee on or shortly after signature of the Order Form, as described in the Billing Guide.

4.1 Additional Charges

We reserve the right to charge additional fees in the following situations:

(a) Any work carried out outside Business Hours; and

(b) Any change in your requirements occurring after completion of the Service Delivery activities listed in Section 3 and outside the scope of the contract (as described in the MSA).

5. Dependencies

We will provide the Web Application Testing subject to the following dependencies:

5.1 Client Obligations

(a) You will provide us details of target URL, full Web Service/API documentation and additional relevant details, including any required limitation around scope (e.g., specific endpoints/methods or HTTPS);

(b) You will provide us the credentials for all authorisation roles to be tested where authenticated testing applies, including documentation of the privileges assigned to and relationships between the authorisation roles where multiple user roles are being tested;

(c) You will obtain authorisation to perform the test from network/hosting providers, or written confirmation that such authorisation is not required in the case of providers such as Microsoft Azure; and

(d) You will ensure that the source IP addresses you provide us are applied to any border firewalls or other whitelists as required.

5.2 Prerequisites

(a) You will provide written approval and sign-off the project before we commence any work pursuant to this Service Description.

5.3 Dependencies

(a) Before commencing the testing, we will provide you with our source IP addresses and you will disable any relevant Web Application firewalls for our source IP;

(b) If applicable, you will provide us details and/or firewall rules set to allow bypass of third-party DDoS/WAF protection;

(c) If applicable, you will provide us details of any Web Application dependent client device and/or software; and

(d) Where multiple IP addresses are resolved from the URL hostname, we will focus the testing on one IP address.

6. Exclusions

Please note that verification of vulnerabilities is not always possible, and we will not attempt exploitation where this would pose any undue risk to the availability or integrity of production systems and/or data.

The excluded items described below are outside the scope of this Service Description:

(a) Performance of additional tests outside the agreed scope and schedule, unless otherwise specified in your ToR;

(b) Completion of any remediation actions;

(c) Creation of risk treatment plans;

(d) Denial of service;

(e) Testing that may affect the availability or integrity of production systems or data;

(f) External or internal network testing, multiple Web Services/API testing, Mobile Application testing, Web Application testing, and thick client application testing;

(g) Non-standard or unusual Web Services are excluded from the testing as we cannot ensure the correct functioning of usual testing tool on an API using a non-standard, unusual or proprietary protocol; and

(h) Other types of API testing (non-web services API).

7. Definitions and Acronyms

7.1 Definitions

In this document “we” or “us” refers to the Supplier, and “you” refers to the Client.

The terms listed have the following meanings:

Term	Meaning
Mobile Application	A piece of computer software which allows users to interact with servers on the internet or other network (e.g. corporate internal network) using a mobile device such as a phone or a tablet.
Terms of Reference	A document which specifically sets out the detail of the testing engagement, how and when we will carry out that test and any dependencies or requirements needed for us to perform that activity.
URL	Uniform Resource Locator; a web address.
Web Application	A piece of computer software which allows users to interact with servers on the internet or other network (e.g. a corporate internal network) using a web browser.
Web Service/API	An API provides the means by which different software components can talk to one another. A web service is a type of API which is exposed over a network such as the internet and uses web technologies such as web servers, HTTP and SSL/TLS to form the communications channel.

7.2 Acronyms

Acronym	Meaning
API	Application Program Interface

DDoS	Distributed Denial of Service
DoS	Denial of Service
HTTPS	Hypertext Transfer Protocol Secure
OWASP	Open Web Application Security Project
SSL	Secure Sockets Layer
TLS	Transport Layer Security protocol
ToR	Terms of Reference
URL	Uniform Resource Locator
WAF	Web Application Firewall

8. Operational Targets

N/A

1. Service Overview

The Web Service/API Testing Service which provides security assessment of a given web service or API based on OWASP principles and guidelines. This test focuses on the application bespoke set of functionalities of the Web Service/API.

Additional information will be included in your Order Form or Terms of Reference (ToR).

2. Service Deliverables

We will provide the necessary technical tools to perform the Web Service/API Testing according to your requirements as stated in your ToR.

If you require assistance with any prerequisite or supporting element, our offensive security team can provide additional pre-test support, including the provision of IP information, credentials, system configurations and other information using secure channels. Additionally, we can assist you to prepare for the Service and to meet the dependencies listed in Section 5. Such additional support will be delivered as part of a separate professional services engagement which will be subject to a separate Fee as indicated on your Order Form.

The Web Service/API Testing process is as follows:

(a) Web Service/API Workflow Mapping (Phase 1) – We will examine the Web Service/API to determine the extent of its standard features and functionality. One of our testers will map the Web Service/API as an unauthenticated user and as each user role. While doing so the tester will also take into consideration the application workflow (e.g. sequence of requests and responses that must be used to submit a valid subsequent request). The objective of this Phase 1 is to gain an understanding of the Web Service/API prior to the main testing.

(b) Security Testing (Phase 2) – We will perform bespoke testing on each request, method and workflow and all of their individual parameters mapped during Phase 1. Where applicable, we will conduct the test from all user roles, including unauthenticated, to attempt the access and/or subversion of requests, methods and workflows, in order to identify vulnerabilities. We will test the following categories:

(i) Broken object level authorisation;

(ii) Broken user authentication;

(iii) Excessive data exposure;

(iv) Lack of resources and rate limiting;

(v) Broken function level authorisation;

(vi) Mass assignment;

(vii) Security misconfiguration;

(viii) Injection;

(ix) Improper assets management; and/or

(x) Insufficient logging and monitoring.

The report will include:

(a) Categorisation of each vulnerability;

(b) Threat exposure;

(c) Root cause of the issue;

(d) Testing technique used to find/reproduce the issue;

(e) Remediation advice; and

(f) Severity ratings.

We will perform the Web Service/API Testing using one or more of the following tools (as we determine to be the most appropriate):

(a) Request repeater (Burp);

(b) API parser/request generator (Soap UI, OpenAPI Parser);

(c) Web service vulnerability scanner (Burp and plugins);

(d) Vulnerability-specific scanner (sqlmap);

(e) SL/TLS scanner (testssl.sh);

(f) Text-based SSL/TLS client (openssl);

(g) Text-based network socket client (netcat);

(h) File metadata extractor (exiftool);

(i) Exploits and exploitation frameworks (Web Service/API dependent); and/or

(j) Where appropriate, the web service/API dependent client (e.g. Web Application, Mobile Application, thick client).

The choice of tools will vary according to your requirements and your host environment. If we agree with you to use specific tools not listed in this Section 2, we will include details of such tools in your ToR.

3. Service Delivery

After order acceptance, we will deliver the Service as follows:

Service Delivery	Us	You
We will discuss with you the Service and your environment to ensure accurate scoping for the penetration test.	●	●
You will provide us details of any required limitation around the scope of the penetration test.		●
You will provide us all the information necessary to conduct the penetration test.		●
You will approve and sign-off the project.		●
We will provide you with a ToR confirming the scope and the schedule of the penetration test prior to commencement.	●	
You will accept and sign the ToR.		●

All service delivery work will be carried out during Business Hours. We will invoice additional charges for any work undertaken out of hours. We reserve the right to charge additional fees for any change in your requirements occurring after completion of the activities listed in the table above and outside the scope of the contract (as described in the MSA).

3.1 Ready for Service

The Ready for Service Date for this Service is the date on which we agree and sign an Order Form with you, unless otherwise specified in your ToR.

(a) Test Date

You can request to postpone the test up to eleven (11) Business Days before the agreed test date indicated in your ToR, in which event we will reschedule the test and agree a new date with you for no additional charge.

In the event that you are not ready for the test on the agreed date, and you fail to submit a request to postpone the test date with at least eleven (11) Business Days' prior notice, you will be able to cancel the test subject to a cancellation fee calculated as follows:

(i) A charge equal to 50% of the Non-Recurring Fee if you submit a cancellation request between eleven (11) and six (6) Business Days before the agreed test date; or

(ii) A charge equal to 100% of the Non-Recurring Fee if you submit a cancellation request less than (6) Business Days before the agreed test date.

For the avoidance of doubt, any test that you wish to reschedule after cancellation shall be deemed a new order subject to a separate Fee.

4. Billing

The Service will be billed as a professional service Non-Recurring Fee on or shortly after signature of the Order Form, as described in the Billing Guide.

4.1 Additional Charges

We reserve the right to charge additional fees in the following situations:

(a) Any work carried out outside Business Hours; and

(b) Any change in your requirements occurring after completion of the Service Delivery activities listed in Section 3 and outside the scope of the contract (as described in the MSA).

5. Dependencies

We will provide the Web Service/API Testing Service subject to the following dependencies:

5.1 Client Obligations

(a) You will provide us details of the target URL, full Web Service/API documentation and additional relevant details;

(b) You will provide us details of limitations around scope, including particular endpoints to which the testing should be limited, particular methods to be used or avoided, and details of whether the testing should only be carried out on HTTPS and not HTTP or any other consideration;

(c) You will provide us details of all IP addresses that are resolved from the URL hostname (our offensive security team will choose one IP and testing will be carried out against this);

(d) Where appropriate, you should provide us details and/or firewall rules set to allow bypass of third-party DDoS/WAF protection. Please note that DDoS simulation tests are not included in the scope of this service. However, we will perform the Web Service/API Testing to assess whether an attacker could bypass the mitigating controls that you have in place at your perimeter (e.g. DDoS prevention or WAF solutions) to provide remediation advice.;

(e) You will obtain authorisation to perform the test from network/hosting providers, or written confirmation that such authorisation is not required in the case of providers such as Microsoft Azure; and

(f) You will provide authorisation or, where appropriate, obtain authorisation from the Web Service/API owner to disable and/or amended as required the web application firewalls and security controls.

5.2 Please note that the accuracy of the report is dependent on you timely performance of the obligations listed in this Section 5.1. Failure to comply with your obligations may prevent us from completing some tests or result in the report including less information than we would have otherwise been able to provide. Prerequisites

(a) You will provide written approval and sign-off the project before we commence any work pursuant to this Service Description.

6. Exclusions

Please note that verification of vulnerabilities is not always possible, and we will not attempt exploitation where this would pose any undue risk to the availability or integrity of production systems and/or data.

The excluded items described below are outside the scope of this Service Description:

(a) Performance of additional tests outside the agreed scope and schedule, unless otherwise specified in your ToR;

(b) Completion of any remediation actions;

(c) Creation of risk treatment plans.

7. Definitions and Acronyms

7.1 Definitions

In this document “we” or “us” refers to the Supplier, and “you” refers to the Client.

The terms listed have the following meanings:

Term	Meaning
Mobile Application	A piece of computer software which allows users to interact with servers on the internet or other network (e.g. corporate internal network) using a mobile device such as a phone or a tablet.
Terms of Reference	A document which specifically sets out the detail of the testing engagement, how and when we will carry out that test and any dependencies or requirements needed for us to perform that activity.
URL	Uniform Resource Locator; a web address.
Web Application	A piece of computer software which allows users to interact with servers on the internet or other network (e.g. a corporate internal network) using a web browser.
Web Service/API	An API provides the means by which different software components can talk to one another. A web service is a type of API which is exposed over a network such as the internet and uses web technologies such as web servers, HTTP and SSL/TLS to form the communications channel.

7.2 Acronyms

Acronym	Meaning
API	Application Program Interface
DDoS	Distributed Denial of Service
DoS	Denial of Service
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
OWASP	Open Web Application Security Project

SSL	Secure Sockets Layer
TLS	Transport Layer Security protocol
ToR	Terms of Reference
URL	Uniform Resource Locator
WAF	Web Application Firewall

8. Operational Targets

N/A

1. Service Overview

This Service is designed to assess the vulnerabilities of your internet facing hosts via automated scanning and manual reviews from one of our certified penetration testers. We will conduct and run the Vulnerability Scanning through our certified tools such as Nessus. Our testers will review the results of the scanning to ensure false positives are removed. The Vulnerability Scanning process is entirely non-intrusive and does not include active exploitation.

This Service can be provided on an ongoing basis with tests scheduled either monthly or quarterly, or as an one-off test.

Additional information may be included in your Order Form or Terms of Reference (ToR).

2. Service Features

The Vulnerability Scanning is designed to complement our penetration testing services as in interim check point to provide a monthly insight into the state of security for a given set of hosts.

We will provide the necessary technical tools to perform the Vulnerability Scanning according to your requirements as stated in your ToR.

If you require assistance with any prerequisite or supporting element, our offensive security team can provide additional pre-test support, including the provision of IP information, credentials, system configurations and other information using secure channels. Additionally, we can assist you to prepare for the Service and to meet the dependencies listed in Section 5. Such additional support will be delivered as part of a separate professional services engagement which will be subject to a separate Fee as indicated on your Order Form.

We can configure the Vulnerability Scanning to run monthly or quarterly. The frequency of your scans will be defined in your ToR. The Vulnerability Scanning process is as follows:

(a) Pre-Engagement (Phase 1) – We will arrange a meeting with you and our testers to plan a timetable for monthly or quarterly Vulnerability Scanning activities, including active scanning times and delivery timescales for reports.

(b) Setup (Phase 2) – Upon the first scheduled scanning date, we will use the information gathered during Phase 1 to configure the scans and their target scope.

(c) Vulnerability Scanning (Phase 3) – We will perform the recurring scans in accordance with the agreed frequency and targeted hosts. We will monitor each scan and review their outputs. The review will be conducted by one of our qualified penetration testers holding either Crest, Tigerscheme, Cyberscheme, CHECK team member or CHECK leader accreditation. The results of this review will be used to prepare a report.

The report will include:

(a) The results of the vulnerability scan;

(b) Remediation advice; and

(c) Our tester's executive summary of the results.

The report will be provided monthly or quarterly, depending on the frequency agreed with you in your ToR.

If you need additional support to review the results of the Vulnerability Scanning, you can procure additional consultancy services to arrange monthly meetings with our offensive security team. Such engagement will be subject to a separate Fee as defined in your Order Form.

We will perform the test using one or more of the following tools (as we determine to be the most appropriate):

(a) Nessus;

(b) Other tolls specifically agreed with you.

The choice of tools will vary according to your requirements and your host environment. If we agree with you to use specific tools not listed in this Section 2, we will include details of such tools in your ToR.

3. Service Delivery

After order acceptance, we will deliver the Service as follows:

Service Delivery	Us	You
We will discuss with you the Service and your environment to ensure accurate scoping for the penetration test.	●	●
You will provide us details of any required limitation around the scope of the penetration test.		●
You will provide us all the information necessary to conduct the penetration test.		●
You will approve and sign-off the project.		●
We will provide you with a ToR confirming the scope and the schedule of the penetration test prior to commencement.	●	
You will accept and sign the ToR.		●

All service delivery work will be carried out during Business Hours. We will invoice additional charges for any work undertaken out of hours. We reserve the right to charge additional fees for any change in your requirements occurring after completion of the activities listed in the table above and outside the scope of the contract (as described in the MSA).

3.1 Ready for Service

4. The Ready for Service Date for this Service is the date on which we agree and sign an Order Form with you, unless otherwise specified in your ToR. Billing

The Service will be billed as a professional service Non-Recurring Fee on or shortly after signature of the Order Form, as described in the Billing Guide.

4.1 Additional Charges

Additional charges can only be incurred at the request of the client, there are options to services on an ad-hoc basis:

(a) Implementation work carried out outside Business Hours; and

(b) Any change in your requirements after completion of the Service Delivery activities listed in Section 3 and outside the scope of the contract (as described in the MSA).

5. Dependencies

We will provide the Vulnerability Scanning Service subject to the following dependencies:

5.1 Client Obligations

(a) You will provide us details of your target hosts and any additional information around the scope of the Service as we may reasonably require (e.g. list of IPs and associated Operating System on which we will be performing the scanning); and

(b) You will ensure that the source IP addresses you provide us are applied to any firewall, router/switch access controls list or other whitelists as required to facilitate access to the target subnets.

5.2 Prerequisites

(a) You will provide written approval and sign-off the project before we commence any work pursuant to this Service Description.

5.3 Dependencies

(a) Access and authentication as requested must be available for the review to be completed; and

(b) If applicable, you will provide us details and/or firewall rules set to allow bypass of any intrusion prevention or other network filtering systems.

6. Exclusions

The excluded items described below are outside the scope of this Service Description:

(a) Any ad-hoc scans performed after discovery of a critical severity vulnerability; and

(b) Any retesting following agreed test period unless specified in your ToR;

7. Definitions and Acronyms

7.1 Definitions

In this document “we” or “us” refers to the Supplier, and “you” refers to the Client.

The terms listed have the following meanings:

Term	Meaning
CHECK	CHECK is the term for the NCSC approved penetration test companies and the methodology used to conduct a penetration test.
Cyber Scheme	The Cyber Scheme is one of the organisations accredited by GCHQ/NCSC to offer examinations that meet UK Government Standards in penetration testing.
CREST	Internationally recognised certification body that provides the professional level examinations and certifications for our Cyber Security professionals.
Terms of Reference	A document which specifically sets out the detail of the testing engagement, how and when we will carry out that test and any dependencies or requirements needed for us to perform that activity.
Tigerscheme	Commercial certification scheme for technical security specialists.

7.2 Acronyms

Acronym	Meaning
CREST	Council for Registered Ethical Security Testers
NCSC	National Cyber Security Centre
ToR	Terms of Reference

1. Service Overview

The Cloud Platform Build Review is designed to review infrastructures hosted on public cloud platforms, such as AWS and Azure, or other SaaS cloud platforms. The review assesses the configuration of cloud environments against best practice benchmarks for security and our own best practice standards for producing secure, minimised risk hosted environments.

The Cloud Platform Build Review is conducted against an industry's CIS benchmarking standard of configuration where available (see https://www.cisecurity.org/cis-benchmarks/ for further details).

Additional information will be included in your Order Form and/or Terms of Reference ("ToR").

2. Service Deliverables

We will provide the necessary technical tools to perform the Service according to your requirements as stated in your ToR. Your scope of your Service and applicable Fees will be specified in your Order Form.

If you require assistance with any prerequisite or supporting element, our offensive security team can provide additional pre-test support, including the provision of IP information, credentials, system configurations and other information using secure channels. Additionally, we can assist you to prepare for the Service and to meet the dependencies listed in Section 5. Such additional support will be delivered as part of a separate professional services engagement which will be subject to a separate Fee as indicated on your Order Form.

2.1 Cloud Platform Build Review

The Cloud Platform Build Review assessment will determine how your cloud infrastructure has been configured to identify potential areas of weakness and misconfiguration. We will:

(a) Investigate identified areas of weakness;

(b) Report on vulnerabilities and mitigation options to provide feedback on your system configuration; and

(c) Indicate how you can reduce your attack surface and prevent malicious actors from gaining a foothold in your environment.

The Cloud Platform Build Review process will be as follows:

(a) Security Roles and Access Controls – A penetration tester will review the environment group policy settings to assess whether best practices are followed for the various roles and controls within your organisation. Our tester will also review access controls to confirm whether appropriately strong protective policies are in place and applied correctly.

(b) Identity and Access Management – We will review the environment identity and access management configuration to assess whether access to such configuration tools are appropriate, all users, power users and administrators are correctly configured, privileged accounts are correctly utilised, and systems cannot be accessed inappropriately.

(c) Data Collection and Storage – We will perform manual and automated review of storage facilities in the cloud environment. We will review controls and encryption levels relating to data storage to assess whether encryption is correctly applied with a sufficient strength and that data in transit and storage is handled securely in line with best practice guidelines.

(d) Security Policies and Recommendations – We will review templates used and policies set for the deployment and build of systems to assess whether best practice is followed and that new builds are secure. We will assess controls around build and deployment and make recommendations as appropriate.

(e) Security Monitoring – We will review cloud security monitoring tools that are available and/or configured to assess whether key security incidents are alerted upon. Where tools are not used, we may make recommendations on key tool utilisation and configuration.

(f) Platform Breach Detection Capabilities – Similarly to Security monitoring, where tools are available to detect breach and compromise, we will review these to assess whether they have been set up correctly and provide visibility to the most common breach types, as well as being able to detect more advanced threats. Where tools are not utilised or are poorly configured, we will make key recommendations in line with best practice.

(g) Token, Keys and Keypair Configuration – Where additional levels of authentication and access controls are leveraged by token(s), certificates, keys or keypairs, we will undertake a review of the methods in place to check whether they are susceptible to attack or compromise. Where key lengths or technical controls are insufficient, or not meeting best practise, we will highlight these and make recommendations to strengthen or replace such controls.

(h) Load Balancing Configuration – Where applicable, we will undertake a review of your environment load balancing configuration to assess whether best practice has been followed and that the configuration ensures equilibrium across devices. We will make recommendations as appropriate regarding how you can correct and optimise settings to prevent your system from being over utilised or susceptible to failure through overload.

(i) Application Resilience – We will review key applications to assess the availability of systems. Where high availability services are enabled, we review their configuration to assess whether it allows for smooth system failover in the event of an issue and where application resilience is not utilised. Where appropriate, we may make recommendations to improve your system availability.

The report will include:

(a) Categorisation of each vulnerability;

(b) Threat exposure;

(c) Root cause of the issue;

(d) Testing technique used to find/reproduce the issue;

(e) Remediation advice; and

(f) Severity ratings.

We will perform the build review service using one or more of the following tools (as we determine to be the most appropriate):

(a) Vulnerability scanner(s);

(b) Manual examination; and/or

(c) Custom written audit and examination scripts.

The choice of tools will vary according to your requirements and your host environment. If we agree with you to use specific tools not listed in this Section 2, we will include details of such tools in your ToR.

3. Service Delivery

After order acceptance, we will deliver the Service as follows:

Service Delivery	Us	You
We will discuss with you the Service and your environment to ensure accurate scoping for the Cloud Platform Build Review .	•	•
You will provide us details of any required limitation around the scope of the Cloud Platform Build Review.		•
You will provide us all the information necessary to conduct the Cloud Platform Build Review.		•
You will approve and sign-off the project.		•
We will provide you with a ToR confirming the scope and the schedule of the penetration test prior to commencement.	•	
You will accept and sign the ToR.		•

All service delivery work will be carried out during Business Hours. We will invoice additional charges for any work undertaken out of hours. We reserve the right to charge additional Fees for any change in your requirements occurring after the completion of the activities listed in the table above and outside the scope of the contract (as described in the MSA).

3.1 Ready for Service

The Ready for Service Date for this Service is the date on which we agree and sign an Order Form with you, unless otherwise specified in your ToR.

(a) Test Date

You can request to postpone the test up to eleven (11) Business Days before the agreed test date indicated in your ToR, in which event we will reschedule the test and agree a new date with you for no additional charge. Please note that this will not change your Ready for Service Date.

In the event that you are not ready for the test on the agreed date, and you fail to submit a request to postpone the test date with at least eleven (11) Business Days' prior notice, you will be able to cancel the test subject to a cancellation Fee calculated as follows:

(i) A charge equal to fifty percent (50%) of the Non-Recurring Fee if you submit a cancellation request between eleven (11) and six (6) Business Days before the agreed test date; or

(ii) A charge equal to one hundred percent (100%) of the Non-Recurring Fee if you submit a cancellation request less than (6) Business Days before the agreed test date.

For the avoidance of doubt, any test that you wish to reschedule after cancellation shall be deemed a new order subject to a separate Fee.

4. Billing

The Service will be billed as a professional service Non-Recurring Fee on or shortly after signature of the Order Form, as described in the Billing Guide.3.1

4.1 Additional Fees

We reserve the right to charge additional Fees in the following situations:

(a) Implementation work carried out outside Business Hours; and

(b) Any change in your requirements occurring after completion of the Service Delivery activities listed in Section **Error! Reference source not found.** and outside the scope o f the contract (as described in the MSA).

5. Dependencies

We will provide the Cloud Platform Build Review Service subject to the following dependencies:

5.1 Client Obligations

(a) You will provide us details of your target platforms and any required information around scope (*e.g*. list of URLs on which we will be performing the review);

(b) You will provide us a read only administrator and/or root level user accounts for the systems being reviewed;

(c) You will provide us your source IP address, network mask, gateway and any relevant VLAN details for the network segments from which the tests should be conducted from; and

(d) You will ensure that the source IP addresses you provide us are applied to any firewall, router/switch access controls list or other allow lists as required to facilitate access to the target subnets.

5.2 Prerequisites

(a) You will provide written approval and sign-off the project before we commence any work pursuant to this Service Description.

5.3 Dependencies

(a) We require access and authentication to be available as needed to enable us to perform the Cloud Platform Build Review; and

(b) If applicable, you will provide us details and/or firewall rules set to allow bypass of any intrusion prevention or other network filtering systems.

6. Exclusions

Please note that verification of vulnerabilities is not always possible, and we will not attempt exploitation where this would pose any undue risk to the availability or integrity of production systems and/or data.

The excluded items described below are outside the scope of this Service Description:

(a) Performance of additional tests outside the agreed scope and schedule, unless otherwise specified in your ToR;

(b) Completion of any remediation actions;

(c) Creation of risk treatment plans;

(d) Denial of service;

(e) Data deletion;

(f) Data alteration;

(g) Power cycling of the host; and

(h) Any activity that would compromise the BAU use of your host.

7. Definitions and Acronyms

7.1 Definitions

In this document “we” or “us” refers to the Supplier, and “you” refers to the Client.

The terms listed have the following meanings:

Term	Meaning
Terms of Reference	A document which specifically sets out the detail of the testing engagement, how and when we will carry out that test and any dependencies or requirements needed for us to perform that activity.
URL	Uniform Resource Locator; a web address.

7.2 Acronyms

Acronym	Meaning
BAU	Business as Usual
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security protocol
ToR	Terms of Reference
URL	Uniform Resource Locator

8. Operational Targets

2. N/A

1. Service Overview

The Build Review Service is designed to help you to understand the level of risk that your individual hosts (workstations, servers, laptops etc) are exposed to from internal or external attacks. Such attacks could be carried out by a rogue employee, an intruder to a building, someone who has stolen a device or by automated/remote means via a malware attack.

The assessment will determine how your system has been configured to identify areas of weakness and investigate how any vulnerabilities raised can be mitigated to harden your system configuration.

The Build Review is conducted against an industry's CIS benchmarking standard of configuration where available (see https://www.cisecurity.org/cis-benchmarks/ for further details). If there is no CIS benchmark available, our consultants will perform the review in line with industry best practice.

Additional information will be included in your Order Form and/or Terms of Reference ("ToR").

2. Service Deliverables

We will provide the necessary technical tools to perform the Service according to your requirements as stated in your ToR. The scope of your Service and applicable Fees will be specified in your Order Form.

If you require assistance with any prerequisite or supporting element, our offensive security team can provide additional pre-test support, including the provision of IP information, credentials, system configurations and other information using secure channels. Additionally, we can assist you to prepare for the Service and to meet the dependencies listed in Section 5. Such additional support will be delivered as part of a separate professional services engagement which will be subject to a separate Fee as indicated on your Order Form.

2.1 Build Review

The Build Review assessment will determine how your in-scope systems have been configured to identify areas of weakness. We will investigate areas of weaknesses and report on vulnerabilities and mitigation options to provide you with feedback on your system configuration and how it could be hardened.

We can carry out the Build Review on servers, laptops, mobile phones, tablets, desktops and thin clients with core areas of examination, including Operating System patching, third party patching, user account and passwords, configured services, applications installed, remote access configuration, general security configuration, antivirus and malware protection, firewall configuration, BIOS/UEFI configuration and disk encryption settings. Your individual requirements will be documented in your ToR.

The Build Review process is as follows:

(a) Once the scope of the test is agreed with you, we will identify the relevant target hosts and their OS. Our consultant will connect to the target system over the most appropriate administrative protocol (*e.g*. SSH, SMB, RDP), using an account set up with administrator level privileges;

(b) Depending on the type of system, we will use automated tools such as Nessus, and/or custom written audit scripts, to determine the patch level of the host and how well hardened it is against industry standard benchmarks;

(c) We will then perform a manual investigation based around the use of the system and any unusual features identified throughout the review process;

(d) Our consultant will review both the automated and manual results to identify risks based on these results and the use and context of the server.

The report will include:

(a) Categorisation of each vulnerability;

(b) Threat exposure;

(c) Root cause of the issue;

(d) Testing technique used to find/reproduce the issue;

(e) Remediation advice; and

(f) Severity ratings.

We will perform the build review using one or more of the following tools (as we determine to be the most appropriate):

(a) Vulnerability scanner(s);

(b) Manual examination; and/or

(c) Custom written audit and examination scripts.

The choice of tools will vary according to your requirements and your host environment. If we agree with you to use specific tools not listed in this Section 2, we will include details of such tools in your ToR.

3. Service Delivery

After order acceptance, we will deliver the Service as follows:

Service Delivery	Us	You
We will discuss with you the Service and your environment to ensure accurate scoping for the Build Review.	•	•

Service Delivery	Us	You
You will provide us details of any required limitation around the scope of the Build Review.		●
You will provide us all the information necessary to conduct the Build Review.		●
You will approve and sign-off the project.		●
We will provide you with a ToR confirming the scope and the schedule of the penetration test prior to commencement.	●	
You will accept and sign the ToR.		●

All service delivery work will be carried out during Business Hours. We will invoice additional charges for any work undertaken out of hours. We reserve the right to charge additional Fees for any change in your requirements occurring after completion of the activities listed in the table above and outside the scope of the contract (as described in the MSA).

3.1 Ready for Service

The Ready for Service Date for this Service is the date on which we agree and sign an Order Form with you, unless otherwise specified in your ToR.

(a) Test Date

You can request to postpone the test up to eleven (11) Business Days before the agreed test date indicated in your ToR, in which event we will reschedule the test and agree a new date with you for no additional charge. Please note that this will not change your Ready for Service Date.

In the event that you are not ready for the test on the agreed date, and you fail to submit a request to postpone the test date with at least eleven (11) Business Days' prior notice, you will be able to cancel the test subject to a cancellation Fee calculated as follows:

(i) A charge equal to fifty percent (50%) of the Non-Recurring Fee if you submit a cancellation request between eleven (11) and six (6) Business Days before the agreed test date; or

(ii) A charge equal to one hundred percent (100%) of the Non-Recurring Fee if you submit a cancellation request less than (6) Business Days before the agreed test date.

For the avoidance of doubt, any test that you wish to reschedule after cancellation shall be deemed a new order subject to a separate Fee.

4. Billing

The Service will be billed as a professional service Non-Recurring Fee on or shortly after signature of the Order Form, as described in the Billing Guide.3.1

4.1 Additional Fees

We reserve the right to charge additional Fees in the following situations:

(a) Any work carried out outside Business Hours; and

(b) Any change in your requirements occurring after completion of the Service Delivery activities listed in Section 3 and outside the scope of the contract (as described in the MSA).

5. Dependencies

We will provide the Build Review Service subject to the following dependencies:

5.1 Client Obligations

(a) You will provide us details of your target hosts and any required information around scope (*e.g.* list of IPs and associated Operating System on which we will be performing the review);

(b) You will provide us local administrator and/or root level user accounts for the systems being reviewed;

(c) You will provide us your source IP address, network mask, gateway and any relevant VLAN details for the network segments from which the tests should be conducted from; and

(d) You will ensure that the source IP addresses you provide us are applied to any firewall, router/switch access controls list or other allow lists as required to facilitate access to the target subnets.

5.2 Prerequisites

(a) You will provide written approval and sign-off the project before we commence any work pursuant to this Service Description.

5.3 Dependencies

(a) We require access and authentication to be available as needed to enable us to perform the Build Review; and

(b) If applicable, you will provide us details and/or firewall rules set to allow bypass of any intrusion prevention or other network filtering systems.

6. Exclusions

Please note that verification of vulnerabilities is not always possible, and we will not attempt exploitation where this would pose an undue risk to the availability or integrity of your production systems and/or data.

The items listed below are outside the scope of this Service Description:

(a) Performance of additional tests outside the agreed scope and schedule, unless otherwise specified in your ToR;

(b) Completion of remediation actions;

(c) Creation of risk treatment plans;

(d) Denial of service;

(e) Data deletion;

(f) Data alteration;

(g) Power cycling of the host; and

(h) Any activity that would compromise the BAU use of your host.

7. Definitions and Acronyms

7.1 Definitions

In this document “we” or “us” refers to the Supplier, and “you” refers to the Client.

The terms listed have the following meanings:

Term	Meaning
BIOS	Basic firmware used to control underlying hardware and facilitate basic setup and control.
Terms of Reference	A document which specifically sets out the detail of the testing engagement, how and when we will carry out that test and any dependencies or requirements needed for us to perform that activity.

7.2 Acronyms

Acronym	Meaning
BAU	Business as Usual
BIOS	Basic Input/Output System
IP	Internet Protocol
OS	Operating System
RDP	Remote Desktop Protocol
SMB	Server Message Block Protocol
SSH	Secure Shell Protocol
ToR	Terms of Reference
UEFI	Unified Extensible Firmware Interface

8. Operational Targets

N/A

1. Service Overview

The Mobile Application Testing Service is designed to assess the level of risk that you and your users are exposed to from an attacker using the target application. The Service provides an security assessment of your Mobile Application based on OWASP mobile principles and guidelines) and a report detailing the findings of the assessment, any weaknesses identified and how vulnerabilities raised can be mitigated.

Common application types include IOS applications and Android applications. Other platforms are supported but require further scoping discussion.

Additional information will be included in your Order Form or Terms of Reference (ToR).

2. Service Deliverables

The Service focuses on the Mobile Application bespoke set of interactions with mobile devices.

We will provide the necessary technical tools to perform the Mobile Application Testing according to your requirements as stated in your ToR.

If you require assistance with any prerequisite or supporting element, our offensive security team can provide additional pre-test support, including the provision of IP information, credentials, system configurations and other information using secure channels. Additionally, we can assist you to prepare for the Service and to meet the dependencies listed in Section 5. Such additional support will be delivered as part of a separate professional services engagement which will be subject to a separate Fee as indicated on your Order Form.

The Mobile Application Testing process is as follows:

(a) Application Mapping (Phase 1) – We will examine the applications to determine the extent of the standard features and functionality. One of our testers will map the applications as an unauthenticated user and as each user role. The objective of this Phase 1 is to gain an understanding of the application prior to the main testing.

(b) Security Testing (Phase 2) – We will perform a test of the categories listed in the OWASP Mobile Application methodology:

(i) Architecture, design and threat modelling;

(ii) Data storage and privacy;

(iii) Cryptography verification;

(iv) Authentication and session management;

(v) Network communication;

(vi) Platform interaction;

(vii) Code quality and build settings; and

(viii) Resiliency against reverse engineering.

The methodology for each category is customised based on the specific mobile device platforms for which the application has been written.

The report will include:

(a) Categorisation of each vulnerability;

(b) Threat exposure;

(c) Root cause of the issue;

(d) Testing technique used to find/reproduce the issue;

(e) Remediation advice; and

(f) Severity ratings.

We will perform the Mobile Application Testing using one or more of the following tools (as we determine to be the most appropriate):

(a) Mobile devices in their default and jailbroken states;

(b) Platform specific Mobile Application testing framework (Drozer, Needle, Frida, MobSF);

(c) Reverse engineering, including disassembly/reassembly (Apktool, Smali/Backsmali, Radare, IDA Pro, Hopper, cycript, APK studio);

(d) Web Service/API security scanning and manual testing (Soap UI, Burp);

(e) Vulnerability-specific web scanner (sqlmap);

(f) SSL/TLS scanner (testssl.sh);

(g) Intercepting proxy (Burpsuite);

(h) Text-based SSL/TLS client (openssl);

(i) Text-based network socket client (netcat);

(j) File metadata extractor (exiftool);

(k) Exploits and exploitation frameworks (application dependent); and/or

(l) Web browser (Chromium/Firefox).

The choice of tools will vary according to your requirements and your host environment. If we agree with you to use specific tools not listed in this Section 2, we will include details of such tools in your ToR.

3. Service Delivery

After order acceptance, we will deliver the Service as follows:

Service Implementation	Us	You
We will discuss with you the Service and your environment to ensure accurate scoping for the penetration test.	●	●
You will provide us details of any required limitation around the scope of the penetration test.		●
You will provide us all the information necessary to conduct the penetration test.		●
You will approve and sign-off the project.		●
We will provide you with a ToR confirming the scope and the schedule of the penetration test prior to commencement.	●	
You will accept and sign the ToR.		●

All service delivery work will be carried out during Business Hours. We will invoice additional charges for any work undertaken out of hours. We reserve the right to charge additional fees for any change in your requirements occurring after completion of the activities listed in the table above and outside the scope of the contract (as described in the MSA).

3.1 Ready for Service

The Ready for Service Date for this Service is the date on which we agree and sign an Order Form with you, unless otherwise specified in your ToR.

(a) Test Date

You can request to postpone the test up to eleven (11) Business Days before the agreed test date indicated in your ToR, in which event we will reschedule the test and agree a new date with you for no additional charge.

In the event that you are not ready for the test on the agreed date, and you fail to submit a request to postpone the test date with at least eleven (11) Business Days' prior notice, you will be able to cancel the test subject to a cancellation fee calculated as follows:

(i) A charge equal to 50% of the Non-Recurring Fee if you submit a cancellation request between eleven (11) and six (6) Business Days before the agreed test date; or

(ii) A charge equal to 100% of the Non-Recurring Fee if you submit a cancellation request less than (6) Business Days before the agreed test date.

For the avoidance of doubt, any test that you wish to reschedule after cancellation shall be deemed a new order subject to a separate Fee.

4. Billing

The Service will be billed as a professional service Non-Recurring Fee on or shortly after signature of the Order Form, as described in the Billing Guide.

4.1 Additional Charges

We reserve the right to charge additional Fees in the following situations:

(a) Any work carried out outside Business Hours; and

(b) Any change in your requirements occurring after completion of the Service Delivery activities listed in Section 3 and outside the scope of the contract (as described in the MSA).

5. Dependencies

We will provide the Mobile Application Testing Service subject to the following dependencies:

5.1 Client Obligations

(a) You will provide us Mobile Application binaries, download URLs, and platform marketplace details as required;

(b) You will provide us backend Web Service/API URL(s) and additional relevant details, including any required limitation around scope (e.g. specific endpoints or HTTPS);

(c) You will provide us the credentials for all user roles to be tested where authenticated testing applies, including documentation of the privileges assigned to and relationships between the user roles where multiple user roles are being tested;

(d) You will obtain authorisation to perform the test from network/hosting providers, or written confirmation that such authorisation is not required in the case of providers such as Microsoft Azure; and

(e) You will ensure all the source IP addresses you provide us are applied to any border firewalls or other whitelists as required.

5.2 Prerequisites

(a) You will provide written approval and sign-off the project before we commence any work pursuant to this Service Description.

5.3 Dependencies

(a) Before commencing the service, we will provide you with our source IP addresses and you will disable any relevant Mobile Application firewalls for our source IP;

(b) If applicable, you will provide us details and/or firewall rules set to allow bypass of third-party DDoS/WAF protection; and

(c) Where multiple IP addresses are resolved from the URL hostname, we will focus the testing on one IP address.

6. Exclusions

Please note that verification of vulnerabilities is not always possible, and we will not attempt exploitation where this would pose any undue risk to the availability or integrity of your production systems and/or data.

The excluded items described below are outside the scope of this Service Description:

(a) Performance of additional tests outside the agreed scope and schedule, unless otherwise specified in your ToR;

(b) Completion of any remediation actions;

(c) Creation of risk treatment plans;

(d) Denial of service;

(e) Testing that may affect the availability or integrity of production systems or data; and

(f) Mobile device testing, multiple Mobile Application testing, Web Application testing, and Web Service/API testing.

7. Definitions and Acronyms

7.1 Definitions

In this document “we” or “us” refers to the Supplier, and “you” refers to the Client.

The terms listed have the following meanings:

Term	Meaning
Mobile Application	A piece of computer software which allows users to interact with servers on the internet or other network (e.g. corporate internal network) using a mobile device such as a phone or a tablet.
Terms of Reference	A document which specifically sets out the detail of the testing engagement, how and when we will carry out that test and any dependencies or requirements needed for us to perform that activity.
URL	Uniform Resource Locator; a web address.
Web Application	A piece of computer software which allows users to interact with servers on the internet or other network (e.g. a corporate internal network) using a web browser.
Web Service/API	An API provides the means by which different software components can talk to one another. A web service is a type of API which is exposed over a network such as the internet and uses web technologies such as web servers, HTTP and SSL/TLS to form the communications channel.

7.2 Acronyms

Acronym	Meaning

API	Application Program Interface
BAU	Business as Usual
DDoS	Distributed Denial of Service
DoS	Denial of Service
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
OWASP	Open Web Application Security Project
SSL	Secure Sockets Layer
TLS	Transport Layer Security protocol
ToR	Terms of Reference
URL	Uniform Resource Locator
WAF	Web Application Firewall

8. Operational Targets

N/A

1. Service Overview

The PCI ASV Scanning is designed to assess the level of risk that you and your users are exposed to from an external attacker, and it is an approved tool certified to be used as supplementary evidence as part of the PCI auditing process. The Service provides an automated vulnerability scanning managed and run through an approved ASV scanning tool provided by Qualys. Qualys has been authorized by the PCI Security Standards Council to conduct the quarterly scans required to show compliance with PCI DSS. The cloud-based Qualys PCI solution can assist you to achieve compliance via a streamlined process to assess the security of your network.

The PCI ASV Scanning is non-intrusive, and the Service does not include a manual result investigation process.

Additional information will be included in your Order Form or Terms of Reference.

2. Service Deliverables

We will provide the necessary technical tools to perform the PCI ASV Scanning according to your requirements as stated in your ToR.

If you require assistance with any prerequisite or supporting element, our offensive security team can provide additional pre-test support, including the provision of IP information, credentials, system configurations and other information using secure channels. Additionally, we can assist you to prepare for the Service and to meet the dependencies listed in Section 5. Such additional support will be delivered as part of a separate professional services engagement which will be subject to a separate Fee as indicated on your Order Form.

The scanning tool is provided through our ASV scanning provider partners at Qualys. Our penetration testers will configure, run and review the results generated from the monthly or quarterly scanning activities to advise on compliance to the PCI approved standards. If our testers identify hosts that do not meet the PCI standard during the scanning process, we will notify you and work with you to understand what actions can be taken to achieve the relevant standard.

Your individual requirements will be specified in your Terms of Reference.

The PCI ASV Scanning process is as follows:

(a) You will provide us details of all IP addresses included in the scope of the scanning. Typically, these will be all external hosts that make up the boundary of your CDE or PCI environment;

(b) We will set up Qualys scanning tool and run the scanning in accordance with the schedule agreed in your ToR;

(c) Once setup is complete, we will agree the scan schedule with you;

(d) We will provide you a report after each scheduled scan has been run, including advice on issue remediation. We will provide you with login details for Qualys tool which will allow you to view the reports at any time. The report formats are approved ASV scanning templates used by Qualys.

The report provided after each scan will include:

(a) Categorisation of each vulnerability;

(b) Threat exposure;

(c) Root cause of the issue;

(d) Remediation advice based on the information produced by the Qualys scan;

(e) Severity ratings.

We will perform the PCI ASV Scanning service using the following tools:

(a) Qualys ASV Scanning.

3. Service Delivery

After order acceptance, we will deliver the Service as follows:

Service Delivery	Us	You
We will discuss with you the Service and your environment to ensure accurate scoping for the penetration test.	•	•
You will provide us details of any required limitation around the scope of the penetration test.		•
You will provide us all the information necessary to conduct the penetration test.		•
You will approve and sign-off the project.		•
We will provide you with a ToR confirming the scope and the schedule of the penetration test prior to commencement.	•	
You will accept and sign the ToR.		•

All service delivery work will be carried out during Business Hours. We will invoice additional charges for any work undertaken out of hours. We reserve the right to charge additional fees for any change in your requirements occurring after completion of the activities listed in the table above and outside the scope of the contract (as described in the MSA).

3.1 Ready for Service

The Ready for Service Date for this Service is the date on which we agree and sign an Order Form with you, unless otherwise specified in your ToR.

4. Billing

As a standard, the Service will be billed as a professional service Non-Recurring Fee and an additional Non-Recurring Fee for the Qualys ASV Scanning licence on or shortly after signature of the Order Form, as described in the Billing Guide.

We may agree payment milestones with you, in which event we will charge you a Non-Recurring Fee for the Qualys ASV Scanning licence on or shortly after signature of the Order Form and the Fees associated with each milestone will be billed as specified in your Order Form and/or ToR, and in accordance with the Billing Guide.

4.1 Additional Charges

We reserve the right to charge additional Fees in the following situations:

(a) Any work carried out outside Business Hours; and

(b) Any change in your requirements occurring after completion of the Service Delivery activities listed in Section 3 and outside the scope of the contract (as described in the MSA).

5. Dependencies

We will provide the PCI ASV Scanning Service is subject to the following dependencies:

5.1 Client Obligations

(a) You will comply with the End User Licence Agreement provided by Qualys;

(b) You will provide us details of your target hosts and any additional information around the scope of the Service as we may reasonably require (e.g. list of IPs and associated Operating System on which we will be performing the scanning);

(c) You will ensure that the source IP addresses you provide us are applied to any firewall, router/switch access controls list or other whitelists as required to facilitate access to the target subnets.

5.2 Prerequisites

(a) You will provide written approval and sign-off the project before we commence any work pursuant to this Service Description.

5.3 Dependencies

(a) Access and authentication as requested must be available for the review to be completed; and

(b) If applicable, you will provide us details and/or firewall rules set to allow bypass of any intrusion prevention or other network filtering systems.

6. Exclusions

The excluded items described below are outside the scope of this Service Description:

(a) Performance of additional tests outside the agreed scope and schedule, unless otherwise specified in your ToR;

(b) Completion of any remediation actions;

(c) Creation of risk treatment plans;

(d) Denial of service;

(e) Data deletion;

(f) Data alteration;

(g) Power cycling of the host;

(h) Any activity that would compromise the BAU use of the host; and

(i) Any activity considered to be active penetration testing.

7. Definitions and Acronyms

7.1 Definitions

In this document “we” or “us” refers to the Supplier, and “you” refers to the Client.

The terms listed have the following meanings:

Term	Meaning
Terms of Reference	A document which specifically sets out the detail of the testing engagement, how and when we will carry out that test and any dependencies or requirements needed for us to perform that activity.

7.2 Acronyms

Acronym	Meaning
AVS	Address Verificaiton Service
BAU	Business as Usual
CDE	Cardholder Data Environment
PCI DSS	Payment Card Industry Data Security Standard
SSL	Secure Sockets Layer
TLS	Transport Layer Security protocol
ToR	Terms of Reference

8. Operational Targets

N/A

1. Service Overview

The Phishing Service is designed to assess the level of risk that your current infrastructure and staff are exposed to from an external attacker attempting to gain access to your internal network via Phishing or Spear Phishing emails.

The Service will test your organisation staff and their reactions to receiving crafted phishing emails of various technicality levels. The purpose of the testing is to provide you with an overview of the risks and effectiveness of your current technical infrastructure in preventing malicious email as well as directly testing the reactions of your staff to phishing mail and the effectiveness of any training programs that you have in place.

Additional information may be included in your Order Form or Terms of Reference (ToR).

2. Service Deliverables

.

We will provide the necessary technical tools to perform the Phishing Service according to your requirements as stated in your ToR.

If you require assistance with any prerequisite or supporting element, our offensive security team can provide additional pre-test support, including the provision of IP information, credentials, system configurations and other information using secure channels. Additionally, we can assist you to prepare for the Service and to meet the dependencies listed in Section 5. Such additional support will be delivered as part of a separate professional services engagement which will be subject to a separate Fee as indicated on your Order Form.

Before commencement of the test, we will agree with you a list of users to be targeted during the Phishing and Spare Phishing exercise. We can prepare this list via an open-source intelligence gathering exercise to identify users and suggest targets. Alternatively, you can provide us your own list of preferred targets.

We will then create different email templates to entice your target users into following or engaging with a hyperlink or other malicious embedded content contained within the message body.

Typically email templates follow the following formats:

(a) Formatted to mimic messages from popular online services;

(b) Formatted to mimic client specific systems, such as an intranet site, captive portals, known internal applications;

(c) Formatted to mimic alerts from others within the organisation, such as the organisation's IT, finance or HR department; and

(d) Formatted to mimic mail specific to a user and their interests.

The Phishing Service process is as follows:

(a) Template Design and Kick off Meetings (Phase 1) – We will hold a kick-off meeting during which we will agree bespoke email templates with you and the list of target users. If needed, we can customise email templates based on the specific set of target users agreed with you.

(b) Campaign Start (Phase 2) - Once the pool of targets and templates have been agreed and designed from Phase 1, we will begin the campaign. Such campaign will be based on your specific requirements agreed with you in your ToR. Unless otherwise agreed with you, we will break down the target list into groups and send phishing emails at random times over the course of the engagement.

(c) Change of Tactics (Phase 3) - Our offensive security team will monitor and review the success of the campaigns. If we have agreed with you to provide a multiple levels campaign, out testers will review and analyse the results from the initial templated email campaign and leverage this information to customise future campaigns with multiple levels of approach. In this event, we will advise you to move from a basic template to a more complex one when appropriate or implement such template at the date and time pre-agreed with you as detailed in your ToR. If we have not agreed with you to provide multiple levels campaign, we will suggest alterations to the template and approach as appropriate to achieve better results.

The report will include:

(a) Categorisation of each vulnerability;

(b) Threat exposure;

(c) Root cause of the issue;

(d) Testing technique used to find/reproduce the issue;

(e) Remediation advice;

(f) Severity ratings.

At the conclusion of each campaign we will review the results along with the statistics showing the number of emails and email campaigns used against the success rate of your targets. We will provide you with a PDF report which will include an executive summary, our general conclusion, the risk factors, the critical recommendations and the general recommendations.

We will perform the Phishing Service using one or more of the following tools (as we determine to be the most appropriate):

(a) Custom built phishing campaign manager;

(b) Mail Servers;

(c) IDE for custom built phishing templates; and/or

(d) TheHarvester (harvesting user data - emails etc).

The choice of tools will vary according to your requirements and your host environment. If we agree with you to use specific tools not listed in this Section 2, we will include details of such tools in your ToR.

3. Service Delivery

After order acceptance, we will deliver the Service as follows:

Service Implementation	Us	You
We will discuss with you the Service and your environment to ensure accurate scoping for the penetration test performance.	•	•
You will provide us details of any required limitation around the scope of the penetration test.		•
You will provide us all the information necessary to conduct the penetration test.		•
You will approve and sign-off the project.		•
We will provide you with a ToR confirming the scope and the schedule of the penetration test prior to commencement.	•	
You will accept and sign the ToR.		•

All service delivery work will be carried out during Business Hours. We will invoice additional charges for any work undertaken out of hours. We reserve the right to charge additional fees for any change in your requirements occurring after completion of the activities listed in the table above and outside the scope of the contract (as described in the MSA).

3.1 Ready for Service

The Ready for Service Date for this Service is the date on which we agree and sign an Order Form with you, unless otherwise specified in your ToR.

(a) Test Date

You can request to postpone the Phishing campaign up to eleven (11) Business Days before the agreed commencement date indicated in your ToR, in which event we will reschedule the Phishing campaign and agree a new date with you for no additional charge.

In the event that you are not ready for the Phishing campaign on the agreed date, and you fail to submit a request to postpone the commencement date with at least eleven (11) Business Days' prior notice, you will be able to cancel the Phishing campaign subject to a cancellation fee calculated as follows:

(i) A charge equal to 50% of the Non-Recurring Fee if you submit a cancellation request between eleven (11) and six (6) business days before the agreed test date; or

(ii) A charge equal to 100% of the Non-Recurring Fee if you submit a cancellation request less than (6) business days before the agreed test date.

For the avoidance of doubt, any Phishing campaign that you wish to reschedule after cancellation shall be deemed a new order subject to a separate charge.

4. Billing

The Service will be billed as a professional service Non-Recurring Fee on or shortly after signature of the Order Form, as described in the Billing Guide.

4.1 Additional Charges

We reserve the right to charge additional fees in the following situations:

(a) Implementation work carried out outside Business Hours; and

(b) Any change in your requirements occurring after completion of the Service Delivery activities listed in Section 3 and outside the scope of the contract (as described in the MSA).

5. Dependencies

We will provide the Phishing Service subject to the following dependencies:

5.1 Client Obligations

(a) You will provide us details of your target users as required and other relevant information around the scope and limitations;

5.2 Prerequisites

(a) You will provide written approval and sign-off the project before we commence any work pursuant to this Service Description.

6. Exclusions

Please note that verification of vulnerabilities is not always possible, and we will not attempt exploitation where this would pose any undue risk to the availability or integrity of production systems and/or data.

The excluded items described below are outside the scope of this Service Description:

(a) Performance of additional tests outside the agreed scope and schedule, unless otherwise specified in your ToR;

(b) Completion of any remediation actions;

(c) Creation of risk treatment plans.

(d) Denial of service;

(e) Data deletion;

(f) Data alteration; and

(g) Unauthorised personal attacks against staff.

7. Definitions and Acronyms

7.1 Definitions

In this document “we” or “us” refers to the Supplier, and “you” refers to the Client.

The terms listed have the following meanings:

Term	Meaning
Phishing	The practice of sending emails to induce individuals to reveal sensitive information or to deploy malicious software.
Spear Phishing	Phishing targeting specific individuals.
Terms of Reference	A document which specifically sets out the detail of the testing engagement, how and when we will carry out that test and any dependencies or requirements needed for us to perform that activity.

7.2 Acronyms

Acronym	Meaning
ToR	Terms of Reference

8. Operational Targets

N/A

1. Service Overview

The Scenario Testing is a scenario based and contextual penetration testing which allows you to interact with our testing team to build a set of customised attack scenarios. The Service is designed to assess the performance of your target platforms when subjected to malicious activities such as penetration testing, malware creation/deployment, and phishing techniques. The scenarios can be generic or bespoke and will be agreed with you based on your requirements.

Additional information may be included in your Order Form or Terms of Reference (ToR).

2. Service Deliverables

The scenario testing service is designed to provide a contextual and bespoke testing package to identify how your targets stands up to a specific attack.

The Scenario Testing can include, but is not limited to, elements of social engineering, malware writing, phishing, hardware/device hacking, scenario based targeted network, asset, platform or device attacks. The techniques and attack types will be outlined in your ToR.

We will provide the necessary technical tools to perform the Scenario Testing according to your requirements as stated in your ToR.

If you require assistance with any prerequisite or supporting element, our offensive security team can provide additional pre-test support, including the provision of IP information, credentials, system configurations and other information using secure channels. Additionally, we can assist you to prepare for the Service and to meet the dependencies listed in Section 6. Such additional support will be delivered as part of a separate professional services engagement which will be subject to a separate Fee as indicated on your Order Form.

The Scenario Testing process is as follows:

(a) Stage 1 – One of our tester will arrange a meeting with you to discuss your current security issues and areas of targeted interest.

(b) Stage 2 – Our offensive security team will review your requirements and design a set of testing scenarios and attack vectors.

(c) Stage 3 – We will agree the scenarios with you and execute them individually at the frequency defined in your ToR. We will discuss the content of each scenario with you and the potential risks, and include details in your ToR.

(d) Stage 4 – We will provide you PDF report of all findings following the completion of the test. We will arrange follow-up meetings to review the results of the Scenario Testing and provide additional feedback which can be used to further customise future scenarios based on your environment.

The report will include:

(a) Categorisation of each vulnerability;

(b) Threat exposure;

(c) Root cause of the issue;

(d) Testing technique used to find/reproduce the issue;

(e) Remediation advice; and

(f) Severity ratings.

We will perform the build review service using one or more of the following tools (as we determine to be the most appropriate):

(a) Metagoofil;

(b) The Harvester;

(c) Nmap;

(d) Nessus;

(e) Metasploit;

(f) Bespoke Phishing templates; and/or

(g) Custom Written Malware.

The choice of tools will vary according to your requirements and your host environment. If we agree with you to use specific tools not listed in this Section 2, we will include details of such tools in your ToR.

3. Service Delivery

After order acceptance, we will deliver the Service as follows:

Service Implementation	Us	You
We will discuss with you the Service and your environment to ensure accurate scoping for the penetration test performance.	•	•
You will provide us details of any required limitation around the scope of the penetration test).		•
You will provide us all the information necessary to conduct the penetration test.		•
You will approve and sign-off the project.		•
We will provide you with a ToR document confirming the scope and the schedule of the penetration test prior to commencement.	•	
You will accept and sign the ToR.		•

All service delivery work will be carried out during Business Hours. We will invoice additional charges for any work undertaken out of hours. We reserve the right to charge additional fees for any change in your requirements occurring after completion of the activities listed in the table above and outside the scope of the contract (as described in the MSA).

3.1 Ready for Service

4. The Ready for Service Date for this Service is the date on which we agree and sign an Order Form with you, unless otherwise specified in your ToR.

(a) Test Date

You can request to postpone the test up to eleven (11) Business Days before the agreed test date indicated in your Terms of Reference, in which event we will reschedule the test and agree a new date with you for no additional charge.

In the event that you are not ready for the test on the agreed date, and you fail to submit a request to postpone the test date with at least eleven (11) Business Days' prior notice, you will be able to cancel the test subject to a cancellation fee calculated as follows:

(i) A charge equal to 50% of the Non-Recurring Fee if you submit a cancellation request between eleven (11) and six (6) business days before the agreed test date; or

(ii) A charge equal to 100% of the Non-Recurring Fee if you submit a cancellation request less than (6) business days before the agreed test date.

For the avoidance of doubt, any test that you wish to reschedule after cancellation shall be deemed a new order subject to a separate charge.

5. Billing

The Service will be billed as a professional service Non-Recurring Fee on or shortly after signature of the Order Form, as described in the Billing Guide.

5.1 Additional Charges

We reserve the right to charge additional fees in the following situations:

(a) Implementation work carried out outside Business Hours; and

(b) Any change in your requirements after completion of the Service Delivery activities listed in Section 3 and outside the scope of the contract (as described in the MSA).

6. Dependencies

We will provide the Scenario Testing Service subject to the following dependencies:

6.1 Client Obligations

(a) You will provide us details of your target hosts and any required information around scope, including limitations and exclusions;

(b) You will provide us details of your targets of interest within your organisation (e.g. hosts, staff etc.);

(c) Where applicable, you will provide us with access to target hardware;

(d) Where relevant, you will obtain authorisation to perform the test from network/hosting providers, or written confirmation that such authorisation is not required in the case of providers such as Microsoft Azure;

(e) You will ensure that the source IP addresses you provide us are applied to any border firewalls or other whitelists as required and where appropriate to meet the test requirements.

6.2 Prerequisites

(a) You will provide written approval and sign-off the project before we commence any work pursuant to this Service Description.

6.3 Dependencies

(a) Access and authorisation as requested must be available for the scenario testing to be undertaken where access to systems and buildings is required;

(b) You must approve a defined list of scenarios.

7. Exclusions

Please note that verification of vulnerabilities is not always possible, and we will not attempt exploitation where this would pose any undue risk to the availability or integrity of production systems and/or data.

The excluded items described below are outside the scope of this Service Description:

(a) Performance of additional tests outside the agreed scope and schedule, unless otherwise specified in your ToR;

(b) Completion of any remediation actions;

(c) Creation of risk treatment plans;

(d) Social engineering such as targeting employees' private lives;

(e) Denial of service unless otherwise specified in your ToR; and

(f) Data destruction unless otherwise specified in your ToR.

8. Definitions and Acronyms

8.1 Definitions

In this document “we” or “us” refers to the Supplier, and “you” refers to the Client.

The terms listed have the following meanings:

Term	Meaning
Terms of Reference	A document which specifically sets out the detail of the testing engagement, how and when we will carry out that test and any dependencies or requirements needed for us to perform that activity.

8.2 Acronyms

Acronym	Meaning
ToR	Terms of Reference

9. Operational Targets

N/A

1. Service Overview

The System Configuration Review is designed to examine how your network devices have been implemented in order to identify areas of potential weakness. We will investigate the weaknesses identified and how any vulnerabilities raised can be mitigated to harden your system configuration.

The System Configuration Review can be carried out on switches, routers, Wi-Fi controllers and firewalls. Core areas of examination include checks to assess whether any device rules allow unauthorised traffic in or out of specified zones/VLANs and whether the devices run insecure administration services (e.g. Telnet, SNMP V1), and to assess the security of any device credentials stored locally as well as to analyse user accounts and their effective permission levels. During the review, we will check firmware version numbers and patching levels for the individual network devices to determine whether the latest version of all software is being run, to identify vulnerabilities relating to any older versions identified, and to understand the risk the devices pose to the network infrastructure.

The System Configuration Review is a non-intrusive service as all testing is carried out on the supplied configurations only. Testing will not be performed directly against the hosts.

The System Configuration Review is conducted against an industry's CIS benchmarking standard of configuration where available (see https://www.cisecurity.org/cis-benchmarks/ for further details). If there is no CIS benchmark available, our consultants will perform the review in line with industry best practice.

Additional information will be included in your Order Form and/or Terms of Reference ("ToR").

2. Service Deliverables

We will provide the necessary technical tools to perform the System Configuration Review according to your requirements as stated in your ToR.

If you require assistance with any prerequisite or supporting element, our offensive security team can provide additional pre-test support, including the provision of IP information, credentials, system configurations and other information using secure channels. Additionally, we can assist you to prepare for the Service and to meet the dependencies listed in Section 5. Such additional support will be delivered as part of a separate professional services engagement which will be subject to a separate Fee as indicated on your Order Form.

The System Configuration Review process is as follows:

(a) We will use a combination of automated tools and manual configuration review to identify weaknesses within the device configuration;

(b) We will conduct checks for any known vulnerabilities against the current device firmware;

(c) We will conduct checks for missing patches;

(d) Where applicable, we will review all access control rules for security best practice;

(e) Where applicable, we will review all firewall rules for security best practice;

(f) Where applicable, we will review all device users and their appropriate security groups; and

(g) We will check all device administration interface settings for security best practice.

The report will include:

(a) Categorisation of each vulnerability;

(b) Threat exposure;

(c) Root cause of the issue;

(d) Testing technique used to find/reproduce the issue;

(e) Remediation advice; and

(f) Severity ratings.

We will perform the System Configuration Review service using one or more of the following tools (as we determine to be the most appropriate):

(a) Vulnerability scanner (Nessus);

(b) Nipper; and/or

(c) Manual configuration review.

The choice of tools will vary according to your requirements and your host environment. If we agree with you to use specific tools not listed in this Section 2, we will include details of such tools in your ToR.

3. Service Delivery

After order acceptance, we will deliver the Service as follows:

Service Implementation	Us	You
We will discuss with you the Service and your environment to ensure accurate scoping for the System Configuration Review.	●	●
You will provide us details of any required limitation around the scope of the System Configuration Review.		●
You will provide us all the information necessary to conduct the System Configuration Review.		●
You will approve and sign-off the project.		●
We will provide you with a ToR confirming the scope and the	●	

schedule of the penetration test prior to commencement.		
You will accept and sign the ToR.		●

All service delivery work will be carried out during Business Hours. We will invoice additional charges for any work undertaken out of hours. We reserve the right to charge additional fees for any change in your requirements occurring after completion of the activities listed in the table above and outside the scope of the contract (as described in the MSA).

3.1 Ready for Service

The Ready for Service Date for this Service is the date on which we agree and sign an Order Form with you, unless otherwise specified in your ToR.

(a) Test Date

You can request to postpone the test up to eleven (11) Business Days before the agreed test date indicated in your ToR, in which event we will reschedule the test and agree a new date with you for no additional charge. Please note that this will not change your Ready for Service Date.

In the event that you are not ready for the test on the agreed date, and you fail to submit a request to postpone the test date with at least eleven (11) Business Days' prior notice, you will be able to cancel the test subject to a cancellation fee calculated as follows:

(i) A charge equal to 50% of the Non-Recurring Fee if you submit a cancellation request between eleven (11) and six (6) Business Days before the agreed test date; or

(ii) A charge equal to 100% of the Non-Recurring Fee if you submit a cancellation request less than (6) Business Days before the agreed test date.

For the avoidance of doubt, any test that you wish to reschedule after cancellation shall be deemed a new order subject to a separate Fee.

4. Billing

The Service will be billed as a professional service Non-Recurring Fee on or shortly after signature of the Order Form, as described in the Billing Guide.

4.1 Additional Charges

We reserve the right to charge additional fees in the following situations:

(a) Any work carried out outside Business Hours; and

(b) Any change in your requirements occurring after completion of the Service Delivery activities listed in Section 3 and outside the scope of the contract (as described in the MSA).

5. Dependencies

We will provide the System Configuration Review Service subject to the following dependencies:

5.1 Client Obligations

(a) You will ensure all device configurations are provided in a plain text human readable format (e.g. XML, JSON, HTML). Output from “show running config” on Cisco and similar devices are all acceptable;

(b) You will ensure paired devices are both submitted where applicable;

(c) You will ensure you are sending the device configurations to us in a secure manner (encrypted); and

(d) For firewall reviews in particular, you will provide us accurate information on context in terms of network diagrams and network context. Please note that the accuracy of the System Configuration Review report is subject to the amount of information provided by you.

5.2 Prerequisites

(a) You will provide written approval and sign-off the project before we commence any work pursuant to this Service Description.

5.3 Dependencies

(a) We require access and authentication to be available as needed to enable us to perform the System Configuration Review; and

(b) If applicable, you will provide us details and/or firewall rules set to allow bypass of any intrusion prevention or other network filtering systems.

6. Exclusions

Please note that the review of live systems is excluded from this scope of this Service and we will only review the configuration that has been exported from your system for the System Configuration Review.

The excluded items described below are outside the scope of this Service Description:

(a) Performance of additional tests outside the agreed scope and schedule, unless otherwise specified in your ToR;

(b) Completion of any remediation actions;

(c) Creation of risk treatment plans; and

(d) We will not be able to review unreadable or corrupt configurations.

7. Definitions and Acronyms

7.1 Definitions

In this document “we” or “us” refers to the Supplier, and “you” refers to the Client.

The terms listed have the following meanings:

Term	Meaning
Terms of Reference	A document which specifically sets out the detail of the testing engagement, how and when we will carry out that test and any dependencies or requirements needed for us to perform that activity.

7.2 Acronyms

Acronym	Meaning
HTML	HTML
JSON	JavaScript Object Notation
ToR	Terms of Reference
XML	EXtensible Markup Language

8. Operational Targets

N/A