PENETRATION TESTING

OX IT SOLUTIONS LTD

PENETRATION TESTING

SCOPING QUESTIONNAIRE

COMMERCIAL IN CONFIDENCE

1. INTRODUCTION

This is an editable document. Please fill in the fields electronically, save the document and send it back to either your account manager or sales@oxitsolutions.co.uk .

This document is how we gather the requirements to accurately and concisely scope your penetration test. Please be as accurate and detailed as possible, as this will help us make sure you get the right test that best fits your requirements.

All detail you supply will be held in the strictest confidence. If you feel any information is of a sensitive nature, we recommend putting an NDA in-place before providing us with the information.

Some answers will impact the details you need you need to supply later on, so please read each question fully and ensure you're filling in all applicable sections. If you need any help in filling-in the questionnaire, please don't hesitate to get in touch.

If you have multiple applications or multiple infrastructures to test, please complete multiple copies of this document with all appropriate information.

2. COMPANY & CONTACT INFORMATION

2.1 Please enter your and your company's details

COMPANY NAME	
ADDRESS	
YOUR NAME	
YOUR EMAIL	
YOUR PHONE	

2.2 Will you be the main point of contact for this test?

YES		NO	

If **NO**, please provide the contact's details below:

CONTACT NAME	
CONTACT EMAIL	
CONTACT PHONE	

3. HIGH-LEVEL QUESTIONS

3.1 Is compliance driving the test requirements?

YES		NO	

If you selected YES, please state the standard(s) driving the requirement for the test.

Please select all that apply.

PCI DSS	
FCA	
ISO	
GOVERNMENT (PSN, ITHC, ETC)	
HIPAA	
OTHER (PLEASE STATE)	

3.2 What type of test(s) do you require?

Please select all that apply.

INFRASTRUCTURE TEST	
APPLICATION TEST	
SOCIAL ENGINEERING	
OTHER (PLEASE STATE)	
UNSURE (WE WILL ADVISE)	

3.3 What are your reasons for this test?

Please select all that apply.

MEET COMPLIANCE REQUIREMENTS	
CUSTOMER REQUESTED WE HAVE TEST	
SUPPLIER REQUESTED WE HAVE TEST	
OUR OWN PEACE OF MIND	
OTHER (PLEASE STATE)	

3.4 What type of test do you require?

Black Box tests are where the penetration tester knows nothing of the infrastructure to be tested. It's more indicative of a real-world, attack, but this method may not always expose all vulnerabilities.

White Box tests are where the penetration tester has access to full, in-depth information on the infrastructure to be tested. Whilst not as realistic as a black box test, it allows for a very thorough test.

Grey Box tests are the most popular form of test that takes a balanced approach between white and black boxes. A grey box test discloses just enough information to perform a thorough, methodical test, whilst keeping the scenario relevant and realistic.

BLACK BOX	
WHITE BOX	
GREY BOX	
UNSURE (WE WILL ADVISE)	

3.5 Is there a specific timeframe the tests must be carried out (specific dates or times of day)?

YES		NO	

If you selected YES, please detail the times/dates required:

Please select all that apply.

WEEKDAYS	
WEEKENDS	
OFFICE HOURS	
OUTSIDE OFFICE HOURS	
DATE(S)	

3.6 Is the test to be carried out on a live (production) environment?

YES		NO	

OX IT SOLUTIONS LTD - SUITE F1, THE KIDLINGTON CENTRE, HIGH STREET, KIDLINGTON, OX5 2DL | TEL: 01865 594 933 | SALES@OXITSOLUTIONS.CO.UK | WWW.OXITSOLUTIONS.CO.UK | REG. NO. 10392088

4. DETAILED QUESTIONS: INFRASTRUCTURE

Only complete this section if you selected 'Infrastructure' in Question 3.2 above.

The next questions depend upon answers you've previously supplied. Please read all questions thoroughly to make sure you have not missed any applicable section.

4.1 If you selected BLACK BOX in Question 3.4

Since a Black Box test assumes nothing of the environment, we need only the minimum details to perform the test. Black box tests only last for a pre-determined amount of days.

4.1.1 Please provide a list of hostnames/IP addresses to be tested.

If you require more space, please include the full list in a separate document, such as a spreadsheet.

HOSTNAME/IP ADDRESSES

HOSTNAME/IP ADDRESSES

4.1.2 Please list any other details we might find relevant

ADDITIONAL DETAILS

4.2 If you selected WHITE BOX or GREY BOX in Question 3.4

4.2.1 Please provide information on the environment to be tested. If IaaS, please include firewalls, load balancers, routers, switches, servers, storage and other physical devices. If PaaS, please provide details on the PaaS being used how it is being consumed:

If you require more space, please include the full list in a separate document, such as a spreadsheet.

EQUIPMENT TYPE	DETAILS

PaaS DETAILS

4.2.2 Please provide a list of hostnames/IP addresses to be tested:

If you require more space, please include the full list in a separate document, such as a spreadsheet.

HOSTNAME/IP ADDRESSES

HOSTNAME/IP ADDRESSES

4.3 If you selected GREY BOX in Question 3.4, do you require an INTERNAL or EXTERNAL test?

Internal tests simulate an attack that has already bypassed your security perimeter. This discovers what an attacker can do internally, such as moving across systems and networks. It also simulates what an insider attack could do.

External tests simulate the ability of an attacker to gain access to your internal network and infrastructure from outside your security perimeter.

INTERNAL (go to 4.3.A)		EXTERNAL (go to 4.3.B)	

4.3.A If you answered INTERNAL to Question 4.3

Would you prefer the test to be carried out on your premises or by providing a secure VPN into the internal environment?

ON-PREMISES		VIA VPN	

4.3.B If you answered EXTERNAL to Question 4.3

4.3.B.1 What type of hosted environment do you require testing?

TYPE OF HOSTING	NAME OF HOSTING PROVIDER
PUBLIC IaaS (E.G. AWS, AZURE)	
PUBLIC PaaS	
PRIVATE CLOUD	
ON-PREMISES	
OTHER (PLEASE STATE)	

4.3.B.2 Do you have security controls that need to allow our IP addresses to be whitelisted before the test can commence?

YES		NO	

If you selected **YES** to 4.3.B.2 (above), please detail what these are.

SECURITY DETAILS

5. DETAILED QUESTIONS: APPLICATIONS

Only complete this section if you selected 'Application' in Question 3.2 above.

The next questions depend upon answers you've previously supplied. Please read all questions thoroughly to make sure you have not missed any applicable section.

5.1 Is it a single or multiple applications to be tested?

SINGLE		MULTIPLE (STATE NUMBER)	

5.2. Type of application

Please select all that apply.

WEB	
MOBILE	
DESKTOP	
OTHER (DESCRIBE)	

5.3 What is the application used for? Please provide a detailed description, including the application's functionality, key components, and other relevant information.

APPLICATION DESCRIPTION

5.4 What frameworks/languages were used to build the application?

FRAMEWORK/LANGUAGES USED

5.5 Is the application web accessible?

YES		NO	

5.6 If you selected WEB application in Question 5.2.1 (above), please let us know the hostname/IP address of the hosted application:

HOSTNAME/IP ADDRESS

5.7 If you selected MOBILE application in Question 5.2.1 (above), is it freely available to download?

Please select all that apply.

NOT AVAILABLE	
AVAILABLE VIA:	
GOOGLE PLAY	
IOS APP STORE	
AMAZON APP STORE	
OTHER (PLEASE SPECIFY)	

If you answered NOT AVAILABLE to the above, please detail how you will provide the application to us

APPLICATION PROVISION DETAIL

5.8 What type of test do you require?

AUTHENTICATED	
UN-AUTHENTICATED	
UNSURE (WE'LL ADVISE)	

6. DETAILED QUESTIONS: SOCIAL ENGINEERING

Only complete this section if you selected 'Social Engineering' in Question 3.2 above.

The next questions depend upon answers you've previously supplied. Please read all questions thoroughly to make sure you have not missed any applicable section.

6.1 What type of social engineering do you require?

Please select all that apply.

PHISHING	
VISHING	
PHYSICAL SECURITY BYPASS	

6.2 If you selected PHISHING or VISHING in Question 6.1 (above), will information on the users to be target be provided in advance of the test?

YES		NO	

6.2.1 If you selected YES, please tell us the number of users.

NUMBER OF USERS	

6.3 If you selected PHYSICAL SECURITY BYPASS in Question 6.1 (above), please detail the type of test you'd like carried out.

For example, passing gatehouse security and gaining access to a specific building or area

PHYSICAL SECURITY BYPASS DETAILS

7. ADDITIONAL INFORMATION

Is there any other information you think we should know? Perhaps you'd like to expand on any of your answers, or provide us with additional detail we haven't explicitly requested. Please use this box:

ADDITIONAL INFORMATION