

SECURITY PENETRATION TESTING SUPPLIER

SERVICE LEVEL AGREEMENT
CHECKLIST



WHY GO THROUGH A SLA CHECKLIST?

The goal of the Service Level Agreement (SLA) should be to protect both the customer and provider, as it manages expectations and solidifies what is agreed upon, upfront. Using a checklist will ensure that you've included all vital items in the agreement and will help to optimise the return on your penetration testing investment.

Risk Crew recommends the following seven requirements to include in your testing provider's SLA.

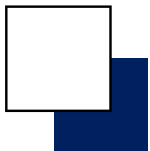
- Objectives
- Compliance Requirements
- Methodology
- Testing Scope
- Qualifications & Schedule
- Reporting Criteria
- Vulnerability Notification

The SLA does not detail legal, liability or insurance requirements that should be included. Rather, it is a list of topics that should be contractually addressed to ensure you get the most from the service.



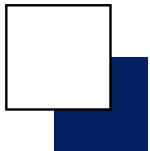
OBJECTIVES AND COMPLIANCE

Ensure the SLA:



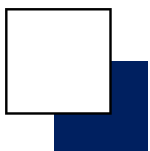
Specifically states the testing objective.

For example: The objective of the test is for the supplier to obtain unauthorised access to our assets, systems services or escalate user privileges etc.) Be specific. Otherwise, you will just receive a list of vulnerabilities that have little or no correlation to a risk.



Requires that the supplier provide a definitive statement in the testing deliverable regarding the outcome of the testing objective.

For example: Unauthorised access was not obtained in testing.

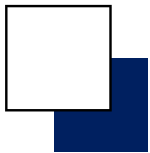


States any specific legislative, regulatory or best practice compliance requirements the testing must meet.

For example: Testing must meet requirements established in the Payment Card Industry and Data Security Standards.

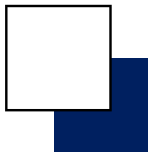
METHODOLOGY

Ensure the SLA specifies:



The testing methodology or standard to be used by the supplier.

For example: Should the supplier use a White Box, Grey Box, Black Box approach or OWASP, NIST or CREST standard? Is this approach or standard conducive to your testing objectives? If you are unsure, discuss it with your supplier.

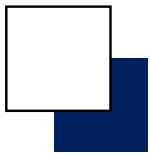


Which tools will be used along side the preferred methodology or standard.

If the contract does not specify a preferred methodology and tools, ensure the supplier identifies them in the report along with the tools that were used.

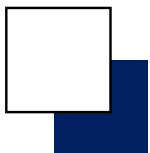
SCOPE

Ensure the SLA specifies:



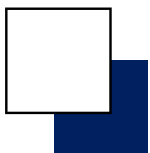
The infrastructure components.

For example: IP addresses, operating systems, supporting infrastructure URLs, applications APIs etc. need to be tested and that this scope is confirmed in the testing report.



The vulnerability classification system to be used by the testers for rating findings.

For example: CVE, CVSS or CWE. If you are unsure, have your supplier explain the differences and select the one more suited to your objectives.

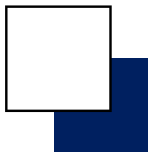


Any exceptions to the testing scope are also clearly stated in the SLA.

Such as a list of any IP addresses, URLs, virtual private network or partner connections that are not to be tested if applicable. This is crucial for purposes of liability.

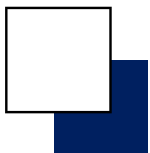
QUALIFICATION AND SCHEDULE

Ensure the SLA supplier provides:



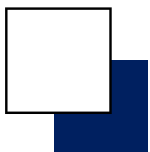
The names and qualifications of each tester that will be involved in the delivery of the service.

Ask the supplier if you can speak with them prior to testing to discuss goals, objectives, and any specific concerns that you may have.



Proof of testing certifications it holds and verify these are valid with the certifying body prior to contract.

For example: Certifications may include CEH, OSCP and CREST.

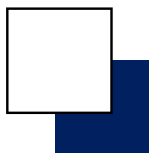


Approved testing times that are clearly established.

For example: Testing will only take place between 09:00 and 17:00 Monday through Friday.

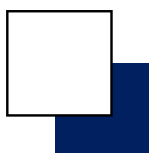
REPORTING & VULNERABILITY NOTIFICATION

Ensure the SLA states:



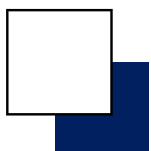
That the supplier provide a report clearly documenting the following for each vulnerability identified in testing:

The location, definition, and a classification of the vulnerability, (see above) results of manual exploitation of the vulnerability (along with visual evidence of its exploitation) the potential impact on the business if this vulnerability were exploited and step-by-step instructions for its remediation. These are just the minimum requirements. A good report is detail rich.



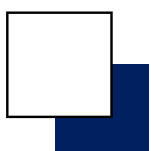
Any testing report formatting or content requirements.

For example: Should report findings and recommendations be submitted in WORD, PDF or Excel format?




Any security requirements associated with the submittal of the test report.

For example: Should the report be password protected, encrypted, mailed in hardcopy etc?



The supplier will contact you immediately if they identify a critical vulnerability during testing.

Critical vulnerabilities should be remediated as soon as they are found. Be sure you make this clear.



This checklist is by no means comprehensive but should serve to help with understanding the breadth and depth associated with a good security penetration test and the importance of a close relationship with your supplier to ensure clarification of your business requirements.

Contact us for more information



5 Maltings Place
169 Tower Bridge Road
London SE1 3JB
United Kingdom



+44 (0) 20 3653 1234



information@riskcrew.com



www.riskcrew.com