KOBREY SEC

Penetration Testing Vendor Scorecard

Vendor Information

Vendor Name _____

Vendor Contact _____

Date _____ **Interviewer** _____

Services Quoted _____

Vendor Scorecard

Scoring scale

- **1** = Weak / unclear / mostly automated / sales answers
- **2** = Basic / partial / vague detail
- **3** = Acceptable / meets expectations
- **4** = Strong / clear evidence of maturity
- **5** = Excellent / clearly manual, experienced, and well-structured

Section	Section Score
[Section A] Technical Depth and Manual Testing	
[Section B] Tester Quality and Staffing Integrity	
[Section C] Communication and Tester Access	
[Section D] Reporting and Post Engagement Support	
[Section E] General Testing and Program Maturity	
Total Score:	

Quick Decision Rules

- Any vendor scoring under 70 is usually not worth further time unless budget is the only driver.
- Any vendor scoring 80+ with a strong Section B and C score is typically a solid choice.

Testing Vendor Red Flags

Below are 10 items to watch out/listen for during the testing vendor interview. While these should not be immediate disqualifiers – they should be noted in the event of a tie.

[ ] No direct access to the tester

Lack of direct communication with the tester limits real-time validation of findings, and meaningful technical discussion. It often results in misunderstandings and weaker testing outcomes.

[ ] Won't name assigned testers ahead of time

Refusal to identify testers in advance prevents validation of their experience, certifications, and relevance to the environment being tested. This can indicate interchangeable or underqualified staffing.

[ ] Heavy intern or junior staffing

Overreliance on junior personnel often leads to checklist-driven testing, missed attack paths, and superficial findings.

[ ] "We run industry standard tools..."

Emphasizing tools rather than methodology suggests a vulnerability scanning mindset rather than an adversarial assessment. Skilled testers validate, exploit, and contextualize them to determine risk.

[ ] Report appears to be scanner output

Reports that resemble raw scanner results typically lack validation, prioritization, and business context. This shifts the burden of risk interpretation to the client and undermines the purpose of a penetration test.

[ ] No clear exploitability testing or chaining

Without exploitability testing or chaining, findings remain theoretical. The absence of demonstrated impact makes it difficult to assess real-world risk or understand how vulnerabilities could be combined.

[ ] Retesting not included

Excluding retesting discourages remediation validation and weakens risk closure. Retesting is essential to confirm fixes, prevent regressions, and ensure that remediation efforts are effective.

[ ] No escalation process for critical findings

Lack of a defined escalation path for critical issues delays response to high-impact risks. This can expose the organization to unnecessary harm during the engagement window.

[ ] Weak evidence standards

Insufficient evidence, such as vague descriptions or missing proof, reduces confidence in findings and complicates remediation efforts.

[ ] No post-engagement support included in scope

Absence of post-engagement support limits the value of the assessment. Clients often need clarification, remediation guidance, and stakeholder explanations after delivery, and excluding this signals a transactional rather than risk-focused approach.

Technical Depth and Manual Testing

Manual vs automated breakdown by service line

Ask: "What's manual vs automated for internal, external, web, wireless, phishing?"	**Score**
Example Answers w/ Scoring • 1 Point: "We run industry standard tools" with no breakdown • 3 Points: Clear split by service type • 5 Points: Clear split plus examples of manual validation and chaining	
Notes	

Exploitability Validation Process

Ask: "How do you validate exploitability and impact?"	**Score**
Example Answers w/ Scoring • 1 Point: Reports tool findings only • 3 Points: Confirms exploitability on key findings • 5 Points: Demonstrates attack paths, chaining, proof, and safe validation	
Notes	

Evidence quality standards

Ask: "Do you include steps to reproduce and evidence for every finding?"	**Score**
Example Answers w/ Scoring • 1 Point: Minimal screenshots, inconsistent proof • 3 Points: Evidence for most findings • 5 Points: Repeatable steps, artifacts, and validation data for all findings	
Notes	

Handling false positives and defensive controls

Ask: "How do you handle WAF/EDR noise and false positives?"	**Score**
Example Answers w/ Scoring • 1 Point: Blames environment • 3 Points: Has a validation process • 5 Points: Has a mature workflow and communicates blockers early	
Notes	

Tester Quality and Staffing Integrity

Named tester assignment and bios upfront

Ask: "Who will test. Can we see resumes/bios?"	**Score**
Example Answers w/ Scoring • 1 Point: "We'll assign resources later" • 3 Points: Names provided before kickoff • 5 Points: Named lead + team, bios, and relevant experience shown	
Notes	

Seniority of hands-on testers

Ask: "Will interns/juniors do hands-on testing?"	**Score**
Example Answers w/ Scoring • 1 Point: Heavy junior staffing, unclear oversight • 3 Points: Mixed team with oversight • 5 Points: Senior testers perform core testing, juniors limited to support tasks	
Notes	

Relevant experience in your environment

Ask: "How many similar engagements have the lead tester run?"	**Score**
Example Answers w/ Scoring • 1 Point: No direct examples • 3 Points: Some comparable work • 5 Points: Many directly comparable, with lessons learned and patterns	
Notes	

Employment model and QA controls

Ask: "Employees vs subcontractors. How do you ensure quality?"	**Score**
Example Answers w/ Scoring • 1 Point: Unknown subcontractors, no QA • 3 Points: Some QA process • 5 Points: Strong internal QA, peer review, consistent delivery standards	
Notes	

Communication and Tester Access

Direct access to the tester during testing

Ask: "Do we communicate with the tester directly?"	**Score**
Example Answers w/ Scoring • 1 Point: "PM-only communication" • 3 Points: Limited access via scheduled calls • 5 Points: Direct channel (Teams/Cell/email) with defined response times	
Notes	

Live check-ins and mid-engagement updates

Ask: "Do you do mid-engagement reviews?"	**Score**
Example Answers w/ Scoring • 1 Point: Kickoff and final only • 3 Points: At least one midpoint check-in • 5 Points: Regular check-ins plus dynamic scoping based on findings	
Notes	

Critical finding escalation speed

Ask: "How fast do you notify us of critical findings?"	**Score**
Example Answers w/ Scoring • 1 Point: Only in final report • 3 Points: Within 24–48 hours • 5 Points: Same day notification with evidence and recommended next steps	
Notes	

Post-test support and remediation availability

Ask: "Can we meet with the tester after delivery?"	**Score**
Example Answers w/ Scoring • 1 Point: Minimal availability • 3 Points: One closeout call • 5 Points: Multiple sessions included and responsive follow-ups	
Notes	

Reporting & Post Engagement Support

Report quality and remediation usefulness

Ask: "What do you deliver and how actionable is remediation?"	**Score**
Example Answers w/ Scoring • 1 Point: Compliance-style report only • 3 Points: Solid remediation notes • 5 Points: Clear, prioritized fixes, technical details & executive summary	
Notes	

Sample report review

Ask: "Can you provide a sanitized sample report?"	**Score**
Example Answers w/ Scoring • 1 Point: Refuses or provides weak sample • 3 Points: Provides one sample • 5 Points: Provides multiple relevant samples with strong detail	
Notes	

Retesting included and clearly defined

Ask: "Is retesting included. What's the SLA?"	**Score**
Example Answers w/ Scoring • 1 Point: Extra cost, unclear • 3 Points: Included for critical/high only • 5 Points: Included retest window with clear timelines and scope	
Notes	

Executive and board presentation support

Ask: "Will you present to leadership/board. How many sessions included?"	**Score**
Example Answers w/ Scoring • 1 Point: "We can" but not included • 3 Points: Included once • 5 Points: Included multiple times, tailored messaging, Q&A support	
Notes	

General Testing and Program Maturity

Rules of Engagement and Safety Controls

Ask: "How do you prevent outages, account lockouts, or disruptions during testing?	**Score**
Example Answers w/ Scoring • 1 Point: No clear ROE, vague "we're careful," no safety specifics • 3 Points: Basic ROE and coordination plan, limited detail on safeguards • 5 Points: Formal ROE, defined guardrails w/ escalation paths well defined	
Notes	

Data Handling and Confidentiality

Ask: "How do you handle sensitive data found during testing. How long is it stored?"	**Score**
Example Answers w/ Scoring • 1 Point: Unclear storage/retention, weak controls, no defined retention policy • 3 Points: Has a retention period and access control, moderate detail • 5 Points: Clear policy, least-privilege access, defined retention/deletion timeline	
Notes	

Risk Rating and Remediation Guidance Quality

Ask: "How do you determine severity and prioritize remediation?"	**Score**
Example Answers w/ Scoring • 1 Point: CVSS-only or generic severity. Generic remediation text • 3 Points: Combines severity with context. Decent remediation guidance • 5 Points: Context-based severity with business impact clearly defined.	
Notes	

Deliverable Turnaround Time and Review Process

Ask: "What's the timeline for report delivery? Do we get to review before finalization?"	**Score**
Example Answers w/ Scoring • 1 Point: Long or undefined timelines. No review meeting • 3 Points: Defined timeline. Review meeting available • 5 Points: Clear draft/final timeline, includes live report review with the tester	
Notes	

VENDOR INTERVIEW SCRIPT

Sample Introduction

Thanks for taking the time today. We're currently evaluating multiple penetration testing vendors for internal/external, web app, wireless, and phishing simulation services. Our goal is to understand how manual your testing is, who the actual testers are, how we communicate during and after the engagement, and what deliverables and executive support you provide. I'll ask a consistent set of questions and leave time for follow-ups."

CORE QUESTIONS

By asking in this order, they will follow the scoring criteria above.

Methodology overview

"Walk me through your methodology for internal, external, web app, wireless, and phishing. What parts are manual versus automated in each? What tools do you typically use, and what do you do manually that the tools do not? Do you chain issues together into attack paths. Can you give an example of what that looks like in a real engagement?"

Validation and exploitability

"How do you validate exploitability and real-world impact instead of reporting tool output?"

Evidence and reproducibility

"For each finding, what evidence do you provide. Steps to reproduce, screenshots, logs, request/response pairs, command output?"

False positives and defensive controls

"How do you handle false positives and environmental constraints like EDR, WAFs, segmentation, or proxies?"

Who will test

"Who exactly will be assigned to our engagement. Can you share the names and bios or resumes of the actual testers in advance?"

Seniority and staffing

"Will any interns or junior staff perform hands-on testing. If yes, what tasks are they allowed to do versus senior testers?"

Lead tester experience

"How many years of hands-on offensive testing does the lead tester have, and how many similar engagements have they personally led?"

Employees vs subcontractors

“Are your testers employees or subcontractors. If subcontractors are used, how do you vet them and ensure quality?”

Direct access to tester during the test

“During the engagement, will we have direct access to the tester. If yes, what communication channel and what response time should we expect?”

Status updates and check-ins

“Do you do mid-engagement check-ins. How often, and what do you cover in those updates?”

Escalation process for critical findings

“If you find a critical issue, how quickly do you notify us and what does that escalation look like?”

Post-Test Support & Remediation

“What does after the engagement look like? Are we able to meet with the tester after the test has concluded? If so, how far after the engagement? Reports can take time to digest, so what does the process look like if we have questions 3/6/9 months down the road?”

Deliverables

“What deliverables do we receive. Executive summary, technical detail, remediation guidance, attack path diagrams, coverage mapping?”

Sample reports

“Can you provide sanitized sample reports relevant to our environment, including web app and internal network examples?”

Retesting

“Do you include retesting by default. What’s included, what’s excluded, and what’s the timeline?”

Post-engagement support

“After the assessment, will the lead tester be available for remediation calls, and will you present results to executives and our board. How many sessions are included?”

Rules of engagement and safety controls

“What are your rules of engagement and safety controls. How do you prevent outages, account lockouts, or service disruption during testing?”

Data handling and evidence protection

“How do you handle sensitive data found during testing. Where is evidence stored, how long is it retained, and how is it secured?”

Risk rating and remediation prioritization

“How do you determine severity and prioritize remediation. Do you provide specific fix guidance tailored to our environment?”

Report timeline and review process

“What’s your timeline for draft and final reports, and do we get a report review meeting with the tester before finalization?”

Sample Closeout

Thanks, as for next steps, please send your proposal including scope, timeline, assigned tester bios, sample report(s), and confirmation of tester access during and after the engagement, plus executive/board presentation support.