PENTESYS

Penetration Test Scoping Workbook

An editable working document for defining objectives, authorised targets, safety controls, responsibilities and acceptance before testing begins



Use this workbook before requesting or approving a penetration test. It helps buyers, system owners and testing providers identify assumptions early, compare proposals consistently and establish a safe, useful engagement.

Important: completing this workbook does not authorise testing. Active scanning, exploitation or other testing may begin only after the relevant system owner has provided explicit written permission and the final scope and rules of engagement have been approved.

Organisation	Click or tap here to enter text
Engagement or project	Click or tap here to enter text
Workbook owner	Click or tap here to enter text
Version	0.1
Prepared on	Click or tap here to enter text
Target test window	Click or tap here to enter text

How to use this workbook

Complete the sections collaboratively. The business owner should explain the decision the test must support; technical owners should confirm the systems and dependencies; the security or assurance owner should agree evidence needs; and the testing provider should challenge gaps before pricing and scheduling are fixed.

Suggested working sequence

Done	Check	Owner or evidence
☐	Name the assurance decision and the people who will rely on it.	
☐	Map the service, data flows, identities, dependencies and third parties.	
☐	Record every in-scope target and obtain written authority from its owner.	
☐	Agree safety controls, prohibited actions, escalation routes and stop conditions.	
☐	Confirm access, test data, monitoring, recovery and other prerequisites.	
☐	Agree outputs, severity approach, remediation support and retest terms.	
☐	Resolve assumptions and complete final technical and business approval.	

Status key

Draft	Information is incomplete or awaiting validation.
Ready for provider review	The buyer believes the scope is complete enough to challenge and price.
Approved	The authorised owner and provider have agreed the controlled engagement documents.

Keep the approved scope and rules of engagement with the contract or statement of work. Record subsequent changes rather than silently replacing the agreed boundary.

1 Assurance objective and success criteria

Start with the decision. A list of assets can define where a tester may operate, but it does not explain what the engagement must establish.

Why is the test being commissioned	Click or tap here to enter text
Decision the result must support	Click or tap here to enter text
Business services or processes affected	Click or tap here to enter text
Primary stakeholders	Click or tap here to enter text
External requirement or deadline	Click or tap here to enter text
What a useful outcome looks like	Click or tap here to enter text
Known concerns or hypotheses	Click or tap here to enter text

Success checks

Done	Check	Owner or evidence
☐	The objective is expressed as a decision or assurance question.	
☐	The intended report audiences are identified.	
☐	Important business workflows and data are named.	
☐	The expected depth is proportionate to the decision.	
☐	Any customer, regulatory, certification or contractual requirement is recorded.	

2 Service map and dependencies

Describe the complete service before reducing it to test targets. Include components that may be out of scope but could affect coverage or safety.

Service or product name	Click or tap here to enter text
Service owner	Click or tap here to enter text
Business purpose	Click or tap here to enter text
Critical user journeys	Click or tap here to enter text
Sensitive data handled	Click or tap here to enter text
Hosting and environments	Click or tap here to enter text
Architecture reference	Click or tap here to enter text

Dependency register

Component or supplier	Purpose	Owner	In scope	Notes
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	

Do not infer permission from connectivity, a commercial relationship or passive visibility. Each actively tested third-party system requires explicit written authority from its relevant owner.

3 Authorised target register

Record the precise targets the tester may touch. Attach a machine-readable asset list where the scope is large, while keeping ownership and authority traceable here.

Target or range	Type and environment	Owner	Authority evidence	Limits or exclusions

Boundary checks

Done	Check	Owner or evidence
☐	Production, staging, development and disaster-recovery environments are distinguished.	
☐	Domains, IP ranges, applications, APIs, cloud accounts and mobile builds are versioned.	
☐	Shared hosting, managed services and third-party components are identified.	
☐	Explicit exclusions and areas not tested are documented.	
☐	Written authority can be evidenced for every active target.	

4 Identities roles and business flows

Access level and business context determine what the test can establish. Provide accounts that represent important roles without exposing real credentials or unnecessary personal data.

Role or journey	Access level	Test account	MFA route	Expected restrictions

Priority business flows	Click or tap here to enter text
Privilege boundaries to validate	Click or tap here to enter text
Account provisioning owner	Click or tap here to enter text
Account expiry or clean-up plan	Click or tap here to enter text

Identity checks

Done	Check	Owner or evidence
☐	Accounts cover the roles needed to test important authorisation boundaries.	
☐	MFA, federation and password-reset routes can be exercised safely.	
☐	Test accounts contain no unnecessary live personal or payment data.	
☐	Account lockout and abuse controls are understood before testing.	

5 Rules of engagement

Translate permission into safe operating rules. The final rules of engagement should be agreed with the testing provider and approved before any active testing begins.

Permitted testing dates and times	Click or tap here to enter text
Time zone	Click or tap here to enter text
Source IP addresses	Click or tap here to enter text
Rate or concurrency limits	Click or tap here to enter text
Permitted techniques	Click or tap here to enter text
Prohibited techniques	Click or tap here to enter text
Production constraints	Click or tap here to enter text
Data access and retention limits	Click or tap here to enter text
Out-of-hours arrangements	Click or tap here to enter text

Common controls to decide explicitly

Done	Check	Owner or evidence
☐	Denial-of-service, stress and destructive techniques are prohibited unless separately authorised.	
☐	Social engineering and physical testing are excluded unless expressly included.	
☐	Persistence, pivoting and access to connected systems have defined limits.	
☐	Sensitive findings and evidence have an approved secure communication route.	
☐	The tester knows what to do if real compromise or unlawful content is discovered.	

6 Monitoring recovery and stop conditions

The customer must be able to observe the environment, respond to unexpected impact and contact an empowered person throughout the agreed test window.

Role	Name	Primary contact	Backup contact	Availability
Business owner				
Technical owner				
Security monitoring				
Incident or escalation				
Testing provider lead				

Monitoring arrangements	Click or tap here to enter text
Backup and recovery readiness	Click or tap here to enter text
Service health indicators	Click or tap here to enter text
Immediate stop conditions	Click or tap here to enter text
Who can pause the test	Click or tap here to enter text
Restart approval process	Click or tap here to enter text

Escalation severity

Level	Example trigger	Notify within	Route
Critical	Material compromise or credible service impact		
High	Serious exploitable weakness requiring prompt action		
Operational	Access, availability or scope issue		

7 Access context test data and prerequisites

Record what must be ready before the start date. Missing prerequisites should trigger an explicit decision about delay, reduced coverage or a controlled scope change.

Done	Check	Owner or evidence
☐	Architecture, data-flow and deployment information is current enough to use.	
☐	Test accounts and MFA routes are working and securely delivered.	
☐	Allow-listing, VPN or jump-host access has been tested.	
☐	Representative test data is available without unnecessary live personal data.	
☐	Logging, alerting and incident response contacts are ready.	
☐	Backups and restoration arrangements have been checked where relevant.	
☐	Internal change freezes, release windows and supplier dependencies are known.	

Prerequisite	Owner	Due date	Status	Evidence or notes

8 Testing approach and depth

Ask the provider to explain how the chosen approach answers the assurance question. Tooling and methodology matter, but neither should substitute for a clear account of coverage, judgement and limitations.

Proposed assessment type	Click or tap here to enter text
Automated coverage	Click or tap here to enter text
Human investigation	Click or tap here to enter text
Business-logic testing	Click or tap here to enter text
Attack-path or chaining expectations	Click or tap here to enter text
Methodologies or standards	Click or tap here to enter text
Relevant provider accreditation	Click or tap here to enter text
Required consultant experience	Click or tap here to enter text
Quality-assurance process	Click or tap here to enter text

Provider challenge questions

Done	Check	Owner or evidence
☐	The provider explains what the proposed effort can and cannot establish.	
☐	Coverage is matched to technologies, roles and important workflows.	
☐	Human expertise is used where judgement, chaining or business logic matters.	
☐	Assumptions about access, documentation and test data are visible.	
☐	Untested areas and limitations will be recorded in the final report.	

9 Evidence reporting remediation and retesting

Agree the complete route from finding to verified closure before work begins. A report is useful only if the right people can understand, own and act on its evidence.

Done	Check	Owner or evidence
☐	Material findings are notified during testing through a secure route.	
☐	Technical findings include reproducible evidence and affected scope.	
☐	Severity includes a transparent rationale and relevant business context.	
☐	The report separates tested scope, exclusions, constraints and limitations.	
☐	Executives receive a proportionate summary of consequences and decisions.	
☐	Remediation guidance is specific enough for an owner to act.	
☐	Retest eligibility, timing, included effort and closure evidence are defined.	

Report recipients	Click or tap here to enter text
Secure delivery route	Click or tap here to enter text
Severity approach	Click or tap here to enter text
Report and evidence formats	Click or tap here to enter text
Remediation support included	Click or tap here to enter text
Retest window and conditions	Click or tap here to enter text
Closure evidence required	Click or tap here to enter text
Evidence retention and deletion	Click or tap here to enter text

10 Commercial assumptions and change control

Make the relationship between scope, effort, timing and price visible. If circumstances change, record the effect and obtain approval rather than relying on informal messages.

Quoted scope and effort	Click or tap here to enter text
Included services and deliverables	Click or tap here to enter text
Optional work	Click or tap here to enter text
Expenses and tax treatment	Click or tap here to enter text
Cancellation or delay terms	Click or tap here to enter text
Dependencies affecting price	Click or tap here to enter text
Assumptions affecting schedule	Click or tap here to enter text

Change register

Date	Requested change	Impact	Decision and approver

11 Final go or no go review

Complete this review before the agreed testing window. A no-go decision protects the organisation and provider when authority, safety or prerequisites are incomplete.

Done	Check	Owner or evidence
☐	The assurance objective and success criteria remain valid.	
☐	The final target register is complete and version controlled.	
☐	Explicit written authority exists for every active target.	
☐	Rules of engagement, exclusions and prohibited actions are approved.	
☐	Test accounts, access routes and test data have been verified.	
☐	Monitoring, recovery, escalation and stop arrangements are operational.	
☐	Sensitive evidence has an approved handling and deletion route.	
☐	Provider team, testing dates, deliverables and commercial assumptions are confirmed.	
☐	Material scope changes will use the agreed change-control process.	

Decision	☐ Go ☐ Conditional go ☐ No go
Conditions or unresolved items	Click or tap here to enter text
Business owner approval	Name: Date:
System owner approval	Name: Date:
Security or assurance approval	Name: Date:
Testing provider acceptance	Name: Date:
Approved scope version	Click or tap here to enter text
Approved rules of engagement version	Click or tap here to enter text

Notes and decisions

Use this page for decisions that do not fit elsewhere. Attach supporting evidence and reference it clearly rather than placing credentials, secrets or unnecessary sensitive data in this workbook.

This workbook is practical preparation guidance, not legal advice and not permission to test. Final authority, contractual terms and rules of engagement must be agreed for the specific engagement.