Checklist for Preparing for a Penetration Test Scoping Call

Define business objectives, authorized targets, operating constraints and expected reporting before agreeing the scope of a test.

Edition 2026-11-03 · Online at newyorkcomputerforensics.com/guides/penetration-test-scoping/

The first scoping call should establish what the business needs to learn and the boundaries within which testing can safely occur. A count of IP addresses or a list of domain names starts the conversation, and the team adds authority, operating constraints, third party permissions, relevant identities and a clear description of the result the organization expects to use. NIST's testing guidance treats planning and analysis as part of the assessment process itself. [NIST SP 800-115]

State the business objective and the intended audience

Explain whether the work supports a customer requirement, a regulatory obligation, a transaction, a new release, remediation verification or another decision. Identify who will use the result and what evidence they need. A vulnerability scan, a penetration test, an application review and an OT assessment answer different questions. Match the deliverable to the specific contractual or regulatory request.

Bring the requirement or request that prompted the work, together with the intended completion date and any review meeting. Ask which deliverables are needed: executive findings, technical reproduction detail, remediation guidance, a retest account or a scoped attestation. Fit proposed assurance wording to the work performed.

Inventory the targets and the owners who can authorize them

List the network ranges, domains, applications, APIs, cloud environments and other proposed targets. Identify their business and technical owners and distinguish production from development or test. Include externally hosted and third party systems, even when your organization uses them daily. Confirm what the owner and provider permit before treating a target as authorized.

For applications, describe the main functions, account roles, authentication process, sensitive workflows and important integrations. State whether source code, documentation or test accounts can be provided through a secure arrangement. Record significant exclusions and why they matter. A small target list may still contain a complex authorization model or a high consequence business function.

Describe operating and safety constraints

Identify services that must stay available, testing windows, change freezes, monitoring arrangements and systems that require a different method. Call out OT, industrial control, medical, safety or physical process dependencies. Those systems are assessed under their own approved approach and operational stop conditions. [NIST SP 800-82 Revision 3]

© 2026 Global Digital Forensics, Inc. All rights reserved.

Define who can stop the test, how that person will be reached and who can authorize resumption. Agree on the handling of an unexpected outage or a suspected active compromise discovered during testing. Identify backups and recovery arrangements relevant to the proposed work.

Prepare identities, access and rules of engagement

Identify the account roles that may be needed, their approval owner and the supported way to deliver credentials. State whether MFA, conditional access, federated identity or device restrictions affect test access.

Discuss permitted techniques and prohibited actions explicitly. The rules of engagement should address the target boundary, test sources, timing, escalation, data handling and evidence needed to demonstrate a finding. Clarify whether exploitation, privilege escalation, social engineering, data access or source code review is included. Name each activity in the rules of engagement. [NIST rules of engagement glossary]

Explain prior findings and relevant changes

Identify earlier reports, known open weaknesses, recent incidents and material changes to the environment. Record the dates and scope of prior work so the assessor can distinguish a retest from a new assessment. A previous report helps focus the conversation, and current testing examines the present state.

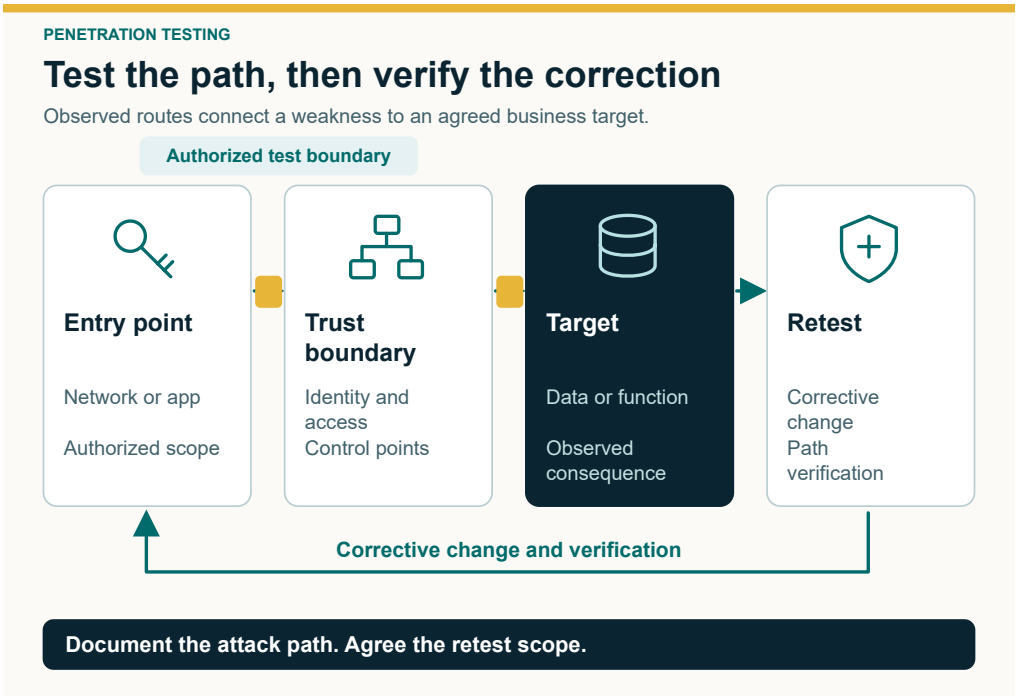
Describe planned releases, migrations or significant provider changes that could invalidate a test's assumptions. Ask whether testing should occur before or after the change and whether follow up work will be needed. If the team wants a comparison over time, agree on what can be compared and how differences in scope or access will be explained.

Agree on evidence, reporting and secure communication

Identify the people authorized to receive findings and the severity of issues that require immediate notice. Discuss how sensitive evidence will be minimized and shared. A finding demonstrates the relevant consequence within the approved scope, using the minimum client or employee information needed.

Before the call ends, confirm the remaining inputs needed for a written scope, the owner of each input and the decision date. Ask how the report will distinguish validated findings, unconfirmed observations and untested areas. Record the arrangements for remediation discussion and any retest. A successful engagement gives the business a supported account of the tested conditions and practical next steps.

© 2026 Global Digital Forensics, Inc. All rights reserved.



A test follows exposures through access to findings the report can prove.

Information Gathering Q&A Checklist

Use this Q&A with the people who own the systems and the relevant legal or business decisions. Mark unknown or not applicable answers explicitly. Record an owner, a confirming source and the date.

Record who controls access to each source and how a secure handoff can be arranged, and keep completed copies with the matter records the company maintains.

What business question should the test answer, and who will read the report?

State the objective, such as proving whether an outsider can reach payment data, and the audience for the findings.

Answer:

Owner, source, date and open questions:

Which networks, applications, APIs and cloud environments can your organization authorize?

Identify third party ownership and permission requirements.

Answer:

Owner, source, date and open questions:

© 2026 Global Digital Forensics, Inc. All rights reserved.

Which assets are hosted or managed by third parties?

List each provider and the written permission or provider policy that allows testing.

Answer:

Owner, source, date and open questions:

Which test perspective fits the objective: black box, gray box or white box?

Record what information, credentials and documentation the testers will receive.

Answer:

Owner, source, date and open questions:

Which test accounts, roles and data will be provided?

Name each account, its role and the person who will create and later disable it.

Answer:

Owner, source, date and open questions:

What are the testing window, stop conditions and escalation contacts?

Identify any OT, safety or production dependency requiring a separate approach. [NIST rules of engagement glossary]

Answer:

Owner, source, date and open questions:

What changed since the last test, and which earlier findings need retesting?

List new systems, major releases and open findings from earlier reports.

Answer:

Owner, source, date and open questions:

Who receives the findings, and how should sensitive results be delivered?

Name the recipients and the secure method for reports and evidence.

Answer:

Owner, source, date and open questions:

© 2026 Global Digital Forensics, Inc. All rights reserved.

Primary sources and further reading

Sources checked November 3, 2026.

1. NIST SP 800-115, Technical Guide to Information Security Testing and Assessment https://csrc.nist.gov/pubs/sp/800/115/final
2. NIST SP 800-82 Revision 3, Guide to OT Security https://csrc.nist.gov/pubs/sp/800/82/r3/final
3. NIST rules of engagement glossary https://csrc.nist.gov/glossary/term/Rules_of_Engagement

Scope Your Assessment

The first call is a free consultation with a senior security lead. We review the systems, the review or audit you face and its timing, and recommend the assessment depth that answers it. Requests are handled in confidence.

Call (800) 868-8189, 24/7 · New York office (212) 561-5860

Email info@evestigate.com or request your consultation at newyorkcomputerforensics.com/contact.