

Preparing for a security assessment

Reviewed: 2026-10-07

Prepare a short summary before a scoping discussion. You do not need to send confidential technical records with your first enquiry.

Prepare the essentials

1. State the question you want the assessment to answer and any decision it must support.
2. Identify the business owner and a technical contact.
3. Describe the systems involved, their purpose and any important dependencies.
4. Note recent changes, relevant previous assessments and known concerns.
5. Identify who owns each proposed target and who can authorise access or testing.
6. Explain operational restrictions, suitable testing windows and any critical services.
7. Agree how findings will be shared, who will review them and who will manage follow up.

Agree before work starts

Confirm the scope, exclusions, permissions, reporting requirements and escalation arrangements in writing. Detailed records and test access should use the agreed secure channel. Scope changes require agreement; a first enquiry does not authorise testing.

Explore Risk Assessments (<https://www.cyberxperts.co.za/services/risk-assessments>) or Penetration Testing (<https://www.cyberxperts.co.za/services/penetration-testing>). The complimentary Pre-Assessment (<https://www.cyberxperts.co.za/security-pre-assessment>) can help you identify questions for the discussion.

The fictional security testing scope scenario (<https://www.cyberxperts.co.za/resources/security-testing-scope-scenario>) explains how permission, boundaries and reporting fit together.

Further reading

NCSC penetration testing guidance (<https://www.ncsc.gov.uk/guidance/penetration-testing>) explains commissioning, scoping, reporting and follow up.