Assessment Scoping Questionnaire

Please complete the information below so KobReySec can understand the requested services and prepare an initial scope and estimate. Estimates are acceptable, and we will follow up only when clarification is needed.

1. Contact Information

Name

Company

Business email

Phone

2. What service are you looking for?

Edge Assessment: identifies and maps internet-facing assets, known vulnerabilities, outdated software, and common configuration issues. **External Infrastructure Penetration Test:** covers everything included in the Edge Assessment, then adds deeper manual testing and controlled exploitation to determine whether identified weaknesses can actually be used to compromise the environment.

- [ ] External infrastructure penetration test
- [ ] Edge assessment
- [ ] Internal infrastructure penetration test
- [ ] Wireless penetration test
- [ ] Web application penetration test
- [ ] Other service or request
- [ ] Vulnerability assessment
- [ ] Security benchmark assessment
- [ ] Configuration review
- [ ] Security awareness / social engineering
- [ ] Not sure. Please recommend an approach

3. Why are you requesting the assessment?

- [ ] Identify vulnerabilities or weaknesses
- [ ] Validate that current security controls are working
- [ ] Meet a customer, audit, or compliance requirement
- [ ] Improve overall security posture

Briefly describe the main concern, goal, or reason for testing

4. Infrastructure Assessment Scope

Complete only the sections that apply to the services selected on Page 1.

External Infrastructure Penetration Test or Edge Assessment

Approximate number of public IP addresses

Approximate number of internet domains

Public network ranges, if available

How complete is the current internet-facing asset inventory?

- [ ] Complete
- [ ] Mostly complete
- [ ] Not confident
- [ ] No inventory
- [ ] Not sure

Internal Infrastructure Penetration Test

Internal network ranges, if available

Approximate active systems

Workstations

Servers

Network devices

Other

Number of physical locations, cloud networks, or isolated segments

Can all internal systems be reached from one connection?

- [ ] Yes
- [ ] No
- [ ] Not sure

Starting access

- [ ] Network only
- [ ] Employee account
- [ ] Not sure

Vulnerability Assessment

External addresses

Internal addresses

Frequency

- [ ] One-time
- [ ] Recurring
- [ ] Not sure

Authenticated internal scanning?

- [ ] Yes
- [ ] No
- [ ] Not sure

Can all internal systems be reached from one testing connection?

- [ ] Yes
- [ ] No
- [ ] Not sure

Approximate counts are acceptable when exact inventories are unavailable.

5. Web Application Penetration Test Scope

List each application separately. For each application, provide a short summary of its purpose, approximate size, user roles, and testing environment or access method.

Application name	Purpose, approximate size, user roles, and environment/access
Example: Customer Portal	*Manages customer accounts; about 40 screens and 60 API endpoints; customer, support, and administrator roles; QA environment with IP allowlisting.*

6. Security Benchmark and Configuration Review Scope

Complete the applicable subsection below.

Security Benchmark Assessment

Technologies or environments

- [ ] Microsoft 365
- [ ] Entra ID
- [ ] Microsoft Azure
- [ ] AWS
- [ ] Windows Server
- [ ] Linux

Approximate size (users, tenants, subscriptions, servers, or cloud resources)

Preferred guidance

- [ ] CIS
- [ ] CISA
- [ ] Please recommend

Configuration Review

Technology or configuration to be reviewed

Vendor and product

Devices or clusters

Independent configurations

Approximate rules, policies, or settings

Are configurations standardized?

- [ ] Yes
- [ ] No
- [ ] Partially
- [ ] Not sure

Primary concerns or areas to emphasize

Complete only the sections that apply to the services selected.

KOBREY SEC

Assessment Scoping Questionnaire

7. Wireless Penetration Test

Number of wireless networks

Number of physical locations

City and state of locations

Are the same wireless networks and configurations used at every location?

☐ Yes ☐ No ☐ Not sure

8. Security Awareness and Social Engineering

Complete this section only if this service was selected.

Activities being considered

☐ Simulated phishing ☐ Controlled sign-in simulation ☐ Removable media ☐ Telephone or text message ☐ Not sure

Approximate participants

Number of scenarios

Employee groups or departments

Scenario development ☐ Collaborate with KobReySec ☐ KobReySec proposes scenarios ☐ Not sure

Groups, themes, or topics to include or avoid

9. Timing and Requirements

Preferred start date or timeframe

Required completion date, if any

Testing restrictions, blackout periods, or special access requirements

Are any in-scope systems owned, hosted, or managed by another organization?

☐ No ☐ Yes ☐ Not sure

Customer, audit, compliance, or regulatory requirement

10. Anything Else We Should Know?

Submission does not authorize testing. Final scope, schedule, and written authorization are required before testing begins.