



# Penetration Test Scope Worksheet

<company name>

Draft 1.0

1. What are the target organization's biggest security concerns:

(Examples include disclosure of sensitive information, interruption of production processing, embarrassment due to website defacement, etc.)

2. Please list specific hosts, network address ranges, or applications that should be tested:

3. Please list specific hosts, network address ranges, or applications that should explicitly NOT be tested:

4. Please list any third parties that own systems or networks that are in scope as well as which systems they own (written permission must have been obtained in advance by the target organization):

5. Will the test be performed against a live production environment or a test environment:

6. Will the penetration test include the following testing techniques: (Y/N)

- Ping sweep of network ranges:
- Port scan of target hosts:
- Vulnerability scan of targets:
- Penetration into targets:
- Application-level manipulation:
- Client-side Java/ActiveX reverse engineering:
- Physical penetration attempts:
- Social engineering of people:
- Other:

7. Will penetration test include internal network testing:

If so, how will access be obtained:

8. Are client/end-user systems included in scope:

If so, how may clients be leveraged:

9. Is social engineering allowed:

If so, how may it be used:

10. Are Denial of Service attacks allowed:

11. Are Dangerous checks/exploits allowed:

Signature of Primary Contact representing Target Organization

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature of Head of Penetration Testing Team

\_\_\_\_\_  
Date

Please return this completed form to [GetEventLog](#).