Security Assessment Proposal

Rules of Engagement

During the test, the following individuals will serve as contact points for the assessment team:

[list of people with name, phone, email, and any other contact information as appropriate who will interface with the client organization]

The following individuals will serve as contact points for [organization name] for the assessment team:

[list of people with name, phone, email, and any other contact information as appropriate who will interface with the assessment team]

The assessment will take place from [start date] to [end date] during [hours of testing permitted]

The following individuals/groups will be made aware of the assessment:

[list of people and groups who will be informed of the test, along with how often and to what level they will be updated]

The following points of information will be provided to the assessment team prior to the start of the assessment:

[list of specific points of information that will be given to the assessment team]

In order to discover vulnerabilities in the resources specified above, the following techniques may be utilized:

[list of penetration techniques that can be used, such as various scans, exploits, social engineering, testing physical security, etc.]

Project Scope

Generally speaking. the proposed assessment will be tailored towards the following areas of concern for [organization name]:

[list of security concerns ranked in order of importance]

These areas of concern are specifically located in the following systems, and will be subjects of the proposed assessment:

[list of resources to test, including domain/ip spaces, physical systems, environments, etc. Restrictions on things like accessing protected information or touching highly critical production systems should also be mentioned here as sub-bullet points of the specific resource, or simply stated if the test is a very black-box approach]

Permission to carry out the assessment will also be required from the following third parties whose resources will be affected by this test:

[list of third parties such as cloud hosting companies, ISP's, contracted systems, etc. that need to give permission, along with specific systems that will be affected for each party]

The assessment will take place utilizing the following environments:

[list of mediums through which the systems will be tested, such as on-site, over remote networks, on local networks, etc.]

[Organization Logo]

Memorandum for File

Subject: Vulnerability Assessment and Penetration Testing Authorization

Date: MMDDYY

The purpose of this memo is to grant authorization to specific members of our information security team to conduct vulnerability assessments and penetration tests against this organization's assets. To that end, the undersigned attests to the following:

1) [Names of testers] have permission to perform the following actions against specified resources owned or leased by [client organization] to find vulnerabilities and measure the risk of said vulnerabilities to [client organization]

These actions are:

[permissible actions and resources that can be affected by them]

This permission is granted for from [start date] until [end date].

2) [Name of approver] has the authority to grant this permission for testing the organization's Information Technology assets.

Signature: _____ Signature: _____

[Name of Approver] [Name of Test Team Lead]

[Title of Approver] [Title of Test Team Lead]

Date: _____ Date: _____

Security Assessment Report

Executive Summary

Between [start date] and [end date], the assessment team performed a series of assessments to measure certain security aspects of [organization name]. The assessment was made to address the following security concerns:

[non-technical description of security concerns, ranked in order of importance]

In accordance with the above concerns, the following resources were assessed

[brief, general description of resources tested]

In the assessment, the following vulnerabilities and their potential impacts were discovered:

[list of security vulnerabilities found in brief, non-technical descriptions, along with a description of what could happen if the vulnerability is exploited]

To mediate these risks, the following steps can be taken:

[list of steps that can be taken to resolve vulnerabilities, in brief non-technical terms]

This form borrowed general outline principles from:
https://www.owasp.org/images/1/19/OTGv4.pdf

Assessment Details

The purpose of the assessment was to address the following areas of concern:

[list of security concerns, ranked by importance. Can be technical in nature]

These areas of concern are specifically located in the following systems, and were the subjects of the proposed assessment:

[list of resources tested, including domain/ip spaces, physical systems, environments, etc. Restrictions on things like accessing protected information or touching highly critical production systems should also be mentioned here as sub-bullet points of the specific resource, or simply stated if the test is a very black-box approach]

Permission to carry out the assessment was obtained rom the following third parties whose resources were affected by this test:

[list of third parties such as cloud hosting companies, ISP's, contracted systems, etc. that needed to give permission, along with specific systems that will be affected for each party]

The assessment utilized the following environments:

[list of mediums through which the systems were tested, such as on-site, over remote networks, on local networks, etc.]

The assessment began on [start date, time] and ended on [end date, time], and took place during [hours of assessment].

A timeline of each day's planned activities, and a brief description of each day's findings, is given below:

[list of activities to be performed during each day of the test, along with brief-nontechnical descriptions of the discoveries, with the dates in chronological order]

This form borrowed general outline principles from:
https://www.owasp.org/images/1/19/OTGv4.pdf

Assessment Results

The vulnerabilities discovered, the possible damage of each vulnerability, and possible solutions to the vulnerability, are given below in order of importance based on the previously mentioned security concerns:

[list of vulnerabilities, in technical detail, along with the possible impacts is given in order of importance based on the previously mentioned security concerns. The possible solutions are listed after the potential impact, in technical detail]

This form borrowed general outline principles from:
https://www.owasp.org/images/1/19/OTGv4.pdf