**Security Assessment Plan**

# Introduction

Federal Information Security Modernization Act (FISMA) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for (client name) Testing security controls is an integral part of the FISMA security authorization requirements. Providing a plan for security control ensures that the process runs smoothly.

The (name of system) will be assessed by an Independent Assessor (IA) of (name of your company). The use of an independent assessment team reduces the potential for conflicts of interest that could occur in verifying the implementation status and effectiveness of the security controls. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39, Managing Information Security Risk states:

Assessor independence is an important factor in: (i) preserving the impartial and unbiased nature of the assessment process; (ii) determining the credibility of the security assessment results; and (iii) ensuring that the authorizing official receives the most objective information possible in order to make an informed, risk-based, authorization decision.

## Purpose

This document consists of a test plan to test the security controls for (name of system). It has been completed by (Name of your organization) for the benefit of (name of client) NIST SP 800-39, Managing Information Security Risk states:

The information system owner and common control provider rely on the security expertise and the technical judgment of the assessor to: (i) assess the security controls employed within and inherited by the information system using assessment procedures specified in the security assessment plan; and (ii) provide specific recommendations on how to correct weaknesses or deficiencies in the controls and address identified vulnerabilities.

# Methodology

(Name of your organization) will perform an assessment of the (name of system) security controls using the methodology described in NIST SP 800-53A. (Your organization) will use NIST SP 800-53A test procedures to evaluate the security controls. Contained in Excel worksheets, these test procedures contain the test objectives and associated test cases to determine if a control is effectively implemented and operating as intended. The results of the testing shall be recorded in the worksheets (provided in Appendix A) along with information that notes whether the control (or control enhancement) is satisfied or not.

Your organization data gathering activities will consist of the following:

* Request (name of agency) to provide NIST required documentation.
* Request any follow-up documentation, files, or information needed that is not provided in NIST required documentation
* Site visit to the (agency) sites as necessary to inspect systems and meet with (name of agency) staff.
* Obtain information through the use of security testing tools

Security controls will be verified using one or more of the following assessment methods:

* Examine: the IA will review, analyze, inspect, or observe one or more assessment artifacts as specified in the attached test cases
* Interview: the IA will conduct discussions with individuals within the organization to facilitate assessor understanding, achieve clarification, or obtain evidence
* Technical Tests: the IA will perform technical tests, including on system components using manual methods

# Test Plan

## Security Assessment Team

The security assessment team consists of individuals from (name of your organization) which are located at the following address: (put address here).Information about (name of your company) can be found at the following URL:

Security control assessors play a unique role in testing system security controls. NIST SP 800-39, Managing Information Security Risk states:

*The security control assessor is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system).*

The members of the IA security testing team are found in Table 5‑1 Security Testing Team.

Table ‑ Security Testing Team

| Name | Role | Contact Information |
| --- | --- | --- |
|  | Team Lead / Assessor Manager |  |
|  | Security Assessor |  |
|  | Security Assessor |  |
|  |  |  |
|  |  |  |

## Schedule

The security assessment testing schedule can be found in Table 5‑5 Testing Schedule below.

Table ‑ Testing Schedule

| Task Name | Start Date | Finish Date |
| --- | --- | --- |
| Kick-off Meeting | **11/2/2018** | **11/2/2018** |
| Develop Draft SAP | **11/2/2018** | **11/30/2018** |
| Meeting to Review SAP | **11/26/2018** | **11/26/2018** |
| Finalize SAP | **11/30/2018** | **11/30/2018** |
| Review (Agency name) Documentation | **11/9/2018** | **12/3/2018** |
| Conduct Interviews of (Agency name) Staff | **12/3/2018** | **12/7/2018** |
| Perform Testing | **12/3/2018** | **12/21/2018** |
| Develop Draft SAR | **1/2/2019** | **1/10/2019** |
| Draft SAR Delivered to Client | **1/10/2019** | **1/10/2019** |
| Issue Resolution Meeting | **1/11/2019** | **1/11/2019** |
| Finalize SAR | **1/11/2019** | **1/14/2019** |
| Send Final Version of SAR Agency Provider and ISSO | **1/14/2019** | **1/14/2019** |

Disclosures

Any testing will be performed according to terms and conditions designed to minimize risk exposure that could occur during security testing.

Security Testing May Include

Security testing may include the following activities:

* Interviews of Agency Personnel
* Examinations of policies and procedures
* Examination of records
* Examination of system documentation
* Testing of implemented security mechanisms/solutions
* Creation, modification, and/or deletion of accounts for testing purposes
* Reviews of configurations on production systems as a live test alternative

Security Testing Will Not Include

Security testing will not include any of the following activities:

* Changes to assigned user passwords
* Intentional modification of user files or system files
* Telephone modem probes and scans (active and passive)
* Intentional viewing of agency staff email, Internet caches, and/or personnel cookie files
* Intentional Denial of service attacks
* Exploits that will introduce new weaknesses to the system
* Intentional introduction of malicious code (viruses, Trojans, worms, etc.)

## End of Testing

(Name of your company) will notify name of Agency POC at (Name f Agency) when security testing has been completed.

## Communication of Test Results

Email and reports on all security testing will be encrypted according to Agency requirements. Security testing results will be sent and disclosed to the Key Agency POC defined to receive Test Results within 30 days after security testing has been completed.

## Limitation of Liability

Name of your organization, and its stated partners, shall not be held liable to (name of Agency) for any and all liabilities, claims, or damages arising out of or relating to the security vulnerability testing portion of this agreement, howsoever caused and regardless of the legal theory asserted, including breach of contract or warranty, tort, strict liability, statutory liability, or otherwise.

(Name of Agency) acknowledges that there are limitations inherent in the methodologies implemented, and the assessment of security and vulnerability relating to information technology is an uncertain process based on past experiences, currently available information, and the anticipation of reasonable threats at the time of the analysis. There is no assurance that an analysis of this nature will identify all vulnerabilities or propose exhaustive and operationally viable recommendations to mitigate all exposure.