

IT 727 Cybersecurity Risk management

system name security ASSESSMENT REPORT (SAR)

date

Prepared by

|  |  |  |
| --- | --- | --- |
| **Identification of Organization that Prepared this Document** | | |
|  | Organization Name | <Enter Company/Organization>. |
| Street Address | <Enter Street Address> |
| Suite/Room/Building | <Enter Suite/Room/Building> |
| City, State Zip | <Enter Zip Code> |

Prepared for

|  |  |  |
| --- | --- | --- |
| **Identification of Cloud Service Provider** | | |
|  | Organization Name | <Enter Company/Organization>. |
| Street Address | <Enter Street Address> |
| Suite/Room/Building | <Enter Suite/Room/Building> |
| City, State Zip | <Enter Zip Code> |

TABLE OF CONTENTS

[1. Information System Name/Title/ABBREVIATION 4](#_Toc36485701)

[2. System Overview 4](#_Toc36485702)

[2.1. Security Categorization 4](#_Toc36485703)

[2.2. System Description 4](#_Toc36485704)

[2.3. Purpose of System 4](#_Toc36485705)

[3. Assessment Methodology 4](#_Toc36485706)

[3.1. Perform Tests 4](#_Toc36485707)

[3.1.1. Assessment Deviations 4](#_Toc36485708)

[3.2. Identification of Vulnerabilities 5](#_Toc36485709)

[3.3. Consideration of Threats 5](#_Toc36485710)

[3.4. Perform Risk Analysis 6](#_Toc36485711)

[3.5. Recommend Corrective Actions 7](#_Toc36485712)

[3.6. Document Results 7](#_Toc36485713)

[4. Risk Exposure Table 7](#_Toc36485714)

[4.1. Security Assessment Summary 10](#_Toc36485715)

[5. Non-Conforming Controls 10](#_Toc36485716)

[5.1. Risks Corrected During Testing 10](#_Toc36485717)

[5.2. Risks with Mitigating Factors 10](#_Toc36485718)

[5.3. Risks Remaining Due to Operational Requirements 11](#_Toc36485719)

[6. Risks Known for Interconnected Systems 12](#_Toc36485720)

[7. Authorization Recommendation 12](#_Toc36485721)

List of Tables

[Table 1‑1. Information System Name and Title 4](#_Toc36485722)

[Table 3‑1 List of Assessment Deviations 4](#_Toc36485723)

[Table 3‑2 Threat Categories and Type Identifiers 5](#_Toc36485724)

[Table 3‑4 Likelihood Definitions 6](#_Toc36485725)

[Table 3‑5 Impact Definitions 6](#_Toc36485726)

[Table 3‑6 Risk Exposure Ratings 7](#_Toc36485727)

[Table 5‑1 Summary of Risks Corrected During Testing 10](#_Toc36485728)

[Table 5‑2 Summary of Risks with Mitigating Factors 10](#_Toc36485729)

[Table 5‑3 Summary of Risks Remaining Due to Operational Requirements 11](#_Toc36485730)

[Table 6‑1 Risks from Interconnected Systems 12](#_Toc36485731)

[Table 7‑1 Risk Mitigation Priorities 12](#_Toc36485732)

# Information System Name/Title/ABBREVIATION

Table 1‑1. Information System Name and Title

| Information System Name | Information System Abbreviation |
| --- | --- |
| Information System Name | Enter Information System Abbreviation |

# System Overview

## Security Categorization

The Information System Abbreviation is categorized as a <choose level> impact system. The Information System Abbreviation categorization was determined in accordance with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.

## System Description

## Purpose of System

# Assessment Methodology

## Perform Tests

Third Party Assessment Organization performed security tests on the Information System Abbreviation, which were concluded on <date>. The SAP separately documents the schedule of testing, which <was/was not> adjusted to provide an opportunity for correcting identified weaknesses and re-validation of those corrections. The results of the tests are recorded in the Security Test Procedures workbooks which are identified in Appendix B Security Test Procedure Workbooks. The findings of the security tests serve as inputs to this SAR. A separate penetration test was performed, with the results documented in a formal Penetration Test Report that is described as an attachment template in Appendix J to this SAR.

## Assessment Deviations

Third Party Assessment Organization performed security tests on the Information System Name and the tests concluded on <date>. The Table 3‑1 List of Assessment Deviations below contains a list of deviations from the original plan for the assessment presented in the SAP.

Table 3‑1 List of Assessment Deviations

| Deviation ID | Deviation Description | Justification |
| --- | --- | --- |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |
| 6 |  |  |

## Identification of Vulnerabilities

Vulnerabilities have been identified by Third Party Assessment Organization for the Information System Abbreviation through security control testing. The results of the security control testing are recorded in the Security Test procedures workbooks and the SAP.

A vulnerability is an inherent weakness in an information system that can be exploited by a threat or threat agent, resulting in an undesirable impact on the protection of the confidentiality, integrity, or availability of the system (application and associated data). A vulnerability may be due to a design flaw or error in configuration which makes the network, or a host on the network, susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in multiple areas of the system or facilities, such as in firewalls, application servers, web servers, operating systems or fire suppression systems.

Whether or not a vulnerability has the potential to be exploited by a threat depends on a number of variables including (but not limited to):

* The strength of the security controls in place
* The ease at which a human actor could purposefully launch an attack
* The probability of an environmental event or disruption in a given local area

An environmental disruption is usually unique to a geographic location. Depending on the level of the risk exposure, the successful exploitation of a vulnerability can vary from disclosure of information about the host to a complete compromise of the host. Risk exposure to organizational operations can affect the business mission, functions, and/or reputation of the organization.

The vulnerabilities that were identified through security control testing (including penetration testing) for the Information System Abbreviation are identified in the Information System Abbreviation SAR Risk Exposure Table.

## Consideration of Threats

A threat is an adversarial force or phenomenon that could impact the availability, integrity, or confidentiality of an information system and its networks including the facility that houses the hardware and software. A threat agent is an element that provides the delivery mechanism for a threat. An entity that initiates the launch of a threat agent is referred to as a threat actor.

A threat actor might purposefully launch a threat agent (e.g., a terrorist igniting a bomb). However, a threat actor could also be a trusted employee that acts as an agent by making an unintentional human error (e.g., a trusted staff clicks on a phishing email that downloads malware). Threat agents may also be environmental in nature with no purposeful intent (e.g., a hurricane). Threat agents working alone, or in concert, exploit vulnerabilities to create incidents. FedRAMP categorizes threats using a threat origination taxonomy of Purposeful (P), Unintentional (U), or Environmental (E) type threats as described in Table 3‑2 Threat Categories and Type Identifiers.

Table 3‑2 Threat Categories and Type Identifiers

|  |  |
| --- | --- |
| Threat Origination Category | Type Identifier |
| Threats launched purposefully | P |
| Threats created by unintentional human or machine | U |
| Threats caused by environmental agents or disruptions | E |

Purposeful threats are launched by threat actors for a variety of reasons and the reasons may never be fully known. Threat actors could be motivated by curiosity, monetary gain, political gain, social activism, revenge or many other driving forces. It is possible that some threats could have more than one threat origination category.

Some threat types are more likely to occur than others. FedRAMP takes threat types into consideration to help determine the likelihood that a vulnerability could be exploited. The threat table shown in Table 3‑3 Potential Threats, is designed to offer typical threats to information systems and these threats have been considered for Information System Abbreviation.

## Perform Risk Analysis

The goal of determining risk exposure is to facilitate decision making on how to respond to real and perceived risks. The outcome of performing risk analysis yields risk exposure metrics that can be used to make risk-based decisions.

The FedRAMP risk analysis process is based on qualitative risk analysis. In qualitative risk analysis the impact of exploiting a threat is measured in relative terms. When a system is easy to exploit, it has a High likelihood that a threat could exploit the vulnerability. Likelihood definitions for the exploitation of vulnerabilities are found in Table 3‑4 Likelihood Definitions.

Table 3‑4 Likelihood Definitions

| Likelihood | Description |
| --- | --- |
| Low | There is little to no chance that a threat could exploit a vulnerability and cause loss to the system or its data. |
| Moderate | There is a moderate chance that a threat could exploit a vulnerability and cause loss to the system or its data. |
| High | There is a high chance that a threat could exploit a vulnerability and cause loss to the system or its data. |

Impact refers to the magnitude of potential harm that could be caused to the system (or its data) by successful exploitation. Definitions for the impact resulting from the exploitation of a vulnerability are described in Table 3‑5 Impact Definitions. Since exploitation has not yet occurred, these values are perceived values. If the exploitation of a vulnerability can cause significant loss to a system (or its data) then the impact of the exploit is considered to be High.

Table 3‑5 Impact Definitions

| Impact | Description |
| --- | --- |
| Low | If vulnerabilities are exploited by threats, little to no loss to the system, networks, or data would occur. |
| Moderate | If vulnerabilities are exploited by threats, moderate loss to the system, networks, and data would occur. |
| High | If vulnerabilities are exploited by threats, significant loss to the system, networks, and data would occur. |

The combination of High likelihood and High impact creates the highest risk exposure. The risk exposure matrix shown in Table 3‑6 Risk Exposure Ratings presents the same likelihood and impact severity ratings as those found in NIST SP 800-30 Risk Management Guide for Information Technology Systems. Analyzing the likelihood and impact of each vulnerability, based upon the potential threats yields a Risk Exposure Table as outlined in Section 4 of this SAR.

Table 3‑6 Risk Exposure Ratings

|  |  |  |  |
| --- | --- | --- | --- |
| Likelihood | Impact | | |
| Low | Moderate | High |
| High | Low | Moderate | High |
| Moderate | Low | Moderate | Moderate |
| Low | Low | Low | Low |

Third Party Assessment Organization and CSP Name reviewed all identified weaknesses and assigned a risk to the weakness based on Table 3‑6 Risk Exposure Ratings. All identified scan risks have been assigned the risk identified by the scanning tool.

## Recommend Corrective Actions

Third Party Assessment Organization and CSP Name record and review all recommendations and corrective actions.

## Document Results

Documenting the results of security control testing creates a record of the security posture for the system at a given moment in time. The record can be reviewed for risk-based decision making and to create plans of action to mitigate risks.

FISMA requires that a Plan of Action and Milestones (POA&M) (using the format guidance prescribed by OMB) be developed and utilized as the primary mechanism for tracking all system security weaknesses and issues. CSP Name will leverage the SAR to create a POA&M for Information System Abbreviation. The POA&M is a mitigation plan designed to address specific residual security weaknesses and includes information on costing, resources, and target dates.

# Risk Exposure Table

For the most current template copy, the SAR Risk Exposure Table can be downloaded from the FedRAMP Template website: <https://www.fedramp.gov/resources/templates-2016/> . Please see SAR Appendix A: Risk Exposure Table.

Delete this instruction from your final version of this document.

The Information System Name SAR Risk Exposure Table describes all security weaknesses found during testing. The following elements for each security weakness are reported in this Table, as follows:

* Column A: Identifier
* Column B: Name
* Column C: Source of Discovery
* Column D: Description
* Column E: Affected internet protocol (IP) Address/Hostname/Database
* Column F: Applicable Threats
* Column G: Likelihood (before mitigating controls/factors)
* Column H: Impact (before mitigating controls/factors)
* Column I: Risk Exposure (before mitigating controls/factors)
* Column J: Risk Statement
* Column K: Mitigating Controls/Factors
* Column L: Likelihood (after mitigating controls/factors)
* Column M: Impact (after mitigating controls/factors)
* Column N: Risk Exposure (after mitigating controls/factors)
* Column O: Recommendation
* Column P: Justification or Proposed Remediation

The reader of the SAR must anticipate that the security weakness elements are described as indicated below.

Identifier: All weaknesses are assigned a vulnerability ID in the form of V#-Security Control ID. For example, the first vulnerability listed would be reported as V1-AC-2(2) if the vulnerability is for control ID AC-2(2). If there are multiple vulnerabilities for the same security control ID, the first part of the vulnerability identification (ID) must be incremented, for example V1-AC-2(2), V2-AC-2(2).

Name: A short name unique for each vulnerability.

Source of Discovery: The source of discovery refers to the method that was used to discover the vulnerability (e.g., web application scanner, manual testing, security test procedure workbook, interview, document review). References must be made to scan reports, security test case procedures numbers, staff that were interviewed, manual test results, and document names. All scan reports are attached in Appendices. Results of manual tests can be found in 7.Appendix G Manual Test Results. If the source of discovery is from one of the security test procedure workbooks, a reference must point to the Workbook name, the sheet number, the row number, the column number. Workbook tests results are found in 7.Appendix B Security Test Procedure Workbooks. If the source of discovery is from an interview, the date of the interview and the people who were present at the interview are named. If the source of discovery is from a document, the document must be named.

Description: All security weaknesses must be described well enough such that they could be reproduced by the CSP, the Information System Security Officer (ISSO), or the AO. If a test was performed manually, the exact manual procedure and any relevant screenshots must be detailed. If a test was performed using a tool or scanner, a description of the reported scan results for that vulnerability must be included along with the vulnerability identifier (e.g., CVE, CVSS, and Nessus Plugin ID etc.) and screenshots of the particular vulnerability being described. If the tool or scanner reports a severity level, that level must be reported in this section. Any relevant login information and role information must be included for vulnerabilities discovered with scanners or automated tools. If any security weaknesses affect a database transaction, a discussion of atomicity violations must be included.

Affected IP Address/Hostname(s)/Database: For each reported vulnerability, all affected IP addresses/hostnames/databases must be included. If multiple hosts/databases have the same vulnerability, list all affected hosts/databases.

Applicable Threats: The applicable threats describe the unique threats that have the ability to exploit the security vulnerability. (Use threat numbers from Table 3-3.)

Likelihood (before mitigating controls/factors): High, Moderate, or Low (see Table 3‑4 Likelihood Definitions).

Impact (before mitigating controls/factors): High, Moderate, or Low (see Table 3‑5 Impact Definitions).

Risk Exposure (before mitigating controls/factors): High, Moderate, or Low (see Table 3‑6 Risk Exposure Ratings).

Risk Statement: Provide a risk statement that describes the risk to the business. (See examples in <System Name Acronym> SAR Risk Exposure Table). Also indicate whether the affected machine(s) is/are internally or externally facing.

Mitigating Controls/Factors: Describe any applicable mitigating controls/factors that could downgrade the likelihood or risk exposure. Also indicate whether the affected machine(s) is/are internally or externally facing. Include a full description of any mitigating factors and/or compensating controls if the risk is an operational requirement.

Likelihood (after mitigating controls/factors): Moderate or Low (see Table 3‑4 Likelihood Definitions) after mitigating control/factors have been identified and considered.

Impact (after mitigating controls/factors): Moderate or Low (see Table 3‑5 Impact Definitions) after mitigating control/factors have been identified and considered.

Risk Exposure (after mitigating controls/factors): Moderate or Low (see Table 3‑6 Risk Exposure Ratings) after mitigating controls/factors have been identified and considered.

Recommendation: The recommendation describes how the vulnerability must be resolved. Indicate if there are multiple ways that the vulnerability could be resolved or recommendation for acceptance of operational requirement.

Justification or Proposed Remediation:

|  |  |
| --- | --- |
| <Rationale for recommendation of risk adjustment>. | <Rationale for operational requirement.> |

## Security Assessment Summary

<Number> vulnerabilities (<Number> high, <Number> moderate, and <Number> low)) discovered as part of the penetration testing were also identified in the operating system or web application vulnerability scanning. These vulnerabilities have been combined in the SAR Risk Exposure Table with the Source of Discovery column containing each of the types of testing that identified the vulnerability.

The summary is contained in the file named <System Name Acronym> SAR Risk Exposure Table, included as an Appendix A to this SAR.

# Non-Conforming Controls

In some cases, the initial risk exposure to the system has been adjusted due to either corrections that occurred during testing or to other mitigating factors.

## Risks Corrected During Testing

Risks discovered during the testing of Information System Abbreviation that have been corrected prior to authorization are listed in Table 5‑1 Summary of Risks Corrected During Testing. Risks corrected during testing have been verified by Third Party Assessment Organization. The verification method used to determine the correction of each of the identified vulnerabilities is noted in the far right-hand column of the table as “Verification Statement”.

Table 5‑1 Summary of Risks Corrected During Testing

| Identifier | Description | Source of Discovery | Initial Risk Exposure | Remediation Description | Date of Remediation | Verification Statement |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

## Risks with Mitigating Factors

Risks that have had their severity levels changed due to mitigating factors are summarized in Table 5‑2 Summary of Risks with Mitigating Factors. The factors used to justify changing the initial risk exposure rating are noted in the far right-hand column of the table. See this SAR Appendix A: <System Name Acronym> Risk Exposure Table for more information on these risks.

Table 5‑2 Summary of Risks with Mitigating Factors

| Identifier | Description | Source of Discovery | Initial Risk Exposure | Current Risk Exposure | Description of Mitigating Factors |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Risks Remaining Due to Operational Requirements

Risks that reside in the <System Name> that cannot be corrected because of operational impact to the system are summarized in Table 5‑3 Summary of Risks Remaining Due to Operational Requirements. An explanation of the operational impact and risks are included below as well as in the appropriate Security Assessment Test Cases and System Security Plan (SSP). Although these risks are not to be corrected, they are listed in this <System Name Acronym> SAR Appendix A: Risk Exposure Table, and tracked in the Plan of Action and Milestones (POA&M) as Operational Requirements.

Instruction: 3PAO must ensure that the content of this table is consistent with the same information documented in <System Name Acronym> SAR Appendix A: Risk Exposure Table.

Delete this instruction from your final version of this document.

Note: The justification that remediating a vulnerability will cause a break in functionality is not a sufficient rationale for permitting the risk to persist. There must also be full descriptions of the mitigating factors and compensating controls that address the ongoing risk to this specific system.

Table 5‑3 Summary of Risks Remaining Due to Operational Requirements

| Identifier | Description | Source of Discovery | Current Risk Exposure | Operational Requirements Rationale and Mitigating Factors |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Risks Known for Interconnected Systems

Inherent relationships between the system and other interconnected systems may impact the overall system security posture. A summary of the risks known for systems that connect to Information System Abbreviation is provided in Table 6‑1 Risks from Interconnected Systems.

Instruction: 3PAO must include any known risks with interconnected systems that they discovered. CSPs shall disclose any known risks with interconnected systems.

Delete this instruction from your final version of this document.

In order to determine this information, it may be necessary to consult other Security Assessment Reports, Interconnection Agreements, Service Level Agreements, Memorandums of Understanding, and US-CERT advisories.

Table 6‑1 Risks from Interconnected Systems

| System | Authorization Date/Status | Date of POA&M | Control Family Identifiers |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Authorization Recommendation

A total of <Number> system risks were identified for Information System Abbreviation. Of the <Number> risks that were identified, there were <Number> High risks, <Number> Moderate risks, <Number> Low risks, and <Number> of operationally required risks. Priority levels were established based on the type of vulnerability identified.

Instruction: In the space below this instruction, 3PAO must render a professional opinion of their analysis of risks for the information system based on the results from the security assessment. Any recommendations must be supported by findings, evidence, and artifacts. This recommendation will be fully reviewed by the AO.

Delete this instruction from your final version of this document.

Table 7‑1 Risk Mitigation Priorities indicates the priority of recommended risk mitigation actions for the Information System Abbreviation.

Table 7‑1 Risk Mitigation Priorities

| Priority Number | Risk Level | Identifier | Vulnerability Description |
| --- | --- | --- | --- |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |
| 8 |  |  |  |
| 9 |  |  |  |
| 10 |  |  |  |

Third Party Assessment Organization attests that the SAR from the Information System Name assessment testing provides a complete assessment of the applicable FedRAMP controls as stipulated in the SAP. Evidence to validate the successful implementation of the various security controls has been collected and validated. Based on the remaining risk as noted in <System Name Acronym> SAR Appendix A: Risk Exposure Table, and the continuous improvement of security related processes and controls, Third Party Assessment Organization recommends an authorization be granted for Information System Name.