# Reusable Component Library System Security Plan

# NIST SP 800-53 Revision 4

## RA: Risk Assessment

### RA-1: Risk Assessment Policy And Procedures

The organization:  
 a. Develops, documents, and disseminates to [Assignment: organization-defined  
personnel or roles]:  
 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities,  
management commitment, coordination among organizational entities, and compliance; and  
 2. Procedures to facilitate the implementation of the risk assessment policy  
and associated risk assessment controls; and  
 b. Reviews and updates the current:  
 1. Risk assessment policy [Assignment: organization-defined frequency]; and  
 2. Risk assessment procedures [Assignment: organization-defined frequency].

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud Service Provider dated 1 May 2013.

##### CivicActions

CivicActions has developed, documented and disseminated to personnel a risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the policy and associated controls. This information is maintained in the CivicActions Risk Assessment (RA) Policy and Procedure that can be found in the CivicActions GitHub repository at <https://github.com/CivicActions/compliance-docs/>.

##### Project

The Client follows the risk assessment policy and procedures formally documented within None. Furthermore, a Risk Assessment Plan was originally initiated to determine the extent of the potential threat and the risk associated with Project throughout its System Development Life Cycle (SDLC). The Project Risk Assessment defines the methodology approach to determine the likelihood risks, and identify potential mitigation options to reduce risks to the Project system.

The Project Risk Assessment will be conducted in accordance with the Department’s risk assessment policy and procedures. By doing so, the responsible parties associated with the Project will be able to determine the risk, likelihood and impact that could result from exploiting vulnerabilities within the system.

This is Agency common control. More data about implementation can be obtained from the Agency common control catalog.

### RA-2: Security Categorization

The organization:  
 a. Categorizes information and the information system in accordance with applicable  
federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;  
 b. Documents the security categorization results (including supporting rationale)  
in the security plan for the information system; and  
 c. Ensures that the authorizing official or authorizing official designated  
representative reviews and approves the security categorization decision.

#### a

##### Project

In accordance with FIPS 199 requirement and guidelines provided in NIST SP800-60 Rev.1, the organization categorized the system as a Low system: Confidentiality (Low), Integrity (Low), Availability (Low).

#### b

##### Project

The security categorization was determined by evaluating the type of information that is stored, processed, and/or transmitted by the application and the potential impact levels associated with the confidentiality, integrity, and availability of that information. The application’s security categorization has been documented in this SSP.

#### c

##### Project

The security categorizations have been reviewed by the designated application POCs, were approved during the C&A effort. The formal security categorization document is available upon request. The system inventory for the Project Project is revalidated semiannually.

### RA-3: Risk Assessment

The organization:  
 a. Conducts an assessment of risk, including the likelihood and magnitude of  
harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;  
 b. Documents risk assessment results in [Selection: security plan; risk assessment  
report; [Assignment: organization-defined document]];  
 c. Reviews risk assessment results [Assignment: organization-defined frequency];  
 d. Disseminates risk assessment results to [Assignment: organization-defined  
personnel or roles]; and  
 e. Updates the risk assessment [Assignment: organization-defined frequency]  
or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

#### a

##### Project

CivicActions/Project will perform risk assessments for the Project system based on SP 800-30 Rev. 1 Guide for Conducting Risk Assessments at least annually and as part of the change management activities for the Project system that warrant a new or updated risk assessment.

#### b

##### Project

The results of risk assessments will be compiled into a risk assessment report to be reviewed by CivicActions Security and relevant personnel, and also added to the GitLab system for the Project system.

#### c

##### Project

CivicActions/Project reviews risk assessment results at least annually.

#### d

##### Project

The Risk Assessment report will be disseminated to the appropriate personnel through the Project Manager and CivicActions Security.

#### e

##### Project

Risk assessments are conducted annually or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system, as defined in NIST Special Publication 800-37 Revision 1. A significant change includes:

* Changing authentication or access control implementations;
* Changing storage implementations;
* Changing a COTS product to another product;
* Changing the backup mechanisms and process; and,
* Adding new interconnections to an outside service provide.

### RA-5: Vulnerability Scanning

The organization:  
 a. Scans for vulnerabilities in the information system and hosted applications  
[Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported;  
 b. Employs vulnerability scanning tools and techniques that facilitate interoperability  
among tools and automate parts of the vulnerability management process by using standards for:  
 1. Enumerating platforms, software flaws, and improper configurations;  
 2. Formatting checklists and test procedures; and  
 3. Measuring vulnerability impact;  
 c. Analyzes vulnerability scan reports and results from security control assessments;  
 d. Remediates legitimate vulnerabilities [Assignment: organization-defined  
response times] in accordance with an organizational assessment of risk; and  
 e. Shares information obtained from the vulnerability scanning process and  
security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: vulnerability scanning.

##### Project

The Project uses vulnerability scanning software to document and determine risks to the system. These scans are run monthly and the results of these scans are being used to inform changes to the system and verify that security controls are working correctly. These scans are used to document the current state of the system, and to analyze security trends as changes are made over time.

#### a

##### CivicActions

CivicActions Operations uses vulnerability scanning software to document and determine risks to the system. Operating system and application vulnerability scans include:

* The CivicActions system environment employs the OpenSCAP scanner with the Red Hat STIG baseline to check for vulnerabilities.
* The CivicActions application environment is tested by the penetration tester OWASP ZAP, an open-source web application security scanner to report on needed updates based on known flaws.

CivicActions Operations has automated the process to perform the scans on a monthly basis. The resulting reports list vulnerabilities and rank them by severity. These reports are stored in Amazon S3 buckets and are used to inform changes to the system and verify that security controls are working correctly. These scans are used to document the current state of the system, and to analyze security trends as changes are made over time.

#### b

##### CivicActions

CivicActions employs the automated vulnerability scanning tools OpenSCAP and OWASP ZAP which are interoperable with standard web browsers, the Open Source Ansible infrastructure provisioning system and other Open Source tools.

#### c

##### CivicActions

The CivicActions Security Office reviews all vulnerabilities identified from automated scans and security assessments. “False positive” findings are documented and may be tailored out. Vulnerabilities found and deemed legitimate are assigned an impact rating and response time thought creation of an issue or ticket. The CivicActions Operations staff reviews current scans and compare with older scans to identify trends and to verify previous vulnerabilities have been mitigated.

#### d

##### CivicActions

Identified and reported vulnerabilities are assigned an impact rating and response time by CivicActions’ Security and must be remediated according to the following time requirements:

* Critical - Within 15 days of discovery (usually within 1 week))
* High - Within 30 days of discovery (usually within 1 week))
* Moderate - Within 90 days of discovery (usually within 2 weeks)
* Low - Within 180 days of discovery

#### e

##### CivicActions

Results of the vulnerability scans and security assessments are shared with all appropriate CivicActions personnel supporting continuous monitoring requirements. CivicActions Security assigns each vulnerability an impact rating and response time through JIRA or the Git issue tool for tracking to the established remediation deadlines listed in RA-5(d).