# 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/>.

### 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.

#### 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 on an audit server 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 uses the automated vulnerability scanning tools OpenSCAP and OWASP ZAP are interoperable with standard web browsers, the Open Source Ansible infrastructure provisioning system and other Open Source tools employed by CivicActions.

#### c

##### CivicActions

CivicActions’ Security Office reviews all vulnerabilities identified from automated scans and security assessments. Vulnerabilities found and deemed legitimate are assigned an impact rating and response time thought creation of an issue or ticket. 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 Office and must be remediated according to the following time requirements: • High - Within 30 days of discovery (usually within 1 week)) • Moderate - Within 90 days of discovery (usually within 2 weeks) • Low - Within 240 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).