# RISK ASSESSMENT

## RA-01 RISK ASSESSMENT POLICY AND PROCEDURES

Control description: <http://800-53.govready.com/control?id=RA-1>

Security control type: Hybrid

#### LINCS specific control or LINCS Responsibility

The Department follows the risk assessment policy and procedures formally documented within in the Department of Education Handbook for Information Technology Security Risk Assessment Procedures (Handbook OCIO-07). Furthermore, a Risk Assessment Plan was originally initiated to determine the extent of the potential threat and the risk associated with LINCS Technology Project throughout its System Development Life Cycle (SDLC). The LINCS Technology Project Risk Assessment defines the methodology approach to determine the likelihood risks, and identify potential mitigation options to reduce risks to the LINCS Technology Project system.

The LINCS Technology 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 LINCS Technology 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.

Additional information is contained within the Department of Education Handbook for Information Technology Security Risk Assessment Procedures (Handbook OCIO-07).

#### CivicActions Responsibility

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 CivicActions that can be found in the CivicActions Github repository at <https://github.com/CivicActions/compliance-docs/>.

#### Amazon Web Services (AWS) US-East/West control support

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

## RA-02 SECURITY CATEGORIZATION

Control description: <http://800-53.govready.com/control?id=RA-2>

Security control type: Hybrid

### Part a)

#### LINCS specific control or LINCS Responsibility

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).

### Part b)

#### LINCS specific control or LINCS Responsibility

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.

### Part c)

#### LINCS specific control or LINCS Responsibility

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 LINCS Technology Project is revalidated semiannually.

## RA-03 RISK ASSESSMENT

Control description: <http://800-53.govready.com/control?id=RA-3>

Security control type: Hybrid

### Part a)

#### LINCS specific control or LINCS Responsibility

CivicActions/LINCS will perform risk assessments for the LINCS 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 LINCS system that warrant a new or updated risk assessment.

### Part b)

#### LINCS specific control or LINCS Responsibility

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 LINCS system.

### Part c)

#### LINCS specific control or LINCS Responsibility

CivicActions/LINCS reviews risk assessment results at least annually.

### Part d)

#### LINCS specific control or LINCS Responsibility

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

### Part e)

#### LINCS specific control or LINCS Responsibility

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-05 VULNERABILITY SCANNING

Control description: <http://800-53.govready.com/control?id=RA-5>

Security control type: Hybrid

#### LINCS specific control or LINCS Responsibility

The LINCS Technology Project uses vulnerability scanning software to document and determine risks to the system. These scans are being run on a regular basis 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.

#### Amazon Web Services (AWS) US-East/West control support

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.

### Part a)

#### CivicActions Responsibility

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 ranks 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.

### Part b)

#### CivicActions Responsibility

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.

### Part c)

#### CivicActions Responsibility

CivicActions Security 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 reviews current scans and compare with older scans to identify trends and to verify previous vulnerabilities have been mitigated.

### Part d)

#### CivicActions Responsibility

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:

* 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

### Part e)

#### CivicActions Responsibility

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 though JIRA or the Git issue tool for tracking to the established remediation deadlines listed in RA-5(d).