# Reusable Component Library System Security Plan

# NIST SP 800-53 Revision 4

## AU: Audit and Accountability

### AU-1: Audit And Accountability Policy And Procedures

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

##### CivicActions

CivicActions has developed, documented and disseminated to personnel an audit and accountability 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 Audit and Accountability (AU) Policy. This document can be found in the CivicActions Compliance Docs GitHub repository at <https://github.com/CivicActions/compliance-docs>.

##### Project

The Project maintains a record of system activity by application process and by user activity. Audit and accountability policy and procedures are documented within the Project SSP. Security software features are used to automatically generate and store security audit log records for use in monitoring security-related events on all multi-user systems. The Client reviews and updates this policy as necessary and it was last updated in April 2008. Additional information is contained within the None.

### AU-2: Audit Events

The organization:  
 a. Determines that the information system is capable of auditing the following  
events: [Assignment: organization-defined auditable events];  
 b. Coordinates the security audit function with other organizational entities  
requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;  
 c. Provides a rationale for why the auditable events are deemed to be adequate  
to support after-the-fact investigations of security incidents; and  
 d. Determines that the following events are to be audited within the information  
system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].

#### a

##### AWS

In this architecture, the following audit methods log all security-relevant user/API activities and Amazon S3 data access activities, and support the capability to audit organizationally defined events:

* AWS CloudTrail logging
* Amazon S3 bucket logging
* Elastic Load Balancing (ELB) logging
* Amazon RDS MySQL error logging

##### CivicActions

CivicActions’ Security Policy provides information about auditing and logging of CivicActions internal users and end-user activity on the servers and within the system application.

##### Drupal

Drupal’s Watchdog log are configured to track all relevant auditable events as defined by Client

* Apache access log: Contains a list of requests for your website that have bypassed Varnish. These requests include pages, theme files, and static media files.
* Apache error log: Records any Apache-level issues. The issues reported here are usually caused by general server issues, including capacity problems, .htaccess problems, and missing files.
* Drupal page request log: Records all Drupal page loads on your website.
* Drupal Watchdog log: Records Drupal-related actions on your website. The Watchdog log is recorded on your database if you have enabled the syslog module.
* MySQL slow query log: Contains a list of MySQL queries that have taken longer than one second to complete.
* PHP error log: Records any issues that occur during the PHP processing portion of a page load. Issues reported here are usually caused by a website’s code, configuration, or content.

##### Ilias

Transaction logs are generated by the Apache web server, Ilias CMS, MySQL database and PHP page processing. Specifically, the following server, application, database and network device audit log events are captured: - Apache access log: Contains a list of requests for your website that have bypassed Varnish. These requests include pages, theme files, and static media files. - Apache error log: Records any Apache-level issues. The issues reported here are usually caused by general server issues, including capacity problems, .htaccess problems, and missing files. - Ilias page request log: Records all Ilias page loads on your website. - Ilias log: Records Ilias-related actions on your website. The log is recorded on your server. - MySQL slow query log: Contains a list of MySQL queries that have taken longer than one second to complete. - PHP error log: Records any issues that occur during the PHP processing portion of a page load. Issues reported here are usually caused by a website’s code, configuration, or content.

#### b

##### CivicActions

Auditable events may change due to changes in the threat environment. CivicActions teams collaborate internally and also communicate with customers and partner organizations to identify and select auditable events. The teams that participate in this process are described in control SA-3(b).

##### Ilias

All security-related issues and events, including requests for server log analysis, are recorded in CivicActions’ JIRA tracking system.

#### c

##### AWS

In this architecture, the following audit methods provide data on activities occurring within the infrastructure:

* AWS CloudTrail logging
* Amazon S3 bucket logging
* Elastic Load Balancing (ELB) logging
* Amazon RDS MySQL error logging

##### Ilias

CivicActions has extensive experience and specialization as a host of websites that are built using the Ilias web learning platform. Should the need for additional logging become evident, we have the ability to do so by modifying the website’s source code to insert additional Ilias logging hooks.

#### d

##### AWS

In this architecture, the following audit methods log all security-relevant events and errors related to IAM user and API activities, Amazon S3 data access, network access, and Amazon RDS database errors, and support the capability to audit organizationally defined events:

* AWS CloudTrail logging
* Amazon S3 bucket logging
* Elastic Load Balancing (ELB) logging
* Amazon RDS MySQL error logging

##### Drupal

Information captured in the transaction logs includes, but is not limited to, the following auditable events:

* Failed login attempts
* Successful login attempts
* User account deletions
* User account blocking/unblocking
* Changes in user role assignments
* Unauthorized attempts to alter protected user fields
* New user account creation
* Password reset instructions mailed
* User logins via a one-time login link
* User logouts
* Content creation (datasets, resources and other content types)
* Content modification
* Content deletion
* Content publishing
* Content unpublishing
* File uploads
* Web page not found
* Website configuration changes
* System administration activities
* Slow query logs.
* PHP error logs: Captures any errors logged during execution of the PHP programming language.

##### Ilias

Information captured in the transaction logs includes, but is not limited to, the following auditable events: - Failed login attempts - Successful login attempts - New user account creation - Password reset instructions mailed - User logins via a one-time login link - Content creation - Content publishing - Web page not found - Website configuration changes - System administration activities - Slow query logs. - PHP error logs: Captures any errors logged during execution of the PHP programming language.

### AU-3: Content Of Audit Records

The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

##### AWS

In this architecture, the following audit methods generate records with the level of detail specified for the control:

* **AWS CloudTrail logging**: Provides information on activities related to infrastructure changes.
* **Amazon S3 bucket logging**: Provides data on activities related to the access or manipulation of data stored in Amazon S3.
* **Elastic Load Balancing (ELB) logging**: Provides information about requests or connections.
* **Amazon RDS MySQL error logging**: Captures errors encountered by the database engine. In addition, the MySQL general query log can be enabled by the customer organization to capture when clients connect or disconnect and SQL statements received from clients.

AWS logging information:

* AWS native logging: https://aws.amazon.com/answers/logging/aws-native-security-logging-capabilities/
* AWS CloudTrail logs: http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference.html
* Amazon S3 bucket logs: http://docs.aws.amazon.com/amazons3/latest/dev/ServerLogs.html
* ELB logs: http://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/access-log-collection.html
* Amazon RDS logs: http://docs.aws.amazon.com/amazonrds/latest/UserGuide/USER\_LogAccess.html

##### Drupal

The logs collected for Drupal sites include the following types of information:

* IP number of the request originator
* Timestamp
* Request URL
* HTTP status code returned
* Username
* Drupal Watchdog message (if applicable)
* Unique numerical ID of the content being modified (for content creation, modification and deletion events) When auditing a Drupal incident, the CivicActions developers aggregate log sources from multiple servers into the Graylog dashboard so that all log entries for a single managed security incident can be analyzed in a single document. Log sources are sorted, filtered and reviewed. Application logs are maintained primarily for an after-the-fact investigation of critical systems or security events.

##### Ilias

The logs collected for Ilias sites include the following types of information: - IP number of the request originator - Timestamp - Username - Ilias log message (if applicable) - Unique numerical ID of the content being modified (for content creation, modification and deletion events) When auditing an Ilias incident, CivicActions’ developers aggregate log sources from multiple servers into the Graylog dashboard so that all log entries for a single managed security incident can be analyzed in a single document. Log sources are sorted, filtered and reviewed. Application logs are maintained primarily for an after-the-fact investigation of critical systems or security events.

### AU-4: Audit Storage Capacity

The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].

##### AWS

In this architecture, logs track dynamic capacity growth to accommodate organizationally defined storage capacity requirements. Amazon S3 buckets are established to store audit logs from the following audit methods:

* AWS CloudTrail logging
* Amazon S3 bucket logging
* Elastic Load Balancing (ELB) logging
* Amazon RDS MySQL error logging

##### CivicActions

CivicActions ensures adequate storage capability requirements listed in AU-11 for all events from the application, database, and hosting environment.

### AU-5: Response To Audit Processing Failures

The information system:  
 a. Alerts [Assignment: organization-defined personnel or roles] in the event  
of an audit processing failure; and  
 b. Takes the following additional actions: [Assignment: organization-defined  
actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].

##### CivicActions

When notified (e.g., via CloudWatch) of an auditing failure, CivicActions Operations staff will review the causes and take corrective action.

#### a

##### AWS

In this architecture, AWS CloudTrail is enabled, and provides the basis for audit processing within the infrastructure.

AWS built-in features include customer alerting of AWS CloudTrail and other service failures through the following:

* AWS Service Health Dashboard (http://status.aws.amazon.com)
* RSS feeds to which the customer organization can subscribe
* email
* alerts sent directly to the AWS account *root user* for critical events
* AWS internal Incident Response and corporate communications processes

### AU-6: Audit Review, Analysis, And Reporting

The organization:  
 a. Reviews and analyzes information system audit records [Assignment: organization-defined  
frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and  
 b. Reports findings to [Assignment: organization-defined personnel or roles].

#### a

##### CivicActions

CivicActions security audit data is collected by the AWS CloudWatch monitoring and observability service to support real time and after-the-fact investigation at the application level for the following:

* Indications of inappropriate or unusual activity
* Assurance that logging is functioning properly
* Adherence to logging standards identified in this procedure

#### b

##### CivicActions

Any significant findings observed during the inspection are reported to CivicActions’ Security Office. If these are considered to constitute a security incident, then the Incident Response process is invoked as described in the implementation of the Incident Response Plan (IR-8).

### AU-8: Time Stamps

The information system:  
 a. Uses internal system clocks to generate time stamps for audit records; and  
 b. Records time stamps for audit records that can be mapped to Coordinated  
Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: organization-defined granularity of time measurement].

##### Project

The Project system clocks are synchronized system-wide and provide time stamps with audit records.

#### a

##### AWS

AWS includes the Amazon Time Sync Service. Running over Network Time Protocol (NTP), this service synchronizes the time on AWS instances using redundant satellite-connected and atomic clocks in all public AWS regions. The Amazon Time Sync Service provides accurate time stamp data to the following audit methods:

* AWS CloudTrail logging
* Amazon S3 bucket logging
* Elastic Load Balancing (ELB) logging
* Amazon RDS MySQL error logging

#### b

##### AWS

The Amazon Time Sync Service provides accurate time stamp data to the following audit methods:

* AWS CloudTrail logging
* Amazon S3 bucket logging
* Elastic Load Balancing (ELB) logging
* Amazon RDS MySQL error logging

Time stamps are recorded as specified in the ISO 8601 standard. ISO 8601 represents local time (with the location unspecified), as UTC, or as an offset from UTC.

### AU-9: Protection Of Audit Information

The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

##### AWS

Access to audit data and tools is determined by access control policies for IAM groups and roles. Only users assigned to IAM groups and roles with access to audit data and tools can access them. Additionally, AWS uses server-side encryption on Amazon S3 bucket logs, and maintains them as read-only files.

##### CivicActions

CivicActions ensures that audit logs are created, stored and maintained. Developers who have been assigned as members of the CivicActions Security Office are the only CivicActions personnel with logical permission to access and review audit logs.

### AU-11: Audit Record Retention

The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

##### AWS

AWS CloudTrail logs are stored in an Amazon S3 bucket, which dynamically allocates storage capacity to support continuous collection and storage of AWS CloudTrail log data. The storage capacity supports indefinite retention, but with 7 year retention specified, and migration to Amazon Glacier after 90 days in AWS regions where Glacier is available.

##### CivicActions

CivicActions audits events from the application, database, and hosting environment, and retains these records for at least 180 days.

### AU-12: Audit Generation

The information system:  
 a. Provides audit record generation capability for the auditable events defined  
in AU-2 a. at [Assignment: organization-defined information system components];  
 b. Allows [Assignment: organization-defined personnel or roles] to select which  
auditable events are to be audited by specific components of the information system; and  
 c. Generates audit records for the events defined in AU-2 d. with the content  
defined in AU-3.

#### a

##### AWS

In this architecture, AWS CloudTrail, Amazon S3 bucket logging, Elastic Load Balancing (ELB) logging, and Amazon RDS MySQL error logging are enabled, but initial Amazon EC2 instances launched by this deployment (bastion host, application servers, proxy servers, and any Amazon EC2-based NAT servers) do not have auditing enabled within the OS, as these are for example purposes only.

AWS built-in features of logging mechanisms provide the audit record generation capability for the auditable events defined in AU-2a. by logging all security-relevant IAM user and API activities which address AWS infrastructure components (AWS Products and services), ELB

##### CivicActions

CivicActions ensures audit records are generated for its web and event logs as required in AU-2 and AU-3 for servers, application, database, and network components.

#### b

##### AWS

In this architecture, AWS CloudTrail, Amazon S3 bucket logging, Elastic Load Balancing (ELB) logging, and Amazon RDS MySQL error logging are enabled AWS CloudTrail is enabled to log all available API events automatically within the AWS infrastructure and Amazon S3 bucket logging is enabled to log bucket activity.

AWS built-in features of Identity and Access Management (IAM) allows policy to be applied to privileged users for administrator/audit access, allowing them to modify Amazon CloudWatch alarms, AWS Config rules, and Amazon S3 bucket logging to select the CloudTrail and Amazon S3 events that are to cause notification, alerting and automated reaction.

##### CivicActions

The selected auditable events described in AU-2 are coordinated by CivicActions internal admins and client security/operations officers for each component of the production system.

#### c

##### AWS

In this architecture, AWS CloudTrail, Amazon S3 bucket logging, Elastic Load Balancing (ELB) logging, and Amazon RDS MySQL error logging are enabled. However, the initial Amazon EC2 instances launched by this deployment (bastion host, application servers, proxy servers, and any Amazon EC2-based NAT servers) DO NOT have any auditing enabled within the OS, as these are in place for example purposes only.

AWS built-in features of native logging generates audit records with the content defined in AU-3.

AWS logging information:

* AWS native logging: https://aws.amazon.com/answers/logging/aws-native-security-logging-capabilities/
* AWS CloudTrail logs: http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference.html
* Amazon S3 bucket logs: http://docs.aws.amazon.com/amazons3/latest/dev/ServerLogs.html
* ELB logs: http://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html
* http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/access-log-collection.html
* Amazon RDS logs: http://docs.aws.amazon.com/amazonrds/latest/UserGuide/USER\_LogAccess.html

##### CivicActions

CivicActions maintained applications generate audit records for their web and event logs as described in AU-2 and AU-3.