# 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].

**Status:** Complete

##### 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>.

### 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].

**Status:** None

#### a

##### AWS

In this architecture, AWS CloudTrail, S3 bucket logging, Elastic Load Balancer (ELB) Logging, and RDS MySQL error logging are employed, which support the capability for audit of organizationally defined events by logging all security-relevant user/API activities and S3 data access activities.

##### 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.

#### 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).

#### c

##### AWS

In this architecture, AWS CloudTrail, S3 bucket logging, Elastic Load Balancer (ELB) Logging, and RDS MySQL error logging are employed to provide the audit data necessary to determine what activities have occurred within the infrastructure.

#### d

##### AWS

In this architecture, AWS CloudTrail, S3 bucket logging, Elastic Load Balancer (ELB) Logging, and RDS MySQL error logging are employed to provide the capability for audit of organizationally defined events by logging security-relevant events and errors related to IAM user and API activities, S3 data access, network access, and RDS database errors.

##### 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.

### 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.

**Status:** Complete

##### AWS

In this architecture, AWS CloudTrail, S3 bucket logging, Elastic Load Balancer (ELB) Logging, and RDS MySQL error logging are employed, which generate audit records that include the level of detail specified in the control. CloudTrail logs provide information on activities related to the manipulation of the infrastructure; S3 bucket logs provide data on activities related to the access or manipulation of data stored in S3; ELB logs provide information about requests or connections; RDS Database MySQL error logs record 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 statement received from clients.

General information about AWS native logging is documented at: https://aws.amazon.com/answers/logging/aws-native-security-logging-capabilities/ Details about CloudTrail logs are documented at http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference.html Details about S3 bucket logs are documented at http://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html Details about ELB logs are available at 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 Details about RDS logs are documented at 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.

### AU-4: Audit Storage Capacity

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

**Status:** Complete

##### AWS

In this architecture, Amazon S3 buckets are established for storage of AWS CloudTrail audit records, S3 Bucket logs, Elastic Load Balancer logs, etc., which provide dynamic capacity growth to accommodate organizationally defined storage capacity requirements

##### 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)].

**Status:** Complete

##### 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, which provides the basis for audit processing within the infrastructure.

AWS built-in features include customer alerting of CloudTrail and other service failures through the AWS Service Health Dashboard (http://status.aws.amazon.com) and through optional RSS feeds subscribed to by customers, as well as through email and other direct alerts to root account owners for events deemed critical enough for direct contact, per 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].

**Status:** Planned

#### 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].

**Status:** Complete

#### a

##### AWS

In this architecture, AWS CloudTrail, S3 bucket logging, Elastic Load Balancer (ELB) Logging, and RDS MySQL error logging are employed.

AWS built-in features of native logging use AWS region internal clocks to time stamp all log entries.

#### b

##### AWS

In this architecture, AWS CloudTrail, S3 bucket logging, Elastic Load Balancer (ELB) Logging, and RDS MySQL error logging are employed.

AWS built-in features of native logging provide time stamps 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.

**Status:** Complete

##### AWS

In this architecture, access to audit data and tools are restricted to only personnel assigned by the organization to IAM groups and roles which are associated with access control policies for such access. In addition, server side encryption of Audit bucket, S3 bucket policies are configured to restrict access to those appropriate IAM groups/roles, and with read-only permissions.

##### 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.

**Status:** Complete

##### AWS

In this architecture, AWS CloudTrail logs are stored in an Amazon S3 bucket, which dynamically allocates storage capacity to support continuous collection and storage of CloudTrail log data with indefinite retention capability, 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.

**Status:** Complete

#### a

##### AWS

In this architecture, AWS CloudTrail, S3 bucket logging, Elastic Load Balancer (ELB) Logging, and RDS MySQL error logging are enabled, but initial EC2 instances launched by this deployment (bastion host, application servers, proxy servers, and any 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 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, S3 bucket logging, Elastic Load Balancer (ELB) Logging, and 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 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, S3 bucket logging, Elastic Load Balancer (ELB) Logging, and RDS MySQL error logging are enabled. However, the initial EC2 instances launched by this deployment (bastion host, application servers, proxy servers, and any 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.

General information about AWS native logging is documented at: https://aws.amazon.com/answers/logging/aws-native-security-logging-capabilities/ Details about CloudTrail logs are documented at http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference.html Details about S3 bucket logs are documented at http://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html Details about ELB logs are available at 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 Details about RDS logs are documented at 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.