



FedRAMP Moderate Templates

Audit and Accountability Implementation Checklist

Policy and Documentation

- ☐ **AU-01:** Develop, document, and disseminate organization-level, mission/business process-level, and system-level audit and accountability policy
- ☐ **AU-01:** Ensure audit and accountability policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
- ☐ **AU-01:** Verify audit and accountability policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
- ☐ **AU-01:** Document procedures to facilitate implementation of the audit and accountability policy and associated controls
- ☐ **AU-01:** Designate an official to manage the development, documentation, and dissemination of audit and accountability policy and procedures
- ☐ **AU-01:** Review and update audit and accountability policy at least every 3 years or as required by federal or organizational policy changes
- ☐ **AU-01:** Review and update audit and accountability procedures at least every 3 years or as required by federal or organizational policy changes

Event Identification and Logging Configuration

- ☐ **AU-02:** Identify all event types the system is capable of logging for audit functions
- ☐ **AU-02:** Configure logging for successful and unsuccessful account logon events
- ☐ **AU-02:** Configure logging for account management events
- ☐ **AU-02:** Configure logging for object access events
- ☐ **AU-02:** Configure logging for policy change events
- ☐ **AU-02:** Configure logging for privilege function events
- ☐ **AU-02:** Configure logging for process tracking events
- ☐ **AU-02:** Configure logging for system events
- ☐ **AU-02:** For web applications, configure logging for all administrator activity



FedRAMP Moderate Templates

- ☐ **AU-02:** For web applications, configure logging for authorization checks
- ☐ **AU-02:** For web applications, configure logging for data deletions
- ☐ **AU-02:** For web applications, configure logging for data access
- ☐ **AU-02:** For web applications, configure logging for data changes
- ☐ **AU-02:** For web applications, configure logging for permission changes
- ☐ **AU-02:** Coordinate event logging function with other organizational entities requiring audit-related information
- ☐ **AU-02:** Specify event types for logging within the system along with frequency or situations requiring logging for each type
- ☐ **AU-02:** Document rationale for why selected event types are adequate to support after-the-fact investigations of incidents
- ☐ **AU-02:** Review and update event types selected for logging at least annually or whenever there is a change in the threat environment

Audit Record Content and Generation

- ☐ **AU-03:** Ensure audit records capture what type of event occurred
- ☐ **AU-03:** Ensure audit records capture when the event occurred
- ☐ **AU-03:** Ensure audit records capture where the event occurred
- ☐ **AU-03:** Ensure audit records capture the source of the event
- ☐ **AU-03:** Ensure audit records capture the outcome of the event
- ☐ **AU-03:** Ensure audit records capture identity of any individuals, subjects, or objects/entities associated with the event
- ☐ **AU-03(01):** Generate audit records containing session, connection, transaction, or activity duration
- ☐ **AU-03(01):** Generate audit records containing number of bytes received and bytes sent for client-server transactions
- ☐ **AU-03(01):** Generate audit records containing additional informational messages to diagnose or identify the event
- ☐ **AU-03(01):** Generate audit records containing characteristics that describe or identify the object or resource being acted upon
- ☐ **AU-12:** Provide audit record generation capability for event types defined in AU-2a on all information system and network components where technically feasible
- ☐ **AU-12:** Allow organization-defined personnel or roles to select event types to be logged by specific system components



FedRAMP Moderate Templates

- ☐ **AU-12:** Generate audit records for event types defined in AU-2c that include audit record content defined in AU-3

Audit Storage and Capacity Management

- ☐ **AU-04:** Allocate audit log storage capacity to accommodate retention requirements in accordance with AU-11
- ☐ **AU-11:** Retain audit records for at least 90 days
- ☐ **AU-11:** Provide support for on-demand audit review, analysis, and reporting for at least one year
- ☐ **AU-11:** Ensure audit record retention is consistent with records retention policy
- ☐ **AU-11:** Ensure audit record retention supports after-the-fact investigations of incidents
- ☐ **AU-11:** Ensure audit record retention meets regulatory and organizational information retention requirements

Audit Processing Failure Response and Alerts

- ☐ **AU-05:** Alert organization-defined personnel or roles within a real-time or near-real-time period in the event of audit logging process failure
- ☐ **AU-05:** Configure system to overwrite oldest audit records when audit logging failures occur, OR
- ☐ **AU-05:** Configure system to shut down when audit logging failures occur

Audit Review, Analysis, and Reporting

- ☐ **AU-06:** Review and analyze system audit records at least weekly for indications of organization-defined inappropriate or unusual activity
- ☐ **AU-06:** Assess potential impact of inappropriate or unusual activity identified during audit review
- ☐ **AU-06:** Report audit review findings to organization-defined personnel or roles
- ☐ **AU-06:** Adjust level of audit record review, analysis, and reporting when there is a change in risk based on law enforcement information, intelligence information, or other credible sources



FedRAMP Moderate Templates

- ☐ **AU-06(01):** Integrate audit record review, analysis, and reporting processes using organization-defined automated mechanisms
- ☐ **AU-06(03):** Analyze and correlate audit records across different repositories to gain organization-wide situational awareness
- ☐ **AU-07:** Provide and implement audit record reduction capability that supports on-demand audit record review, analysis, and reporting requirements
- ☐ **AU-07:** Provide and implement audit record reduction capability that supports after-the-fact investigations of incidents
- ☐ **AU-07:** Ensure audit record reduction and report generation capability does not alter original content of audit records
- ☐ **AU-07:** Ensure audit record reduction and report generation capability does not alter time ordering of audit records
- ☐ **AU-07(01):** Provide and implement capability to process audit records for events of interest based on organization-defined fields within audit records
- ☐ **AU-07(01):** Provide and implement capability to sort audit records for events of interest based on organization-defined fields within audit records
- ☐ **AU-07(01):** Provide and implement capability to search audit records for events of interest based on organization-defined fields within audit records

Time Stamp Generation and Synchronization

- ☐ **AU-08:** Use internal system clocks to generate time stamps for audit records
- ☐ **AU-08:** Record time stamps for audit records that meet one second granularity of time measurement
- ☐ **AU-08:** Configure time stamps to use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or include local time offset as part of the time stamp

Audit Information Protection

- ☐ **AU-09:** Protect audit information from unauthorized access, modification, and deletion
- ☐ **AU-09:** Protect audit logging tools from unauthorized access, modification, and deletion
- ☐ **AU-09:** Alert organization-defined personnel or roles upon detection of unauthorized access to audit information



FedRAMP Moderate Templates

- ☐ **AU-09:** Alert organization-defined personnel or roles upon detection of unauthorized modification of audit information
- ☐ **AU-09:** Alert organization-defined personnel or roles upon detection of unauthorized deletion of audit information
- ☐ **AU-09(04):** Authorize access to management of audit logging functionality to only an organization-defined subset of privileged users or roles
- ☐ **AU-09(04):** Document and maintain list of privileged users or roles authorized to manage audit logging functionality

Key Timeframes Summary

- **Policy Review:** At least every 3 years or when federal/organizational policy changes occur
- **Event Type Review:** At least annually or whenever threat environment changes
- **Audit Record Review:** At least weekly
- **Audit Record Retention:** Minimum 90 days with one year of on-demand access capability
- **Failure Alerts:** Real-time or near-real-time