CloudCheckr NIST 800-53 Audit and Accountability

FISMA NIST 800-53 (Rev 4)
Audit and Accountability: Shared Public Cloud Infrastructure Standards

Standard	Requirement per NIST 800-53 (Rev. 4)	CloudCheckr Action
AU-3/ AU3(1)	**AU-3 CONTENT OF AUDIT RECORDS** **Control:** 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. **Supplemental Guidance:** Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred). Related controls: AU-2, AU-8, AU-12, SI-11. **Control Enhancements: (1) CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION Supplemental Guidance:** Detailed information that organizations may consider in audit records includes, for example, full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest.	**Change Monitoring integrates CloudTrail to track changes on daily, weekly, and monthly basis** **EC2** • Security Groups • Security Group Rules • Key Pairs • AMIs • Spot Instances • Reserved Instance • Instances • Volumes • Snapshots • Placement Groups • Elastic Load Balancers (including attaching or detaching instances to them) • Network Interfaces • Elastic IPs **IAM** • Account Aliases • Account Summaries • Access Keys • MFA Devices • Policies • Password Policies • Groups • Users **S3** • Bucket Logging • Logging Target Bucket • Bucket Logging Prefix • Bucket Website Enabled • Bucket Website Index Document • Bucket Website Error Document • Bucket Notifications Enabled • Public Buckets • Bucket Notifications • Bucket Lifecycle Rules • Bucket Permissions **ElastiCache** • ElastiCache Clusters • Cache Nodes • Security Groups • Parameter Groups • Reserved Nodes

Standard	Requirement per NIST 800-53 (Rev. 4)	CloudCheckr Action
AU-4/ AU-4(1)	**AU-4 AUDIT STORAGE CAPACITY** **Control:** The organization allocates audit record storage capacity. **Supplemental Guidance:** Organizations consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability. Related controls: AU-2, AU-5, AU-6, AU-7, AU-11, SI-4. **Control Enhancements: (1) AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE** **Supplemental Guidance:** Off-loading is a process designed to preserve the confidentiality and integrity of audit records by moving the records from the primary information system to a secondary or alternate system. It is a common process in information systems with limited audit storage capacity; the audit storage is used only in a transitory fashion until the system can communicate with the secondary or alternate system designated for storing the audit records, at which point the information is transferred.	**Historical records and environment changes are stored for the life of service** All records of service usage are available through Trending Analysis reporting. All records of deployments changes are available through Change Monitoring and CloudTrail. CloudCheckr storage retains sufficient capacity to maintain the integrity of the records. SLA guarantees confidentiality of records.
AU-5	**RESPONSE TO AUDIT PROCESSING FAILURES** **Control:** The information system: a. Alerts in the event of an audit processing failure; and b. Takes the following additional actions: [organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)]. **Supplemental Guidance:** Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Organizations may choose to define additional actions for different audit processing failures (e.g., by type, by location, by severity, or a combination of such factors). This control applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the total audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both. Related controls: AU-4, SI-12.	**Automated audit collection features with failure alerts** Automated notifications for failures to correctly process collection procedures. Ability to automatically recollect and reprocess information if failure occurs.

Standard	Requirement per NIST 800-53 (Rev. 4)	CloudCheckr Action
AU-6/ AU-6(1)(3)	**AUDIT REVIEW, ANALYSIS, AND REPORTING** **Control:** The organization: a. Reviews and analyzes information system audit records with organization-defined frequency for indications of organization-defined inappropriate or unusual activity; and b. Reports findings to organization-defined personnel or roles. **Supplemental Guidance:** Audit review, analysis, and reporting covers information security-related auditing performed by organizations including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP. Findings can be reported to organizational entities that include, for example, incident response team, help desk, information security group/department. If organizations are prohibited from reviewing and analyzing audit information or unable to conduct such activities (e.g., in certain national security applications or systems), the review/analysis may be carried out by other organizations granted such authority. Related controls: AC-2, AC-3, AC-6, AC-17, AT-3, AU-7, AU-16, CA-7, CM-5, CM-10, CM-11, IA-3, IA-5, IR-5, IR-6, MA-4, MP-4, PE-3, PE-6, PE-14, PE-16, RA-5, SC-7, SC-18, SC-19, SI-3, SI-4, SI-7. **Control Enhancements:** **(1) AUDIT REVIEW, ANALYSIS, AND REPORTING | PROCESS INTEGRATION** The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. **Supplemental Guidance:** Organizational processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, contingency planning, and Inspector General audits. Related controls: AU-12, PM-7.	Information is available on a regular and as-requested basis. Delivery can be pre-set and automated. Account and information access controls are available. All reporting is fully automated.

Standard	Requirement per NIST 800-53 (Rev. 4)	CloudCheckr Action
AU-6/ AU-6(1)(3) Cont.	**(3) AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES** The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. **Supplemental Guidance:** Organization-wide situational awareness includes awareness across all three tiers of risk management (i.e., organizational, mission/business process, and information system) and supports cross-organization awareness. Related controls: AU-12, IR-4.	
AU-7/ AU-7(1)	**AUDIT REDUCTION AND REPORT GENERATION** **Control:** The information system provides an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and b. Does not alter the original content or time ordering of audit records. **Supplemental Guidance:** Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same information system or from the same organizational entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the information system can generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient. Related control: AU-6. **Control Enhancements:** **(1) AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING** The information system provides the capability to process audit records for events of interest based on organization-defined audit fields within audit records. **Supplemental Guidance:** Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or subnetwork)	User-defined detailed and summary reporting Reporting across multiple cloud resource groups available on service and granular levels Filtering, sorting, and export capabilities. Automated controls are available. Reporting is fully customizable. Audit records contain unalterable information, time stamp, and sequencing.

Standard	Requirement per NIST 800-53 (Rev. 4)	CloudCheckr Action
AU-8/ AU-8(1)	**TIME STAMPS** **Control:** 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]. **Supplemental Guidance:** Time stamps generated by the information system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between information system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities. Related controls: AU-3, AU-12. **Control Enhancements:** **(1) TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE:** The information system: (a) Compares the internal information system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source]; and (b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period]. **Supplemental Guidance:** This control enhancement provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.	All reports are time stamped to UTC. Single internal clock used for logging changes. Reporting is also customizable to local time zones.

Standard	Requirement per NIST 800-53 (Rev. 4)	CloudCheckr Action
AU-9/ AU-9(4)	**PROTECTION OF AUDIT INFORMATION** **Control:** The information system protects audit information and audit tools from unauthorized access, modification, and deletion. **Supplemental Guidance:** Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. This control focuses on technical protection of audit information. Physical protection of audit information is addressed by media protection controls and physical and environmental protection controls. Related controls: AC-3, AC-6, MP-2, MP-4, PE-2, PE-3, PE-6. **Control Enhancements:** **(4) PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS:** The organization authorizes access to management of audit functionality to only organization-defined subset of privileged users. **Supplemental Guidance:** Individuals with privileged access to an information system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records. This control enhancement requires that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges. Related control: AC-5.	All reporting securely stored Users do not have ability to modify, alter, or delete data. Individual permissioning and access control is available.
AU-11	**AUDIT RECORD RETENTION** **Control:** The organization retains audit records for 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. **Supplemental Guidance:** Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention. Related controls: AU-4, AU-5, AU-9, MP-6.	Automated report retention for life of service is standard

Standard	Requirement per NIST 800-53 (Rev. 4)	CloudCheckr Action
AU-12	**AUDIT GENERATION** **Control:** The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at organization-defined information system components; Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations b. Allows organization-defined personnel 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.	Provides complete monitoring and reporting of the infrastructure layer and its associated changes. Automated Change Monitoring and CloudTrail alerts provide notice and records of all auditable events.