CloudCheckr

CloudCheckr NIST 800-53 Matrix

FISMA NIST 800-53 (Rev 4)

Shared Public Cloud Infrastructure Standards

NIST CONTROL	CLOUDCHECKR SUPPORT ACTIVITY
AC-2 ACCOUNT MANAGEMENT Control: The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types]; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]; g. Monitors the use of, information system accounts;	CloudCheckr supports this control by providing visibility and reporting into user access management. By analyzing and reporting on IAM CloudCheckr enables the user to actively monitor and identify user accesses and maintain proper privileges in their environment. In addition, CloudCheckr specifically supports controls (d) and (i) In addition, CloudCheckr specifically supports Control Enhancement 1
Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	

NIST CONTROL	CLOUDCHECKR SUPPORT ACTIVITY
(1) ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT The organization employs automated mechanisms to support the management of information system accounts. Supplemental Guidance: The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using telephonic notification to report atypical system account usage.	
AC-3 ACCESS ENFORCEMENT Control: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations also be employed at the application and service level to provide increased information security. Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3.	CloudCheckr performs automated reporting of IAM and other policies. Notifications are provided when policies are violated.

NIST CONTROL	CLOUDCHECKR SUPPORT ACTIVITY
CA-7 CONTINUOUS MONITORING Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].	CloudCheckr provides continuous monitoring of the AWS infrastructure. Change Monitoring collects and reports resource, user, configuration, and other changes. CloudCheckr leverages CloudTrail information to enable users to continually view their complete environment, its costs, its resources, and its configurations. CloudCheckr also provides alerts and notifications tied to configuration errors, unauthorized access attempts, perimeter security, configurations, and other performance issues. In addition, CloudCheckr specifically supports Control Enhancement 1 by providing an independent security assessment.

NIST CONTROL	CLOUDCHECKR SUPPORT ACTIVITY
Supplemental Guidance: Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of information systems. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4. Control Enhancements: (1) CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to monitor the security controls in the information system on an ongoing basis.	
Supplemental Guidance: Organizations can maximize the value of assessments of security controls during the continuous monitoring process by requiring that such assessments be conducted by assessors or assessment teams with appropriate levels of independence based on continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in advocacy positions for the organizations acquiring their se	

NIST CONTROL	CLOUDCHECKR SUPPORT ACTIVITY
CM-2 BASELINE CONFIGURATION Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	CloudCheckr creates and maintain full baselines for all infrastructure configurations, resources, security groups, and IAM permissions.
Supplemental Guidance: This control establishes baseline configurations for information systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture. Related controls: CM-3, CM-6, CM-8, CM-9, SA-10, PM-5, PM-7. Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations Control Enhancements: (1) BASELINE CONFIGURATION | REVIEWS AND UPDATES The organization reviews and updates the baseline configuration of the information system: (a) [Assignment: organization-defined frequency]; (b) When required due to [Assignment organization-defined circumstances]; and (c) As an integral part of information system component installations and upgrades. Supplemental Guidance: Related control: CM-5. (2) BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY	In addition, CloudCheckr supports Control Enhancements 1 and 2 by automating the reporting process and creating alerts when infrastructure configurations change. CloudCheckr supports Control Enhancement 3 by retaining a full record of all baseline and subsequent data.
The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.	
CM-3 CONFIGURATION CHANGE CONTROL Control: The organization: a. Determines the types of changes to the information system that are configuration-controlled;	CloudCheckr provides complete details of all infrastructure layer configuration changes.

NIST CONTROL	CLOUDCHECKR SUPPORT ACTIVITY
b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; c. Documents configuration change decisions associated with the information system; d. Implements approved configuration-controlled changes to the information system;	In addition, CloudCheckr supports Control Enhancement 2 by documenting and disseminating all configuration changes.
e. Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period]; f. Audits and reviews activities associated with configuration-controlled changes to the information system; and g. Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]]. Supplemental Guidance: Configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of information systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities. Typical processes for managing configuration changes to information systems include, for example, Configuration Control Boards that approve proposed changes to systems. For new development information systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards. Auditing of changes includes activities before and after changes are made to organizational information systems and the auditing activities required to implement such changes. Related controls: CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12. Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations Control Enhancements:	

NIST CONTROL	CLOUDCHECKR SUPPORT ACTIVITY
(2) CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system. Supplemental Guidance: Changes to information systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-6. Organizations ensure that testing does not interfere with information system operations. Individuals/groups conducting tests understand organizational security policies and procedures, information system security policies and procedures, and the specific health, safety, and environmental risks associated with particular facilities/processes. Operational systems may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If information systems must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. If testing cannot be conducted on operational systems, organizations employ compensating controls (e.g., testing on replicated systems).	
CM-6 CONFIGURATION SETTINGS Control: The organization: a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and	CloudCheckr automates the documentation of all configuration settings and records all changes. The Best Practice and Policy engines report deviations through automated alerts

NIST CONTROL	CLOUDCHECKR SUPPORT ACTIVITY
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. Supplemental Guidance: Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part of the systems configuration baseline. Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. Common secure configurations include the	
Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations Control Enhancements: (1) CONFIGURATION SETTINGS | AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [Assignment: organization-defined information system components]. Supplemental Guidance: Related controls: CA-7, CM-4.	

NIST CONTROL	CLOUDCHECKR SUPPORT ACTIVITY
CM-8 INFORMATION SYSTEM COMPONENT INVENTORY Control: The organization: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and b. Reviews and updates the information system component inventory [Assignment: organization-defined frequency].	CloudCheckr creates and updates a full inventory of all infrastructure components. This inventory can be viewed within a single account or in an aggregation of 100s of accounts. The inventory is updated automatically with all inventory changes recorded and saved.
Supplemental Guidance: Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location. Related controls: CM-2, CM-6, PM-5. Control Enhancements: (1) INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates. (3) INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION The organization: (a) Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and (b) Takes the following actions when unauthorized components are detected: [Selection (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles]]. Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations	In addition, CloudCheckr's automated collection supports Control Enhancements 1 and 3.

NIST CONTROL	CLOUDCHECKR SUPPORT ACTIVITY
(5) INFORMATION SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories. Supplemental Guidance: This control enhancement addresses the potential problem of duplicate accounting of information system components in large or complex interconnected systems.	
IR-4 INCIDENT HANDLING Control: The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.	CloudCheckr automates the identification of infrastructure, configuration issues, and related security concerns. Results are automatically stored for forensic analysis.
Supplemental Guidance: Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). Related controls: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7. Control Enhancements: (1) INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES The organization employs automated mechanisms to support the incident handling process. Supplemental Guidance: Automated mechanisms supporting incident handling processes include, for example, online incident management systems.	
IR-5 INCIDENTMONITORING Control: The organization tracks and documents information system security incidents.	CloudCheckr identifies policy and best practice exceptions.

NIST CONTROL	CLOUDCHECKR SUPPORT ACTIVITY
Supplemental Guidance: Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Related controls: AU-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.	Results are automatically stored and presented within individual and trending formats. All related information system settings are fully available for complete forensic analysis.
IR-6 INCIDENT REPORTING Control: The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and b. Reports security incident information to [Assignment: organization-defined authorities]. Supplemental Guidance: The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. Related controls: IR-4, IR-5, IR-8.	CloudCheckr automates reporting of potential security incidents. Email and alert capabilities ensure that incidents are properly reported.
Control Enhancements: (1) INCIDENT REPORTING | AUTOMATED REPORTING The organization employs automated mechanisms to assist in the reporting of security incidents. Supplemental Guidance: Related control: IR-7.	

NIST CONTROL	CLOUDCHECKR SUPPORT ACTIVITY
IR-7 INCIDENT RESPONSE ASSISTANCE Control: The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents. Supplemental Guidance: Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required. Related controls: AT-2, IR-4, IR-6, IR-8, SA-9. Control Enhancements: (1) INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT The organization employs automated mechanisms to increase the availability of incident response-related information and support. Supplemental Guidance: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.	CloudCheckr provides a complete history of infrastructure policy and best practice exceptions. In addition all related configuration, security, group, and user information is automatically collected and stored.
RA-5 VULNERABILITY SCANNING Control: The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).	CloudCheckr provides daily scans of infrastructure vulnerabilities. Results are reported and stored along with corresponding system configurations. Incremental changes in the system are reported with past results and current results both accessible.

NIST CONTROL	CLOUDCHECKR SUPPORT ACTIVITY
Supplemental Guidance: Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations Common Vulnerability Scoring System (CVSS). Related controls: CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2. Control Enhancements: (1) VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY	
The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.	

NIST CONTROL	CLOUDCHECKR SUPPORT ACTIVITY
Supplemental Guidance: The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible. Related controls: SI-3, SI-7. (2) VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED The organization updates the information system vulnerabilities scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported]. Supplemental Guidance: Related controls: SI-3, SI-5. 5) VULNERABILITY SCANNING | PRIVILEGED ACCESS The information system implements privileged access authorization to [Assignment: organization-identified information system components] for selected [Assignment: organization-defined vulnerability scanning activities]. Supplemental Guidance: In certain situations, the nature of the vulnerability scanning may be more intrusive or the information system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning.	
SA-2 ALLOCATION OF RESOURCES Control: The organization: a. Determines information security requirements for the information system or information system service in mission/business process planning;	CloudCheckr supports the budgeting portion of resource allocation. Automated alerts and cost allocation ensure that budget integrity is maintained.
b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and	
c. Establishes a discrete line item for information security in organizational programming and budgeting documentation. Supplemental Guidance: Resource allocation for information security includes funding for the initial information system or information system service acquisition and funding for the sustainment of the system/service. Related controls: PM-3, PM-11.	

NIST CONTROL	CLOUDCHECKR SUPPORT ACTIVITY
SA-5 INFORMATION SYSTEM DOCUMENTATION Control: The organization: a. Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/ mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations b. Obtains user documentation for the information system, system component, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and 3. User responsibilities in maintaining the security of the system, component, or service; c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [Assignment: organization-defined actions] in response;	CloudCheckr provides detailed instruction regarding proper configuration and mitigation instruction when improper or insecure configurations are identified.

NIST CONTROL	CLOUDCHECKR SUPPORT ACTIVITY
d. Protects documentation as required, in accordance with the risk management strategy; and e. Distributes documentation to [Assignment: organization-defined personnel or roles]. Supplemental Guidance: This control helps organizational personnel understand the implementation and operation of security controls associated with information systems, system components, and information system services. Organizations consider establishing specific measures to determine the quality/completeness of the content provided. The inability to obtain needed documentation may occur, for example, due to the age of the information system/component or lack of support from developers and contractors. In those situations, organizations may need to recreate selected documentation if such documentation is essential to the effective implementation or operation of security controls. The level of protection provided for selected information system, component, or service documentation is commensurate with the security category or classification of the system. For example, documentation associated with a key DoD weapons system or command and control system would typically require a higher level of protection than a routine administrative system. Documentation that addresses information system vulnerabilities may also require an increased level of protection. Secure operation of the information system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation. Related controls: CM-6, CM-8, PL-2, PL-4, PS-2, SA-3, SA-4.	
SI-4 INFORMATION SYSTEM MONITORING Control: The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections;	CloudCheckr provides full infrastructure monitoring. Configurations and exceptions are noted and stored. A full inventory with utilization and cost data is updated in real time. Environment and resource data is always accessible.

NIST CONTROL	CLOUDCHECKR SUPPORT ACTIVITY
b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods]; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations the Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].	Budget, resource, policy, and change alerts are provided. All functions are automated.

NIST CONTROL	CLOUDCHECKR SUPPORT ACTIVITY
Supplemental Guidance: Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless. Related controls: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7. Control Enhancements:	

<table>
<tr><th>NIST CONTROL</th><th>CLOUDCHECKR SUPPORT ACTIVITY</th></tr>
<tr><td>(2) INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS
The organization employs automated tools to support near real-time analysis of events.
Supplemental Guidance: Automated tools include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by organizational information systems.
(4) INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC
The information system monitors inbound and outbound communications traffic [Assignment: organization-defined frequency] for unusual or unauthorized activities or conditions.
Supplemental Guidance: Unusual/unauthorized activities or conditions related to information system inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within organizational information systems or propagating among system components, the unauthorized exporting of information, or
Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems
and Organizations
signaling to external information systems. Evidence of malicious code is used to identify potentially compromised information systems or information system components.
(5) INFORMATION SYSTEM MONITORING | SYSTEM-GENERATED ALERTS
The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].</td><td></td></tr>
<tr><td>Supplemental Guidance: Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the notification list can include, for example, system administrators, mission/business owners, system owners, or information system security officers. Related controls: AU-5, PE-6.</td><td></td></tr>
</table>

NIST CONTROL	CLOUDCHECKR SUPPORT ACTIVITY
SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES Control: The organization: a. Receives information system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	CloudCheckr automates both the collection and dissemination of infrastructure related security and usage concerns. Configurable checks are used to ensure policy adherence.
Supplemental Guidance: The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations. Related control: SI-2.	