Security at Scale: Logging in AWS

How AWS CloudTrail can help you achieve compliance by logging API calls and changes to resources

October 2015

Table of Contents

Abstract

The logging and monitoring of API calls are key components in security and operational best practices, as well as requirements for industry and regulatory compliance. AWS CloudTrail is a web service that records API calls to supported AWS services in your AWS account and delivers a log file to your Amazon Simple Storage Service (Amazon S3) bucket. AWS CloudTrail alleviates common challenges experienced in an on-premise environment and in addition to making it easier for you to demonstrate compliance with policies or regulatory standards, the service makes it easier for you to enhance your security and operational processes.

This paper provides an overview of common compliance requirements related to logging and details how AWS CloudTrail features can help satisfy these requirements. There is no additional charge for AWS CloudTrail, aside from standard charges for S3 for log storage and SNS usage for optional notification.

Introduction

Amazon Web Services (AWS) provides a wide variety of on-demand IT resources and services that you can launch and manage with pay-as-you-go pricing. Recording the AWS API calls and associated changes in resource configuration is a critical component of IT governance, security, and compliance. AWS CloudTrail provides a simple solution to record AWS API calls and resource changes that helps alleviate the burden of on-premises infrastructure and storage challenges by helping you to build enhanced preventative and detective security controls for your AWS environment. On-premises logging solutions require installing agents, setting up configuration files and centralized log servers, and building and maintaining expensive, highly durable data stores to store the data. AWS CloudTrail eliminates this burdensome infrastructure set-up and allows you to turn on logging in as little as two clicks and get increased visibility into all API calls in your AWS account. CloudTrail continuously captures API calls from multiple servers into a highly available processing pipeline. To turn on CloudTrail, you simply sign-in to the AWS Management Console, navigate to the CloudTrail console, and click to enable logging. Learn more about services and regions available for use with AWS CloudTrail on the AWS CloudTrail website.

This paper was developed by taking an inventory of logging requirements across common compliance frameworks (e.g. ISO 27001:2005, PCI DSS v2.0, FedRAMP, etc.) and combining those into generalized controls and logging domains. You may leverage this paper for a variety of use-cases such as security and operational best-practices, compliance with internal policies, industry standards, legal regulations, and more. The paper is written generically to allow anyone to understand how AWS CloudTrail can enhance your existing logging and monitoring activities.

Control Access to Log Files

To maintain the integrity of your log data, it is important to carefully manage access around the generation and storage your log files. The ability to view or modify your log data should be restricted to authorized users. A common log-related challenge for on-premise environments is the ability to demonstrate to regulators that access to log data is restricted to authorized users. This control can be time-consuming and complicated to demonstrate effectively because most on-premise environments do not have a single logging solution or consistent logging security across all systems.

With AWS CloudTrail, access to Amazon S3 log files is centrally controlled in AWS, which allows you to easily control access to your log files and help demonstrate the integrity and confidentiality of your log data.

	Common logging requirements	How AWS CloudTrail can help you achieve compliance with requirements
Control Access to Log Files	Controls exist to prevent unauthorized access to logs.	AWS CloudTrail provides you the ability to restrict access to your log files. You can prevent and control access to make changes to your log file data by configuring your AWS Identity and Access Management (IAM) roles and Amazon S3 bucket policies to enforce read-only access to your log files. Learn more. Additionally, you can fortify your authentication and authorization controls by enabling AWS Multi Factor Authentication (AWS MFA) on your Amazon S3 bucket(s) that store(s) your AWS CloudTrail logs. Learn more.
	Controls exist to ensure access to log records is role-based.	AWS CloudTrail provides you the ability to control user access on your log files based on detailed role-based provisioning. AWS Identity and Access Management (IAM) enables you to securely control access to AWS CloudTrail for your users; And using IAM roles and Amazon S3 bucket policies, you can enforce role-based access to the S3 bucket that stores your AWS CloudTrail log files. Learn More.

Obtain Alerts on Log File Creation and Misconfiguration

Near-real-time alerts to misconfigurations of logs detailing API calls or resource changes is critically important to effective IT governance and adherence to internal and external compliance requirements. Even from an operational perspective, it is imperative that logging is configured properly to give you the ability to oversee the activities of your users and resources. However, variability and breadth of logging infrastructure in on-premise environments has made it overwhelming to actively monitor and alert you when there are misconfigurations or changes to your logging configuration.

Once you enable AWS CloudTrail for your account, the service will deliver log files to your S3 bucket. Optionally, CloudTrail will publish notifications for log file deliveries to an SNS topic so that you can take action upon delivery. These alerts include the Amazon S3 bucket log file address to allow you to quickly access object metadata about the event from the source log files. Moreover, your AWS Management Console will alert you if your log files are misconfigured and therefore logging is no longer taking place.

	Common logging requirements	How AWS CloudTrail can help you achieve compliance with requirements
Receive Alerts for Log File Creation and Misconfiguration	Provide alerts when logs are created or fail and follow organization-defined actions in the event of a misconfiguration.	AWS CloudTrail provides you immediate notification related to problems with your logging configuration through your AWS Management Console. Learn more.
	Alerts related to log misconfiguration will direct users to relevant logs for additional details (and will not divulge unnecessary amount of detail).	AWS CloudTrail records the Amazon S3 bucket log file address every time a new log file is written. AWS CloudTrail publishes notifications for log file creation so that customers can take near-real-time action when log files are created. The notification is delivered to your Amazon S3 bucket and is shown in the AWS Management Console. Optionally, Amazon SNS messages can be pushed to mobile devices or distributed services, configured via API or the AWS Management Console. The SNS message for log file creation provides the log file address, which limits the information divulged to only the necessary amount, while also enabling you to easily link to obtain additional event details. Learn more.

Manage Changes to AWS Resources and Log Files

Understanding the changes made to your resources is a critical component of IT governance and security. Moreover, preventing changes and unauthorized access to this log data directly impacts the integrity of your change management processes and your ability to comply with internal, industry and regulatory requirements around change management. A major challenge faced in on-premise environments is the ability to log resource changes or changes to logs because there are only finite resources at your disposal to monitor what feels like an infinite amount of data.

AWS CloudTrail allows you to track the changes that were made to an AWS resource, including creation, modification and deletion. Additionally, by reviewing the log history of API calls, AWS CloudTrail helps you investigate an event to determine if unauthorized or unexpected changes occurred by reviewing who initiated them, when they occurred, and where they originated. Optionally, CloudTrail will publish notifications to an SNS topic so that you can take action upon delivery of the new log file to your Amazon S3 bucket.

Manage Changes to IT Resources and Log Files	Common logging requirements	How AWS CloudTrail can help you achieve compliance with requirements
	Provide log of changes to system components (including creation and deletion of system-level objects).	AWS CloudTrail produces log data on system change events to enable tracking of changes made to your AWS resources. AWS CloudTrail provides visibility into any changes made to your AWS resource from its creation to deletion by logging changes made using API calls via the AWS Management Console, the AWS Command Line Interface (CLI), or the AWS Software Development Kits (SDKs). Learn more.
	Controls exist to prevent modifications to logs of changes or failures associated with logs.	By default, API call log files are encrypted using S3 Server Side Encryption (SSE) and placed into your S3 bucket. Modifications to log data can be controlled through use of IAM and MFA to enforce read-only access to your Amazon S3 bucket that stores your AWS CloudTrail log files. Learn more.

Storage of Log Files

Industry standards and legal regulations may require that log files be stored for varying periods of time. For example, PCI DSS requires logs be stored for one year, HIPAA requires that records be retained for at least six years, and other requirements mandate longer or variable storage periods depending on the data being logged. As such, managing the requirements for log file storage for different data on different systems can be an administrative and technological burden. Moreover, storing and archiving large volumes of log data in a persistent and secure way can be a challenge for many organizations.

AWS CloudTrail is designed to seamlessly integrate with Amazon S3 and Amazon Glacier, allowing customization of S3 buckets and lifecycle rules to suit your storage needs. AWS CloudTrail provides you an indefinite expiration period on your logs, so you can customize the period of time you store your logs to meet your regulators' requirements.

	Common logging requirements	How AWS CloudTrail can help you achieve compliance with requirements
Storage of Log Files	Logs are stored for at least one year.	For ease of log file storage, you can configure AWS CloudTrail to aggregate your log files across all regions and/or across multiple accounts to a single S3 bucket. AWS CloudTrail provides the ability to customize your log storage period by configuring your desired expiration period(s) on log files written to your Amazon S3 bucket. You control the retention policies for your CloudTrail log files. You can retain log files for a time period of your choice or indefinitely. By default, log files are stored indefinitely. You can also move your log file data to Amazon Glacier for additional cost savings associated with cold storage. Learn more.
	Store logs for an organization-defined period of time.	
	Store logs real-time for resiliency.	AWS CloudTrail provides you with log file resiliency by leveraging Amazon S3, a highly durable storage infrastructure. Amazon S3's standard storage is designed for 99.999999999% durability and 99.99% availability of objects over a given year. Learn more.

Generate Customized Reporting of Log Data

From an operational and security perspective, API call logging provides the data and context required to analyze user behavior and understand certain events. API calls and IT resource change logs can also be used to demonstrate that only authorized users have performed certain tasks in your environment in alignment with compliance requirements. However, given the volume and variability associated with logs from different systems, it can be challenging in an on-premise environment to gain a clear understanding of the activities users have performed and the changes made to your IT resources.

AWS CloudTrail produces data you can use to detect abnormal behavior, retrieve event activities associated with specific objects, or provide a simple audit trail for your account. You can evolve your current logging analytics by using the 25+ different fields in the event data that AWS CloudTrail provides to build queries and create customized reports focused on internal investigations, external compliance, etc. AWS CloudTrail enables you to monitor API calls for specific known undesired behavior(s) and raise alarms using your log management or security incident and event management (SIEM) solutions. The enriched data provided by AWS CloudTrail can accelerate your investigation time and decrease your incident response time. Additionally, data provided by AWS CloudTrail may enable you to perform a deeper security analysis on API calls to identify suspicious behavior and latent patterns that don't trigger immediate alarms but which may represent a

security issue. Finally, AWS CloudTrail works with an extensive range of partners with ready-to-run solutions for security, analytics, and alerting. Learn more about our partner solutions on the AWS CloudTrail website.

	Common logging requirements	How AWS CloudTrail can help you achieve compliance with requirements
Generate Customized Reporting of Log Data	Log individual user access to resources, by system accessed and actions taken. "Individual user access" includes access by system administrators and system operators; "Resources" includes audit trail logs.	AWS CloudTrail provides the ability to generate comprehensive and detailed API call reports by logging activities performed by all users who access your logged AWS resources, including root, IAM users, federated users, and any users or services performing activities on behalf of users, using any access method. Learn more.
	Produce logs at an organization-defined frequency.	AWS CloudTrail provides the ability to use log analysis tools to retrieve log file data at customized frequencies by creating logs in near-real-time and generally delivering the log data to your Amazon S3 bucket within 15 minutes of the API call. You can use the log files as an input into industry leading log management and analysis solutions to perform analytics. Learn more.
	Provide a log of when logging activity was initiated.	AWS CloudTrail logs all API calls, including enabling and disabling AWS CloudTrail logging. This allows you to track when CloudTrail itself was turned on or off. Learn more.
	Generate logs synched to a single internal system clock to provide consistent time stamp information.	AWS CloudTrail produces log data from a single internal system clock by generating event time stamps in Coordinated Universal Time (UTC), consistent with the ISO 8601 Basic Time and date format standard. Learn more.
	Provide logs that can show if inappropriate or unusual activity has occurred.	AWS CloudTrail enables you to monitor API calls by recording authorization failures in your AWS account allowing you to track attempted access to restricted resources or other unusual activity. Learn more.
	Provide logs with adequate event details.	AWS CloudTrail delivers API calls with detailed information such as type, data and time, location, source/origin, outcome (including exceptions, faults and security-event information), affected resource (data, system, etc.) and associated user. AWS CloudTrail can help you identify the user, time of the event, IP address of the user, request parameters provided by the user, response elements returned by the service and optional error code and error message. Learn more.

Conclusion

You can run nearly anything on AWS that you would run on on-premise: websites, applications, databases, mobile apps, email campaigns, distributed data analysis, media storage, and private networks. The services AWS provides are designed to work together so that you can build complete solutions. AWS CloudTrail provides a simple solution to log user activity that helps alleviate the burden of running a complex logging system. Another benefit of migrating workloads to AWS is the ability to achieve a higher level of security, at scale, by utilizing the many governance-enabling features offered. For the same reasons that delivering infrastructure in the cloud has benefits over on-premise delivery, cloud-based governance offers a lower cost of entry, easier operations and improved agility by providing more visibility, security control, and central

automation. AWS CloudTrail is one of the services you can use to achieve a high level of governance of your IT resources using AWS.

Additional Resources

Below are links in response to commonly asked questions related to logging in AWS:

- What can I do with AWS? Learn more.
- How can I get started with AWS? Learn more.
- How can I get started with AWS CloudTrail? Learn more.
- Does AWS CloudTrail have a list of FAQs? Learn more.
- How can I achieve compliance while using AWS? Learn more.
- How can I prepare for an audit while using AWS? Learn more.

Appendix: Compliance Program Index

The information in the whitepaper above was presented by logging requirement domains. For your reference, the logging requirements by common compliance frameworks are listed in the table below:

AWS Compliance Program	Compliance Requirement
Payment Card Industry (PCI) Data Security Standard (DSS) Level 1 AWS is Level 1 compliant under the PCI DSS. You can run applications on our PCI-compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud. Learn more.	**PCI 5.2:** Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.
	PCI 10.1: Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.
	PCI 10.2: Implement automated audit trails for all system components to reconstruct the following events: **10.2.1:** All individual accesses to cardholder data **10.2.2:** All actions taken by any individual with root or administrative privileges **10.2.3:** Access to all audit trails **10.2.4:** Invalid logical access attempts **10.2.5:** Use of identification and authentication mechanisms **10.2.6:** Initialization of the audit logs **10.2.7:** Creation and deletion of system-level objects
	PCI 10.3: Record at least the following audit trail entries for all system components for each event: **10.3.1:** User identification **10.3.2:** Type of event **10.3.3:** Date and time **10.3.4:** Success or failure indication **10.3.5:** Origination of the event **10.3.6:** Identity or name of affected data, system component, or resource
	PCI 10.4.2: Time data is protected.
	PCI 10.5: Secure audit trails so they cannot be altered.
	PCI 10.5.1: Limit viewing of audit trails to those with a job-related need.
	PCI 10.5.2: Protect audit trail files from unauthorized modifications.
	PCI 10.5.3: Promptly back up audit trail files to a centralized log server or media that is difficult to alter.

AWS Compliance Program	Compliance Requirement
Payment Card Industry (PCI) Data Security Standard (DSS) Level 1 AWS is Level 1 compliant under the PCI DSS. You can run applications on our PCI-compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud. Learn more.	**PCI 10.5.4:** Write logs for external-facing technologies onto a log server on the internal LAN.
	PCI 10.5.5: Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).
	PCI 10.6: Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).
	PCI 10.7: Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).
	PCI 11.5: Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.
	PCI 12.2: Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).
	PCI A.1.2.d: Restrict each entity's access and privileges to its own cardholder data environment only.
	PCI A.1.3: Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.
	PCI 11.4: Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.

AWS Compliance Program	Compliance Requirement
Payment Card Industry (PCI) Data Security Standard (DSS) Level 1 AWS is Level 1 compliant under the PCI DSS. You can run applications on our PCI-compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud. Learn more.	**PCI 11.5:** Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.
Service Organization Controls 2 (SOC 2) The SOC 2 report is an attestation report that expands the evaluation of controls to the criteria set forth by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles. These principles define leading practice controls relevant to security, availability, processing integrity, confidentiality, and privacy applicable to service organizations such as AWS. Learn more.	**SOC 2 Security 3.2.g:** Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: Restriction of access to system con-figurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).
	SOC 2 Security 3.3: Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.
	SOC 2 Security 3.7: Procedures exist to identify, report, and act upon system security breaches and other incidents.
	SOC 2 Availability 3.5.f: Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: Restriction of access to system configurations, superuser functionality, master pass-words, powerful utilities, and security devices (for example, firewalls).
	SOC 2 Availability 3.6: Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other sys-tem components such as firewalls, routers, and servers.

AWS Compliance Program	Compliance Requirement
Service Organization Controls 2 (SOC 2) The SOC 2 report is an attestation report that expands the evaluation of controls to the criteria set forth by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles. These principles define leading practice controls relevant to security, availability, processing integrity, confidentiality, and privacy applicable to service organizations such as AWS. Learn more.	**SOC 2 Availability 3.10:** Procedures exist to identify, report, and act upon system availability issues and related security breaches and other incidents.
	SOC 2 Confidentiality 3.3: The system procedures related to confidentiality of data processing are consistent with the documented confidentiality policies.
	SOC 2 Confidentiality 3.8.1: Procedures exist to restrict logical access to the system and the confidential information resources maintained in the system including, but not limited to, the following matters: Restriction of access to system con-figurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).
	SOC 2 Confidentiality 3.13: Procedures exist to identify, report, and act upon system confidentiality and security breaches and other incidents.
	SOC 2 Confidentiality 4.2: There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its system confidentiality and related security policies.
	SOC 2 Integrity 3.6.g: Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls)
	SOC 2 Integrity 4.1: System processing integrity and security performance are periodically re-viewed and compared with the defined system processing integrity and related security policies.
	SOC 2 Integrity 4.2: There is a process to identify and ad-dress potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system processing integrity and related security policies.

AWS Compliance Program	Compliance Requirement
International Organization for Standardization (ISO) 27001 ISO 27001 is a widely-adopted global security standard that outlines the requirements for information security management systems. It provides a systematic approach to managing company and customer information that's based on periodic risk assessments. Learn more.	*Due to copyright laws, AWS cannot provide the requirement descriptions for ISO 27001. You may purchase a copy of the ISO 27001 standard online from various sources, including ISO.org*
Federal Risk and Authorization Management Program (FedRAMP) FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services up to the Moderate level. Learn more.	**FedRAMP NIST 800-53 Rev 3 AU-2:** The organization: a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [Assignment: organization-defined list of 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 list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [Assignment: organization- defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event].
	FedRAMP NIST 800-53 Rev 4 AU 2: The organization: a. Determines that the information system must be 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 subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event].
	FedRAMP NIST 800-53 Rev 3 AU-3: The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.

AWS Compliance Program	Compliance Requirement
Federal Risk and Authorization Management Program (FedRAMP) FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services up to the Moderate level. Learn more.	**FedRAMP NIST 800-53 Rev 4 AU-3:** The information system produces audit records containing information that, at a minimum, 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 user or subject associated with the event.
	FedRAMP NIST 800-53 Rev 3 AU-4: The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.
	FedRAMP NIST 800-53 Rev 4 AU-4: The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].
	FedRAMP NIST 800-53 Rev 3 AU-5: The information system: a. Alerts designated organizational officials 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)].
	FedRAMP NIST 800-53 Rev 4 AU-5: The information system: a. Alerts [Assignment: organization-defined personnel] 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)].
	FedRAMP NIST 800-53 Rev 3 AU-6: The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.
	FedRAMP NIST 800-53 Rev 3 AU-6: 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].
	FedRAMP NIST 800-53 Rev 3 AU-8: The information system uses internal system clocks to generate time stamps for audit records.

AWS Compliance Program	Compliance Requirement
Federal Risk and Authorization Management Program (FedRAMP) FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services up to the Moderate level. Learn more.	**FedRAMP NIST 800-53 Rev 4 AU-8:** The information system: a. Uses internal system clocks to generate time stamps for audit records; and b. Generates time in the time stamps that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: organization-defined granularity of time measurement].
	FedRAMP NIST 800-53 Rev 3 AU-9: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.
	FedRAMP NIST 800-53 Rev 4 AU-9: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.
	FedRAMP NIST 800-53 Rev 3 AU-10: The information system protects against an individual falsely denying having performed a particular action.
	FedRAMP NIST 800-53 Rev 4 AU-10: The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [Assignment: organization-defined actions to be covered by non-repudiation].
	FedRAMP NIST 800-53 Rev 3 AU-11: 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.
	FedRAMP NIST 800-53 Rev 4 AU-11: 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.