



A-LIGN

Universal Technical
Resource Services, Inc.

Type 2 SOC 3

2022



SOC 3 FOR SERVICE ORGANIZATIONS REPORT

July 1, 2021 to June 30, 2022

Table of Contents

SECTION 1 ASSERTION OF UNIVERSAL TECHNICAL RESOURCE SERVICES, INC. MANAGEMENT	1
SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT	3
SECTION 3 UNIVERSAL TECHNICAL RESOURCE SERVICES, INC.'S DESCRIPTION OF ITS WEB-BASED ANALYTICAL TOOL (WBAT) SYSTEM THROUGHOUT THE PERIOD JULY 1, 2021 TO JUNE 30, 2022.....	7
OVERVIEW OF OPERATIONS.....	8
Company Background	8
Description of Services Provided	8
Principal Service Commitments and System Requirements.....	8
Components of the System.....	9
Boundaries of the System.....	14
Changes to the System in the Last 12 Months.....	14
Incidents in the Last 12 Months	14
Criteria Not Applicable to the System	15
Subservice Organizations	15
COMPLEMENTARY USER ENTITY CONTROLS.....	17

SECTION 1

**ASSERTION OF UNIVERSAL TECHNICAL RESOURCE
SERVICES, INC. MANAGEMENT**

ASSERTION OF UNIVERSAL TECHNICAL RESOURCE SERVICES, INC. MANAGEMENT

August 19, 2022

We are responsible for designing, implementing, operating, and maintaining effective controls within Universal Technical Resource Services, Inc.'s ('UTRS' or 'the Company') Web-Based Analytical Tool (WBAT) System throughout the period July 1, 2021 to June 30, 2022, to provide reasonable assurance that UTRS' service commitments and system requirements relevant to Security, Processing Integrity, and Confidentiality (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in "Universal Technical Resource Services, Inc.'s Description of Its Web-Based Analytical Tool (WBAT) System throughout the period July 1, 2021 to June 30, 2022" and identifies the aspects of the system covered by our assertion.

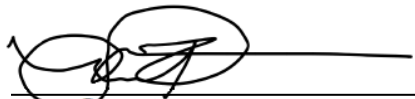
We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2021 to June 30, 2022, to provide reasonable assurance that UTRS' service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Processing Integrity, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. UTRS' objectives for the system in applying applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "Universal Technical Resource Services, Inc.'s Description of Its Web-Based Analytical Tool (WBAT) System throughout the period July 1, 2021 to June 30, 2022".

UTRS uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at UTRS, to achieve UTRS' service commitments and system requirements based on the applicable trust services criteria. The description presents UTRS' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of UTRS' controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve UTRS' service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of UTRS' controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period July 1, 2021 to June 30, 2022 to provide reasonable assurance that UTRS' service commitments and system requirements were achieved based on the applicable trust services criteria.



Marc Snyderman
General Counsel
Universal Technical Resource Services, Inc.

SECTION 2
INDEPENDENT SERVICE AUDITOR'S REPORT



INDEPENDENT SERVICE AUDITOR'S REPORT

To: Universal Technical Resource Services, Inc.

Scope

We have examined Universal Technical Resource Services, Inc.'s ('UTRS' or 'the Company') accompanying description of Web-Based Analytical Tool (WBAT) System titled "Universal Technical Resource Services, Inc.'s Description of Its Web-Based Analytical Tool (WBAT) System throughout the period July 1, 2021 to June 30, 2022" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria)*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period July 1, 2021 to June 30, 2022, to provide reasonable assurance that UTRS' service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Processing Integrity, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

UTRS uses AWS to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at UTRS, to achieve UTRS' service commitments and system requirements based on the applicable trust services criteria. The description presents UTRS' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of UTRS' controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at UTRS, to achieve UTRS' service commitments and system requirements based on the applicable trust services criteria. The description presents UTRS' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of UTRS' controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

UTRS is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that UTRS' service commitments and system requirements were achieved. UTRS has provided the accompanying assertion titled "Assertion of Universal Technical Resource Services, Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. UTRS is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within UTRS' Web-Based Analytical Tool (WBAT) System were suitably designed and operating effectively throughout the period July 1, 2021 to June 30, 2022, to provide reasonable assurance that UTRS' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

The SOC logo for Service Organizations on UTRS' website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of UTRS, user entities of UTRS' Web-Based Analytical Tool (WBAT) during some or all of the period July 1, 2021 to June 30, 2022, business partners of UTRS subject to risks arising from interactions with the Web-Based Analytical Tool (WBAT), and those who have sufficient knowledge and understanding of the complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
August 19, 2022

SECTION 3

UNIVERSAL TECHNICAL RESOURCE SERVICES, INC.'S DESCRIPTION OF ITS WEB-BASED ANALYTICAL TOOL (WBAT) SYSTEM THROUGHOUT THE PERIOD JULY 1, 2021 TO JUNE 30, 2022

OVERVIEW OF OPERATIONS

Company Background

UTRS was founded in 1985 as a commercial information technology professional placement business. In 1995, UTRS expanded their services to include consulting and engineering in diverse technical areas expanding their customer base to include government clients such as the Department of Defense (DOD), the Federal Aviation Administration (FAA), and the Federal Laboratory Consortium for Technology Transfer (FLC).

As its footprint within the federal marketplace increased, UTRS expanded service offerings to include many other technical disciplines and won SBA Prime Contractor of the Year for Region II in 2009 and 2013. Recognizing their commitment to recruiting, hiring and retaining veterans, the Labor Department awarded the UTRS the HIRE Vets Medallion Award in both 2020 and 2021.

Description of Services Provided

The UTRS Aviation Safety Division is focused on a safety culture where a fundamental understanding of risk identification, avoidance and mitigation is present and used as the cornerstone for all decisions. Working in support of the FAA, UTRS has developed and maintained a voluntary safety reporting tool in support of the Aviation Safety Action Program (ASAP) and Safety Management Systems (SMS). This tool, known as Web-Based Analytical Tool (WBAT), provides a comprehensive solution for the day-today management and operation of ASAP and incident reporting programs, including risk assessment, identification of appropriate remedial measures, and tracking of corrective actions. WBAT can be utilized by any company seeking to improve its operational safety culture. Based on open-source cloud-based software, this platform can be customized to fit any organization's structure:

- WBAT is the only FAA supported and verified system for safety reporting, including ASAP, Line Operational Safety Audits (LOSA) and the new Safety Management System (SMS)
- WBAT supports the submission, management, and analysis of confidential employee reports, including ASAP, incident, fatigue, LOSA, and general safety/hazard via the web or mobile device
- WBAT serves 194 operators and ~275,000 users representing all sectors of the aviation community: passenger flight, cargo, charter, flight schools, and MROs
- WBAT's Safety Management System (SMS) modules are fully compliant with 14 CFR Part 5: Safety Management System language
- WBAT de-identifies, warehouses, and distributes voluntary safety data to support multiple voluntary reporting programs such as Aviation Safety Reporting System (ASRS), Air Traffic Safety Action program (ATSAP), and Safety Trend Evaluation, Analysis and Data Exchange System (STEADDES)

Principal Service Commitments and System Requirements

The UTRS Aviation Safety Division designs its processes and procedures to meet its objectives for the Company's procedures. Those objectives are based on the service commitments that the UTRS Aviation Safety Division makes to its user entities, the laws and regulations that govern the provision of the Company's services, and the financial, operational, and compliance requirements that the UTRS Aviation Safety Division has established for those services. The Company's services are subject to state security and privacy requirements in the jurisdictions in which the UTRS Aviation Safety Division operates.

Security, processing integrity, and confidentiality commitments to user entities are documented and communicated in the service level agreements (SLAs) and other customer agreements, as well as in the description of services provided on its website. Security, processing integrity and confidentiality commitments are standardized and include, but are not limited to the following:

- The UTRS Aviation Safety Division shall protect the confidentiality of all information data, instruments, studies, reports, records, and other materials

- The UTRS Aviation Safety Division shall employ security measures and standards, including best practice encryption technologies, as may be necessary or proper, and as mutually agreed upon in the WBAT Software and Related Services Agreement
- The UTRS Aviation Safety Division warrants that the services shall remain accessible 24/7 except for scheduled outages for maintenance and other service level provisions agreed in writing and processed as mutually agreed upon in the contract

The UTRS Aviation Safety Division establishes the operational requirements that support the achievement of its security, processing integrity, and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Company system policies and procedures, system design documentation, and contracts with customers. The UTRS Aviation Safety Division policies define an organization-wide approach to how systems and data are protected, the processing of the system is maintained and monitored, and confidentiality of customer and the UTRS Aviation Safety Division data is maintained. The Division’s policies include how the service is designed and developed, how the system is operated and maintained, and how the internal business systems and networks are managed and how employees are hired and trained.

Components of the System

Infrastructure

The primary infrastructure used to provide UTRS’ WBAT System includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
Amazon Simple Storage Service (Amazon S3)	AWS	Document storage, logs, backups, and DNS redirects
Amazon Elastic Compute Cloud (EC2)		Virtual server instances
Amazon Elastic File System (EFS)		Elastic File System (NFS) - shared data drives
Elastic Load Balancing (ELB)		Elastic Load Balancing for front end services
VPC (Virtual Private Cloud)		Provides networking and network security
CloudTrail		Monitoring and Auditing of AWS Activity
CloudWatch		Logging and Monitoring of AWS and Server Activity
GuardDuty		Intrusion Detection
Amazon Relational Database Service (RDS)		Managed Database Servers (PostgreSQL)
Route53		DNS Hosting
Amazon Simple E-mail Service (SES)		Support for outbound SMTP E-mail
Amazon Simple Notification Service (Amazon SNS)		Simple Notification Service - E-mail Notifications for AWS events

Software

Primary software used to provide UTRS' WBAT System includes the following:

Primary Software		
Software	Operating System	Purpose
Apache	Ubuntu Linux	Web Server
Racket	Ubuntu Linux	Web/Application Server
PostgreSQL	Ubuntu Linux / AWS RDS	Database Server; client tools on Linux, server via Relational Database Service (RDS)/Software as a Service (SaaS)
Subversion	Ubuntu Linux	Software and configuration version and revision control, repository
Alfresco	Ubuntu Linux	Document management system

People

The Aviation Safety Division has a staff of approximately 22 employees and consultants including both full and part-time and those utilized on an as-needed basis.

UTRS Corporate provides ancillary support services, including:

- Human Resources
- Contracting
- Payroll
- Vendor Management
- Accounting

The UTRS Aviation Safety Division is organized in the following functional areas:

- Development and Operations:
 - Systems Network Administration:
 - Systems Administration
 - Cybersecurity
 - Software Development
 - Data Science
- Shared Services:
 - Technical Writer
 - Project Facilitator
- WBAT:
 - Program Management:
 - Customer Support
 - Business Development

The Division is headed by the Vice President, UTRS Aviation Safety Division and includes separate groups for WBAT, Development and Operations, and Shared Services.

The Development and Operations Group is led by the Vice President (VP), UTRS Aviation Safety Division, and includes the System Network Administrator, Systems Administrators and the Cybersecurity Manager who are primarily responsible for user administration, second-level security support security event monitoring and security incident response and management. The software developers and UX/UI designers and Data Scientist belong in this group and are tasked with developing and maintaining the WBAT software components, including upgrades, bugs, hotfixes, etc., and maintaining a consistent user experience.

The Shared Services Group is led by the VP, UTRS Aviation Safety Division and comprises the Technical Writer who drafts, edits and formats UTRS Aviation Safety Division documents for both internal and external users. The Project Facilitator provides administrative functions for the team including reservations and travel arrangement and approval and review of payroll and consultant invoicing, etc.

The WBAT Group is led by the WBAT Program Manager (PM), who reports to the VP, UTRS Aviation Safety Division. The WBAT PM is responsible for the overall function and operation of the WBAT team members. The Business Development Team includes marketing of the product along with the SMS Manager and team. The Customer Support Team provides direct support to customers, and product management which involves overseeing the entire change process (customer request, upgrades, bugs, etc.) using the ticketing system to track changes through the entire process from request to final validation and release.

Users of the system primarily consist of the following:

- Customers whose employees have access to the front-end application/dashboards via separate instances
- UTRS Aviation Safety Division supports employees who have access to front end applications/dashboards
- Specific UTRS Aviation Safety Division personnel who have access to the databases via SSH through a bastion host
- All UTRS Aviation Safety Division employees who are assigned unique user IDs that grant them role-based access to specific system resources and data
- Specific Administrative users from the UTRS Aviation Safety Division who have AWS Management Console access and SSH access to the systems for support

Data

Confidential policies and processes have been implemented to limit access to logical input routines and physical media to authorized individuals. Data determined to be confidential is subject to the policies which define protection requirements, access rights, and access restrictions, as well as retention and destruction requirements:

- Customer information and data is presumed confidential by default
- Vendor and business partner information is presumed to be confidential
- All non-public customer information is confidential

All inputs and outputs are conducted via a web browser and/or mobile application using best practice encryption method while in-transit.

WBAT data is customer owned/controlled:

- Submissions by employee users
- Employee submitted attachments (optional)
- Reports created/modified by customer analysts
- Additional reports created/modified during the customer review process

In addition to safety submission created by customers' employees, WBAT accepts operational data (employee lists and flight-schedule files) from customers.

Once data has entered the WBAT boundary, all data is encrypted at rest using best practice encryption methods, and processed within distinct virtual networks and segmented subnets, with the most secure subnets (data processing and databases) inaccessible from direct outside connections.

All Information Technology (IT) support operations are conducted via SSH or through the AWS console, using best practices for encryption and secure connections.

WBAT provides data back to end users either directly via web browser or mobile app, or by downloadable CSV and XML output using best practice encryption methods while in-transit.

WBAT provides data sharing connections with participating entities, such as NASA, ASIAs and the FAA. All connection arrangements are conducted using best practice encryption methods while in transit.

WBAT maintains session logs so that all activity is logged and can be audited in the event of a data incident or processing error. This includes user activity and data sharing activity.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the UTRS policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any UTRS team member.

Physical Security

WBAT and its supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls for WBAT. Specifics of security controls are available in various AWS certifications including both SOC 1 and 2, NIST RMF and FedRAMP ATO/P-ATO.

Logical Access

The UTRS Aviation Safety Division is a fully remote organization and does not use or maintain a "network." All access to WBAT is via the public internet. All WBAT team members are required to have a suitable password or passphrase that conforms to the WBAT Passphrase/Passphrase Protection Policy which conforms to the latest recommendations in NIST SP 800-63B Digital Identity Guidelines.

Upon hire, the appropriate Program Manager is notified of the new employee's start date. The Program Manager requests employee access to WBAT. The Systems Administrators provide access by applying a Role Based Access Control matrix to the employee's role determined by the Program Manager. The Program Manager is responsible for requesting access changes or removal of access based on transfer, promotion, or termination.

Semi-annually, Systems Administrators provide Program Managers with a list of employees/consultants with access to WBAT resources and the level of access granted. The Program Managers review the list and verify that both system access and the access level granted is still required.

WBAT/WBAT procedures follow the principles of "least privilege" and "that which is not explicitly allowed is denied."

System Administrators adhere to the highest security controls, which include full encryption both in-transit and at-rest (locally and remotely, i.e., on laptops and on servers). This includes the use of day-to-day management tools and protocols such as Secure Socket Shell (SSH), and Multi-factor Authentication (MFA) security tokens and best practice encryption methods.

Developers do not have access to the Production environment. Only System Administrators have access to update the Production environment, and only after new software has gone through a tightly controlled release and validation process.

Customers access individualized WBAT instances by default with a strong password/passphrase. WBAT also supports authentication with Single Sign-on solutions (SAML Federated). Customers are responsible for their employees' access rights and permissions. All WBAT data is customer property.

Computer Operations - Backups

All WBAT data is backed up multiple times per day using scripts and multiple automatic processes. Apart from AWS RDS Snapshots, all backups are performed using standard AWS tools and data formats which mitigate the risk of failure due to lost or unsupported versions of backup software.

In the event of an error, Sysadmins are automatically notified and troubleshoot to identify the cause, correct the issue and either re-run the backup job immediately or let it run as part of the next scheduled backup. Sysadmins manually validate backups to ensure each backup succeeded within the past 24 hours for each environment and address any issues.

WBAT uses AWS virtual infrastructure and services to backup and replicate databases, storage objects, AMIs, etc. All backups are encrypted, as are S3 buckets which are also versioned. Primary backups are stored in US-East and replicated to US-West (NorCal). In addition to data, Current versions of AMIs are maintained in US-West (NorCal) as "cold storage" for disaster recovery.

As an additional measure, once per day, encrypted backups are securely transferred to rsync.net which is independent of AWS.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents.

WBAT is hosted in AWS, and as a result, there are certain controls that are the responsibility of AWS (physical, power, cooling, certain aspects of security and intrusion detection), however WBAT is responsible for those controls which fall under its domain and control.

These controls for which WBAT is responsible include backups, firewall rules, incident monitoring and logging, performance monitoring and provisioning, and software/operating system updates and patching.

Systems Administrators monitor the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. WBAT is configured to use several AWS services to notify Systems Administrators when instance capacity reaches a predetermined point. Based on the frequency of warnings, instance type can be modified, or virtual capacity can be increased. Metrics are regularly monitored to determine if the base resources are adequate (CPU, memory, filesystems) and scaled up if necessary.

Change Control

The UTRS Aviation Safety Division maintains Change Management policies and procedures to guide personnel in documenting and implementing application and virtual infrastructure changes.

The change control procedure includes processes for identifying and logging change (bugs or enhancements), initiating changes, validating changes, approvals, and integrating changes into production systems. Change requests are submitted as either bugs via the system or Zendesk help center tickets, or as enhancements via feedback or Zendesk help center tickets. The Zendesk application seamlessly integrates with Podio to automatically create a task within Podio from the help center ticket.

All change requests, regardless of source, are merged into Podio and assigned to a release or sprint, with the impact and effort assessed by the development team.

All changes completed in a sprint and/or release are made in a branch of the software, so the changes are isolated until they are functionally validated and meet customer requirements.

Once all changes have been validated, the branch is merged into the main software branched and tagged as a release, validated again, and then approved by the VP, UTRS Aviation Safety Division.

The finished Release is then pushed to all systems by Systems Administrators.

Data Communications

WBAT utilizes AWS components to tightly control firewall rules (via Access Control Lists- ACL) and Security Groups (SG), to only allow traffic and protocols that are necessary, and denying all others which are not explicitly permitted or required. ACLs control access through the non-routable IP Address used by the Virtual Private Cloud. SGs provide individual instance-level access control, i.e., each EC2 and RDS “virtual server” instance can be provided with individualized access. This in effect provides both a network (VPC) and server (SG) firewall.

Redundancy is a key feature of cloud-based systems such as AWS. WBAT utilizes a combination of AWS components and self-managed architecture and techniques to provide for resiliency of the application: load balancing, redundancy, and fail-over. These features are applied to both the application and database layers.

WBAT utilizes a combination of AWS and other components to monitor for intrusions, seeks recommendations of configuration findings and also performs vulnerability scans regularly to find security issues that need to be corrected.

Vulnerability scanning is conducted monthly, and the results are reviewed, and corrective action taken when required.

Boundaries of the System

The scope of this report includes the WBAT System performed in Cherry Hill, New Jersey.

This report does not include the cloud hosting services provided by AWS at the multiple regional facilities.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Criteria Not Applicable to the System

All Security, Processing Integrity and Confidentiality criteria were applicable to the UTRS WBAT System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS at multiple regional facilities.

Subservice Description of Services

AWS provides cloud hosting services, which includes implementing physical and environmental controls to protect the housed in-scope systems. Controls include, but are not limited to, visitor sign-ins, required use of badges for authorized personnel, and monitoring and logging of physical access to the facilities.

Complementary Subservice Organization Controls

UTRS' services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to UTRS' services to be solely achieved by UTRS control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of UTRS.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - AWS		
Category	Criteria	Control
Common Criteria/Security	CC6.1, CC6.4	Recovery key materials used for disaster recovery processes by KMS are physically secured offline so that no single AWS employee can gain access to the key material.
	CC6.1, CC6.6	Network devices are configured by AWS to only allow access to specific ports on other server systems within Amazon S3.
		External data access is logged with the following information: data accessor IP address, object and operation. Logs are retained for at least 90 days.
		S3 generates and stores a one-way salted HMAC of the customer encryption key. This salted HMAC value is not logged.
		Requests in KMS are logged in AWS CloudTrail.
	CC6.1, CC6.6, CC6.7	Customer master keys used for cryptographic operations in KMS are logically secured so that no single AWS employee can gain access to the key material.
		AWS Services that integrate with AWS KMS for key management use a 256-bit data key locally to protect customer content.
		The key provided by KMS to integrated services is a 256-bit key and is encrypted with a 256-bit advanced encryption standard (AES) master key unique to the customer's AWS account.
	CC6.4	Physical access to data centers is approved by an authorized individual.

Subservice Organization - AWS		
Category	Criteria	Control
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Access to server locations is managed by electronic access control devices.
	CC6.4, CC7.2	Closed circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
	CC6.5	All AWS production media is securely decommissioned and physically destroyed prior to leaving AWS Secure Zones.
		AWS provides customers the ability to delete their content. Once successfully removed the data is rendered unreadable.
		AWS retains customer content per customer agreements.
CC7.2	Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.	
Confidentiality	C1.1	AWS retains customer content per customer agreements.
		If enabled by the customer, RDS backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.
		S3 performs continuous integrity checks of the data at rest. Objects are continuously validated against their checksums to prevent object corruption.
		When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.
		Objects are stored redundantly across multiple fault-isolated facilities.
		The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service.
	C1.2	All AWS production media is securely decommissioned and physically destroyed prior to leaving AWS Secure Zones.
		AWS provides customers the ability to delete their content. Once successfully removed the data is rendered unreadable.

UTRS management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, UTRS performs monitoring of the subservice organization controls, including the following procedures:

- Annual review of the AWS SOC 2 Type 2 attestation report
- Annual review of the AWS CSA Consensus Assessments Initiative Questionnaire (CAIQ)
- Annual review of AWS compliance programs and services

COMPLEMENTARY USER ENTITY CONTROLS

UTRS' services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to UTRS' services to be solely achieved by UTRS control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of UTRS'.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to UTRS.
2. User entities are responsible for notifying UTRS of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own systems of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of UTRS services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize UTRS services.
6. User entities are responsible for providing UTRS with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying UTRS of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.