A-LIGN

Automation Anywhere, Inc.

Type 2 SOC 3

2022

AUTOMATION ANYWHERE

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

November 1, 2021 to October 31, 2022

Table of Contents

SECTION 1

ASSERTION OF AUTOMATION ANYWHERE, INC. MANAGEMENT

ASSERTION OF AUTOMATION ANYWHERE, INC. MANAGEMENT

January 9, 2023

We are responsible for designing, implementing, operating, and maintaining effective controls within Automation Anywhere, Inc.'s ('Automation Anywhere' or 'the Company') Automation 360 Cloud Services System throughout the period November 1, 2021 to October 31, 2022, to provide reasonable assurance that Automation Anywhere's service commitments and system requirements relevant to Security, Availability, and Confidentiality (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in "Automation Anywhere, Inc.'s Description of Its Automation 360 Cloud Services System throughout the period November 1, 2021 to October 31, 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 November 1, 2021 to October 31, 2022, to provide reasonable assurance that Automation Anywhere's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, 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*). Automation Anywhere's 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 "Automation Anywhere, Inc.'s Description of Its Automation 360 Cloud Services System throughout the period November 1, 2021 to October 31, 2022".

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

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Automation Anywhere's 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 Automation Anywhere's 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 November 1, 2021 to October 31, 2022 to provide reasonable assurance that Automation Anywhere's service commitments and system requirements were achieved based on the applicable trust services criteria.

Prince Kohli

Prince Kohli
Chief Technology Officer
Automation Anywhere, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Automation Anywhere, Inc.:

Scope

We have examined Automation Anywhere, Inc.'s ('Automation Anywhere' or 'the Company') accompanying description of Automation 360 Cloud Services System titled "Automation Anywhere, Inc.'s Description of Its Automation 360 Cloud Services System throughout the period November 1, 2021 to October 31, 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 November 1, 2021 to October 31, 2022, to provide reasonable assurance that Automation Anywhere's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, 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*).

Automation Anywhere uses Amazon Web Services ('AWS') and Google Cloud Platform ('GCP') to provide cloud hosting services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Automation Anywhere, to achieve Automation Anywhere's service commitments and system requirements based on the applicable trust services criteria. The description presents Automation Anywhere's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Automation Anywhere's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, 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 Automation Anywhere, to achieve Automation Anywhere's service commitments and system requirements based on the applicable trust services criteria. The description presents Automation Anywhere's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Automation Anywhere's 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

Automation Anywhere 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 Automation Anywhere's service commitments and system requirements were achieved. Automation Anywhere has provided the accompanying assertion titled "Assertion of Automation Anywhere, Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Automation Anywhere 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.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

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 Automation Anywhere's Automation 360 Cloud Services System were suitably designed and operating effectively throughout the period November 1, 2021 to October 31, 2022, to provide reasonable assurance that Automation Anywhere's 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 Automation Anywhere's 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 Automation Anywhere, user entities of Automation Anywhere's Automation 360 Cloud Services during some or all of the period November 1, 2021 to October 31, 2022, business partners of Automation Anywhere subject to risks arising from interactions with the Automation 360 Cloud Services, 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
January 9, 2023

SECTION 3

AUTOMATION ANYWHERE, INC.'S DESCRIPTION OF ITS AUTOMATION 360 CLOUD SERVICES SYSTEM THROUGHOUT THE PERIOD NOVEMBER 1, 2021 TO OCTOBER 31, 2022

OVERVIEW OF OPERATIONS

Company Background

Automation Anywhere’s goal is to enable companies to operate with unprecedented productivity and efficiency by automating any part of the enterprise that can be automated with their intelligent and intuitive robotic process automation platform.

The company’s vision is to take the robot out of the human. To liberate employees from mundane, repetitive tasks, allowing the employee to spend more time using their intellect and creativity to solve higher order business challenges. Automation Anywhere envisions a world where every employee will be empowered to be more productive and to drive more innovation, with all manual and routine tasks automated.

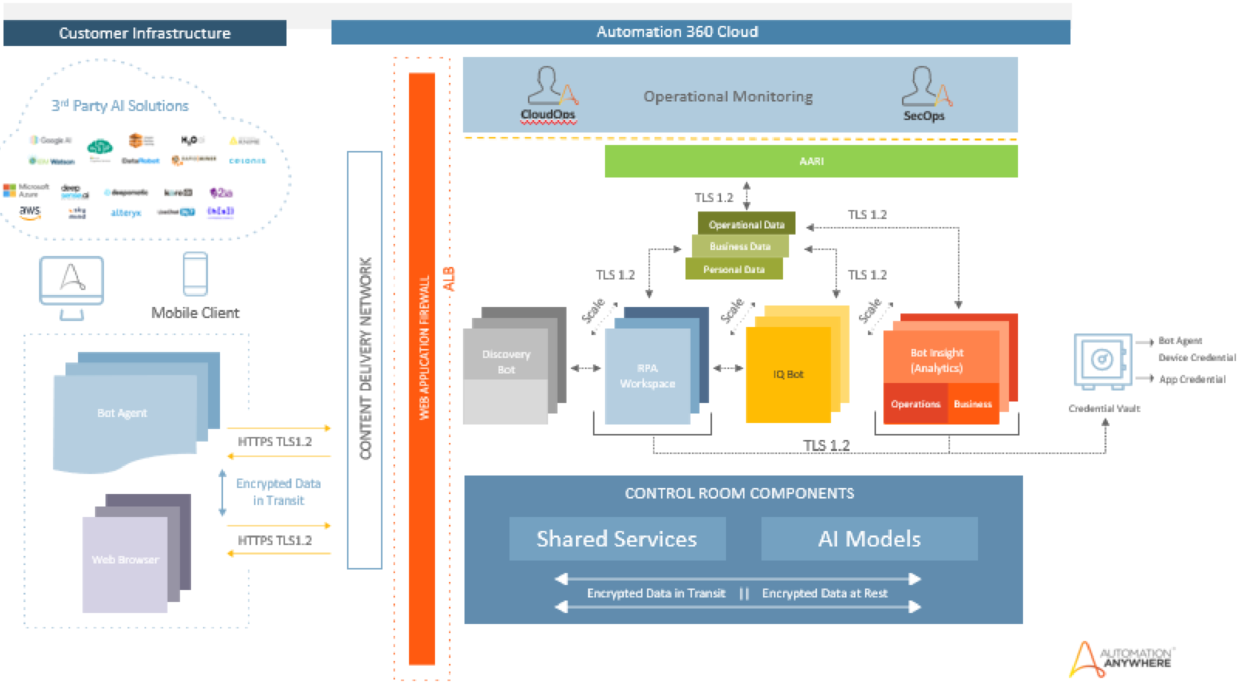
Automation 360 Cloud is a cloud-native intelligent automation platform, enabling companies to transcend front- and back-office silos and systems, both SaaS and legacy. Automation Anywhere Robotic Interface (AARI) is the digital assistant that simplifies automation so anyone can automate their business processes.

Description of Services Provided

The Automation 360 Cloud service is a hosted Automation Anywhere service delivery platform which supports the Automation 360 platform.

The Automation 360 platform comprises integrated Control Room and bot (short for robot) creation capabilities hosted on the Automation 360 Cloud with the ability to run cloud connected bot Agent nodes on the customer’s infrastructure via a secure and encrypted channel. The Automation 360 Cloud provides the same functionality as Automation 360 software deployed by the customer on their infrastructure but is deployed and operated by Automation Anywhere’s Cloud Operations team. Automation Anywhere’s Automation 360 Cloud allows Automation Anywhere to continually monitor and scale the supporting infrastructure for the customer. This provides multi-node high availability that powers service level agreement (SLA)-driven performance and business continuity, even when there are dramatic swings in automation workload.

A360 Cloud Reference Architecture



Principal Service Commitments and System Requirements

Automation Anywhere provides deployment and organizational security controls employed in connection with Automation 360 Cloud subscriptions.

The deployment model for Automation 360 Cloud involves customers building their bots and managing the bot deployments from the control room on Automation 360 Cloud. Once the bots are built, they are tested and run on the users' own compute infrastructure. Automation Anywhere's service commitment for Automation 360 Cloud is to maintain at least 99.9% monthly uptime on user browser access to the Automation 360 control room in a specified region.

Components of the System

Infrastructure

The in-scope system and supporting infrastructure is hosted by commercial Cloud Service Providers (CSP) AWS and GCP. As such, the CSP's are responsible for the physical infrastructure of the in-scope services.

AAI production environments are hosted is the following CSP regions:

AWS

us-west-2, us-west-1, ap-northeast-1, sa-east-1, me-south-1, eu-west-1, ap-southeast-1, ap-south-1, ap-southeast-2, us-east-1, af-south-1, us-gov-west-1.

GCP

us-central1, europe-west4, europe-west2, northamerica-northeast1, australia-southeast1.

AAI also utilities additional regions for its disaster recovery, and non-production environments (test, staging, and development).

Software

Primary software used to provide Automation 360 Cloud Services include the following:

Primary Software		
Software	**Type of Software**	**Purpose**
AWS Virtual Private Cloud (VPC)	Not applicable (Cloud Service)	Demarcation points to ensure all components are protected. AWS VPC allow provisioning of a logically isolated section of the AWS Cloud where the company can launch AWS resources in a virtual network that can be defined
AWS Network Address Translation (NAT) Gateway	Not applicable (Cloud Service)	Internet access for private instances
AWS Internet Gateway	Not applicable (Cloud Service)	Internet access for inbound traffic and public instances
AWS S3 (Object Storage)	Not applicable (Cloud Service)	Store's customer files for Discovery and IQ Bot services. Store Terraform (TF) state files, code artifacts etc.

Primary Software		
Software	**Type of Software**	**Purpose**
AWS Application Load Balancing (ALB)	Not applicable (Cloud Service)	Load balancing and allows external connectivity from customers
AWS Network File Share (EFS)	Not applicable (Cloud Service)	File share for Container Registry (CR) containers
AWS Route 53 (Domain Name System (DNS)	Not applicable (Cloud Service)	Domain name resolution
AWS Relational Database System (RDS) - MSSQL Database	Not applicable (Cloud Service)	Datastore for CR
AWS ElasticSearch	Not applicable (Cloud Service)	Logging for CR
AWS EC2 (Virtual Servers)	Linux	Elastic Kubernetes Service (EKS) Worker Nodes
AWS EC2 (Virtual Servers)	Windows Server 2016	IQ Bot instances
AWS EC2 (Virtual Servers)	Linux	Bastion Host
AWS Web Application Firewall (WAF)	Not applicable (Cloud Service)	Web Firewall Protection
AWS Identity and Access Management (IAM)	Not applicable (Cloud Service)	IAM service is used to provide access to cloud resources and services
AWS Elastic Kubernetes Service (EKS)	Not applicable (Cloud Service)	AWS EKS is a fully managed Kubernetes service
AWS Elastic Container Registry (ECR)	Not applicable (Cloud Service)	AWS ECR is a managed AWS Docker registry service that is secure, scalable, and reliable. AWS ECR supports private Docker repositories with resource-based permissions using AWS IAM so that specific users or AWS EC2 instances can access repositories and images
AWS GuardDuty	Not applicable (Cloud Service)	Threat and intrusion detection service
AWS Systems Manager (parameter stores)	Not applicable (Cloud Service)	Systems management service
AWS Secrets Manager	Not applicable (Cloud Service)	Secrets management service
AWS CloudFormation	Not applicable (Cloud Service)	Deploying security lambda functions into cloud security AWS account
AWS Certificate Manager (ACM)	Not applicable (Cloud Service)	ACM handles creating and managing public secure socket layer (SSL), transport layer security (TLS) certificates for AWS based websites and applications
AWS CloudWatch	Not applicable (Cloud Service)	Observability of AWS resources and applications on AWS

Primary Software		
Software	**Type of Software**	**Purpose**
AWS Key Management Service (KMS)	Not applicable (Cloud Service)	AWS key management service is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2
AWS Lambda	Not applicable (Cloud Service)	AWS Lambda lets users run code without provisioning or managing servers. Customers pay only for the compute time each consume
AWS Inspector	Not applicable (Cloud Service)	AWS Vulnerability scanner
GCP Cloud Armor	Not applicable (Cloud Service)	Web Application Firewall
GCP Cloud DNS	Not applicable (Cloud Service)	Domain Name System
GCP Cloud Key Management	Not applicable (Cloud Service)	Cloud hosted key management key systems
GCP Cloud Network Address Translation (NAT)	Not applicable (Cloud Service)	Network Address Translation to isolate internal Internet Protocol (IP) addresses from the Internet
GCP Cloud SQL	Not applicable (Cloud Service)	Cloud database
GCP Cloud Volumes	Not applicable (Cloud Service)	Cloud file storage
GCP ElasticSearch	Not applicable (Cloud Service)	Distributed JSON-based search and analytics engine
GCP - GKE Worker Nodes	Not applicable (Cloud Service)	Worker machines in Kubernetes are called nodes. GCP GKE worker nodes run in your GCP account and connect to your cluster's control plane via the cluster API server endpoint
GCP Compute - Bastion Host	Linux	A bastion host is a special-purpose computer designed to provide access to networked cloud resources
GCP Projects	Not applicable (Cloud Service)	Logical service subscription and isolation boundary
GCP Google Container Registry (GCR)	Not applicable (Cloud Service)	Managed Docker Registry service
GCP Google Cloud Storage (GCS)	Not applicable (Cloud Service)	Cloud object storage
GCP Google Kubernetes Engine (GKE)	Not applicable (Cloud Service)	Google managed Kubernetes service
GCP Google Secrets Manager	Not applicable (Cloud Service)	Secrets management service
GCP Internet Routes	Not applicable (Cloud Service)	Cloud network routing service

Primary Software		
Software	**Type of Software**	**Purpose**
GCP Load balancer	Not applicable (Cloud Service)	Cloud Load Balancing
GCP Virtual Private Cloud (VPC)	Not applicable (Cloud Service)	Virtual Private Cloud (VPC)
Lacework	Not applicable (Cloud Service)	Container security solution
Terraform	Not applicable	Infrastructure as code
Jenkins	Container Linux	Deployment automation tool a main component in continuous integration/continuous delivery (CI/CD) pipeline
Ops Genie	Not applicable (Cloud Service)	IT service management system
Site 24x7 (status page)	Not applicable (Cloud Service)	Website monitoring service
HELM Charts	Not applicable	Helm chart is a tool for building and versioning containers
Qualys	Not applicable (Cloud Service)	Vulnerability Scanner for Windows & Linux
Sumo Logic	Not applicable (Cloud Service)	Infrastructure monitoring and Security incident & event management (SIEM) tool
DigiCert CA	Not applicable (Cloud Service)	https://www.digicert.com/tls-ssl/compare-certificates
Okta	Not applicable (Cloud Service)	Single Sign-On (SSO)

People

Automation Anywhere staff is organized into following key functional areas:

- Corporate: Executives, senior operations staff, and company administrative support staff, such as legal, compliance, internal audit, training, contracting, accounting, finance, and human resources (HR). These individuals use the Automation 360 Cloud for reports done for Automation Anywhere's user entities
- Customer Success and Customer Support: Staff that provides technical assistance to the Automation 360 Cloud users
- Engineering: Staff that is responsible for the development and maintenance of the Automation 360 application, including the application services that are running within the Automation 360 Cloud:
    - The staff take issues from the customer support and customer success teams and work them to resolution, using tools within the Automation 360 Cloud. This team does not, by default, have access to the customers Automation 360 Control Room but may be granted access by the customer to facilitate providing support
    - The software development staff develops and maintains the custom software for Automation Anywhere. The staff includes software developers, database administration, software quality assurance, and technical writers

- Cloud Operations: Staff that administer the Automation 360 Cloud. They provide the direct day-to-day services such as maintaining and upgrading systems, quality assurance monitoring, network support, and reporting:
    - The infrastructure, networking, and systems administration staff typically have no direct access to or use of the Automation 360 Cloud. Rather this team supports Automation Anywhere's Cloud infrastructure, which is used by the software. A systems administrator will deploy the releases of the Automation 360 Cloud and other software into the production environment for the customer to use
    - The information security staff supports the Automation 360 Cloud indirectly by monitoring internal and external security threats and maintaining current antivirus software
- Security Operations: The Security Operations (SecOps) team oversees the security of all production accounts and applications. They are responsible to monitor for and triage security alerts, identify vulnerabilities and other security related findings for in scope systems:
    - SecOps Operations team manages the security incidents reported by the customer or customer success team, investigate the reported incidents, and work with the various Automation Anywhere teams to drive resolution. Resolution of the reported incident can include changes to the Automation Anywhere application, CSP infrastructure, or implementation of additional security controls
    - SecOps Engineering team builds the secure architecture of the Automation 360 Cloud Service using infrastructure as code to support an automated build process within the respective CSP to deliver a consistent and secure infrastructure
    - SecOps Risk & Compliance monitors the Automation 360 Cloud for effective security practices that comply with multiple standards including ISO 27001, CSA-CCM, SOC2, HITRUST, FedRAMP etc.
- Information Technology (IT): Provides the corporate Information Technology services that are used throughout Automation Anywhere including by the teams responsible for the Automation 360 Cloud Services:
    - Help desk, IT infrastructure, IT networking, IT system administration, information security, and IT operations personnel

Data

The Automation 360 Cloud is a hosted Automation Anywhere service delivery platform upon which Automation 360 based services are offered. The Automation 360 Cloud comprises integrated Control Room and bot creation capabilities hosted on the Automation 360 Cloud with the ability to run cloud connected bot runner nodes located on the customer infrastructure. In addition, the following products are applications running on the Automation 360 Cloud - Bot Insight, and AARI.

Bot Insight - Easy access to insights about your intelligent automation program in a single, friendly, interactive visual dashboard. Share insights directly from the dashboard to increase visibility and organizational buy-in. Manipulate data with flexibility in Microsoft Power BI, Tableau, or any analytics of your choice via native connectors or APIs.

Automation Anywhere Robotic Interface (AARI) - Automation Anywhere's RPA integrated Digital Assistant that is used by individuals to automate routine tasks and to provide information from multiple backend systems within the consolidated AARI interface.

Data Collection

The deployment model for Automation 360 Cloud involves customers building their bots and managing the bot deployments from the Control Room located on the Automation 360 Cloud. Once the bots are built, they are tested and run on the customers own compute infrastructure. By default, the data involved in the actual automation does not enter the Automation 360 Cloud unless specific automation functionality is used. This default configuration significantly reduces the data collected by and stored within Automation 360 Cloud.

When users use various products including Document Automation, Bot Insight, and AARI additional data can be stored on the Automation 360 Cloud. This can also happen when features such as Recorder, AISense and WLM are used.

These AAI products can store customer data as part of a customer defined automation, albeit typically temporarily during the automation process defined by the customer. For example, IQ Bot use typically involves uploading images for processing. Recorder and AISense store recorded screenshots (note Secure Recording can be enabled by administrators to ensure these are not stored). AARI stores data processed by attended forms. Bot Insight can be used to create dashboards made from tagged business data being processed by a bot.

There are three types of data processed in the Automation 360 Cloud.

Operational Data

This includes status and log information that aids in running the automations such as error logs, audit logs, device connectivity stats, and operational dashboards.

Business Data

This is data used in operating a business and that is being passed between systems as part of the bot automation such as customers' client data, invoice numbers, or images of PoS. An example is the data uploaded to the cloud for processing documents using Document Automation.

The customer has control over what business data is stored on the Automation 360 cloud. Note that the source data remains with the customer and the customer is in control of deleting the data on the Automation 360 Cloud. The customer has the principal copy of the data in their systems.

Note this business data may contain personal information related to a customer's business.

Personal Data

This is any data that could be used to identify an individual and is governed by laws such as GDPR and CCPA. Examples of such personal information include, but are not limited to, individual names, telephone numbers, e-mail addresses, job titles, and contact information contained in invoices or e-mails.

The deployment model involves customers building their boots and managing the bot deployments from the Control Room in the cloud. Once the bots are built, they are tested and deployed to execute on the users' compute infrastructure.

The table below describes the data collected for the Automation 360 Cloud portfolio. The table provides guidance on which data could possibly be used to identify a natural person:

Data Item	Data Category	Description
Username	Personal	E-mail, First and Last name, preferred name, time zone, last login, password, questions set, AD-domain
User password	Personal	User password
Password security key	Personal	Credential Vault password security key
Bot Agent device access	Personal	Device username and access credentials
Role definitions	Personal	Admin, creator, etc.

Data Item	Data Category	Description
Roles mapped to users, device, resource	Personal	User roles
Bot device IP / FQDN	Personal	Device IP address or FQDN can be tracked to a user
Bot definition (repository)	Operational	Data stored as part of the bot definition
Bot application credentials	Personal	Application user, URL, public key, routing name
Control Room bot schedules	Operational	Bot management - When and where to run bots
WLM workflow definition	Operational	When and where to run bots in which sequence
Audit logs	Personal	May contain identifiers: device message log, deployment message log, e-mail message log, job execution log: (start/end time, user ID, schedule, automation name, deployment ID. Device name, bot name, username), User Management Edit Log, Credential Vault Message Log, Server & Database Change Logs
Errors logs	Personal	May contain identifiers
Operational analytics	Operational	Service status
Business analytics	Business / Personal	Business data tagged in automated processes for analysis by Bot Insight
Intelligent Document Processing Data	Business / Personal	Documents uploaded to IQ Bot or Document Automation for extraction and processing For IQ Bot or Document Automation: uploaded documents and extraction results
Intelligent Document Processing Data	Operational	For IQ Bot or Document Automation: Users learning instances, domains, operational statistics, and validation changes
Telemetry Usage data	Operational	Feature usage, licenses enabled, aggregated with no personal/user data identifiers

Data Item	Data Category	Description
Process and Workflow data	Business / Personal	For AARI: AARI Web Workflow Definition: Describing how a process executes (including but not limited to bot, forms, and other steps required to execute the process) AARI Web Dataflow: Store’s data incidentally generated by executing the process (including all inputs and outputs from the various process steps) For Discovery Bot: Process Data: This includes recordings performed by the end user about their process. The artifacts are stored in the form of JSON files, database tables (meta data e.g., application name, action name, source link), and images (snapshots of the screens while recording)
Other Data	Business / Personal	For AARI: AARI Web Team Definitions: Describing team membership, and process access rules AARI Web File Storage: Stores files uploaded as a part of the request's dataflow

Processes, Policies and Procedures

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

Physical Security

The in-scope system and supporting infrastructure are hosted by cloud service providers (CSP) AWS and GCP. As such, the CSP’s are responsible for the physical security controls for the in-scope systems. Refer to the ‘Subservice Organizations’ table below for controls managed by AWS and GCP.

Automation Anywhere Facility Security

Physical access to Automation Anywhere facilities is protected. All exterior ingress doors are restricted to users possessing an access card/Identification Document (ID) that has been assigned access to use the door. The access card/ID system uses zones to control access. Each exterior door and doors to restricted areas within the facilities are assigned to door zones. Access to zones is restricted through the use of access control lists. Employees and vendors granted access cards are assigned to roles based on their job responsibilities.

Visitors check in with the receptionist or security guard stationed in the reception area. Visitors must present a valid, government-issued photo ID. The visitor’s name and purpose for the visit are recorded in a visitor log and his or her visit must be escorted by an Automation Anywhere employee who is authorized to sign nonemployees into the facility.

Upon an employee's termination of employment, the HR system automatically generates an access deletion record in the event management system on the last day of employment. This record is routed to the access administrators for deletion. In addition, terminated employees turn over their access cards/IDs during their exit interview.

Access listings are generated by security and distributed to the zone owners via the event management system. Zone owners review the listings and indicate the required changes in the event management record.

Logical Access

Automation Anywhere uses a role-based security architecture and requires support users of the system to be identified and authenticated prior to accessing any CSP hosted system resources. Resources are protected through the use of native system security and add-on single sign on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists.

All resources are managed in the asset inventory system and each asset is assigned an owner by their role. Owners are responsible for approving access to the resource and for performing quarterly reviews of access by role.

Passwords must conform to defined password standards and are enforced through parameter settings in the Automation Anywhere SSO. These settings are part of the configuration standards and force users to change passwords at a defined interval, have complex passwords, and support account lockout for failed login attempts.

Upon hire, Automation Anywhere employees are assigned to a position in the HR management system. One week prior to the employees' start date, the HR management system creates a report of employee user IDs to be created and default system access that is to be granted. The report is then used by the IT help desk to create user IDs and associated application access based upon pre-defined rules. Access rules have been pre-defined based on defined user roles. The system generated list includes employees with position changes and the associated roles to be changed within the access rules.

On a quarterly basis, logical access rules for each role with access to the CSP are reviewed by the respective team leadership and the results are documented within the respective ticket tracking system. In evaluating role access, respective team leaders consider job duties requiring segregation, risks associated with access, and validating that all access changes (addition, change, deletion) are properly documented. Completed rules are reviewed and approved by the Chief Technology Officer (CTO) organization. As part of this process, the CTO organization reviews access by privileged roles and requests modifications based on this review. Physical and virtual private network (VPN) access reviews are conducted at least quarterly.

The HR system generates a request for terminated employees when a termination event occurs. This event is used by the IT help desk to delete employee access through the use of a bot that runs on a daily basis. On an annual basis, HR runs a list of active employees. The IT help desk uses this list to suspend user IDs and delete all access roles from IDs belonging to terminated employees.

Customer employees access Automation 360 Cloud services through the Internet using transport layer security (TLS) functionality of their web-browser to ensure that the information is encrypted while transmitted over the Internet. The customer employees must supply a valid user ID and password to gain access to customer cloud resources or have configured single sign-on with the customer's directory service.

Computer Operations - Backups

Customer data is backed up and monitored by Automation 360 Cloud Operations (CloudOps) personnel for completion and exceptions. In the event of an exception, CloudOps personnel perform troubleshooting to identify the root cause and then rerun the backup job immediately or as part of the next scheduled backup job depending on customer indicated preference within the documented work instructions.

CSP native services are used for creating backups.

This section explains where all of the cloud service data resides as well as where it is backed up. This information is used to locate and restore data in the event of a disaster:

Data	Cloud Service	Data Type	Backup Frequency	Backup Location
MSSQL Database	AWS RDS	SQL database for application	Every 6 hours	AWS RDS to another region
ElasticSearch (ES)	AWS ES	Audit and server logs	Every 6 hours	AWS S3 to another region
Filesystem	AWS Encrypting File System (EFS)	Control room system files	Every 6 hours	AWS EFS to another region
MSSQL Database	GCP SQL	SQL database for application	Every 6 hours	GCP SQL to another region
Balanced Persistent Disk	GCP Storage	Control room system files	Every 6 hours	GCP Storage to another region
Standard Storage	GCP Storage	Audit and server logs	Every 6 hours	GCP Storage to another region

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to incidents.

Automation Anywhere monitors the capacity utilization of all Automation 360 Cloud components within the company’s hosted computing infrastructure and customer application load to ensure that service delivery matches or exceeds SLAs.

Automation Anywhere evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Compute
- Memory
- Storage
- Network bandwidth

Vulnerability Management

The primary purpose of the vulnerability management is to ensure that all identified vulnerabilities in the AAI managed Cloud Service environment at the application (AAI Custom Code), container operating system (Docker & Kubernetes), host operating system and network & Internet layer will be protected from exposure and exploitation by attackers.

For ease of implementation, the vulnerability management operating procedures are divided into the following key phases:

- Preparation & Discovery Phase
- Scanning & Prioritization Phase
- Remediation Phase
- Validation and Closure Phase

Patch Management

The goal of Patch Management is to keep the components that form of the IT infrastructure (hardware, software, and services) up to date with the latest fixes and functionality through updates. Patch management is an important part of keeping the components of the IT infrastructure available to the end user.

For ease of implementation, the operating procedures are divided into the following key areas:

- Information systems and equipment to be patched
- Obtaining patch/update information
- Identification and testing of required patches/updates
- Deployment of patches/updates
- Rollback of patches/updates if required

Change Control

Automation Anywhere maintains an SDLC that the development and test team have to follow:

Every release goes through various gates before going into production. Essentially the release goes from Development to Quality Assurance (QA) to Stage to Production with checks / tests at every stage before it gets promoted. Customer data is not used for any non-production environment - test data generated by the QA team is used to simulate tenant data in all environments outside of production.

A ticketing system is utilized to ensure adherence to the change control procedures for changes in the application and implementation of new changes. QA testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment using test data. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes made to individual developers.

Data Communications

A Web Application Firewall (WAF) is in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized or that matches suspicious activity. Administrative access to the WAF is restricted to authorized employees. Network Address Translation (NAT) functionality is utilized to manage internal IP addresses and to prevent the leakage of internal IP addresses to the Internet.

Redundancy is built into the system infrastructure that is deployed by Automation Anywhere within the respective CSP like the servers, in the event that when a primary server fails, the redundant system is configured to take its place. Outside access and data from the entity's environment is controlled and restricted to appropriate ports/devices. Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. Data coming into the environment is secured and monitored using firewalls and an Intrusion Detection System (IDS) at the network perimeter.

Penetration Testing

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Automation Anywhere. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can potentially be exploited via the penetration test, simulating a disgruntled or disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by the Security Team at least monthly by using vulnerability scanning tools i.e., Veracode, Black Duck, Qualys, Burp Suite, Lacework or CSP provided tools as per Automation Anywhere policy. SecOps uses industry standard scanning technologies and a formal methodology specified by Automation Anywhere. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as-needed basis. Scans are performed during non-peak windows. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled. Tools requiring installation in the Automation Anywhere system are implemented through the Change Management process.

Authorized employees may access the system from the Internet using leading VPN technology. Employees are authenticated using a token-based multi-factor authentication (MFA) system.

Boundaries of the System

The Automation 360 Cloud Services System is hosted by the cloud service providers AWS or GCP. Automation Anywhere's corporate headquarters is located in San Jose, California USA with additional offices in Bengaluru and Vadodara, India.

The scope of this report does not include the cloud hosting services provided by AWS or GCP at their facilities.

Changes to the System in the Last 12 Months

Automation Anywhere added Canada as a new GCP region.

Incidents in the Last 12 Months

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

Criteria Not Applicable to the System

All Common Criteria / Security, Availability, and Confidentiality criterion were applicable to the Automation 360 Cloud Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS or GCP at multiple facilities around the world.

Complementary Subservice Organization Controls

Automation Anywhere’s 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 Automation Anywhere’s services to be solely achieved by Automation Anywhere control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Automation Anywhere.

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

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		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.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic IDS are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Availability	A1.2	Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in CSP-owned data centers.
		CSP-owned data centers are protected by fire detection and suppression systems.
		CSP-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		CSP-owned data centers have generators to provide backup power in case of electrical failure.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies.

Subservice Organization - GCP		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	Data center server floors network rooms and security systems are physically isolated from public spaces and/or delivery areas.
		Access to sensitive data center zones requires approval form authorized personnel and is controlled via badge access readers, biometric identification mechanism, and/or physical locks.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.
		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of the visit.
		Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.
		Data centers are continuously staffed and monitored by security personnel through the use of real time video surveillance and/or alerts generated by security systems.
Availability	A1.2	Critical power and telecommunications equipment in data centers is physically protected from destruction and damage.
		Data centers are equipped with fire detection alarms and protection equipment.
		Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power sources.
		The organization conducts disaster recovery testing on an ongoing basis (and at least annually) to enable infrastructure and application teams to test communication plans, fail-over scenarios, operational transition, and other emergency responses. Participating teams create testing plans and document the results and lessons learned from the tests.

Automation Anywhere 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 SLAs. In addition, Automation Anywhere performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

Automation Anywhere's 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 Trust Services Criteria related to Automation Anywhere's services to be solely achieved by Automation Anywhere control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Automation Anywhere's.

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 Automation Anywhere.
2. User entities are responsible for notifying Automation Anywhere 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 Automation Anywhere 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 Automation Anywhere services.
6. User entities are responsible for providing Automation Anywhere with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Automation Anywhere of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
8. User entities are responsible for provisioning and de-provisioning access to their environments.