HITRUST
6175 Main Street
Suite 400
Frisco, TX 75034

June 1, 2023

Automation Anywhere, Inc.
633 River Oaks Parkway
San Jose, California 95134

Based upon representation from management as to the accuracy and completeness of information provided, the procedures performed by an Authorized External Assessor to validate such information, and HITRUST's independent confirmation that the work was performed in accordance with the HITRUST® Assurance Program requirements, the following platform, facilities, and supporting infrastructure of the Organization ("Scope") meet the HITRUST CSF® v9.3 Risk-based, 2-year (r2) certification criteria:

Platform:

- Automation Anywhere 360 Cloud Services residing at af-south-1, ap-northeast-1, ap-south-1, ap-southeast-1, ap-southeast-2, australia-southeast1, eu-west-1, europe-west4, me-south-1, northamerica-northeast-1, sa-east-1, us-central1, us-east-1, and us-west-2

Facilities:

- us-east-1 (Data Center) managed by Amazon Web Services located in Virginia, United States of America
- ap-south-1 (Data Center) managed by Amazon Web Services located in India
- ap-southeast-2 (Data Center) managed by Amazon Web Services located in Sydney, Australia
- us-west-2 (Data Center) managed by Amazon Web Services located in Oregon, United States of America
- af-south-1 (Data Center) managed by Amazon Web Services located in Cape Town, South Africa
- me-south-1 (Data Center) managed by Amazon Web Services located in Bahrain
- ap-northeast-1 (Data Center) managed by Amazon Web Services located in Tokyo, Japan
- sa-east-1 (Data Center) managed by Google Cloud Platform located in Sao Paulo, Brazil
- eu-west-1 (Data Center) managed by Amazon Web Services located in Ireland
- ap-southeast-1 (Data Center) managed by Amazon Web Services located in Singapore

- australia-southeast1 (Data Center) managed by Google Cloud Platform located in Melbourne, Australia
- us-central1 (Data Center) managed by Google Cloud Platform located in Iowa, United States of America
- northamerica-northeast-1 (Data Center) managed by Google Cloud Platform located in Montreal, Canada
- europe-west4 (Data Center) managed by Google Cloud Platform located in Netherlands

The certification is valid for a period of two years assuming the following occurs. If any of these criteria are not met, HITRUST will perform an investigation to determine ongoing validity of the certification and reserves the right to revoke the Organization's certification.

- Annual progress is being made on areas identified in the Corrective Action Plan(s) (CAPs),

- No data security breach reportable to a federal or state agency by law or regulation has occurred within or affecting the assessed environment,

- No significant changes in the business or security policies, practices, controls, and processes have occurred that might impact its ability to meet the HITRUST Risk-based, 2-year (r2) certification criteria, and

- Timely completion of the HITRUST Interim Assessment for r2 Certification as defined in the HITRUST Assurance Program Requirements.

HITRUST has developed the HITRUST CSF, a certifiable framework that provides organizations with the needed structure, detail and clarity relating to information protection. With input from leading organizations, HITRUST identified a subset of the HITRUST CSF controls that an organization must meet to be HITRUST Risk-based, 2-year (r2) Certified. For certain HITRUST CSF controls that were not being met, the Organization developed a CAP that outlined its plans for meeting such controls.

HITRUST performed a quality assurance review to ensure that the control maturity scores were consistent with the results of testing performed by the Authorized External Assessor. Users of this letter can refer to the document Leveraging HITRUST Assessment Reports: A Guide for New Users for questions on interpreting this letter and can contact HITRUST customer support at support@hitrustalliance.net. Users of this letter are assumed to be familiar with and understand the services provided by the organization listed above, and what specific services are being used by the user organization.

A full HITRUST Validated Assessment Report has also been issued by HITRUST which can also be requested from the organization listed above directly. Additional information on the HITRUST Assurance Program can be found at the HITRUST website at https://hitrustalliance.net.

HITRUST

HITRUST

Enclosures (2):

- Assessment Context
- Scope of Systems in the Assessment

Assessment Context

The assessed entity completed the following tailoring questionnaire to derive this assessment's customized set of HITRUST CSF requirements based on organizational, geographical, technical, and regulatory risk factors.

Assessment Type	
HITRUST Risk-based, 2-year (r2) Security Assessment	
General Risk Factors	
Organization Type	Service Provider (Information Technology, IT)
Entity Type	Healthcare - Business Associate
Do you offer Infrastructure as a Service (IaaS)?	No
Geographic Risk Factors	
Geographic Scope of Operations Considered	Off-shore (outside U.S.)
Organizational Risk Factors	
Number of Records that are currently held	Less than 10 Million Records
Technical Risk Factors	
Is the system(s) accessible from the Internet?	Yes
Is the scoped system(s) (on-premise or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)?	Yes
Does the system(s) transmit or receive data with a third-party?	No - Automation Anywhere's system(s) does/do not transmit or receive data with a third-party.
Is the system(s) publicly positioned?	No - Automation Anywhere's system(s) is/are not publicly positioned.
Number of interfaces to other systems	Fewer than 25
Number of users of the system(s)	Fewer than 500
Number of transactions per day	Fewer than 6,750
Does the scoped environment allow dial-up/dial-in capabilities (i.e., functional analog modems)?	No - Automation Anywhere's scoped environment does not allow dial-up/dial-in capabilities (i.e., functional analog modems).
Is scoped information sent and/or received via fax machine (i.e., an actual machine, excluding efax or scan to email)?	No - Automation Anywhere does not send and/or receive scoped information via fax machine (i.e., an actual machine, excluding efax or scan to email).

Do any of the organization's personnel travel to locations the organization deems to be of significant risk?	No - Automation Anywhere does not allow organizational personnel to travel to locations the organization deems to be of significant risk.
Are hardware tokens used as an authentication method within the scoped environment?	No - Automation Anywhere does not use hardware tokens as an authentication method within the scoped environment.
Does the organization allow personally owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device)?	No - Automation Anywhere does not allow personally-owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device).
Are wireless access points in place at any of the organization's in-scope facilities?	No - All in-scope systems are with the cloud providers facilities
Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component?	No - Automation Anywhere does not perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component.
Does the organization use any part of the scoped systems, system components, or system services to sell goods and/or services?	No - Automation Anywhere does not use any part of the scoped systems, system components, or system services to sell goods and/or services.
Does the organization allow the use of electronic signatures to provide legally binding consent within the scoped environment, e.g., simple or basic electronic signatures (SES), advanced electronic or digital signature (AES), or qualified advanced electronic or digital signatures (QES)?	No - Automation Anywhere does not allow the use of electronic signatures to provide legally binding consent within the scoped environment, e.g., simple or basic electronic signatures (SES), advanced electronic or digital signature (AES), or qualified advanced electronic or digital signatures (QES).
Is scoped information sent by the organization using courier services, internal mail services, or external mail services (e.g., USPS)?	No - Automation Anywhere does not send scoped information using courier services, internal mail services, or external mail services (e.g., USPS).
Is any aspect of the scoped environment hosted on the cloud?	Yes
Does the system allow users to access the scoped environment from an external network that is not controlled by the organization?	Yes

Regulatory Risk Factors (Optional)

No regulatory risk factors (i.e. additional authoritative sources such as NIST SP 171) were included in this HITRUST CSF assessment

Scope of the Assessment

Company Background

Automation Anywhere is the leader in intelligent automation and the Automation Success Platform is infused with generative AI and offers process discovery, RPA, end-to-end process orchestration, document processing, and analytics, with a security and governance-first approach. Automation Anywhere empowers organizations worldwide to unleash productivity gains, drive innovation, improve customer service and accelerate business growth. The company is guided by its vision to fuel the future of work by unleashing human potential through intelligent automation.

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 the most intelligent and intuitive robotic process automation platform called Automation 360.

The company's vision is to take the robot out of the human. To liberate employees from mundane, repetitive tasks, allowing them more time to use their intellect and creativity to solve higher-order business challenges. Automation Anywhere envisions a world where every employee will work alongside digital workers, making them exponentially more productive and far more fulfilled

In-scope Platform

The following table describes the platform that was included in the scope of this assessment.

Automation Anywhere 360 Cloud Services	
Description	The Automation 360 Enterprise Edition cloud services are deployed in the AWS & GCP cloud via a multitenant architecture. Each customer tenant is deployed in a logical tenant within a containerized environment running Control Room and other cloud services. Each tenant is logically segmented based on a unique tenant identifier. A different database is created on a relational database storage instance per tenant and a different directory mount is created per tenant on a common file system.
Application(s)	N/A
Database Type(s)	AWS-RDS, GCP-Cloud SQL
Operating System(s)	Linux, K8s Linux, Ubuntu, Windows2019

Residing Facility	• af-south-1 • ap-northeast-1 • ap-south-1 • ap-southeast-1 • ap-southeast-2 • australia-southeast1 • eu-west-1 • europe-west4 • me-south-1 • northamerica-northeast-1 • sa-east-1 • us-central1 • us-east-1 • us-west-2
Exclusion(s) from Scope	None

In-scope Facilities

The following table presents the facilities that were included in the scope of this assessment.

Facility Name	Type of Facility	Third-party Managed?	Third-party Provider	City	State	Country
us-east-1	Data Center	Yes	Amazon Web Services		Virginia	United States of America
ap-south-1	Data Center	Yes	Amazon Web Services			India
ap-southeast-2	Data Center	Yes	Amazon Web Services	Sydney		Australia
us-west-2	Data Center	Yes	Amazon Web Services		Oregon	United States of America
af-south-1	Data Center	Yes	Amazon Web Services	Cape Town		South Africa
me-south-1	Data Center	Yes	Amazon Web Services			Bahrain
ap-northeast-1	Data Center	Yes	Amazon Web Services	Tokyo		Japan
sa-east-1	Data Center	Yes	Google Cloud Platform	Sao Paulo		Brazil

Facility Name	Type of Facility	Third-party Managed?	Third-party Provider	City	State	Country
eu-west-1	Data Center	Yes	Amazon Web Services			Ireland
ap-southeast-1	Data Center	Yes	Amazon Web Services			Singapore
australia-southeast1	Data Center	Yes	Google Cloud Platform	Melbourne		Australia
us-central1	Data Center	Yes	Google Cloud Platform		Iowa	United States of America
northamerica-northeast-1	Data Center	Yes	Google Cloud Platform	Montreal		Canada
europe-west4	Data Center	Yes	Google Cloud Platform			Netherlands

Services Outsourced

The following table presents outsourced services relevant to the scope of this assessment. The "Consideration in this Assessment" column of this table specifies the method utilized for each service provider relevant to the scope of this r2 assessment.

Organizations undergoing r2 validated assessments have two options of how to address situations in which a HITRUST CSF requirement is fully or partially performed by a service provider (e.g., by a cloud service provider):

- The Inclusive method, whereby HITRUST CSF requirements performed by the service provider are included within the scope of the assessment and addressed through full or partial inheritance, reliance on third-party assurance reports, and/or direct testing by the external assessor, and

- The Exclusive (or Carve-out) method, whereby HITRUST CSF requirements performed by the service provider are excluded from the scope of the r2 assessment and marked N/A with supporting commentary explaining that the HITRUST CSF requirement is fully performed by a party other than the assessed entity (for fully outsourced controls) or through commentary explaining the excluded partial performance of the HITRUST CSF requirement (for partially outsourced controls).

Third-party Provider	Relevant Service(s) Provided	Consideration in this Assessment
Google Cloud Platform	Cloud provider	Included
Amazon Web Services	Cloud provider	Included

Overview of the Security Organization

The responsibility for securing Automation Anywhere's cloud based Automation360 SaaS service and its public cloud infrastructure lies with the following three teams.

1. The Engineering Product and Cloud Security team - 12 member team reporting to Director, Cloud Security, responsible for the following four functions:

   - Risk and Compliance - defining the cloud security policies and standards, managing and tracking of risks, aligning AAI cloud security best practices with controls from various well known compliance frameworks and standards to achieve certifications like SOC1, SOC2, HIPAA, HITRUST, CSA STAR etc.

   - Product Security / Application Security - responsible for application threat modelling, vulnerability management with secure code analysis and open source scans, application pen testing and bug bounty programs

   - Cloud Security Engineering and Architecture - responsible for design and testing of cloud security architecture, infrastructure vulnerability management, monitoring and reacting to 0-day threats and advisories, Identification and tracking of cloud configuration violations, and administration of third-party and/or native cloud security tools

   - Cloud Security Operation Center - configuring and tuning of detection and prevention rules, building SIEM content, threat rules, proactively searching and hunting for threats, monitoring and triaging of alerts and events 24x7, ensuring all security incidents are investigated, contained, and recovered from, in a timely manner.

2. The Cloud Operations team: 30-member team reporting to the Senior Director, of Cloud Operations responsible for the operation, maintenance, and availability of the cloud infrastructure.

3. IT Organization: 41-member team reporting to VP of IT, responsible for support of corporate applications, resources, facilities, users and their endpoint assets. The IT Information Security team also maintains the compliance posture for the enterprise wide ISO 27001 standard and certification

6. Procedures Performed by the External Assessor

An Authorized HITRUST External Assessor Organization (i.e., the external assessor) performed procedures to validate the assessed entity's asserted control maturity scores. These validation procedures were designed by the external assessor based upon the assessment's scope in observance of HITRUST's Assurance Program Requirements and consisted of inquiry with key personnel, inspection of system-generated evidence (e.g., access lists, logs, configurations, sample items), on-site or virtual observations, and (optionally) reperformance of controls.

For certain portions of the assessment and as allowed by HITRUST's Assurance Program requirements, the external assessor may have utilized the work of other assessors, auditors, and/or inspectors in lieu of direct testing. All assessment procedures performed by the external assessor, including those where the external assessor utilized the work of others, were subject to HITRUST's quality assurance review procedures. The table below details assessments utilized by the external assessor.

Potential options available for using the work of others allowed by HITRUST's Assurance Program Requirements include the following and are reflected in the "Utilization Approach" column of the below table if leveraged in this assessment:

- Inheritance of results from or reliance on another HITRUST validated assessment,
- Reliance on a recent third-party assurance report, and/or
- Reliance on testing performed by the assessed entity (i.e., by internal assessors).

Assessment Utilized	Assessed Entity	Assessment Type	Report Date(s)	Utilization Approach	Relevant Platforms	Relevant Facilities	Assessment Domains
Amazon Web Services (AWS) - 2022 AWS Validated Assessment	Amazon Web Services	v9.6.0 VALIDATED	06/14/2022	Inheritance	Automation Anywhere 360 Cloud Services	us-east-1 us-west-2 af-south-1 me-south-1 ap-northeast-1 eu-west-1 ap-southeast-1	04 Mobile Device Security, 05 Wireless Security, 06 Configuration Management, 07 Vulnerability Management, 08 Network Protection, 09 Transmission Protection, 11 Access Control, 15 Incident Management, 16 Business Continuity & Disaster Recovery, 18 Physical & Environmental Security
Google LLC - GCP & Workspace 2021 (HITRUST CSF v9.4)	Google, LLC	v9.4 VALIDATED	10/29/2021	Inheritance	Automation Anywhere 360 Cloud Services	ap-south-1 ap-southeast-2 sa-east-1	04 Mobile Device Security, 05 Wireless Security, 06 Configuration Management, 07 Vulnerability Management, 08 Network Protection, 09 Transmission Protection, 11 Access Control, 15 Incident Management, 16 Business Continuity & Disaster Recovery, 18 Physical & Environmental Security

Assessment Utilized	Assessed Entity	Assessment Type	Report Date(s)	Utilization Approach	Relevant Platforms	Relevant Facilities	Assessment Domains
GCP SOC 2 report Winter 2023..pdf	Google, LLC	Period-of-time assessment report	The assessment report's issuance date 04/03/2023 The assessment report's audit period start date 03/01/2022 The assessment report's audit period end date 02/28/2023	Reliance	Automation Anywhere 360 Cloud Services	ap-south-1 ap-southeast-2 sa-east-1	06 Configuration Management, 14 Third Party Assurance

Assessment Utilized	Assessed Entity	Assessment Type	Report Date(s)	Utilization Approach	Relevant Platforms	Relevant Facilities	Assessment Domains
System and Organization Controls (SOC) 2- Report Current (Apr 1 2022_- Sept 30 2022)	Amazon Web Services	Period-of-time assessment report	The assessment report's issuance date 11/14/2022 The assessment report's audit period start date 04/01/2022 The assessment report's audit period end date 09/30/2022	Reliance	Automation Anywhere 360 Cloud Services	us-east-1 us-west-2 af-south-1 me-south-1 ap-northeast-1 eu-west-1 ap-southeast-1	06 Configuration Management, 14 Third Party Assurance