HITRUST®

6175 Main Street
Suite 400
Frisco, TX 75034

June 13, 2023

UiPath, Inc.
452 5th Avenue
22nd Floor
New York, NY 10018

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® v9.6.2 Risk-based, 2-year (r2) certification criteria:

Platform:

- Automation Cloud residing at Microsoft Azure

Facilities:

- Microsoft Azure (Data Center) managed by Microsoft Azure located in Portland, Oregon, United States of America
- Microsoft Azure (Data Center) managed by Microsoft Azure located in Tokyo, Japan
- Microsoft Azure (Data Center) managed by Microsoft Azure located in Oslo, Norway
- Microsoft Azure (Data Center) managed by Microsoft Azure located in Canberra, Australia
- Microsoft Azure (Data Center) managed by Microsoft Azure located in Toronto, Canada

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.

- 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.

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	Between 10 and 60 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?	Yes
Is the system(s) publicly positioned?	No - The in-scope system is not publicly positioned.
Number of interfaces to other systems	Fewer than 25
Number of users of the system(s)	Greater than 5,500
Number of transactions per day	Greater than 85,000
Does the scoped environment allow dial-up/dial-in capabilities (i.e., functional analog modems)?	No - The in-scope environment does not have or allow dial-up/dial-in capabilities.
Is scoped information sent and/or received via fax machine (i.e., an actual machine, excluding efax or scan to email)?	No - The in-scope environment does not use fax capability to transmit data.

Do any of the organization's personnel travel to locations the organization deems to be of significant risk?	No - There are no personnel traveling to areas with significant risk.
Are hardware tokens used as an authentication method within the scoped environment?	No - Hardware tokens are not used as an authentication method within the in-scope environment.
Does the organization allow personally owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device)?	No - UiPath does not allow personally-owned devices (i.e., BYOD) to connect to in-scope organizational assets.
Are wireless access points in place at any of the organization's in-scope facilities?	No - There are no wireless access points at any in scope facilities.
Does the organization use any part of the scoped systems, system components, or system services to sell goods and/or services?	No - UiPath 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 - UiPath does not use eSignatures in the scoped environment.
Is scoped information sent by the organization using courier services, internal mail services, or external mail services (e.g., USPS)?	No - Scoped information is not sent by UiPath using courier services, internal mail services, or external mail services.
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
Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component?	Yes

Compliance Factors (Optional)

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

Scope of the Assessment

Company Background

UiPath is a global provider of a suite of Robotic Process Automation (RPA) and related automation software products, which are the technologies that allows anyone today to configure computer software, or a “robot” to emulate and integrate the actions of a human interacting within digital systems to execute business processes. UiPath Automation Cloud is a Software as a Service (SaaS) solution, offered only via the web to customers who want to manage their automations without the overhead of going through installing and managing the on-prem version of UiPath’s orchestrator solution.

UiPath’s mission is to accelerate human achievement. Its end-to-end automation platform helps organizations discover tasks that can be automated, build robots to automate those tasks, manage a fleet of robots, run the automations, engage with humans to complete tasks, and finally measure and align automations with strategic business outcomes.

In-scope Platform

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

Automation Cloud	
Description	The UiPath Automation Cloud platform is a SaaS solution, offered via the web to customers who want to manage their automations without the overhead of going through installing and managing the on-prem version of UiPath’s Orchestrator and other management solutions. UiPath Automation Cloud allows customers to manage their licenses, add multiple tenants with different services, manage user access for these services, access Orchestrator services to create robots, environments, machines, processes, run jobs, create schedules — essentially allowing customers to perform robot management activities from one centralized, secure location on the cloud. UiPath’s Automation Cloud is hosted at Microsoft Azure (Azure) data centers, using a variety of Azure offerings including App Service, Kubernetes, SQL Server, and Cosmos DB. The Azure regions from which the services.
Application(s)	Orchestrator, Platform Services, Portal, Automation Hub and Insights
Database Type(s)	SQL Server
Operating System(s)	Linux and Windows

Automation Cloud	
Residing Facility	Microsoft Azure
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
Microsoft Azure	Data Center	Yes	Microsoft Azure	Portland	Oregon	United States of America
Microsoft Azure	Data Center	Yes	Microsoft Azure	Tokyo		Japan
Microsoft Azure	Data Center	Yes	Microsoft Azure	Oslo		Norway
Microsoft Azure	Data Center	Yes	Microsoft Azure	Canberra		Australia
Microsoft Azure	Data Center	Yes	Microsoft Azure	Toronto		Canada

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. HITRUST's Assurance Program Requirements allow the use of both the inclusive and exclusive methods on HITRUST r2 assessments.

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
Looker	Data visualization tool from Google	Included
Snowflake	Datawarehouse and Analytics	Included
ATLAS MÜNCHEN (TES)	IT assets disposal service provider, provides collection of assets and secure disposal of assets.	Included
BishopFox	External Pentest provider and Provider of continuous monitoring of vulnerabilities scanning of the exposed interface, reporting to UiPath based on risk based on preliminary exploitability assessment.	Included
Microsoft Azure	Cloud provider for UiPath Automation Cloud.	Included

Overview of the Security Organization

UiPath maintains an ISO 27001:2013 certification for all of our core platform products and cloud services. Our ISO 27001 certification shows that UiPath has adopted a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes. Our ISO 27001 Certification can be found here.

UiPath has implemented and will continue to maintain and enforce an information security program that includes administrative, technical and physical safeguards that are appropriate to the Software and Services provided by UiPath, as such it may be evaluated and adjusted from time to time, in light of any relevant changes in the industry standards, technology and material changes to UiPath's business.

Our security, availability, and confidentiality commitments for our Cloud Platform include, but are not limited to, the following:

- Operational Practices: A range of security and confidentiality controls designed to address the security and confidentiality criteria of UiPath Cloud Platform. Such security and confidentiality controls include a role-based access management system that permits and restricts user access to customer data, based on roles and responsibilities and a formal process for granting and revoking access.
- Product Security: A range of security controls UiPath implements to keep the UiPath Cloud Platform and customer's data safe. This includes the use of encryption technologies to protect customer data at rest and in transit and continuous testing of application attack surface.
- Reliability and Availability: Hosting data with Atlassian's cloud hosting partners while focusing on product resiliency to minimize downtime, as well as optimal performance with redundancy and failover options globally while maintaining multiple locations and availability zones across regions.
- Security Process: A range of methods to detect security defects, that allows UiPath to address identified gaps as soon as possible to minimize impact. This includes continuous monitoring, alerting and incident management
- Security Personnel: UiPath Security Team (UST) comprises of highly experienced subject matter experts. This world class security team comprises of more than forty members maintaining high level of skills in their respective domains and up to date security knowledge.

Cyber Security Governance

UiPath recognizes the importance of implementing appropriate technical and organizational security measures in order to prevent any unauthorized access, disclosure, alteration or destruction of such data. For this purpose, UiPath implements industry standard security controls and maintains a comprehensive security program.

Risk Management

UiPath has a risk management process in place based on which it designs the set of security controls meant to reduce security risks to an acceptable level. A Risk Assessment is conducted at least annually and identified risks are mitigated according to risk severity and business priorities and captured in a Risk Treatment Plan.