OutSystems, Inc.

System and Organization Controls Report (SOC 3)

Independent Report of the Controls to meet the criteria for the Security, Availability, Processing Integrity, and Confidentiality categories for the period of July 1, 2020 through June 30, 2021.

KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

ASSERTION OF OUTSYSTEMS, INC. MANAGEMENT

ASSERTION OF OUTSYSTEMS, INC. MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within OutSystems, Inc.'s application development and delivery platform system (system) throughout the period July 1, 2020, to June 30, 2021, to provide reasonable assurance that OutSystems, Inc.'s service commitments and system requirements relevant to Security, Availability, Processing Integrity, and Confidentiality were achieved. Our description of the boundaries of the system is presented in section A 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, 2020, to June 30, 2021, to provide reasonable assurance that OutSystems, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, 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*). OutSystems, Inc.'s objectives for the system in applying the 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 section B.

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, 2020, to June 30, 2021, to provide reasonable assurance that OutSystems, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

INDEPENDENT SERVICE AUDITOR'S REPORT

Paulo Rosado
Chief Executive Officer
OutSystems, Inc.
Rua Central Park 2, 2A
2795-242 Linda-a-Velha
Portugal

Scope

We have examined OutSystems, Inc.'s accompanying assertion titled "Assertion of OutSystems, Inc. Management" (assertion) that the controls within OutSystems, Inc.'s application development and delivery platform system (system) were effective throughout the period July 1, 2020, to June 30, 2021, to provide reasonable assurance that OutSystems, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, 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*).

Service Organization's Responsibilities

OutSystems, Inc. is responsible for its service commitment and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that OutSystems, Inc.'s service commitments and system requirements were achieved. OutSystems, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, OutSystems, Inc. is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. 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 management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve OutSystems, Inc.'s service commitments and system requirements based on the applicable trust services criteria

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve OutSystems, Inc.'s service commitments and system requirements based on the applicable trust services criteria

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

Inherent Limitations

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 were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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 OutSystems, Inc.'s application development and delivery platform system were effective throughout the period July 1, 2020, to June 30, 2021, to provide reasonable assurance that OutSystems, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

August 9, 2021

OUTSYSTEMS, INC.'S DESCRIPTION OF ITS APPLICATION DEVELOPMENT AND DELIVERY PLATFORM SYSTEM

SECTION A:
OUTSYSTEMS, INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS APPLICATION DEVELOPMENT AND DELIVERY PLATFORM SYSTEM

Services Provided

OutSystems, Inc. (OutSystems) offers a platform-as-a-system (PaaS) designed for efficient development and delivery of web and mobile applications. The platform is model driven with the following artificial intelligence (AI) assistance and features:

- Full-stack visual development
- In-app feedback
- Single-click deployment
- Automatic and guided refactoring
- Architecture that scales

The in-scope locations for this audit are

- Linda-a-Velha, Portugal
- Proença-a-Nova, Portugal
- Braga, Portugal
- Kuala Lumpur, Malaysia
- Tokyo, Japan

Engagement Process

OutSystems progresses clients through the following stages:

1. Onboarding (about 30 days)
2. Building the first application in the platform (about four months)
3. Evolving (varies)
4. Scaling (one to two years)
5. Optimizing (reading release notes and teaching others)

Clients first learn of OutSystems from browser searches or word of mouth. The first contact typically occurs via the chatbot on the OutSystems site. After a client request, the Solutions Architect partners with the client to determine their specific needs and provide pitches, presentations, and workshops. Then, the Account Manager takes the information to create a contract using Salesforce, and each contract is tailored to the client's needs. Contracts include a breakdown of pricing, a customized payment schedule that works for the client, and scoping information. When the client has signed the contract, the agreed-upon solution is provisioned, which usually takes less than a day, but the organization reserves the right to take up to five days. Next, Customer Success works with the client to train one-on-one, and ongoing training is provided for the customer thereafter.

OutSystems commits to clients that all reasonable efforts are made to protect confidential information during the contract period and for three years thereafter. While some access to client data may be necessary, access to the data is restricted to select employees, and client data access

is logged, tracked, and forwarded to the client along with changes to the client's environment or application.

Each client has their own virtual private cloud (VPC) within Amazon Web Services (AWS), including separate environments for production and non-production. Each environment is composed of Elastic Compute Cloud (EC2) instances, Relational Database Services (RDS) instances, and both internal and external Application Load Balancers. The production environment has an additional failover RDS instance for high availability. After initial onboarding, clients can interact with its customized platform without assistance from OutSystems. All processes are customizable and repeatable for the client throughout the product lifecycle.

Infrastructure

OutSystems maintains a formal network diagram to depict the relationships among the network and systems within the organization. The Cloud Orchestration Teams are responsible for keeping the diagram up to date.

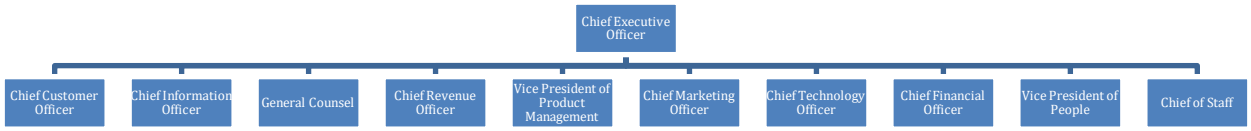
Software

OutSystems maintains a software inventory list to reflect the critical software in use and licensing information. Licensing management takes place via Trend Micro.

People

The organization's board of directors oversees the development and performance of company objectives. The board is composed mostly of investors, but also of advisors and the CEO and co-founder to encompass all perspectives that may impact the best interest of the organization.

OutSystems follows a traditional hierarchy with clear delineation and reporting lines. The organization is divided into departments that are each headed by a different representative from management, and representatives to management report to C-Level Executives. The following organization chart depicts the leadership structure of OutSystems.



Data

The organization provides secure environments for clients to store or process data, and OutSystems provides guidance for clients to secure their environments. The Data Processing Agreement outlines that the customer has sole liability for their data in the platform. The organization also maintains specifications for handling data based on the following categories:

- Public
- Internal
- Restricted
- Confidential

The organization uses SHA512 to store passwords, and passwords are only transmitted using Transport Layer Security (TLS) 1.2. TLS 1.2 is also enabled for client applications. OutSystems requires new systems to enable and document encryption parameters, and the organization is responsible for client-facing and server-facing encryption. Upon the end of a contract, the organization retains client data for three months unless specified otherwise.

The organization maintains a logical separation of the client-facing platform and OutSystems back end. OutSystems separates its production environment from all other environments to restrict access to production and to ensure data security

OutSystems maintains data flow diagrams to depict the flow of information throughout the organization's environments.

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices

SECTION B:
PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Regulatory Commitments

OutSystems complies with General Data Protection Regulation (GDPR) requirements, and information is provided to clients regarding their rights under GDPR.

Contractual Commitments

The organization requires clients to complete a master service agreement (MSA) upon engagement, and OutSystems communicates its service commitments to clients via the organization website. The Support Terms and Conditions state that the organization guarantees 99.95% availability to Enterprise-tier clients and 99.5% availability to other clients.

System Design

OutSystems, Inc. designs its application development and delivery platform system to meet its regulatory and contractual commitments. These commitments are based on the services that OutSystems, Inc. provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that OutSystems, Inc. has established for its services. OutSystems, Inc. establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in OutSystems, Inc.'s system policies and procedures, system design documentation, and contracts with clients.