OutSystems

System and Organization Controls Report (SOC 3)

Independent Report of the Controls to meet the criteria for the Security, Availability, Processing Integrity, Confidentiality, and Privacy categories for the period of July 1, 2018 through June 30, 2019.

KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

ASSERTION OF OUTSYSTEMS MANAGEMENT

ASSERTION OF OUTSYSTEMS MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within OutSystems' Sentry Application Development and Delivery Platform System (system) throughout the period July 1, 2018, to June 30, 2019, to provide reasonable assurance that OutSystems' service commitments and system requirements relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy 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, 2018, to June 30, 2019, to provide reasonable assurance that OutSystems' service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (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' 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, 2018, to June 30, 2019, to provide reasonable assurance that OutSystems' 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
Rua Central Park 2, 2A
2795-242 Linda-a-Velha, Portugal

Scope

We have examined OutSystems' accompanying assertion titled "Assertion of OutSystems Management" (assertion) that the controls within OutSystems' Sentry Application Development and Delivery Platform System (system) were effective throughout the period July 1, 2018, to June 30, 2019, to provide reasonable assurance that OutSystems' service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (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 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' service commitments and system requirements were achieved. OutSystems has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, OutSystems 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' 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' 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' Sentry Application Development and Delivery Platform system were effective throughout the period July 1, 2018, to June 30, 2019, to provide reasonable assurance that OutSystems' 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 6, 2019

OUTSYSTEMS' DESCRIPTION OF ITS SYSTEM

SECTION A:
OUTSYSTEMS' DESCRIPTION OF THE BOUNDARIES OF ITS SENTRY APPLICATION DEVELOPMENT AND DELIVERY PLATFORM SYSTEM

Services Provided

OutSystems is a rapid application development and delivery platform for mobile and web applications, available in a Platform as a Service (PaaS) model. From a commercial and delivery perspective, OutSystems' PaaS is segmented in different offers.

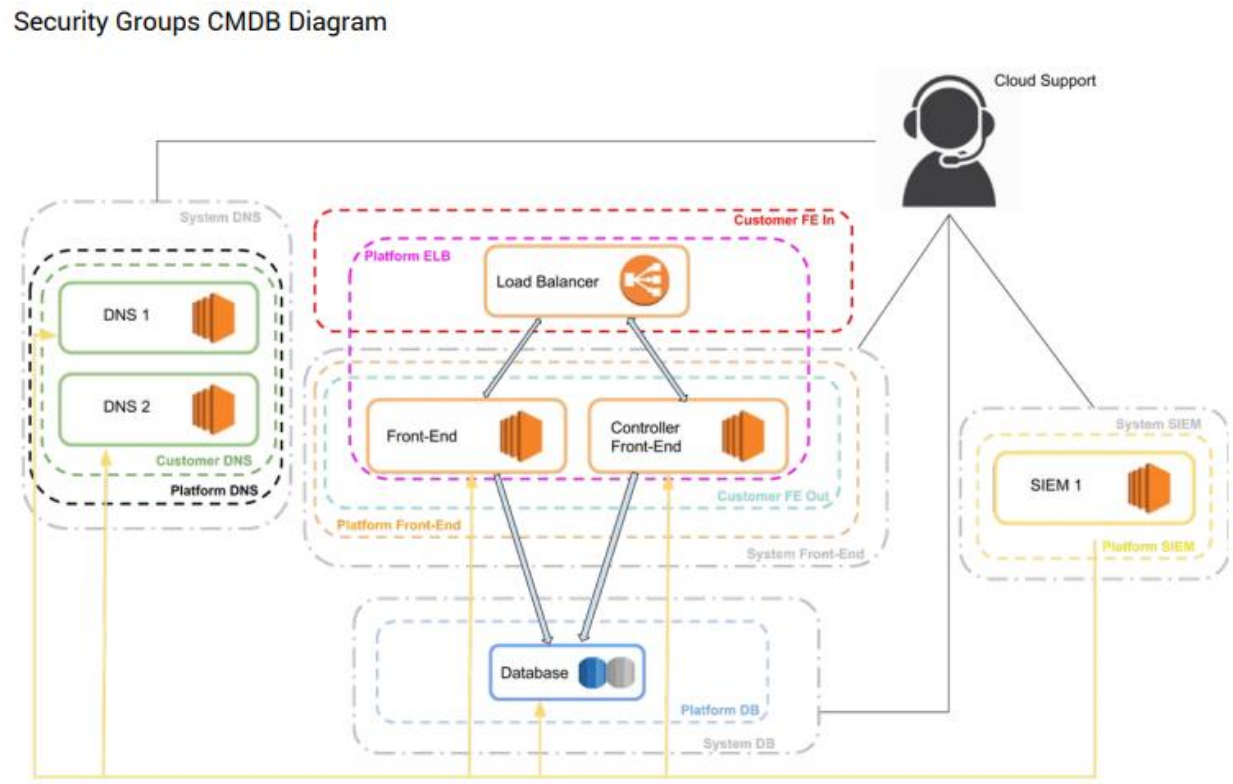
The organization supplies PaaS offerings intended to meet SOC2 requirements for organizations with a cloud first strategy that need to capture and store sensitive data such as customer, financial, or classified information, and need a secure cloud solution. OutSystems provides certified cloud environments with proactive security monitoring, built in redundancy, and support offered at all times to significantly reduce the likelihood of a data breach and to accelerate detection.

The following OutSystems locations are in scope:

- Atlanta, USA
- Boston, USA
- Braga, Portugal
- Frankfurt, Germany
- Hong Kong, China
- Tokyo, Japan
- Kuala Lumpur, Malaysia
- Linda-a-Velha, Portugal
- Melbourne, Australia
- Utrecht, Netherlands
- Proenca-a-Nova, Portugal
- Singapore, Singapore
- Sydney, Australia
- London, United Kingdom
- Dubai City, U.A.E.

Infrastructure

The following diagram reflects the organization's network:



Splunk auto-generates the network diagram as needed based on application programming interfaces within the Splunk Heavy Forwarder. Splunk gets network information from Amazon Web Services (AWS) as it is configured to send critical logs to Splunk for storage, alerting, and documentation.

A complete inventory of systems including virtual technologies is maintained by the organization. The inventory is stored in the BackOffice application and is maintained by the System Engineering personnel. It is regularly compared to the Splunk and AWS inventories.

Software

The organization maintains a complete software inventory, including licensing documentation. Inventories require the name of the software, version number, vendor, and function. Software change history is also maintained within the inventory. Software inventories are segmented into the following departments:

- Windows 2012 Controller Front-End
- Windows 2016 Controller Front-End
- Database
- SIEM Collector
- DNS Server
- Trend Micro Relay

- Trend Micro Proxy
- Chef Server
- Radius Server
- Workspace

People

The organization adheres to the following traditional structure:

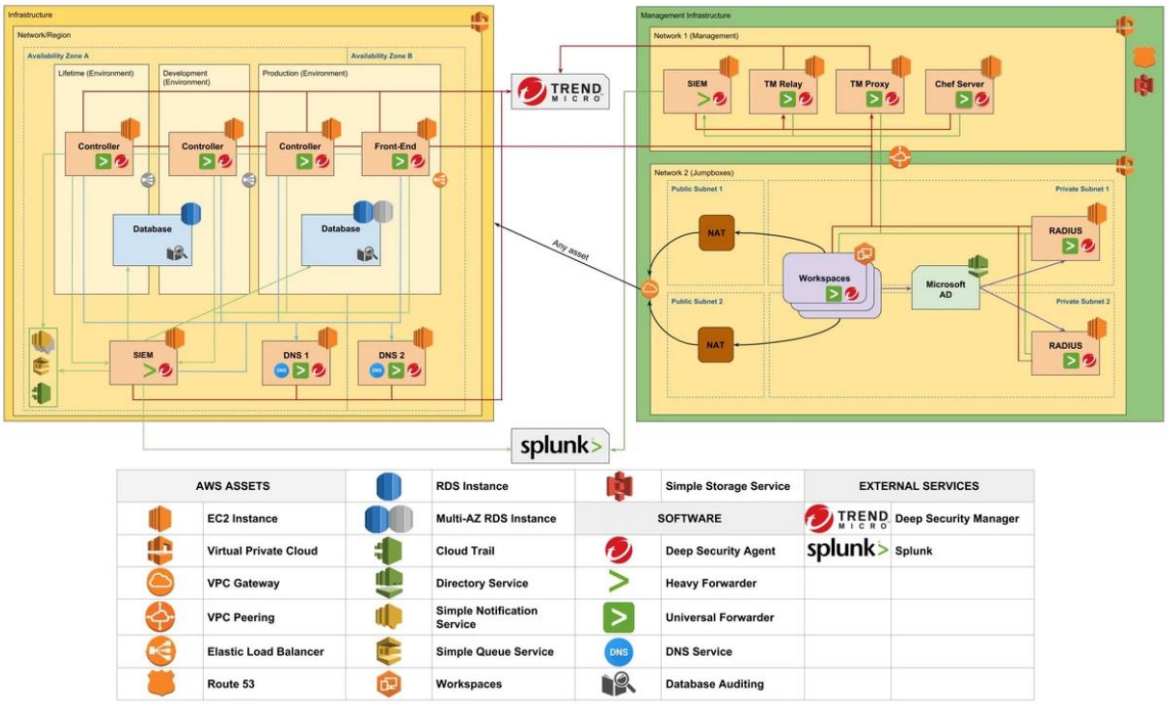
Executive leadership consists of a Chief Executive Officer, Chief Financial Officer, Chief People Officer, Chief Revenue Officer, and a Chief Marketing Officer. Other members of leadership include the Vice Presidents of the Engineering, Project X and Product Management, and People

departments. The leadership team is overseen by shareholders. Reporting lines are documented within the ISMS Roles and Responsibilities.

The board of directors consists of nine members that are independent from the leadership team. They are experienced executives from the technology industry.

Data

The following Data Flow Diagram demonstrates how sensitive data moves throughout the organization:



Data Flow Diagrams are automatically generated by Splunk. The diagram indicates ports and protocols used to transfer data within the environment. A chart is also maintained to indicate logical access methods. The support team is responsible for implementing the Data Flow Diagram to the environment. Every change to data flow must be approved and documented as soon as it is implemented.

The MSA addresses data retention requirements related to customer data. The MSA also contains the following data processing definitions:

- Confidential Information: non-public information that either Party may obtain from the other or have access to by virtue of this Agreement, including, but not limited to, each Party's data and each Party's proprietary Software and computer operations, all code, inventions, algorithms, business concepts, workflow, marketing, financial, business and technical information, the terms and pricing under this Agreement, authentication credentials associated with the use of the Software and the Professional Services, personal data and all information clearly identified as confidential.

- Personal Data: any information of any type, irrespective of the type of medium involved, including sound and image, relating to an identified or identifiable natural person.

Any time sensitive data is to be transmitted over open, public networks it is secured. OutSystems is responsible for formal channels provided to clients and provides guidance to clients to help them avoid insecure transmission processes. AWS Security Groups will limit any customer-caused data insecurities.

The following best practice standards underpin the organization's encryption methods for the open transmission of sensitive data:

- Payment Card Industry (PCI) Security Standards Council
- International Organization for Standardization (IOS)
- General Data Protection Regulation (GDPR)

Information involved in application service transactions is protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication and replay. Data in transit is divided into one of two categories

- Between the front-ends and the database instances
- Between the front-ends and external endpoints

The protocols and ciphers used to ensure data security during transmission are regularly evaluated for proper functioning.

Processes and Procedures

The organization implements Splunk, which is a comprehensive monitoring system that negates the need for most daily operational security procedures. Log monitoring and alerts are monitored by Splunk and can be broken down into the following:

- Platform monitoring
- Server OS logs
- DB logs
- AWS security groups and firewall logs
- IDS alerts
- FIM logs

SECTION B:
PRINCIPLE SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Contractual Commitments

OutSystems has established its Master Subscription Agreement (MSA) that clarifies the responsibilities that the organization has to their client and limits the types of data and applications that will be hosted for customers. Service Level Agreements (SLA) are documented within the MSA. Compliance is monitored by SolarWinds. SolarWinds generates compliance reports for the Security Operations team to review.

System Design

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