outsystems

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, 2019 through June 30, 2020.

KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

KirkpatrickPrice. innovation. integrity. delivered.

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 Sentry Application Development and Delivery Platform System (system) throughout the period July 1, 2019, to June 30, 2020, 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, 2019, to June 30, 2020, 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, 2019, to June 30, 2020, 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

INDEPENDENT SERVICE AUDITOR'S REPORT

Paulo Rosado
CEO
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 Sentry Application Development and Delivery Platform system (system) were effective throughout the period July 1, 2019, to June 30, 2020, 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 Sentry Application Development and Delivery Platform system were effective throughout the period July 1, 2019, to June 30, 2020, 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

July 29, 2020

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

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

Services Provided

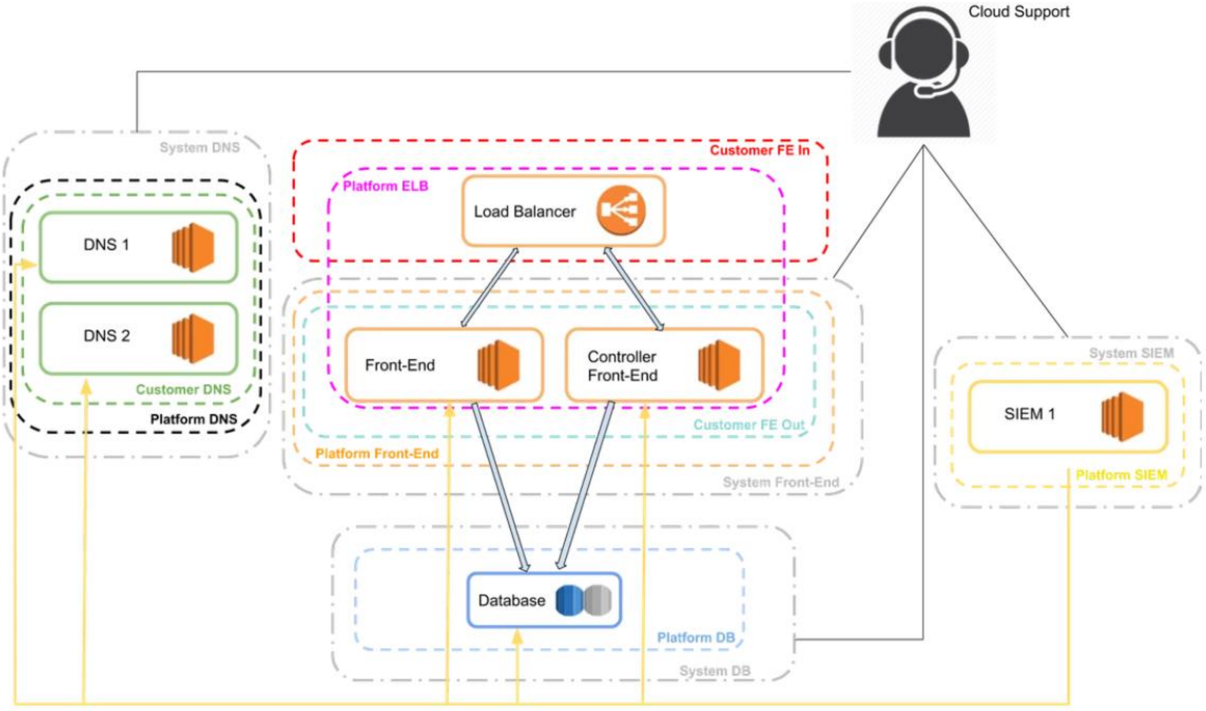
Located in Linda-a-Velha, Portugal, OutSystems, Inc. (OutSystems) is a rapid application development and delivery platform for mobile and web applications, available in a Platform as a Service (PaaS) model. The organization supplies PaaS offerings intended to meet SOC 2 requirements for organizations 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 constantly available support to significantly reduce the likelihood of a data breach and to accelerate detection.

From a commercial and delivery perspective, OutSystems' PaaS is segmented in different offers. The Sentry application development and delivery platform system is the reinforced OutSystems cloud offer. Sentry provides the experience of OutSystems with additional security, risk management, and monitoring for a SOC 2 Type II compliant low-code cloud platform. OutSystems Sentry provides additional security features specifically designed for the enterprise and for organizations working with sensitive, core, and customer data. The additions of Sentry include the following:

- Comprehensive security
    - Secure private networks
    - Defense
    - Integrity monitoring
    - Antivirus and malware protection
- Proactive monitoring and support
    - Dedicated SecOps and CSIRT
    - Intrusion prevention
    - Active log and network monitoring
    - Global threat intelligence
- Risk management
    - Change request procedures
    - Log retention and storage
    - Built-in high availability
    - Dedicated environment

Infrastructure

OutSystems maintains a formally documented network diagram, pictured below, that illustrates the relationship among networks and systems. The diagram is auto-generated from Splunk as needed, and changes made to the environment are immediately reflected in the Splunk environment. The system inventory is also represented in the network diagram and is compiled regularly using the Splunk inventory, the AWS inventory screen, and individual inventories maintained in various applications.



Software

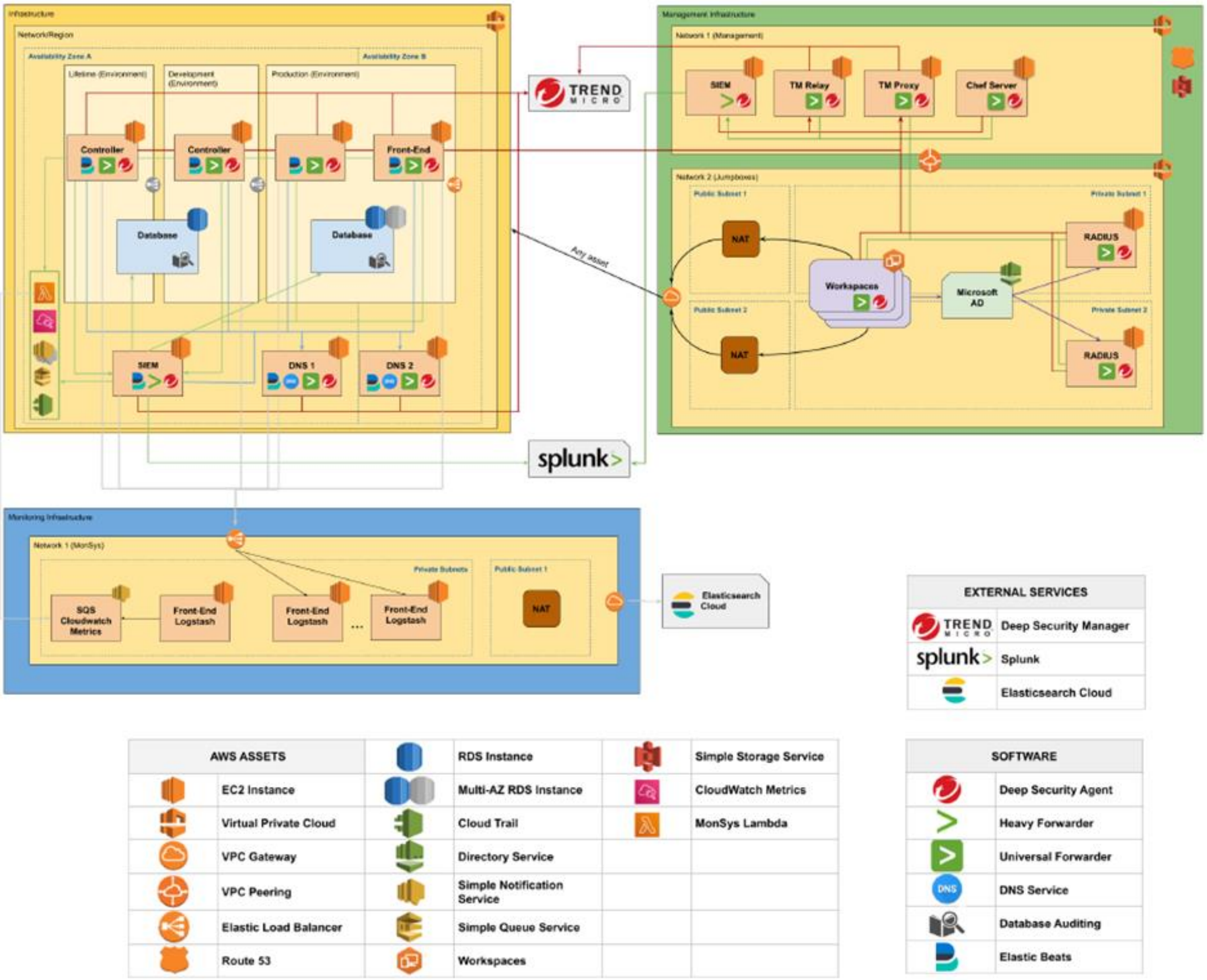
OutSystems maintains a software inventory that reflects the critical software in use and licensing information. All software components are tracked in the cloud architecture knowledgebase, and licensing is tracked for paid software; the Cloud Architecture Team updates the documentation as needed.

People

OutSystems maintains a traditional structure, with leadership and management providing oversight. A Board of Directors provides oversight for the organization's development and performance. The organization is divided into clearly defined groups, with leaders supervising each department; the separation ensures operational independence when necessary. For instance, security personnel, SOC, and compliance personnel have a reporting structure independent of product design and development. The company maintains an Organization Chart that is maintained in BambooHR, and it illustrates the company's structure and reporting lines.

Data

OutSystems maintains a platform that allows customers to develop their own applications and provides a secure baseline for customer application development. The organization does not have visibility into the types or nature of data stored or into what sensitive data might be stored by customers. The organization maintains a data flow diagram that illustrates the movement of sensitive data through the systems:



The organization maintains an Information Classification and Handling Policy that defines how data is classified. The policy details criteria and proper use for five levels of data security: unclassified/public, internal, restricted, confidential, or secret. Only select personnel are allowed to access each type of data. The policy provides examples and details the impact of each data type.

OutSystems maintains a key management process to ensure that encryption keys are appropriately protected. The Key and Certificate Management Policy requires that keys be stored on separate machines from those they encrypt and prescribes advanced protection methods for access. Keys must be encrypted with an encryption at least as strong as the encryption managed by the key.

Secure channels are maintained to ensure that data can be safely transmitted or received via open, public networks. The organization uses encryption to ensure that transmissions are protected against common vulnerabilities; transport layer security (TLS) is supported with acceptable ciphers. Data in transit can be divided into two categories: between the front-ends and the database instances, and between the front-ends and external endpoints. OutSystems is responsible for formal channels provided to clients, and it provides guidance to customers to attempt to prevent weak insecure processes on the customer's end. The organization's data is structured to ensure that a single client building in an insecure channel cannot provide access to other client's data.

Processes and Procedures

Management has developed and communicated processes and procedures to employees to ensure the execution of policy documentation and critical business processes. Changes to company procedures are performed annually and are authorized by management. Current processes and procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from the 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, passwords, powerful utilities, and security devices

SECTION B:
PRINCIPLE SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Regulatory Commitments

OutSystems has committed to adhere to certain regulatory requirements in the provision of its services. Regulatory requirements related to its services include the Payment Card Industry Data Security Standard Self-Assessment Questionnaire (PCI DSS SAQ) and the General Data Protection Regulation (GDPR). OutSystems acts as a Cloud Service Provider that provides a PaaS service to customers, and it does not use payment applications, such as payment gateways, PED terminals, and other payment processing software, within the OutSystems in-scope environments.

Contractual Commitments

OutSystems maintains contractual materials that define the scope of services clients can expect to receive. The Master Subscription Agreement (MSA) clarifies the responsibilities that the organization has to its clients and limits the types of data and applications that are hosted for customers. The MSA includes the following information:

- Definitions
- Subscription
- License
- Professional Services
- Fees and Payment Terms
- Intellectual Property Rights, Ownership and Title
- Confidentiality
- Term and Termination
- Warranties
- Limitation of Liability
- General Provisions

The organization also maintains service-level agreements (SLAs) with customers. SLAs are associated with the product offerings available on the web to all customers, and they address support severity levels and response times, support access periods, and support level availability.

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' system policies and procedures, system design documentation, and contracts with clients.