
# OutSystems

## Service Organization Control Report (SOC 3)

Independent Report of the Controls to meet the criteria for the Security, Availability, Processing Integrity, and Confidentiality principles for the period of January 1, 2017through June 30, 2017.



KirkpatrickPrice

Kirkpatrick Price, LLC
1228 East 7th Ave., Suite 200
Tampa, FL 33605

# TABLE OF CONTENTS

# MANAGEMENT OF OUTSYSTEM'S ASSERTION REGARDING ITS APPLICATION DEVELOPMENT SERVICES THROUGHOUT THE PERIOD JANUARY 1, 2017 TO JUNE 30, 2017

# OUTSYSTEMS' ASSERTION

OutSystems maintained effective controls over the Security, Availability, Processing Integrity, and Confidentiality of its Application Development Services "System" to provide reasonable assurance that:

- The System was protected against unauthorized access (both physical and logical)
- The System was available for operation and used as committed and agreed
- The System was complete, accurate, timely, and authorized
- Information from the System designated as confidential protected as committed or agreed

During the period January 1, 2017 through June 30, 2017, based on the criteria for the Security, Availability, Processing Integrity, and Confidentiality set forth in the American Institute of Certified Accountants (AICPA) TSP section 100, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

This included System Description of the OutSystems Application Development Services and its boundaries identifies the aspects of the OutSystems Application Development Services covered by our assertion.

# INDEPENDENT SERVICE AUDITOR'S REPORT

on the OutSystems Application Development Services Relevant to Security, Availability, Processing Integrity, and Confidentiality

# INDEPENDENT SERVICE AUDITOR'S REPORT

Paulo Rosado
CEO
OutSystems
5901 Peachtree Dunwoody
Road NE, Building C 495
Atlanta, GA 30328

We have examined management's assertion that OutSystems throughout the period January 1, 2017 to June 30, 2017 maintained effective controls to provide reasonable assurance that:

- The System was protected against unauthorized access (both physical and logical)
- The System was available for operation and used as committed and agreed
- The System was complete, accurate, timely, and authorized
- Information from the System designated as confidential protected as committed or agreed

Based on the criteria of Security, Availability, Processing Integrity, and Confidentiality in the TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) (applicable trust services criteria). The assertion is the responsibility of OutSystems management. Our responsibility is to express an opinion based on our examination.

We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we (1) obtain and understanding of OutSystems' relevant Security, Availability, Processing Integrity, and Confidentiality controls, (2) test and evaluate the operating effectiveness of the controls, (3) perform such other procedures as we consider necessary in the circumstances. We believe our examination provides a reasonable basis for our opinion.

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

In our opinion, in all material respects, based on the criteria identified in OutSystems' assertion and the applicable trust services criteria are fairly stated.

Damon Sullivan, CPA

KirkpatrickPrice, LLC
1228 East 7th Ave. Suite 200
Tampa, FL 33605

July 15, 2017

# OUTSYSTEMS' DESCRIPTION OF ITS APPLICATION DEVELOPMENT SYSTEM THROUGHOUT THE PERIOD JANUARY 1, 2017 TO JUNE 30, 2017

## Background

The OutSystems application Platform as a Service is a rapid application development platform for mobile and web applications, which is available in a Platform as a Service (PaaS) model. From a commercial and delivery perspective, OutSystems PaaS is segmented in that it maintains different offers. The OutSystems Sentry PCI subscription is one of these offers, which is targeted to Customers seeking a PCI compliant eCommerce platform to host their applications. The OutSystems Sentry and OutSystems Enterprise offers are also available in a PaaS model.

The organization uses several critical service providers and third-parties that provide services for OutSystems. The following identifies and describes the third-party services utilized most by the organization:

- Amazon Web Services, Inc. – Cloud Service Provider that provides servers, communications, and storage
- IDW - Consultoria em Serviços de Informação, Lda. – FortiSIEM provider and also provides penetration reports and vulnerabilities scans upon request

OutSystems ensures that compliance requirements are being met or supported by its service providers by requesting and documenting service providers' PCI compliance on annual basis, requesting and documenting service providers' SOC2 compliance on a bi-annual basis. Additionally, a full list of service providers and third parties that are accessing card networks can be found in the Service Providers Log.

## Software

The organization implements administrative and logical controls associated with the management of application change items throughout the SDLC. There are two types of change control procedures:

- Change control for the operational team is documented in the change management policy. All changes to the OutSystems PaaS fall into one of three categories:
  - Standard Changes
  - Normal Changes
  - Emergency Changes
- The R&D team changes the OutSystems software on new releases, following its software development lifecycle. This document provides guidelines for OutSystems R&D personnel involved in any task related to planning, creating, testing, or releasing the OutSystems platform.

The organization implements administrative and logical controls associated with the execution of code review activities. To ensure the quality of the OutSystems platform, code review is part of the R&D software development life cycle. The code review process is performed using Upsource, which is integrated with the version control tool (SVN):

- All commits performed in SVN are tracked in Upsource.
- When a code change requires a review (by developer request or team leader decision), a new Review is created in Upsource over the corresponding commit.
- The Review thread between the developer and the reviewers is handled in Upsource, while code corrections and improvements are committed in SVN; the Review ID is referenced in the SVN commit.
- The review process finishes when the change is accepted by all reviewers.

OutSystems uses Subversion for source code access control and versioning. The Subversion environment utilizes AD group permissions to grant access to the repository. New R&D members are assigned to the right AD groups and distribution lists, as part of the R&D onboarding procedure.

OutSystems maintains clear distinction between the staff responsible for each stage of the application delivery, since the development of the software (OutSystems platform) until the availability of the customer application. The customer's development/testing environments are separated from the customer production environment. This separation comprises the following:

- Distinct AWS accounts
- Distinct hosting servers
- Distinct Amazon RDS databases
- Network segregation (different VPCs)
- Segregated access—only the Cloud Security Team has access to the production environment
- Distinct user accounts

## People

The organization implements administrative controls associated with the organization's documentation of organizational responsibilities relating to information security. The organizational leadership consists of a CEO, CFO, CMO and four VPs who are overseen by a group of shareholders. Security reporting lines are also documented. Most of the security functions report to the CISO who reports to the VP of Engineering.

## Procedures

The following policies and procedures are in place:

- Acceptable Use of Resources Policy
- Acceptable Use Policy
- Access Management Policy
- Antivirus and Malicious Software Policy
- Backup Procedures
- Business Continuity Policy
- Change Control Procedure
- Change Management Policy
- Cloud Users Security Policy
- Data Privacy Policy
- Disposal and Destruction Policy
- Exercising and Testing Plan
- Global Compliance Policies
- Incident Management Response Plan
- Information Classification Policy
- Information Security Policy
- Information Transfer Policy
- Log Review Procedure
- Logical Access Policy
- Operational Policy
- Password Policy
- Penetration Testing Policy
- Physical Security and Environmental Policy
- Risk Assessment Methodology
- Security Awareness Program
- Security Operational Policy
- Software Development Lifecycle
- Supplier Security Policy
- Systems Application Development Policy
- Systems Hardening Policy
- Third Parties Policy
- Transportation Plan
- Vulnerability Management Policy
- Vulnerability Management Procedure
- Wireless Access Policy

## Data

The organization implements administrative controls associated with the retention of data within the organization's PaaS offerings.

All data in transit that is transmitted through public network is done over encrypted channels that use Industry wide accepted protocols like TLS. Management access is done using secure protocols like RDP and SSH.

The organization implements administrative controls associated with the use of formal standards for selecting controls for data in transit. Classification of data is in place within OutSystems, this includes the classification on data cardholder data and Personal Identifiable Information. These classification guidelines are communicated via the OutSystems Information Classification Policy.

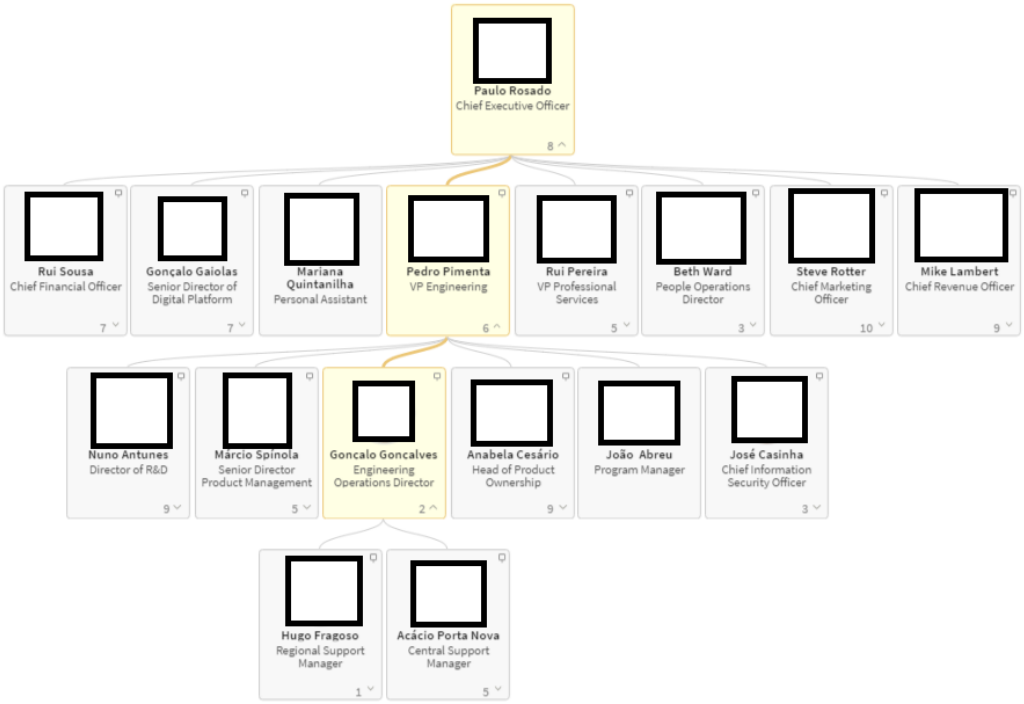
OutSystems uses connection-oriented protocols and UDP traffic tunnels over a VPN between the customer production environment and the management infrastructure, both on AWS. Over these tunnels, operations are done using industry accepted protocols like SSH and RDP. Users access the Management infrastructure via RDP that runs over a VPN tunnel established between OutSystems LaV office and the Management VPC on AWS.

# RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION SYSTEMS, AND MONITORING OF CONTROLS

## Control Environment

### Management Philosophy

An organization chart is maintained to highlight the division of responsibility within the company:




### Security, Availability, Processing Integrity, and Confidentiality Management

The OutSystems executive management sets tone and direction for the company employees by email. There is a quarterly web session where the CEO communicates business results and goals for the next quarter. Additionally, other sessions are promoted regularly by the CISO to ensure information security tone and guidance are also provided.

### Security, Availability, Processing Integrity, and Confidentiality Policies

The organization implements administrative controls associated with the ongoing revision and approval of organizational policies. The Chief Information Security Officer is responsible for operational coordination of the ISMS as well as for reporting about the performance of the ISMS to the SMT. Additionally, the OutSystems Information Security Officer has overall responsibility for the creation and distribution of security policies to the OutSystems employees or by email to third parties authorized to OutSystems assets.

The Senior Management Team must review the ISMS at least once a year or each time a significant change occurs, and prepare minutes from that meeting. The purpose of the management review is to establish the suitability, adequacy, and effectiveness of the ISMS.

The Chief Information Security Office must ensure that all employees of OutSystems, as well as appropriate external parties, are familiar with the OutSystems policies. All staff is reminded that the policies and related documents are sensitive and classified and therefore distribution must not be removed from OutSystems premises or networks.

All information security policies are reviewed by the Information Security Office team when necessary or at least on an annual basis. Senior Management is consulted for ensuring that the ISMS is implemented and maintained according to policy, and for ensuring all necessary resources are available.

Any changes made to the policies must be approved by the Chief Information Security Officer and communicated to all relevant and in scope employees, teams, or groups. Procurement and other Financial Departments are also responsible for maintaining their policies which are communicated via the HR department, People Ops.

### Controls Related to Personnel

The organization implements administrative controls associated with the development and distribution of an employee handbook. The organization maintains policies that address employee conduct, expectations and associated requirements relating to employment with the organization. Upon hire employees sign a form which addresses acknowledgment of the code of conduct as well as the data privacy policy. Discipline measures are also included in the policy.

Operational level agreements have been defined for the following departments:

- Digital Platform
- IT Services
- Legal
- Marketing
- People Ops
- Procurement
- Product Management
- R&D

The People Operations Department (HR) is responsible for hiring and onboarding new OutSystems personnel. The recruitment procedures include screening candidates for qualifications and experience with several interviews which are used to assess both the candidate's soft skills and technical skills related to the job in question. If in any interview there is evidence that the candidate is not a fit for the job, the candidate is disqualified and informed.

Upon hire, the candidates must present the individual criminal history record and education diplomas. All employees are also required to sign a contractual non-disclosure agreement and take knowledge of several OutSystems policies such as the Code of Ethics and Conduct, Data Privacy Policy, and Acceptable Use of Resources Policy. The People Operations is also

responsible for the employee's and contractual partners termination procedures, which include the request to revoke access to the internal IT Services Department.

OutSystems ensures that employees have access to training and development programs addressed to cover specific needs identified by managers and/or HR team in line with their professional role or specific business needs. Training and Development at OutSystems include all types of events, sessions, virtual or live meetings that have a learning and development outcome applicable in the context of OutSystems business. There are two main categories of Training and Development at OutSystems:

- Cross-Company Skills - Can be defined as the category that includes cross-sectional and can have a positive business impact overall (e.g. Soft Skills, Language Skills). The training and development of cross-company skills is managed by People Operations in collaboration with Managers and other Teams/Departments.
- Technical Skills - Can be defined as the category that includes specific technical skills associated with Teams/Department specific business objectives and learning needs. The training and development of technical skills is managed by different Teams/Departments.

## Security Policies

### Physical Security and Environmental Controls

The organization implements administrative controls associated with the restriction of physical access to the corporate facility. OutSystems protects secure areas in accordance with its Physical Security Policy. The physical access points within OutSystems are controlled at the building ingress and entry points using video surveillance, intrusion detection systems, and security guards monitoring the building 24/7. Additionally, the building security staff maintain written logs that record all physical access to the OutSystems office building, which are retained for 5 years. This process also includes recording any visitor/contractor access. Visitors and contractors present identification, and sign-in and sign out of the visitor log, and are continually escorted by authorized staff.

The OutSystems headquarters building has several layers of security controls in place to protect the buildings or premises that house OutSystems resources and assets, communication systems and computer systems. Physical security measures are in place to prevent unauthorized access to unauthorized persons to some asset. Due to the security of customers' data and OutSystems equipment, these accesses are reserved and must be strictly controlled.

OutSystems has a Disposal and Destruction Policy, documented on an organizational knowledge database (Confluence), which is applicable to any computer/technology equipment or peripheral devices that are no longer needed within OutSystems including, but not limited to the following:

- Personal computers and laptops
- Servers
- Hard drives
- Smartphones and handheld computers
- Peripherals (i.e., keyboards, mice, speakers)
- Network switches, routers, wireless access points
- Printers

- Scanners
- Portable storage devices (i.e., USB drives)
- Batteries
- Printed materials

The policy states the following:

- When technology assets have reached the end of their useful life, they are sent to OutSystems' IT for proper disposal.
- An appropriate external company with expertise on the disposal and destruction of IT assets is contracted.
- All storage mediums are securely erased in accordance with current industry best practices.
- All data, including all files and licensed software, must be removed from equipment using disk sanitizing software that cleans the media by overwriting each disk sector of the machine.
- No computer or technology equipment is sold to any individual.
- No computer equipment shall be disposed of via skips, dumps, landfill etc.
- All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives must also be removed and rendered unreadable (drilling, crushing or other demolition methods).
- Technology equipment with non-functioning memory or storage technology must have the memory or storage device removed and it must be physically destroyed.

The following guidelines are in place for visitors:

- All visitors and external personnel are required to present identification and are signed in at the building security front desk and office reception front desk.
- Visitors must be on the daily guest list to pass through the building security staff, or in case they are not on the guest list, the security staff will notify office reception front desk of the unlisted guest and explicit authorization must be given for the visitor to enter the building facilities.
- Upon leaving the building, visitors are asked to sign out of the building by the office reception front desk and building security front desk.
- All visitor access to high-security level areas must be escorted by an OutSystem employee at all times.
- Visitors must under no circumstances be allowed to move unaccompanied through areas of the building where cardholder data is processed or maintained without management authorization.
- Visitors are asked to leave the building and can only remain in the facilities from 8 AM to 8 PM on the same day.
- The building visitor log records the following information:
    - Visitor's name
    - Type of ID checked
    - ID number
    - Onsite contact
    - Date & time

- The corporate office visitor log records the following information:
    - Visitor's name
    - Company
    - Onsite contact
    - Date & time

The following guidelines are in place for authorized staff access:

- The system that controls the physical access to the OutSystems offices facilities includes biometric/code recognition systems or, alternatively, access can be made with proximity badges.
- Within all spaces of the OutSystems offices, authorized staff must be authenticated with fingerprint and code readers systems to access the data center/technical rooms floors, or in the alternative with an access badge for non-technical rooms areas.
- Moving between secure physical areas of the building requires repeated interaction with biometric/code readers or access badges.
- OutSystems only provides access and information to employees and contractors who have a legitimate business need for such privileges. For instance, access to data center/technical rooms is limited to a very restricted number of employees.
- When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of OutSystems.

Access points are equipped with security cameras that monitor and record access activity. Live feeds from the security cameras are displayed and monitored by security personnel. Data from the security cameras is retained for a minimum of 70 days and is available for payback.

OutSystems has environmental controls in place for general office areas and data centers & technical rooms:

- General Office Areas
    - Automatic fire detection equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all office areas and produces audible alarms in the office rooms. These areas are protected by carbon dioxide and dry chemical fire extinguishers, that can cover A, B, & C fires.
    - Firehoses are also available at the public areas in a way that can cover Class A fires in the building as well as some of the fire extinguishers in the offices.
    - Fire suppression systems described are reviewed and maintained at least yearly in accordance with regional regulations.
    - Alarm buttons exist in the public areas in the event of a fire alarm occurs the building security clerks will inform the local authorities including the local fireman department.
- Data Centers & Technical Rooms
    - Climate control is required to maintain a constant operating temperature for servers and other hardware in the Data Centers and Technical Rooms, which prevents overheating and reduces the possibility of service outages.
    - Data Centers are conditioned to maintain atmospheric conditions at optimal levels.

- OutSystems IT personnel control the temperature and humidity at appropriate levels.
- All structures surrounding or belonging to technical areas or technical centers must be non-combustible or fire resistant. Any openings in these structures must also be leakproof, non-combustible, or fire resistant.
- Every Data Center and Technical Room must have their own fire detection controls in place and fire extinguishers.
- The Data Center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week.
- An uninterruptible power supply (UPS) unit provide backup power in the event of an electrical failure for critical and essential loads in the facility.

**Change Management**

The organization implements administrative and logical controls associated with the management of infrastructure changes in the environment. OutSystems PaaS abstracts users from the underlying platform infrastructure for all operations. The customers' infrastructure(s) are automatically provisioned, abstracted, and managed. To ensure optimum performance and reliability of the environments, customers must not have direct access to the servers through remote access or Telnet/SSH.

Configurations changes follow a formal approval process, with a predefined set of criteria that the approver must analyze before allowing the execution by a different OutSystems employee. Change requests are duly recorded and compared against system activity during log review. Any unexpected change will trigger the Security Incident Management procedure.

To correctly achieve compliance with the OutSystems security policies and configuration standards, support specialists, R&D architects, and specialists collaborate to review standards when a significant change is necessary or at least quarterly. In these meetings, infrastructure, data, software, and policies and procedures are updated as necessary to comply with the requirements. An exception report is prepared and remediation plans are developed and tracked.

The organization implements administrative controls associated with the ongoing review and revision of system hardening requirements. The organizational hardening baselines are based on AWS documentation and the CIS hardening guide for Windows and Linux Servers. A formal document that lists all hardening procedures is maintained at the Cloud Security knowledge base. This document is reviewed quarterly or when there are significant changes to the environment by members of both Cloud Framework and CSIRT. To attest to compliance with this document, regular hardening reviews are performed.

The organization maintains subscriptions to data sources that provide information relating to changing trends in information security. OutSystems personnel actively follows security notifications and updated information from AWS and technology stack vendors.

The organization implements administrative controls associated with the communication of information relating to events impacting system security or availability. When changes are

required during the maintenance period, notification is sent to the client via email. The Maintenance task's communications will be sent at least two days ahead.

### System Monitoring

The organization implements administrative and logical controls associated with the monitoring and logging of system events and other data. For SIEM, OutSystems uses FortiSIEM, which allows both agent-based and agentless configurations. OutSystems is employing the agentless configuration where information is collected from the machines either via SNMP or WMI. Collected information varies from performance metrics to windows event logs.

For endpoint protection (anti-malware, web reputation, file integrity monitoring, intrusion prevention, and firewall flows) OutSystems uses TrendMicro Deep Security Agents. Each event generated by the agent is sent to the SIEM via syslog where they are analyzed. TrendMicro Deep Security Manager sends events to the SIEM via syslog.

The organization implements administrative and logical controls associated with the organization's use of systems to monitor system capacity and other critical resources. FortiSIEM collects system performance information via WMI and SNMP. This information is displayed both as an aggregated view and individual view per server. There are configured alarms that trigger if a pre-defined threshold is reached. Such alarms exist for CPU, memory, and disk.

### Problem Management

The organization implements administrative controls associated with the organization's establishment of formal procedures supporting incident response activities. OutSystems Security Incident Response Policy is publicly available and it:

- Sets out OutSystems' high level requirements for the business recovery of OutSystems' Enterprise aPaaS assets in the event of a system breach. Specific attention is paid to the storage, processing, or transmission of customer data.
- Defines the Incident Response statement for OutSystems Enterprise aPaaS business.
- Applies to all data processing operations for OutSystems Enterprise aPaaS business.

The Security Incident Management Procedure details the steps required to ensure all suspected information security incidents are reported promptly to OutSystems Management and that the correct procedures are performed to respond appropriately to security incidents. It is applied to all OutSystems employees interacting with the PCI Environment(s) or Management Infrastructure(s) as well as OutSystems information resources, application, and systems software within the cardholder data environment.

Any violation of OutSystems security policies is defined as a potential security incident, and security incidents that affect the installation must be assessed to determine their impact on the operation and management of OutSystems (card) processing operations, which includes (1) loss or theft of secret keys used for encrypting credit card data or (2) loss or theft of hardware containing encrypted credit card data.

### Data Backup and Recovery

The organization implements administrative and logical controls associated with the backup and restoration of data. RDS backups are automatically taken, enabling point-in-time restore for 15 days, with no downtime and a minimum impact. Customers are responsible for requesting database restores to OutSystems, when necessary to fix any data corruption issue. Database restores will be executed according to the terms and conditions of the OutSystems public cloud service. From the backups, OutSystems is able to recover all application source versions, all configurations and application runtime data. Backup snapshots of each server within the Management Infrastructure are produced before and after any significant change takes place.

### System Account Management

The organization implements administrative controls associated with the execution of account management activities. The account roles policies that are issued to roles within OutSystems environment are based on the principle of the need to know basis, i.e., permissions policies must have the minimum required permissions to allow people to perform their duties.

OutSystems follows a formal procedure to authorize/approve users prior to access, whether dealing with internal employees or partners. Depending on the user profile and role, several logical access procedures address the request, approval, and provisioning process of authorizing and implementing user IDs.

Users are assigned a unique ID before being allowed access to system components. After the creation of the user on BambooHR, it will be created automatically in the AD, on Intranet/ Extranet and on Google Accounts 48 working hours before the actual hire date. It will also require the IT Services to manually assign the appropriate distribution lists (DLs). Moreover, depending on the location and functional area (e.g. sales, marketing), accesses might have to be assigned to specific applications.

Access to OutSystems' information systems is immediately revoked for any terminated/ separated employees after communication by PeopleOps or by the employee manager. This is also performed according to a formal procedure by IT Services. It is OutSystems policy to determine that:

- As soon as an employee ceases functions at OutSystems, this fact must be immediately communicated to the IT Services by PeopleOps to guarantee that his/her access rights are immediately revoked.
- All accounts that have not been accessed for more than six (6) weeks are considered inactive and must be automatically locked to prevent access or misuse.
- Inactive accounts that are reactivated must require the password to be changed.
- Inactive accounts that have remained locked for more than ninety (90) days are considered expired accounts.
- Expired accounts are maintained, disabled, or removed from the system.

Within the OutSystems Support services to the customer, anyone can put in the request via the support portal. Validation of the identity is performed over the phone for client accounts or in person for OutSystems accounts. The ticket then generates a new change request. The support manager/team leader reviews the change request and may choose to approve or deny the change

request. The Cloud Support then implements the approved change. Communication then occurs between the Support and either the internal or external point of contact.

The organization implements administrative and logical controls associated with the use and configuration of automated access controls. The identity and authorization management are centralized within the components used. Additionally, the Firewall and Router Security Policy addresses firewall configuration and the use of forms which support the review of firewall rules as well as the documentation of justified ports and protocols.

The organization implements administrative controls associated with the provisioning and termination of accounts for client access to systems.

The organization implements administrative and logical controls associated with the implementation of MFA to constrain access to the organization's AWS environment. Two-factor authentication is therefore required when accessing:

- The machine Operating Systems - The Web Application Duo Security is used as MFA Identity Provider within the OutSystems PCI components, namely the access to the CDE and Management Machines.
- The Amazon Web Services Web Console - Using AWS IAM policies and Secure Token Service enforcing MFA authentication as well.
- Trend Micro Deep Security Agent Web Console - Using the provided MFA capabilities.

## Risk Assessment Process

The organization implements administrative controls associated with the execution of risk assessment and risk management activities. OutSystems risk management program identifies and analyzes the risk as an ongoing management process. This process aligns with ISO 27001 and ISO 22301 certification since the business continuity aspects are considered first and then a risk assessment is conducted at least annually with the internal teams critical to ensure proper resilience in the service(s) provided to customers.

A comprehensive list of relevant risks is compiled and registered in the Risk Treatment Plan, which is managed by the Security Office team to categorize, track, and mitigate specific security and compliance risks. At least annually the members of the Security Office team and other business owners meet to review and update the Risk Assessment and Risk Treatment Plan.

The OutSystems methodology for risk assessment is based on a hybrid approach, where risk is determined as a function (multiplication) of the impact on a certain asset subgroup, the likelihood of occurrence and the value of that asset subgroup. The impact of a certain threat affecting a determined asset is calculated based on 4 vectors: availability, integrity, authenticity, and confidentiality.

These 4 vectors have a binary weight, whether that vector can be affected by a certain threat/vulnerability or not and corresponding weights were determined based on OutSystems context analysis as well as strategic directions. By summing each one of the 4 vectors' weights, it is possible to obtain the value of the impact used to determine the risk value:

- Confidentiality

    - High=1; Low=0 - characteristic of the information by which it is available only to authorized persons or systems;
- Integrity
    - High=3; Low=0 - characteristic of the information by which it is changed only by authorized persons or systems in an allowed way;
- Availability
    - High=4; Low=0 - characteristic of the information by which it can be accessed by authorized persons when it is needed;
- Authenticity
    - High=2; Low=0 - property that an entity is what it claims to be.

## Information and Communication Systems

The organization implements administrative controls associated with the development and communication of policies relating to the organization's information security program. This Policy is applied to the scope of the OutSystems' Information Security Management System (ISMS) included in their compliance requirements. Users of this document are all employees of OutSystems as well as relevant external parties.

General objectives for the information security management system are the following:

- Increase customer trust and success
- Reducing the damage caused by potential incidents
- Increase organization reputation
- Security goals are in line with the organization's business objectives, strategy, and business plans

Policies are defined and published by the Security Office, approved by the senior management team and CEO, and communicated by email to the whole company by the HR Department—People Ops—to all the employees and business partners that have access to any of the OutSystems IT resources.

The Chief Information Security Officer is responsible for reviewing these general ISMS objectives and setting new ones. Objectives for individual security controls or groups of controls are proposed by Managers and approved by Chief Information Security Officer. OutSystems' SMT representatives measure the fulfillments of all the objectives.

The Chief Information Security Officer is responsible for setting the method for measuring the achievement of the objectives. The measurement is performed at least once a year and Chief Information Security Officer will analyze and evaluate the measurement results and report them to top management as input materials for the management review. All the objectives must be reviewed at least once a year.

The organization implements administrative controls associated with the development and communication of acceptable use policies. OutSystems designates responsibilities for information security personnel as well as the expected behaviors of all personnel in support of information security objectives.

OutSystems engages in regular training sessions to ensure that staff is fully aware of the implications of disaster situations on business continuity. Additionally, OutSystems promotes and enforces the continual training on relevant technical and security related qualifications required for employees with advanced security responsibilities by attending annual security training events, including security conferences, courses, vendor training sessions or maintaining security related certifications.

The organization implements administrative controls associated with the publication of reporting procedures for incidents or complaints. Customers sign a Subscription Agreement with the organization, which explicitly mentions the organization's obligations for responding to service requests, and includes instructions for customers to submit them.

OutSystems specifically enforces the use of non-disclosure agreements in the course of its operations with third-parties, whether they are providers or customers.

The organization implements administrative controls associated with the execution of recurring activities in support of information security objectives. All logs generated for systems within the cardholder data environments and management infrastructures are reviewed daily based on the flow of cardholder data over the OutSystems PCI CDE and management network, including the following components:

- Operating System Logs
- Database Audit Logs
- Firewalls
- IDS Logs
- Antivirus Logs
- File integrity monitoring system logs
- All system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD
- All servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)

## Monitoring Controls

The organization implements administrative controls associated with the implementation of quality monitoring and management initiatives. The OutSystems Support center main units are Product Support, Cloud Support, and Customer service. They produce and monitor a variety of KPIs including response times, the number of interactions, the level of effort, satisfaction survey scores, security incidents.

On a weekly basis, a report of non-satisfied client incidents is produced and analysis is performed by operations.

OutSystems ensures that sufficient technical safeguards are installed and configured to monitor, defend, and react to external or internal security threats using the following:

- Intrusion Prevention System or Intrusion Detection Systems

- Firewall and De-Militarized Zone (DMZs) to isolate and protect cardholder data environment
- Anti-Virus & Anti-Malware software
- File Integrity Monitoring software
- Amazon Web Services CloudTrail service
- Two-factor Authentication software
- Automated log backup systems
- External Uptime Monitors

Upon detection of a security alert, the staff member who receives the alert informs the CSIRT if the alert is genuine. On-demand, a root cause analysis can be conducted for the client. Lessons learned and action items are logged in the ticket system(s) and addressed as soon as possible.

# TRUST SERVICES SECURITY, AVAILABILITY, PROCESSING INTEGRITY, AND CONFIDENTIALITY PRINCIPLES AND CRITERIA

| Criteria Common to All Security, Availability, Processing Integrity, and Confidentiality Principles | | | |
|---|---|---|---|
| **1.0 Common Criteria Related to Organization and Management** | | | |
| **Ctrl #** | **Control Activity** | **Testing of Operating Effectiveness** | **Test Results** |
| 1.1 | The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance and monitoring of the system enabling it to meet its commitments and requirements as they relate to Security, Availability, Processing Integrity, and Confidentiality. | | |
| 1.2 | Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and placed in operation. | | |
| 1.3 | Personnel responsible for designing, developing, implementing, operating, maintaining and monitoring the system affecting Security, Availability, Processing Integrity, and Confidentiality have the qualifications and resources to fulfill their responsibilities. | | |
| 1.4 | The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to Security, Availability, Processing Integrity, and Confidentiality. | | |

| Criteria Common to All Security, Availability, Processing Integrity, and Confidentiality Principles | | | |
|---|---|---|---|
| **2.0 Common Criteria Related to Communications** | | | |
| **Ctrl #** | **Control Activity** | **Testing of Operation Effectiveness** | **Test Results** |
| 2.1 | Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external system users to permit users to understand their role in the system and the results of system operation. | | |
| 2.2 | The entity's Security, Availability, Processing Integrity, and Confidentiality commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal system users to enable them to carry out their responsibilities. | | |
| 2.3 | The entity communicates the responsibilities of internal and external users and others whose roles affect system operation. | | |
| 2.4 | Internal and external personnel with responsibility for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the Security, Availability, Processing Integrity, and Confidentiality of the system, have the information necessary to carry out those responsibilities. | | |
| 2.5 | Internal and external system users have been provided with information on how to report Security, Availability, Processing Integrity, and Confidentiality failures, incidents, concerns, and other complaints to appropriate personnel. | | |
| 2.6 | System changes that affect internal and external system user responsibilities or the entity's commitments and requirements relevant to Security, Availability, Processing Integrity, and Confidentiality are communicated to those users in a timely manner. | | |

| Criteria Common to All Security, Availability, Processing Integrity, and Confidentiality Principles | | | |
|---|---|---|---|
| **3.0 Common Criteria Related to Risk Management and Design and Implementation of Controls** | | | |
| **Ctrl #** | **Control Activity** | **Testing of Operation Effectiveness** | **Test Results** |
| 3.1 | The entity (1) identifies potential threats that would impair system Security, Availability, Processing Integrity, and Confidentiality commitments and requirements, (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including controls and other mitigation strategies). | | |
| 3.2 | The entity designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy. | | |
| 3.3 | The entity (1) identifies and assesses changes (for example, environmental, regulatory, and technological changes) that could significantly affect the system of internal control for Security, Availability, Processing Integrity, and Confidentiality and reassesses risks and mitigation strategies based on the changes and (2) reassesses the suitability of the design and deployment of control activities based on the operation and monitoring of those activities, and updates them as necessary. | | |

| Criteria Common to All Security, Availability, Processing Integrity, and Confidentiality Principles | | | |
|---|---|---|---|
| **4.0 Common Criteria Related to Monitoring of Controls** | | | |
| **Ctrl #** | **Control Activity** | **Testing of Operation Effectiveness** | **Test Results** |
| 4.1 | The design and operating effectiveness of controls are periodically evaluated against Security, Availability, Processing Integrity, and Confidentiality commitments and requirements, corrections and other necessary actions relating to identified deficiencies are taken in a timely manner. | | |

| Criteria Common to All Security, Availability, Processing Integrity, and Confidentiality Principles | | | |
|---|---|---|---|
| **5.0 Common Criteria Related to Logical and Physical Access Controls** | | | |
| **Ctrl #** | **Control Activity** | **Testing of Operating Effectiveness** | **Test Results** |
| 5.1 | Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized user access to system components, or portions thereof, authorized by management, including, hardware, data, software, mobile, devices, output, and offline elements; and (3) prevention and detection of unauthorized access. | | |
| 5.2 | New internal and external system users are registered and authorized prior to being issued system credentials, and granted the ability to access the system. User system credentials are removed when user access is no longer authorized. | | |
| 5.3 | Internal and external system users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data). | | |
| 5.4 | Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them. | | |
| 5.5 | Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel. | | |
| 5.6 | Logical access security measures have been implemented to protect against Security, Availability, Processing Integrity, and Confidentiality threats from sources outside the boundaries of the system. | | |
| 5.7 | The transmission, movement, and removal of information is restricted to authorized users and processes, and is protected during transmission, movement, or removal enabling the entity to meet its commitments and requirements as they relate to Security, Availability, Processing Integrity, and Confidentiality. | | |
| 5.8 | Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software. | | |

| Criteria Common to All Security, Availability, Processing Integrity, and Confidentiality Principles | | | |
|---|---|---|---|
| **6.0 Common Criteria Related to Systems Operations** | | | |
| **Ctrl #** | **Control Activity** | **Testing of Operation Effectiveness** | **Test Results** |
| 6.1 | Vulnerabilities of system components to Security, Availability, Processing Integrity, and Confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated and countermeasures are implemented to compensate for known and new vulnerabilities. | | |
| 6.2 | Security, Availability, Processing Integrity, and Confidentiality incidents, including logical and physical security breaches, failures, concerns, and other complaints, are identified, reported to appropriate personnel, and acted on in accordance with established incident response procedures. | | |

| Criteria Common to All Security, Availability, Processing Integrity, and Confidentiality Principles | | | |
|---|---|---|---|
| **7.0 Common Criteria Related to Change Management** | | | |
| **Ctrl #** | **Control Activity** | **Testing of Operating Effectiveness** | **Test Results** |
| 7.1 | Security, Availability, Processing Integrity, and Confidentiality commitment and requirements are addressed, during the system development lifecycle including design, acquisition, implementation, configuration, testing, modification, and maintenance of system components. | | |
| 7.2 | Infrastructure, data, software, and procedures are updated as necessary to remain consistent with the system commitments and requirements as they relate to Security, Availability, Processing Integrity, and Confidentiality. | | |
| 7.3 | Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring. | | |
| 7.4 | Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented in accordance with Security, Availability, Processing Integrity, and Confidentiality commitments and requirements. | | |

| Additional Criteria for Availability | | | |
|---|---|---|---|
| **Ctrl #** | **Control Activity** | **Test of Operation Effectiveness** | **Test Results** |
| 1.1 | Current processing capability and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet availability commitments and requirements. | | |
| 1.2 | Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements. | | |
| 1.3 | Procedures supporting system recovery in accordance with recovery plans are periodically tested to help meet availability commitments and requirements. | | |

| Additional Criteria for Processing Integrity | | | |
|---|---|---|---|
| **Ctrl #** | **Control Activity** | **Test of Operation Effectiveness** | **Test Results** |
| 1.1 | Procedures exist to prevent, detect, and correct processing errors to meet processing integrity commitments and requirements. | | |
| 1.2 | System inputs are measured and recorded completely, accurately, and timely in accordance with processing integrity commitments and requirements. | | |
| 1.3 | Data is processed completely, accurately, and timely as authorized in accordance with processing integrity commitments and requirements. | | |
| 1.4 | Data is stored and maintained completely and accurately for its specified life span in accordance with processing integrity commitments and regulations. | | |
| 1.5 | System output is complete, accurate, distributed, and retained in accordance with processing integrity commitments and requirements. | | |
| 1.6 | Modification of data is authorized, using authorized procedures in accordance with processing integrity commitments and requirements. | | |

| Additional Criteria for Confidentiality | | | |
|---|---|---|---|
| **Ctrl #** | **Control Activity** | **Test of Operation Effectiveness** | **Test Results** |
| 1.1 | Confidential information is protected during the system design, development, testing, implementation, and change processes in accordance with confidentiality commitments and requirements. | | |
| 1.2 | Confidential information within the boundaries of the system is protected against unauthorized access, use, disclosure during input, processing, retention, output, and disposition in accordance with confidentiality commitments and requirements. | | |
| 1.3 | Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties in accordance with confidentiality commitments and requirements. | | |
| 1.4 | The entity obtains confidentiality commitments that are consistent with the entity's confidentiality requirements from vendors and other third parties whose products and services comprise part of the system and have access to confidential information. | | |
| 1.5 | Compliance with confidentiality commitments and requirements by vendors and other third parties whose products and services comprise part of the system is assessed on a periodic and as-needed basis and corrective action is taken, if necessary. | | |
| 1.6 | Changes to confidentiality commitments and requirements are communicated to internal and external users, vendors, and other third parties whose products and services are included in the system. | | |