OutSystems

Service Organization Control Report (SOC 3)

Independent Report of the Controls to meet the criteria for the Security, Availability, Processing Integrity, Confidentiality, and Privacy principles for the period of July 1, 2017 through June 30, 2018.

KirkpatrickPrice

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

TABLE OF CONTENTS

MANAGEMENT OF OUTSYSTEMS' ASSERTION REGARDING ITS SENTRY APPLICATION DEVELOPMENT AND DELIVERY PLATFORM SYSTEM THROUGHOUT THE PERIOD JULY 1, 2017 TO JUNE 30, 2018

OUTSYSTEMS' ASSERTION

OutSystems maintained effective controls over the Security, Availability, Processing Integrity, Confidentiality, and Privacy of its Sentry Application Development and Delivery Platform System "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 July 1, 2017 through June 30, 2018, based on the criteria for the Security, Availability, Processing Integrity, Confidentiality, and Privacy set forth in the American Institute of Ceritifed Accountants (AICPA) TSP section 100, Trust Services Principles and Criteria for Security, Availabilty, Processing Integrity, Confidentiality, and Privacy.

This included System Description of the OutSystems' Sentry Application Development and Delivery Platform System and its boundaries identifies the aspects of the OutSystems Sentry Application Development and Delivery Platform System covered by our assertion.

INDEPENDENT SERVICE AUDITOR'S REPORT

on the OutSystems Sentry Application Development and Delivery Platform SystemRelevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy

INDEPENDENT SERVICE AUDITOR'S REPORT

Paulo Rosado
CEO
OutSystems
374 Congress St
Boston, MA 02210

We have examined management's assertion that OutSystems throughout the period July 1, 2017 to June 30, 2018 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, Confidentiality, and Privacy 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 an understanding of OutSystems relevant Security, Availability, Processing Integrity, Confidentiality, and Privacy 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 20, 2018

OUTSYSTEMS' DESCRIPTION OF ITS SENTRY APPLICATION DEVELOPMENT AND DELIVERY PLATFORM SYSTEM THROUGHOUT THE PERIOD JULY 1, 2017 TO JUNE 30, 2018

Background

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.

Software

The organization maintains a complete inventory of their critical software in use, including software license documentation. All software components are tracked in the cloud architecture knowledge base. Licensing is tracked for paid software. The versions, vendor, and functions are all tracked as well. The administration staff has access for historical data and audit information.

The organization has change control procedures in place. There is a two-fork approach implemented at the organization in regard to change control, Operational Team changed and R&D changes. Policies require documentation of all changes, require approval for all changes, and require communication for all changes.

The organization ensures that platform components are not vulnerable to injection flaws, buffer overflow, cryptographic storage, insecure communications, improper error handling, and "High" vulnerabilities. All commit changes are tracked in SVP and Upsource. Code reviews are tracked and documented in SVN. The OWASP Guide, SANS CWE Top 25, and CERT Secure Coding are used by OutSystems. Code review by an additional developer and documentation of the review is required before deployment.

Subversion is used for source code control, and Active Directory is the permissions source for SVN. IssueManager is used for tracking changes. Clients are provided with separate environments for the development and production of their applications. For the product provided by the organization, a continuous improvement model is used where changes are submitted to the staging environment and then pushed to production once tested and approved by production engineering staff. Production and staging are separated by AWS groups, providing limited network connectivity and limiting user access. The organization maintains clear delineations between the staff responsible for each stage of application delivery. There are several teams responsible for the initial development and delivery of the OutSystems' platform and tools for self-service as provided to the organization's customers. There is a team responsible for testing and validation, and a Release Team that is separate from the Development Team that publishes changes. Additionally, the Support Team is responsible for the administration of systems.

People

The organization has a typical structure in place, with executive leadership and clearly defined groups. The executive leadership for the company consists of the CEO, CFO, CMO, CCO, CPO, CRO, and three VPs that are overseen by shareholders. An Organization Chart is maintained in the Bamboo HR application, which is maintained by the HR department. The Chart is available to all employees and affiliates using the application directly. The Organization Chart is shown below.

Data

The organization has the Master Subscription Agreement in place and the Terms of Use which communicate data retention policies as they apply to customers' data. The organization secures sensitive data at any time it is to be transmitted or received via an open, public network. The organization is responsible for formal channels provided to clients, but it is possible for clients to build an insecure process by which their data is exposed. The organization provides guidance to customers to avoid this, but is not ultimately responsible for any customer-caused insecure channels. The organization's data is structured such that a single client building in an insecure channel will not provide access to other client's data.

OutSystems protects information involved in application service transactions to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication, and replay. 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. The organization continually evaluates both protocols and ciphers used to ensure data security in transmission.

Processes and Procedures

The organization has daily operational security procedures in place that relate to their internal security processes. Log monitoring and alerts are primarily monitored for in Splunk. Alerts are created by alert rules that automatically run log searches at regular intervals. If the results of the log search match particular criteria, then an alert record is created via ticket on the ticketing system. The rule can then automatically run one or more actions to proactively notify personnel of the alert or invoke another process. Different types of alert rules use different logic to perform this analysis. Upon any detection or suspicion, log review should be conducted by a Security Analyst that will act as an initial responder to a suspected security event in order to:

1. Evaluate an incoming event for security-relevance if it is, in fact, a security incident.
2. Determine the extent and criticality of a security incident.
3. Escalate to security incident manager if necessary.

Logs and alerts can be broken down into the following categories:

- Platform Monitoring
    - Aberrant geographical logins, brute force attacks, module integrity
- Server OS Logs
    - New accounts, failed user logins, brute force attempts, Windows SLOs, log gaps, CPU performance, system file changes, audit trail accesses, clock skew
- Database Logs

    - Failed user attempts, DB role changes, application password changes, all actions performed with DBA privileges, log gaps, new DB creation, schema connections, role changes for existing users, and system performance
- AWS Security Group and Firewall Logs
    - ACL violations, invalid logins, firewall changes, rogue machines, VPC operational changes
- IDS Alerts
    - CVE monitoring, DDoS attacks, unexpected traffic, pre-attack traffic indicating reconnaissance
- FIM Logs
    - Any changes to system files, access to audit trails, all actions taken by administrative accounts

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

Control Environment

Management Philosophy

Management's communication sets the tone and direction for the entire organization. Most communication from the CEO happens via email or web session. During the quarterly web session, the CEO communicates business results and goals. Additionally, other sessions by the CISO are used to communicate security-related guidance. A kickoff conference is held within each department annually, to set the tone and direction for the next year and to align everyone with the company and department goals.

The OutSystems Code of Business Conduct and Ethics sets forth the guiding principles by which the organization operates and conducts daily business with stockholders, customers, vendors, and personnel. These principles apply to all of the directors, officers, and employees of OutSystems and its subsidiaries and affiliates. The Senior Management Team of OutSystems has adopted this Code in order to promote:

- Honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest
- Full, fair, accurate, timely, and understandable disclosure in the periodic reports required to be filed by OutSystems
- Compliance with applicable governmental rules and regulations
- Accountability for adherence to this Code

Employees receive and review the policies and Code as part of the on-boarding process. This documentation is included in the overall Employee Handbook type information.

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

The organization's security, availability, processing integrity, confidentiality, and privacy requirements are managed using a combination of documented policies and procedures, management oversight, and network systems and hardware. These management practices are implemented in all areas of the control environment to protect systems, data, and personnel and to ensure compliance with industry best practices and standards.

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

Management has methods in place for creating, approving, and maintaining the organization's policies. CISO has the responsibility for coordinating the ISMS and policy updates. Policies are reviewed as necessary or on an annual basis. Policies clearly communicate responsibility for updating and update criteria, including time and system/process changes.

Personnel Security

The organization has a collection of documents in place that details the content typically included in an Employee Handbook, and these policies are made available to employees via the Intranet or email. The policies address the following topics:

- Employee Conduct
- Expectations
- Requirements related to employment
- Display Measures

Employees are required to sign an acknowledgement of the Code of Conduct and Business Ethics, the Information Security Policy, the Data Privacy Policy, and the Acceptable Use Policy at the time of hire.

Physical Security and Environmental Controls

The organization has physical security controls in place for protecting secure areas. OutSystems has a Physical Security Policy in place that states 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 at all times. The OutSystems corporate office is located in a eight-story office building, where the ground level is retail space and then floors one through seven are office space. The building is basically a square with an elevator shaft in each of the four corners. Most of the building is only four stories tall. Floors five, six, and seven are a tower on the SE corner of the building. Only elevator four goes to these floors. OutSystems occupies all of floors one, two, and most of three in the main building as well as floors five and seven in the tower. Those floors are strictly for meetings/training and a breakroom. There are two single-office tenants on the third floor that have no access to OutSystems' office. OutSystems currently has no office space on the fourth floor in the main building or the sixth floor in the tower.

Street level access is only through one of the four corners which consists of a security guard at the security desk, and the elevator. The doors are unlocked during the business hours of 8AM - 7PM. Non-employees must give the security guard a photo ID and the security guard keeps a visitor log. Visitor logs are also maintained at the reception desk, and are retained indefinitely. The logs record visitor’s name, their onsite contact, and date in/out.

After business hours, the doors are locked and can only be opened by security guards; there is no electronic access after-hours. Employees must ring a buzzer and identify themselves. The security guard checks against the approved access list before allowing entry to the building. The list is updated weekly.

Elevators open to a secured landing on each floor. All access points are secured by locked doors equipped with card/biometric readers to limit access to only authorized onsite personnel. Visitors must be escorted at all times since the visitor cards have no access capabilities.

All stairwells are equipped with card readers so that access from the stairs requires either a card swipe or a biometric scan. The stairwells only open outwards at ground level using a crashbar to release the lock. There are no handles or card readers or key locks on the exterior of the door.

They can be used as an exit point only. The server room requires an additional level of access which is granted to authorized IT personnel only as required for job responsibilities.

The security video camera system is operated by building security. There are interior and exterior security cameras at each of the four access points in each of the four corners of the building. There are additional cameras placed around the facility and the live feeds are displayed on monitors in the Security Operations Center. The surveillance data from the video cameras is retained for 30 days and can only by reviewed by court order or with a subpoena. The retention period and viewing requirements are in accordance with Portuguese law.

OutSystems has multiple security cameras of their own inside the server room. The cameras record all access to the server room and all activity inside the server room. The data from the security cameras is retained for 30 days and can only be viewed by court order or with a subpoena. The retention period and viewing requirements are in accordance with Portuguese law.

OutSystems has equipment and/or media destruction policies and procedures in place. There is very little hard copy of any kind printed in the OutSystems corporate office facility. The office is equipped with shredders for secure destruction of any hard copy media. There is no destruction of computer equipment. Most equipment is leased and is wiped by OutSystems' IT Personnel prior to return upon lease expiration.

The organization has controls in place to protect against external and environmental hazards. The corporate office has protections in place against fire and power outages, as well as environmental monitoring for technical rooms. The utility power supply is steady and reliable due the office's proximity to Portugal's national emergency broadcast and response facility. The server room in equipped with two redundantly configured UPS battery backups, and two dedicated A/C units. The facility has smoke detectors, fire alarms, and a fire suppression system that consists of manual fire extinguishers and manual fire hoses in place.

Change Management

The organization has configuration standards implemented and maintained within the Systems Hardening Policy. Quarterly meetings are held with representatives from all relevant teams where standards are reviewed, and policies and procedures are updated as necessary. The OutSystems Support Team is responsible for the technical review of the Systems Hardening Policy and associated documentation in conjunction with the Security Office Team. This review is done quarterly or as needed. Server hardening standards are documented and in place. Hardening is based on AWS standards, and CIS hardening guidelines for Operating Systems. AWS Trusted Advisor is utilized for security review.
Personnel with responsibilities for system configurations stay knowledgeable of appropriate ways to securely configure the organization's systems. The organization's technical personnel are frequent attendees and speakers at technical conferences, and use Slack with connections to multiple third-party and vendor-specific security-related forums to stay knowledgeable of current information.

OutSystems has a Change Management Policy in place that makes allowances for emergency changes, and provides a clear structure to be followed in those cases. Changes are handled in one of two categories based on the systems affected, and three different types based on the nature of the change. Releases are tested via a continuous integration system and all code must pass the CIS testing. Changes follow policy from proposal, to manager validation, through scheduling into implementation and are followed up with a lesson learned. Status is tracked via a Zendesk ticket and tracked through completion. Ticket tracks risk, schedule, and approvals.

The organization implements administrative and logical controls associated with the configuration and tracking/documentation of configurations of the AWS Security Groups and Virtual Private Clouds. Firewall rules are maintained via Security Groups in the AWS System Center. Security Groups are managed via AWS Web Console. Any change to the Security Groups require the following:

- Change procedure with proper approval.
- Each change must be reflected in the diagram flows and Security Groups documentation and/or Firewall Rules baselines.
- Notifying the Security Operations team about the change which is going to happen in order for them to classify the change alert as a non-security incident.

System Monitoring

The organization implements administrative and logical controls associated with the monitoring and logging of networks. Splunk is utilized for log aggregation and storage, system and access monitoring, and system and network monitoring. AWS CloudTrail supplements Splunk agents to monitor API calls, which are also routed to Splunk for retention or action. Endpoints are monitored via TrendMicro Deep Security Manager and TrendMicro logs are also sent to Splunk.

The organization implements administrative controls associated with the monitoring of system capacity and planning for future capacity. The SIEM collects system performance information via the heavy Forwarders. 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. All logs are concatenated via SIEM and multiple dashboards are available to review CPU, memory, and disk usage.

All data is concatenated in Splunk which generates and displays dashboard and reports, and also generates alerts as needed. TrendMicro is installed with anti-malware, firewall, intrusion prevention, and intrusion monitoring modules active. Security Operators make use of Zendesk (ticket tracking) as an aggregator of alerts and track investigations and responses in tickets.

Problem Management

OutSystems has established a Security Incident Management Policy that clearly defines the roles and responsibilities among the operational and security teams to produce an effective and timely response for any security event or incident that might occur. All of the operational teams are requested to develop security incident response plans for their areas of work that are aligned with the following phases of security incident handling:

- Preparation
- Detection and Analysis

- Containment and Eradication
- Recovery and Stabilization
- Close and Post-Mortem

An Incident Response Team is staffed and defines to provide assistance to end-customers with Triage, Incident Coordination, and Incident Resolution should the security incident be customer-specific as a result of customer processes or code.

OutSystems Security Operations, Digital, Support, and CSIRT teams maintain records of incident response activities. All Security Incidents Records are put on a form according to the Security Incident Management Policy and procedures implemented in each practice. All events and alerts from components are centralized in a common ticketing system, managed by the operational teams and accessible to the CSIRT team for coordination of major security incidents. All the security incidents initiated by the customer are held in their support portal cases, only accessible to them and their predesignated company peers.

All members of the Incident Response Team must participate in training on the Incident Response Plan in order to ensure that staff is fully aware of the implications of disaster situations on business continuity. 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, and/or maintaining security related certifications.

Customers are provided a process for informing the organization about security breaches and for submitting complaints. Customers sign a Master Subscription Agreement which provides information on the organization's responsibilities to respond, and the method for reporting security incidents and issues. Additionally, the organization has established a secure communication channel, so customers can report issues, vulnerabilities, or suspicious events.

Data Backup and Recovery

The organization has policies and procedures in place for creating backups and restoring the organization's customer data, as well as for the environment failover to another availability zone. The infrastructure is in multiple availability-zones in AWS with warm standby servers should the primary environment suffer failure. The organization's customer data is backed up for 15 days and can be recovered from backup at customer request.

OutSystems has established a Business Continuity Management System (BCMS) aligned with ISO 22301. This management system has been certified by independent auditors. The scope of the BCMS is the Engineering Operations area, which consists of three areas:

- Support Concierge
- Cloud Service Support
- OutSystems Business Continuity Policy and Technical Support

The OutSystems Business Continuity Plan consists of two major parts: Incident Response Plan which defines direct response to the occurrence of various types of incidents, and recovery plans for individual activities. These are prepared separately for each activity.

Each business area plan is developed and maintained by the business area owners and define how to maintain or restore operations and ensure availability of information at the required level and in the required timescales following an interruption to, or failure of, critical business processes. These plans are managed in the BCMS documentation and each of the Business Continuity Plans is tested at least annually to ensure proper training within the operational teams with different kinds of scenarios.

Plans are updated at least yearly for the ISO 22301/2012 audit. Additionally, CISO is required to update/review them at least annually. Testing must be conducted once a year, and the CISO is responsible for writing an exercise and testing the processes, procedures, and controls. Plans must be updated more frequently than annually when there is a change to processes or solutions.

System Account Management

The organization implements administrative and logical controls associated with the policies on access rights and privileges granted to user IDs. The Logical Access Control Policy references principals of "least privilege" and defines access granting as role-related. Policy specifically forbids the creation group, generic, or shared accounts. All users have unique IDs for all systems. BambooHR tracks the user account creation and automatically creates Active Directory and Google accounts 48 hours before start date, and IT services manually assigns any elevated access. The organization's clients are given authorization codes as part of customer creation and set their own passwords.

The organization uses AWS Directory Service to manage end user credentials. First-time user creation emails a temporary password and forces password change. Temporary passwords are not documented anywhere. AWS password settings including complexity, failure timeout, and multi-factor authentication (MFA) requirements. MFA is provided via RADIUS (FreeRadius) service integrated with the Google Authenticator. A 'jumpbox' configuration is used for administrative access and AWS workspaces. Thorough logging is relayed to the Splunk server for all authentication attempts, both successful and failed.

Clients are provided a process for registering and de-registering for online access to the organization’s services. Users are required to self-register with a provided license number. Passwords are not manually set at any point in the process either by client for sub-users or by the organization's support or administrative staff. Client's processes around account creation and removal for their subsequent users/customers are not under the organization's control. De-registration is a process that takes place manually upon client request (via support ticket) or when licenses expire.

The Logical Access Policy requires that access to OutSystems’ information systems is immediately revoked for any terminated/separated employees after communication from PeopleOps (HR) or by the employee. For end-client personnel changes, the organization is reliant upon the client to create a change ticket. For the organization's employees and contractors, accounts are terminated immediately upon knowledge of the employee separation. HR notifies IT via ticket creation from BambooHR which generates an email to appropriate technical teams.

Risk Assessment Process

The organization has an annual Risk Assessment process in place that follows ISO 27001 and ISO 22301 international standards and considers Risk Identification, Risk Profiling, and Risk Treatment or Acceptance. The decision to mitigate or accept is driven by their risk appetite of 20%. The assessment matrix is updated at least annually by the Security Office and the business owners.

The organization's 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 (Risk = Impact x Likelihood x Asset value). The organization's Security Team works with each business unit to ensure the comprehensiveness of the risk assessment.

Information and Communication Systems

The organization communicates any requirements for proper use of the system and/or the information it produces to internal and external users. Internal employees and contractors acknowledge and are expected to adhere to proper security procedures, while clients are guided as to what security best practices and features are available to them. Client-facing documentation is available at all times to the clients and includes links to support as well as documentation status (in-progress, final).

The organization has an Information Security Policy in place. The CISO has overall responsibility and ownership of the maintenance and distribution of the Policy to all employees and necessary third parties authorized to use OutSystems' assets. The Policy is required to be reviewed annually or when needed, to be compliant with relevant legal and regulatory requirements, and to be approved by the CISO.

Security responsibilities within the organization are defined in specific policies rather than as a whole by position. The Business Continuity Policy has language detailing the responsibilities of the CISO, the Business Continuity Manager, and the Business Continuity Management Team, while the Change Management Policy documents responsibilities of the R&D Platform Architects, the Engineering Operations Manager, and Cloud Support managers. Acceptable Use Policy and Information Security Policies contain the processes and policies that must be followed by all employees in regard to their relationship with information security.

The organization has procedures in place for practicing due diligence prior to sharing information with third-parties. The Supplier Security Policy requires that service providers implement a comprehensive Information Security Policy that protect OutSystems' assets, and specifies that service providers are evaluated annually or every six months to check for consistency with compliance requirements. OutSystems collects SOC2 reports from technological suppliers on an annual basis and uses a security questionnaire to determine appropriate security level of suppliers. OutSystems specifically enforces the use of Non-Disclosure Agreements in the course of its operations with third-parties, whether they are providers or customers. Documentation is tracked in DocuSign which ensures availability.

All logs from critical servers are sent to Splunk which is configured with alerts for scanning, unauthorized access, and unauthorized changes in addition to standard environmental monitoring (disk space, CPU utilization). Antivirus and anti-malware is monitored by TrendMicro. Additionally, AWS CloudTrail is used to facilitate the auditing of access as needed.

Monitoring Controls

Management performs monitoring activities to ensure operational quality and control. Weekly reports of non-satisfied clients are reviewed by Operation's management. Additionally, the various monitors for system health, IDS/IPS, uptime monitors, etc. are available to management on a continuous basis. Executive management defines key objectives and communicates these objectives to departments to implement. The Security Steering meeting is held monthly.

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

Criteria Common to All Security, Availability, Processing Integrity, Confidentiality, and Privacy 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, Confidentiality, and Privacy.		
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, Confidentiality, and Privacy 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, Confidentiality, and Privacy.		

Criteria Common to All Security, Availability, Processing Integrity, Confidentiality, and Privacy 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, Confidentiality, and Privacy 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, Confidentiality, and Privacy 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, Confidentiality, and Privacy 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, Confidentiality, and Privacy are communicated to those users in a timely manner.		

Criteria Common to All Security, Availability, Processing Integrity, Confidentiality, and Privacy 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, Confidentiality, and Privacy 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, Confidentiality, and Privacy 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, Confidentiality, and Privacy 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, Confidentiality, and Privacy 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, Confidentiality, and Privacy 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, Confidentiality, and Privacy 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, Confidentiality, and Privacy.		
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, Confidentiality, and Privacy 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, Confidentiality, and Privacy 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, Confidentiality, and Privacy 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, Confidentiality, and Privacy Principles			
7.0 Common Criteria Related to Change Management			
Ctrl #	**Control Activity**	**Testing of Operating Effectiveness**	**Test Results**
7.1	Security, Availability, Processing Integrity, Confidentiality, and Privacy 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, Confidentiality, and Privacy.		
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, Confidentiality, and Privacy 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.		