Projector.IS Inc.
Type 2 SOC 3
2019

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

August 15, 2019 To November 15, 2019

Table of Contents

SECTION 1

ASSERTION OF PROJECTOR.IS INC. MANAGEMENT

ASSERTION OF PROJECTOR.IS INC. MANAGEMENT

December 15, 2019

We are responsible for designing, implementing, operating, and maintaining effective controls within Projector.IS Inc.'s ('Projector.IS' or 'the Company') SaaS System throughout the period August 15, 2019 to November 15, 2019, to provide reasonable assurance that Projector.IS' service commitments and system requirements relevant to Security and Confidentiality applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in "Projector.IS Inc.'s Description of Its SaaS System Throughout the Period August 15, 2019 to November 15, 2019" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period August 15, 2019 to November 15, 2019, to provide reasonable assurance that Projector.IS' service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity and Privacy* (AICPA, *Trust Services Criteria*). Projector.IS' objectives for the system in applying applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "Projector.IS Inc.'s Description of Its SaaS System Throughout the Period August 15, 2019 to November 15, 2019".

Projector.IS uses Amazon Web Services ('AWS') to provide data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Projector.IS, to achieve Projector.IS' service commitments and system requirements based on the applicable trust services criteria. The description presents Projector.IS' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Projector.IS' controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Projector.IS' service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Projector.IS' controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period August 15, 2019 to November 15, 2019 to provide reasonable assurance that Projector.IS' service commitments and system requirements were achieved based on the applicable trust services criteria.

Ben Lilienthal

Ben Lilienthal
CEO
Projector.IS Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Projector.IS Inc.

Scope

We have examined Projector.IS Inc.'s accompanying description of SaaS system titled "Projector.IS Inc.'s Description of Its SaaS System Throughout The Period August 15, 2019 To November 15, 2019" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period August 15, 2019 to November 15, 2019, to provide reasonable assurance that Projector.IS' service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Projector.IS uses AWS to provide data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Projector.IS, to achieve Projector.IS' service commitments and system requirements based on the applicable trust services criteria. The description presents Projector.IS' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Projector.IS' controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Projector.IS, to achieve Projector.IS' service commitments and system requirements based on the applicable trust services criteria. The description presents Projector.IS' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Projector.IS' controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Projector.IS is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Projector.IS' service commitments and system requirements were achieved. Projector.IS has provided the accompanying assertion titled "Assertion of Projector.IS Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Projector.IS is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Projector.IS' SaaS System were suitably designed and operating effectively throughout the period August 15, 2019 to November 15, 2019, to provide reasonable assurance that Projector.IS' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

The SOC logo for Service Organizations on Projector.IS' website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Projector.IS, user entities of Projector.IS' SaaS system during some or all of the period August 15, 2019 to November 15, 2019, business partners of Projector.IS subject to risks arising from interactions with the SaaS system, and those who have sufficient knowledge and understanding of the complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

December 15, 2019
Tampa, Florida

SECTION 3

PROJECTOR.IS INC.'S DESCRIPTON OF ITS SAAS SYSTEM THROUGHOUT THE PERIOD AUGUST 15, 2019 TO NOVEMBER 15, 2019

OVERVIEW OF OPERATIONS

Company Background

Projector.IS, also known as ScreenMeet, was founded in January 2016 with the objective of building the first cloud-based screen sharing platform. Their initial product in the market was a simple screen sharing solution for online meetings and presentations. Projector.IS pivoted from a meeting product into the remote support business while continuing to leverage the cloud-first architecture and platform that was internally developed. Projector.IS has achieved success in the remote support market due to the compelling and unique nature of their product offering. The company is based in San Francisco, California.

Projector.IS has certified Apps with third-party CRM vendors including Zendesk, Salesforce, ServiceNow and Microsoft Dynamics (Q3, '18).

Vertical served by Projector.IS include high tech hardware (PC/smartphone), Software (SaaS/Web/Mobile), Hospitality, Pharma, E-commerce and others.

Description of Services Provided

Projector.IS develops co-browsing and remote support that is cloud-native and web-based. Their solution, known as ScreenMeet, directly integrates into leading web-based 3rd party CRM and help desk solutions like Salesforce, ServiceNow, Zendesk and Microsoft Dynamics. With ScreenMeet, support agents can, from a web browser, see and takeover any device and any application in real-time over the Internet with the end-user's consent. The simple and powerful nature of the product means that it saves customers time and reducing their customers' frustration when resolving technical issues. This results in lower operating costs and increased customer satisfaction.

Principal Service Commitments and System Requirements

Projector.IS designs its processes and procedures related to screenmeet.com to meet its objectives for its remote support services. Those objectives are based on the service commitments that Projector.IS makes to user entities, the laws and regulations that govern the provision of remote support services, and the financial, operational, and compliance requirements that Projector.IS has established for the services. The remote support services of Projector.IS are subject to the security and privacy requirements of relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which Projector.IS operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

Security principles within the fundamental designs of screenmeet.com that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.

Use of encryption technologies to protect customer data both at rest and in transit.

Projector.IS establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Projector.IS' system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of screenmeet.com.

Components of the System

Infrastructure

Primary infrastructure used to provide Projector.IS' SaaS system includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
AWS	Database servers	Cloud Hosting Platform
Google Cloud	Intranet	Cloud Hosting Platform

Software

Primary software used to provide Projector.IS' SaaS system includes the following:

Primary Software	
Software	**Purpose**
Jira	Issue Tracking
Bitbucket	Version Control Repository
Confluence	Document control and training
Google	E-mail
Slack	Internal Communication
Intercom	External communication and support tickets
AWS	Cloud Hosting Platform
Stripe	Payment Processor

People

The Projector.IS staff provides support for the above services in each of the following functional areas:

- Executive management - provides general oversight and strategic planning of operations
- Development team - responsible for delivering a high availability SaaS platform that fully complies with the functional specifications
- Quality assurance team - verifies that the system complies with the functional specification through functional testing procedures
- System administrators and DevOps - responsible for effective provisioning, installation/configuration, operation and maintenance of systems hardware and software relevant to the system
- Customer Support - serves customers by providing product and service information that involves resolving product and service issues
- Audit and Compliance - performs regularly scheduled audits relative to defined standards provides continuous improvement feedback and assesses legal and regulatory requirements

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. Customer data is captured which is utilized by Projector.IS in delivering its co-browsing and remote support system. Such data includes, but is not limited to, the following:

- Alert notifications and monitoring reports generated from the commercial monitoring applications
- Alert notifications received from automated backup systems
- Vulnerability or security alerts received from various sources including security subscriptions, scanning tools, IDS alerts, or automated patching systems
- Incident reports documented via the ticketing systems

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All employees are expected to adhere to the Projector.IS policies and procedures that define how services should be delivered. These are available by any Projector.IS employee or contractor.

Physical Security

The in-scope service and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls for the in-scope service.

Logical Access

Projector.IS uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resource. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists for those systems.

Computer Operations - Backups

Customer data is backed up and monitored by Projetor.IS' CTO for completion and exceptions. In the event of an exception, technical personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job.

Backup infrastructure is physically removed from the Projector.IS' offices. It is part of the cloud-hosted deployments and Projector.IS does not have physical access to it.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Projector.IS monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches SLAs. Projector.IS evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- AWS Data Center
- Google Cloud Data Center

Projector.IS has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operation system patches. Projector.IS staff validate that all patches have been installed and if applicable that reboots have been completed.

Change Control

Projector.IS, Inc's system change policy ensure that changes to systems and applications are properly planned, evaluated, reviewed, approved, communicated, implemented, documented, and reviewed, thereby ensuring the greatest probability of success. Where changes are not successful, this document provides mechanisms for conducting post-implementation review such that future mistakes and errors can be prevented.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

Load balancers and Amazon security groups are in place to restrict unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. GuardDuty Intrusion Detection System (IDS) monitors and alerts on suspicious traffic heading into the production environment. Network Address Translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the cloud services to help ensure that there is no single point of failure among production systems. In the event that a primary availability zone fails, the redundant systems can be stood up in additional availability zones.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Illumant. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by a qualified internal resource on a quarterly basis in accordance with the Information Security policy. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the Projector.IS production environment are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system through from the Internet through secure connections. Employees are authenticated through the use of a token-based two-factor authentication system.

Boundaries of the System

The scope of this report includes Projector.IS' SaaS System performed in the San Francisco, California facilities.

This report does not include the data center hosting services provided by AWS at the multi-location facilities.

Changes to the System Since the Last Review Period

In the past 12 months, Projector.IS moved to a new office at 50 Fremont Street, San Francisco, CA 94105 to for additional workspace. In addition. Projector.IS has deployed its software product in new regions in AWS to improve user experience and reduce latency. However, these changes did not impact the scope of the audit during the review period.

Incidents Since the Last Review Period

No significant incidents have occurred to the services provided to user entities since the end of the last review period.

Criteria Not Applicable to the System

All Common Criteria/Security and Confidentiality criterion was applicable to the Projector.IS SaaS system.

Subservice Organizations

This report does not include the data center hosting services provided by AWS at the multi-location facilities.

Subservice Description of Services

AWS provides data center hosting services, which includes implementing physical security controls to protect the housed in-scope systems. Controls include, but are not limited to, visitor sign-ins, required use of badges for authorized personnel, and monitoring and logging of the physical access to the facilities.

Complementary Subservice Organization Controls

Projector.IS' services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Projector.IS' services to be solely achieved by Projector.IS control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Projector.IS.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

Projector.IS management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as SLAs. In addition, Projector.IS performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

Projector.IS' services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Projector.IS' services to be solely achieved by Projector.IS control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Projector.IS'.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Projector.IS.
2. User entities are responsible for notifying Projector.IS of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Projector.IS services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Projector.IS services.
6. User entities are responsible for providing Projector.IS with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Projector.IS of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.