transifex

System and Organization Controls (SOC) 2 Type I
Report on Management's Description of its

Translation & Localization Management Platform

And the Suitability of Design of Controls Relevant to the Trust Services Criteria for Security, Availability, and Confidentiality

As of June 1, 2022

Together with
Independent Service Auditors' Report

Table of Contents

I. Independent Service Auditors’ Report

SENSIBA SAN FILIPPO LLP

CERTIFIED PUBLIC ACCOUNTANTS AND BUSINESS ADVISORS

Independent Service Auditors’ Report

To the Management of Transifex Opco LLC (Transifex)

Scope

We have examined Transifex‘s accompanying description of its Translation & Localization Management Platform titled “Description of Transifex's Translation & Localization Management Platform” (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 of controls stated in the description as of June 1, 2022, to provide reasonable assurance that Transifex’s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization’s Responsibilities

Transifex 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 Transifex‘s service commitments and system requirements were achieved. Transifex has provided the accompanying assertion titled “Assertion of Transifex Management” (assertion) about the description and the suitability of the design of controls stated therein. Transifex 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 Auditors’ Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design 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 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 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.
- 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.
- Evaluating the overall presentation of the description.

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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 report users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design 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.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects,

a. The description presents Transifex‘s Translation & Localization Management Platform that was designed and implemented as of June 1, 2022, in accordance with the description criteria.
b. The controls stated in the description were suitably designed as of June 1, 2022, to provide reasonable assurance that Transifex service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date.

Restricted Use

This report is intended solely for the information and use of Transifex, user entities of Transifex's Translation & Localization Management Platform as of June 1, 2022, business partners of Transifex subject to risks arising from interactions with the Translation & Localization Management Platform, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

Sensiba San Filippo LLP

San Jose, California
June 30, 2022

II. Assertion of Transifex Management

Assertion of Transifex Management

We have prepared the accompanying description of Transifex's Translation & Localization Management Platform system titled *"Description of Transifex's Translation & Localization Management Platform*" as of June 1, 2022, (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). The description is intended to provide report users with information about the Translation & Localization Management Platform system that may be useful when assessing the risks arising from interactions with Transifex's system, particularly information about system controls that Transifex has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, 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*).

We confirm, to the best of our knowledge and belief, that:

a. The description presents Transifex's Translation & Localization Management Platform system that was designed and implemented as of June 1, 2022, in accordance with the description criteria.

b. The controls stated in the description were suitably designed as of June 1, 2022, to provide reasonable assurance that Transifex's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date.

Signed by Transifex Management

June 30, 2022

III. Description of Transifex's Translation & Localization Management Platform

Description of Transifex's Translation & Localization Management Platform

Company Background

Transifex was founded in 2009, with the mission to help companies - from Startups to the Enterprise - go global. With the Transifex SaaS-based Translation and Localization Platform, organizations can easily translate digital content such as websites, mobile apps, games, video, help centers, subtitles, and more on a continuous basis.

Transifex is a US-based company, with employees working remotely all around the globe, including Greece, Mexico, and UK.

Services Provided

Transifex provides a Software as a Service (SaaS) localization platform which allows users to:

1. Create projects and upload their localizable content into the platform, either through the Web UI, API, command line client, and/or integrations.
2. Setup teams to manage the localization process and use the Transifex tools (editor, translation memory, glossary etc.) to facilitate and monitor the localization progress.
3. Download content into the user's systems to be used in production as soon as the content is translated into the selected target languages.

The service is accessible to the customer in a SaaS model, within a multi-tenant, cloud-based environment. Users can sign-up for an account in Transifex and create a new organization or be invited to existing organizations and be assigned appropriate permissions.

Principal Service Commitments and System Requirements

Transifex designs its processes and procedures related to its platform to meet its objectives for its services. Those objectives are based on the service commitments that Transifex makes to user entities, the laws and regulations that govern the provision of Transifex services, and the financial, operational, and compliance requirements that Transifex has established for the services. The localization services of Transifex are subject to the security and privacy requirements of state and local privacy security laws and regulations in the jurisdictions in which Transifex 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 the Transifex platform 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.

Transifex establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Transifex’s 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 the Transifex platform.

Components of the System

Infrastructure

Primary infrastructure used to provide Transifex's system includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
AWS	Various Services, including VPC, IAM, Lambda Function, Load Balancer,	Transifex’s microservices architecture is hosted on AWS. Various AWS networking services are used to ensure user inbound requests are securely managed and routed to the correct infrastructure
AWS	Elastic Kubernetes Service, EC2, KMS, S3, EBS, RDS, ElasticCache, OpenSearch	Transifex uses AWS VMs to execute customer block requests. Each block is a Docker container which is loaded and executed in response to schedule or triggered runs. Container’s data access is limited to their tenant data

Software

Primary software used to provide Transifex's system includes the following:

Primary Software		
Software	Operating System	Purpose
AWS CloudWatch, AWS GuardDuty, Prometheus	AWS	Schedules and routes alerts to operations personnel
Fluentbit	AWS	Log collection and aggregation
AWS IAM	AWS	Provides authentication and authorization for the platform
NewRelic	NewRelic	Monitoring application used to provide monitoring, alter, and notification services for Transifex platform
Github	Github	Source control and software development
JIRA	JIRA	Project management
PagerDuty	PagerDuty	Schedules and routes alerts to operations personnel
Google Workspace	Google Workspace	Provides authentication and authorization for the platform

People

Transifex has a staff of approximately 50 employees organized in the following functional areas:

- Corporate. Executives, senior operations staff, and company administrative support staff, such as legal, compliance, internal audit, training, contracting, accounting, finance and people operations. These individuals use the TMS primarily as a tool to measure performance at an overall corporate level. This includes reporting done for internal metrics as well as for Transifex’s user entities.
- Demand Generation and Customer Success.
- Product and Engineering: software systems development and application support, are in charge of developing and maintaining the application lifetime.

Data

Data, as defined by Transifex, constitutes the following:

- Customer Input Data

- Customer Output Data
- Platform data
- Operational data

Customer Input Data: Data used by the Transifex platform to drive localization process. Input data can be uploaded directly by a customer (by using files), by connecting Transifex with an Operational system using data-connectors (for example from Zendesk integration), or by using the Transifex API or CLI tools.

Customer Output Data: Data generated by Transifex, containing translated phrases into multiple languages, based on input data. Customers can access this data on the Transifex platform, export it to files, retrieve them through the Transifex API or CLI tools.

Platform Data: Data and meta-data used by the Transifex platform for ongoing operations of the software and service. For example, list of users in Transifex organizations, translation teams or user permissions.

Operational Data: Telemetry and log data produced by the Transifex platform. For example, an error log or performance KPIs.

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 teams are expected to adhere to the Transifex policies and procedures that define how services should be delivered. These are located on the Company's "Drata" platform and can be accessed by any Transifex team member.

Physical Security

All data is hosted by Amazon Web Services (AWS). AWS data centers do not allow Transifex employees physical access.

Logical Access

Transifex uses role-based security architecture using Google Workspace and AWS IAM and requires users of the system to be identified and authenticated prior to the use of any system resources. 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. In the event incompatible responsibilities cannot be segregated, Transifex implements monitoring of one or more of the responsibilities. Monitoring must be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role.

Employees and approved vendor personnel sign on to cloud resources using Google Workspace for Single Sign-On (SSO). Users are also required to separately sign on to any systems or applications that do not implement Google SSO using passwords that conform to Transifex security policies.

Employees accessing cloud resources are required to enable token-based (OTP) multi-factor authentication as supported by each service provider. All cloud-based services are accessed through SSL-secured connections.

Two days prior to a new employee's start date, their manager creates a list of employee access to be granted. Access rules have been pre-defined based on the defined roles.

On an annual basis, access rules for each role are reviewed by Transifex's operations team. As part of this process, the CTO/Devops reviews access by privileged roles and requests modifications based on this review.

Computer Operations – Backups

Customer data is backed up by Transifex's operations team. In the event of an exception, operations 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 maintained in AWS, with physical access restricted according to applicable AWS policies. All backups are encrypted using KMS-managed encryption keys, with access restricted to key personnel via AWS IAM permissions.

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.

Transifex monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. Transifex 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:

- CPU & Memory Usage
- Disk storage
- Network bandwidth

Transifex has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and Transifex system owners review proposed operating system patches to determine whether the patches are applied. Customers and Transifex systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Transifex staff validate that all patches have been installed and if applicable that reboots have been completed.

Change Control

Transifex maintains documented Systems Development Life Cycle (SDLC) policies and procedures in "Drata" Platform to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

Jira is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. 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.

Github 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.

Transifex has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and Transifex system owners review proposed operating system patches to determine whether the patches are applied. Customers and Transifex systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Transifex staff validate that all patches have been installed and if applicable that reboots have been completed.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. 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 data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Vulnerability scanning is performed by AWS Inspector on a daily basis in accordance with Transifex policy. AWS Inspector uses industry standard scanning technologies and a formal methodology specified by Transifex. Falco is used for continuous risk and threat detection across Kubernetes and containers. AWS GuardDuty continuously monitors AWS accounts and workloads for malicious activity and delivers detailed security findings. 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 Transifex system 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 from the Internet through the use of leading IAP technology. Employees are authenticated through the use of a token-based two-factor authentication system.

Boundaries of the System

The scope of this report includes the Transifex platform. This report does not include the data center hosting services provided by AWS.

The applicable trust services criteria and the related controls

Common Criteria (Security)
Security refers to the protection of information during its collection or creation, use, processing, transmission, and storage and systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability
Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality
Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Transifex’s control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Transifex’s ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management’s actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

Transifex management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.
- Ongoing managerial reviews and periodic performance reviews are conducted across the organization.
- Retrospectives and root-cause analysis are implemented as part of the software development practices.

Management's Philosophy and Operating Style

Transifex's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole.
- Industry reports and market research is shared with executive management and leadership on ongoing basis.

Organizational Structure and Assignment of Authority and Responsibility

Transifex's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Transifex's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

Transifex's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Transifex's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

Risk Assessment Process

Transifex's risk assessment process identifies and manages risks that could potentially affect Transifex ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Transifex identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by Transifex, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk – changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance – legal and regulatory changes

Transifex has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm’s internal controls. The approach is intended to align the entity’s strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Transifex attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Transifex’s app system; as well as the nature of the components of the system result in risks that the criteria will not be met. Transifex addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Transifex’s management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication is an integral component of Transifex’s internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity’s operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Transifex, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Transifex personnel via e-mail messages.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Transifex’s management performs monitoring activities to continuously assess the quality of internal control over time using Drata platform. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Transifex's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Transifex's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Transifex's personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Criteria Not Applicable to the System

All relevant trust services criteria were applicable to Transifex's Translation & Localization Management Platform.

Subservice Organizations

Transifex Opco LLC's 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 Transifex's services to be solely achieved by Transifex‘s control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Transifex.

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.
		Closed circuit television camera (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
		Access to server locations is managed by electronic access control devices.
Availability	A1.2	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment.
		AWS maintains a formal risk management program to identify, analyze, treat and continuously monitor and report risks that affect AWS' business objectives and regulatory requirements. The program identifies risks, documents them in a register as appropriate, and reports results to leadership at least semi-annually.
		AWS has a process in place to review environmental and geo-political risks before launching a new region.
		Access to server locations is 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.
		Amazon-owned data centers are protected by fire detection and suppression systems.

Subservice Organization – AWS		
Category	Criteria	Control
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers and third-party colocation sites where Amazon maintains the UPS units.
		Amazon-owned data centers have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units (unless maintained by Amazon), and redundant power supplies. Contracts also include provisions requiring communication of incidents or events that impact Amazon assets and/or customers to AWS.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
		Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.

Subservice Organization – AWS		
Category	Criteria	Control
		AWS contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents. The AWS contingency plan is tested on at least an annual basis.
		AWS maintains a capacity planning model to assess infrastructure usage and demands at least monthly, and usually more frequently (e.g., weekly). In addition, the AWS capacity planning model supports the planning of future demands to acquire and implement additional resources based upon current resources and forecasted requirements.

Transifex 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 service level agreements. In addition, Transifex performs monitoring of the subservice organization controls, including the following procedures

- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

Complementary User Entity Controls

Transifex's 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 the SOC 2 Criteria related to Transifex's services to be solely achieved by Transifex's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Transifex's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the SOC 2 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 Transifex.

2. User entities are responsible for notifying Transifex 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 Transifex 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 Transifex services.
6. User entities are responsible for providing Transifex with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Transifex of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

IV. Description of Design of Controls and Results Thereof

Description of Design of Controls and Results Thereof

Relevant trust services criteria and Transifex related controls are an integral part of management's system description and are included in this section. Sensiba San Filippo LLP performed testing to determine if Transifex controls were suitably designed to achieve the specified criteria for the Security, Availability, and Confidentiality categories set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria)*, as of June 1, 2022.

Criteria Number	Description of Company Controls	Result
CC1.0 - Control Environment		
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.		
CC1.1.1	The entity has a documented code of conduct that includes its commitments to integrity and ethical values.	Control is suitably designed
CC1.1.2	Personnel are required to read and accept the code of conduct upon being hired.	Control is suitably designed
CC1.1.3	New employees and contractors are subjected to background and/or reference checks as a condition of their employment, as permitted by local laws.	Control is suitably designed
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
CC1.2.1	The company demonstrates a commitment to integrity and ethical values by completing an annual review of ethical management and hiring practices.	Control is suitably designed
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
CC1.3.1	The company reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
CC1.3.2	An organizational chart has been defined to appropriately document reporting lines in terms of information security.	Control is suitably designed
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
CC1.4.1	Job requirements and responsibilities are documented in job descriptions.	Control is suitably designed
CC1.4.2	New employees and contractors are subjected to background and/or reference checks as a condition of their employment, as permitted by local laws.	Control is suitably designed
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
CC1.5.1	Security awareness training is provided to all employees on an annual basis.	Control is suitably designed
CC1.5.2	Managers are required to complete performance appraisals for direct reports at least annually.	Control is suitably designed
CC2.0 - Communication and Information		
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
CC2.1.1	The company uses a SOC 2 compliance platform called Drata which objectively and continuously monitors the company's control environment and alerts management when internal control and security issues arise.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
CC2.2.1	Personnel are required to read and accept the code of conduct upon being hired.	Control is suitably designed
CC2.2.2	Personnel are required to read and accept an acceptable use agreement upon being hired.	Control is suitably designed
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.		
CC2.3.1	Privacy policies are posted on the entity's website to communicate the entity's privacy practices.	Control is suitably designed
CC2.3.2	The company maintains a Terms of Service that is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems.	Control is suitably designed
CC3.0 - Risk Assessment		
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
CC3.1.1	The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Control is suitably designed
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		
CC3.2.1	A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		
CC3.2.2	When identifying risks to include in the risk assessment, the entity considers relevant laws and regulations specific to the types of data they possess (i.e. Protected Health Information, Personally Identifiable Information, etc.).	Control is suitably designed
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
CC3.3.1	A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	Control is suitably designed
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.		
CC3.4.1	The company reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	Control is suitably designed
CC3.4.2	A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	Control is suitably designed
CC4.0 - Monitoring Activities		
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
CC4.1.1	Cloud infrastructure is monitored through AWS monitoring that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner.	Control is suitably designed
CC4.1.2	Monitoring configured to identify suspicious activity. When anomalous traffic activity is identified, the web application firewall appropriately blocks malicious traffic.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.		
CC4.2.1	The entity has incident response policies and procedures in place that includes plans for escalating to internal personnel.	Control is suitably designed
CC4.2.2	The company provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.	Control is suitably designed
CC5.0 - Control Activities		
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
CC5.1.1	As part of its annual risk assessment, management linked the identified risks to controls that have been designed and operated to address them. When the need for new controls is identified, management develops the requirements for the new controls and uses the change management process to implement them.	Control is suitably designed
CC5.1.2	The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Control is suitably designed
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.		
CC5.2.1	Vulnerability scans are performed on a quarterly basis to identify vulnerabilities and management takes action based on the results of the scan.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
CC5.3.1	IT and security policies are defined for protecting against unauthorized access that could compromise the availability, integrity, confidentiality, and privacy of information or systems. IT and security policies are reviewed by appropriate members of management on an annual basis.	Control is suitably designed
CC5.3.2	Management has approved the company's security policies, and all employees agree to these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	Control is suitably designed
CC6.0 - Logical and Physical Access Controls		
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
CC6.1.1	Access to corporate network, production machines, network devices, and support tools requires a unique ID.	Control is suitably designed
CC6.1.2	No public SSH is allowed.	Control is suitably designed
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
CC6.2.1	Prior to granting new hires access to system resources, HR must submit a completed access request form.	Control is suitably designed
CC6.2.2	A termination checklist is completed to ensure that system access, including physical access, for terminated employees has been removed within one business day.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
CC6.3.1	The company's access reviews are performed on an annual basis.	Control is suitably designed
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
CC6.4.1	The company relies on AWS physical and environmental controls, as defined and tested within AWS SOC 2 reports.	The Criterion is carved out and the responsibility of the subservice organization.
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.		
CC6.5.1	Procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.	Control is suitably designed
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
CC6.6.1	Inbound and outbound traffic to AWS is appropriately restricted.	Control is suitably designed
CC6.6.2	AWS cloud firewalls are in place to protect the company from outside threats.	Control is suitably designed
CC6.6.3	Multi-factor authentication (MFA) is required to access the AWS Management Console.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		
CC6.7.1	The company uses HTTPS to encrypt communications over the internet.	Control is suitably designed
CC6.7.2	Customer data at rest is encrypted.	Control is suitably designed
CC6.7.3	Full-disk encryption is implemented for all workstations and laptops.	Control is suitably designed
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
CC6.8.1	Antivirus software is installed on workstations to protect the network against malware.	Control is suitably designed
CC7.0 - System Operations		
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		
CC7.1.1	Vulnerability scans are performed on a quarterly basis to identify vulnerabilities and management takes action based on the results of the scan.	Control is suitably designed
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
CC7.2.1	Version control software is used to manage source code, track changes to source code, and roll back changes following an unsuccessful implementation.	Control is suitably designed
CC7.2.2	Access to the cloud source code version control system is restricted to appropriate personnel.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		
CC7.3.1	The incident response team follows defined incident response procedures for resolving and escalating reported security issues.	Control is suitably designed
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
CC7.4.1	The incident response team follows defined incident response procedures for resolving and escalating reported security issues.	Control is suitably designed
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.		
CC7.5.1	Business and system recovery plans are documented, which provide roles and responsibilities and detailed procedures for recovery of systems.	Control is suitably designed
CC8.0 - Change Management		
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		
CC8.1.1	A software development life cycle policy is defined to ensure that appropriate controls are in place over the acquisition, development, and maintenance of technology and its infrastructure.	Control is suitably designed
CC8.1.2	Version control software is used to manage source code, track changes to source code, and roll back changes following an unsuccessful implementation.	Control is suitably designed
CC8.1.3	Access to the cloud source code version control system is restricted to appropriate personnel.	Control is suitably designed
CC8.1.4	Code changes to the company are tested prior to implementation.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		
CC8.1.5	The company's releases are approved by appropriate personnel prior to the release being implemented in production.	Control is suitably designed
CC9.0 - Risk Mitigation		
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
CC9.1.1	The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Control is suitably designed
CC9.1.2	A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	Control is suitably designed
CC9.1.3	The company has created a business continuity plan to define the criteria for continuing business operations for the organization in the event of a disruption.	Control is suitably designed
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.		
CC9.2.1	The company's team collects and reviews the SOC reports of its sub-service organizations on an annual basis.	Control is suitably designed
CC9.2.2	The company has implemented a Vendor Risk Management program with a framework for managing the lifecycle of vendor relationships.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
A1.0 - Additional Criteria for Availability		
A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.		
A1.1.1	Cloud infrastructure is monitored through AWS monitoring that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner.	Control is suitably designed
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.		
A1.2.1	The company relies on AWS physical and environmental controls, as defined and tested within AWS SOC 2 reports.	The Criterion is carved out and the responsibility of the subservice organization.
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
A1.3.1	Backups are performed daily and retained in accordance with a pre-defined schedule in the Backup Policy.	Control is suitably designed
A1.3.2	The entity has documented a disaster recovery plan that is tested annually to ensure that recovery procedures are complete and accurate.	Control is suitably designed
C1.0 - Additional Criteria for Confidentiality		
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
C1.1.1	The entity establishes written policies related to retention periods for the confidential information it maintains.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
C1.1.2	The entity has established a data classification policy in order to identify the types of confidential information possessed by the entity and types of protection that are required.	Control is suitably designed
C1.2 - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
C1.2.1	Formal policies and procedures are in place to guide personnel in the disposal of any sensitive data.	Control is suitably designed