TESSIAN

Tessian Limited

Report on Controls at a Service Organization Relevant to Security, Confidentiality, and Availability

SOC 3[SM] Report

For the Period December 1, 2020 to February 28, 2021

SOC 3 is a registered service mark of the American Institute of Certified Public Accountants (AICPA)

BARR ADVISORY

Independent Service Auditor's Report

To the Management of Tessian Limited (Tessian):

Scope

We have examined Tessian's accompanying assertion titled "Assertion of Tessian Management" (assertion) that the controls within Tessian's Human Layer Security Platform (system) were effective throughout the period December 1, 2020 to February 28, 2021, to provide reasonable assurance that Tessian's service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, and availability (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

Tessian 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 Tessian's service commitments and system requirements were achieved. Tessian has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Tessian is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that controls were not effective to achieve Tessian's service commitments and system requirements based on the applicable trust services criteria; and,
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Tessian's service commitments and system requirements based on the applicable trust services criteria.

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

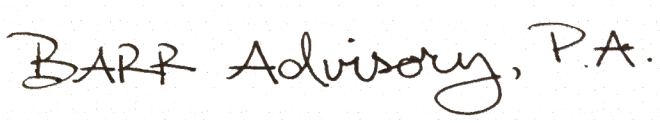
Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within Tessian's Human Layer Security Platform were effective throughout the period December 1, 2020 to February 28, 2021, to provide reasonable assurance that Tessian's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.



Fairway, KS

March 31, 2021

Assertion of Tessian Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Tessian's Human Layer Security Platform (system) throughout the period December 1, 2020 to February 28, 2021, to provide reasonable assurance that Tessian's service commitments and system requirements relevant to security, confidentiality, and availability were achieved. Our attached system description of the Human Layer Security Platform identified 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 December 1, 2020 to February 28, 2021, to provide reasonable assurance that Tessian's service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, and availability (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). Tessian's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the attached system description.

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 December 1, 2020 to February 28, 2021, to provide reasonable assurance that Tessian's service commitments and system requirements were achieved based on the applicable trust services criteria.

Tessian Limited

March 31, 2021

Overview of Operations

Description of Services Provided

Tessian (the "company") provides email security and data loss prevention services throughout Europe and the United States. The company was founded in 2013 and uses machine learning to automatically predict and eliminate advanced threats on email caused by human error—including data exfiltration, accidental data loss, business email compromise, and phishing attacks—with minimal disruption to employees' workflow.

Tessian's core product is the Human Layer Security (HLS) Platform delivered as Software as a Service (the "system").

The system includes the following core components:

- **Tessian Defender:** Essential defense against inbound security threats.
- **Tessian Guardian:** Automatically prevent accidental data loss via email.
- **Tessian Enforcer:** Automatically prevent data exfiltration over email.
- **Tessian HLS Intelligence:** Insights, automated threat intelligence, and tools for rapid investigation and remediation of threats prevented by Tessian's Human Layer Security Platform.

In addition to these core services, Tessian provides integrations with Microsoft Office 365, Microsoft Exchange, and G Suite. Further, Tessian HLS Intelligence directly integrates with numerous Security Incident and Event Management (SIEM) Security Orchestration, Automation, and Response (SOAR) platforms via a Representational state transfer (RESTful) HTTP API.

Principal Service Commitments and System Requirements

Tessian designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments Tessian makes to user entities, the laws and regulations that govern its services, and the financial, operational, and compliance requirements Tessian has established. The system services are subject to the security, confidentiality, and availability commitments established internally for its services.

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 include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role;
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system;
- Regular vulnerability scans over the system and network, and external penetration tests over the production environment; and,
- Operational procedures for managing security incidents and breaches, including notification procedures.

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit;
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties; and,
- Confidential information must be used only for the purposes explicitly stated in agreements between Tessian and user entities.

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components;
- Responding to customer requests in a reasonably timely manner;
- Business continuity and disaster recovery plans that include detailed instructions, recovery point objectives (RPOs), recovery time objectives (RTOs), roles, and responsibilities; and,
- Operational procedures supporting the achievement of availability commitments to user entities.

Such requirements are communicated in Tessian'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 are documented on how to carry out specific manual and automated processes required in the operation and development of the system.

Components of the System Used to Provide the Services

The purpose of the system description is to delineate the boundaries of the system, which includes the services and commitments outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure

The system is hosted in Amazon Web Services (AWS) in a virtual private cloud (VPC) environment which protects the network from unauthorized external access. The network topology includes segmented VPCs and access control lists (ACLs). User requests to Tessian's web-based systems are encrypted using Transport Layer Security (TLS) using certificates from an established third party certificate authority.

Remote system administration access to Tessian web and application servers is available exclusively through a secure virtual private network (VPN) connection and designated bastion hosts. The hardware components that make up the aforementioned system include servers hosted, managed, and protected by AWS. Production servers at AWS maintain failover capabilities in the event of physical hardware or logical software failures. This infrastructure is hosted in high availability data centers with multiple availability zones.

Software

Tessian is responsible for managing the development and operation of the HLS Platform including infrastructure components such as servers, database, and storage systems. The in-scope Tessian infrastructure and software components are shown in the table below:

People

Tessian currently has a staff of approximately 141 employees organized in the following main functional areas:

- **Corporate:** Responsible for overseeing company wide activities, establishing and accomplishing goals, and overseeing objectives.
- **Engineering:** Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.
- **Platform:** Responsible for maintaining the availability of production infrastructure, and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.
- **Security:** Responsible for access controls and security of the production environment.
- **People:** Responsible for recruiting and onboarding new personnel, defining roles and positions for new hires, performing background checks, and facilitating the employee termination process.
- **IT:** Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.
- **Customer Success:** Responsible for customer success and customer support activities.
- **Sales:** Responsible for sales and account management.

Data

Information assets are assigned a sensitivity level based on the audience for the information. If the information has been previously classified by regulatory, legal, contractual, or company directive, then that classification will take precedence. The sensitivity level then guides the selection of protective measures to secure the information. All data is to be assigned one of the following classification levels:

Customer data is deleted upon customer termination. Tickets are maintained once the data has been deleted.

Policies and Procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by senior management. These procedures cover the following key security life cycle areas:

- Information security policy and organization
- Risk management
- Asset management
- Access control
- Communications and network security
- Change management and secure development life cycle
- Vulnerability management
- Incident management and response
- Business continuity and planning
- Endpoint management
- Personnel security
- Data classification (data at rest, in motion, and output)

Complementary User Entity Controls

Tessian controls were designed with the assumption that certain internal controls would be in place at customer organizations. The application of such internal controls by customer organizations is necessary to achieve certain trust services criteria identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for processing of transactions for Tessian customers.

For customers to rely on the information processed through the Tessian Human Layer Security Platform, each customer is expected to evaluate its own internal controls to ensure appropriate control activities are in place. The following general procedures and controls should be considered. They should not, however, be regarded as a comprehensive list of all controls that should be implemented by customer organizations.

- User entity is responsible for protecting established user IDs and passwords within their organizations.
- User entity is responsible for reviewing customer access to the Tessian Human Layer Security Platform periodically to validate appropriateness of access levels.
- User entity is responsible for approving and creating new user access to the Tessian Human Layer Security Platform.
- User entity is responsible for removing terminated employee access to the Tessian Human Layer Security Platform.
- User entity is responsible for implementing policies and procedures over the types of data that are allowed to be entered into the Tessian Human Layer Security Platform. User entity is responsible for sending data to Tessian via a secure connection and/or the data should be encrypted.
- User entity is responsible for notifying Tessian if they detect or suspect a security incident related to the Human Layer Security Platform.
- User entity is responsible for reviewing email and other forms of communications from Tessian, related to changes that may affect Tessian customers and users, and their security or availability obligations.
- User entity is responsible for establishing, monitoring, and maintaining controls over the security for system-generated outputs and reports from the Platform.
- User entity is responsible for endpoint protection of workstations used to access the platform.
- User entity is responsible for developing their own business continuity and disaster recovery plan.

Complementary Subservice Organization Controls

Tessian uses subservice organizations in support of its system. Tessian's controls related to the system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria over the Human Layer Security Platform to be achieved solely by Tessian. Therefore, user entity controls must be evaluated in conjunction with Tessian's controls described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Tessian periodically reviews the quality of the outsourced operations by various methods including:

- Review of subservice organizations' SOC reports;
- Regular meetings to discuss performance; and,
- Non-disclosure agreements.

Control Activity Expected to be Implemented by Subservice Organization	Subservice Organization	Applicable Criteria
Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.	AWS	CC6.1, CC6.2, CC6.3, CC6.5, CC7.2
Physical access to the data center facility is restricted to authorized personnel.	AWS	CC6.4, CC6.5
Environmental protections, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.	AWS	CC6.4, A1.2
Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically.	AWS	A1.3
Policies and procedures to document repairs and modifications to the physical components of a facility including, but not limited to, hardware, walls, doors, locks, and other physical security components.	AWS	A1.2
Procedures are implemented to help ensure confidential data is protected and disposed of in accordance with defined commitments and agreements.	AWS	C1.1, C1.2