SYSTEM AND ORGANIZATION CONTROLS (SOC) 3 REPORT ON MANAGEMENT'S ASSERTION RELATED TO ITS

Turbot Guardrails and Turbot Pipes

Relevant to Security, Availability and Confidentiality

For the period April 16, 2023 to April 15, 2024

TOGETHER WITH INDEPENDENT AUDITORS' REPORT

Prepared by:

Sensiba

Table of Contents

1. Independent Service Auditors' Report

To the Management of Turbot HQ, Inc (Turbot)

Scope

We have examined Turbot's accompanying assertion titled "Assertion of Turbot Management" (assertion) that the controls within the Turbot Guardrails and Turbot Pipes (system) were effective throughout the period April 16, 2023 to April 15, 2024, to provide reasonable assurance that Turbot'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 (trust services criteria).*

Service Organization's Responsibilities

Turbot 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 Turbot's service commitments and system requirements were achieved. Turbot has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Turbot 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 Auditors' 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 Turbot 's service commitments and system requirements based on the applicable trust services criteria.

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Turbot'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.

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

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 the Turbot Guardrails and Turbot Pipes were effective throughout the period April 16, 2023 to April 15, 2024, to provide reasonable assurance that Turbot's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Sensiba LLP

San Jose, California

May 14, 2024

2. Assertion of Turbot Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the Turbot HQ, Inc (Turbot) Turbot Guardrails and Turbot Pipes (system) throughout the period April 16, 2023 to April 15, 2024, to provide reasonable assurance that Turbot's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of the Turbot Guardrails and Turbot Pipes," (description) 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 April 16, 2023 to April 15, 2024, to provide reasonable assurance that Turbot'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).*

Turbot'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 accompanying 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 April 16, 2023 to April 15, 2024, to provide reasonable assurance that Turbot's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by Turbot Management

May 14, 2024

3. Description of the Turbot Guardrails and Turbot Pipes

Company Background

Turbot HQ, Inc (Turbot) is the “Company.” And Turbot’s product offerings (Turbot Guardrails and Turbot Pipes) or services are the “Service.”

The Company provides cloud governance solutions designed for companies that want to maximize the value of their cloud computing investments and increase their security posture through automated controls.

Timeline of Company milestones:

- The Company was founded by Nathan Wallace in 2014 as a US Corporation headquartered in New Jersey.
- In 2015 the company announced the general availability of its Turbot Enterprise software.
- In 2016 the Company expanded its virtual office across varying US states.
- In 2017 the Company announced an expansion in the United Kingdom (Turbot HQ Limited) and India (Turbot HQ India Private Limited).
- In 2018 the Company started operations in Australia (Turbot HQ Private Limited).
- In 2020 the Company announced the general availability of its Turbot Cloud (SaaS) (now called Turbot Guardrails) service along with its v5 major version release.
- In 2021 the Company announced its new open-source project, Steampipe.
- In 2022 the Company announced Steampipe Cloud (now called Turbot Pipes) in preview.
- In 2023 the Company rebranded their Turbot product to Turbot Guardrails and Steampipe Cloud to Turbot Pipes.
- In 2023 the Company announced a new open-source project, Flowpipe.
- In 2024 the Company announced a new open-source project, Powerpipe.

Services Provided

The Company offers products that allow businesses to govern their cloud workloads and cloud data with reliability, flexibility, and scalability. They help improve discovery and insights across a massive amount of data to help decipher what resources I own, how they change, and how can I optimize my environment and increase my security posture. Turbot offers two primary products:

Turbot Guardrails:- automates Cloud Security and FinOps controls for organizations to detect and auto-remediate misconfigurations in AWS, Azure, GCP, Kubernetes, and ServiceNow.

Turbot Pipes:- provides cloud intelligence & security with a zero-ETL approach to integrate all your cloud data with a SQL interface, visualize insights & security posture with interactive dashboards, share and collaborate on that data or reports with your team. Built into Pipes is our three open-source projects:

- **Steampipe**:- our open-source approach to Pipes, specifically to run locally as an individual to query, join and report on any API with SQL.
- **Powerpipe**:- dashboards-as-code for visualizing clouds with interactive dashboards.
- **Flowpipe**:- pipelines-as-code to automate workflows around cloud services.

Principal Service Commitments and System Requirements

The Company makes service commitments to its customers and has established system requirements as part of the Service. Some of these commitments are principal to the performance of the Service and relate to applicable trust services criteria. The Company is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the Service to provide reasonable assurance that the service commitments and system requirements are achieved.

Service and security commitments to customers are documented and communicated in the Service Level Agreement and other customer agreements such as the Turbot Master Subscription and Privacy Policy agreements, as well as the description of the Service offerings provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Service 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 encryption technologies to protect customer data both at rest and in transit.

The Company establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in the Company’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 Service.

Components of the System

Infrastructure

Turbot products are hosted on Amazon Web Services (AWS) and Google Cloud Platform (GCP) leveraging various cloud services to transmit, process, and store Service Data, application code, as well as related system monitoring utilities. Service Data is defined as custom configurations that are set specific to the customer's environment that are solely stored and managed in Turbot. Only credential information for Turbot products to access customer environments is sensitive. No other information is intended to be sensitive (e.g., personal information). All data stored by Turbot products are subject to technical safeguards, as described in Turbot's Master Subscription Agreement

Software

The software consists of application programs and IT system software that supports application programs (operating systems, middleware, and utilities). Turbot's software stacks consist of AWS and GCP native cloud services capabilities for Container and Relational Database services. Turbot's products are distributed as container images in AWS' Elastic Container Service (ECS) and GCP's Kubernetes Engine services. All software and image builds are updated frequently and contain the latest patches and updates. Customers do not have access to this tier as the software is distributed into containers that are not accessible for login. Turbot uses cloud-native capabilities within AWS and GCP for monitoring and maintaining its software & infrastructure.

People

People consist of the personnel involved in the governance, operation, and use of a system. Turbot has a staff of employees worldwide in the following functional areas:

- Product Team consists of multiple sub-teams focused on product management, product engineering, and foundational product and infrastructure engineering support, and:
  - Product management is responsible for designing new features and core capabilities based on the voice of customer feedback. Product management works closely with Customer Success & Support teams for feedback, along with Turbot's Product Engineering teams for design reviews.
  - Product engineering is responsible for the development, testing, deployment, and maintenance of new code for Turbot production applications & products. Engineering consists of multiple global teams with specific assignments including Engineering teams focused on feature development and core services.
  - Foundational product and infrastructure engineering support is responsible for managing infrastructure and network configuration changes, overall system availability, logging, monitoring, backup, and recovery. Additionally, it is responsible for granting logical access to the systems, performing periodic reviews of access to

those systems, and revoking logical access rights upon user termination. Also works closely with Security to patch discovered system vulnerabilities.

- Customer Success (Customer Services & Support)
  - Responsible for managing customer interactions via email, chat, and phone. The team fields and resolves customer inquiries and issues, training, professional services for onboarding, and other technical issues related to the software. Customer Success is also responsible for communicating information to customers regarding new issues and/or developments, changes in processing schedules, system enhancements, new product features and updates, security incidents, and other relevant information.

- Operations Team consists of general people operations (HR), procurement, legal, security, and general internal information technology needs.
  - People Operations (HR) are responsible for onboarding new personnel, defining the role/position of new hires, performing background checks, handling internal employment logistics, and facilitating the employee termination process.
  - Procurement is responsible for accurate and timely billing with customers.
  - Legal is responsible for setting contractual obligations with third parties and technology partners/suppliers, including (i) negotiation, and drafting of legal terms and conditions; (ii) ensuring compliance with internal contractual standards; and (iii) review of information security and privacy issues.
  - Security is responsible for overall security governance, security monitoring, security tools (e.g., password manager), vulnerability & penetration testing, security awareness, incident response, and compliance & audit oversight. The security consists of multiple teams within the Product for specific assignments and responsibilities.

Information Technology (IT) is responsible for managing corporate computing devices (laptops/endpoints), business applications, supporting toolsets, and employee and contractor identities. It grants access to SaaS applications and to systems, working closely with HR and Product teams on appropriate access to systems using Turbot’s identity provider (single sign-on (SSO).

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by a system. Within Turbot’s applications, the customer defines and controls the data they load and store. This data is loaded into the environment and accessed remotely from customer systems via the Internet. Turbot classifies this data as Service Data.

Turbot also stores user credentials, which are used to authenticate to the Turbot applications, and for Turbot to access customer systems as part of the service offering the customer is using. Credential data, consisting of unique usernames and passwords is considered sensitive. Any logging of this information is filtered out prior to the logs being written to disk.

The databases storing Service or Credential Data are encrypted at rest, all connections to the databases are encrypted, and Turbot rotates the credentials for connecting automatically and continuously. Each customer also has their own unique key for encrypting data automatically, Sensitive Data specific to the customer is encrypted with this key automatically.

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 Turbot policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Turbot team member.

Physical Security

All data is hosted by AWS and GCP. AWS and GCP data centers do not allow Turbot employees physical access. Turbot is a globally distributed virtual office, there are no physical office locations.

Logical Access

The System Access Control Policy establishes the access control requirements for requesting and provisioning user access to the system. The policy requires that access be denied by default, follow the least privilege principle, and be granted only upon business need.

Each user account is unique and is identifiable to an individual user. Segregation of duties is established for critical functions within the environment to minimize the risk of unauthorized changes to production systems.

Domain account management requests are routed to the designated asset owner or an associated employee according to established account provisioning and de-provisioning processes for approval. Typically, access is controlled through the addition of individual user accounts to established domain security groups within the domain. Based on the configuration of a security group, any access requests require an explicit approval from the assigned security group owner.

Employee status data is used to facilitate the provisioning and removal of user accounts in the system. Account management processes prevent the creation of an account for individuals that do not have valid HR records. Select users can request the removal of user accounts from the system. In addition, system owners can directly remove users from security groups. Upon termination, employees are required to return any Company data back to Turbot.

Automated mechanisms have been implemented to manage the appropriateness of access granted to information systems. Manual periodic reviews of individual accounts and security group memberships on assets are performed by authorized individuals, as appropriate, to evaluate whether access is still required. Remediation action is taken, as necessary, based on the review.

Policies and standards have been established and implemented to enforce appropriate user account password expiration, length, complexity, and history. Turbot personnel are required to follow the Turbot password policy for all domains as well as local user accounts for all assets.

Access to the production environments is controlled through a designated set of access points and restricted to the appropriate Turbot team members. Users are authenticated to access points using domain credentials depending on where the production assets are located. Passwords, along with two-factor authentication used to access infrastructure services, are restricted to authorized individuals and system processes based on job responsibilities.

Cryptographic controls and approved algorithms are used for information protection within the service environment and are implemented based on Company policies and standards. Cryptographic keys are managed throughout their lifecycle (e.g., ownership, generation, storage, distribution, periodic rotation, revocation) in accordance with key management procedures.

Turbot maintains a detailed inventory of all information systems. All such assets are assigned ownership by a designated department or team within the Company and prioritized based on the asset’s business value and criticality to the organization. The classification process is owned by each service owner and reviewed by Security. Information and data assets are subject to the data management policy that defines parameters for the ownership, classification, security, storage, and retention of data. Software and hardware assets are subject to the asset management policy and vendor management policy that defines parameters for the acquisition, development, maintenance, security, and disposal of information system assets. There are four categories for classification: public, internal, customer confidential, and company confidential. Steps are taken to protect assets commensurate with the respective asset's classification and its data sovereignty.

The inventory of infrastructure components is monitored and maintained by the security & engineering teams. Regularly, the Company checks for the completeness and accuracy of the inventory to ensure that it represents the production environment appropriately. In addition, network architecture is maintained as part of the inventory process. Metadata of the assets are collected and maintained within the inventory that provides an overview and flow of the network.

Computer Operations – Backups

Where Turbot manages the database tier which hosts Service Data, Turbot configures full, daily database backups for all data stored by our cloud services provider. If a database instance is deleted, all automated associated backups are also automatically deleted, with the manual backups preserved per the Backup Data Protection Policies.

Backups are periodically tested by the Turbot Product team.

Computer Operations – Availability

Automated mechanisms and periodic scanning have been deployed to detect and troubleshoot exceptions or deviations from the baseline in the production environment.

Where applicable, mechanisms are in place for services to re-image production servers with the latest baseline configuration. The engineering team reviews and updates configuration settings and baseline configurations regularly.

The Company has implemented cloud-native service-based monitoring within the environment to provide automated logging and alerting capabilities. The logging solutions are enabled on all production systems. The monitoring system detects potential unauthorized activity and security events. The Product team is responsible for monitoring a defined set of user and administrator events, aggregating log events, and alerting Security and the system owner of any abnormal events.

Turbot has established a policy that restricts the log and monitors access to only authorized staff with a business need to access such systems. The engineering team determines the specific events that need to be captured in consideration with a baseline. Administrator, operator, and system activities performed, such as logon or logoff within the environment, are logged and monitored.

The Company has implemented a system to provide real-time alerting through the automatic generation of emails and alarms based on the log information captured by the monitoring infrastructure. The engineering team is responsible for configuring the events to be alerted. The event and warning logs are routinely examined for anomalous behavior and, when necessary, appropriate actions are taken in accordance with the incident handling procedures described in the Incident Response Policy. The engineering team manages the response to malicious events, including escalation to and engaging support groups. In addition, the Company monitors relevant external information to stay up-to-date and share current threat scenarios and countermeasures.

Turbot has established incident response procedures and centralized tracking tools that consist of different channels for reporting production system incidents and weaknesses. Automated mechanisms include system monitoring processes for alerting per defined and configured events, thresholds, or metric triggers. Incidents may also be reported via email. Users are made aware of their responsibilities of reporting incidents that shall be investigated without any negative consequences for the reporter. The Company incident response provides 24/7 event and incident monitoring and response services. The team assesses the health of various components along with access to detailed information when issues are discovered.

Turbot teams use the established incident classification, escalation, and notification process for assessing an incident's criticality and severity, and accordingly escalating to the appropriate groups for timely action. The engineering team documents, tracks, and coordinates responses to incidents. Where required, security incidents are escalated to the executive management team following established forensic procedures to support potential legal action after an information security incident.

Post-mortem activities are conducted for customer-impacting incidents or incidents with high severity. The post-mortems are reviewed by the engineering team during recurring engineering meetings with senior management. Incident and security post-mortem trends are reviewed and evaluated periodically and, where necessary, the platform or security program may be updated to incorporate improvements identified because of incidents.

Change Control

The Change Management process has been established to plan, schedule, approve, apply, distribute, and track changes to the production environment through designated responsibilities with the objective of minimizing risk and customer impact. It further controls the integrity and reliability of the environment while maintaining the pace of change required for business purposes.

Software, system, and configuration changes, including major releases, minor releases, and hotfixes, are managed through a formal change and release management procedure, and tracked using a centralized ticketing system. Changes are requested, approved, tracked, and implemented throughout the release life cycle, which can include product and engineering planning, release management, deployment, and post-deployment support phases. Change requests are documented, assessed for their risks, and evaluated and approved for acceptance by the designated personnel.

Quality assurance testing may be performed prior to the software release through each pre-production environment (e.g., local development and staging) based on defined acceptance criteria. Changes are reviewed for their adherence to established change and release management procedures prior to closure.

Once deployed, changes are monitored for success, failed implementations are immediately rolled back, and the change is not considered complete until it is implemented and validated to operate as intended.

Turbot’s software development practices are aligned with the software development life cycle (SDLC) methodology. This development process introduces security and privacy control specifications during the feature and component design and throughout the development process.

Data Communications

Turbot maintains a description of the service environment and its boundaries that is communicated to internal and external authorized users. System logic is coded into the system and generates on-screen alerts if there are any issues when establishing a connection between the Turbot application and the production infrastructure systems and tools. For instance, when customer infrastructure data is manually typed into the application, the system is configured with input validation checks to ensure that the necessary information is provided to process the transaction. Historical security and compliance data related to the customer's control environment is retained for the life of a customer account. No customer data is purged until the customer account is deleted and data deletion is requested.

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. If a primary system fails, the redundant hardware is configured to take its place.

The Company carries out frequent scans to identify vulnerabilities and assess the effectiveness of the patch management process. These scans are used to ensure compliance with baseline configuration templates, validate that relevant patches are installed, and identify vulnerabilities. The scanning reports are reviewed by the appropriate personnel and remediation efforts are conducted in a timely manner.

The applicable security patches are applied immediately or during a scheduled release to the environment based on the severity of the vulnerability. Processes are in place to evaluate patches and their applicability to the environment. Once the patches have been reviewed and their criticality level determined, service teams determine the patch implementation strategy without service disruption.

Penetration testing is performed at least annually on the system by a programmatic independent third party. The penetration test scope is determined based on Turbot's areas of risk and compliance requirements and findings from the vulnerabilities discovered to attempt known patterns to ethically penetrate the system / expose the vulnerability further.

Boundaries of the System

The scope of this report includes the Turbot Guardrails and Turbot Pipes services performed by Turbot. This report does not include the data center hosting services provided by AWS and GCP.

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

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 Turbot’s control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Turbot’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.

Turbot has developed a Code of Conduct that addresses acceptable business practices, conflicts of interest, and expected standards of ethical and moral behavior. Turbot has also developed personnel confidentiality agreements that prohibit the inappropriate use and disclosure of customer or Company information. These documents are provided to all new employees and contractors and are required to be signed prior to the employee’s start date. All personnel are required to accept (review & acknowledge acceptance) the code of conduct and security policies.

Employees and contractors who violate the code of conduct are subject to disciplinary actions. Where applicable, employees and contractors process a background check before starting work.

Commitment to Competence

Turbot's 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 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 jobs and translated required skills and knowledge levels into written position requirements.
- Training and Certifications are encouraged to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

Turbot'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 reviewing regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

Organizational Structure and Assignment of Authority and Responsibility

Turbot'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.

Turbot’s assignment of authority and responsibility activities includes 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 understands 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.

Turbot’s organizational structure through Organizational Charts is created, along with individual role responsibilities as part of the periodic employee check-ins with direct managers, and Team Leaders have documented responsibilities that are communicated for key areas of authority and responsibility.

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

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

Human Resource Policies and Practices

Turbot’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. Turbot’s human resources policies and practices relating 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 and contractors are required to sign a confidentiality agreement following new hire orientation on or before their first day of employment.
- New employees and contractors are required to review and agree to the Company’s Code of Conduct, and other security-related policies and procedures. Employees and contractors review and agree to these policies annually and when a major change is introduced.
- Evaluations for each employee are performed on a 6-month review basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

Risk Assessment Process

Turbot has a risk assessment process to identify and manage risks that could affect the Company's ability to provide reliable services to its clients. This process requires management to identify significant risks in their areas of responsibility and to implement measures to address those risks. In designing its controls, the Company has considered the risks that could prevent it from effectively addressing the criteria under the security and processing integrity Trust Services Categories.

Turbot ensures that risks are evaluated and that controls are designed, implemented, and operated to address all areas, as appropriate, to detect, respond to, mitigate, and recover from security events based on the assessed risks. Areas for evaluation include systems development, computer operations, program changes, and access to programs and data. Implemented controls include preventive and detective controls, such as manual, automated, or IT-dependent controls based on the environment in which the entity operates; the nature and scope of the entity's operations; and its specific characteristics. The Company 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. The Company's risk assessment process includes an analysis of possible threats and vulnerabilities relative to each of the objectives. The risk identification process includes consideration of both internal and external factors and their impact on the achievement of the objectives.

Turbot considers the potential for fraud in assessing risks to the achievement of objectives. The assessment of fraud risk considers fraudulent reporting, possible loss of assets or data, and corruption resulting from the various ways that fraud and misconduct can occur. It also considers opportunities for unauthorized acquisition, use, or disposal of assets, altering of the entity's reporting records, or committing other inappropriate acts and how management and other personnel might engage in or justify inappropriate actions.

Turbot identifies and assesses changes that could significantly impact the system of internal control. The risk identification process considers changes to the regulatory, economic, and physical environment in which the Company operates. The Company considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations, rapid growth, and new technologies on the system of internal control.

Identified risks are analyzed through a process that includes estimating the potential significance of the risk. Turbot's risk assessment process includes considering how the risk should be managed and whether to accept, avoid, mitigate, or share the risk. The Company determines mitigation strategies for the risks that have been identified and designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy.

Security risks related to external parties (such as contractors and vendors) are identified and addressed based on Turbot's vendor review process.

Turbot considers the inherent risk of working with vendors and business partners as part of the annual risk assessment performed by the Security team. Internal and external cyber threats and vulnerabilities are identified and assessed based on the likelihood that they could prevent the entity from achieving its objectives. Consideration is given to cyber threats and vulnerabilities such relationships may present and whether Turbot's controls reduce such risks to a level consistent with Turbot's objectives and risk acceptance.

Information and Communications Systems

Turbot has documented policies, procedures, and system environment descriptions that are updated regularly and communicated to authorized users. System changes are also communicated to authorized users when they occur. The internal communication of cybersecurity information for employees according to their role in the organization is described in the Turbot information security policy, which is available to all employees.

Turbot obtains or generates and uses relevant information to support the functioning of internal control through annual control/risk self-assessments, annual vulnerability/penetration testing, system monitoring alerts, and incident response procedures.

As is the typical business practice by most organizations, Turbot restricts the communication of matters related to the functioning of Turbot's system to only those stakeholders and business partners who have a need to know such information. This information may be communicated via mediums appropriate to the nature of the information and the urgency of the situation and may include conference calls, emails, real-time chat messages, documents, or in-person meetings. In the rare instances when public disclosure of such matters would be necessary or appropriate, Turbot's legal counsel is responsible for jointly distributing and communicating such disclosures.

Customers are notified of system changes that may affect their processing. Customers are provided a means to report system failures, incidents, concerns, or other complaints, as well as technical support resources relating to system operations. Turbot's privacy policy is provided on its website.

Monitoring Controls

Turbot selects, develops, and performs ongoing or separate evaluations to ascertain whether the components of internal control are present and functioning. Internal personnel conduct periodic assessments and tests of internal controls that include (a) working with process/service owners to identify specific security threats and vulnerabilities and how the associated risk is being addressed and (b) tests of the design, implementation, and operating effectiveness of internal controls that address risks.

Members of the internal assessment team have the requisite knowledge of and experience with cybersecurity risks and controls.

Turbot also uses external parties to independently evaluate the state of the control environment. Annual vulnerability & penetration tests are performed by an external service provider to identify specific technical threats and vulnerabilities and to benchmark the environment against leading cybersecurity practices. Every year, Turbot engages a service provider to perform an independent assessment of the system program to evaluate alignment with leading industry practices and consistency with Company policies to identify gaps and potential opportunities for improvement.

Both internal and external evaluations are made using a risk-based approach that may vary with the nature, timing, and extent of testing.

The results of all monitoring activities, regardless of source, are entered into a vulnerability tracking system for the evaluation and identification of remediation activities that may be needed. Identified vulnerabilities are assessed regarding the likelihood and magnitude of exploitation. All vulnerabilities evaluated are identified for remediation or additional monitoring. Responsibilities for corrective action plans are assigned and determined. The security and applicable engineering team members review the list of open vulnerabilities regularly to monitor progress toward resolution and to identify trends and responses.

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 the Turbot Guardrails and Turbot Pipes.

Subservice Organizations

Turbot HQ, Inc’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 Turbot’s services to be solely achieved by Turbot‘s control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Turbot.

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

Security Category	
Criteria	Controls expected to be in place
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.	AWS and GCP is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the entity's system resides.
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.	
CC6.3 - 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.	

Security Category	
Criteria	Controls expected to be in place
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.	
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
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.	
CC6.4 - The entity restricts physical access to facilities and protected information assets (e.g., datacenter facilities, backup media storage and other sensitive locations) to authorized personnel to meet the entity’s objectives.	AWS and GCP is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers where the entity's system resides.

Availability Category	
Criteria	Controls expected to be in place
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.	AWS and GCP is responsible for managing environmental protections within the data centers that house network, virtualization management, and storage devices for its cloud hosting services where the entity's system resides.

Turbot 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, Turbot 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

Turbot’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 Turbot’s services to be solely achieved by Turbot‘s control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Turbot’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 Turbot.
2. User entities are responsible for notifying Turbot 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 Turbot 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 Turbot services.
6. User entities are responsible for providing Turbot with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Turbot of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.