Qase, Inc.

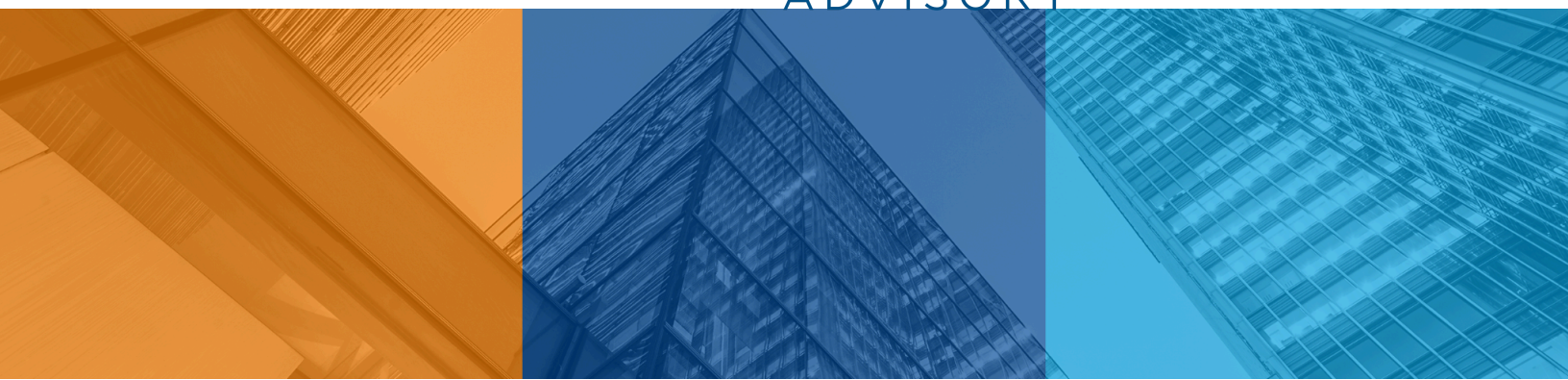
Report on Controls at a Service Organization Relevant to Security

SOC 3®

For the Period February 1, 2023 to January 31, 2024

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 Qase, Inc. (Qase):

Scope

We have examined Qase's accompanying assertion titled "Assertion of Qase Management" (assertion) that the controls within the Qase Application (system) were effective throughout the period February 1, 2023 to January 31, 2024, to provide reasonable assurance that Qase's service commitments and system requirements were achieved based on the trust services criteria relevant to security (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

Qase 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 Qase's service commitments and system requirements were achieved. Qase has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Qase 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 Qase'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 Qase'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.

Relevant Ethical Requirements

We are required to be independent of Qase 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 Qase Application were effective throughout the period February 1, 2023 to January 31, 2024, to provide reasonable assurance that Qase'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 15, 2024

Assertion of Qase Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the Qase Application (system) throughout the period February 1, 2023 to January 31, 2024, to provide reasonable assurance that Qase's service commitments and system requirements relevant to security were achieved. Our attached system description of the Qase Application 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 February 1, 2023 to January 31, 2024, to provide reasonable assurance that Qase's service commitments and system requirements were achieved based on the trust services criteria relevant to security (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). Qase'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 February 1, 2023 to January 31, 2024, to provide reasonable assurance that Qase's service commitments and system requirements were achieved based on the applicable trust services criteria.

Qase, Inc.

March 15, 2024

Qase's Description of the Boundaries of Its Qase Application

Description of Services Provided

Qase, Inc. ("Qase" or the "company") provides test management services throughout the United States. The company was founded in 2019 and provides Software as a Service (SaaS).

Qase's core product, the Qase Application (the "system"), is a SaaS solution that includes the following services:

- **Test management:** A service that contains repositories of test cases, requirements, and test environments.
- **Test reporting:** A service related to integration with automated test frameworks.
- **Test analytics:** A service that provides build charts based on statistics.

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, data, and processes and procedures.

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). Qase employs intrusion detection systems (IDS) at strategic points in its network that complement its security policy network settings. User requests to Qase'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 Qase web and application servers is available through a virtual private network (VPN) connection. The hardware components that make up the aforementioned system include servers hosted, managed, and protected by AWS.

Software

Qase is responsible for managing the development and operation of the Qase Application including infrastructure components such as servers, databases, and storage systems.

People

Qase is organized in the following functional areas:

- **Board of Directors:** Responsible for matters related to business objectives, finances, operations, internal controls, human resources, compliance, and audits, as necessary.
- **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. Also responsible for the product life cycle, including adding additional product functionality, and incident management.

- **Operations/Security:** Responsible for access controls, information security policies and procedures, risk management, business continuity, vulnerability and incident management, and security of the production environment. Also responsible for overseeing the development and performance of internal control and is composed of members with varying backgrounds for objective decision-making. Members independent of control operators oversee the development and performance of internal control.
- **Human Resources:** Responsible for recruiting and onboarding new personnel, defining roles and positions for new hires, and facilitating the employee onboarding and termination process.
- **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 sales, account management, customer success, and customer support activities.

Data

Data, as defined by Qase, constitutes the following:

- Customer operating data
- Qase Application data (tags, comments, teams)
- Output reports
- System files
- Access credentials

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 sensitivity levels:

Sensitivity Level	Description	Example(s) of Data
Confidential	Highly sensitive data requiring the highest levels of protection; access is restricted to specific employees or departments, and these records can only be passed to others with approval from the data owner or a company executive.	• Customer operating data • Customer personal identifiable information (PII) • Data subject to a confidentiality agreement with a customer
Restricted	Qase proprietary information requiring thorough protection; access is restricted to employees with a "need-to-know" based on business requirements. This data can only be distributed outside the company with approval. This is default for all company information unless stated otherwise.	• Contracts • Internal policies • Legal documents • Email
Public	Documents intended for public consumption which can be freely distributed outside Qase.	• Product release notes • Marketing materials • External facing policies

Processes 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:

- Access Control
- Asset Management
- Code of Conduct
- Cryptography
- Data Management
- Human Resource Security
- Incident Response
- Information Security
- Information Security Roles and Responsibilities
- Operations Security
- Physical Security
- Risk Management
- Secure Development
- Third-party Management

Principal Service Commitments and System Requirements

Qase designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Qase makes to user entities, the laws and regulations that govern its services, and the financial, operational, and compliance requirements that Qase has established. The system services are subject to the security 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 identify potential security attacks from users outside the boundaries of the system;
- Daily vulnerability scans over the system, network, and production environment and resolving identified vulnerabilities; and,
- Operational procedures for managing security incidents, including notification procedures.

Qase establishes system requirements that support the achievement of service commitments, relevant operational and compliance requirements, applicable laws and regulations, and other system requirements including the following:

- System functional and nonfunctional requirements derived from service commitments, published documentation of system functionality, and other descriptions of the system; and,
- Business processing rules, standards, and regulations.

Such requirements are communicated in Qase'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.

