Qliktech Inc.

Report on the Qliktech Inc.'s Qlik Cloud Services System Relevant to Security and Availability

System and Organization Controls (SOC) 3 Report

For the Period October 1, 2019 through September 30, 2020

Qliktech Inc.

Report on the Qliktech Inc.'s Qlik Cloud Services System Relevant to Security and Availability

For the Period October 1, 2019 through September 30, 2020

Table of Contents

Section I.
Independent Service Auditor's Report Provided by KPMG LLP

KPMG LLP
1601 Market Street
Philadelphia, PA 19103-2499

Independent Service Auditor's Report

Board of Directors of Qliktech Inc.:

Scope

We have examined Qliktech Inc.'s (Qlik's) accompanying assertion titled "Qliktech Inc.'s Assertion" (assertion) that the controls within Qlik's Qlik Cloud Services (QCS) system (system) were effective throughout the period October 1, 2019, to September 30, 2020, to provide reasonable assurance that Qlik's service commitments and system requirements were achieved based on the trust services criteria relevant to security 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

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

Service Auditor's Responsibilities

Our responsibility is to express an opinion, 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 Qlik'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 Qlik's service commitments and system requirements based the applicable trust services criteria

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

KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.

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 are 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 Qlik's QCS system were effective throughout the period October 1, 2019, to September 30, 2020, to provide reasonable assurance that Qlik's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

KPMG LLP

Philadelphia, Pennsylvania
November 10, 2020

Section II.
Qliktech Inc.’s Assertion

Qliktech Inc.'s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls with Qlik's QCS system throughout the period October 1, 2019 to September 30, 2020, to provide reasonable assurance that Qlik's service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the systems is presented in Section III 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 October 1, 2019, to September 30, 2020, to provide reasonable assurance that Qlik's service commitments and system requirements were achieved based on the trust services criteria relevant to security 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).* Qlik'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 Section III.

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 October 1, 2019 to September 30, 2020, to provide reasonable assurance that Qlik's service commitments and system requirements were achieved based on the applicable trust services criteria.

Marie Rainis

Director, R&D Compliance

November 10, 2020

Section III.
Description of Qlik Cloud Services Provided by Qliktech Inc.

Overview of Company and Services

Founded in Lund, Sweden in 1993, Qliktech Inc. ("Qlik" or "the company") provides an end-to-end data management and analytics platform for transforming entire businesses. Qlik does business in more than 100 countries and serves over 48,000 customers around the world. Qlik provides multiple types of software to help customers analyze their data via an associative in-memory technology and visualization client accessed through a web browser.

Description of Services Provided

Qlik provides QCS, a cloud-based service offering, to customers for analyzing and visualizing data. Customer data is hosted in Qlik's Amazon Web Services (AWS) production environment and is a multi-tenant implementation. Customers use QCS to upload or create analytic applications (documents) into which they load and model their data and then visualize it. They are then able to provide that analysis to other users in their organization.

To use either of the Qlik Sense Business (QSB) or Qlik Sense Enterprise (QSE) product offerings that run in QCS, customers can start with an online trial (for QSB), evaluation tenant (for QSE), or purchase directly. Once the Service Account Owners (SAO) set up their domain name and their desired Identity Provider, additional users can be invited to the tenant and analytics content can then be uploaded or created.

Scope of the Report

The scope of this report is intended to provide specified parties with information about QCS's design of internal controls that meet the criteria for the Security and Availability categories set forth in TSP Section 100, *Trust Services (AICPA, Trust Services Criteria)*. This report does not encompass all aspects of the services or procedures performed by Qlik as an enterprise.

Principal Service Commitments and System Requirements

Qlik designs its processes and procedures related to its QCS environment to provide the end-to-end data management and analytics platform.

Security commitments to user entities are documented and communicated in customer solicitations and agreements, as well as in the description of the service offering provided online. Security commitments include, but are not limited to, the following:

- Use of encryption technologies to protect customer data both at rest and in transit.
- Security principles within the system 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.
- Scheduled and monitored virus and vulnerability scans as well as penetration testing.

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

- QCS is available 24 hours, 7 days a week outside of outages or expected downtime, which is communicated to customers and also published on Qlik's external website at status.qlikcloud.com.
- Qlik maintains a disaster recovery plan (DRP) covering QCS to help ensure continued availability. The DRP is tested at least annually to help ensure it is up-to-date.
- Data backups are managed by two separate service providers, AWS and Google Cloud Platform, to help ensure redundancy.
- System restoration occurs as soon as technically feasible for all functions. Restoration tests are performed on at least an annual basis to help ensure processes are up-to-date and backups are functioning appropriately.

Qlik establishes operational requirements that support the achievement of security and availability commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Qlik's system policies and procedures and system design documentation. Information security policies define an organization-wide approach to how systems are protected. These include policies around how the service is designed and developed, how the system is operated, how the 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 QCS.

System Overview

Qlik has designed its processes and procedures based on its system requirements and service commitments to user entities, the laws and regulations that govern the provisioning of QCS, and the financial, operational, and compliance requirements that Qlik has established for QCS.

The system is designed and implemented to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system, which includes the services and commitments outlined above, and the five components of the system described below:

Infrastructure

The supporting infrastructure consists of the following infrastructure, applications and databases, as shown in the table below:

Infrastructure	Description
AWS (Subservice organization)	AWS directs and controls operations as well as establishes, communicates, and monitors policies and procedures for all of the QCS production environments. In addition, AWS operates, manages and controls the components from the virtualization layer to the physical security of the facilities in which the QCS components operate. Qlik assumes responsibility for, and management of, the operating system (including updates and security patches), application software and the configuration of the security group firewall provided by the service provider. Key AWS services utilized by Qlik include: • Elastic Compute Cloud (EC2) • Simple Storage Service (S3) • Elastic Load Balancer (ELB) • Relational Database Service (RDS) • Identity Access Management (IAM) • Virtual Private Cloud (VPC) • Security Groups (SGs) • Elastic File System (EFS) • CloudWatch (CW) • GuardDuty • Config • DynamoDB • CloudFront

Infrastructure	Description
Google Cloud Platform (GCP) (Subservice organization)	Qlik utilizes the Google Cloud Storage service within the GCP platform to perform nightly backups of the AWS environment.

Software

The software consists of the following applications and tools, as shown in the tables below:

Software	Description
Change Management	
Jira	Jira is a ticketing application used to track and assign work items. Jira also provides a system for planning, scheduling, implementing and tracking changes for QCS.
GitHub	GitHub is a centralized source code control system. It is implemented internally for the management of code repositories.
CircleCI	CircleCI is a tool that supports continuous integration, a development practice software teams use to build, test and deploy applications on multiple platforms.
Configuration Management	
TwistLock	TwistLock is a security tool deployed throughout the production environment that is used to monitor Kubernetes for compliance with Qlik-defined security hardening and configuration baselines.
Kubernetes	Kubernetes is an open-source system for automating deployment, scaling and management of containerized applications. It groups containers that make up an application into logical units for management and discovery.
Identity and Access Management	
Microsoft Active Directory® (AD)	Qlik's AD stores user accounts, group memberships, and account data, and is used to manage access to the Qlik corporate network. Internal users are required to have a Qlik AD user name and password to authenticate to the Qlik corporate network and the Qlik or enterprise production servers.
Multifactor authentication services	Access to production environments at Qlik requires strong, multifactor authentication. Two multifactor authentication solutions are used at Qlik, such as OKTA and Duo Security.

Software	Description
People Resources	
Workday	Workday is a People Resources tool used to manage Qlik personnel's account and employment information.
Systems Monitoring	
Expel	Expel is a third party service that monitors the QCS environment 24 hours per day x 7 days per week. They investigate and respond and provide transparent managed security.
Prometheus	Prometheus is a centralized availability monitoring tool used for enterprise services.
Training and Awareness	
Skillsoft SkillPort	Skillsoft SkillPort is used to deliver security training modules to Qlik personnel, collect completed module results and remind users and management of incomplete modules.
Vulnerability Management	
Nessus	Nessus is a vulnerability scanner used to perform vulnerability scans across Qlik's infrastructure. It is used to identify and report vulnerabilities based on severity.
Workstream Applications	
Confluence	Confluence is a content management repository used to store documents, track workflows and manage work.

Database	Description
Change Management	
MongoDB Atlas	MongoDB Atlas is a database that is used to store data used in QCS.

People

Qlik is comprised of the following departments:

- The X-team (Executive Management) – Responsible for overseeing company-wide activities, creating corporate level VSGs (Vision, Strategies, and Goals), measuring goals and overseeing objectives.
- Culture and Talent (C&T) – Responsible for working with teams to create an innovative culture. C&T is organized into Centers of Excellence teams, which include:
    - Recruitment
    - Talent Development
    - Total Rewards
    - Internal Communications
    - Business Partners
    - Systems and People Analytics
- Global Products Organization - Responsible for anticipating customer needs, defining and refining product requirements and communicating to our customers product capabilities. The Global Products Organization is comprised of:
        - Product Management
        - Product Marketing
        - Strategic Marketing Operations
        - Product Packaging and Pricing
        - Product Operations
        - Market Intelligence
- Global Technology Product Organization Responsible for designing and developing solutions to address customer needs, via product requirements and ensuring that software and solutions meet the highest standards. The Global Product Technology Organization is comprised of:
    - Product Design
    - Engineering, i.e. Product Development
    - Quality Engineering, i.e. Product Testing
    - Site Reliability Engineering (SRE)
    - Product Architecture & Research
    - Software Services
    - Information Technology (IT)
    - Program Management & Compliance

- Software Security Office, i.e. Secure Software Development
- IT Security & Compliance, i.e. Corporate Security and Compliance

- Finance – The Finance team is responsible for continuous oversight of the financial aspects of Qlik, including budgeting, payroll, and accounts payable and receivable, and is comprised of the following teams:
  - Accounting
  - Global Procurement & Real Estate
  - Revenue Assurance & Operations
  - Financial Planning & Analysis
  - Tax & Treasure
- Customer Success – The Customer Success team is responsible for increasing customers, as well as increasing satisfaction and identifying additional solutions for current customers.
- Other teams include Office of Strategy Management, Sales, Legal and Global Marketing.

Procedures

Human Resources Hiring and Termination

Qlik has organizational charts in place to communicate the defined key areas of authority, responsibility and lines of reporting to personnel. These organizational charts are updated as needed as the company expands. In addition, documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for all current positions and expected job openings.

Hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties outlined in the job description. As part of the hiring process, background checks are performed for potential employees (as allowed by country laws), and new employees are required to sign employment contracts. Further, employees are required to complete the Global Privacy and Information Security and Code of Conduct training upon initial hire and annually thereafter to understand their responsibilities to comply with legal and information security policies and procedures.

When necessary, Qlik follows an established termination process, where network access is revoked and off-boarding checklists are followed.

Access Authentication and Authorization

The production server operating systems and application are configured to enforce two-factor user authentication that requires a unique user account and password and a one-time passcode.

Passwords for production database administrator accounts are securely stored within a password safe application. Administrative access privileges to the production server operating systems, production databases, application and VPNs are restricted to user accounts accessible by SRE

personnel. Web servers utilize secure sockets layer (SSL) encryption for web communication sessions.

Access Requests and Access Revocation

Documented policies and procedures are in place to guide personnel when provisioning and de-provisioning access and conducting user access reviews.

User access requests are documented on a standard access request form and require the approval of a manager. Administrative access privileges to the production server operating systems, databases, application and VPN are restricted to user accounts accessible by authorized personnel.

A termination checklist is completed and access is revoked for employees as a component of the employee termination process. SRE personnel review user access on at least a semiannual basis to help ensure that access to data and production systems is restricted and provides for appropriate segregation of duties.

Change Management

Release policies and procedures are in place to guide the Global Products Organization in the release and change management processes. Engineering personnel complete a Jira change ticket for all application updates (i.e. bug fixes, enhancements and new development requests) and system changes. Both Engineering and Quality Engineering personnel perform tests prior to promoting any changes to production or release branches.

All changes must be approved by a peer reviewer with applicable domain knowledge prior to the migration of the changes into the production environment. Access privileges to develop code libraries and promote changes into the production environment are restricted to user accounts accessible by authorized Engineering personnel.

Monitoring tools are used to log application and system changes implemented into the production environment. For QCS, GitHub, CircleCI and Kubernetes are used to promote new changes roll back changes to a previous version.

The production environment is segmented from the development and staging environments.

Engineers promote changes upon completing checks agreed upon in the SRE Partnership Agreement. The agreement establishes at the requirements for releasing code into a production environment.

Data Backup and Disaster Recovery

Automated replication and backup systems are in place to perform scheduled replication and backups of production databases (MongoDB) and customer data to AWS. Data is also copied nightly to GCP to allow for additional reliability. Failed backups are logged for investigation by the SRE team. Disaster recovery (DR) is tested at least annually and any deficiencies are documented for investigation, along with mitigation analysis.

Incident Response

Documented policies and procedures are in place to guide the appropriate teams in identifying, reporting and resolving failures, incidents, concerns and other complaints. Security Operations personnel use Jira Security Operations to document the identification, escalation, and resolution of security incidents.

Incidents that require a change to the system follow the change management process.

Security sprint meetings are held every two weeks to discuss incidents and corrective measures to ensure that incidents are resolved.

System Monitoring

Qlik utilizes AWS's CloudWatch service to monitor system changes and availability of services and infrastructure. CloudWatch analyzes availability and change data and provide alerts to the SRE team. Usage for CPU and storage is handled by AWS as part of the services provided. Security alerts identified by CloudWatch and GuardDuty are documented and investigated by Expel, and if needed, escalated to SRE personnel.

Additionally, Qlik's monitoring tool, Prometheus, is used to monitor all service level indicators of services and infrastructure internally. Prometheus notifies the SRE team upon identification of latency issues that may affect QCS. Security Operations reviews event logs on an ongoing basis and identified security incidents are formally documented for investigation. Alterations to the configuration of threshold alerts within Prometheus are secured within GitHub and follow the change management process. In addition, Qlik utilizes Twistlock for runtime protection, which uses machine learning to automatically build a 3D model of every application. Models define all the known-good behaviors of hosts and containers, across process, network, file system and system call sensors.

Vulnerability Management

Security Operations personnel perform internal and external vulnerability assessments of the production environment on a semiannual basis. Vulnerabilities that are identified are formally documented, along with mitigation strategies, for management review.

Data

QCS

Location of Data

Qlik utilizes AWS to operate QCS in three networked data centers: Dublin, Ireland; Northern Virginia, USA; and Sydney, Australia.

Personal Data Collection

The only personal data that Qlik receives relates to authentication information. Qlik also processes statistical data on the use of QCS to assist with troubleshooting issues and, on an aggregate, anonymized basis, to ensure the quality of service and improve their products.

Content Data Access and Use by Qlik

Qlik employees do not access a user's cloud content unless the user actively shares it with someone at Qlik (e.g. in a Support Services context). Only a specific, limited group of Qlik employees can access the storage where individual user content is located. In order for a Qlik team member to access data within the QCS environment, they must be on VPN or in a Qlik office and then log into a bastion environment, which isolates the production system onto a virtual environment. The bastion requires multiple layers of authentication (including MFA) using a laptop or desktop. The QCS environment is configured so that customer data is encrypted in transit, at rest, and at the application layer, additionally the QCS environment is logically separated from the user's laptop or desktop.

Architecture and Security

Hosting Locations

QCS is hosted through AWS. AWS shares the responsibility for the privacy of data as part of hosting services. The AWS Privacy Policy is available at: https://aws.amazon.com/privacy/.

Retention of Content Data

Users may at any time delete their applications and the associated content is controlled by the user. Once deleted by the user, all information hosted by Qlik in that application is deleted, with backups deleted after a period of time in accordance with Qlik's internal data retention rules. Qlik may delete dormant tenants (i.e. any tenant that is not associated to an active subscription for more than 12 months).

Data Privacy Management

With increasing privacy/data protection regulations, in particular the EU General Data Protection Regulation (GDPR), Qlik realizes that privacy is a significant concern for its customers and partners. Qlik takes this concern seriously and adheres to data protection laws by implementing both security- and privacy-by-design methods in its development process. The Qlik Product Privacy Policy addresses how data privacy is managed within the Qlik product portfolio.

Data Access

The QCS environment provides a platform that hosts QSB and Enterprise QSE. This platform enables customers to upload data and gain insight into that data. The type of data varies and is controlled by each customer. Based on the nature and extent of the service offering, users of this report are responsible for ensuring user access to the data is appropriately limited. SRE works proactively to maintain the availability and security of customer data throughout its service and implements separation of management and production traffic.