QlikTech Inc.

Report on QlikTech Inc.'s Qlik Cloud System Relevant to Security, Availability and Confidentiality

System and Organization Controls® (SOC) 3 Report

For the Period October 1, 2022 through September 30, 2023

QlikTech Inc.

Report on QlikTech Inc.'s Description of Qlik Cloud System Relevant to Security, Availability and Confidentiality

For the Period October 1, 2022 through September 30, 2023

Table of Contents

Section I.

Independent Service Auditors' Report Provided by KPMG LLP

KPMG LLP
1601 Market Street
Philadelphia, PA 19103-2499

Independent Service Auditors' Report

The Management of QlikTech Inc.:

Scope

We have examined management of QlikTech Inc.'s accompanying assertion titled "Management of QlikTech Inc.'s Assertion" (the Assertion) that the controls within QlikTech Inc.'s Qlik Cloud system (the System) were suitably designed and operating effectively throughout the period October 1, 2022 to September 30, 2023 to provide reasonable assurance that QlikTech Inc.'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*, in AICPA *Trust Services Criteria*.

QlikTech Inc. uses subservice organizations identified in management of QlikTech Inc.'s Attachment D - QlikTech Inc.'s Complementary Subservice Organization Controls (Attachment D). Management of QlikTech Inc.'s Attachment D indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at QlikTech Inc., to achieve QlikTech Inc.'s service commitments and system requirements based on the applicable trust services criteria. Management of QlikTech Inc.'s Attachment D presents the types of complementary subservice organization controls assumed in the design of QlikTech Inc.'s controls. Management of QlikTech Inc.'s Attachment D does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Management of QlikTech Inc.'s Attachment C - QlikTech Inc.'s Complementary User Entity Controls (Attachment C) indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at QlikTech Inc., to achieve QlikTech Inc.'s service commitments and system requirements based on the applicable trust services criteria. Management of QlikTech Inc.'s Attachment C presents the complementary user entity controls assumed in the design of QlikTech Inc.'s System. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

QlikTech Inc. 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 QlikTech Inc.'s service commitments and system requirements were achieved. Management of QlikTech Inc. has provided the accompanying Assertion about the suitability of the design and operating effectiveness of controls within the System. QlikTech Inc. is also responsible for preparing the Assertion, including the completeness, accuracy, and method of presentation of the Assertion; providing the services covered by the Assertion; selecting, and identifying in the Assertion, the applicable trust services criteria; identifying the risks that threaten the achievement of QlikTech Inc.'s service commitments and system requirements; and having a reasonable basis for the Assertion by performing an assessment of the suitability of the design and operating effectiveness of the controls within the System.

Service Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on the Assertion that controls within the System were suitably designed and operating effectively throughout the period to provide reasonable assurance that QlikTech Inc.'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 the examination to obtain reasonable assurance about whether the 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 QlikTech Inc.'s service commitments and system requirements
- assessing the risks that controls were not suitably designed or did not operate effectively to achieve QlikTech Inc.'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 suitably designed to provide reasonable assurance that QlikTech Inc. would achieve its service commitments and system requirements based on the applicable trust services criteria if those controls operated effectively
- testing the operating effectiveness of controls within the System to provide reasonable assurance that QlikTech Inc. achieved its 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 examination 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 suitability of the design and operating 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, the Assertion that the controls within QlikTech Inc.'s System were suitably designed and operating effectively throughout the period October 1, 2022 to September 30, 2023 to provide reasonable assurance that QlikTech Inc.'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 30, 2023

Section II.

Management of QlikTech Inc.’s Assertion

Management of QlikTech Inc.’s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within QlikTech Inc.’s Qlik Cloud system (the System) throughout the period October 1, 2022 to September 30, 2023 to provide reasonable assurance that QlikTech Inc.’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*, in AICPA *Trust Services Criteria*. Our description of the boundaries of the System is presented in our Attachment A – QlikTech Inc.’s Overview of Services and the System (Attachment A) and identifies the aspects of the System covered by the Assertion.

QlikTech Inc. uses subservice organizations identified in our Attachment D – QlikTech Inc.’s Complementary Subservice Organization Controls (Attachment D). Our Attachment D indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at QlikTech Inc., to achieve QlikTech Inc.’s service commitments and system requirements based on the applicable trust services criteria. Our Attachment D presents the types of complementary subservice organization controls assumed in the design of QlikTech Inc.’s controls.

Our Attachment C – QlikTech Inc.’s Complementary User Entity Controls (Attachment C) indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at QlikTech Inc., to achieve QlikTech Inc.’s service commitments and system requirements based on the applicable trust services criteria. Our Attachment C presents the complementary user entity controls assumed in the design of QlikTech Inc.’s System.

We have performed an evaluation of the suitability of the design and operating effectiveness of the controls within the System throughout the period October 1, 2022 to September 30, 2023 to provide reasonable assurance that QlikTech Inc.’s service commitments and system requirements were achieved based on the applicable trust services criteria. QlikTech Inc.’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 our Attachment B - QlikTech Inc.’s Principal Service Commitments and System Requirements (Attachment B).

We assert that the controls within the System were suitably designed and operating effectively throughout the period October 1, 2022 to September 30, 2023 to provide reasonable assurance that QlikTech Inc.’s service commitments and system requirements were achieved based on the applicable trust services criteria.

November 30, 2023

Attachment A

Management of QlikTech Inc.'s Description of the Boundaries of its Qlik Cloud System

Overview of Company and Services

QlikTech Inc.'s ("Qlik's" or "the Company's") Qlik's vision is a data-literate world, where everyone can use data and analytics to improve decision-making and solve their most challenging problems. Qlik offers real-time data integration and analytics solutions, powered by Qlik Cloud, to close the gaps between data, insights, and action. Qlik serves more than 38,000 active customers in over 100 countries.

Description of Services Provided

Qlik's cloud-based service offering, Qlik Cloud, provides data integration and analytics products for integrating, analyzing, and visualizing data. Customer data is hosted in Qlik's Amazon Web Services (AWS) multi-tenant, production environment. Customers use Qlik Cloud to connect to data and create analytic applications (dashboards). Qlik Cloud includes an array of analytics capabilities such as cataloging and dashboarding.

To use Qlik Cloud Service's products, customers start with a tenant onboarding email which includes entitlement to the product(s) they are trialing or have purchased. Once the Service Account Owner (SAO) has set up their tenant and their desired identity provider, additional users can be invited to the tenant so data can be uploaded and analytics content created.

Scope of the Report

The scope of this report is intended to provide specified parties with information about Qlik Cloud'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.

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 Qlik Cloud, and the financial, operational, and compliance requirements that Qlik has established for Qlik Cloud.

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 are described below:

Infrastructure

The supporting infrastructure consists of the following infrastructure, applications, and databases:

Infrastructure	Description
AWS (Subservice organization)	AWS directs and controls operations for infrastructure and also establishes and communicates policies and procedures and implements monitoring activities to help ensure compliance with these for all of the Qlik Cloud 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 Qlik Cloud 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, but are not limited to: • Elastic Compute Cloud (EC2) • Simple Storage Service (S3) • Elastic Load Balancer (ELB) • Identity Access Management (IAM) • GuardDuty • Config • DynamoDB • CloudFront • AWS Backup
GCP (Subservice organization)	Qlik utilizes the Google Cloud Storage service within the GCP platform to perform nightly backups of the AWS environment. From Oct 1, 2022 to August 1, 2023, GCP was used to back up one of the Qlik Cloud regions.
MongoDB Atlas	MongoDB Atlas is a database that is used to store data used in Qlik Cloud.

Software

The software consists of the following applications and tools:

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 Qlik Cloud.
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.
Concourse	Concourse is a Continuous deployment tool that schedules builds and other deployment-related tasks, including testing where required.
Launch Darkly	Launch Darkly is used for Feature Flag management in release development and management.
Configuration Management	
Palo Alto Prisma Cloud Compute Edition (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.
Terraform	Terraform is a tool for building, changing and versioning infrastructure.
Docker	Docker is a tool that packages, provisions and runs containers independent of the operating system.
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.
Multi-factor authentication (MFA) services	Access to production environments at Qlik requires strong MFA. Two MFA solutions are used at Qlik (OKTA, Inc. and Duo Security).

Software	Description
1Password	1Password is a password manager that restricts generic service accounts to appropriate personnel through the 1Password vault.
HashiCorp® Vault	HashiCorp Vault stores encryption keys and other sensitive configurations.
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 Qlik Cloud environment 24 hours per day, 7 days per week. They investigate and respond to issues and provide transparent managed security.
GitHub advanced security	A GitHub add-on for monitoring GitHub public repositories for secret and sensitive data.
InsightCloudSec	InsightCloudSec is a tool for monitoring cloud security posture and notifying Qlik of abnormalities.
Splunk	Splunk is a tool for collecting, analyzing and indexing security logs, such as system audit logs, and reporting on Qlik-defined, critical system events.
PagerDuty	PagerDuty is a notification platform that is used for alert management.
Prometheus	Prometheus is a centralized availability monitoring tool used for enterprise services.
Training and Awareness	
Skillsoft Percipio	Skillsoft Percipio is used to deliver security training modules to Qlik personnel, collect completed module results and remind users and management of incomplete modules.
InfoSec IQ	InfoSec IQ platform is used to deliver annual secure coding training to Qlik personnel.
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.

Software	Description
Endpoint Management	
JAMF	JAMF is the Endpoint Protection Platform for managing endpoints (Mac).
Ivanti	Ivanti is the Endpoint Protection Platform for managing endpoints (Windows).
Microsoft Intune	Intune is the Endpoint Protection Platform for managing endpoints (Windows).
CrowdStrike	CrowdStrike Endpoint Protection goes beyond traditional antivirus software and offers real-time threat prevention, endpoint detection and response, threat intelligence, and cloud-native architecture.
Web Application Firewall	
Signal Science	Signal Science is a web application firewall.
Incident Management	
FireHydrant	FireHydrant is a tool that is used as an incident management and response console.
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 Qlik Cloud.
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.
Concourse	Concourse is a continuous deployment tool; it schedules builds and other deployment-related tasks, including testing where required.
Configuration Management	
Palo Alto Prisma Cloud Compute Edition (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.
Terraform	Terraform is a tool for building, changing and versioning infrastructure.

Software	Description
Docker	Docker is a tool that packages, provisions, and runs containers independent of the operating system.
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.
Multi-factor authentication (MFA) services	Access to production environments at Qlik requires strong MFA. Two MFA solutions are used at Qlik (OKTA, Inc. and Duo Security).
1Password	1Password is a password manager that restricts generic service accounts to appropriate personnel through the 1Password vault.
HashiCorp Vault	HashiCorp Vault stores encryption keys and other sensitive configurations.
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 Qlik Cloud environment 24 hours per day, 7 days per week. They investigate and respond to issues and provide transparent managed security.
GitHub advanced security	A GitHub add-on for monitoring GitHub public repositories for secret or sensitive data.
InsightCloudSec	A tool for monitoring the cloud security posture and notifying Qlik of abnormalities
Splunk	Splunk is a tool for collecting, analyzing, and indexing security logs, such as system audit logs, and reporting on Qlik-defined, critical system events.
PagerDuty	PagerDuty is a platform that is used for alert management.
Prometheus	Prometheus is a centralized availability monitoring tool used for enterprise services.

Software	Description
Training and Awareness	
Skillsoft Percipio	Skillsoft Percipio 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.
Endpoint Management	
JAMF	JAMF is an endpoint protection platform responsible for Mac endpoints' anti-virus, data encryption, and data loss prevention.
Ivanti	Ivanti is an endpoint protection platform responsible for Windows endpoints' anti-virus, data encryption, and data loss prevention.
CrowdStrike	CrowdStrike is an endpoint protection platform for protecting endpoints' anti-virus, data encryption, and data loss prevention.
Web Application Firewall	
Signal Science	Signal Science is a web application firewall.
Incident Management	
FireHydrant	FireHydrant is a tool that is used as an incident management and response console.

People

Qlik is comprised of the following departments:

1. The X-team (Executive Management) – Responsible for overseeing company-wide activities, creating corporate level VSGs (Vision, Strategies, and Goals), measuring progress towards 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 Cloud & Technology Services – Responsible for defining Qlik's technology strategy, managing and maintaining the infrastructure for the cloud platform, and designing and developing solutions to address customer needs. The Cloud & Technology Services Global Product Technology Organization is comprised of:
  - Product Design
  - Engineering, including Cloud Product Development Platform
  - Quality Engineering, including Product Testing
  - Site Reliability Engineering (SRE)
  - Product Architecture & Research
  - Design and User Experience
  - Product Content & Media and Globalization
  - Program Management & Compliance
  - Security & Compliance, including Corporate Security and Compliance and Secure Software Development
- Data Business Unit – This business unit defines the product and business strategy for Qlik's Data Integration Products (Data Movement and Transformation, Governance and Data Quality) and supports critical product and business investments as part of the Data Integration go-to-market strategy. go-to-market strategy. The Data Business Unit is comprised of:
  - Product Management – Data
  - R&D – Data
  - Product Marketing – Data
- Analytic Business Unit – This business unit defines the product and business strategy for Qlik's Analytics Product and supports critical product and business investments as part of the analytics go-to-market strategy. The Analytic Business Unit is comprised of:
  - Product Management – Analytics
  - R&D – Analytics
  - Product Marketing – Analytics
  - Offering Management – Analytics
- Finance – Responsible for the financial aspects of Qlik, including budgeting, payroll, and accounts payable and receivable. Finance is comprised of:
  - Accounting
  - Global Procurement & Real Estate
  - Revenue Assurance & Operations
  - Financial Planning & Analysis
  - Tax & Treasury
- Other teams include Chief Operating Office, Chief Legal Office, Chief Marketing Office, Office of Strategy Management and Global Sales.

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. Qlik team members are required to complete, on an annual basis, a combination of Incident Response (IR), Business Continuity (BC) and/or secure coding training based on their role:

- SRE team members are required to review BC and IR documentation and also complete secure coding training.
- Developers are required to review IR documentation and complete the secure coding training.
- Information Security team members are required to review IR documentation.

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. Qlik has lockout policies configured to lock out a workstation after 10 minutes of inactivity and shut down a bastion session after 30 minutes of inactivity.

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 Cloud & Technology Service, Data Business Unit and Analytic Business Unit 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. Development of the system is not outsourced.

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 Qlik Cloud, GitHub, CircleCI and Kubernetes are used to promote new changes or 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 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. The primary backup process backs up customer data stored in Elastic File System (EFS) into AWS Backup nightly.

The secondary backup process replicates/duplicates that data to another region in the same geographical area:

- GCP is used for Asia-Pacific (AP) region from Oct 1, 2022 to August 1, 2023.
- AWS is used for AP (Sydney), Ireland (EU/eu-west-1), Singapore (ap-southeast-1) and Virginia (us-east-1) region, and, as of July 2023, new regions London (eu-west-2) and Frankfurt (eu-central-1).

The SRE team logs failed backups for investigation. Disaster recovery (DR) is tested at least annually and any deficiencies are documented for investigation, along with a mitigation analysis. The latest annual DR test was performed in Q4 2022.

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. SRE personnel use Jira 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 the availability of services and infrastructure. CloudWatch analyzes availability and change data and provides 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 Qlik Cloud. 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. For runtime protection and notifications, Qlik uses Twistlock, which uses machine learning to automatically build a 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

Qlik Cloud

Location of Data

Qlik utilizes AWS to operate Qlik Cloud in six networked data centers: Dublin, Ireland; Northern Virginia, USA; Sydney, Australia; London, UK; Frankfurt, Germany; and Singapore.

Personal Data Collection

The only personal data that Qlik receives relates to user/authentication information, which is then used for authentication and other product-related purposes, such as customer support. Qlik also processes statistical data on the use of Qlik Cloud to assist with troubleshooting issues and, on an aggregate, anonymized basis, to ensure the quality of service and improve their products. Personal data (content of which is controlled by the customer) may also be present within a customer's content (e.g. Qlik Apps), if the customer so chooses.

Content Data Access and Use by Qlik

Qlik employees do not access customer data. Qlik employees can only view a user's unencrypted cloud content if the tenant administrator of that account invites the Qlik employee into their tenant (e.g. in a Support Services context). The configuration of the Qlik Cloud environment ensures that customer data is encrypted in transit, at rest and at the application layer. Only a specific, limited group of Qlik employees can access the operational encrypted data stores where individual user content is located, but they will not be able to view it, as it can only be decrypted by the customer's unique encryption keys, to ensure access is limited to members of their tenant.

In a break-glass scenario (e.g. for restoration purposes), for a Qlik team member to access these encrypted data stores, they must be on the Qlik VPN or physically present in a Qlik office location and can only use their laptop or desktop. The team member must have access to a bastion environment, which is the isolated entry point to the production environments that requires multiple levels of authentication (including MFA). Mobile access authentication into the production environment is not authorized.

Customer Managed Keys

The Customer Managed Key capability is a cloud architecture technology that allows customers to supply their own encryption key to protect data stored in their Qlik Cloud tenant. The Customer Managed Key capability is available per tenant and gives customers the ability to manage encryption keys, e.g. rotate and revoke.

Architecture and Security

Retention of Content Data

Users may, at any time, delete their applications, which also deletes all information hosted by Qlik in that application; backups will be 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 Access

Qlik Cloud provides a platform that enables customers to upload, manage and gain insight into 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 maintains the availability and security of customer data throughout its service and implements separation of management and production traffic.

System Incident or Personal Data Incident Disclosures

There were no identified system or personal data incidents noted during the examination period that prohibited Qlik from meeting their security, availability and confidentiality commitments.

Attachment B.

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Qlik designs its processes and procedures related to its Qlik Cloud 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:

- Qlik Cloud 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 Qlik Cloud to help ensure continued availability. The DRP is tested at least annually to help ensure it is up-to-date.
- Qlik has implemented backup and recovery procedures to help ensure the availability and redundancy of data.
- 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.

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

- Qlik identifies and maintains confidential information to meet regulatory standards and the clients' objectives. Qlik only provides the infrastructure where the teams host their data. Qlik has established parameters to prevent a Qlik employee from accessing customer data.
- Qlik is responsible for maintaining the per-tenant encryption keys for accessing a customer's tenant when the customer is not using a Customer Managed Key. Qlik offers two options for encrypting the customer's data at rest within a Qlik Cloud tenant. One option allows the customer to supply their own encryption keys and other is where Qlik manages the encryption keys per customer tenant. In both options, Qlik users cannot access the customer's data in the tenant unless the customer has granted the Qlik users access.
- Qlik employees can only view a user's unencrypted cloud content if the tenant administrator of that account invites the Qlik employee into their tenant whether they are utilizing a Customer Managed Key or not.

Qlik establishes operational requirements that support the achievement of security, availability and confidentiality commitments and compliance with relevant laws and regulations, as well as 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 regarding 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. Qlik Cloud is not responsible for electronic commerce and it is not within the scope of the system. 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 Qlik Cloud.

Attachment C.

QlikTech Inc.’s Complementary User Entity Controls

Complementary User Entity Controls

The system was designed with the assumption that controls included in this section would be implemented by user entities (i.e. “customers”). In certain situations, the application of specific controls by the customer is necessary to achieve certain criteria included in this report. The complementary user entity controls presented below should not be regarded as a comprehensive list of all of the controls that should be employed by the user entity. The implementation of additional controls may be appropriate.

Controls Expected to be Implemented at User Entity Organizations	Complementary Criteria Ref. Number
Customers are responsible for provisioning user access to their enterprise account and managing the privileges assigned to their users.	CC 6.2
Customers are responsible for removing users from their enterprise account when the user is terminated or access is no longer required.	CC 6.2
Customers are responsible for reviewing and validating account access within their Qlik Cloud environment.	CC 6.1, CC 6.2, CC 6.4
Customers are responsible for disposal of data in their Qlik Cloud environment at termination or as needed.	C 1.2

Attachment D.

QlikTech Inc.’s Subservice Organizations and Complementary Subservice Organization Controls

Subservice Organizations and Complementary Subservice Organization Controls

Qlik Cloud uses subservice organizations, not subject to examination by KPMG LLP, to perform a range of functions. The following describes the subservice organization used by Qlik Cloud:

Subservice Organization	Function	Criteria Intended to be Met by the Controls of the Subservice Organization	Complementary Subservice Organization Controls	Qlik Cloud's Monitoring Procedures Over the Subservice Organization
Amazon Web Services (AWS)	Infrastructure and Software	CC3.2 CC6.4 CC6.5 A1.2 A1.3 C1.2	The following controls should be in place at AWS: • Provide risk assessments for data centers that identify assets, risks, vulnerabilities and the likelihood of threats occurring. • Provide policies/procedures for identifying, disposing of and destroying hardware. • Policies and procedures exist for managing system assets.	Management reviews AWS's SOC 2 report on an annual basis to review for complementary user entity controls, issues identified and controls currently in place. Management has the controls below defined as part of their vendor monitoring process:

Subservice Organization	Function	Criteria Intended to be Met by the Controls of the Subservice Organization	Complementary Subservice Organization Controls	Qlik Cloud's Monitoring Procedures Over the Subservice Organization
			• Policies and procedures exist to ensure that physical access to facilities housing information systems is restricted to authorized personnel. • Policies and mechanisms are in place to help ensure that infrastructure and corresponding operating systems are monitored for incidents. • Physical access to restricted areas of the facility is protected by walls with non-partitioned ceilings, secured entry points and/or manned reception desks. • Provisioning of physical access to facilities housing information systems requires approval from appropriate personnel.	9.2-1 Contracts or Master Service Agreements (MSAs) with vendors and service providers include a service definition, statement of delivery, licensing arrangements, code ownership, intellectual property rights and compliance, privacy and confidentiality requirements. 9.2-4 Qlik performs risk assessments of Qlik Cloud third-party vendors (including assessments of the vendors' compliance with Qlik's Vendor Information Security Standard) and performs an annual review of vendor assurance reports issued for critical third-party vendors, including reviewing the vendors' performance against agreed-upon Service Level Agreements.

Subservice Organization	Function	Criteria Intended to be Met by the Controls of the Subservice Organization	Complementary Subservice Organization Controls	Qlik Cloud's Monitoring Procedures Over the Subservice Organization
			• De-provisioning of physical access to facilities housing information systems requires approval from appropriate personnel. • Provide nightly backups and monitoring of backups. • Fire detection and suppression systems are implemented and tested at appropriate intervals. • Temperature and humidity levels of data halls are monitored and maintained at appropriate levels. • Uninterruptible power supplies (UPS) and generators have been installed to support critical systems in the event of a power disruption or failure.	A1.1-1 Qlik uses Kubernetes to generate alerts when capacity/usage thresholds on the system have been exceeded and reallocate resources where necessary.

Subservice Organization	Function	Criteria Intended to be Met by the Controls of the Subservice Organization	Complementary Subservice Organization Controls	Qlik Cloud's Monitoring Procedures Over the Subservice Organization
GCP (From Oct 1, 2022 to August 1, 2023)	Backup	CC6.4 CC6.5 A1.2	The following controls should be in place at GCP: • Policies and procedures exist to ensure that physical access to facilities housing information systems is restricted to authorized personnel. • Physical access to restricted areas of the facility is protected by walls with non-partitioned ceilings, secured entry points and/or manned reception desks. • Provisioning of physical access to facilities housing information systems requires approval from appropriate personnel.	Management reviews daily automated backup verifications. Management reviews GCP's SOC 2 report on an annual basis to review for complementary user entity controls, issues identified, and controls currently in place. Management has the controls below defined as part of their vendor monitoring process: 9.2-1 Contracts or MSAs with vendors and service providers include a service definition, statement of delivery, licensing arrangements, code ownership, intellectual property rights and compliance, privacy and confidentiality requirements.

Subservice Organization	Function	Criteria Intended to be Met by the Controls of the Subservice Organization	Complementary Subservice Organization Controls	Qlik Cloud's Monitoring Procedures Over the Subservice Organization
			• De-provisioning of physical access to facilities housing information systems requires approval from appropriate personnel. • Policies and mechanisms are in place to help ensure that infrastructure and corresponding operating systems are monitored for incidents. • Provide nightly backups and monitoring of backups. • Fire detection and suppression systems are implemented and tested at appropriate intervals. • Temperature and humidity levels of data halls are monitored and maintained at appropriate levels.	9.2-4 Qlik performs risk assessments of Qlik Cloud third-party vendors (including assessments of the vendors' compliance with Qlik's Vendor Information Security Standard) and performs an annual review of vendor assurance reports issued for critical third-party vendors, including reviewing the vendors' performance against agreed-upon Service Level Agreements.

Subservice Organization	Function	Criteria Intended to be Met by the Controls of the Subservice Organization	Complementary Subservice Organization Controls	Qlik Cloud's Monitoring Procedures Over the Subservice Organization
			• UPS and generators have been installed to support critical systems in the event of a power disruption or failure.	
Expel	System Monitoring	CC6.8	The following controls should be in place at Expel: A monitoring environment is used to collect data from system infrastructure components, monitor for potential security threats, and investigate issues and send alerts to the SRE team, if needed. The system restricts the ability to remove system information or transmit or move system information to other systems or networks.	Management has the controls below defined as part of their vendor monitoring process: 6.8-3 On at least an annual basis, the SRE team undergoes an IR test. The results of the test are documented in a ticket and reviewed with the SRE team for lessons learned and performance improvement opportunities. 9.2-1 Contracts or MSAs with vendors and service providers include a service definition, statement of delivery, licensing arrangements, code ownership, intellectual property rights and compliance, privacy and confidentiality requirements.

Subservice Organization	Function	Criteria Intended to be Met by the Controls of the Subservice Organization	Complementary Subservice Organization Controls	Qlik Cloud's Monitoring Procedures Over the Subservice Organization
				9.2-4 Qlik performs risk assessments of Qlik Cloud third-party vendors (including assessments of the vendors' compliance with Qlik's Vendor Information Security Standard) and performs an annual review of vendor assurance reports issued for critical third-party vendors, including reviewing the vendors' performance against agreed-upon Service Level Agreements.