KYRIBA CORP.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE

FOREIGN EXCHANGE RISK MANAGEMENT:
CASH FLOW APPLICATION SERVICES SYSTEM

FOR THE PERIOD OF NOVEMBER 1, 2024, TO OCTOBER 31, 2025

Attestation and Compliance Services

INDEPENDENT SERVICE AUDITOR'S REPORT

To Kyriba Corp.:

Scope

We have examined Kyriba Corp.'s ("Kyriba") accompanying assertion titled "Assertion of Kyriba Corp. Service Organization Management" ("assertion") that the controls within Kyriba's Foreign Exchange Risk Management: Cash Flow Application Services (Cash Flow) system ("system") were effective throughout the period November 1, 2024, to October 31, 2025, to provide reasonable assurance that Kyriba's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality (applicable trust services criteria) set forth in TSP section 100, Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Kyriba uses a subservice organization for cloud hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Kyriba, to achieve Kyriba's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Kyriba 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 Kyriba's service commitments and system requirements were achieved. Kyriba has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Kyriba is responsible for selecting, and identifying in its assertion, the applicable trust services 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 systems 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 Kyriba'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 Kyriba's service commitments and system requirements based on the applicable trust services criteria.

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

Inherent Limitations

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that Kyriba'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 Kyriba's Cash Flow system were effective throughout the period November 1, 2024, through October 31, 2025, to provide reasonable assurance that Kyriba's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Schellman & Company, LLC

Columbus, Ohio
November 8, 2025

ASSERTION OF KYRIBA SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Kyriba Corp.'s ("Kyriba") Foreign Exchange Risk Management: Cash Flow Application Services (Cash Flow) system ("system") throughout the period November 1, 2024, to October 31, 2025, to provide reasonable assurance that Kyriba's service commitments and system requirements relevant to security, availability, processing integrity, and confidentiality were achieved. Our description of the boundaries of the system is presented below 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 November 1, 2024, to October 31, 2025, to provide reasonable assurance that Kyriba's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Kyriba's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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 November 1, 2024, to October 31, 2025, to provide reasonable assurance that Kyriba's service commitments and systems requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE FOREIGN EXCHANGE RISK MANAGEMENT: CASH FLOW APPLICATION SERVICES SYSTEM

Company Background

Kyriba Corp. is a software-as-a-service (SaaS) provider that offers a web-based treasury management application and internet data center services to medium and large-sized financial institutions and corporations. Kyriba was founded in 2000 and launched the Kyriba Business Application (KApp) SaaS application in 2002. In 2019 Kyriba further expanded the available service offerings with the acquisition of FiREapps, the Foreign Exchange (FX) Risk Management Platform. Kyriba's headquarter is located in Paris, France. Information security and several back-office services is performed in Paris, France. Customer care personnel are located in New York, New York; London, England; Paris, France; Tokyo, Japan; and Singapore. Development teams are located in Warsaw, Poland; London, England; and Paris, France.

Description of Services Provided

The Kyriba FX services (previously referred to as the FiREapps services) are a separate cloud offering that may be integrated with the Kyriba application through secure single sign on and APIs. FX products are purchased separately or included as part of a Kyriba enterprise subscription.

Kyriba's FX services are designed to help corporations optimize FX processes. These solutions are intended to help customers mitigate risk while increasing profitability and operational efficiencies. Kyriba develops and operates its FX management application in a SaaS model. Kyriba offers a hosted application to which clients subscribe, as well as ongoing services necessary to implement the application for clients and to address their needs with respect to FX management.

Kyriba provides its customers with scalable, adaptable, and extensible currency analytics solutions to provide insight into underlying currency data and increase the reliability of financial results. The Kyriba FX application provides customized workflows for balance sheet, cash flow, and income statements for their customers. The Foreign Exchange Risk Management: Cash Flow Application Services (Cash Flow) enables compatibility with other enterprise resource planning systems, performs data analysis for scheduled and ad-hoc needs, and enables customers to generate profit and loss, monetary asset, and liability reviews along with mapping and data derivations. The Cash Flow application delivers data collection, FX exposure, and FX hedging recommendations. Multi-user access and field-level user access controls are available within Cash Flow along with audit trail functionality.

Additionally, the Cash Flow application allows for system configurations based on entities, accounts, company codes, profit centers, cost centers, product lines, models, dates, or geography. There is user-defined reporting that is based on roles and preferred internal communication standards. There is also end-to-end workflow development, which starts by addressing unique file formatting issues and continues through mapping, data aggregation, data derivation, specialized reporting, and integration issues with internal systems.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Principal Service Commitments and System Requirements

The principal service commitments and system requirements related to security, availability, processing integrity and confidentiality of the Cash Flow system are documented and communicated in service level agreements (SLAs), the Kyriba product technology guide, and the publicly available website, and include the following:

Principal Service Commitments and System Requirements		
Trust Services Category	**Service Commitments**	**Related Requirements**
Security and Confidentiality	Kyriba will maintain adequate administrative, technical, organizational, and physical safeguards designed to ensure the security and confidentiality of customer data.	• Screen potential employees and perform background checks as part of the hiring process. • Enforce user authentication required via user identification (ID) and password, multi-factor authentication, and/or single sign-on. • Encrypt block and file data using a 256-bit encryption protocol before storing onto the disks and solid state drive (SSD)s in the storage system. • Implement industry standard / accepted intrusion prevention system that monitors network and system activities and produces reports and alerts. • Configure an external firewall used to filter open access from the Internet, block dangerous IP addresses, and control flows and communications with the Internet. • Perform penetration testing on Kyriba networks and application on an annual basis. • Implement a software security program that aligns Kyriba with secure software development practices provided by Open Web Application Security Project (OWASP) and SANS Institute. • Enforce physical access security to Kyriba's office premises to ensure that only authorized individuals have access. • Dispose of customer data after retention requirements have elapsed.

Principal Service Commitments and System Requirements		
Trust Services Category	**Service Commitments**	**Related Requirements**
Availability	System availability equals or exceeds 99.9% during each calendar month.	• Provide monitoring of system availability on an ongoing basis. • Perform weekly full and daily incremental backups of customer and Kyriba data with a ten-year retention period for full server backups. • Provide active/standby mode for backup and recovery of customer data in which data and servers are replicated. • Use reasonable efforts to ensure that the minimum necessary services are carried out with a recovery time objective (RTO) of six hours and recovery point objective (RPO) of two hours. • Maintain and regularly test an enforced disaster recovery plan.
Processing Integrity	Kyriba's system is committed to consistently executing its intended functions – such as FX data analysis for scheduled and ad-hoc needs, cash forecasting, liquidity management, and transaction processing – accurately and reliably, in accordance with Kyriba's processing integrity policies.	• Provide Kyriba connectivity via a secure link over the Internet to send and receive files to and from financial institutions. • Provide access to Kyriba customer support via telephone, e-mail, and Kyriba social customer portal. • Respond to processing integrity incidents based on the assigned priority level and within the timeframes defined within the SLA. • Isolate the data for each customer based on the concept of data segregation using a data domain unique identifier.

In accordance with Kyriba's assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to system users, in each individual case.

Infrastructure

As noted, Kyriba has outsourced infrastructure resource requirements for the Cash Flow application to Microsoft Azure (Azure). Kyriba does not own or maintain any of the hardware located in the Azure data centers, and operates under a shared security responsibility model, where Azure is responsible for the security of the underlying cloud infrastructures (e.g., physical infrastructure, components from the host operating system, storage, etc.) Kyriba is responsible for securing the Cash Flow system deployed in Azure (e.g., identity access management, network firewall configurations, applications, etc.).

Kyriba utilizes multiple Azure regions and availability zones within each region for redundancy and disaster recovery purposes to help ensure the availability of the application. Development, testing, and production environments including customer data reside within Azure. For users to access the application, Kyriba provides a web-based application that is accessible from any internet browser.

The in-scope infrastructure consists of multiple systems as shown in the table below:

Primary Infrastructure			
Production System	**Business Function Description**	**Platform**	**Physical Location**
Identity Management Platform	Okta identity management platform is utilized to authenticate access to production systems.	Okta	Azure
Cloud Network Domain	Active Directory is utilized for managing user access credentials for internal production systems.	Microsoft Windows	
Production Network Domains	Active Directory is utilized for managing internal and external user credentials for the Cash Flow.		
Production Server Operating Systems	Production server operating systems supporting the Cash Flow.		
Databases	Databases used to store and maintain data that supports the Cash Flow.	Microsoft SQL	Azure
Azure Management Console	Web portal provided by the subservice organization used for management of virtual machines and networking systems.	Azure	

Software

Supporting software utilized by Kyriba to deliver services for the Cash Flow system includes the following:

- Jira ticketing system is utilized for onboarding and offboarding of employees, and for documenting incident and change management activities.
- Salesforce ticketing system is utilized for documenting and tracking customer care support tickets.
- Azure Web Application Firewall (WAF) is utilized for filtering unauthorized inbound network traffic from the Internet.
- Microsoft Defender is utilized for malware protection and antivirus monitoring.
- Palo Alto is utilized as a virtual private network (VPN) client for establishing encrypted remote sessions.
- Azure Monitoring and Opsgenie are utilized for availability monitoring / alerting of Information Technology (IT) personnel of infrastructure and systems.
- Tenable Nessus is utilized for automated vulnerability scanning of the production environment.
- Bitbucket / Github is utilized as version control software for maintaining the source code.
- Axonius, Cycode, and Panorama are used to monitor changes committed to the version control software for the separation of change management duties.
- Vault is utilized as a password management system.
- SENATORFX by Seculux is used to administer physical access to the Paris office facility.
- Cohesity and NetApp are used to schedule and manage data backups and geo-redundant data.

People

The following personnel are involved in the operation and maintenance of the Cash Flow system:

Area of Operation	Responsibilities

Product Team	• Product definition (together with product marketing):
	  ○ Anticipating the evolution of the market/competition
	  ○ Analyzing client enhancement requests
	• Product engineering:
	  ○ Designing new functionalities
	  ○ Writing the detailed functional specifications and maintaining specifications through change requests
	  ○ Managing the life cycle of change requests in sync with the overall release plan
	  ○ Coordinating with the build team in reviewing and controlling development and test planning
	  ○ Planning and controlling the deployment of releases, service packs, patches on prototyping, preproduction, and production platforms
	  ○ Writing the product documentation
	  ○ Transferring product knowledge to the customer care, sales, and consulting teams
	• Quality acceptance (QA):
	  ○ Monitoring the tests performed by the test team
	  ○ Performing parallel acceptance testing of new releases, service packs, and patches
	  ○ Analyzing pending defects and reviewing impact descriptions / severity to determine the correction priority
	  ○ Determining which errors to correct/changes to implement through service packs
	• Support:
	  ○ Customer care: analyzing the client cases that were escalated by customer care
	  ○ Presales: helping the sales teams answer request for proposals (RFPs), participating in marketing events
	  ○ Client implementation: helping implementation consultants design the setup of business rules

Area of Operation	Responsibilities

Engineering – Build Team	• Planning:
	  ○ Planning developments
	  ○ Planning build deliveries
	• Architecture:
	  ○ Identifying the necessary low-level components
	  ○ Designing and managing database upgrades
	• Development:
	  ○ Developing the low-level components to be used in functional developments
	  ○ Developing functional features
	  ○ Analyzing and optimizing performances
	  ○ Analyzing client cases
	• Package upgrades:
	  ○ Assembling and controlling new releases, service packs, patches
	  ○ Testing deployment scripts
	  ○ Deploying new releases, service packs, patches on test and integration platforms

Engineering – Test Team	• Test:
	  ○ Performing unit and integration, functional, and technical tests
	  ○ Automating tests
	  ○ Documenting tests

Technical Operations (TechOps)	• Platform operations:
	  ○ Managing application delivery to clients according to service level agreements (SLAs)
	  ○ Handling the incident escalation process across internal teams and external service providers
	  ○ Monitoring and troubleshooting platforms
	  ○ Analyzing and optimizing performance and plan capacity
	• IT service processes:
	  ○ Managing platform design and configurations
	  ○ Updating internal documentation to keep track of changes
	  ○ Interacting with the product team to plan and follow-up on changes (patch / service pack deployment, maintenance operations impacting availability, etc.)
	  ○ Planning, implementing, maintaining, and supporting automation routines
	  ○ Planning service recovery
	• Data center management:
	  ○ Managing relationships with the host provider, account operations managers, technical team leaders, and support helpdesks
	  ○ Leading steering committees and technical meetings
	  ○ Reviewing the monthly reports, comparing reported SLAs with the Kyriba internal monitoring results, investigating discrepancies, proposing requesting improvements and changes, and requesting credits
	• Architecture design and implementation:
	  ○ Designing, analyzing, and improving the application architecture
	  ○ Defining and validating new technical foundations

Area of Operation	Responsibilities

Risk and Compliance	• Compliance:
	  ○ Managing the day to day activities of the risk and compliance life cycle
	  ○ Creation and management of security policies and processes
	  ○ Managing and monitoring of employee security compliance
	  ○ Managing and monitoring of the security awareness training program
	  ○ Managing, coordinating, and enforcing compliance requirements
	• Risk management:
	  ○ Managing the risk assessment process
	  ○ Completing annual corporate risk assessment
	  ○ Completing risk assessments and enforcing risk mitigation plans
	  ○ Providing risk and compliance consultation to the organization

Customer Care	• Client support:
	  ○ Registering client queries in ServiceNow, tracking progress, and informing clients of the status / timing of resolutions
	  ○ Analyzing client site configurations and interfaces between the client information system and the Kyriba system
	  ○ Providing a single point of contact for client support problems and related issues
	  ○ Responding to client inquiries relating to software functionality
	  ○ Escalating obstacles influencing the timely resolution of client requests
	  ○ Providing feedback to the product team & development teams
	  ○ Producing a weekly report including statistics
	  ○ Refining support procedures to optimize the efficiency of the Kyriba support
	• Client account management:
	  ○ Opening / closing client accounts and service accounts in accordance with client contracts
	  ○ Opening / closing bank connections in accordance with client contracts

Procedures

Documented policies and procedures are in place to guide personnel in security topics related to access management including acceptable use, authentication requirements, and password management.

Access and Authentication

The in-scope systems, including Okta, the Azure portal, production servers and databases, and the Cash Flow application, are configured to authenticate users via Azure Active Directory (AAD). Additionally, the production systems are configured to enforce multi-factor authentication with Okta. Direct access to the production servers and databases requires the use of secret passwords known only to authorized personnel and stored within the Azure portal. A monitoring application is configured to monitor access related events including administrator logons and failed login attempts and configured to notify IT personnel for review. Administrative access to the in-scope systems is restricted to user accounts accessible by authorized personnel.

Access Management

A formal process has been established for managing user accounts and controlling access to Kyriba resources within the production environment. When a new employee is hired, onboarding requirements are documented within a new hire checklist and user access provisioning is documented within an automated ticketing system. Access requests are initiated by HR and permissions are granted based on the requirements of the job role as authorized and approved by a manager before being provisioned. Upon termination, IT personnel remove system

access rights to ensure that employees do not retain any access permissions. The deprovisioning is tracked within a termination checklist and a ticket.

Customer service representatives (CSRs) are provisioned access to the customer environment within the cash flow application with explicit documented approval of the customer. Access is granted for a specified time interval based on the expected need and ongoing support for the customer account. CSR assignments are made with a terminating date for access after which the CSR will no longer have access to the customer instance.

Remote Access

Remote access to the corporate network is restricted through an encrypted VPN governed through the central firewall to ensure the privacy and integrity of the data passing through the network. Users are authenticated via a user account and password before establishing a VPN session. Administrative access is restricted to authorized personnel.

Change Management

Documented change management policies and procedures are in place to guide personnel in the change control practices from initiation of the change request to implementation. Change requests are initiated for multiple reasons including, but not limited to, changes in response to an incident or problem, introduction of new functionality, or infrastructure upgrade.

An automated ticketing system is utilized to centrally maintain, manage, and monitor application and infrastructure changes through implementation. Development and QA tasks, including testing and approvals are documented, and changes are reviewed and approved prior to implementation. Kyriba employs continuous integration with the use of automated development and deployment platforms. Release notes are documented and available on the customer portal for users and management regarding application changes and maintenance.

A source code repository is utilized to manage code and provide rollback capabilities to review the previous versions of code when changes impair system operation. Logical access controls are in place to restrict write access privileges to source code libraries within the version control software to authorized personnel. The ability to promote application code changes into the production environment is restricted to authorized personnel. Source code and administrative privileges within the source code repository are restricted to user accounts accessible by authorized personnel. The source code repository is configured to automatically create a build every time a developer commits code. Cycode and Axonius have been integrated with the source code repository to identify users with access to implement changes (which requires authorized users with admin access to the cloud domain). Cycode compares the accounts with commits performed in the source code repository for separate change management duties. If a developer has access to promote application code changes into the production environment (code commits to master branch) an automated event is generated and sent to the Splunk where security personnel is alerted to review the changes committed to ensure the change was authorized.

The version control software requires a code review and approval prior to merging code. In addition, the continuous integration platform is configured to automatically perform testing on certain application changes and a deployment tool is used to assist in the application deployment process. Change committee meetings are held on a biweekly basis (twice weekly) to review and approve change requests that affect the system. The ticketing system uses an automated workflow to enforce review and approval from the change committee prior to implementation. Development and test environments are logically and physically segregated from the production environment.

Data Backup

Kyriba subscribes to Azure for automated structured query language (SQL) Server and Cosmos database backup and replication services. Access to administer and configure database backup and replication services is restricted to authorized personnel with access to the Azure Portal. Azure SQL Server is configured to automatically perform a full daily snapshot of the production databases and encrypt data at rest utilizing keys managed through Azure Key Vault. These snapshots are retained for 35 days. The Cosmos databases are automatically backed up every four (4) hours and the most recent two backups are available for restoration. Both the SQL Server and Cosmos database are replicated in a geographically redundant manner for enhanced availability to permit the resumption of operations in the event of a disaster. Backup restoration tests are performed on an as needed basis through an automated script by request to Azure support.

Disaster Recovery

Disaster recovery plans are in place to guide personnel in the procedures to protect against disruptions caused by an unexpected event and the recovery of system operations. Disaster recovery plans are tested on at least an annual basis to help ensure that the system is operating in accordance with principal service commitments and requirements.

The integrity of backup media is tested on an as needed basis, to ascertain the integrity of the backup media.

Azure Network Security Groups and Rules

Azure network security groups are configured to provide security for the production environment maintained within Azure. The security groups manage incoming traffic by analyzing the data packets and determining whether they should be allowed based on the defined rules. Kyriba is responsible for the initial configuration and maintenance of the ruleset. Administrative access privileges to manage the security groups are restricted to authorized personnel with access to the Azure management console.

Encryption

To protect data while in transit, communication sessions between the application and its users are transmitted utilizing Secure Shell (SSH), hypertext transfer protocol secure (HTTPS), and transport layer security (TLS) encryption protocols.

Vulnerability Management

Kyriba utilizes a third-party vulnerability tool to perform internal and external vulnerability assessments of the production environment and web application on a monthly basis. Remediation activities of any identified vulnerabilities are tracked through resolution within a ticketing system. In addition to vulnerability scans, Kyriba utilizes a third-party specialist to perform external penetration tests of the production environment on an annual basis. Similar to the vulnerability scans, the remediation plans for findings are tracked through resolution within the ticketing system.

Network Security Devices

Kyriba relies on a threat detection service to monitor and analyze the production systems for malicious or unauthorized behavior. The threat detection service is configured to communicate findings to IT personnel of suspected attacks for review.

Incident Response

Incident response and escalation policies and procedures are in place to manage incidents impacting the business. The incident response process defines activities for identifying and mitigating security breaches and managing communications with Kyriba personnel and customers. The process also has defined roles, including an incident coordination team and a computer emergency response team (CERT), to outline the responsibilities for managing and investigating incidents. The details, including responses and resolutions, are tracked within a reporting template, and any incidents requiring a Cash Flow application change follow standard change control procedure and are documented within the ticketing system.

Data

Information (data) classification is designed to ensure information receives the required level of protection in accordance with its importance to the organization and to its customers. Kyriba information is classified as the following:

- Unclassified (class 1) – non-sensitive information available for external release (e.g., information accessible for external use such as marketing documentation and public facing website).
- Confidential (class 2) – information that is sensitive within the company and may be intended for use only by specified groups of Kyriba employees (e.g., policies, procedures, intracompany e-mails, customer sales agreements, customer and client information, personnel information, and Kyriba's employee organizational chart).

- Restricted (class 3) – information that is extremely sensitive and is intended for use only by named individuals within the company (e.g., strategic plans, financial results, capitalization table and personally identifiable information (PII)).

Kyriba takes reasonable precautions to protect data in its possession from loss, misuse and unauthorized access, disclosure, alteration, and destruction. Kyriba uses physical, electronic, and administrative security measures to protect data and limits access to data to those persons within the organization that have a specific business purpose for maintaining and processing the data or approved third-party vendors that are involved in the processing of the data. Individuals who have been granted access to data are made aware of their specific responsibilities to protect the security, confidentiality, and integrity of the data, and are provided training and instruction on how to do so as required.

In order to fulfill its foreign exchange risk management services, the Cash Flow application processes data files provided by customers, however, no personal data is included or tracked by the Cash Flow application. Customers are responsible for directly uploading and formatting data for use within the application, and only CSRs have controlled access to customer data with the explicit authorization from the customer. Kyriba encrypts any sensitive data while in transit through the use of transport layer security (TLS) encryption over hypertext transfer protocol secure (HTTPS) connections and file transfer protocol (FTP) sites for web communications with its customers.

Subservice Organizations

The cloud hosting services provided by Azure were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at Azure, alone or in combination with controls at Kyriba, and the types of controls expected to be implemented at Azure to achieve Kyriba's principal service commitments and system requirements based on the applicable trust services criteria.

Ref.	Control Activities Expected to be Implemented by Subservice Organization	Applicable Trust Services Criteria
CSOC.01	Azure is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the production systems reside.	CC6.1 - CC6.3, CC6.5, CC6.6
CSOC.02	Azure is responsible for ensuring the following: • Access to the facility hosting the production systems is restricted to personnel or visitors authorized by the tenant and reviewed periodically by management for appropriateness • Access to the facility hosting production systems is not granted to personnel or visitors unless authorized by the tenant • Access to the facility hosting the production systems is removed/disabled upon tenant notification • Access to the facility is controlled via a keycard system or other preventative access control systems • Access to the entrances and sensitive areas is monitored and/or recorded by security cameras	CC6.4
CSOC.03	Azure is responsible for ensuring that decommissioned hardware is inventoried, stored in a secure location, and destroyed and/or wiped in accordance with established requirements.	CC6.5
CSOC.04	Azure is responsible for implementing controls to restrict and protect information during transmission, movement, and removal from the underlying storage devices for its cloud hosting services.	CC6.7

Ref.	Control Activities Expected to be Implemented by Subservice Organization	Applicable Trust Services Criteria
CSOC.05	Azure is responsible for ensuring controls are implemented to prevent or detect and act upon the introduction of unauthorized or malicious software on the underlying network and virtualization management software and infrastructure for its cloud hosting services where production systems reside.	CC6.8
CSOC.06	Azure is responsible for ensuring environmental protection controls are in place to meet Kyriba's availability commitments and requirements.	A1.2

Complementary User Entity Controls

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, processing integrity, and confidentiality categories are applicable to the Foreign Exchange Risk Management: Cash Flow Application Services system.