KYRIBA CORP.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE

TREASURY MANAGEMENT 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 Treasury Management Application Services 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 various subservice organizations for colocation services, cloud hosting services, and market data feed 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 organizations. 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.

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 Treasury Management Application Services 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") Treasury Management Application Services 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 TREASURY MANAGEMENT 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 in 2002. 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

Kyriba provides a web-based treasury management application to medium and large-sized financial institutions and corporations. The core of the Kyriba application (Treasury Management Application Services) is a multiple tier, component-based architecture and a framework that integrates third-party solutions, existing systems, and evolving technology standards. The Kyriba application enables its customer's access to electronic banking, e-payment, cash forecasting, liquidity management, foreign exchange (FX) management, and collection processing, and reporting in a multinational and multi-banking environment.

Kyriba has relationships with various partners to deploy the Kyriba application and utilizes different hosting providers depending on those relationships. In instances where Kyriba has a direct contract with the client, Kyriba utilizes various hosting providers, and monitors system availability according to the service level agreement (SLA).

The Treasury Management Application Services system provides transaction processing for user-initiated transactions. User entities are responsible for the procedures, by which transactions are initiated, authorized, corrected as necessary, and transferred to reports and other information presented to them; additionally, user entities are responsible for the procedures and controls governing the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, and report transactions processed within the Treasury Management Application Services system; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for those user entities.

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.

[Intentionally Blank]

Principal Service Commitments and System Requirements

The principal service commitments and system requirements related to security, availability, processing integrity and confidentiality of the Treasury Management Application Services system are documented and communicated in service level agreements, 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. • The retention of confidential data in accordance with defined Kyriba policies.

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 electronic banking, e-payment, FX management, and collection processing – accurately and reliably, in a multinational and multi-banking environment, 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

The infrastructure supporting the Treasury Management Application services system is hosted within the following secured data center facilities:

- Equinix:
  - Saint-Denis, France
  - Pantin, France

- Amazon Web Services, Inc. (AWS):
    - Boardman, Oregon, United States
    - Paris, France
    - Dublin County, Ireland
    - Montreal, Canada
    - Northern Virginia, United States
    - Ohio, United States
    - Stockholm, Sweden

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	Okta identity management platform is utilized to authenticate Kyriba administrative access to production infrastructure and services.	Okta	Third-party data centers
Cloud network domain	Active Directory is utilized for managing user access credentials for internal production systems supporting the Kyriba application.	Microsoft Windows operating system	Equinix, AWS
Wallix Bastion Privileged Access Management (PAM) system	PAM system utilized for managing Kyriba administrative user access credentials for production systems supporting the Kyriba application.		
Production Server Operating Systems	Production server operating systems supporting the Kyriba application.	Microsoft Windows and Linux operating systems	
Databases	Databases used to store and maintain data that supports the Kyriba application.	Oracle, PostgreSQL, and MongoDB databases	
Kyriba Application	Front-end user interface, including reporting functionality for the Kyriba application.	Microsoft Windows and Linux operating systems	
Identity Management Platform - Keycloak	Keycloak identity management platform is used to identify and authenticate customer access to the Treasury Management Application. In addition, access to each customer's instance is still controlled by the customer and Kyriba does not have access.	Keycloak	Third-party data centers
AWS Management Console	Administrative web portal provided by the subservice organization used by Kyriba for the management of virtual machines and networking systems.	AWS	AWS

Supporting software utilized by Kyriba to deliver services for Treasury Management Application system includes the following:

- Jira ticketing system is utilized for onboarding and offboarding of employees, and for documenting incident and change management activities.

- ServiceNow ticketing system is utilized for documenting and tracking customer care support tickets.
- Wavefront and Opsgenie are utilized for availability monitoring / alerting of Information technology (IT) personnel of infrastructure and systems.
- Crowdstrike antivirus is utilized for malware protection and antivirus monitoring.
- Palo Alto firewalls are utilized for filtering unauthorized inbound network traffic from the Internet and providing intrusion prevention/detection system (IPS/IDS) monitoring services.
- Palo Alto is utilized as a virtual private network (VPN) client for establishing encrypted remote sessions.
- Splunk is utilized for security monitoring of in-scope system infrastructure.
- Tenable Nessus is utilized for automated vulnerability scanning of the production environment.
- Bitbucket / Github is utilized as version control software for maintaining the Kyriba application source code.
- Jenkins is utilized to orchestrate implementation of code changes.
- Axonius, Cycode, and Panorama are used to monitor changes committed to the version control software for the separation of change management duties.
- SENATORFX by Seculux is used to administer physical access to the Paris office facility.
- Vault is utilized as a password management system.
- 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 Treasury Management Application Services 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

Area of Operation	Responsibilities

Product Team	• 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

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 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

Area of Operation	Responsibilities

Technical Operations (TechOps)	• 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

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 Authentication and Authorization

The in-scope systems, including Okta identity management platform, the cloud network domain, production servers, databases, the Kyriba application and its reporting functionality, Keycloak, Wallix Bastion PAM system, and AWS management console, are configured to authenticate users via a user account and password. Additionally, the

AWS management console is configured to enforce multi-factor authentication utilizing Okta. User account password requirements are enforced on the in-scope systems that include minimum password length, minimum password history, password expiration intervals, password complexity, and invalid password lockout threshold. Administrative access to the in-scope systems is restricted to user accounts accessible by authorized personnel.

Access Requests and Access Revocation

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, user access provisioning is documented within the Jira 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, system administrators remove system access rights to ensure that employees do not retain any access permissions. The deprovisioning is tracked within a termination ticket via the Jira ticketing system. User access reviews are performed on a quarterly basis to ensure that system access is restricted and authorized.

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, and Kyriba reporting functionality.

An automated ticketing system is utilized to centrally maintain, manage, and monitor application, reporting functionality, 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 has 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.

Physical and Environmental Security

Office Facility

Kyriba maintains one office facility used to support the IT operations of the Treasury Management Application system. The multi-tenant office facility is owned by a third-party management company and located in Paris, France. Documented policies and procedures are in place that address physical security activities including granting and controlling physical access to the office facility. The main entrance to the office facility is monitored and controlled by a receptionist during business hours. Visitors are required to present a government issued identification card (ID) and sign into a visitor log prior to entering the office facility. While accessing the office facility, visitors are required to wear a visitor badge and be escorted by an authorized employee.

Access to and within the office facility is controlled by a badge access system, which maintains an archived log of access attempts traceable to specific badge access cards. Administrative access privileges to the badge access system are restricted to authorized personnel. Requests for badge access privileges to the office facility require management approval and are documented within the Jira ticketing system. Physical access to the office facility is revoked as a component of the employee termination process.

Data Center Facilities

The production infrastructure is located in third-party colocation data centers provided by Equinix, and a managed hosting data center provided by AWS. When an employee requires physical access to Equinix colocation data center facilities, a ticket is submitted by a senior manager on the third-party colocation data centers customer portals to document approval for the physical access request. On at least an annual basis, a review of physical access privileges to the colocation data center facilities is performed to help ensure that access is restricted to authorized employees.

AWS and Equinix are responsible for restricting physical access to facilities housing the in-scope systems.

Data Backup

Documented policies and procedures are in place to guide personnel in backup and recovery activities. The Cohesity automated backup system is configured to perform scheduled backups of production data and files for the colocation and managed hosting environments, respectively. Incremental backups of the Kyriba application files and databases are performed on a daily basis to a local backup server. In addition, full backups of Kyriba application files and databases are performed on a weekly basis to a local backup server. The automated backup systems are configured to monitor the status of data backup jobs and notify TechOps personnel upon failed backup jobs.

The automated backup systems are configured to replicate backup media to geo-redundant locations on a near real-time basis and retain backup media for ten years via Amazon Simple Storage Service (S3) Glacier for the colocation and managed hosting environments. The automated backup systems are configured to encrypt production database backups utilizing data at rest encryption to protect from unauthorized access.

Administrative access privileges to the automated backup systems are restricted to authorized users and shared accounts, in which the passwords are managed by the Vault password management software and restricted to authorized personnel.

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 a regular basis. On at least a quarterly basis, an IT infrastructure engineer restores the most recent backup for the colocation and managed hosting environments to a test environment to ascertain the integrity of the backup media.

Security Monitoring and Incident Response

Kyriba has installed Palo Alto firewall systems within the colocation and managed hosting environments to filter unauthorized inbound network traffic from the Internet and to only permit access defined by a firewall system rule. Firewall system administrators are authenticated via a user account and password before being granted access to perform firewall system administration tasks, including the modification of firewall system rules. Administrative access privileges to the firewall system are restricted to user accounts accessible by authorized personnel. Management reviews firewall system rulesets on a quarterly basis to ensure rules are up-to-date and to address any new threats.

Additionally, Kyriba has configured the Palo Alto software to operate as an IPS/IDS to inspect network traffic and notify TechOps personnel of possible or actual security breaches.

The Tenable Nessus automated vulnerability scanning tool is configured to scan the production environment on at least a monthly basis to identify threats and assess their potential impact to system security. Any security

vulnerabilities that are detected as part of the vulnerability scan are documented within the Jira ticketing system and investigated by TechOps personnel and monitored through resolution.

Additionally, Kyriba has engaged with a third-party vendor to perform penetration testing of the network and application on at least an annual basis.

Kyriba's incident management process identifies incidents and allows personnel to report and track the incident through resolution. The process is formally documented in order to guide personnel in the monitoring, documenting, escalation, and resolution of issues. Cloud operations personnel utilize the Jira ticketing system to document security incident details including the violation, responses, and resolutions. Incident details such as the description, priority, escalation, and resolution are tracked within each incident ticket. In addition to the documentation of incidents, weekly meetings are held to discuss incidents and corrective measures to help ensure that incidents are resolved.

Availability Monitoring

The Wavefront enterprise monitoring application is configured to monitor the Kyriba application performance and capacity levels on an ongoing basis. Opsgenie is utilized to send e-mail alert notifications to TechOps personnel when predefined events occur related to monitoring of items such as central processing unit (CPU) utilization, memory, and disk space. Additionally, Apache load balancers are utilized to direct incoming requests to an available server and distribute client workload across multiple servers to maximize system availability.

Market Data and Bank Feeds

The Kyriba application allows clients to retrieve bank statements for their cash accounts and market data from financial institutions and integrate this information into one system. Clients work with Kyriba to establish the interfaces with the client's bank in order to retrieve their data; however, clients are responsible for establishing their bank accounts on the Kyriba application.

Kyriba receives market data feeds (e.g., currency rates, interest rates, and security prices) through automated feeds that are transmitted on a daily basis from each of the third-party Market Data Feed Vendors. A certificate-based exchange protocol is used to authenticate that the market data feeds received by Kyriba are from authorized vendors. The Kyriba application is configured to send e-mail alert notifications to product team personnel regarding the completion status of the automated market data and bank feed import job on a daily basis. The product team reviews the Kyriba application to ascertain whether the market data feeds were successfully received and imported into the application. If the market data feed is not received as expected or if the market data feed is not successfully collected and integrated, the product team will research and resolve the discrepancy.

Product team personnel document and track processing integrity incidents, including market data and bank feed discrepancies, within the Jira ticketing system. Incident management meetings are held on a weekly basis to review these processing integrity incidents and help ensure the research and resolution of market data and bank feed discrepancies.

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.

Subservice Organizations

Kyriba utilizes the colocation services provided by Equinix, Inc. (Equinix), the cloud hosting services provided by AWS, and the market data feed services provided by Blackrock Cachematrix, Crane Data, Reuters, Six Financial Information, and Xignite (hereby collectively referred to as the "Market Data Feed Vendors"). Kyriba's Treasury Management Application Services system is designed with the assumption that certain controls will be implemented by the subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the control objectives related to Kyriba's Treasury Management Application Services system to be solely achieved by Kyriba's control activities. Accordingly, subservice organizations, in conjunction with the Treasury Management Application Services system, should establish their own internal controls or procedures to complement those of Kyriba.

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

Ref.	Control Activities Expected to be Implemented by Subservice Organizations	Applicable Trust Services Criteria
CSOC.01	AWS 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	The Market Data Feed Vendors are responsible for ensuring that logical security over access to the data feed software is restricted to authorized personnel.	CC6.1 - CC6.3
CSOC.03	Equinix and AWS are responsible for restricting physical access to facilities housing the in-scope systems to authorized personnel.	CC6.4, CC6.5
CSOC.04	The Market Data Feed Vendors are responsible for ensuring that physical access to the market data vendor office facilities and data centers are restricted to authorized personnel.	CC6.4
CSOC.05	The Market Data Feed Vendors are responsible for ensuring that only authorized program changes are made to the data feed software and are subject to testing and approval prior to implementation into the production environment.	CC8.1
CSOC.06	Equinix and AWS are responsible for ensuring environmental protection controls are in place to meet Kyriba's availability commitments and requirements.	A1.2
CSOC.07	The Market Data Feed Vendors are responsible for ensuring that issues or significant events related to data feeds are reported to Kyriba by authorized personnel in a timely manner.	PI1.2, PI1.3

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 Treasury Management Application Services system.