KUBRA Data Transfer Ltd

System and Organization Controls Report (SOC 3®) - iDoxs® Platform

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls
For the period of January 1, 2024 – December 31, 2024

Threat IQ
Committed to keeping you secure. ALWAYS

www.threatiq.io 1 (866)-837-0773

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations
™

Contents

Section I: Independent Service Auditor's Report....3
Section II: Assertion of KUBRA Data Transfer LTD.'s Management....7
Section III: Description of KUBRA Data Transfer LTD.'s iDoxs® System....10
Infrastructure 12
Software 12
People....12
Data 14
Procedures....14
Communications 15
Monitoring 16
Risk Assessment 16
Control Activities....17
Complementary Controls at User Organizations 20
Subservice organization controls related to the Trust Services Principles. 23
Management Response to Noted Exceptions 25

Section I: Independent Service Auditor's Report

Threat IQ
Committed to keeping you secure. ALWAYS

Mr. Gavin Pinho
VP, Information Security, Privacy and Risk Management
KUBRA Data Transfer Ltd.
5050 Tomken Rd
Mississauga, Ontario L4W 5B1

Scope

We have examined KUBRA Data Transfer Ltd.'s (the "Company") accompanying description of its iDoxs® system found in Section III titled "KUBRA Data Transfer Ltd.'s Description of its iDoxs® System" (the "description"). This was performed throughout the period of January 1, 2024 to December 31, 2024 (the "period") based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (the "description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period of January 1, 2024 to December 31, 2024. These examinations aim to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, Processing Integrity, and Privacy (the "applicable trust services criteria") set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Complementary user entity controls

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The description presents the Company's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the Company's controls. 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 controls.

Subservice organizations

The Company uses a subservice organization to provide data center and cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The description presents the Company's controls, the applicable trust services criteria, and the types of complementary subservice organization control assumed in the design of the Company's controls. The description 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

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

Service auditor's responsibilities

Our responsibility is to express an opinion on the description and the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with the 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, in all material respects, the description is presented by the description criteria. This includes determining whether the weather controls stated therein, were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included the following:

- 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 KUBRA iDoxs's platform 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 KUBRA iDoxs's platform commitments and system requirements based on the applicable trust services criteria

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

Service Auditor's Independence and Quality Control

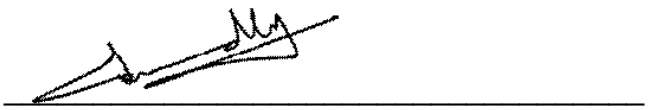
We are required to be independent and to meet our other ethical responsibilities in accordance with the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants. We have complied with those requirements. We applied the Statements on Quality Control Standards established by the AICPA and the International Standards on Quality Management issued by the IAASB and, accordingly, maintain a comprehensive system of quality control.

Inherent limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Furthermore, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or due to a potential deterioration in the degree of compliance with the policies or procedures.

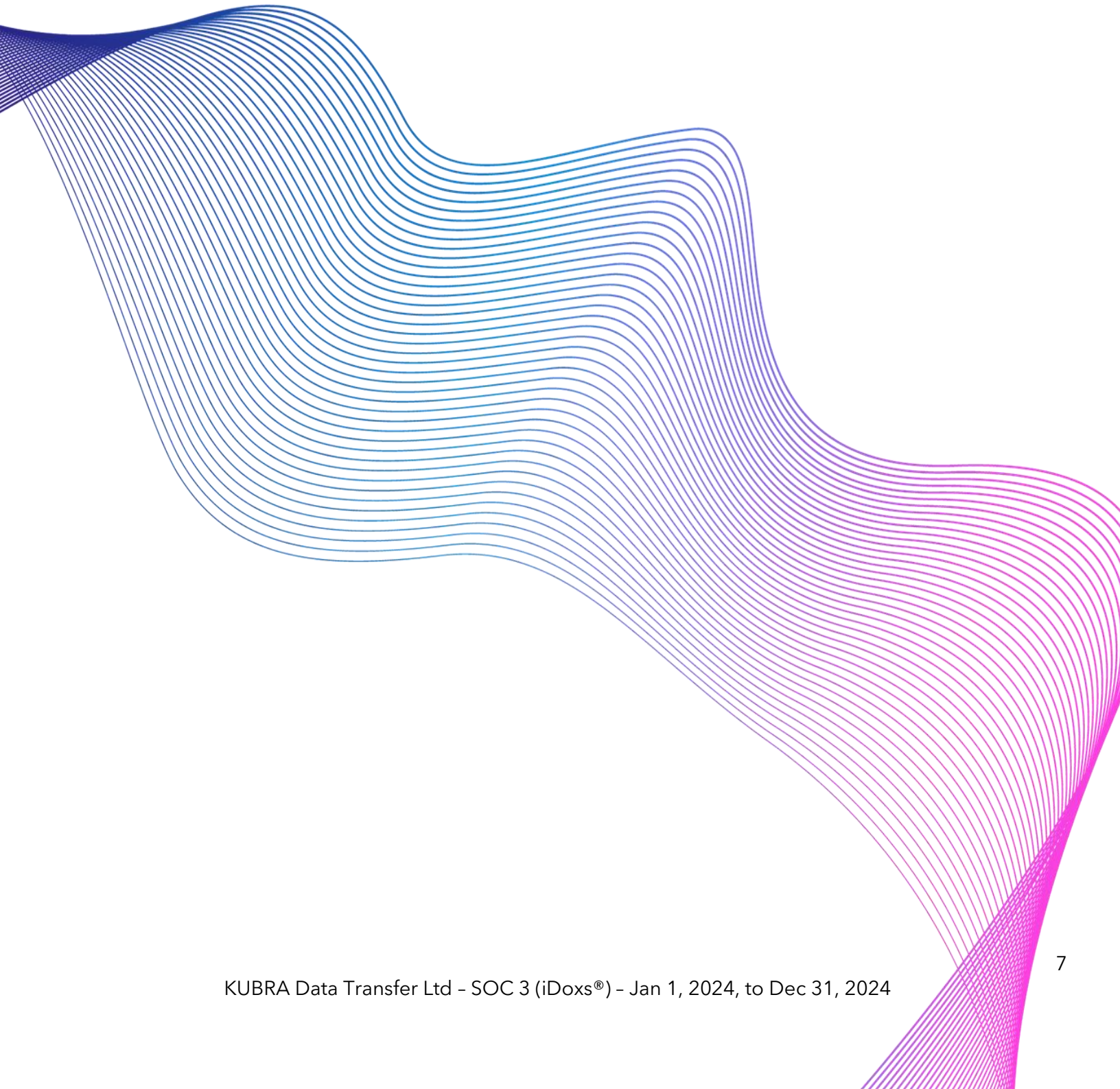
Opinion

In our opinion, management's assertion that the controls within KUBRA iDoxs's platform were effective throughout the period January 1, 2024 to December 31, 2024, to provide reasonable assurance that KUBRA iDoxs's platform commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.



Sudheendran Cheenikkal, CPA, CMA, AICPA
TIQ Accounting Professional Corporation
February 7th, 2025

Section II: Assertion of KUBRA Data Transfer LTD.'s Management



Section II: Management's Assertion of KUBRA Data Transfer Ltd.

We have prepared the description of KUBRA Data Transfer Ltd.'s (the "Company") iDoxs® system entitled "KUBRA Data Transfer Ltd.'s Description of Its iDoxs® System" (the "description") for processing user entities' transactions throughout the period January 1, 2024, to December 31, 2024 (the "period") for user entities of the system during some or all of the period and their auditors who audit and report on such user entities' financial statements or internal control over financial statement reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves when assessing the risks of material misstatement of user entities' financial statements.

The Company uses a subservice organization for data center hosting services when processing user entities transactions. The description includes only the control objectives and related controls of the Company and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organization.

The title description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls, assumed in the design of the Company's controls, are suitably designed, and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

1) The description fairly presents the Company's iDoxs® system made available to user entities of the system during some or all the period for processing user entities' transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were the description:

a) Presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable:
   i. The types of services provided, including, as appropriate, the classes of transactions processed.
   ii. The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.
   iii. The information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
   iv. How the system captures and addresses significant events and conditions other than transactions.
   v. The process is used to prepare reports and other information for user entities.
   vi. The services performed by a subservice organization, if any, including whether the carve-out or the inclusive method has been used with them.
   vii. The specified control objectives and controls designed to achieve those objectives include, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the controls.
   viii. Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

b) Includes relevant details of changes to the iDoxs® system during the period covered by the description.

c) Does not omit or distort information relevant to the system while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors and may not, therefore, include every aspect of the iDoxs® system that each user entity of the system and its auditor may consider important in its environment.

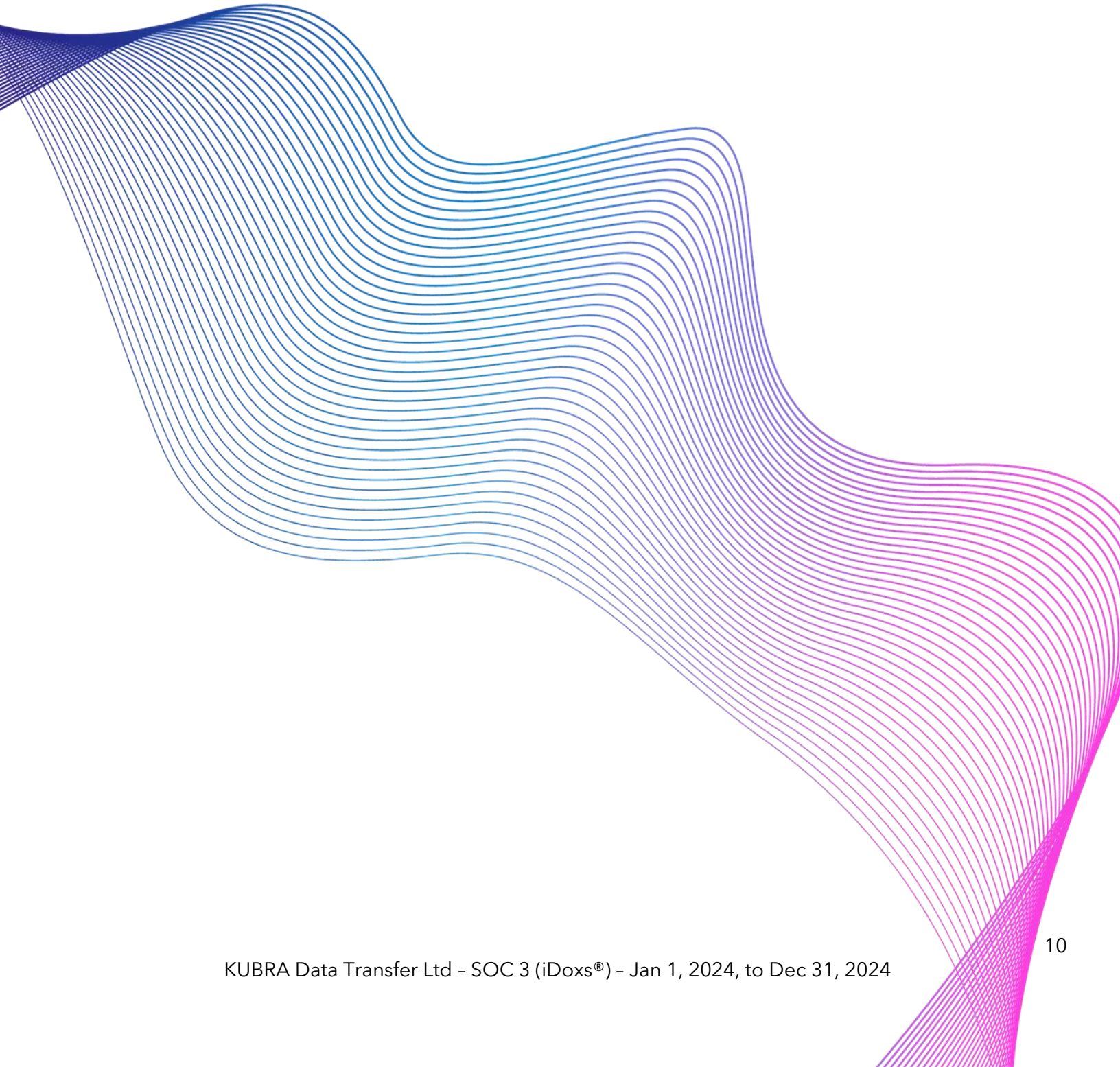
2) The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of the Company's controls throughout the period. The criteria we used in making this assertion were that:
   a) The risks that threaten the achievement of the control objectives stated in the description have been identified by management.
   b) The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.
   c) The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

By: Gavin Pinho

Title: Vice President, Information Security, Privacy and Risk Management

Date: February 7th, 2025

Section III: Description of KUBRA Data Transfer LTD.'s iDoxs® System



DESCRIPTION OF OPERATIONS AND CONTROLS PROVIDED BY MANAGEMENT

Company Background

KUBRA Data Transfer, Ltd. (KUBRA) is a Canadian corporation that maintains multiple business units across North America, with facilities in Dallas, Texas; Gardena, California; Piscataway, New Jersey and Mississauga, Ontario.

KUBRA develops and markets Client Communication Management solutions via a portfolio of business process outsourcing, information software, and professional services.

KUBRA's integrated solutions enable companies to compose, deliver, manage, and process complex, high-volume, personalized information assets for maximizing the client relationship management potential of every client contact. KUBRA has over 600 user entities including some of the largest Communication, Utility, Insurance, Financial Services, Media, and Manufacturing/Distribution organizations.

KUBRA's outsourced document production, print, and mail solution is referred to as KUBRA iMail™. The KUBRA iMail™ solution portfolio includes an integrated suite of advanced services for capturing, composing, personalizing, producing, and distributing bills, statements, and invoices via the mail stream.

The iDoxs® suite provides an e-billing platform for distributing bills, electronic statements, and invoices electronically via the Internet. The Document Web (DocWeb) application is required to support the use of iDoxs® in the capture, composition, personalization, and production of documents.

KUBRA iDoxs® Products and Services Overview

KUBRA's iDoxs® suite facilitates the capturing, personalizing, composing, and distributing of electronic bills, electronic statements, electronic invoices, and correspondence via KUBRA's iDoxs® Direct Product.

Additionally, KUBRA has a process monitoring product, DocWeb, which provides user entities with complete monitoring, control, and access to their critical data.

The iDoxs® suite is an e-billing and self-service platform that is delivered as an active server page-based solution. The iDoxs® suite provides the following services:

- Electronic billing
- Non-Enrolled one-time payments
- Inbound Electronic payment consolidation
- Electronic Document (bill) archival and retrieval

KUBRA's iDoxs® suite is composed of the following modules:

- KUBRA iDoxs® Alerts – automated outbound email, SMS text, and voice messages
- KUBRA Call Center Console – cloud-based document archival with a document retrieval tool for Customer Service Representatives
- KUBRA iDoxs® Consolidator – e-bill delivery to consolidator and digital mailbox services such as Fiserv, FIS Global
- KUBRA iDoxs® Marketing – includes tools for managing marketing messages for e-billing such as banner ads, pop-up ads, email messages, and e-inserts
- KUBRA iDoxs® Mobile – e-bill delivery via SMS text message, mobile web, and iOS and Android apps
- KUBRA iDoxs® Payment – enrolled and non-enrolled payments via IVR, call center, web, secure email attachment, and mobile; real-time and batch connections to ACH originators, credit card processors, and debit card networks; and a payment reporting and reconciliation engine for tracking inbound payment transactions
- This module integrates with our KUBRA EZ-PAY®, EZ-PAY+™ (EZ-PAY v6.0) and KUBRA iRemit® solutions to provide additional payment options and remittance data aggregation, respectively.
- KUBRA iDoxs® Portal – tools for enrollment, document presentment, account management, self-service, and notifications by email, automated voice, and two-way text messaging

Boundaries of the Systems

The scope of this report includes the iDoxs® services performed in Dallas, Texas; Gardena, California; Piscataway, New Jersey; and Mississauga, Ontario facilities. Additionally, the scope includes services hosted within the Amazon Web Services (AWS) cloud environment, including the AWS regions in North America.

This report does not include data center hosting services provided in the U.S. by Cyxtera & Equinix, nor data center hosting services in Canada provided by eStruxture.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT, MONITORING, INFORMATION, AND COMMUNICATION

Infrastructure

The Company's information system operates in a hybrid environment, with some infrastructure on-premises and other services hosted in the cloud using Amazon Web Services (AWS). The systems are secured through network segmentation, firewalls, and access controls. The system enables secure data exchanges with clients using methods such as Secure File Transfer Protocol (SFTP), Transport Layer Security (TLS), and Virtual Private Network (VPN).

Software

KUBRA provides on-demand application support for client software used by the system. The software applications used by the system are documented in the Product and Services Overview section of this report.

Software utilized by IT to manage and support the Environment includes:

- Backup management
- Anti-Virus
- System monitoring
- Network monitoring
- Security monitoring
- Change management

People

Human Resource Security

KUBRA observes Human Resources (HR) policies, procedures, and guidelines within its Employee Handbook. Management updates these policies as appropriate. KUBRA managers observe these policies, procedures, and guidelines as well as applicable federal and state laws, as they relate to the recruitment, selection, and hiring of employees and contractors.

Management collects all company property and assets (e.g., company credit cards, keys, computers, cellphones, etc.) from terminated employees. All company proprietary files are secured, and access to all electronic resources (e.g., telephone, network, computer, email, etc.) is terminated. HR maintains records on all active and terminated employees.

Accountability

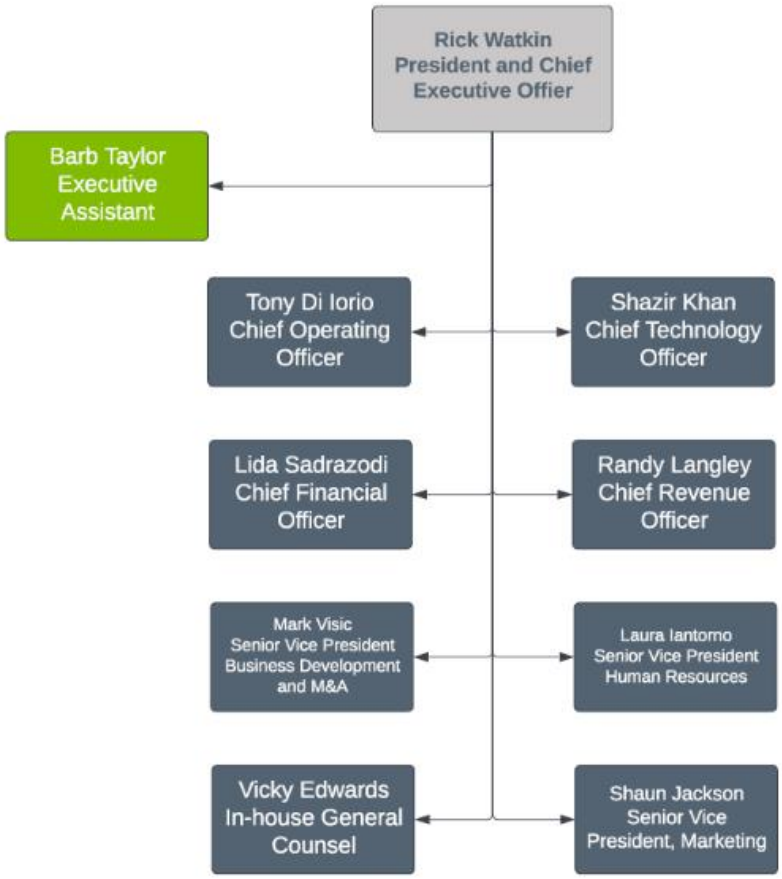
Individual users are responsible for ensuring that others do not access data or information from their systems. Users must take great care in protecting their usernames and passwords and this information is never to be loaned or given to other members of the Company or outside individuals. Disclosing this information could lead to vulnerabilities in the system as well as in the data and information contained in the system.

Responsibility for guaranteeing appropriate security for data, systems, and networks is assigned to the VP of Information Security, Privacy and Risk Management. The VP is responsible for designing, implementing, and maintaining security protection, but management retains responsibility for ensuring compliance with this policy. In addition to management and information technology staff, the individual user is responsible for the information technology equipment and resources under his or her control.

Roles and Responsibilities

Everyone at KUBRA has some responsibility for achieving the obligations of the Company. Proper lines of communication are in place to discuss operational activities and risks of the Company promptly management. The Company's management encourages individuals and teams to use initiative in addressing issues and resolving problems.

The following organizational chart depicts the Company's corporate structure:



Commitment to Competency and Accountability

The Company defines competence as the knowledge and skills necessary to accomplish tasks that define an employee's roles and responsibilities. The Company seeks only high-quality staff with significant experience, education, and understanding of working in a team environment. Management analyzes the knowledge and skills required to complete given tasks and confirms the individuals are capable of completing the tasks through interviewing, reference, and background checks, as well as other investigative means.

Data

Data processed by the system is managed and stored by the relevant data protection policies and procedures. The data is managed, transmitted, and stored in a range of system and database technologies. Data owned, used, created, or maintained by KUBRA is classified into the following categories:

- Confidential
- Sensitive
- Private
- Public

Data flowing through KUBRA infrastructure is encrypted, and access is restricted to authorized individuals requiring such access including the Company's customer base. Logical access controls ensure access is restricted to authorized individuals based on job functions.

Confidentiality and Privacy

All members of the Company are obligated to protect confidential data in their control. The Information Security Policies and Procedures document discusses the methods of protecting such information and procedures to safeguard the data during transmission.

Procedures

Automated and manual procedures related to the services provided include procedures by which service activities are initiated, authorized, performed, and delivered and reports or other information is prepared. Operating procedures have been documented and made available to all users who need them. These procedures cover the following areas:

- Access management
- Change management
- Information security controls
- Security incident response

Security is critical to the physical network, computer operating systems, and application programs. Each area offers its own set of security issues and risks. The Company has implemented a comprehensive security program that offers a high level of protection corresponding with the value of the assets.

Processing Integrity

Data is identified and specific jobs are built to customer specifications. Each new job goes through the same onboarding and testing processes. Some customers take the additional step to formally approve, through the portal, jobs before processing. After processing, print jobs are verified using a variety of methods to ensure complete and accurate processing and delivery to mail services. iDoxs® performs electronic billing, payment consolidation, and electronic document archival. iDoxs® receives electronic documents from DocWeb and has processing checkpoints to ensure information is processed accurately. Customers can retrieve documentation from iDoxs® directly.

Additional Elements of the Control Environment

The Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include integrity and ethical values, the competence of the entities people; management's philosophy and operating style; the way management assigns authority and responsibility and organizes and develops its people. The company has established contact that fosters shared values and teamwork in pursuit of the organization's objectives.

Integrity and Ethical Values

Integrity and high ethical standards are qualities essential to the Company's business and are viewed as fundamental standards of behavior for all employees. The effectiveness of internal controls cannot rise above the integrity and ethical values of the people, who create, administer, and monitor them. The Company established programs and policies designed to communicate and reinforce the integrity and ethical standards of the company. Any employee found to have violated the ethics policy may be subject to disciplinary action, up to and including termination.

Management Oversight and Organizational Structure

The Company's organizational structure provides the framework within which its activities for achieving entity-wide objectives are completed and analyzed. The Company is organized in a manner that defines key areas of authority while maintaining adequate separation of duties.

Communications

The Company uses a variety of communication methods to ensure that significant events and issues are sent in on time so that staff understands their responsibility over service and controls. These methods include the following: new hire training, ongoing training, policy and process updates, departmental meetings summarizing events and changes, and the use of e-mail systems. The Company maintains systems that manage the flow of information and facilitate communication with its customers.

Management communicates objectives related to confidentiality and privacy and any changes made to those objectives as needed. The Employee Handbook contains the principles that guide the conduct of employees and provides details of the personnel policies and benefits offered by KUBRA. Employees sign an Employee Acknowledgement Form regarding the KUBRA Employee Handbook stating that they have received and read the manual.

The communication system between senior management and KUBRA staff includes the use of the office e-mail system, written memos when appropriate, and periodic meetings. Staff and training meetings are utilized to inform staff of new policy and technology updates. Communication is encouraged at all levels to promote the operating efficiency of KUBRA.

Policies

KUBRA maintains a suite of comprehensive policies designed to provide both management's stated direction (policy) and staff working practices (procedures).

Policies address the reasons for security; the rules and procedures required to achieve security; and the personnel and roles who work to enforce the security policies. The accompanying table lists an example of the policy documents that have been adopted by KUBRA.

Policies	Description
Acceptable Use Policy Employee Handbook	Policies governing how computing resources may be used
Data Classification and Control Policy Data Management Policy and Procedures	Policies related to the creation, exposure, and disposal of data, both corporate and client
Information Security Policies and Procedures User Right Assignment Reviews Password Policy	Policies that cover the security of network-attached resources and the network infrastructure that serves these resources
Backup Procedure	Policies, rules, and procedures covering actions that affect the ongoing maintenance and availability of a secure infrastructure

Policies	Description
Business Continuity and Disaster Recovery Plan Change and Release Management Policy Computer Virus Detection Incident Response Plan and Procedures Risk Assessment Policy Vendor Management	
Physical Security Policy Encryption Policy	Policies covering the security of Information Technology assets

Published Job Descriptions

Job descriptions aid in establishing hiring criteria, orienting new employees to their jobs, identifying the requirements of each position, setting standards for employee performance evaluations, and establishing a basis for making reasonable accommodations for individuals with disabilities. KUBRA makes every effort to create and maintain accurate job descriptions for all positions within the organization. Each description at a minimum includes the job title and the duties for the position. Additional requirements are listed depending on the position.

Training

KUBRA has implemented various methods of communication to help ensure that employees understand their roles and responsibilities over user data and controls and that significant events are communicated in a timely manner. KUBRA is committed to training as an essential part of the success of each employee. IT management conducts security training programs for all employees. Newly hired employees undergo security awareness training to introduce the employee to confidentiality and privacy requirements. In addition, managers oversee the training and awareness of the topics contained in the Employee Handbook. All employees are trained to perform multiple jobs, tasks, and functions of the company for business continuity.

Monitoring

Company management performs monitoring activities as part of normal business operations to assess the quality of the internal control environment. Management performs regular reviews of tasks assigned to their teams. Monitoring activities are used to initiate corrective action through team meetings, client conference calls, and informal notifications. Corrective actions are taken as required to correct deviations from company policy and procedures. Tasks that are not addressed on time are manually escalated and resolved.

Performance Evaluations

The primary objective of a performance evaluation is to measure the performance of an individual against the objective standards established for a specific position. Consequently, the main purpose of the KUBRA performance evaluation program is to provide an equitable method to assess an employee's job performance, discuss performance and actions to improve job performance, identify an employee's development needs, and provide for salary administration.

KUBRA employees undergo performance reviews to identify both strengths and areas in need of improvement. All employees, regardless of classification or length of service, are expected to meet and maintain company standards for job performance and behavior. Performance goals are determined for the next year.

Risk Assessment

Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is the establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to the achievement of Company objectives and forming a basis for determining how the risks should be managed. Because economic, industry, regulatory, and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.

Management identifies risks that threaten client commitments by performing a formal risk assessment annually. The risk assessment includes the analysis of fraud, threats, probabilities of occurrence, potential business impacts, and associated mitigation plans. Management holds risk management meetings throughout the year so that it can react swiftly to address emerging risks. Risk mitigation strategies include prevention and elimination through the implementation of internal controls and transference of risk through insurance policies.

The Company maintains insurance coverage to transfer certain identified risks. The company maintains a general liability and umbrella policy to protect against unforeseen events. Additional insurance policies may be acquired as needed to satisfy certain contractual obligations.

Control Activities

Security Management

KUBRA implements security practices to help protect physical access to data and systems and to limit access to authorized personnel. KUBRA has instituted Security Awareness Training and the KUBRA workforce is trained on security expectations. Additionally, KUBRA meets periodically to discuss current security issues and concerns for its services.

Physical Security

Main Office

Access to the office suite is restricted to authorized users via the badge access system. Visitors are required to sign a visitor log while on the premises. Entrances to the building and critical areas are monitored 24 hours a day, 7 days several security cameras.

Data Center

Entrances to the data center are locked at all times. Entry is controlled by a proximity access card system. Only authorized personnel have access to the data center facility. Cameras monitor the facility; there are no areas that cannot be seen via the security cameras in the data center.

Environmental Security

HVAC systems are in place to protect computer equipment and maintain a comfortable work environment. Periodic maintenance is performed to ensure the systems are operating as intended. The facility is equipped with fire detection and prevention systems that include water sprinklers, smoke detectors, handheld fire extinguishers, and pre-action dry pipe fire suppression. Periodic inspections of the fire suppression systems are performed.

Backup Power – The Company utilizes a redundant source of Uninterruptible Power Supply (UPS) systems. In the event of an electrical failure, the battery-powered electrical supply system keeps critical systems running until the backup generator kicks in. The UPS units and generators are inspected and maintained by a third- party periodically.

The data center is equipped with raised flooring to elevate equipment and help facilitate cooling.

Information Security

The information security program provides reasonable protection against unauthorized access, disclosure, modification, or destruction, as well as assures the availability, integrity, usability, authenticity, and confidentiality of information. This applies to all systems that manage or store data.

Logical Access

Access to resources and data is granted to individuals based on their job responsibilities. A ticketing system is used to track requests, approvals, and granting of access by appropriate individuals. Individual access capabilities are removed immediately by IT or data owners upon the notification of termination of employment, change of responsibilities, or

termination of a contract with a client that uses the system. System security access levels are periodically reviewed by IT and data owners to ensure individual access rights are appropriate based on job information.

Password Settings

KUBRA follows the structured user and password management procedures that are documented within the KUBRA Password Policy. KUBRA utilizes an initial strong complex password for the user. Password history, maximum password age, minimum password, age, and minimum password lengths are enabled and established.

Computer Operations & Data Communications

The Company utilizes several network security technologies to protect and defend Internet-accessible systems.

Firewalls

Firewalls protecting the intranet from the public network are implemented, configured, and managed by the KUBRA administration staff. Firewalls utilized access rules to grant or deny access to internal resources.

Demilitarized Zone (DMZ)

Network computers exposed to the Internet can subject the entire network to hacker attacks. This can lead to compromised data, viruses, and other types of malicious acts that could damage the Company's credibility and operations.

A Demilitarized Zone has been established to isolate the Company's computers from the Internet. A Demilitarized Zone is a small network of computers exposed to the external world (Internet). Identifiable security incidents occurring on the DMZ computers are evaluated, and steps are taken to prevent future breaches of the DMZ.

Network Address Translation (NAT)

NAT allows computers on a private network to access the Internet through an intermediary called the Network Address Translator. The Network Address Translator examines all packets destined for the Internet, removes the private IP address from the IP header, substitutes the address of the NAT public interface, and forwards it to the destination. When the resource at the destination IP address responds to the request, the Network Address Translator receives it, checks its internal table to see which client the packet belongs to, and forwards it to the proper client.

NAT is used on the firewall to provide hidden Internet addresses to internal computers. This mitigates the possibility of external sources finding the addresses of internal computers.

Data Transmission and Encryption

Data in motion is encrypted using TLS-level encryption and two-factor authentication. Data can be accessed remotely using a virtual private network. A VPN is used to provide secure, encrypted communication between a network and a remote host or other remote networks over the public Internet. VPNs allow the establishment of an encrypted tunnel that protects the flow of network traffic from eavesdroppers. Instead of using a dedicated, real-world connection such as a leased line, a VPN uses virtual connections routed through the Internet from the private network to the remote site or employee.

Private Data

The KUBRA privacy policy is available to data subjects and when receiving private, or sensitive data, KUBRA obtains consent in compliance with applicable regulations. KUBRA reviews the privacy policy annually and any changes are communicated to data subjects timely. As new services are developed, KUBRA has a process to identify when new private data is required so that consent can be obtained timely. KUBRA has several processes in place to validate that the private information received from data subjects is accurate and complete. Private data is only retained for as long as needed provided services to its clients.

Secure Storage, Media, Data, and Document Destruction

The Company has established a policy directing how and when to destroy data. All computer systems, electronic devices, and electronic media are properly cleaned of sensitive data and software before being transferred outside of the corporate

office for vendor trade-in, servicing, or disposal. The Data Management Policy and Procedures document cover the retention period and the procedure to purge data based on the agreed retention period.

Incident Response

The Company has a formal Incident Response Plan and Procedures whereby responsibilities regarding notification and action took are clearly defined. Security incidents are handled by various members of management. The VP of Information Security, Privacy and Risk Management is responsible for keeping management apprised of incident status through resolution.

Malicious Code Management

Anti-virus tools are used to protect servers. A comprehensive virus management solution works to prevent virus infections and automates the virus definition updating process. The installed anti-virus application scans production servers for viruses and infected files. Infected files are cleaned. Files that cannot be cleaned are quarantined. Quarantined files are removed and/or a virus removal tool is used to clean/remove them.

Backup and Disaster recovery

KUBRA has implemented various backup methods as part of its production operations. Automated software is utilized to perform the backups of production servers. System snapshots are taken to restore systems by established recovery point objectives. Backups are performed daily.

Backup Testing

Restore testing is performed through the course of normal operations and as part of periodic testing. It involves restoring files from backup media or the secure internet vaulting service.

Monitoring

The backup system logs the results back to a monitoring tool and sends email alerts for backup failures.

Recovery

KUBRA has a documented business continuity and disaster recovery plan in place, and it is reviewed. The plan is tested annually and any issues resulting from these tests are incorporated into the plan and updates are made accordingly.

Network Monitoring

Monitoring policies and procedures are utilized for addressing issues relating to outages of critical services or other issues needing immediate action. These procedures vary based on the defined severity level of the problem. Company engineers use several monitoring tools to identify and provide alerts.

KUBRA utilizes a suite of monitoring tools to provide proactive incident identification and response services. The Company's Information Technology team regularly monitors the network. Overall health and capacity planning are monitored to ensure the system will meet clients' needs. The monitoring applications generate alerts when predefined thresholds are exceeded on the monitored devices. Information Technology monitors security access violations, including server logs and reports.

System Maintenance and Change Management

Infrastructure Change Management

The Company has a formal Change and Release Management Policy which guides the application of changes to the production system in proportion to the availability requirements of the data and the impact of the change on the user community. A change request form must be completed and approved by management for all changes affecting the production system. Controls include:

- Change Request
- Testing the Change
- Approval
- Execution
- Record of the Change

Software Development Life Cycle ("SDLC")

KUBRA follows a controlled approach to developing, testing, approving, and building each release of the system that is designed to ensure the continued quality of the released product before it is available to the client base. This documented development policy is referred to as the KUBRA Secure Software Development Process.

A software application is used to manage the application development tickets utilizing a defined process.

Company personnel performs quality testing on the application development and enhancements. Upon approval from management and completion of testing, the updated code is released to production. The Company maintains version controls utilizing a source code library which is restricted to authorized personnel. Separate environments are in place for development, quality assurance ("QA"), and production.

Complementary Controls at User Organizations

The Company's applications are designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve the control objectives included in this report. This section describes additional controls that should be in operation at user organizations to complement the controls at the Company. User auditors should consider whether the following controls have been placed in operation at the user organizations:

Security

ID	Criteria
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
	• User organizations are responsible for controls to input complete and accurate information and comply with the operating instructions of the Company's products and applications.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
	• User organizations are responsible for controls to comply with the operating instructions of the Company's products and applications.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.
	• User organizations are responsible for controls to communicate with the company regarding failures, incidents, concerns, and other matters when complying with the operating instructions of the Company's products and applications.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

ID	Criteria
	• User organizations are responsible for informing the Company of any regulatory issues that may affect the services provided by the Company.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives
	• User organizations are responsible for risks related to the use of IT and access to information when granting access to the services provided by the Company.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.
	• User organizations are responsible for controls to comply with the operating instructions of the Company's products and applications. • User organizations are responsible for controls to notify the Company on time when changes are made to technical, billing, or administrative contact information.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	• User organizations are responsible for controls to provide reasonable assurance that output reports are reviewed by appropriate individuals for completeness and accuracy. • User organizations are responsible for system sign-on controls and procedures for the selection and printing of available reports at their respective locations. • User organizations are responsible for controls to ensure that user organizations adopt the strong operating system and application password management procedures, including using passwords that cannot be easily compromised and require change regularly. • User organizations are responsible for controls to ensure the confidentiality of any user IDs and passwords assigned.
CC6.2	Before issuing system, credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users, whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	• User organizations are responsible for system sign-on controls and procedures for the selection and printing of available reports at their respective locations. • User organizations are responsible for controls to ensure that user organizations adopt the strong operating system and application password management procedures, including using passwords that cannot be easily compromised and require change regularly. • User organizations are responsible for controls to ensure the confidentiality of any user IDs and passwords assigned.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.
	• User organizations are responsible for controls to notify the Company on time when changes are made to technical, billing, or administrative contact information.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

ID	Criteria
	• User organizations are responsible for procedures to define develop, maintain, and test their business continuity plans ("BCP").
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
	• User organizations are responsible for controls to provide reasonable assurance of the transmission and receipt of information not provided by the Company.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
	• User organizations are responsible for controls to immediately notify the Company of any actual or suspected information security breaches, including compromised user accounts.
CC7.3	The entity evaluates security events to determine whether they could or have failed the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
	• User organizations are responsible for controls to immediately notify the Company of any actual or suspected information security breaches, including compromised user accounts.

Availability

ID	Criteria
A1.2	The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.
	• User organizations are responsible for controls to provide reasonable assurance that the customer has procedures in place for developing, maintaining, and testing their business continuity plans ("BCP"). • User organizations are responsible for approving the telecommunications infrastructure controls between themselves and the Company.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.
	• User organizations are responsible for controls to provide reasonable assurance that the customer has procedures in place for developing, maintaining, and testing their business continuity plans ("BCP").

Processing Integrity

ID	Criteria
PI1.2	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.
	• User organizations are responsible for controls to provide reasonable assurance that erroneous input data are corrected and resubmitted.
PI1.3	The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.
	• User organizations are responsible for controls for approving the telecommunications infrastructure between itself and the Company.

	• User organizations are responsible for controls to provide reasonable assurance those transactions are appropriately authorized, complete, and accurate.
PI1.4	The entity implements policies and procedures to make available or deliver output completely, accurately, and timely by specifications to meet the entity's objectives.
	• User organizations are responsible for controls to provide reasonable assurance that changes to processing options (parameters) are appropriately authorized, approved, and implemented. • User organizations are responsible for controls to provide reasonable assurance that output reports are reviewed by appropriate individuals for completeness and accuracy.

Privacy

ID	Criteria
P6.5	The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on by established incident response procedures to meet the entity's objectives related to privacy.
	• User organizations are responsible for controls to immediately notify the Company of any actual or suspected information security breaches, including compromised user accounts.
P6.6	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.
	• User organizations are responsible for informing the Company of any regulatory issues that may affect the services provided by the Company. • User organizations are responsible for controlling user organizations to ensure compliance with contractual requirements. • User organizations are responsible for controls for the supervision, management, and control of the use of the Company's applications by its personnel. • User organizations are responsible for controls to maintain their systems of recordkeeping. • User organizations are responsible for controls to dictate the use of encryption.

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. The processing of information for customers by the Company covers only a portion of the overall internal control structure of each customer. The Company's products and services were not designed to be the only control component in the internal control environment. Additional control procedures are required to be implemented at the customer level. It is not feasible for all the control objectives relating to the processing of transactions to be completely achieved by the Company. Therefore, each customer's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

Subservice organization controls related to the Trust Services Principles.

Infrastructure – All networking, servers, backup and disaster and recovery infrastructure, connection points, routing equipment, firewalls, and internet service provider connections required in the hosted production environment is maintained by the subservice organization.

Controls in operation are verified annually by the service organization through the review of the independent third-party audit report on the subservice organization controls and operating effectiveness (SOC 2 Type 2).

Software – Applications required for the hosted production environment including network operating systems, virtual services, application and performance monitoring, malicious code management, intruder detection and prevention, data backup and replication including disaster recovery required in the hosted production environment are maintained by the subservice organization.

Controls in operation are verified annually by the service organization through the review of the independent third-party audit of the subservice organization controls and operating effectiveness (SOC 2 Type 2).

People – Personnel required for the maintenance and operation of the hosted production environment is maintained by the subservice organization.

Controls in operation are verified annually by the service organization through the review of the independent third-party audit of the subservice organization controls and operating effectiveness (SOC 2 Type 2).

Procedures - All procedures required to meet the Service Level Agreements (SLA) in the operation of the hosted production environment are maintained by the service organization. Physical access controls and procedures as well as environmental controls and procedures are provided by the subservice organization.

Controls in operation are verified annually by the service organization through the review of the independent third-party audit of the subservice organization controls and operating effectiveness (SOC 2 Type 2).

Data – Subservice organizations do not process data for the service organization and its users.

The following are applicable trust service criteria that are intended to be met by controls at the subservice organization and the types of controls expected to be implemented at the subservice organization that is necessary to meet the criteria, alone or in combination with controls at KUBRA Data Transfer Ltd.

Security Principle – Criteria expected to be addressed by the subservice organization.

ID	Criteria
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
CC 6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.
CC 7.3	The entity evaluates security events to determine whether they could or have failed the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Availability Principle – Criteria expected to be addressed by the subservice organization.

ID	Criteria
A 1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.
A 1.2	The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.
A 1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.

Trust Services Criteria Not Relevant to the System

ID	Criteria	Reason for Exclusion
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control as they relate to Security, Availability, Confidentiality, Processing Integrity, and Privacy.	The board is made up of both independent and dependent members. The CEO is on the board.
P5.2	The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and the reason for such denial to meet the entity's objectives related to privacy.	The company does not communicate directly with the data subject.
P6.1	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained before disclosure to meet the entity's objectives related to privacy.	Personal information is not disclosed to third parties.
P6.4	The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.	Personal information is not disclosed to third parties.
P6.5	The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on by established incident response procedures to meet the entity's objectives related to privacy.	Personal information is not disclosed to third parties.
P6.7	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subject's request, to meet the entity's objectives related to privacy.	The company does not communicate directly with the data subject.

Significant Changes to the System

During the audit period, it was observed that KUBRA made improvements to the disaster recovery system. Two new data centres were included in the 2024 audit scope and were part of the sampling process of the SOC2 Type2 audit.

CAC1 was introduced to the system on October 15, 2024, and USW2 was added on November 11, 2024. These two AWS data centres have been integrated into the iDoxs® application to function as disaster recovery sites. Both sites were included in the 2024 SOC2 Type2 audit, validating the effectiveness of controls.

Management Response to Noted Exceptions

Control Number	Description of KUBRA Control Activities	Management Response
CC6.2	Termination procedures are in place for the removal of access to all systems upon notification of the termination.	Going forward, KUBRA will closely monitor and reinforce the termination procedures as well as implement an automated account deactivation tool.

CC6.3	Management utilizes and retains HR termination checklists.	The exception occurred due to a timing issue. Moving forward, all checklists will aim for final sign-off within one month of the last day to avoid delays
CC6.4	Access cards are disabled timely upon receipt of termination notice from the appropriate manager.	The exception occurred because physical access was removed on the termination date, but the ticket was documented at a later time. Moving forward, KUBRA will closely monitor the process to ensure the physical access removal date is accurately recorded in the tickets without delay.

KUBRA Data Transfer Ltd.
5050 Tomken Rd
Mississauga, Ontario, L4W 5B1