KPA, LLC

Report on Controls at a Service Organization Relevant to Security

SOC 3[SM] Report

For the Period July 1, 2022 to December 31, 2022

SOC 3 is a registered service mark of the American Institute of Certified Public Accountants (AICPA)

Independent Service Auditor's Report

To the Management of KPA, LLC ("KPA"):

Scope

We have examined KPA's accompanying assertion titled "Assertion of KPA Management" (assertion) that the controls within its KPA EHS system (system) were effective throughout the period July 1, 2022 to December 31, 2022, to provide reasonable assurance that KPA's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

Service Organization's Responsibilities

KPA 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 KPA's service commitments and system requirements were achieved. KPA has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, KPA is responsible for selecting, and identifying in its assertion, the applicable trust service 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 system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that controls were not effective to achieve KPA's service commitments and system requirements based on the applicable trust services criteria; and,
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve KPA'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.

Relevant Ethical Requirements

We are required to be independent of KPA and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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 the KPA EHS system were effective throughout the period July 1, 2022 to December 31, 2022, to provide reasonable assurance that KPA's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Fairway, KS

February 15, 2023

Assertion of KPA Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the KPA EHS system (system) throughout the period July 1, 2022 to December 31, 2022, to provide reasonable assurance that KPA's service commitments and system requirements relevant to security were achieved. Our attached system description of the KPA EHS system identified 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 July 1, 2022 to December 31, 2022, to provide reasonable assurance that KPA's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria). KPA's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the attached system description.

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 July 1, 2022 to December 31, 2022, to provide reasonable assurance that KPA's service commitments and system requirements were achieved based on the applicable trust services criteria.

KPA

February 15, 2023

Overview of Operations

Description of Services Provided

KPA (the "company"), formerly known as iScout, provides safety training and reporting services throughout the United States. The company was founded in 2014 and empowers teams with the resources they need to keep each other safe.

KPA's core product, the KPA EHS System (the "system"), is a Software as a Service (SaaS) solution. KPA is a safety management system designed to foresee and control hazards associated with workplace safety and performance. The system is an application suite that is designed to strategically ensure the integrity of employees, equipment and processes and includes the following services:

- **KPA Environmental Health and Safety (EHS) Reporting:** Core enterprise platform made up of the following functions.
    - **Reporting:** Design forms for employees to fill out in the field. This most commonly includes job safety assessments, incident reports, driver-vehicle inspections, and PTO requests. But you can design a form for nearly any company specific need.
    - **Training:** Design, assign, and track employee training and certifications.
    - **Safety alerts:** Send safety alerts that require sign-offs. The alerts can be company-wide or targeted at specific individuals or groups. For example, they can be automated for all onboarding employees or ad-hoc due to the adverse weather conditions of a specific region.
    - **Assets:** Define any kind of equipment asset that fits your organization. Common assets include vehicles, harnesses, tablets, tool kits, and fire extinguishers. Then track them all through scheduled inspections.
    - **Resources:** Upload standard operating procedures (SOPs) for employees to reference in the field.
- **KPA EHS Integration:** An interface that enables the system to communicate in real-time to third party user entity systems.
    - **API:** A token-based JSON application programming interface (API) for pulling/pushing data from/to KPA.
    - **SFTP:** A secure dropbox for automatic data load ingestion. Data loads are special files used to bulk import data into our system. We support many kinds of data loads, but the most common usage is to continually sync employees and equipment.

Principal Service Commitments and System Requirements

KPA designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that KPA makes to user entities, the laws and regulations that govern its services, and the financial, operational, and compliance requirements that KPA has established. The system services are subject to the security commitments established internally for its services.

Commitments to user entities are documented and communicated in service-level agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

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

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role;
- Use of intrusion detection/prevention systems to identify potential security attacks from users outside the boundaries of the system;
- Security awareness training for employees completed annually;
- vulnerability scans and penetration testing over the system; and,
- Operational procedures for managing security incidents and breaches, including notification procedures.

Such requirements are communicated in KPA's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the system.

Components of the System Used to Provide the Services

The purpose of the system description is to delineate the boundaries of the system, which includes the services and commitments outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure

The system is hosted in Amazon Web Services (AWS) and Heroku in a virtual private cloud (VPC) environment which protects the network from unauthorized external access. Server hardware consists of a combination of servers fully hosted, managed, and protected by AWS and Heroku. User requests to KPA's web-based systems are encrypted using Transport Layer Security (TLS) using certificates from an established third-party certificate authority.

Software

KPA is responsible for managing the development and operation of the KPA platform including infrastructure components such as servers, databases, and storage systems. Additional software supporting the KPA platform includes Heroku Runtime (Platform as a Service (PaaS) used to build, run, and operate the KPA EHS programs cluster), Microsoft Office 365 (provides single sign-on (SSO) and multi-factor authentication), GitHub (Source code repositories, version control systems, and build software), MongoDB (document database for housing client data), Files.com (SFTP for data loads), Amazon Web Services.

People

KPA has a staff organized in the following functional areas:

- **Executive Management:** Independent of control operators and responsible for overseeing company wide activities, establishing and accomplishing goals, and overseeing objectives.
- **Engineering:** Responsible for the development, testing, deployment, and maintenance of the source code for the system. Also responsible for the product life cycle, including adding additional product functionality.

- **Security:** Responsible for access controls and security of the production environment. Security oversees risk management, incident management, third party risk management, training, vulnerability management, and internal control, and includes members independent from control operators. Also responsible for meeting at least annually to review policies and procedures and set the information security program roadmap.
- **People:** Composed of HR and the help desk, responsible for recruiting and onboarding new personnel, defining roles and positions for new hires, performing background checks, and facilitating the employee termination process.
- **Customer Support:** Responsible for account management, customer success, and customer support activities.
- **Sales:** Responsible for sales and marketing.

Data

Data, as defined by KPA, constitutes the following:

- Transaction data
- Electronic interface files
- Output reports
- Input reports
- System files
- Error logs

Output reports are available and include data and files systematically generated from the system. The availability of these reports is limited by job function. Reports delivered externally are only sent using a secure method as requested by the customer—email or secure web links to customer users.

Information assets are assigned a sensitivity level based on the audience for the information. If the information has been previously classified by regulatory, legal, contractual, or company directive, then that classification will take precedence. The sensitivity level then guides the selection of protective measures to secure the information. All data is to be assigned one of the following sensitivity levels:

Data Sensitivity	Description	Examples
Public	Public data is information that may be disclosed to any person regardless of their affiliation with KPA. The “public” classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to any data that does not require any level of protection from disclosure. While it might be necessary to protect original (source) documents from unauthorized modification, public data may be shared with a broad audience both within and outside KPA, and no steps need be taken to prevent its distribution.	• How-to and video guides • Client logos (when authorized in the subscription agreement) • Marketing materials • Terms of service available on company website
Internal	Internal data is information that is potentially sensitive and should not be shared with the public. Internal data generally should not be disclosed outside of KPA without the permission of KPA management. It is the responsibility of the data owner to designate information as internal where appropriate. Unauthorized access has the potential to influence KPA's operational effectiveness, cause a significant financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence.	• Client contact information • Employee data • Payroll data • Technology suite • Project roadmaps • Unreleased marketing materials
Company Confidential	Company-confidential data is information that, if made available to unauthorized parties, might adversely affect KPA. This information is to be protected against unauthorized disclosure or modification, and might be limited to executives, HR, and legal parties employed by or under contract with KPA. Company-confidential data should be used only by pre-authorized parties and should be protected both when it is in use and when it is being stored, processed, or transmitted. Unauthorized access has the potential to influence KPA's operational effectiveness, violate contractual confidentiality agreements, initiate a security incident, or cause a major drop in employee, customer, and industry confidence.	• Source code • Authentication data • Contract data

Data Sensitivity	Description	Examples
Customer Confidential	Customer-confidential data is information that, if made available to unauthorized parties, may adversely affect KPA customers. This classification also includes data that KPA is required to keep confidential, either by law or under a confidentiality agreement with non-customer third parties, such as vendors. This information is to be protected against unauthorized disclosure or modification. Customer-confidential data should be used only when necessary for business purposes with the permission of the customer and should be protected both when it is in use and when it is being stored, processed, or transmitted. Unauthorized access has the potential to influence KPA's operational effectiveness, violate contractual confidentiality agreements, initiate a security incident, or cause a major drop in both customer and industry confidence.	• Email address • Name • Employee number • Form responses • Training completions
Public	Public data is information that may be disclosed to any person regardless of their affiliation with KPA. The “public” classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to any data that does not require any level of protection from disclosure. While it might be necessary to protect original (source) documents from unauthorized modification, public data may be shared with a broad audience both within and outside KPA, and no steps need be taken to prevent its distribution.	• How-to and video guides • Client logos (when authorized in the subscription agreement) • Marketing materials • Terms of service available on company website

Processes and Procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by senior management. These procedures cover the following key security life cycle areas:

- Information Security Policy and organization
- Risk management
- Asset management
- Access control
- Communications and network security
- Change management and secure development life cycle
- Vulnerability management
- Incident management and response
- Compliance
- Endpoint management
- Personnel security
- Data classification (data at rest, in motion, and output)

Principal Service Commitments and System Requirements

KPA designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that KPA makes to user entities, the laws and regulations that govern its services, and the financial, operational, and compliance requirements that KPA has established. The system services are subject to the security commitments established internally for its services.

Commitments to user entities are documented and communicated in service-level agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

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

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role;
- Security awareness training for employees completed annually;
- Monthly vulnerability scans and annual penetration testing over the system; and,
- Operational procedures for managing security incidents and breaches, including notification procedures.

Such requirements are communicated in KPA's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained.

In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the system.

Complementary User Entity Controls

KPA controls were designed with the assumption that certain internal controls would be in place at customer organizations. The application of such internal controls by customer organizations is necessary to achieve certain trust services criteria identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for processing of transactions for KPA customers.

For customers to rely on the information processed through the KPA EHS application, each customer is expected to evaluate its own internal controls to ensure appropriate control activities are in place. The following general procedures and controls should be considered. They should not, however, be regarded as a comprehensive list of all controls that should be implemented by customer organizations.

- User entity is responsible for protecting established user IDs and passwords within their organizations.
- User entity is responsible for reviewing customer access to the KPA EHS application periodically to validate appropriateness of access levels.
- User entity is responsible for approving and creating new user access to the KPA EHS application.
- User entity is responsible for removing terminated employee access to the KPA EHS application.
- User entity is responsible for implementing policies and procedures over the types of data that are allowed to be entered into the KPA EHS application.
- User entity is responsible for sending data to KPA EHS via a secure connection and/or the data should be encrypted.
- User entity is responsible for notifying KPA EHS if they detect or suspect a security incident related to the KPA EHS System by contacting security@kpaehs.com.
- User entity is responsible for reviewing email and other forms of communications from KPA EHS, related to changes that may affect KPA EHS customers and users, and their security or availability obligations.
- User entity is responsible for establishing, monitoring, and maintaining controls over the security for system-generated outputs and reports from the system.
- User entity is responsible for endpoint protection of workstations used to access the system.
- User entity is responsible for developing their own business continuity and disaster recovery plan.

Complementary Subservice Organization Controls

KPA EHS uses subservice organizations in support of its system. KPA EHS's controls related to the system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria over the KPA EHS System to be achieved solely by KPA EHS. Therefore, user entity controls must be evaluated in conjunction with KPA EHS's controls described in Section IV of this report, considering the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below.

KPA EHS periodically reviews the quality of the outsourced operations by various methods including:

- Review of subservice organizations' SOC reports;
- Regular meetings to discuss performance; and,
- Non-disclosure agreements.

Control Activity Expected to be Implemented by Subservice Organizations	Subservice Organizations	Applicable Criteria
Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.	Heroku, MongoDB	CC6.1, CC6.2, CC6.3, CC6.5, CC7.2
Physical access to the data center facility is restricted to authorized personnel.	Heroku, Microsoft Office 365	CC6.4, CC6.5
Environmental protections, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.	Heroku, MongoDB, Microsoft Office 365	CC6.4
Production instances are hardened upon deployment, monitored for vulnerabilities, and updated on a regular basis with the most recent security patches.	Heroku	CC6.6, CC6.7, CC6.8, CC7.1, CC8.1, CC7.2,
Firewall rules and security VPCs are deployed and only network ports, protocols, and services listening on the system with a business need run. Default-deny rules drop traffic except those services and ports that are explicitly allowed.	Heroku	CC6.1, CC6.6, CC6.7

Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For tests of controls requiring the use of IPE (e.g., controls requiring system-generated populations for sample-based testing), BARR Advisory, P.A. performed a combination of the following procedures, where possible, based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used:

1. Inspect the source of the IPE;
2. Inspect the query, script, or parameters used to generate the IPE;
3. Tie data between the IPE and the source; and/or,
4. Inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity.

In addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of controls (e.g., periodic reviews of user access lists), BARR Advisory, P.A. inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

