# iScout

Report on Controls at a Service Organization Relevant to Security

## SOC 3[SM] Report

For the Period September 1, 2020 to November 30, 2020

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

BARR ADVISORY

# Independent Service Auditor's Report

To the Management of iScout:

**Scope**

We have examined iScout's accompanying assertion titled "Assertion of iScout Management" (assertion) that the controls within iScout's System (system) were effective throughout the period September 1, 2020 to November 30, 2020, to provide reasonable assurance that iScout'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**

iScout 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 iScout's service commitments and system requirements were achieved. iScout has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, iScout 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 iScout'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 iScout'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.

©2021 iScout All rights reserved 

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 iScout system were effective throughout the period September 1, 2020 to November 30, 2020, to provide reasonable assurance that iScout's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.


Fairway, KS

January 15, 2021

©2021 iScout All rights reserved | 

# Assertion of iScout Management

We are responsible for designing, implementing, operating, and maintaining effective controls within iScout's System (system) throughout the period September 1, 2020 to November 30, 2020, to provide reasonable assurance that iScout's service commitments and system requirements relevant to security were achieved. Our attached system description of the iScout 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 September 1, 2020 to November 30, 2020, to provide reasonable assurance that iScout'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). iScout'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 September 1, 2020 to November 30, 2020, to provide reasonable assurance that iScout's service commitments and system requirements were achieved based on the applicable trust services criteria.

**iScout**

January 15, 2021

©2021 iScout All rights reserved 

**Description of Services Provided**

iScout (the "company") 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.

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

- **iScout 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
    - Training: Design, assign, and track employee training and certifications
    - Acknowledgements: Send safety alerts that require sign-offs
    - Assets: Track and assign equipment inspections
    - Resources: Upload standard operating procedures (SOPs) for employees to reference in the field
- **Webhooks:** An integration workflow that enables the system to communicate in real-time to third party user entity systems.
    - API: A token based JSON API for pulling/pushing data from/to iScout
    - SFTP: A secure dropbox for automatic file ingestion

**Principal Service Commitments and System Requirements**

iScout designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that iScout makes to user entities, the laws and regulations that govern its services, and the financial, operational, and compliance requirements that iScout 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 systems to prevent and identify potential security attacks from users outside the boundaries of the system;
- Regular vulnerability scans over the system and network; and,
- Operational procedures for managing security incidents and breaches, including notification procedures.

©2021 iScout All rights reserved 

Such requirements are communicated in iScout'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 iScout's web-based systems are encrypted using Transport Layer Security (TLS) using certificates from an established third party certificate authority.

### Software

iScout is responsible for managing the development and operation of the iScout platform including infrastructure components such as servers, database and storage systems.

### People

iScout has a staff organized in the following functional areas:

- **Technical:** Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.
- **Support:** Responsible for account management, customer success, and customer support activities.
- **Sales:** Responsible for sales and marketing.

### Data

Data, as defined by iScout, 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 are to be assigned one of the following sensitivity levels:

- **Public**: Public data is information that may be disclosed to any person regardless of their aliation with iScout. The "public" classication 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 iScout, and no steps need be taken to prevent its distribution.
- **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 iScout without the permission of iScout management. It is the responsibility of the data owner to designate information as internal where appropriate. Unauthorized access has the potential to influence iScout's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence.
- **Company Confidential**: Company-confidential data is information that, if made available to unauthorized parties, might adversely affect iScout. 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 iScout. 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 iScout's operational effectiveness, violate contractual confidentiality agreements, initiate a security incident, or cause a major drop in employee, customer, and industry confidence.
- **Customer Confidential**: Customer-confidential data is information that, if made available to unauthorized parties, may adversely affect iScout customers. This classification also includes data that iScout is required to keep condential, 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 iScout's operational effectiveness, violate contractual confidentiality agreements, initiate a security incident, or cause a major drop in both customer and industry confidence.

## 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

©2021 iScout All rights reserved 

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

©2021 iScout All rights reserved 

# Complementary User Entity Controls

iScout 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 iScout customers.

For customers to rely on the information processed through the iScout 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 iScout application periodically to validate appropriateness of access levels.
- User entity is responsible for approving and creating new user access to the iScout application.
- User entity is responsible for removing terminated employee access to the iScout application.
- User entity is responsible for implementing policies and procedures over the types of data that are allowed to be entered into the iScout application.
- User entity is responsible for sending data to iScout via a secure connection and/or the data should be encrypted.
- User entity is responsible for notifying iScout if they detect or suspect a security incident related to the iScout System by contacting security@iscout.com.
- User entity is responsible for reviewing email and other forms of communications from iScout, related to changes that may affect iScout 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

iScout uses subservice organizations in support of its system. iScout'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 iScout System to be achieved solely by iScout. Therefore, user entity controls must be evaluated in conjunction with iScout's controls, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

iScout 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 Organization | Subservice Organization | Applicable Criteria |
|---|---|---|
| Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate. | AWS, Heroku | CC6.1, CC6.2, CC6.3, CC6.5, CC7.2 |
| Physical access to the data center facility is restricted to authorized personnel. | AWS, Heroku | CC6.4, CC6.5 |
| Environmental protections, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements. | AWS, Heroku | CC6.4 |
| Security hardening of server infrastructure, including maintenance and monitoring controls, are implemented. | AWS, Heroku | CC6.6, CC6.8, CC7.1, CC7.2 |
| Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system. | AWS, Heroku | CC6.8, CC7.2 |