JOHANSON GROUP

# System and Organization Controls (SOC) 2 Type II Report on Management's Description of its Continuous Vulnerability Scanning Platform

And the Suitability of Design of Controls and Test of Operating Effectiveness of Controls Placed in Operation Relevant to Security

For the Period
March 24, 2025, to June 22, 2025

Together with Independent Service Auditor's Report

HostedScan

# TABLE OF CONTENTS



# Section I

INDEPENDENT SERVICE AUDITOR'S REPORT

**HostedScan LLC**

## Scope

We have examined HostedScan LLC's accompanying description of its Continuous Vulnerability Scanning Platform (system) titled "Description of the Continuous Vulnerability Scanning Platform " throughout the period March 24, 2025, to June 22, 2025 (description) 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 (With Revised Implementation Guidance — 2022)* in AICPA, *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period March 24, 2025, to June 22, 2025, to provide reasonable assurance that HostedScan LLC's service commitments and system requirements were achieved based on trust services criteria relevant to security principles (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

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

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

The information included in Section V, "Other Information Provided by Management," is presented by the management of HostedScan LLC to provide additional information and is not a part of the description. Information about HostedScan LLC's response to an exception noted has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of the controls, to achieve HostedScan LLC's service commitments and system requirements based on the applicable trust services criteria.

## Service Organization's Responsibilities

HostedScan LLC 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 HostedScan LLC's service commitments and system requirements were achieved. HostedScan LLC has provided an assertion titled "Assertion of HostedScan LLC's Management" (assertion) about the description and the suitability of the design and operating effectiveness of the controls stated therein. HostedScan LLC is 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 on the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the 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.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

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

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

## 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 users may consider important to meet their informational needs.

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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.

## Description of Test of Controls

The specific controls tested and the nature, timing, and results of those tests are presented in the section of our report titled "Description of Test of Controls and Results Thereof."

## Opinion

In our opinion, in all material respects,

a. The description presents HostedScan LLC's Continuous Vulnerability Scanning Platform (system) that was designed and implemented throughout the period March 24, 2025, to June 22, 2025, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period March 24, 2025, to June 22, 2025, to provide reasonable assurance that HostedScan LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of HostedScan LLC's controls throughout the period.
c. The controls stated in the description operated effectively throughout the period March 24, 2025, to June 22, 2025, to provide reasonable assurance that HostedScan LLC's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of HostedScan LLC's controls operated effectively throughout the period.

## Restricted Use

This report, including the description of tests of controls and results thereof in the section of our report titled "Description of Test of Controls and Results Thereof" is intended solely for the information and use of HostedScan LLC; user entities of HostedScan LLC's Continuous Vulnerability Scanning Platform during some or all of the period March 24, 2025, to June 22, 2025, business partners of HostedScan LLC subject to risks arising from interactions with the HostedScan LLC's processing system; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls, and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

JohansonGroup LLP

Colorado Springs, Colorado
October 29, 2025

# Section II

ASSERTION OF HOSTEDSCAN LLC MANAGEMENT

We have prepared the accompanying description of HostedScan LLC's "Description of the Continuous Vulnerability Scanning Platform" for the period March 24, 2025, to June 22, 2025, (description) 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 (With Revised Implementation Guidance — 2022)* in AICPA, *Description Criteria* (description criteria). The description is intended to provide report users with information about HostedScan LLC's Continuous Vulnerability Scanning Platform (system) that may be useful when assessing the risks arising from interactions with HostedScan LLC's system, particularly information about system controls that HostedScan LLC has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

HostedScan LLC uses a subservice organization to provide data center facility and hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at HostedScan LLC, to achieve HostedScan LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents HostedScan LLC's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of HostedScan LLC's controls. The description does not disclose the actual controls at the subservice organization.

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

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

a. The description presents HostedScan LLC's Continuous Vulnerability Scanning Platform (system) that was designed and implemented throughout the period March 24, 2025, to June 22, 2025, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period March 24, 2025, to June 22, 2025, to provide reasonable assurance that HostedScan LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of HostedScan LLC's controls throughout that period.
c. The controls stated in the description operated effectively throughout the period March 24, 2025, to June 22, 2025, to provide reasonable assurance that HostedScan LLC's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of HostedScan LLC's controls operated effectively throughout that period.

HostedScan LLC Management
October 29, 2025

# Section III

DESCRIPTION OF THE CONTINUOUS VULNERABILITY SCANNING PLATFORM

## COMPANY BACKGROUND

HostedScan LLC, founded in 2018, is a fully remote company headquartered in Seattle, Washington. HostedScan provides external vulnerability scanning for websites, servers, networks, and APIs to help their customers secure their IT assets, meet compliance goals, and protect them from breaches and malicious attacks.

## DESCRIPTION OF SERVICES OVERVIEW OR SERVICES PROVIDED

The Continuous Vulnerability Scanning Platform provides customers with vulnerability scanning and vulnerability management. The system description in this section of the report details the Continuous Vulnerability Scanning Platform. Any other HostedScan services are not within the scope of this report.

The Continuous Vulnerability Scanning Platform focuses on the following activities: scanning websites, networks, and servers for vulnerabilities, managing the resulting reports and vulnerability details, and monitoring the vulnerabilities for remediation. Vulnerability scans may be set up to run on an automated schedule, and the resulting scans may be sent out via email or Slack notifications. Additionally, vulnerability data from other platforms may be aggregated into HostedScan. Customers use the platform to scan their assets for misconfigurations, configuration weaknesses, known vulnerabilities, and CVEs, both to help secure their business and meet compliance goals.

## PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

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

HostedScan's commitments to users are communicated through our Service Level Agreement in our Master Service Agreement, and in HostedScan's online Privacy Policy

### Security Commitments

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

- Use of encryption technologies to protect customer data both at rest and in transit.
- Uptime availability of production systems.

### Components of the System

The System description is comprised of the following components:

- Software - The application programs and IT system software that support application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- People - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- Data – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- Procedures – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

### Infrastructure

HostedScan maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents device name, inventory type, description, and owner. To outline the topology of its network, the organization maintains the following network diagram(s).

| Hardware | Type | Purpose (optional) |
|---|---|---|
| AWS Elastic Compute Cloud (EC2) | AWS | |
| AWS Elastic Load Balancers | AWS | Load balance internal and external traffic |
| Virtual Private Cloud | AWS | Protects the network perimeter and restricts inbound and outbound access |
| Linode VPS | VPS | Runs HostedScan scanning software |
| AWS Lambda | AWS | Runs HostedScan scanning software |
| AWS ECS | AWS | Runs HostedScan scanning software |

## Software

HostedScan is responsible for managing the development and operation of the Continuous Vulnerability Scanning Platform system, including infrastructure components such as servers, databases, and storage systems. The in-scope HostedScan infrastructure and software components are shown in the table provided below:

| System/Application | Operating System | Purpose |
|---|---|---|
| GuardDuty | AWS | Security application used for automated intrusion detection (IDS) |
| Amazon Web Services | AWS | Infrastructure supporting HostedScan scanning software |
| Calendly | Saas | Scheduling calls with customers |
| Certn (Partner) | Saas | Background checks for employees |
| FirstPromoter | Saas | Manage affiliate program for partners |
| GitHub | Saas | Code repository for HostedScan software |
| Google Analytics | Saas | Analyze traffic patterns to the HostedScan site |
| Google Drive | Saas | Manage HostedScan documents |
| Google Workspace | Saas | Provides email addresses for contractors and employees, and business document storage |
| Grafana Cloud | Saas | Analyze logs from HostedScan services |
| Grain | Saas | Record and transcribe internal meetings |
| GrooveHQ | Saas | Public knowledge base for HostedScan content |
| LinkedIn | Saas | Recruiting software for hiring HostedScan contractors and employees |
| Linode | Saas | Provides VPS services for running HostedScan software |
| MailerLite | Saas | Marketing emails from HostedScan |
| Mailgun | Saas | Transactional emails for HostedScan |
| MongoDB Atlas | Saas | Database for HostedScan software |
| Netlify | Saas | Hosting for HostedScan marketing website |
| PostHog | Saas | Analytics for the HostedScan product |
| Prismic | Saas | Content Management System for HostedScan blog |
| Sentry | Saas | Track errors from HostedScan software |
| Slack | Saas | Internal communication tool for HostedScan |
| Stripe | Saas | Payment processing software for HostedScan |
| Trello | Saas | Internal task management tool |
| Vanta | Saas | HostedScan's SOC 2 management tool |

## People

The company employs dedicated team members to handle major product functions, including operations and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

HostedScan has a staff of approximately 3, organized in the following functional areas:

Management: Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.

This includes:

- CEO - Kyle Cooper
- CFO - John Snyder
- CTO - Kyle Cooper
- COO - Richard Bliss

Operations: Responsible for maintaining the availability of production infrastructure and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.

Information Technology: Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.

Product Development: 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.

## Data

Data, as defined by HostedScan, constitutes the following:

User and account data - this includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Data is categorized into the following major types of data used by HostedScan

| Category | Description | Examples |
|---|---|---|
| Public | Public information is not confidential and can be made public without any implications for HostedScan. | • Press releases<br>• Public website |
| Internal | Access to internal information is approved by management and is protected from external access. | • Internal memos<br>• Design documents<br>• Product specifications<br>• Correspondences |

| | | |
|---|---|---|
| Customer data | Information received from customers for processing or storage by HostedScan. HostedScan must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information. | • Customer operating data<br>• Customer PII<br>• Customer's customers' PII<br>• Anything subject to a confidentiality agreement with a customer |
| Company data | Information collected and used by HostedScan to operate the business. HostedScan must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information. | • Legal documents<br>• Contractual agreements<br>• Employee PII<br>• Employee salaries |

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured, which is utilized by the company in delivering its services.

All personnel and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, HostedScan has policies and procedures in place for proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

## 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 management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

### Physical Security

HostedScan's production servers are maintained by AWS and Linode. The physical and environmental security protections are the responsibility of AWS and Linode. HostedScan reviews the attestation reports and performs a risk analysis of AWS and Linode on at least an annual basis.

### Logical Access

HostedScan provides employees and contractors access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and repeatable user provisioning and deprovisioning processes.

Access to these systems is split into admin roles, user roles, and no access roles. User access and roles are reviewed on an annual basis to ensure least privilege access.

Management is responsible for providing access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing HostedScan's policies, completing security training. These steps must be completed within 14 days of hire.

When an employee is terminated, management is responsible for deprovisioning access to all in-scope systems within 3 days of that employee's termination.

## Computer Operations - Backups

Customer data is backed up and monitored by the CTO for completion and exceptions. If there is an exception, CTO will perform troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS and Linode, with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

## Computer Operations - Availability

HostedScan maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting, and acting upon breaches or other incidents.

HostedScan internally monitors all applications, including the web UI, databases, and cloud storage, to ensure that service delivery matches SLA requirements.

HostedScan utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open source dependencies and maintains an internal SLA for responding to those issues.

## Change Management

HostedScan maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

## Data Communications

HostedScan has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the HostedScan application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

The PaaS provider also automates the provisioning and deprovisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on underlying hardware.

HostedScan uses a number of vulnerability detection tools, including GitHub Dependabot, AWS Guard Duty, and HostedScan itself, to scan for vulnerabilities on a weekly basis.

## BOUNDARIES OF THE SYSTEM

The boundaries of the Continuous Vulnerability Scanning Platform are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Continuous Vulnerability Scanning Platform.

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

## THE APPLICABLE TRUST SERVICES CRITERIA AND THE RELATED CONTROLS

| **Common Criteria (to the Security Category)** |
| --- |
| Security refers to the protection of<br><br>i. Information during its collection or creation, use, processing, transmission, and storage, and<br>ii. Systems that use electronic information to process, transmit, or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removals of information or system resources, misuse of the software, and improper access to or use of, alteration, destruction, or disclosure of information. |

## CONTROL ENVIRONMENT

### Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of HostedScan's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of HostedScan's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees to sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties, is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

### Commitment to Competence

HostedScan's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated the required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

## Management's Philosophy and Operating Style

The HostedScan management team must balance two competing interests: continuing to grow and develop in a cutting-edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way HostedScan can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally, any regulatory changes that may require HostedScan to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- Executive management meetings are held to discuss major initiatives and issues that affect the business.

## Organizational Structure and Assignment of Authority and Responsibility

HostedScan's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities

HostedScan's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

## Human Resource Policies and Practices

HostedScan's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top-quality personnel who ensure the service organization is operating at maximum efficiency. HostedScan's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgment forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Personnel termination procedures are in place to guide the termination process and are documented in a termination checklist.

## RISK ASSESSMENT PROCESS

HostedScan's risk assessment process identifies and manages risks that could potentially affect HostedScan's ability to provide reliable and secure services to our customers. As part of this process, HostedScan maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular HostedScan product development process so they can be dealt with predictably and iteratively.

### Integration with Risk Assessment

The environment in which the system operates, the commitments, agreements, and responsibilities of HostedScan's system, as well as the nature of the components of the system, result in risks that the criteria will not be met. HostedScan addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, HostedScan's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

## INFORMATION AND COMMUNICATION SYSTEMS

Information and communication are an integral component of HostedScan's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

HostedScan uses several information and communication channels internally to share information with management, employees, contractors, and customers. HostedScan uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, HostedScan uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

## MONITORING CONTROLS

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. HostedScan's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

### On-Going Monitoring

HostedScan's management conducts quality assurance monitoring on a regular basis, and additional training is provided based on the results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in HostedScan's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of HostedScan's personnel.

## Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

## CHANGES TO THE SYSTEM

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

## INCIDENTS

No significant incidents have occurred in the services provided to user entities in the 12 months preceding the end of the review date.

## CRITERIA NOT APPLICABLE TO THE SYSTEM

All Common Security Criteria were applicable to the HostedScan's Continuous Vulnerability Scanning Platform system.

## SUBSERVICE ORGANIZATIONS

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

## SUBSERVICE DESCRIPTION OF SERVICES

The Cloud Hosting Services provided by AWS support the physical infrastructure of the entity's services.

## COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

HostedScan’s services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to HostedScan’s services to be solely achieved by HostedScan's control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of HostedScan.

The following subservice organization controls have been implemented by AWS and Linode and included in this report to provide additional assurance that the trust services criteria are met.

| **Subservice Organization - AWS** | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| Security | CC 6.4 | Physical access to data centers is approved by an authorized individual. |
| | | Physical access is revoked within 24 hours of the employee or vendor record being deactivated. |
| | | Physical access to data centers is reviewed on a quarterly basis by appropriate personnel. |
| | | Closed-circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations. |
| | | Access to server locations is managed by electronic access control devices. |

HostedScan management, along with the subservice provider, defines the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, HostedScan performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and subservice organization(s).
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organizations.

## COMPLEMENTARY USER ENTITY CONTROLS

HostedScan's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to HostedScan's services to be solely achieved by HostedScan's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of HostedScan's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to HostedScan.
2. User entities are responsible for notifying HostedScan of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of HostedScan services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize HostedScan services.
6. User entities are responsible for providing HostedScan with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying HostedScan of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

# Section IV

DESCRIPTION OF TEST OF CONTROLS AND RESULTS THEREOF

Relevant trust services criteria and HostedScan LLC's related controls are an integral part of management's system description and are included in this section. Johanson Group LLP performed testing to determine if HostedScan LLC's controls were suitably designed and operating effectively to achieve the specified criteria for the security category set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, Trust Services Criteria, throughout the period March 24, 2025, to June 22, 2025.

Tests of the controls included inquiry of appropriate management, supervisory, and staff personnel, observation of HostedScan LLC activities and operations, and inspection of HostedScan LLC documents and records. The results of those tests were considered in the planning, the nature, timing, and extent of Johanson LLP's testing of the controls designed to achieve the relevant trust services criteria. As inquiries were performed for substantially all HostedScan LLC controls, this test was not listed individually for every control in the tables below.

| Trust Services Criteria | Description of HostedScan LLC's Controls | Service Auditor Test of Controls | Results of Service Auditor Test of Controls |
|---|---|---|---|
| ***CC1.0 - Control Environment*** | | | |
| CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values. | The company performs background checks on new employees. | Inspected HostedScan LLC's sample checks to determine that the company performs background checks on new employees. | No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that there were no new hires during the review period. |
| | The company requires contractor agreements to include a code of conduct or reference to the company's code of conduct. | Inspected HostedScan LLC's Code of Conduct Policy to determine that the company requires contractor agreements to include a code of conduct or reference to the company's code of conduct. | No exceptions noted. |
| | The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy. | Inspected HostedScan LLC's Code of Conduct to determine that the company requires employees to acknowledge a code of conduct at the time of hire. | No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that there were no new hires during the review period. |
| | The company requires contractors to sign a confidentiality agreement at the time of engagement. | Inspected HostedScan LLC's Human Resource Security Policy to determine that the company requires contractors to sign a confidentiality agreement at the time of engagement. | No exceptions noted. |
| | The company requires employees to sign a confidentiality agreement during onboarding. | Inspected HostedScan LLC's employee agreement to determine that the company requires employees to sign a confidentiality agreement during onboarding. | No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that there were no new hires during the review period. |
| | The company managers are required to complete performance evaluations for direct reports at least annually. | Inspected HostedScan LLC's human resource security policy to determine that the company managers are required to complete performance evaluations for direct reports at least annually. | Exception noted. Note: Testing of the control activity disclosed that the performance evaluations were not conducted during the audit period. |

| Trust Services Criteria | Description of HostedScan LLC's Controls | Service Auditor Test of Controls | Results of Service Auditor Test of Controls |
|---|---|---|---|
| CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. | The company's board members have sufficient expertise to oversee management's ability to design, implement, and operate information security controls. The board engages third-party information security experts and consultants as needed. | Inspected HostedScan LLC's ethical management survey to determine that the company's board members have sufficient expertise to oversee management's ability to design, implement, and operate information security controls. The board engages third-party information security experts and consultants as needed. | No exceptions noted. |
| CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls. | Inspected HostedScan LLC's security policies to determine that the company management has established defined roles and responsibilities to oversee. The design and implementation of information security controls. | No exceptions noted. |
| | The company maintains an organizational chart that describes the organizational structure and reporting lines. | Inspected HostedScan LLC's organizational chart to determine that the company maintains and describes the organizational structure and reporting lines. | No exceptions noted. |
| | Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. | Inspected HostedScan LLC's Information Security Roles and Responsibilities to determine that the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the policy. | No exceptions noted. |
| CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. | Inspected HostedScan LLC's Information Security Roles and Responsibilities to determine that the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the policy. | No exceptions noted. |
| | The company performs background checks on new employees. | Inspected HostedScan LLC's sample checks to determine that the company performs background checks on new employees. | No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that there were no new hires during the review period. |
| | The company managers are required to complete performance evaluations for direct reports at least annually. | Inspected HostedScan LLC's human resource security policy to determine that the company managers are required to complete performance evaluations for direct reports at least annually. | Exception noted. Note: Testing of the control activity disclosed that the performance evaluations were not conducted during the audit period. |
| | The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter. | Inspected HostedScan LLC's security awareness training to determine that the company requires employees to complete the training within thirty days of hire and at least annually thereafter. | No exceptions noted. |

| Trust Services Criteria | Description of HostedScan LLC's Controls | Service Auditor Test of Controls | Results of Service Auditor Test of Controls |
|---|---|---|---|
| CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. | Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. | Inspected HostedScan LLC's Information Security Roles and Responsibilities to determine that the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the policy. | No exceptions noted. |
| | The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy. | Inspected HostedScan LLC's Code of Conduct to determine that the company requires employees to acknowledge a code of conduct at the time of hire. | No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that there were no new hires during the review period. |
| | The company managers are required to complete performance evaluations for direct reports at least annually. | Inspected HostedScan LLC's human resource security policy to determine that the company managers are required to complete performance evaluations for direct reports at least annually. | Exception noted. Note: Testing of the control activity disclosed that the performance evaluations were not conducted during the audit period. |
| ***CC2.0 - Communication and Information*** | | | |
| CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. | The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA. | Inspected HostedScan LLC's continuous security monitoring record to determine that it performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively and that corrective actions are taken based on relevant findings. | No exceptions noted. |
| | The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives. | Inspected HostedScan LLC's log management tool to determine that the company utilizes a tool to identify events that may have a potential impact on. The company's ability to achieve its security objectives. | No exceptions noted. |
| | Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation. | Inspected HostedScan LLC's vulnerability scan to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation. | No exceptions noted. |
| CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. | The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns. | Inspected HostedScan LLC's anonymous whistleblower to determine that the company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns. | No exceptions noted. |
| | The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls. | Inspected HostedScan LLC's security policies to determine that the company management has established defined roles and responsibilities to oversee. The design and implementation of information security controls. | No exceptions noted. |

| Trust Services Criteria | Description of HostedScan LLC's Controls | Service Auditor Test of Controls | Results of Service Auditor Test of Controls |
|---|---|---|---|
| | Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. | Inspected HostedScan LLC's Information Security Roles and Responsibilities to determine that the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the policy. | No exceptions noted. |
| | The company's information security policies and procedures are documented and reviewed at least annually. | Inspected HostedScan LLC's Information Security Policies to determine that the company's policies and procedures are documented and reviewed at least annually. | No exceptions noted. |
| | The company communicates system changes to authorized internal users. | Inspected HostedScan LLC's internal communications to determine that the company communicates system changes to authorized internal users. | No exceptions noted. |
| | The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. | Inspected HostedScan LLC's Incident Response Plan to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. | No exceptions noted. |
| | The company provides a description of its products and services to internal and external users. | Inspected HostedScan LLC's network diagram and product documentation site to determine that the company provides a description of its products and services to internal and external users. | No exceptions noted. |
| | The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter. | Inspected HostedScan LLC's security awareness training to determine that the company requires employees to complete the training within thirty days of hire and at least annually thereafter. | No exceptions noted. |
| CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control. | The company notifies customers of critical system changes that may affect their processing. | Inspected HostedScan LLC's public change log or release notes to determine that the company notifies customers of critical system changes that may affect their processing. | No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no critical system changes occurred during the audit period. |
| | The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel. | Inspected HostedScan LLC's customer support to determine that the company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel. | No exceptions noted. |
| | The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS). | Inspected HostedScan LLC's MSA template and publicly available terms of service to determine that the company's security commitments are communicated to customers. | No exceptions noted. |

| Trust Services Criteria | Description of HostedScan LLC's Controls | Service Auditor Test of Controls | Results of Service Auditor Test of Controls |
|---|---|---|---|
| | The company provides guidelines and technical support resources relating to system operations to customers. | Inspected HostedScan LLC's external support resources to determine that the company provides guidelines and technical support resources relating to system operations to customers. | No exceptions noted. |
| | The company provides a description of its products and services to internal and external users. | Inspected HostedScan LLC's network diagram and product documentation site to determine that the company provides a description of its products and services to internal and external users. | No exceptions noted. |
| | The company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity. | Inspected HostedScan LLC's available privacy policy and publicly available terms of service to determine that the company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity. | No exceptions noted. |
| ***CC3.0 - Risk Assessment*** | | | |
| CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. | The company specifies its objectives to enable the identification and assessment of risks related to the objectives. | Inspected HostedScan LLC's risk management policy and risk assessment to determine that the company specifies its objectives to enable. The identification and assessment of risk related to the objectives. | No exceptions noted. |
| | The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected HostedScan LLC's risk management policy to determine that the company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |
| CC3.2 - COSO Principle 7: 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. | The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually. | Inspected HostedScan LLC's tabletop disaster recovery exercise to determine that the company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually. | No exceptions noted. |
| | The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified, and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected HostedScan LLC's Risk Assessment exercise to determine that it is performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified, and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | No exceptions noted. |

| Trust Services Criteria | Description of HostedScan LLC's Controls | Service Auditor Test of Controls | Results of Service Auditor Test of Controls |
|---|---|---|---|
| | The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected HostedScan LLC's risk management policy to determine that the company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |
| | The company has a vendor management program in place. Components of this program include:<br>- critical third-party vendor inventory;<br>- vendor's security and privacy requirements; and<br>- Review of critical third-party vendors at least annually. | Inspected HostedScan LLC's vendor management program to determine that the components of this program include:<br>- critical third-party vendor inventory;<br>- vendor's security and privacy requirements; and<br>- Review of critical third-party vendors at least annually. | No exceptions noted. |
| CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives. | The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified, and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected HostedScan LLC's Risk Assessment exercise to determine that it is performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified, and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | No exceptions noted. |
| | The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected HostedScan LLC's risk management policy to determine that the company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |
| CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control. | The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment. | Inspected HostedScan LLC's Operations Security Policy and CI/CD system to determine that the company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment. | No exceptions noted. |

| Trust Services Criteria | Description of HostedScan LLC's Controls | Service Auditor Test of Controls | Results of Service Auditor Test of Controls |
|---|---|---|---|
| | The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified, and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected HostedScan LLC's Risk Assessment exercise to determine that it is performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified, and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | No exceptions noted. |
| | The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected HostedScan LLC's risk management policy to determine that the company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |
| ***CC4.0 - Monitoring Activities*** | | | |
| CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. | The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA. | Inspected HostedScan LLC's continuous security monitoring record to determine that it performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively and that corrective actions are taken based on relevant findings. | No exceptions noted. |
| | The company has a vendor management program in place. Components of this program include:<br>- critical third-party vendor inventory;<br>- vendor's security and privacy requirements; and<br>- Review of critical third-party vendors at least annually. | Inspected HostedScan LLC's vendor management program to determine that the components of this program include:<br>- critical third-party vendor inventory;<br>- vendor's security and privacy requirements; and<br>- Review of critical third-party vendors at least annually. | No exceptions noted. |
| | Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. | Inspected HostedScan LLC's vulnerability scan to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. | No exceptions noted. |

| Trust Services Criteria | Description of HostedScan LLC's Controls | Service Auditor Test of Controls | Results of Service Auditor Test of Controls |
|---|---|---|---|
| CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate. | The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA. | Inspected HostedScan LLC's continuous security monitoring record to determine that it performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively and that corrective actions are taken based on relevant findings. | No exceptions noted. |
| | The company has a vendor management program in place. Components of this program include:<br>- critical third-party vendor inventory;<br>- vendor's security and privacy requirements; and<br>- Review of critical third-party vendors at least annually. | Inspected HostedScan LLC's vendor management program to determine that the components of this program include:<br>- critical third-party vendor inventory;<br>- vendor's security and privacy requirements; and<br>- Review of critical third-party vendors at least annually. | No exceptions noted. |
| ***CC5.0 - Control Activities*** | | | |
| CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. | The company's information security policies and procedures are documented and reviewed at least annually. | Inspected HostedScan LLC's Information Security Policies to determine that the company's policies and procedures are documented and reviewed at least annually. | No exceptions noted. |
| | The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected HostedScan LLC's risk management policy to determine that the company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |
| CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives. | The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements. | Inspected HostedScan LLC's Secure Development Policy to determine that the company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements. | No exceptions noted. |
| | The company's information security policies and procedures are documented and reviewed at least annually. | Inspected HostedScan LLC's Information Security Policies to determine that the company's policies and procedures are documented and reviewed at least annually. | No exceptions noted. |
| | The company's access control policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access. | Inspected HostedScan LLC's Access Control Policy to determine that the company's policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access. | No exceptions noted. |

| Trust Services Criteria | Description of HostedScan LLC's Controls | Service Auditor Test of Controls | Results of Service Auditor Test of Controls |
|---|---|---|---|
| CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. | The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. | Inspected HostedScan LLC's Data Management Policy to determine that the company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. | No exceptions noted. |
| | The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. | Inspected HostedScan LLC's Operation Security Policy and sample code changes to determine that the company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. | No exceptions noted. |
| | The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements. | Inspected HostedScan LLC's Secure Development Policy to determine that the company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements. | No exceptions noted. |
| | The company's data backup policy documents requirements for backup and recovery of customer data. | Inspected HostedScan LLC's Data Management and Operations Security Policy to determine that the company's data backup policy documents requirements for the backup and recovery of customer data. | No exceptions noted. |
| | Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. | Inspected HostedScan LLC's Information Security Roles and Responsibilities to determine that the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the policy. | No exceptions noted. |
| | The company's information security policies and procedures are documented and reviewed at least annually. | Inspected HostedScan LLC's Information Security Policies to determine that the company's policies and procedures are documented and reviewed at least annually. | No exceptions noted. |
| | The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. | Inspected HostedScan LLC's Incident Response Plan to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. | No exceptions noted. |
| | The company specifies its objectives to enable the identification and assessment of risks related to the objectives. | Inspected HostedScan LLC's risk management policy and risk assessment to determine that the company specifies its objectives to enable. The identification and assessment of risk related to the objectives. | No exceptions noted. |

| Trust Services Criteria | Description of HostedScan LLC's Controls | Service Auditor Test of Controls | Results of Service Auditor Test of Controls |
|---|---|---|---|
| | The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected HostedScan LLC's risk management policy to determine that the company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |
| | The company has a vendor management program in place. Components of this program include:<br>- critical third-party vendor inventory;<br>- vendor's security and privacy requirements; and<br>- Review of critical third-party vendors at least annually. | Inspected HostedScan LLC's vendor management program to determine that the components of this program include:<br>- critical third-party vendor inventory;<br>- vendor's security and privacy requirements; and<br>- Review of critical third-party vendors at least annually. | No exceptions noted. |
| ***CC6.0 - Logical and Physical Access Controls*** | | | |
| 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. | The company maintains a formal inventory of production system assets. | Inspected HostedScan LLC's inventory items to determine that the company maintains a formal inventory of production system assets. | No exceptions noted. |
| | The company restricts access to migrate changes to production to authorized personnel. | Inspected HostedScan LLC's access to migrate changes to production to determine that the company restricts privileged access to authorized personnel. | No exceptions noted. |
| | The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as a unique SSH key. | Inspected HostedScan LLC's authentication to production datastores to determine that they use authorized secure authentication mechanisms, such as a unique SSH key. | No exceptions noted. |
| | The company restricts privileged access to encryption keys to authorized users with a business need. | Inspected HostedScan LLC's access to encryption keys to determine that the company restricts privileged access to encryption keys to authorized users with a business need. | No exceptions noted. |
| | The company's datastores housing sensitive customer data are encrypted at rest. | Inspected HostedScan LLC's data stores housing sensitive customer data to determine that they are encrypted at rest. | No exceptions noted. |
| | The company requires authentication for systems and applications to use a unique username and password or authorized Secure Socket Shell (SSH) keys. | Inspected HostedScan LLC's authentication to systems and applications to determine that they use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys. | No exceptions noted. |
| | The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel. | Inspected HostedScan LLC's Data Management Policy to determine that the company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel. | No exceptions noted. |
| | System access restricted to authorized access only | Inspected HostedScan LLC's access to the application to determine that system access is restricted to authorized access only. | No exceptions noted. |

| Trust Services Criteria | Description of HostedScan LLC's Controls | Service Auditor Test of Controls | Results of Service Auditor Test of Controls |
|---|---|---|---|
| | The company's access control policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access. | Inspected HostedScan LLC's Access Control Policy to determine that the company's policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access. | No exceptions noted. |
| | The company restricts privileged access to databases to authorized users with a business need. | Inspected HostedScan LLC's user access to databases to determine that the company restricts privileged access to databases to authorized users with a business need. | No exceptions noted. |
| | The company restricts privileged access to the firewall to authorized users with a business need. | Inspected HostedScan LLC's firewall configuration to determine that the company restricts privileged access to the firewall to authorized users with a business need. | No exceptions noted. |
| | The company restricts privileged access to the operating system to authorized users with a business need. | Inspected HostedScan LLC's OS access to determine that the company restricts privileged access to the operating system to authorized users with a business need. | No exceptions noted. |
| | The company restricts privileged access to the production network to authorized users with a business need. | Inspected HostedScan LLC's network access to determine that the company restricts privileged access to the production network to authorized users with a business need. | No exceptions noted. |
| | The company ensures that user access to in-scope system components is based on job role and function, or requires a documented access request form and manager approval prior to access being provisioned. | Inspected HostedScan LLC's access request ticket and history to determine that the company ensures that user access to in-scope system components is based on job role and function, or requires a documented access request form and manager approval prior to access being provisioned. | No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that there were no access requests during the review period. |
| | The company requires authentication to the production network to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys. | Inspected HostedScan LLC's authentication to the production network to determine that they use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys. | No exceptions noted. |
| | The company requires passwords for in-scope system components to be configured according to the company's policy. | Inspected HostedScan LLC's password policy configuration to determine that the company requires passwords for in-scope system components to be configured according to the company's policy. | No exceptions noted. |
| | The company's production systems can only be remotely accessed by authorized employees via an approved, encrypted connection. | Inspected HostedScan LLC's SSL/TLS on the admin page of the infrastructure console to determine that the company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection. | No exceptions noted. |
| | The company's network is segmented to prevent unauthorized access to customer data. | Inspected HostedScan LLC's network segregation to determine that the company's network is segmented to prevent unauthorized access to customer data. | No exceptions noted. |

| Trust Services Criteria | Description of HostedScan LLC's Controls | Service Auditor Test of Controls | Results of Service Auditor Test of Controls |
|---|---|---|---|
| | The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method. | Inspected HostedScan LLC's multi-factor authentication to determine that the company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method. | No exceptions noted. |
| CC6.2 - Prior to 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. | The company's access control policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access. | Inspected HostedScan LLC's Access Control Policy to determine that the company's policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access. | No exceptions noted. |
| | The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion. | Inspected HostedScan LLC's proof of completed access reviews to determine that the company conducts these reviews at least quarterly for the in-scope system components, to help ensure that access is restricted appropriately. Required changes are tracked to completion. | No exceptions noted. |
| | The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs. | Inspected HostedScan LLC's Human Resource Security Policy to determine that the company completes termination checklists to ensure that access is revoked for terminated employees within SLAs. | No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no terminated employees occurred during the review period. |
| | The company ensures that user access to in-scope system components is based on job role and function, or requires a documented access request form and manager approval prior to access being provisioned. | Inspected HostedScan LLC's access request ticket and history to determine that the company ensures that user access to in-scope system components is based on job role and function, or requires a documented access request form and manager approval prior to access being provisioned. | No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that there were no access requests during the review period. |
| | The company requires authentication to the production network to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys. | Inspected HostedScan LLC's authentication to the production network to determine that they use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys. | No exceptions noted. |

| Trust Services Criteria | Description of HostedScan LLC's Controls | Service Auditor Test of Controls | Results of Service Auditor Test of Controls |
|---|---|---|---|
| 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, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. | The company's access control policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access. | Inspected HostedScan LLC's Access Control Policy to determine that the company's policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access. | No exceptions noted. |
| | The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion. | Inspected HostedScan LLC's proof of completed access reviews to determine that the company conducts these reviews at least quarterly for the in-scope system components, to help ensure that access is restricted appropriately. Required changes are tracked to completion. | No exceptions noted. |
| | The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs. | Inspected HostedScan LLC's Human Resource Security Policy to determine that the company completes termination checklists to ensure that access is revoked for terminated employees within SLAs. | No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no terminated employees occurred during the review period. |
| | The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned. | Inspected HostedScan LLC's access request ticket and history to determine that the company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned. | No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that there were no access requests during the review period. |
| | The company requires authentication to the production network to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys. | Inspected HostedScan LLC's authentication to the production network to determine that they use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys. | No exceptions noted. |
| CC6.4 - 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. | The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion. | Inspected HostedScan LLC's proof of completed access reviews to determine that the company conducts these reviews at least quarterly for the in-scope system components, to help ensure that access is restricted appropriately. Required changes are tracked to completion. | No exceptions noted. |
| | The entity does not operate any physical hardware, such as servers and network devices, but rather uses subservice organizations and relies on its own controls for physical access. | Not Applicable - Control is implemented and maintained by subservice organizations. | Control is implemented and maintained by subservice organizations. |

| Trust Services Criteria | Description of HostedScan LLC's Controls | Service Auditor Test of Controls | Results of Service Auditor Test of Controls |
|---|---|---|---|
| CC6.5 - 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. | The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed. | Inspected HostedScan LLC's Asset Management Policy to determine that the company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed. | No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no media or devices were considered for destruction during the review period. |
| | The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. | Inspected HostedScan LLC's Data Management Policy to determine that the company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. | No exceptions noted. |
| | The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs. | Inspected HostedScan LLC's Human Resource Security Policy to determine that the company completes termination checklists to ensure that access is revoked for terminated employees within SLAs. | No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no terminated employees occurred during the review period. |
| CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries. | The company requires authentication to the production network to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys. | Inspected HostedScan LLC's authentication to the production network to determine that they use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys. | No exceptions noted. |
| | The company's production systems can only be remotely accessed by authorized employees via an approved, encrypted connection. | Inspected HostedScan LLC's SSL/TLS on the admin page of the infrastructure console to determine that the company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection. | No exceptions noted. |
| | The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches. | Inspected HostedScan LLC's intrusion detection system to determine that the company uses it to provide continuous monitoring of. The company's network and early detection of potential security breaches. | No exceptions noted. |
| | The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. | Inspected HostedScan LLC's SSL/TLS settings on the company website to determine that the company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. | No exceptions noted. |
| | The company reviews its firewall rulesets at least annually. Required changes are tracked to completion. | Inspected HostedScan LLC's firewall review to determine that the company reviews its firewall rulesets at least annually. Required changes are tracked to completion. | No exceptions noted. |

| Trust Services Criteria | Description of HostedScan LLC's Controls | Service Auditor Test of Controls | Results of Service Auditor Test of Controls |
|---|---|---|---|
| | The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually. | Inspected HostedScan LLC's operations security policy to determine that the company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually. | No exceptions noted. |
| | The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. | Inspected HostedScan LLC's vulnerability scan to determine that the company has infrastructure supporting the service, patched as a part of routine maintenance, and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. | No exceptions noted. |
| | The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method. | Inspected HostedScan LLC's multi-factor authentication to determine that the company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method. | No exceptions noted. |
| | The company uses firewalls and configures them to prevent unauthorized access. | Inspected HostedScan LLC's firewall configuration to determine that the company uses firewalls and configures them to prevent unauthorized access. | No exceptions noted. |
| 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. | The company encrypts portable and removable media devices when used. | Inspected HostedScan LLC's device encryption to determine that the company encrypts portable and removable media devices when used. | No exceptions noted. |
| | The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service. | Inspected HostedScan LLC's Vanta Device Monitoring Agent to determine that it is in place to centrally manage mobile devices supporting the service. | No exceptions noted. |
| | The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. | Inspected HostedScan LLC's SSL/TLS settings on the company website to determine that the company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. | No exceptions noted. |
| CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives. | The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements. | Inspected HostedScan LLC's Secure Development Policy to determine that the company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements. | No exceptions noted. |

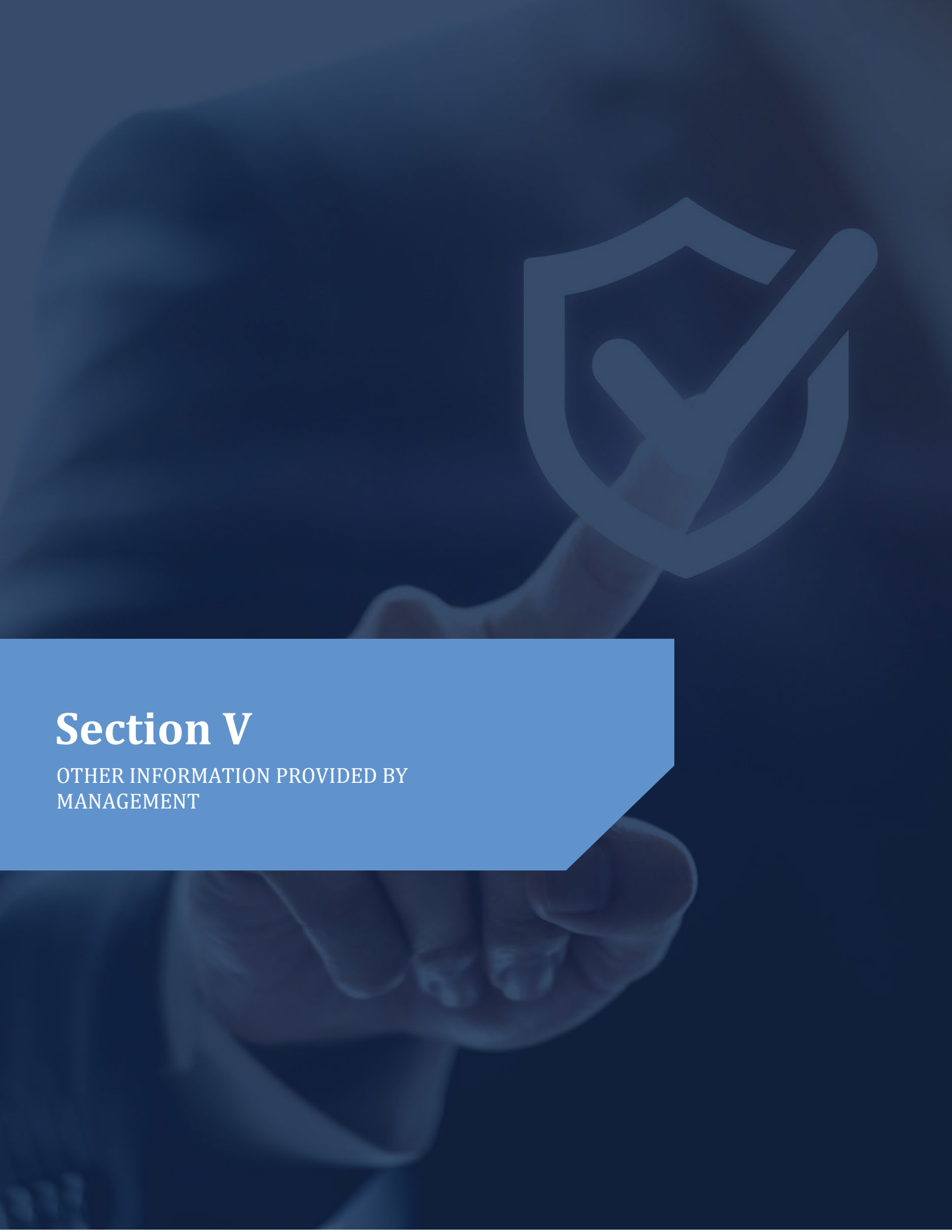
| Trust Services Criteria | Description of HostedScan LLC's Controls | Service Auditor Test of Controls | Results of Service Auditor Test of Controls |
|---|---|---|---|
| | The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems. | Inspected HostedScan LLC's malware detection settings on computers to determine that the company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems. | No exceptions noted. |
| | The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. | Inspected HostedScan LLC's vulnerability scan to determine that the company has infrastructure supporting the service, patched as a part of routine maintenance, and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. | No exceptions noted. |
| ***CC7.0 - System Operations*** | | | |
| CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. | The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment. | Inspected HostedScan LLC's Operations Security Policy and CI/CD system to determine that the company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment. | No exceptions noted. |
| | The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. | Inspected HostedScan LLC's Operation Security Policy and sample code changes to determine that the company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. | No exceptions noted. |
| | The company's formal policies outline the requirements for the following functions related to IT/Engineering: vulnerability management and system monitoring. | Inspected HostedScan LLC's operations security policy to determine that the company's formal policies outline the requirements for the following functions related to IT/Engineering: vulnerability management and system monitoring. | No exceptions noted. |
| | The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected HostedScan LLC's Risk Assessment exercise to determine that it is performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified, and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | No exceptions noted. |

| Trust Services Criteria | Description of HostedScan LLC's Controls | Service Auditor Test of Controls | Results of Service Auditor Test of Controls |
|---|---|---|---|
| | Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation. | Inspected HostedScan LLC's vulnerability scan to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. | No exceptions noted. |
| 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. | The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches. | Inspected HostedScan LLC's intrusion detection system to determine that the company uses it to provide continuous monitoring of. The company's network and early detection of potential security breaches. | No exceptions noted. |
| | The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives. | Inspected HostedScan LLC's log management tool to determine that the company utilizes a tool to identify events that may have a potential impact on. The company's ability to achieve its security objectives. | No exceptions noted. |
| | An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met. | Inspected HostedScan LLC's infrastructure monitoring tool to determine that it is utilized to monitor systems, infrastructure, and performance, and generates alerts when specific predefined thresholds are met. | No exceptions noted. |
| | The company's formal policies outline the requirements for the following functions related to IT/Engineering: vulnerability management and system monitoring. | Inspected HostedScan LLC's operations security policy to determine that the company's formal policies outline the requirements for the following functions related to IT/Engineering: vulnerability management and system monitoring. | No exceptions noted. |
| | The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. | Inspected HostedScan LLC's vulnerability scan to determine that the company has infrastructure supporting the service, patched as a part of routine maintenance, and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. | No exceptions noted. |
| | Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation. | Inspected HostedScan LLC's vulnerability scan to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation. | No exceptions noted. |
| CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a | The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. | Inspected HostedScan LLC's Incident Response Plan to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. | No exceptions noted. |

| Trust Services Criteria | Description of HostedScan LLC's Controls | Service Auditor Test of Controls | Results of Service Auditor Test of Controls |
|---|---|---|---|
| failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures. | The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. | Inspected HostedScan LLC's resolved P1 security issues to determine that the company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. | No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no security and privacy incidents were logged during the review period. |
| CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate. | The company tests its incident response plan at least annually. | Inspected HostedScan LLC's incident tabletop exercise to determine that the company tests its incident response plan at least annually. | No exceptions noted. |
| | The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. | Inspected HostedScan LLC's Incident Response Plan to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. | No exceptions noted. |
| | The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. | Inspected HostedScan LLC's resolved P1 security issues to determine that the company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. | No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no security and privacy incidents were logged during the review period. |
| | The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. | Inspected HostedScan LLC's vulnerability scan to determine that the company has infrastructure supporting the service, patched as a part of routine maintenance, and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. | No exceptions noted. |
| | Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation. | Inspected HostedScan LLC's vulnerability scan to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation. | No exceptions noted. |
| CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents. | The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually. | Inspected HostedScan LLC's tabletop disaster recovery exercise to determine that the company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually. | No exceptions noted. |
| | The company tests its incident response plan at least annually. | Inspected HostedScan LLC's incident tabletop exercise to determine that the company tests its incident response plan at least annually. | No exceptions noted. |

| Trust Services Criteria | Description of HostedScan LLC's Controls | Service Auditor Test of Controls | Results of Service Auditor Test of Controls |
|---|---|---|---|
| | The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. | Inspected HostedScan LLC's Incident Response Plan to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. | No exceptions noted. |
| | The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. | Inspected HostedScan LLC's resolved P1 security issues to determine that the company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. | No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no security and privacy incidents were logged during the review period. |
| ***CC8.0 - Change Management*** | | | |
| CC8.1 - The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives. | The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. | Inspected HostedScan LLC's Operation Security Policy and sample code changes to determine that the company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. | No exceptions noted. |
| | The company restricts access to migrate changes to production to authorized personnel. | Inspected HostedScan LLC's access to migrate changes to production to determine that the company restricts privileged access to authorized personnel. | No exceptions noted. |
| | The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements. | Inspected HostedScan LLC's Secure Development Policy to determine that the company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements. | No exceptions noted. |
| | The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually. | Inspected HostedScan LLC's operations security policy to determine that the company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually. | No exceptions noted. |
| | The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. | Inspected HostedScan LLC's vulnerability scan to determine that the company has infrastructure supporting the service, patched as a part of routine maintenance, and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. | No exceptions noted. |

| Trust Services Criteria | Description of HostedScan LLC's Controls | Service Auditor Test of Controls | Results of Service Auditor Test of Controls |
|---|---|---|---|
| | Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation. | Inspected HostedScan LLC's vulnerability scan to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation. | No exceptions noted. |
| ***CC9.0 - Risk Mitigation*** | | | |
| CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. | The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel. | Inspected HostedScan LLC's Business Continuity and Disaster Recovery Plan to determine that it outlines communication plans in order to maintain information security continuity in the event of the unavailability of key personnel. | No exceptions noted. |
| | The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified, and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected HostedScan LLC's Risk Assessment exercise to determine that it is performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified, and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | No exceptions noted. |
| | The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected HostedScan LLC's risk management policy to determine that the company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |
| CC9.2 - The entity assesses and manages risks associated with vendors and business partners. | The company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity. | Inspected HostedScan LLC's available privacy policy and publicly available terms of service to determine that the company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity. | No exceptions noted. |
| | The company has a vendor management program in place. Components of this program include:<br>- critical third-party vendor inventory;<br>- vendor's security and privacy requirements; and<br>- Review of critical third-party vendors at least annually. | Inspected HostedScan LLC's vendor management program to determine that the components of this program include:<br>- critical third-party vendor inventory;<br>- vendor's security and privacy requirements; and<br>- Review of critical third-party vendors at least annually. | No exceptions noted. |



# Section V

OTHER INFORMATION PROVIDED BY MANAGEMENT

The information included in Section V of this report is presented by the management of HostedScan LLC to provide additional information to user entities and is not a part of the description of the system. The information included here in Section V has not been subjected to the procedures applied in the examination of the description of the system related to the description of the system, and accordingly, Johanson Group LLP expresses no opinion on it.

## Management's Response to Exceptions Noted:

| Description of Company Controls | Criteria Number | Service Auditor's Test of Controls | Result | Management's Response |
|---|---|---|---|---|
| The company managers are required to complete performance evaluations for direct reports at least annually. | CC1.1.6<br>CC1.4.3<br>CC1.5.3 | Inspected HostedScan LLC's human resource security policy to determine that the company managers are required to complete performance evaluations for direct reports at least annually. | Exception noted.<br><br>Service Auditor noted that the performance evaluations were not conducted during the audit period (March 24, 2025 - June 22, 2025) as required by the control. | Performance evaluations are conducted at year's end, and do not occur in the audit window. |