Thoropass™
Assurance

VisiumKMS

System and Organization Controls

(SOC) 2 Type 1 Report

VisiumKMS LLC's Description of the Visium Platform & Guardian and on the Suitability of the Design of Its Controls Relevant to Security As of February 19, 2026

TABLE OF CONTENTS

SECTION 1

Independent Service Auditor's Report

Independent Service Auditor's Report

To: VisiumKMS LLC ("VisiumKMS" or "the Company")

Scope

We have examined VisiumKMS's accompanying description of the Visium Platform & Guardian found in Section 3 titled "Description of the Visium Platform & Guardian As of February 19, 2026" (description), based on the criteria for a description of a service organization's system set forth in DC Section 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 of controls stated in the description as of February 19, 2026, to provide reasonable assurance that VisiumKMS's service commitments and system requirements would be achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022), in AICPA, Trust Services Criteria*.

VisiumKMS uses subservice organizations for infrastructure and data hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at VisiumKMS, to achieve VisiumKMS's service commitments and system requirements based on the applicable trust services criteria. The description presents VisiumKMS's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of VisiumKMS's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

VisiumKMS 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 VisiumKMS's service commitments and system requirements were achieved. In Section 2, VisiumKMS has provided the accompanying assertion titled "Assertion of VisiumKMS LLC Management" (assertion) about the description and the suitability of design of controls stated therein. VisiumKMS is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed 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 a description of a service organization's system and the suitability of the design 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.
- 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.
- Evaluating the overall presentation of the description.

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

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement, including the Code of Professional Conduct established by the AICPA, and we have complied with those requirements. In addition, we applied the Statements on Quality Control Standards established by the AICPA, and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual 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. The projection to the future of any conclusions about the suitability of the design 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.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects—

a. The description presents the Visium Platform & Guardian that were designed and implemented as of February 19, 2026, in accordance with the description criteria.
b. The controls stated in the description were suitably designed as of February 19, 2026, to provide reasonable assurance that VisiumKMS's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organizations applied the complementary controls assumed in the design of VisiumKMS's controls as of that

date.

Restricted Use

This report is intended solely for the information and use of VisiumKMS; user entities of the Visium Platform & Guardian as of February 19, 2026, business partners of VisiumKMS subject to risks arising from interactions with the Visium Platform & Guardian, 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, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- 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.

Thoropass Assurance

Arlington, Virginia

March 11, 2026

SECTION 2

Assertion of VisiumKMS LLC Management

Assertion of VisiumKMS LLC Management

We have prepared the accompanying description of the Visium Platform & Guardian in Section 3 titled “Description of the Visium Platform & Guardian As of February 19, 2026” (description), based on the criteria for a description of a service organization’s system set forth in DC Section 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 the Visium Platform & Guardian that may be useful when assessing the risks arising from interactions with the Visium Platform & Guardian, particularly information about system controls that VisiumKMS 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 Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022), in AICPA, Trust Services Criteria*.

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

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

a. The description presents the Visium Platform & Guardian that were designed and implemented as of February 19, 2026, in accordance with the description criteria.
b. The controls stated in the description were suitably designed as of February 19, 2026, to provide reasonable assurance that VisiumKMS's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organizations applied the complementary controls assumed in the design of VisiumKMS's controls as of that date.

VisiumKMS LLC

SECTION 3

Description of the Visium Platform & Guardian As of February 19, 2026

Description of the Visium Platform & Guardian As of February 19, 2026

Overview of Operations

VisiumKMS LLC ("VisiumKMS" or "the Company") offers the Visium Platform & Guardian, a cloud-based environmental, health, safety (EHS), and operational risk management system designed to help organizations centralize compliance activities, manage safety programs, and track risk-related actions across the enterprise. Both platforms provide the same core functionality but are hosted in different cloud environments.

Guardian is hosted in Amazon Web Services (AWS) and utilizes MongoDB database services, while the Visium Platform is hosted in Microsoft Azure. The system enables users to document incidents, conduct risk assessments, manage audits, assign corrective actions, and monitor recurring compliance obligations within structured, workflow-driven processes. By consolidating safety, regulatory, and operational data into a single system, the platforms support transparency, accountability, and standardized execution of EHS and process safety activities.

The Visium Platform & Guardian are designed to streamline regulatory compliance, improve visibility into organizational risk posture, and enhance oversight through configurable dashboards and reporting capabilities. The systems support role-based access, action tracking, and auditable records to promote operational consistency and readiness for internal and external reviews, while maintaining the confidentiality, integrity, and availability of safety and compliance data.

The system description in this section of the report details the Visium Platform & Guardian. Any other Company services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of the subservice organizations).

Principal Service Commitments and System Requirements

Service commitments are declarations made by management to customers regarding the performance and security of the Visium Platform & Guardian. The Master Service Agreement (MSA) includes the communication of the Company's commitments to its customers. Changes to any commitments are communicated to customers.

System requirements are specifications that define how the Visium Platform & Guardian are designed and operated in order to meet the Company's principal commitments to customers. These requirements are specified in the Company's policies and procedures, system design documentation, contractual obligations, and applicable laws and regulations.

The Company's principal service commitments and system requirements related to the Visium Platform & Guardian include the following:

Security Service Commitment and System Requirements

VisiumKMS will implement reasonable security and safety policies, procedures, and rules to protect customer data.

To meet this commitment, the Company has established system requirements, including:

- Change Management
- Encryption Standards
- Identity and Access Management
- Network Security and Segmentation

- Policy Management and Governance
- Security Awareness Training
- Security Incident Response
- Security Monitoring and Reporting
- Threat and Vulnerability Management
- Vendor Risk Management

The Components of the System Used to Provide the Service

The boundaries of the Visium Platform & Guardian include the aspects of the Company's infrastructure, software, people, procedures, and data that are necessary to deliver the service and directly support its operation. Supporting functions that are integral to the operation and control of the service (for example, IT support and human resources) are also considered within the system boundaries. Functions and activities that do not directly or indirectly contribute to the delivery, security, or availability of the service are excluded from the boundaries of the Visium Platform & Guardian.

The subsections below describe the components that support the operation of the Visium Platform & Guardian.

Infrastructure

The Company utilizes AWS and MongoDB as subservice organizations to provide infrastructure and data hosting services that support Guardian. The Company also utilizes Microsoft Azure as a subservice organization to provide infrastructure and data hosting services that support the Visium Platform. By leveraging the resiliency, scalability, and security features of these infrastructure services, the Company is able to host and operate the Visium Platform & Guardian in a secure and reliable manner that meets current and future demand.

The Company remains responsible for designing, configuring, and maintaining the system architecture within AWS, Microsoft Azure, and MongoDB to ensure that security, availability, and resiliency requirements are met.

The in-scope hosted infrastructure components are outlined in the table below:

Infrastructure Component	Business Function	Hosted Location
Amazon Elastic Compute Cloud (EC2)	Cloud Compute	AWS
Amazon Elastic Container Service (ECS)	Container Orchestration	AWS
Amazon Simple Storage Service (S3)	Data Storage	AWS
Amazon Virtual Private Cloud (VPC)	Network Segmentation	AWS
AWS Security Groups	Network Traffic Control	AWS
Azure App Service	Application Hosting and Deployment	Azure
Azure Network Security Groups	Network Traffic Control	Azure
Azure SQL	Data Storage	Azure

Infrastructure Component	Business Function	Hosted Location
Azure Storage	Data Storage	Azure
Azure Virtual Machine (VM)	Virtual Machine	Azure
Azure Virtual Network	Network Traffic Control	Azure
Microsoft SQL Server	Data Storage	AWS
MongoDB Atlas	Data Storage	MongoDB

Software

The Company leverages software components to operate the Visium Platform & Guardian and deliver services to its customers. These include applications, platforms, and supporting tools used to build, secure, monitor, and maintain the environment. The Company remains responsible for selecting, implementing, and maintaining these software components to ensure that applicable system requirements are met.

The in-scope software components are outlined in the table below:

Software Component	Business Function
Amazon CloudWatch	Infrastructure Monitoring
Amazon Elastic Container Registry (ECR)	Container Registry
Amazon GuardDuty	Threat Detection
Amazon Identity Access Management (IAM)	Identity and Access Management
AWS CloudTrail	Security Monitoring and Log Management
Azure Activity Logs	Security Monitoring and Log Management
Azure DevOps	Code Development and Deployment
Azure Monitor	Infrastructure Monitoring
Certn	Employment Background Checks
GitHub	Code Repository
Jira	Ticketing System

Software Component	Business Function
Microsoft Defender for Cloud	Threat Detection
Microsoft Entra ID	Single Sign-On (SSO) and Authentication

People

The Company's personnel are responsible for operating, securing, and supporting the Visium Platform & Guardian. Personnel perform activities necessary to deliver the Company's services, including governance, operations, customer support, and security-related functions. The Company remains responsible for recruiting, training, and overseeing personnel to ensure that their roles are performed in accordance with applicable policies and requirements.

The in-scope personnel roles and responsibilities are outlined in the table below:

Role/Unit Name	Responsibilities
Engineering	Responsible for the design, development, testing, deployment, and maintenance of software and system components.
Executive Management	Responsible for providing strategic leadership, overseeing company-wide activities, and ensuring organizational goals and objectives are established, communicated, and achieved.

Procedures

The Company relies on documented automated and manual procedures to govern the operation, security, and support of the Visium Platform & Guardian. These procedures are maintained in alignment with the Company's Information Security Policy and are reviewed and updated as necessary for changes in the business, but no less than annually. The Company remains responsible for developing, implementing, and maintaining these procedures to ensure they are followed consistently and support the Company's operational and compliance objectives.

The in-scope procedures are outlined in the table below:

Procedure	Description
Access Control	How the Company restricts access to its systems and facilities, provisions and removes access rights, and prevents unauthorized access.
Asset Management	How the Company tracks and manages its assets, including hardware and software, to ensure accurate records, compliance with requirements, and protection of resources.

Procedure	Description
Business Continuity and Disaster Recovery	How the Company identifies the steps to be taken in the event of a disaster to help resume business operations.
Change Management	How the Company identifies, reviews, and implements system changes using a controlled process to prevent unauthorized or untested changes.
Data Classification, Handling, and Retention	How the Company classifies data, establishes requirements for its secure handling and storage, determines retention periods in compliance with requirements, and securely disposes of records when no longer needed.
Incident Management	How the Company detects, reports, responds to, and manages incidents that could affect the operation or protection of the system, in order to minimize impact and support recovery.
Monitoring and Logging	How the Company collects, reviews, and analyzes system activity logs and alerts to detect and respond to unusual or unauthorized activity.
Risk and Vendor Management	How the Company identifies, assesses, and mitigates risks to the system, including risks arising from business disruptions, operations, and the use of vendors and business partners by evaluating, selecting, and monitoring vendors to ensure they meet security and compliance requirements.
Security Awareness and Training	How the Company trains personnel on security and compliance requirements and monitors completion of training activities.
System Operations	How the Company manages and monitors system operations and responds to deviations, including security-related events.

Data

Data refers to transaction streams, files, data stores, tables, and other outputs used or processed by the Visium Platform & Guardian. While the Company maintains data necessary for the operation and support of the Visium Platform & Guardian, customers remain responsible for defining and controlling the data they provide and maintain within the Visium Platform & Guardian. The Company remains responsible for managing and protecting that data in accordance with its policies, contractual commitments, and applicable regulatory requirements.

Encryption is enabled for data stores housing customer data. Secure data transmission protocols are used to encrypt customer data when transmitted over public networks.

System Incidents

A system event is defined as an occurrence that could lead to the loss of, or disruption to, operations, services, or functions and result in VisiumKMS's failure to achieve its service commitments or system requirements. Such an occurrence may arise from actual or attempted access or use by internal or external parties and may:

- Impair or potentially impair the availability, integrity, or confidentiality of information or systems.
- Result in unauthorized disclosure or theft of information or other assets, or the destruction or corruption of data.
- Cause damage to systems.

Such occurrences also may arise from the failure of the Visium Platform & Guardian to process data as designed or from the loss, corruption, or destruction of data used by the Visium Platform & Guardian.

On the other hand, a system incident is defined as a system event that requires action on the part of VisiumKMS management to prevent or reduce the impact of the event on VisiumKMS's achievement of its service commitments and system requirements.

There were no identified significant system incidents that (a) resulted from controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements, or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements as of February 19, 2026.

The Applicable Trust Services Criteria and Related Controls

Applicable Trust Services Criteria

The Trust Services Category that is in scope for the purposes of this report is Security.

- **Security:** Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

The common criteria are organized as follows:

1. **Control Environment:** The criteria relevant to how the entity is structured and the processes the entity has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values, qualifications of personnel, and the environment in which they function.
2. **Information and Communication:** The criteria relevant to how the entity communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.
3. **Risk Assessment:** The criteria relevant to how the entity (i) identifies potential risks that would affect the entity’s ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.
4. **Monitoring Activities:** The criteria relevant to how the entity monitors the system, including the suitability and design and operating effectiveness of the controls, and acts to address deficiencies identified.
5. **Control Activities:** The criteria relevant to the actions established through policies and procedures that help ensure that management’s directives to mitigate risks to the achievement of objectives are carried out.
6. **Logical and Physical Access Controls:** The criteria relevant to how the entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
7. **System Operations:** The criteria relevant to how the entity manages the operation of a system and detects and mitigates processing deviations, including logical and physical security deviations.
8. **Change Management:** The criteria relevant to how the entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
9. **Risk Mitigation:** The criteria relevant to how the entity identifies, selects, and develops risk mitigation

activities arising from potential business disruptions and the use of vendors and business partners.

This report is focused solely on the Security category.

Control Environment

Integrity and Ethical Values

VisiumKMS places emphasis on ethics and communication within the organization. Management communicates and oversees the Code of Conduct, which defines expected responsibilities and behavior regarding data and information system usage. All personnel are required, upon hire, to acknowledge in writing that they have received, read, and understood its contents.

VisiumKMS demonstrates its commitment to integrity in all interactions with customers, vendors, and personnel by maintaining documented policies that establish ethical and business conduct standards. These policies guide decision-making, reinforce accountability, and support the control environment.

As part of its compliance framework, VisiumKMS maintains an inventory of third-party service providers that support the system. These providers are contractually obligated to adhere to information security requirements and to report cybersecurity incidents in a timely manner, ensuring that vendor practices align with VisiumKMS's integrity and security requirements.

Oversight and Authority

The Risk Committee is tasked with governance, oversight, and responsibilities relative to internal control. The Risk Committee includes members that are independent of the internal control function. The Risk Committee meets quarterly and maintains formal meeting minutes.

Organizational Structure

VisiumKMS's organizational structure provides a framework for planning, executing, and controlling business operations. Roles and responsibilities are formally documented, communicated, and assigned to ensure adequate staffing, operational efficiency, segregation of duties, and oversight of the security and control environment. Management has also established clear authority levels and reporting lines for key personnel to maintain accountability. VisiumKMS follows a formal onboarding program to assist new personnel as they become familiar with organizational processes, systems, policies, and procedures. This structure supports alignment of responsibilities with the Company's internal control, compliance, and security objectives.

Management's Philosophy and Operating Style

VisiumKMS's management adopts an active and engaged approach to business operations, maintaining close communication with the workforce and key vendor representatives. Management emphasizes ethical conduct, responsibility, and compliance with established policies across all areas of the organization.

The leadership team is directly involved in setting strategic objectives, overseeing operational activities, and reinforcing the importance of security, confidentiality, and integrity in daily practices. This operating style promotes a culture of transparency, responsiveness, and proactive risk management, ensuring that decisions align with the Company's objectives and requirements.

Authority and Responsibility

VisiumKMS assigns appropriate levels of authority and responsibility to personnel across the organization to facilitate effective internal control. Roles and responsibilities are documented and communicated through job descriptions, policies, and procedures to ensure individuals understand their obligations in maintaining security and compliance.

Oversight mechanisms are in place to review and approve critical activities, ensuring that responsibilities are appropriately segregated to reduce the risk of conflicts of interest and unauthorized actions.

Human Resources

All new personnel are subject to pre-employment screening, such as reference or background checks, consistent with the Company's hiring practices, before being granted access to production systems or sensitive data. As part of the onboarding process, personnel are also required to review and sign confidentiality agreements, reinforcing their obligation to safeguard company and customer information and prohibiting unauthorized disclosure of data.

The Company follows a structured onboarding program to familiarize new personnel with security policies, operational processes, and role-specific responsibilities. Information security training is mandatory upon hire and reinforced through annual refresher training to ensure personnel understand the Company's security practices, their role in protecting systems and data, and key concepts such as cybersecurity threats, phishing and social engineering, malware, secure data handling, authentication practices, and incident reporting. Supplemental awareness campaigns and targeted communications are also used to strengthen security awareness throughout the year.

The Company has implemented a performance management process to provide feedback, assess effectiveness, and align individual objectives with organizational goals.

Information and Communication

VisiumKMS maintains an Information Security Policy that defines the information security rules and requirements for the service environment. The policy is reviewed and approved by management and communicated to all relevant personnel.

Processes are in place to ensure that critical information related to security, system availability, and compliance objectives is communicated effectively both internally and externally. Management ensures that personnel receive timely updates on new or revised policies, control requirements, and operational procedures through established communication channels such as internal knowledge bases, scheduled briefings, and formal announcements.

The Company maintains documented guidance describing how personnel should escalate incidents, compliance concerns, or process deviations. Communication lines are structured to ensure that information reaches the appropriate decision-makers without unnecessary delay, including mechanisms for reporting control exceptions and protocols for sharing updates with clients and vendors.

To promote transparency with stakeholders, VisiumKMS provides documentation describing service features, security practices, and compliance measures. This documentation is reviewed and updated periodically to reflect changes in systems or requirements.

Risk Assessment and Mitigation

VisiumKMS maintains a formal risk assessment process to identify, evaluate, and manage risks that could affect its objectives and the delivery of secure, reliable services. Each identified risk is evaluated and rated to ensure that appropriate controls are designed and implemented to mitigate the most significant threats to the Company's systems and operations.

The risk assessment is conducted annually and updated in response to significant changes in technology, operations, regulatory requirements, business strategy, or other emerging risks. This ensures new risks are identified and addressed in a timely manner.

VisiumKMS applies a structured methodology that includes:

- Identifying threats – considering internal and external factors such as technology, operations, personnel, vendor dependencies, and regulatory changes.
- Analyzing vulnerabilities – assessing weaknesses in processes, technology, and personnel that could expose the Company to exploitation.
- Estimating likelihood of impact – evaluating the probability that a vulnerability could be successfully exploited.
- Assessing severity of impact – analyzing potential consequences, including operational, financial, reputational, and regulatory implications.
- Ranking and prioritizing risks – combining likelihood and impact ratings to establish a risk score and guide remediation priorities.

Assessment results are reviewed by management and used to inform the design and implementation of controls, security policies, and ongoing risk mitigation activities. Mitigation strategies include implementing preventive and detective controls, monitoring key risk indicators, and formally tracking remediation activities through completion.

The process is integrated into the Company’s governance, risk, and compliance (GRC) framework to ensure that risks are continuously identified, evaluated, and addressed in strategic planning and operational decision-making.

Vendor Management

VisiumKMS maintains a Vendor Management Policy that governs the selection, onboarding, and ongoing oversight of third-party service providers. The policy includes requirements for classifying vendors based on criticality, assessing risks associated with the procurement of third-party services, and reviewing vendor performance on an ongoing basis.

Formal agreements are established with all critical vendors, and these agreements include commitments applicable to the services provided. To ensure that vendor controls remain effective, VisiumKMS obtains and reviews third-party attestation reports or performs a vendor risk assessment on an annual basis. Exceptions or control gaps identified in these reviews are evaluated to determine their potential impact on the Visium Platform & Guardian and addressed through remediation or compensating measures where necessary.

Through these activities, vendor risks are identified, monitored, and mitigated as part of VisiumKMS's broader GRC framework.

Monitoring

The systems within the boundary are configured to support continuous monitoring, detection, alerting, and testing for vulnerabilities and threats. Management reviews system alerts promptly and supports monitoring through preventive, detective, and corrective audit logging. Relevant monitoring outputs are shared with executive and management personnel to ensure timely awareness and action.

Vulnerability Management and Testing

VisiumKMS maintains a documented Vulnerability Management Policy that defines methods for identifying vulnerabilities, assessing their severity, and prioritizing remediation or mitigation activities within defined timelines. The policy provides the framework for consistent execution of vulnerability management practices.

In alignment with this policy, VisiumKMS performs both automated and manual security testing at regular intervals. Container image vulnerability scans are performed on a scan-on-push basis to identify, quantify, and prioritize vulnerabilities. Infrastructure supporting the service is patched as a part of routine maintenance to help ensure that systems supporting the service are hardened against security threats. Penetration testing is performed annually to identify vulnerabilities that could be exploited to gain access to the production environment. Identified vulnerabilities are ranked and remediated in accordance with the Company's Vulnerability Management Policy and related procedures.

Threat Monitoring and Logging

The Company employs log management tools to monitor and analyze security events and trends that may impact its ability to achieve security objectives. A system monitoring tool is utilized to monitor system availability and performance and generates alerts when specific, predefined thresholds are met. An intrusion detection system (IDS) is used to provide continuous monitoring of the Company's network and early detection of potential security breaches and generates alerts when security events occur. Anti-malware technology is deployed for environments commonly susceptible to malicious attacks and is configured to be updated routinely, logged, and installed on production servers.

Alerting and Escalation

The Company employs a distributed monitoring approach that combines commercially available tools, custom code, and instant messaging platforms. This system attributes critical security events to their source and sends targeted alerts to authorized personnel with the authority and context necessary to validate them. Alerts are reviewed by authorized personnel, who address them when appropriate or escalate to designated teams for resolution.

Control Activities

VisiumKMS has implemented documented policies, procedures, and technical controls to mitigate identified risks and support the Company's objectives and requirements. Control activities are designed and implemented across the organization, embedded into business processes, and aligned with objectives for safeguarding systems and data. These activities include:

- **Governance and Policy Controls** – Documented policies and standards that define responsibilities and expected practices for personnel.
- **Technical and Monitoring Controls** – Safeguards and monitoring mechanisms designed to prevent, detect, and respond to unauthorized or anomalous activity.
- **Operational Controls** – Processes that integrate security and compliance practices into daily operations.
- **Third-Party Oversight Controls** – Oversight of vendors and service providers through contractual requirements, risk assessments, and periodic reviews.

Together, these control activities form a structured framework that mitigates risks to the service and supports the Company's objectives and requirements.

Logical Access

VisiumKMS maintains a documented Access Control Policy that defines the requirements for provisioning and deprovisioning users, performing access reviews and recertifications, and restricting access based on separation of duties and least privilege. Access reviews are conducted to confirm that system access remains appropriate and access is modified or removed as necessary. Password configurations for system components are enforced in accordance with VisiumKMS's Password Policy.

Access to system components is based on job role and function, and requires a documented request with manager approval prior to provisioning. Users are assigned unique user IDs before being granted access. Access rights are assigned using Role-Based Access Control (RBAC) and the principle of least privilege, ensuring users are granted only the access required for their job duties. Privileged access to system components is restricted to authorized users with a business need, and access to production infrastructure requires valid multi-factor authentication (MFA) tokens. Access to system components is revoked within 24 hours of termination as part of the termination process.

System Operations

VisiumKMS maintains a documented Incident Response Policy that establishes a structured process for preparing for, detecting, responding to, and recovering from incidents. The policy also defines requirements for analysis, communication, follow-up, and training to strengthen resilience and improve future response. Personnel responsibilities during a breach, the steps for managing an incident, and the importance of information security awareness are documented and communicated to all personnel.

The Incident Response Team employs industry-standard procedures such as identification, verification, classification, and prioritization to drive effective resolution during business-impacting events. Alerts are reviewed, triaged, and escalated according to severity, ensuring timely involvement of technical and management stakeholders.

Post-mortems are convened after any significant operational issue, regardless of whether external impact occurred. Findings are documented to capture the root cause, identify lessons learned, and track preventative or corrective actions to completion. The incident response plan is tested annually to assess the effectiveness of the incident response program.

Change Management

VisiumKMS maintains a documented Change Management Policy to guide the processes for requesting, documenting, reviewing, approving, testing, scheduling, and implementing changes. All changes are recorded in a centralized system of record to ensure traceability, accountability, and auditability. Changes that may affect system availability, security, or confidentiality are communicated to management and any affected partners.

System configuration standards are documented and implemented to ensure systems and network devices are securely configured. Hardening standards are documented and include guidance on baseline security requirements for production systems before deployment to the production environment.

Secure Software Development: VisiumKMS applies a systematic approach to software development so that changes to customer-impacting services are reviewed, tested, approved, and communicated. Prior to deployment, changes are:

- Developed in an environment segregated from production.
- Reviewed by authorized personnel for accuracy, appropriateness, and security impact.

- Tested to confirm expected functionality and ensure performance and security are not adversely affected.
- Approved by authorized personnel to provide oversight and confirm that business impacts are understood.

Complementary User Entity Controls (CUECs)

In designing its controls, VisiumKMS management did not identify any CUECs that would be necessary, in combination with controls at VisiumKMS, to provide reasonable assurance that its principal service commitments and system requirements would be achieved. Accordingly, no CUECs are required to achieve the service commitments and system requirements based on the applicable trust services criteria.

User Entity Responsibilities

VisiumKMS's controls related to the Visium Platform & Guardian are sufficient, in and of themselves, to achieve its principal service commitments and system requirements. Accordingly, no CUECs are required. However, user entities remain responsible for implementing and maintaining their own internal controls to ensure the proper use of the Visium Platform & Guardian within their environments. These responsibilities are intended to support each user entity’s broader control environment, ensure the effective use of the services provided, and help user entities derive benefit from those services. The following responsibilities are illustrative and should not be considered a comprehensive listing.

User entities should:

- Report any material changes to their control environment that may impact the services performed by the Company, in accordance with contractually defined time frames.
- Notify the Company of changes to the authorized user list and vendor security requirements.
- Grant access only to authorized and trained personnel and revoke access timely when access is no longer required.
- Maintain physical security and environmental controls at their facilities and for remote workers.
- Implement controls for managing user IDs and passwords used to access the Company’s services.
- Notify the Company of any known or suspected security incidents.

Each user entity should assess its own control environment to determine whether additional responsibilities are needed to ensure the effective use of the services and to derive benefit from them.

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS, Microsoft Azure, and MongoDB as subservice organizations. The Company’s controls related to the Visium Platform & Guardian cover only a portion of the overall internal control for each user entity of the Visium Platform & Guardian. The description does not extend to the services provided by the subservice organizations. Section 4 of this report and the description of the system only cover the Trust Services Criteria and related controls of the Company and exclude the related controls of AWS, Microsoft Azure, and MongoDB.

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. Accordingly, CSOCs are expected to be in place at AWS, Microsoft Azure, and MongoDB as described in the CSOC table below.

Through its operational activities, Company management monitors the services performed by AWS, Microsoft

Azure, and MongoDB to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organizations to monitor compliance with the service agreement, stay informed of changes planned at the hosting facilities, and relay any issues or concerns to AWS, Microsoft Azure, and MongoDB management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the Visium Platform & Guardian to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and related tests and results described in Section 4 of this report, taking into account the related CSOCs expected to be implemented at AWS, Microsoft Azure, and MongoDB as described below.

Criteria	Complementary Subservice Organization Controls (CSOCs)
CC6.1	AWS, Microsoft Azure, and MongoDB are responsible for encrypting customer data at rest and in transit within the managed infrastructure to mitigate the risk of unauthorized access to sensitive data. AWS, Microsoft Azure, and MongoDB are responsible for implementing access control over the managed infrastructure to mitigate the risk of unauthorized access or privilege escalation.
CC6.4	AWS, Microsoft Azure, and MongoDB are responsible for restricting physical access to their data centers through approval and revocation processes, surveillance and access control mechanisms, periodic reviews of access rights, and retention of monitoring records to mitigate the risk of unauthorized access, intrusion, or physical tampering.
CC6.5	AWS, Microsoft Azure, and MongoDB are responsible for securely decommissioning production assets in their control and ensuring that data is rendered unreadable or unrecoverable through logical deletion, cryptographic erasure, or physical destruction once no longer required, to mitigate the risk of unauthorized recovery of data from retired equipment.
CC6.6	AWS, Microsoft Azure, and MongoDB are responsible for applying security patches to the managed infrastructure as part of routine maintenance to mitigate the risk of vulnerabilities being exploited due to outdated systems.
CC7.2	AWS, Microsoft Azure, and MongoDB are responsible for implementing and maintaining environmental protection measures at their data centers, including fire detection and suppression systems, temperature and humidity controls, uninterruptible power supply (UPS) units, backup power sources, and monitoring of environmental conditions, to mitigate the risk of outages, equipment failure, or data loss due to environmental hazards or power disruptions.
CC8.1	AWS, Microsoft Azure, and MongoDB are responsible for implementing managed infrastructure changes to mitigate the risk of unauthorized or untested changes affecting system availability, integrity, or confidentiality.

Specific Criteria Not Relevant to the System

There were no specific Security Trust Services Criteria as set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022), in AICPA, Trust Services Criteria* that were not relevant to the system as presented in this report.

Report Use

The description does not omit or distort information relevant to the Visium Platform & Guardian while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to their particular needs.

SECTION 4

Trust Services Criteria and Related Controls Relevant to the Security Category

Trust Services Criteria and Related Controls Relevant to the Security Category

This SOC 2 Type 1 Report was prepared in accordance with the AICPA Attestation Standards based on the criteria for a description of a service organization's system set forth in DC Section 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 of controls stated in the description as of February 19, 2026.

Description of Evaluation Procedures Performed

Thoropass Assurance evaluated the design and implementation of the controls listed in this section as of February 19, 2026. Our evaluation included procedures we considered necessary in the circumstances to determine whether the control activities were suitably designed to achieve the service commitments and system requirements based on the relevant trust services criteria and had been implemented as described as of February 19, 2026.

In determining the nature, timing, and extent of procedures performed, we considered the following factors:

- The nature and timing of the controls being tested.
- The types of evidential matter.
- The appropriateness of the control design relative to the applicable trust services criteria.
- The assessed level of control risk.
- The entity's control environment and related governance processes.

The procedures performed included:

- **Inquiry:** Conducted detailed discussions with relevant stakeholders to understand the control environment and assess the design and implementation of each control.
- **Observation:** Observed the design and implementation of controls to confirm they were implemented as described.
- **Inspection:** Inspected relevant documentation, configurations, and reports to corroborate that controls were suitably designed and in place.

Where applicable, we evaluated the reliability of Information Produced by the Entity (IPE) used in the execution of control activities by:

- Inspecting the source of the IPE.
- Reviewing the logic or parameters used to generate the information.
- Comparing the information to the source records to confirm its accuracy and completeness.

These procedures were designed to assess the suitability of design and implementation of the controls.

This section of the report includes 2 tables:

Table 1: VisiumKMS Controls Mapped to the Security Criteria

Table 2: Description of the Applicable Control Activities

Table 1: VisiumKMS Controls Mapped to the Security Criteria

Control Environment		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC1.1	REQ-7 REQ-8 REQ-9 REQ-10 REQ-11 REQ-14	The entity demonstrates a commitment to integrity and ethical values.
CC1.2	REQ-3 REQ-4	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3	REQ-2 REQ-4 REQ-15 REQ-16	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Control Environment

Criteria	Applicable Control Activities	Criteria Description
CC1.4	REQ-12 REQ-13 REQ-14 REQ-15	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5	REQ-7 REQ-8 REQ-14 REQ-15	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Information and Communication

Criteria	Applicable Control Activities	Criteria Description
CC2.1	REQ-4 REQ-19 REQ-20 REQ-39 REQ-46 REQ-47	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

Information and Communication

Criteria	Applicable Control Activities	Criteria Description
CC2.2	REQ-2 REQ-12 REQ-13 REQ-15 REQ-56	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
CC2.3	REQ-5 REQ-6 REQ-22	The entity communicates with external parties regarding matters affecting the functioning of internal control.

Risk Assessment

Criteria	Applicable Control Activities	Criteria Description
CC3.1	REQ-17 REQ-18	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
CC3.2	REQ-17 REQ-19 REQ-58 REQ-59	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.

Risk Assessment

Criteria	Applicable Control Activities	Criteria Description
CC3.3	REQ-17 REQ-19	The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4	REQ-17 REQ-19 REQ-44 REQ-45	The entity identifies and assesses changes that could significantly impact the system of internal control.

Monitoring Activities		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC4.1	REQ-4 REQ-19 REQ-20 REQ-23 REQ-44 REQ-45 REQ-46 REQ-47	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
CC4.2	REQ-4 REQ-19 REQ-20 REQ-23	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.

Control Activities

Criteria	Applicable Control Activities	Criteria Description
CC5.1	REQ-17 REQ-20	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
CC5.2	REQ-17 REQ-20	The entity also selects and develops general control activities over technology to support the achievement of objectives.
CC5.3	REQ-1 REQ-17 REQ-21 REQ-24 REQ-32 REQ-42 REQ-48 REQ-51 REQ-53	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Logical and Physical Access Controls

Criteria	Applicable Control Activities	Criteria Description
CC6.1	REQ-25 REQ-26 REQ-28 REQ-33 REQ-34 REQ-36 REQ-54 REQ-57	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.
CC6.2	REQ-29 REQ-30 REQ-31	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.
CC6.3	REQ-29 REQ-30 REQ-31	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.
CC6.4	The Company's production environment is hosted at third-party data centers, which have been carved out for the purposes of this report.	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.

Logical and Physical Access Controls

Criteria	Applicable Control Activities	Criteria Description
CC6.5	REQ-32 REQ-33	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.
CC6.6	REQ-27 REQ-35 REQ-37 REQ-40 REQ-43	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7	REQ-35 REQ-39	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.
CC6.8	REQ-38 REQ-39 REQ-43	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

System Operations

Criteria	Applicable Control Activities	Criteria Description
CC7.1	REQ-19 REQ-46 REQ-47	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.
CC7.2	REQ-39 REQ-40 REQ-41 REQ-43 REQ-44 REQ-45 REQ-46 REQ-47	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.
CC7.3	REQ-39 REQ-44 REQ-45 REQ-46 REQ-47 REQ-48	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

System Operations

Criteria	Applicable Control Activities	Criteria Description
CC7.4	REQ-43 REQ-48 REQ-49 REQ-50	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
CC7.5	REQ-48 REQ-49 REQ-50 REQ-58 REQ-59	The entity identifies, develops, and implements activities to recover from identified security incidents.

Change Management

Criteria	Applicable Control Activities	Criteria Description
CC8.1	REQ-43 REQ-54 REQ-55 REQ-57	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Risk Mitigation

Criteria	Applicable Control Activities	Criteria Description
CC9.1	REQ-17 REQ-48 REQ-49 REQ-58 REQ-59	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2	REQ-22 REQ-23	The entity assesses and manages risks associated with vendors and business partners.

Table 2: Description of the Applicable Control Activities

Control activities tested in connection with determining the design of controls relative to the applicable Trust Services Criteria are described below.

Control #	Applicable Control Activities
REQ-1	An Information Security Policy is documented and defines the information security rules and requirements for the service environment. The policy is version controlled, reviewed annually, approved by management, and communicated to authorized users.
REQ-2	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment.
REQ-3	The Risk Committee is tasked with governance, oversight, and responsibilities relative to internal control. The Risk Committee includes members that are independent of the internal control function.
REQ-4	The Risk Committee meets quarterly and maintains formal meeting minutes.
REQ-5	The Master Service Agreement (MSA) includes the communication of the Company's commitments to its customers.
REQ-6	Technical support resources related to system operations are provided on the Company's website.
REQ-7	The Code of Conduct describes employee responsibilities and expected behavior regarding data and information system usage.
REQ-8	Upon hire, employees acknowledge that they have read and agree to the Code of Conduct.
REQ-9	The employee confidentiality agreement prohibits any disclosure of information and other data to which the employee has been granted access.
REQ-10	Upon hire, employees acknowledge that they have read and agree to the confidentiality agreement.
REQ-11	New employees offered employment are subject to background checks prior to their start date.

Control #	Applicable Control Activities
REQ-12	New employees complete security awareness training upon hire.
REQ-13	Employees complete security awareness training annually.
REQ-14	Managers complete performance appraisals for direct reports annually.
REQ-15	Job descriptions are documented for employees supporting the service and include authorities and responsibilities in support of the system.
REQ-16	An organization chart is documented and defines the organizational structure and reporting lines.
REQ-17	A Risk Management Policy is documented and 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.
REQ-18	The Company specifies its objectives in its annual risk assessment to enable the identification and assessment of risks related to the objectives.
REQ-19	A risk assessment is performed annually. As part of this process, threats and changes 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.
REQ-20	As part of its annual risk assessment, management selects and develops manual and IT general control activities that contribute to the mitigation of identified risks.
REQ-21	A Vendor Management Policy is documented and includes guidance on performing the following vendor management functions: - Requirements for the classification of third-party vendors - Requirements for the assessment of risks resulting from the procurement of third-party services - Annually reviewing critical third-party attestation reports or performing a vendor risk assessment

Control #	Applicable Control Activities
REQ-22	Formal agreements are in place with critical vendors. These agreements include commitments applicable to that entity.
REQ-23	A third-party attestation report is reviewed annually for all critical vendors. Exceptions noted in the reports are evaluated to determine their impact on the service.
REQ-24	An Access Control Policy is documented and includes guidance for performing the following system access control functions: - Provisioning users - Deprovisioning users - Access reviews and recertification - Restricting access based on separation of duties and least privilege
REQ-25	Authentication to the following system components requires unique usernames and passwords: - Network - Visium Platform & Guardian - Operating System (OS) - Data Stores - AWS Console - Azure Portal - MongoDB Atlas User Interface - Code Repository
REQ-26	Passwords for the following system components are configured according to the Password Policy: - Network - Visium Platform & Guardian - OS - Data Stores - AWS Console - Azure Portal - MongoDB Atlas User Interface - Code Repository

Control #	Applicable Control Activities
REQ-27	Access to production infrastructure is restricted to authorized users with valid multi-factor authentication (MFA) tokens.
REQ-28	Privileged access to the following system components is restricted to authorized users with a business need: - Network - Visium Platform & Guardian - OS - Data Stores - AWS Console - Azure Portal - MongoDB Atlas User Interface - Code Repository
REQ-29	Semi-annual access reviews are conducted to help ensure that system access is restricted appropriately for the following system components: - Network - Visium Platform & Guardian - OS - Data Stores - AWS Console - Azure Portal - MongoDB Atlas User Interface - Code Repository The reviews are documented, and access is modified or removed where applicable.
REQ-30	Access to system components is based on job role, function, and requires a documented access request with manager approval prior to access being provisioned.
REQ-31	Access to system components is revoked within 24 hours of termination as part of the termination process.
REQ-32	A Data Retention and Disposal Policy is documented and includes guidance for the secure retention and disposal of customer data.

Control #	Applicable Control Activities
REQ-33	An inventory of production system assets is maintained by management.
REQ-34	Encryption is enabled for data stores housing customer data.
REQ-35	Secure data transmission protocols are used to encrypt customer data when transmitted over public networks.
REQ-36	The network is segmented to prevent unauthorized access to customer data.
REQ-37	AWS security groups and Azure network security groups are configured to prevent unauthorized access to the production environment.
REQ-38	Anti-malware technology is deployed for environments commonly susceptible to malicious attacks and is configured to be updated routinely, logged, and installed on production servers.
REQ-39	A log management tool is utilized to monitor and identify security events and trends that may have a potential impact on the Company's ability to achieve its security objectives and generates alerts when security events occur.
REQ-40	An intrusion detection system (IDS) is used to provide continuous monitoring of the Company's network and early detection of potential security breaches and generates alerts when security events occur.
REQ-41	A system monitoring tool is utilized to monitor system availability and performance and generates alerts when specific, predefined thresholds are met.
REQ-42	A Vulnerability Management Policy is documented and includes guidance for performing the following vulnerability management functions: - Methods for identifying vulnerabilities and frequency - Assessing the severity of identified vulnerabilities - Prioritizing and implementing remediation or mitigation activities for identified vulnerabilities based on severity and defined timelines

Control #	Applicable Control Activities
REQ-43	Infrastructure supporting the service is patched as a part of routine maintenance to help ensure that systems supporting the service are hardened against security threats.
REQ-44	Penetration testing is performed annually to identify vulnerabilities that could be exploited to gain access to the production environment.
REQ-45	A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities identified during the annual penetration test.
REQ-46	Container image vulnerability scans are performed on a scan-on-push basis to identify, quantify, and prioritize vulnerabilities.
REQ-47	A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities identified during scan-on-push container image vulnerability scans.
REQ-48	An Incident Response Policy is documented and includes guidance for detecting, responding to, and recovering from security events and incidents.
REQ-49	The incident response plan is tested annually to assess the effectiveness of the incident response program.
REQ-50	All incidents related to security are logged, tracked, evaluated, and communicated to affected parties by management until the Company has recovered from the incidents.
REQ-51	Hardening standards are documented and include guidance on baseline security requirements for production systems before deployment to the production environment.
REQ-53	A Change Management Policy is documented and includes guidance for documenting, testing, reviewing, and approving changes to information systems.
REQ-54	Access to migrate changes to production is restricted to authorized personnel.

Control #	Applicable Control Activities
REQ-55	Changes to software and infrastructure components are authorized, documented, tested, reviewed, and approved prior to being implemented in the production environment.
REQ-56	System changes are communicated to authorized internal users.
REQ-57	Branch protection rules are configured in the development tool to require a code review by an individual separate from the developer before code is committed to the main branch.
REQ-58	A business continuity and disaster recovery (BC/DR) plan is documented to support continuity and recovery of critical services and business processes after unexpected business interruptions.
REQ-59	The BC/DR plan is tested annually to assess the effectiveness of management's readiness to respond to unexpected business interruptions.