



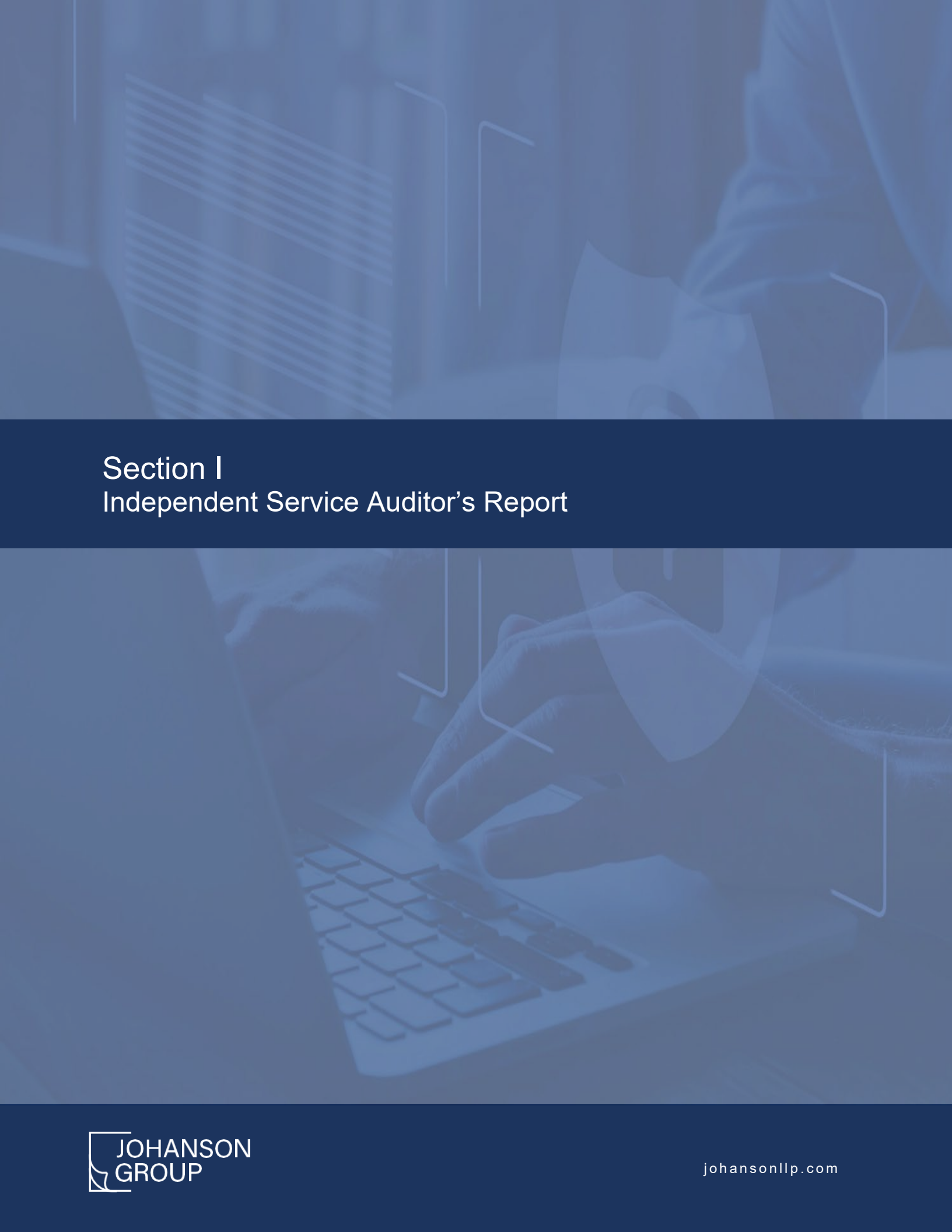
System and Organization Controls (SOC) 3

Relevant to the Trust Service Criteria for Security

For the Period
February 1, 2026 to May 1, 2026

Table of Contents

I.	Independent Service Auditor's Report	3
II.	Assertion of HRMLESS, LLC Management	6
III.	Description of HRMLESS System	8



Section I

Independent Service Auditor's Report

I. Independent Service Auditor's Report

HRMLESS, LLC

Scope

We have examined HRMLESS, LLC's accompanying assertion titled "Assertion of HRMLESS, LLC Management" (assertion) that the controls within HRMLESS, LLC's HRMLESS (system) were effective throughout the period February 1, 2026 to May 1, 2026, to provide reasonable assurance that HRMLESS, LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (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.

Service Organization's Responsibilities

HRMLESS, 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 HRMLESS, LLC's commitments and system requirements were achieved. HRMLESS, LLC has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, HRMLESS, LLC is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

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

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

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

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

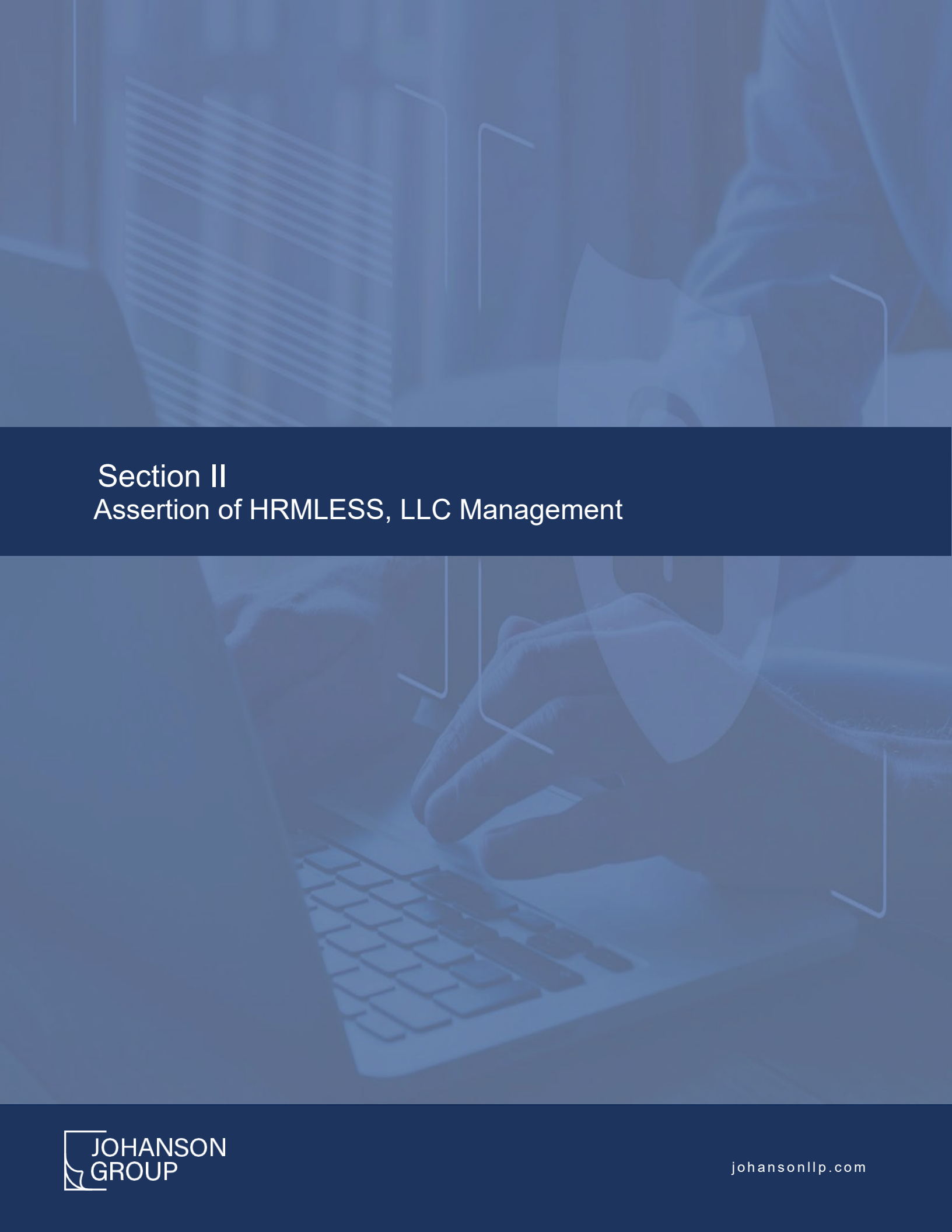
Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within HRMLESS, LLC's HRMLESS (system) were effective throughout the period February 1, 2026 to May 1, 2026, to provide reasonable assurance that HRMLESS, LLC service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Johanson Group LLP

Colorado Springs, Colorado
June 2, 2026



Section II

Assertion of HRMLESS, LLC Management



II. Assertion of HRMLESS, LLC Management

We are responsible for designing, implementing, operating, and maintaining effective controls within HRMLESS, LLC's HRMLESS (system) throughout the period February 1, 2026 to May 1, 2026, to provide reasonable assurance that HRMLESS, LLC's service commitments and system requirements relevant to Security were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of HRMLESS" and identifies the aspects of the system covered by our assertion.

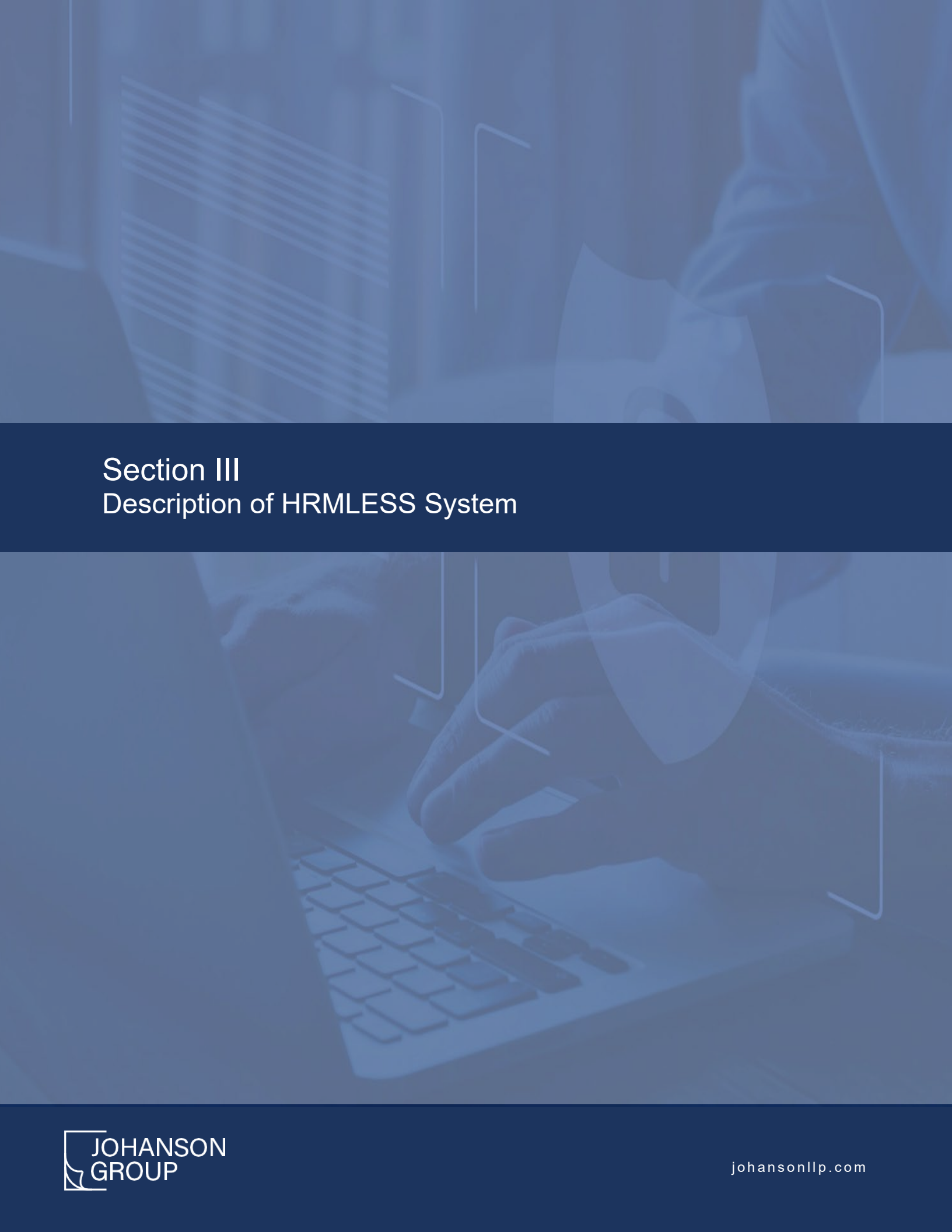
We have performed an evaluation of the effectiveness of the controls within the system throughout the period February 1, 2026 to May 1, 2026, to provide reasonable assurance that HRMLESS, LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022) in AICPA, Trust Services Criteria.

HRMLESS, LLC's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the accompanying system description.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period February 1, 2026 to May 1, 2026, to provide reasonable assurance that HRMLESS, LLC's commitments and system requirements were achieved based on the applicable trust services criteria.

HRMLESS, LLC Management
June 2, 2026



Section III

Description of HRMLESS System



III. Description of HRMLESS System

Company Background

HRMLESS is an AI-powered recruitment technology company co-founded by Anthony Tomes and Ben Schuster. The founders recognized that traditional recruitment screening – relying on manual phone screens and in-person first-round interviews – is expensive, inconsistent, and slow, particularly for high-volume hiring roles. HRMLESS was created to automate and standardize early-stage candidate evaluation through AI-conducted video interviews, enabling hiring teams to evaluate more candidates with greater consistency and at lower cost.

The company operates as a five-person team based in the United States. Its core product, the HRMLESS Platform (the "System"), is a cloud-hosted Software as a Service (SaaS) solution offered to business customers ("user entities") on a subscription basis.

The company's Trust Center is published at trust.hrmless.com and makes the security posture, subprocessor list, and audit attestations available to customers and prospective customers.

Description of Services Overview or Services Provided

The HRMLESS Platform enables organizations to automate candidate screening at scale through structured, AI-conducted video interviews. The four service lines delivered to user entities are:

1. Organization and Account Management – Self-service registration, multi-level organizational hierarchy support, and role-based user administration enabling customers to configure their own user environments.
2. Position Creation and Candidate Management – Creation of job openings with configurable interview questionnaires and evaluation criteria, bulk candidate upload, ATS/HRIS integration via Kombo.dev, and end-to-end candidate pipeline tracking.
3. AI-Conducted Video Interviews – Real-time WebRTC video sessions in which an AI-powered conversational agent conducts structured interviews based on the hiring team's defined question set, using ElevenLabs for AI voice synthesis and Cloudflare for WebRTC media relay.
4. Interview Transcription and AI Grading – Automatic generation of transcripts and AI-scored evaluations against customer-defined criteria using OpenAI and Anthropic models, delivering a structured assessment to the hiring team.

This system description covers all four service lines above. No other HRMLESS products or services are within the scope of this report.

Principal Service Commitments and System Requirements

HRMLESS designs its policies, processes, and technical controls to meet the following service commitments made to user entities and to satisfy applicable legal, regulatory, and contractual requirements.

Security Commitments

- Logical access to customer data is restricted to authorized customer users – enforced via Keycloak JWT authentication and organization-scoped access controls – and to authorized HRMLESS personnel with a documented business need.



- Secrets (database passwords, API keys, client secrets) are sourced from HashiCorp Vault at pod startup via the Vault Agent Injector and are never embedded in container images or committed to source control.
- Production changes follow a two-trunk (dev/main) branching model with mandatory CTO code review and Principal AI Engineer peer review before merge to main.
- All data in transit between user entities and the HRMLESS Platform is encrypted using TLS 1.2 or higher, enforced at the Cloudflare edge.
- All customer data at rest in DigitalOcean managed PostgreSQL and DigitalOcean Spaces is encrypted using AES-256.
- Vulnerability scanning of application dependencies occurs continuously via GitHub Dependabot with remediation SLAs prioritized by CVSS score.
- Vendors with material access to customer data maintain SOC 2 Type II attestations (or equivalent) and are reviewed annually per the Vendor Management Policy.

Confidentiality Commitments

- Encryption protects system data both at rest (AES-256) and in transit (TLS 1.2+).
- Confidentiality and non-disclosure agreements are executed with all employees and contractors as a condition of engagement.
- Customer data is used only for the purposes explicitly stated in the Master Service Agreement and Privacy Policy.
- Interview recordings and transcripts are classified Confidential and subject to strict access controls.

Availability Commitments

- Production application health is monitored via the Microsoft Teams ERROR Notifications channel, providing real-time visibility into error-class events to engineering personnel.
- HRMLESS maintains a Business Continuity and Disaster Recovery Plan with documented RTO and RPO targets for the production environment.
- Customer inquiries and incident notifications are responded to per documented SLA targets in the Master Service Agreement.

Governing Policies and Plans

The following policies and plans constitute the governing framework and are maintained as approved documents in Probo:

Document	Version
Information Security Policy	v3.2
Acceptable Use Policy	v1.0
Access Control Policy	v2.1



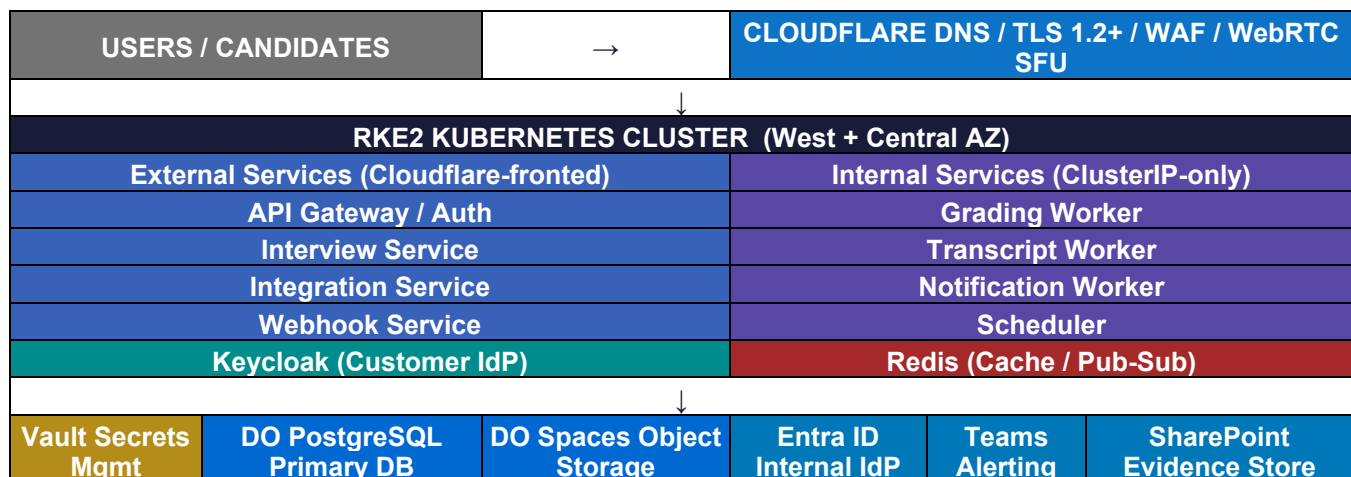
Document	Version
Audit Log Policy	v1.0
Business Continuity and DR Plan	v1.1
Change Management Policy	v2.3
Confidentiality Policy	v2.0
Data Encryption Standards	v1.2
Data Retention and Deletion Policy	v1.4
Incident Response Plan	v3.0
Privacy Policy	v1.0
Risk Management Policy	v1.0
Vendor Management Policy	v1.0
Vulnerability Management Policy	v1.3
Security Awareness Training Policy	v1.0

Components of the System

The System is comprised of five components: Infrastructure, Software, People, Data, and Procedures. Each component is described below.

Infrastructure

The HRMLESS Platform is hosted on infrastructure provided by American Cloud and DigitalOcean. Physical and environmental security at all data centers is the responsibility of the respective subservice organizations. HRMLESS reviews each provider's SOC 2 Type II attestation or equivalent on an annual basis.



Legend

- Customer-facing service
- Internal service
- DigitalOcean managed
- Microsoft 365 / Entra
- HashiCorp Vault



The following providers are responsible for hosting and operating the system infrastructure. Physical and environmental security at these facilities is the responsibility of the respective subservice organizations.

Component	Provider / Location	Purpose
CloudStack Virtual Machines	American Cloud – West + Central AZ	RKE2 Kubernetes worker and control-plane nodes
Managed PostgreSQL	DigitalOcean	Primary relational data store; separate clusters per env
DigitalOcean Spaces	DigitalOcean	Interview recordings, transcripts, object storage
Container Registry	DigitalOcean	Docker image registry

Software

HRMLESS is responsible for the design, development, and operation of the HRMLESS Platform. The application layer is a Python FastAPI backend organized into externally-facing and internally-facing services, deployed as containerized workloads in Kubernetes. Source code is maintained in private GitHub repositories. The production deployment is coordinated via the documented Deployment Runbook , executed by the CTO following release approval.

External Services (customer-facing, Cloudflare-fronted)

Service	Purpose
API Gateway / Auth Service	Customer-facing API requests, JWT validation, and routing
Interview Service	WebRTC session orchestration and real-time interview coordination
Integration Service	ATS/HRIS integrations via Kombo.dev
Webhook Service	Outbound webhook delivery to customer endpoints

Internal Services (ClusterIP-only, not internet-exposed)

Service	Purpose
Grading Worker	AI interview scoring against customer evaluation criteria (OpenAI / Anthropic)
Transcript Worker	Interview transcription processing
Notification Worker	Outbound email and SMS delivery via Sendgrid / Twilio
Scheduler	Cron-based scheduled task execution

Supporting Security Software

Software	Purpose
GitHub Dependabot	Automated dependency vulnerability scanning and PR-based remediation
Vault Agent Injector	Runtime secret injection into Kubernetes pods; eliminates standing credentials
Cloudflare WAF	Web application firewall; blocks OWASP Top 10 class attacks at the edge



Software	Purpose
Microsoft Entra ID	Endpoint protection, MFA enforcement, and Conditional Access for internal staff, Internal staff IdP (SSO, MFA, Conditional Access)

Platform / Application Components

The following components are operated by HRMLESS within the hosting infrastructure described above. HRMLESS is responsible for the configuration, patching, and security of these components.

Component	Provider / Location	Purpose
RKE2 Kubernetes – Prod	West AZ + Central AZ (HA)	Production workload orchestration
RKE2 Kubernetes – Dev	West AZ	Dev/test workloads; fully isolated from production
PgBouncer	In-cluster (both envs)	PostgreSQL connection pooling
HashiCorp Vault (HA Raft)	West AZ + Central AZ	Secret storage and dynamic credential injection
Redis	In-cluster	Cache and pub/sub message broker
Keycloak	In-cluster	Customer-facing identity provider (JWT issuance)

Supporting / Third-Party Services

The following third-party services support the system but do not host or operate the system infrastructure. They are not classified as subservice organizations under the carve-out method.

Component	Provider / Location	Purpose
Cloudflare	Global edge	DNS, TLS, WAF, and WebRTC SFU for video interviews
Microsoft Teams	Microsoft 365	Internal communication and error alerting
Microsoft SharePoint	Microsoft 365	SOC 2 binary evidence artifact storage

People

HRMLESS operates as a five-person team across technical and business functions. Security-relevant personnel and their responsibilities are listed below.

Name	Title	Security Responsibilities
Anthony Tomes	Founder, CEO & CRO	Accountable executive for ISMS; policy approver; release approval authority; customer-facing incident communication; vendor relationship management
Ben Schuster	Founder, CTO	Security program owner; infrastructure, Vault, and Kubernetes administration; code review; access provisioning and quarterly access reviews; vulnerability triage; incident response lead; risk register; SOC 2 program lead



Name	Title	Security Responsibilities
Nicholas Vidal	Principal AI Engineer	AI/ML and application development; peer code review; staging validation; incident response support; infrastructure recovery backup; SOC 2 evidence ownership
Christian Raso	Account Executive	Sales; customer relationship management; security policy compliance; incident reporting
Kolt Korpi	Account Executive	Sales; customer relationship management; security policy compliance; incident reporting

Governance Bodies

Body	Cadence	Purpose
Security Committee	Monthly	Reviews risk register, monitors control health, manages open findings, and approves policy changes
Change Advisory Board	Monthly	Reviews and approves significant infrastructure and application changes
Management Review	Quarterly	Executive review of ISMS performance, resource adequacy, and scope changes; risk residual acceptance

Personnel Security Controls

- All employees execute a Confidentiality and Non-Disclosure Agreement and acknowledge the Acceptable Use Policy during onboarding.
- All employees complete the Security Awareness Training curriculum.
- Access to systems and data is reviewed periodically and adjusted as personnel roles change.

Data

The following data categories are processed and stored by the HRMLESS Platform. Data classifications follow the HRMLESS Data Classification framework maintained in Probo. Customer PII and interview data are classified Confidential and subject to the most restrictive access and retention controls.

Category	Classification	Description	Storage
Account / Org Data	Confidential	Organization profiles, subscription info, configuration	DO managed PostgreSQL
User Account Data	Confidential	Names, email addresses, authentication credentials	DO PostgreSQL; Keycloak
Candidate Data	Confidential	Candidate names, emails, phones, and uploaded PII	DO managed PostgreSQL
Interview Recordings	Confidential	Video recordings of AI-conducted interviews	DigitalOcean Spaces
Interview Transcripts	Confidential	AI-generated text transcripts of candidate interviews	DO Spaces; ref from PostgreSQL



Category	Classification	Description	Storage
Evaluation / Scores	Confidential	AI-generated scores and assessment results	DO managed PostgreSQL
Integration Creds	Confidential	ATS/HRIS OAuth tokens via Kombo.dev	Vault; PostgreSQL
Application Secrets	Confidential	DB credentials, API keys, service account secrets	HashiCorp Vault only
Audit / Event Logs	Internal	Application errors, Entra sign-in logs, K8s control logs	Teams / Entra

Data in transit: all data transmitted between user entities and the HRMLESS Platform is encrypted using TLS 1.2 or higher, enforced at the Cloudflare edge. Inter-service communication within the Kubernetes cluster is secured via Kubernetes-managed TLS certificates. Data at rest: DigitalOcean managed PostgreSQL and Spaces apply AES-256 encryption by default. HashiCorp Vault applies its own encryption layer for all stored secrets.

Processes and Procedures

HRMLESS maintains a documented policy and procedure framework. Source-of-truth policies are maintained as POLICY and PLAN documents in Probo. Operating evidence is maintained as RECORD documents in Probo, with binary artifacts stored in SharePoint.

Procedure	Type	Security Domain (TSC)
Information Security Policy	POLICY	Program governance (CC1)
Access Control Policy	POLICY	Access control (CC6)
Change Management Policy	POLICY	Change management (CC8)
Vulnerability Management Policy	POLICY	Threat and vulnerability (CC7)
Data Encryption Standards	POLICY	Cryptography (CC6.7)
Data Retention and Deletion Policy	POLICY	Data lifecycle (CC6.5)
Audit Log Policy	POLICY	Monitoring (CC7)
Vendor Management Policy	POLICY	Supply chain (CC9)
Security Awareness Training Policy	POLICY	Personnel controls (CC1.4)
Incident Response Plan	PLAN	Incident response (CC7.3, CC7.4)
Business Continuity / DR Plan	PLAN	Availability (CC7.5, CC9.1)
Team Structure and Roles	GOVERNANCE	Organizational structure (CC1)
Developer Onboarding Guide	RECORD	Personnel competence (CC1.4)
Deployment Runbook	RECORD	Change management (CC8.1)

Physical Security

All data is hosted by American Cloud and Digital Ocean. These data centers do not permit HRMLESS employees to have physical access to their facilities.



Boundaries of The System

The following components are within the scope of this report:

- The HRMLESS application source repository and all Kubernetes services deployed from it (external-facing and internal services, shared libraries).
- Both Kubernetes clusters (development and production) and all supporting infrastructure: PgBouncer, DigitalOcean managed PostgreSQL, DigitalOcean Spaces, DigitalOcean Container Registry, HashiCorp Vault, Redis, Cloudflare, and Keycloak.
- Microsoft Entra ID as the identity provider for HRMLESS internal staff administrative access.
- HRMLESS-managed policies, procedures, personnel practices, and governance bodies.
- The Probo compliance platform as the system of record for policies, evidence, and findings.

Out-of-Scope Boundary (Explicitly Excluded)

Excluded Component	Rationale
Rancher UI	Convenience UI for Kubernetes cluster administration. Cluster access is equivalently obtainable via kubectl with Vault-issued credentials. No distinct access surface for audit purposes.
User entity controls	User entity responsibilities are described in Complementary User Entity Controls.
Physical data center controls	Physical and environmental security at American Cloud and DigitalOcean facilities are the responsibility of those subservice organizations.

The Applicable Trust Services Criteria and The Related Controls

Common Criteria (to the Security Category)
<p>Security refers to the protection of</p> <ol style="list-style-type: none"> information during its collection or creation, use, processing, transmission, and storage and 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 removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Control Environment

Integrity and Ethical Values

HRMLESS's control environment is founded on management's commitment to integrity and ethical behavior, demonstrated through formal policy and daily operations:



- A formally documented Code of Conduct is acknowledged by all employees during onboarding, establishing behavioral expectations and data-handling obligations.
- Confidentiality and Non-Disclosure Agreements are executed with all personnel as a condition of employment.
- Background checks are conducted for all employees prior to access provisioning.
- The Information Security Policy and Acceptable Use Policy establish clear rules governing the handling of customer data, acceptable system use, and consequences for policy violations.
- Policy acknowledgment records are maintained in Probo and SharePoint, providing an auditable trail of each employee's commitment to security obligations.

Commitment to Competence

- Written role descriptions for the CTO and Principal AI Engineer specify required technical skills including security-relevant capabilities.
- The Developer Onboarding Guide formally documents the technical environment, access patterns, development workflow, and security practices for engineering personnel.
- All personnel complete the Security Awareness Training curriculum, with role-specific content for technical staff.
- New engineering personnel complete the onboarding training before receiving production access.

Management's Philosophy and Operating Style

The HRMLESS management team balances rapid product innovation with conservative stewardship of customer data, recognizing that candidate PII and interview recordings are among the most sensitive data types that hiring organizations handle:

- Management meets monthly via the Security Committee to review risks, evaluate open findings, and make treatment decisions.
- Major product changes with security implications are reviewed by the Change Advisory Board before implementation.
- The CTO presents quarterly ISMS performance reports to the CEO, documenting control health, open findings, and remediation progress.
- Security investment decisions (tooling, training, audit firm engagement) are approved by the CEO as accountable executive for the ISMS.

Organizational Structure and Assignment of Authority and Responsibility

HRMLESS's organizational structure provides clear separation of security-relevant authorities:

- CEO: accountable executive for the ISMS; manages customer-facing communications for material security incidents.
- CTO: owns and operates the security program; holds Vault and infrastructure administration authority; approves access provisioning, change management, and incident response actions.
- Principal AI Engineer: performs peer code review; serves as backup incident responder and infrastructure recovery resource.
- Sales and Business Operations staff: no access to production infrastructure or customer data; authority confined to M365 applications covered by Entra ID access controls.



Risk Assessment Process

Enterprise risks are tracked in the Probo Risk Register with inherent and residual likelihood and impact scores, owner assignment, treatment decision (Accept, Mitigate, or Transfer), and linkage to mitigating measures and evidence artifacts. The register contains 13 active risk entries covering information security, availability, vendor, and personnel risk categories.

- The CTO reviews the full risk register annually and presents results at the Security Committee.
- Quarterly spot-checks during Security Committee meetings assess whether material changes warrant a register update.
- The CEO participates in the annual review, providing business context and approving residual risk acceptance decisions.
- Material changes to the environment (new vendors, significant architecture changes, new TSC scope) trigger an out-of-cycle risk assessment.

Information and Communication Systems

Internal Communication

- Security Committee, Change Advisory Board, and Management Review records are maintained monthly/quarterly in Probo, providing a continuous governance paper trail.
- The Microsoft Teams ERROR Notifications channel is the primary real-time control for application error detection and triage. Engineering personnel monitor it daily.
- Security-relevant communications (incident alerts, vulnerability notifications, access requests) are handled in dedicated Microsoft Teams channels.

External Communication

- The HRMLESS Trust Center (trust.hrmless.com) publishes the company's security policies, subprocessor list, and audit attestations to customers.
- Customer-facing security commitments are documented in the Master Service Agreement and Privacy Policy.
- In the event of a security incident affecting customer data, the CEO is responsible for timely customer notification per the Incident Response Plan.

Monitoring Controls

Activity	Frequency	Evidence Artifact
Application error monitoring (Teams channel)	Daily	Evidence Log – Infrastructure Monitoring and Alerting
Access review campaigns (7 access sources)	Quarterly	Probo access review campaign records
Risk register review	Quarterly / Annual	Security Committee and Management Review records
Dependency vulnerability scan (Dependabot)	Continuous	Evidence Log – Dependency and Supply-Chain Vulnerability Mgmt



Activity	Frequency	Evidence Artifact
Policy and compliance platform monitoring	Continuous	Probo policy approval, signature, and measure state

Changes to the System

Changes during the observation window (February 1 – May 1, 2026) are tracked in Change Advisory Board minutes and deployment-level changes are captured in GitHub pull-request history. Material changes include:

- Refactoring of internal services for improved separation of concerns (Q1 2026).
- Rollout of automated dependency scanning (GitHub Dependabot) with PR-based remediation workflow (Q1 2026).
- Establishment of the Teams ERROR Notifications channel as the in-scope application monitoring control (Q1 2026).
- Entra ID log retention remediation (FND-002): 30-day default retention limitation identified; Diagnostic Settings export to Log Analytics workspace planned for Q2/Q3 2026.
- Publication of Developer Onboarding Guide, Change Management Worked Examples, Deployment Runbook, Dev/Prod Infrastructure Separation evidence, and Dependency Vulnerability Management evidence (April 2026).
- Publication of six code-level Evidence Logs covering Application Authorization and RBAC, Application Security Controls, Account and Data Lifecycle, Error Monitoring Implementation, Internal Test Harness, and Kubernetes Secret and TLS Management (April 2026).

Incidents

No significant incidents occurred during the audit period.

Criteria Not Applicable to the System

All relevant trust services criteria were applicable to HRMLESS system.

Subservice Organizations

HRMLESS'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 HRMLESS's services to be solely achieved by HRMLESS control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of HRMLESS.

The data center hosting services provided by the subservice organizations' colocation providers were not included within the scope of this examination. The following table presents the subservice organizations carved out of this System Description. The scope of this engagement is limited to the Security Trust Services Criteria; accordingly, the carve-out applies to relevant physical security controls at the subservice organizations.

Subservice Organization	Role in the System	Attestation on File
American Cloud	CloudStack compute infrastructure hosting RKE2 Kubernetes nodes (West + Central availability zones)	SOC 2 Type II on file
DigitalOcean	Managed PostgreSQL databases, Spaces object storage, and container registry	SOC 2 Type II on file

Complementary Subservice Organization Controls

The following subservice organization controls should be implemented by the respective providers to provide additional assurance that the trust services criteria described within this report are met.

Subservice Organization — American Cloud

Ref.	Control	TSC
CA-47	The company's CEO is responsible for approving access to the EGN datacenter.	CC6.4
CA-48	Management contracts with EGN to provide physical access security of its production systems. (Control responsibility delegated to EGN colocation provider.)	CC6.4

Subservice Organization — DigitalOcean

Ref.	Control	TSC
CSOC.01	Colocation data centers are responsible for implementing controls that ensure physical access to data center facilities, backup data, and other system components such as virtual systems and servers is restricted.	CC6.4
CSOC.02	Colocation data centers are responsible for implementing controls that ensure the data center facilities are equipped with physical and environmental security safeguards.	CC6.4

Third-Party Service Providers

The following third-party service providers are used by HRMLESS but are not classified as subservice organizations under the carve-out method. Their services are integrated into the HRMLESS platform; however, they do not host or operate the system infrastructure. HRMLESS monitors their security posture through annual SOC 2 report review per the Vendor Management Policy.

Provider	Role in the System	Attestation on File
Cloudflare	DNS, TLS termination, WAF, and WebRTC SFU for video interview sessions	SOC 2 Type II
Microsoft	Internal staff identity provider (Entra ID); collaboration platform (M365, Teams); evidence storage (SharePoint)	SOC 2 Type II + ISO 27001



Provider	Role in the System	Attestation on File
Stripe	Payment and subscription processing	SOC 2 Type II + PCI DSS
OpenAI	Interview grading and AI evaluation services	SOC 2 Type II
Anthropic	Interview analysis AI services	SOC 2 Type II
ElevenLabs	Conversational AI voice synthesis for AI-conducted interviews	SOC 2 on file
Kombo.dev	ATS/HRIS integration middleware between HRMLESS and customer HR systems	SOC 2 Type II

Complementary User Entity Controls

Customers (user entities) of HRMLESS are responsible for the following controls. The service auditor should consider these CUECs when evaluating the effectiveness of HRMLESS controls:

#	Control Area	User Entity Responsibility
1.	Account Administration	User entities are responsible for managing their own user accounts in the HRMLESS Platform via Keycloak, including timely de-provisioning when their employees leave or change roles.
2.	Strong Authentication	User entities are responsible for enforcing strong authentication (including MFA where available) on their own Platform user accounts.
3.	Data Accuracy	User entities are responsible for the accuracy of candidate contact information and any other data they upload to the Platform.
4.	Webhook Endpoint Security	User entities that subscribe to outbound webhook events from HRMLESS are responsible for securing their receiving endpoints, including HTTPS enforcement and webhook signature verification.
5.	Legal Basis for Processing	User entities are responsible for obtaining all required candidate consents to record, transcribe, and AI-score video interviews under applicable data-protection laws.
6.	ATS Integration Credentials	User entities that connect their ATS/HRIS via Kombo.dev are responsible for scoping the permissions they grant to the integration and for rotating those credentials on a regular schedule.