JOHANSON
GROUP

System and Organization Controls (SOC) 3

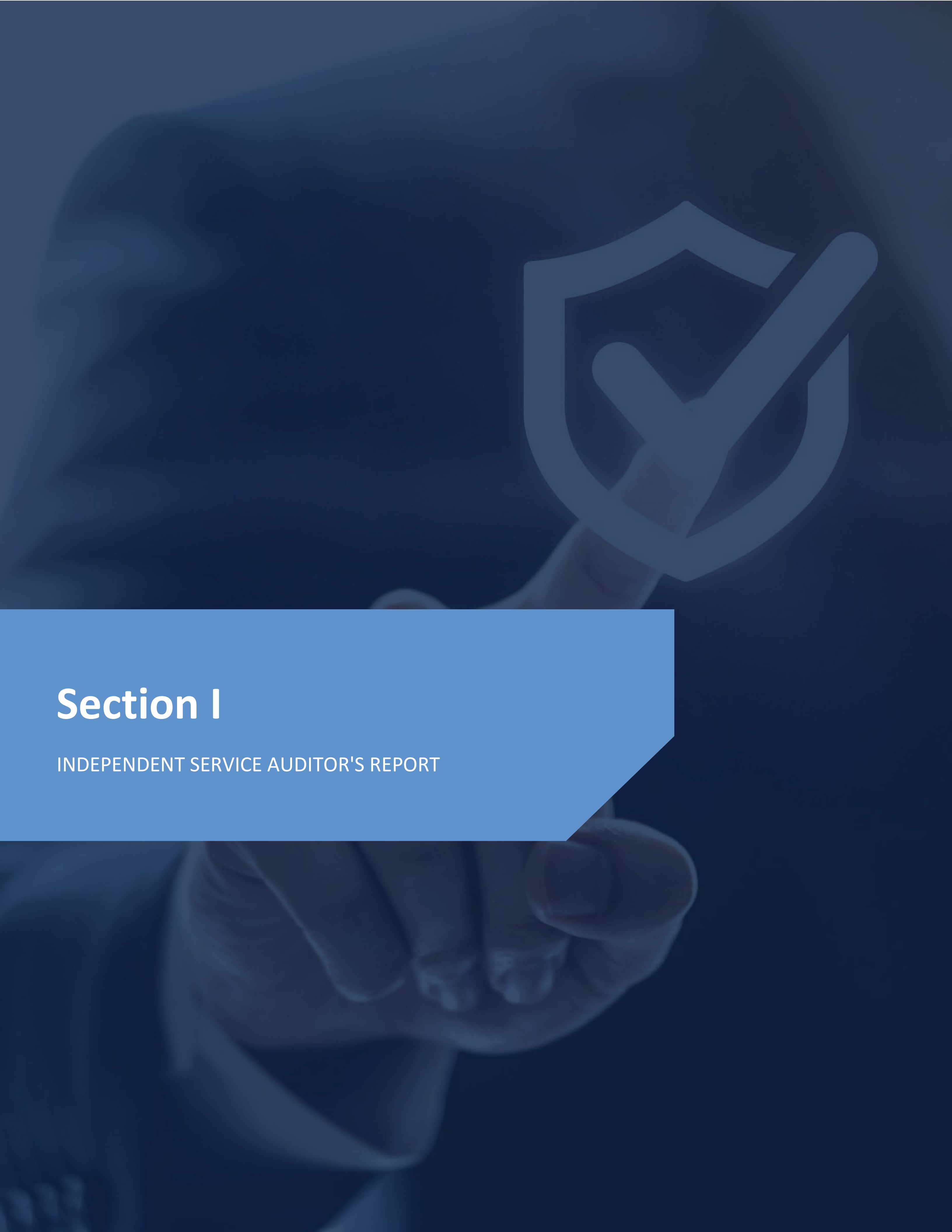
Relevant to the Trust Services Criteria for
Security, Availability, and Confidentiality

For the Period
April 16, 2024 to April 15, 2025

Together with Independent Service
Auditor's Report

wps
unlocking potential

TABLE OF CONTENTS



Section I

INDEPENDENT SERVICE AUDITOR'S REPORT

Manson Western, LLC dba Western Psychological Services

Scope

We have examined Manson Western, LLC dba Western Psychological Services' accompanying assertion titled "Assertion of Manson Western, LLC dba Western Psychological Services Management" (assertion) that the controls within Manson Western, LLC dba Western Psychological Services' Western Psychological Services (system) were effective throughout the period April 16, 2024 to April 15, 2025, to provide reasonable assurance that Manson Western, LLC dba Western Psychological Services' 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

Manson Western, LLC dba Western Psychological Services 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 Manson Western, LLC dba Western Psychological Services' service commitments and system requirements were achieved. Manson Western, LLC dba Western Psychological Services has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Manson Western, LLC dba Western Psychological Services 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 Manson Western, LLC dba Western Psychological Services' 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 Manson Western, LLC dba Western Psychological Services' service commitments and system requirements based on the applicable trust services criteria.

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

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.

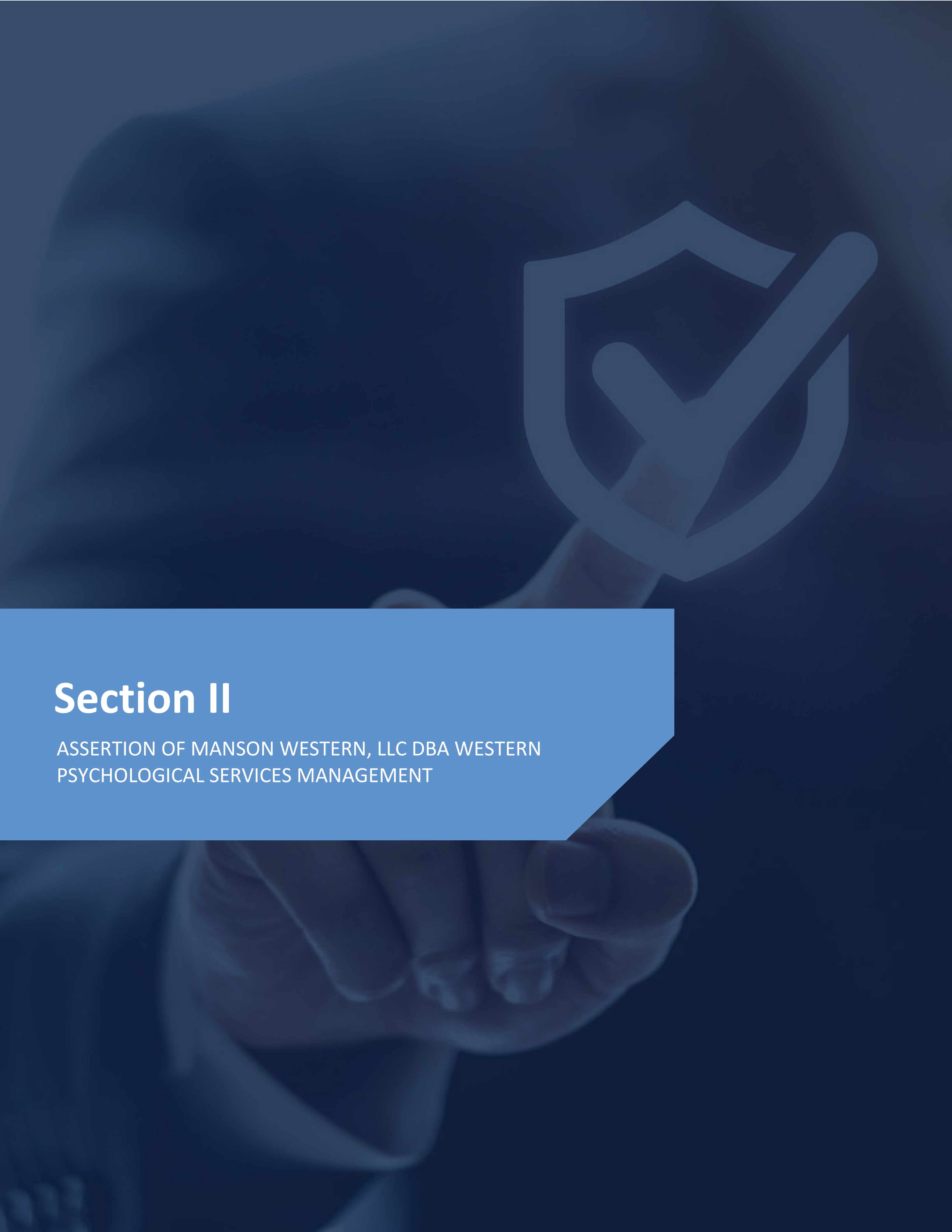
Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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 Manson Western, LLC dba Western Psychological Services' Western Psychological Services were effective throughout the period April 16, 2024 to April 15, 2025, to provide reasonable assurance that Manson Western, LLC dba Western Psychological Services service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

JohansonGroup LLP

Colorado Springs, Colorado
June 10, 2025



Section II

ASSERTION OF MANSON WESTERN, LLC DBA WESTERN
PSYCHOLOGICAL SERVICES MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Manson Western, LLC dba Western Psychological Services' Western Psychological Services (system) throughout the period April 16, 2024 to April 15, 2025, to provide reasonable assurance that Manson Western, LLC dba Western Psychological Services's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of Western Psychological Services" 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 April 16, 2024 to April 15, 2025, to provide reasonable assurance that Manson Western, LLC dba Western Psychological Services' 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.*

Manson Western, LLC dba Western Psychological Services' 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 April 16, 2024 to April 15, 2025, to provide reasonable assurance that Manson Western, LLC dba Western Psychological Services' service commitments and system requirements were achieved based on the applicable trust services criteria.

Manson Western, LLC dba Western Psychological Services Management
June 10, 2025

Section III

DESCRIPTION OF WESTERN PSYCHOLOGICAL SERVICES

COMPANY BACKGROUND

WPS is a leading independent publisher of educational and psychological assessments and related intervention resources. With more than 75 years of experience, we've built a global reputation as assessment experts in the areas of autism, speech and language, school and clinical psychology, and occupational therapy. WPS is a profitable, dynamic, and growing company engaged in work that makes a difference in people's lives. We offer the stability of a third-generation family business combined with the entrepreneurial spirit of a startup. We recognize that the world is changing fast, and that equally applies to our field and industry. For years, we've been investing in digital transformation and new ways of working. This has only accelerated in a post-COVID world. Our mission is "unlocking potential." Inspired by our customers, who dedicate themselves to helping others in need, we hope to better understand the impact of our products and services on their lives. We are equally dedicated to applying the same to ourselves as we continue to invest in a company culture that encourages growth, innovation, creativity, transparency, and collaboration.

DESCRIPTION OF SERVICES OVERVIEW OR SERVICES PROVIDED

We develop assessments used by educators/practitioners (e.g., school psychologists, speech and language pathologists, occupational therapists, reading specialists, social workers, teachers, and others) in the areas of autism, dyslexia, oral language, sensory processing, social/emotional/behavioral development, cognition, and adaptive functioning, to improve clinical evaluation, inform diagnosis, and guide intervention.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

WPS will use commercially reasonable efforts to make our services available with an uptime percentage of at least 99.99%. WPS knows that providing the best possible support to our customers is critical to making our customers successful. Email, phone, and chat support are available from 6 am - 4 pm PST (M-F).

WPS would provide ongoing support to customers using the approved service support channel and knowledge base resources. When a request or transaction is submitted, WPS will authenticate the customer to verify their identity in proportion to the risk of the request or transaction.

The WPS Online Evaluation System is an Internet-based platform for administering and scoring assessments. It improves clinical efficiency by allowing you to administer and score WPS assessments electronically. This industry-leading digital solution streamlines assessment delivery, allowing you more time to help your clients. The WPS Online Evaluation System provides access to a variety of assessments, mostly for children and adolescents.

Internet access is required along with one of the following compatible web browsers:

1. Mozilla Firefox version 54 and later (recommended)
2. Google Chrome version 58 and later
3. Microsoft Internet Explorer version 10 and later
4. Apple Safari version 10.0

Additional User Guides can be found here: https://platform.wpspublish.com/Home/help.

COMPONENTS OF THE SYSTEM

Infrastructure

The primary infrastructure services used to provide and support WPS's Online Evaluation System include the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Atlassian	Jira and Confluence	Internal business communications, storage of organizational documents, and project management.
AWS	VPCs VPN EC2 Instances ECS Load Balancers Route53 Internet Gateway Transit Gateway	Allow for the service, processing, and directing of network traffic and data.
AWS	S3 Buckets	Cloud-hosted storage solutions with encryption capabilities are used to store objects created during development and business operations, i.e., artifacts, user avatars, authentication files, and CloudTrail logs.
AWS	ElasticCache CloudFront OpenSearch Service SES CloudFormation DynamoDB API Gateway	Misc AWS modules hosted on Serverless infrastructure using Infrastructure as a code (IaaS).
AWS	KMS GuardDuty Security Groups NACLs Secrets Manager CloudWatch CloudTrail IAM WAF	Misc AWS Security
AWS	Lambda	Identity server code execution + APIs
AWS	SNS	Email notification services
AWS	SQS	Application messaging queuing service
CookieYes	Website Cookie Consent	Allow customer cookie opt-in and opt-out choices and manage cookie preferences.
Datadog	Logging, Instrumentation, and Monitoring	Application Metrics such as response and request times, distributed tracing, and complete serverless monitoring.
GitHub	Codebase & CICD/Pipeline	Codebase is used for versioning, testing, and deployment of changes to the environments. Also used for source control check-ins, container repositories, PRs, and token management for publishing private packages.
HubSpot	Website chatbot	Chatbot used for technical support
Meta Platforms	React UI	Used for Front End UI. A modern single-page application that uses microservices for I/O needs.

Microsoft	C# .NET Framework	Primary development language/runtime for all applications.
Microsoft	ASP.NET MVC	A web application framework is used to power the web application.
Microsoft	SQL Server	Relational database for customer data.
OpenJS	NodeJS	A programming language for microservices.
Rapid7	Infrastructure vulnerability scanning	Continuously scan and monitor infrastructure for vulnerabilities.
SonarQube	Code analysis	Static application security testing (SAST)
StackHawk	Web application scanning	Dynamic application security testing (DAST)

People

WPS has a staff of 200 employees and contractors organized into the following functional areas:

- Management: Responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.
- Product Management: Helps WPS define product requirements that meet customer needs by collecting customer insights and market research data to identify product viability, new product opportunities, and business scalability to meet larger company objectives across both paper and digital products, including our digital platform.
- IT Infrastructure & Support: Responsible for ongoing procurement, support, maintenance, and management of the servers, networking, data storage, computers, applications, and other systems used to support WPS services. Also, responsible for providing timely resolution of employees' technical issues and problems.
- Product Engineering: Designs and implements new functionality, assesses and remediates any issues or bugs found in the WPS Platform, and architects and deploys the underlying cloud infrastructure on which the platform runs. Develops and enforces coding standards and best practices, including performance, security, monitoring policies, and procedures.
- Customer Service: Responsible for providing internal and external customer support via phone, email, and live engagement. Additional responsibilities consist of order management, quote processing, general inquiries, and product returns.
- Accounting & Finance: The Accounting and Finance department is responsible for the recording and reporting of all financial transactions within the business, including the preparation of customer bills, payment of bills and payroll, maintenance of the general ledger, and preparation of financial statements. Additionally, the department is responsible for tax and business compliance as well as analyzing financial data and preparing departmental and company budgets and forecasts.
- Marketing: Responsible for ongoing communication, strategic vision, and execution of all marketing programs, plans, and promotions, including but not limited to paid advertising, email, conference exhibit, eCommerce site, social media, and content development. Also responsible for internal support of the WPS Sales and Training Departments and for any WPS customer-facing channel used for promotion or advertising of products.
- Project Management: Responsible for project planning and execution of all projects across the company through cross-collaboration and communication.
- Design: Executes design and copyediting work on WPS assessment products, marketing and sales collateral, and training presentations. Maintains, upholds, and evolves WPS brand style. Interfaces with the WPS Procurement department and external vendors to ensure timely delivery and high-quality standards across printed products.
- Facilities: Responsible for the maintenance, security, and upkeep of the WPS facility in Torrance.
- Fulfillment: Responsible for the receipt, storage, inventory control/management, assembly, picking, and shipping of WPS goods and services.
- Professional Development & Training: Responsible for delivering high-quality professional training experiences to our customers, including continuing education for independent study products, webinars, and in-person courses. Includes responsibility for all related order processing and activating, and delivering courses through the WPS Learning Management System (WPS LMS).
- People: The People Department is responsible for the various traditional Human Resource responsibilities of compliance, employee life cycle processing, engagement, benefits administration, and coaching. Our department is also responsible for payroll processing and the positive reinforcement of culture, policy, and practices.

- Procurement: Responsible for ongoing procurement, purchasing requests are filled – both goods and services are purchased by purchasers and delivered by suppliers. Strategic activities, like demand planning, are responsible for finding new suppliers, running various sourcing activities, and negotiating terms and conditions. Take part in new savings initiatives, KPIs, and on-time, on-quality, and on-cost deliveries. Communication and teamwork, maintaining information about existing suppliers, giving operational visibility, keeping track of daily tasks, and automating routine processes.
- Research & Development: Responsible for developing WPS assessments by working with authors to develop and refine item content for rating scales and performance measures, collecting nationally representative data and clinical samples, analyzing data and developing norms, and producing manuals and content for forms, easels, and record forms. Also, responsible for developing and delivering training and intervention products and providing customer support across all products.
- Rights & Permissions: Responsible for asserting intellectual property rights over WPS proprietary content, managing WPS' publishing agreements, approving and issuing licensing and permissions arrangements, processing licensing revenue, collecting royalty recipients' contact and tax ID information for provision to WPS Accounting, assisting authors or their estates in the transfer of rights as appropriate, and approving and issuing WPS Research Discounts. Also assists other departments with consultant agreements and other contracts related to outside contributions to WPS-owned content.
- Sales: Responsible for supporting our customers in their assessment needs and purchases. We focus on providing solutions, be that training on products through site visits, webinars, or convention attendance, providing quotes, assisting with vendor registrations, or processing orders.
- IT Security & Compliance: Responsible for providing ongoing information security to WPS' assets (people, applications, infrastructure, and data). Also responsible for supporting and maintaining ongoing regulatory compliance initiatives.
- Operations: Responsible for trade compliance, strategic and operational objectives, budgets, quality control, facility upkeep, the safety of staff, and finding ways to increase the quality of customer service.
- IT DevOps: Responsible for deployment governance, including CI/CD, SecOps integration of SAST and DAST Tools, and Source Code and Release Management with tagging, branching, and Merging. Ensuring highly available solutions, including replication, clustering, etc. Communicate and coordinate with other IT teams to successfully resolve support, security, and maintenance issues.
- Database Engineering: Responsible for implementing database solutions. Develops and enforces database standards and best practices, including performance, security, monitoring policies, and procedures.

Data

There are three major types of data used by WPS:

- **Configuration Data:** Data used to configure, manage, and secure WPS systems.
- **Customer Data:** Data owned by WPS customers that is input via a web browser to SaaS applications.
- **Log Data:** Logs and traces produced by WPS systems.

Configuration Data is treated as sensitive by WPS. It is stored with a limited lifetime when possible. Access controls limit configuration data access. WPS operators may access configuration data to troubleshoot customer issues or to gather feedback for improving the product. Configuration data is stored in GitHub, Jira, Confluence, and Office365 and includes:

- Credentials for accessing data warehouses, SaaS applications, and source code repositories, including usernames, passwords, OAuth tokens, and certificates.
- The names of databases, schemata, tables, columns, custom objects, and custom fields in SaaS applications.
- System settings include parameters and settings of servers, databases, network devices, and other IT infrastructure.
- Software configurations include details about software versions, patches, and any specific settings within applications.
- Security controls include the configuration of firewalls, intrusion detection systems, and other security tools.
- User access levels include information about who has access to what resources and what permissions they have.
- Change management includes the documentation of all changes made to the system, who made the changes, why they were made, and when they were made.
- Audit logs covering changes to each of the above items.

Customer Data is the most sensitive data in WPS systems. Only authorized WPS operators are permitted to access customer data, and only for justifiable business use cases, such as debugging failures, training, technical support, or other operational issues.

Log Data is produced by various services to make it easier for WPS operators to monitor the health of the system and track down any issues. Log data may be stored by vendors that WPS has entrusted for purposes like indexing, monitoring, and trending.

All data types processed by WPS are encrypted in transit between our app and our servers. WPS supports the latest recommended secure cipher suites to encrypt all traffic in transit, including the use of TLS 1.2 or greater protocols, AES256 encryption, and SHA2 signatures, whenever supported by the clients. Data at rest in WPS' production network is encrypted using industry-standard 256-bit Advanced Encryption Standard (AES256), which applies to all types of data at rest within WPS' systems, databases, file stores, database backups, etc. WPS encrypts customer usernames and passwords used to access WPS services using cryptographic hash functions.

PROCESSES AND PROCEDURES

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to WPS policies and procedures that define how services should be delivered. These are located in WPS' GRC platform and our shared and acknowledged at least annually by all WPS staff and contractors.

Physical Security

All customer data is hosted and stored by Amazon Web Services (AWS) in the United States. AWS data centers do not allow WPS employees physical access. Physical access to WPS's main office and facilities is restricted by using appropriate access control and identification mechanisms. Security clauses are incorporated into all third-party contracts for the maintenance of the facility. All visitors shall be escorted within the facilities and are required to follow visitor access procedures.

Logical Access

WPS's access management procedures are documented in its Access Control Policy. WPS uses Role-based authorization to control access to its network infrastructure. WPS uses the principle of least privilege to determine the type and level of access to grant users. A number of standards are in place that WPS uses when granting access to its systems:

- Valid access authorization from the immediate supervisor or system owner.
- The principle of least privilege allows only authorized access to users, including privileged users, based on their job functions and intended system usage.
- Considering the separation of duties between individuals, to prevent malicious activity without collusion.
- Other attributes as required by the WPS or business function.
- Restrict user accounts from installing software on devices.
- Administrator, system, and generic accounts shall be strictly controlled and given access based on authorization from designated personnel. WPS shall authorize and monitor the use of guest/anonymous and temporary accounts.
- Temporary and inactive accounts that are no longer required, and accounts of terminated or transferred users, shall be deactivated promptly. Account access privileges shall be reviewed periodically.
- Access Approval: WPS shall follow a documented formal access approval process for granting or changing access privileges.

An employee can have one of the following access levels:

- Administrator - can alter policies and provision or de-provision users
- User - has read/write access
- Limited User - has read-only access
- No access

WPS identifies employees primarily by their Azure/Active Directory account, which functions as our corporate directory and SSO provider. The WPS password policy mandates that employees and contractors use their Azure/Active Directory accounts to sign in to SaaS applications and cloud tools when supported. When Azure/Active Directory sign-in is not available, employees may authenticate using a strong, unique password, which must be stored in an approved password manager.

The WPS Azure/Active Directory tenant requires users to use a second factor for authentication. In addition, any SaaS applications used by the company that don't use Azure/Active Directory sign-in must be configured to use a second factor when possible.

The People Department and IT teams are responsible for onboarding new employees. IT is responsible for provisioning Azure/Active Directory accounts and other SaaS accounts as dictated by the employee's role.

WPS has several personnel security procedures in place, specifically during the onboarding process. These include:

- Background checks for new employees are performed by the People Department.
- Employees must read and agree to all security policies.
- Roles within the organization have been clearly defined and are reflected in the organizational chart.
- Employees are granted access/authorization based on their role and in accordance with the principle of least privilege.
- Upon hire and bi-monthly thereafter, security awareness training is completed by all WPS employees.
- Employees are directed to report any potential security incidents to the Cyber Security Officer.
- Violations of WPS security policies have clearly defined repercussions.

When an employee is terminated or separated, the IT team is responsible for removing or disabling all the employee's accounts at the time of separation.

WPS employees must use a company-provided computer to perform their duties. Any computer on which an employee performs sensitive work must employ full-disk encryption and have an approved endpoint monitoring tool installed. On employee termination or separation, IT will ensure the return of company-owned devices and handle their de-provisioning or reprovisioning based on the company's Asset Management policy.

Computer Operations - Backups

WPS uses redundant AWS Availability Zones, automated container recovery, and multiple enterprise-level data backups throughout the day to minimize data loss. Engineers have designed a highly scalable and resilient product architecture within AWS. Our product withstands sophisticated attacks and is highly adaptable. Our system's performance within the product architecture is monitored for key metrics, ensuring the load on any one system is within an acceptable range. Should any components become overloaded or experience a fault, automated processes will be executed to bring additional temporary systems online or to cycle out existing systems for new ones. Automation is built into the WPS architecture, so system monitoring, updates, and corrective actions can take place as needed with no downtime. For data located at HQ, backups are run multiple times throughout the day and backed up to the cloud via enterprise backup solutions. For end users, WPS uses OneDrive, which acts as a backup. WPS backup logs are monitored daily for failures. Any failures are rectified and backups are re-run until successful.

This Backup and Restoration Policy includes:

- Backup data shall be protected with the same level of security as the production data.
- The frequency, extent, and retention of backups shall be in accordance with the importance of the information and the acceptable risk as determined by the data owner.
- Backup data shall not be stored in the same location as the production data.
- Backup jobs shall be monitored to check for and correct errors.
- Backups shall be periodically tested to ensure that they are recoverable and to verify data integrity.
- Records demonstrating the review of logs and test restores should be kept, demonstrating compliance with this policy for auditing purposes.
- All backup data shall be stored encrypted using strong encryption mechanisms or the same access controls as the data in production.
- Access to backup data shall be reviewed at least annually.

Computer Operations - Availability

WPS maintains an Incident Response Policy that gives any employee the ability to initiate a response to a potential security incident by notifying the internal security team through several channels and assists in classifying the severity of the incident.

Our primary goals will be to investigate, contain any exploitations, eradicate any threats, recover WPS systems, and remediate any vulnerabilities. Throughout this process, thorough documentation will be required as well as a postmortem report.

Specific steps that WPS will take are:

- The Security Officer will manage the incident response effort.
- A recurring Incident Response Meeting will be held at regular intervals until the incident is resolved.
- WPS will inform all necessary parties of the incident without undue delay.
- Should the breach involve the release or loss of control of PHI, WPS will refer to its HIPAA Policies and Procedures.
- Addendum to the Incident Response Plan. The addendum lays out specific definitions as well as a comprehensive plan for remediation.

WPS has various internal infrastructure, security, and physical environmental monitoring solutions in place that will alert on many factors such as hardware failures, security incidents and breaches, capacity monitoring, and environmental issues.

Systems used for monitoring and alerting are as follows:

- AWS CloudWatch: Used for monitoring network usage, availability, and overall performance and health of network resources. Also logs metrics for fine-tuning alarms and alerts as usage data is received. Amazon CloudWatch Logs are used in conjunction with AWS CloudTrail to monitor for failed and successful authorization attempts.
- Vulnerability Management Platform: Monitor multiple aspects of your attack surface, including employee devices, networking, server infrastructure, and AWS resources for potential configuration vulnerabilities and tracking necessary patches/updates.
- AWS CloudTrail: Used to log actions taken by users and services within our AWS accounts.
- WAF: Provide metrics regarding attempted and successful requests to the application.
- 3rd Party Penetration Testing: Validate WPS systems in an attempt to identify weaknesses and/or security gaps in all areas of an organization, from the web or mobile applications to supporting network landscapes.
- Endpoint Security: Securing endpoints or entry points of end-user devices such as desktops, laptops, and mobile devices from being exploited by malicious actors and campaigns. Endpoint security systems protect these endpoints on a network or in the cloud from cybersecurity threats.
- Intrusion Prevention/Detection System: Continuously monitor the network for malicious activity and take action to prevent it, including reporting, blocking, or dropping it, when it does occur.
- Security Assurance: Platform used to manage and monitor our InfoSec and Compliance program, as well as security posture vulnerabilities with some of our systems.
- Managed Detection & Response – MDR: Identify and remove cyber threats from a company's environment with the help of an expert off-site security operation center and a dedicated security team. This is a 24/7 operation that's also proactive. Security analysts can step into the customer's environment to look for adversarial behavior rather than rely on a tool that reactively detects that something is going on.
- AWS GuardDuty: Continuous security monitoring service that analyzes and processes the following Data sources: VPC Flow Logs, AWS CloudTrail management event logs, CloudTrail S3 data event logs, and DNS logs. It uses threat intelligence feeds, such as lists of malicious IP addresses and domains, and machine learning to identify unexpected and potentially unauthorized and malicious activity within your AWS environment. This can include issues like escalations of privileges, uses of exposed credentials, or communication with malicious IP addresses and or domains.
- Datadog, SumoLogic: Application metrics such as response and request times, distributed tracing, and complete serverless monitoring.
- StackHawk, SonarQube: Application security testing tools that check source code for common security issues as well as for vulnerabilities identified in open-source dependencies.

WPS contracts a third party to perform annual penetration tests and uses a Vulnerability Management System to monitor for new vulnerabilities. A Security Assurance Platform is also used to manage and monitor our InfoSec and Compliance program, as well as security posture vulnerabilities with some of our systems. The process for reporting any deficiencies with regard to WPS policies and procedures is clearly spelled out in each relevant policy.

WPS also utilizes a 3rd party outsourced Security Operations Center (SOC) that monitors our security infrastructure 24/7 for any evidence of security incidents or breaches.

Change Management

WPS's change management procedures are detailed in the Change Management Policy. There are six key requirements for all changes to the organization, business processes, information processing facilities, and systems that affect information security in WPS' production environment. They are as follows:

- All change requests must be entered into the ticketing system of record, and all approvals, scheduling, comments, and implementation details will be recorded as part of the entered ticket.
- Changes to the information system shall be authorized, documented, and controlled using a formal change control procedure.
- All changes are tested and reviewed before deployment to production.
- Development/test environments are separated from production environments with access control in place to enforce separation.
- Production data shall not be used for testing or development.
- A rollback process must be used for unsuccessful deployments.

Data Communications

WPS uses a fully encrypted VPN solution as well as HTTPS and TLS 1.2 or greater to communicate with and access its network. Furthermore, MFA is required to access any production code base, and SSO is used wherever possible.

Access Control to the production code base is limited via the following controls:

- VPN credentials must be used to access any part of WPS's codebase.
- The production code branch is protected, requiring a merge request and approval before any changes can be made. This also protects the branch from being deleted.
- The RBAC approach is used for accessing the application code repository.

BOUNDARIES OF THE SYSTEM

The scope of this report includes the Services performed by WPS. This report does not include the data center hosting services provided by AWS and Microsoft.

THE APPLICABLE TRUST SERVICES CRITERIA AND THE RELATED CONTROLS

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

Availability
Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality
Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary and intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding the collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

CONTROL ENVIRONMENT

Integrity and Ethical Values

WPS is committed to protecting employees, customers, partners, vendors, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Our Corporate Ethics Policy establishes behavioral and ethical standards for WPS employees, vendors, and the company and serves to guide business behavior to ensure ethical conduct.

WPS employees will maintain the highest ethical standards in the conduct of company business. The intent is that each associate will conduct WPS's business with integrity and comply with all applicable laws in a manner that excludes considerations of personal advantage or gain.

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

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

Commitment to Competence

WPS management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's careful consideration and review of detailed job descriptions for roles. These job descriptions outline accountabilities, skills necessary to do the work, and behavioral competencies. These job descriptions are updated each time a role needs to be filled, a promotion is outlined, or the role's requirements have changed. Employees are asked to review these new job descriptions upon entry into their new roles.

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

- Management has considered the competence levels for jobs and translated the required skills and knowledge levels into written position requirements.
- Training is provided to current staff on an as-needed basis to maintain the skill level of personnel.

Management's Philosophy and Operating Style

WPS is a stable, successful company engaged in work that makes a difference in people's lives. We have the stability of a third-generation family business combined with the entrepreneurial drive of a startup. WPS is a place where people come to build careers. Many of our employees have been with us for 10, 20, or even 30 years or more.

WPS' management team is committed to creating a productive and encouraging work environment as well as providing a secure product for our customers and users.

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

- Quarterly "all hands" meetings for employees to voice their blocks, successes, and concerns
- A rigorous QA program ensures that software development meets industry security standards
- Meetings are held between managers monthly to prioritize objectives and tasks
- Employees are encouraged to engage in the process of collaborative problem-solving in dealing with any challenging or unexpected situation.

Organizational Structure and Assignment of Authority and Responsibility

WPS has a simple organizational structure. Employees report directly to the Department Heads, Managers, or Supervisors, who ultimately provide direction. WPS has clearly defined job descriptions, and as the organization grows, we have in place roles and responsibilities that will allow for the dissemination of managerial responsibilities as necessary.

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

- A regularly updated organization chart is fully accessible to employees
- Responsibilities of roles are clearly defined in policies and job descriptions.

Human Resource Policies and Practices

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

Our culture is one that involves collaboration and individualized care based on the specific situation surrounding an issue. Each issue is resolved with the mission, labor law, and values of the organization in mind.

It is our mission to:

- Build trust: Our organization succeeds and grows on a foundation of trust.
- Create an atmosphere that fosters belonging, creativity, collaboration, and career growth.
- Commit to doing and acting openly, equitably, and consistently.
- Promote ethical and legal conduct in personal and business practices.
- Communicate in a candid and fair manner.
- Foster diversity and inclusion in our workforce.

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

- Evaluations for each employee are performed on a bi-annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.
- Regular feedback and team collaboration on projects.
- Bi-monthly employee cyber security awareness training and annual safety training.
- New employees are required to sign a confidentiality agreement upon hire.
- WPS recognizes that policies and procedures often need to change to serve the needs of the organization. To accomplish this, all security procedures are regularly reviewed and updated based on need.

RISK ASSESSMENT PROCESS

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

WPS's risk assessment process shall focus on the following five types of activities:

1. Identification of Strategic Objectives
2. Identification of Risks
3. Analysis of Risks
4. Mitigation Planning
5. Tracking and Controlling Risks

The risk assessment focuses on the likelihood and potential impact of risks to WPS. Likelihood can be assessed as not likely, somewhat likely, or very likely. The impact can be assessed as not impactful, somewhat impactful, or very impactful. These factors together will give an overall risk ranking. WPS’ stance towards any given risk is based on the assessment described above. Where WPS chooses a risk response other than “Accept”, it shall develop a Risk Treatment Plan. WPS’ stance will fall into one of the following categories:

- Mitigate: WPS may take actions or employ strategies to reduce the risk.
- Accept: WPS may decide to accept and monitor the risk at the present time. This may be necessary for some risks that arise from external events.
- Transfer: WPS may decide to pass the risk on to another party. For example, contractual terms may be agreed upon to ensure that the risk is not borne by WPS, or insurance may be appropriate for protection against financial loss.
- Eliminate: The risk may be such that WPS could decide to cease the activity or change it in such a way as to end the risk.

WPS' risk assessment process considers several factors, each of which contributes to both the likelihood and potential impact of a given risk. These include:

- The criticality of potentially impacted business processes.
- Whether a risk could potentially impact the confidentiality, availability, and security of customer data, PII, or PHI.
- Potential monetary loss
- The ability of risk to impact WPS’s business objectives.
- Potential impact on WPS customers or vendors.

Integration with Risk Assessment

WPS is committed to handling and remediating risks inherent in any commitments, agreements, or responsibilities it may enter into or take on during the operation of the company. Due to the nature of these risks, it may be necessary for WPS to develop specialized controls. WPS considers all relevant factors, contractual, legal, and regulatory when designing these controls. In general, WPS' risk assessment procedure is still applicable to risks inherent in WPS' commitments and contractual responsibilities and should be applied to determining the severity of risks.

INFORMATION AND COMMUNICATION SYSTEMS

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

WPS uses Slack and MS Teams for restricted internal communications. WPS also uses video conferencing tools and Office 365 email for both internal and external communications.

For workflow, project management, and sharing of internal documents, WPS uses Jira and Confluence as well as OneDrive. In addition, WPS communicates with customers via chat on our company website.

MONITORING CONTROLS

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

On-Going Monitoring

WPS has a highly interconnected business process, allowing for visibility and insight by management into the operations of each department. Corrective action is initiated through various mediums. Within departments, process reviews and quality assurance help ensure internal controls are being followed and implemented.

CHANGES TO THE SYSTEM

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

INCIDENTS

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

CRITERIA NOT APPLICABLE TO THE SYSTEM

All relevant trust services criteria were applicable to WPS services.

SUBSERVICE ORGANIZATIONS

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

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

Category	Criteria	Control
Subservice Organization Controls - AWS and Microsoft		
Common Criteria/Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed-circuit television cameras (CCTV). Images are retained for 90 days unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

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

- Holding periodic discussions with vendors and subservice organizations.
- Reviewing attestation reports over services provided by vendors and subservice organizations.
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization.

COMPLEMENTARY USER ENTITY CONTROLS

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

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

1. User entities are responsible for the security and integrity of data housed under user entity control, particularly the data utilized by company systems and services.
2. User entities assign responsibility to personnel, and those personnel identifies which data used by the company is to be considered 'sensitive'.
3. User entities are responsible for understanding and complying with their contractual obligations to WPS.
4. User entities are responsible for notifying WPS of changes made to technical or administrative contact information.
5. User entities are responsible for maintaining their own system(s) of record.
6. User entities are responsible for ensuring the supervision, management, and control of the use of WPS services by their personnel.
7. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize WPS services.
8. User entities are responsible for immediately notifying WPS of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
9. User entities are responsible for the determination of personnel who need specific functionality, and the granting of such functionality is the responsibility of authorized personnel at the user entity. This includes allowing access to WPS' application keys and API keys for access to the web service API.