bakertilly

Proprietary & Confidential

PrePass System

SOC 3
Relevant to Security

JULY 16, 2025 TO OCTOBER 31, 2025

Table of Contents

I. Independent Service Auditor's Report

PrePass, LLC
101 N 1st Ave, Suite 2200
Phoenix, AZ 85003

To the Management of PrePass, LLC:

Scope

We have examined PrePass, LLC's accompanying assertion in Section II titled "PrePass, LLC's Assertion" (assertion) that the controls within PrePass, LLC's PrePass System (system) were effective throughout the period July 16, 2025 to October 31, 2025, to provide reasonable assurance that PrePass, 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 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*.

PrePass, LLC uses a cloud service provider that has a SOC 2 Type 2 report for cloud hosting services (subservice organization). PrePass, LLC's description of the boundaries of its system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at PrePass, LLC, to achieve PrePass, LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of PrePass, LLC's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

PrePass, 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 PrePass, LLC's service commitments and system requirements were achieved. PrePass, LLC has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, PrePass, LLC is responsible for selecting, and identifying in its assertion, the applicable trust services 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 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.

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

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve PrePass, 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 to achieve PrePass, LLC's service commitments and system requirements based on the applicable trust services criteria

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

Inherent Limitations

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

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 PrePass, LLC's PrePass System were effective throughout the period July 16, 2025 to October 31, 2025, to provide reasonable assurance that PrePass, LLC's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Baker Tilly US, LLP

Seattle, Washington
December 31, 2025

II. PrePass, LLC's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within PrePass, LLC's PrePass System (system) throughout the period July 16, 2025 to October 31, 2025, to provide reasonable assurance that PrePass, 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 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*. Our description of the boundaries of the system is presented in Attachment A 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 July 16, 2025 to October 31, 2025, to provide reasonable assurance that PrePass, LLC's service commitments and system requirements were achieved based on the trust services criteria. PrePass, 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 Attachment B.

PrePass, LLC uses a cloud service provider that has a SOC 2 Type 2 report for cloud hosting services (subservice organization). The description of the boundaries of our system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at PrePass, LLC, to achieve PrePass, LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of PrePass, LLC's controls. The description does not disclose the actual controls at the subservice organization.

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 July 16, 2025 to October 31, 2025, to provide reasonable assurance that PrePass, LLC's service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A - PrePass, LLC's Description of the Boundaries of Its PrePass System

A. System Overview

1. Services Provided

PrePass, LLC (or the Company) is a leading provider of intelligent transportation solutions that enhance highway safety and operational efficiency for commercial fleets across North America. Founded in 1993 as a public-private partnership, PrePass operates as a non-profit entity under the PrePass Safety Alliance, reinvesting net proceeds into the transportation industry to support its mission. Headquartered in Phoenix, Arizona, PrePass delivers innovative services such as weigh station bypassing, toll payment management, and safety compliance tools through its integrated platforms. The organization is governed by a board of directors and maintains strategic oversight through regular reporting to its parent entity. With a commitment to secure, data-driven solutions, PrePass continues to lead the industry in advancing roadway safety and fleet performance.

PrePass includes weigh station bypass, electronic toll payment services and the INFORM data portals as follows:

- *PrePass Platform* – A suite of proprietary applications that manage bypass eligibility, toll transactions, safety analytics, and customer account management.
- *Mobile Applications* – The PrePass app provides bypass functionality, driver alerts, and safety notifications via mobile devices.
- *INFORM™ Software* – A web-based analytics tool that provides carriers with insights into safety performance and inspection history.

Core offerings include:

WEIGH STATION BYPASS

- Enables qualified commercial vehicles to bypass inspection facilities at highway speeds.
- Utilizes both Radio-frequency identification (RFID) transponders and a mobile app for flexible bypass options.
- Available at PrePass and third-party sites nationwide.

ELECTRONIC TOLL PAYMENT SERVICES

- Offers PrePass Plus, an integrated toll payment solution.
- Provides a single statement for nationwide tolling, dispute resolution, and access to toll discounts.

SAFETY SCORE MANAGEMENT

- Includes INFORM™ Safety Software to help fleets monitor and improve safety scores.
- Offers insight into inspection history, violations, and trends to support compliance efforts.

DRIVER SAFETY ALERTS

- ALERTS ™ system provides real-time, heads-up notifications for:
  - Traffic incidents
  - Road congestion
  - Truck parking availability
  - Work zone
  - Rest areas
  - Weather hazards (e.g., gusty winds)
  - Crash alerts
  - Steep grades and brake check areas

TECHNOLOGY INTEGRATION

- Compatible with leading Electronic Logging Devices (ELDs).
- Supports RFID and Commercial Mobile Radio Services (CMRS) for reliable data transmission.

INFRASTRUCTURE DEVELOPMENT & INNOVATION

- Invests in bypass infrastructure at no cost to states.
- Partners with government and transportation entities to advance technologies like Level VIII inspections and e-screening.

PREPASS CUSTOMERS

PrePass serves a broad range of customers across the commercial transportation industry. Its solutions are tailored to meet the needs of:

- *Private Fleets* – Companies that operate their own trucks to transport goods for internal use.
- *For-Hire Carriers* – Commercial trucking companies that transport goods for other businesses.
- *Owner-Operators* – Independent drivers who own and operate their own trucks.

These customers span various sectors including logistics, freight, retail distribution, and manufacturing. PrePass supports over 750,000 drivers across North America, helping them improve operational efficiency, reduce costs, and enhance safety through its integrated platform of bypass, tolling, and safety management services.

SUBSERVICE ORGANIZATIONS

PrePass uses a cloud service provider that has a SOC 2 Type 2 report as a subservice organization for cloud hosting services (subservice organization). This subservice organization is excluded from the scope of this report.

2. Infrastructure

CLOUD HOSTING

PrePass systems are cloud-hosted on the subservice organization's environment, which provides scalable compute, storage, and networking resources. The subservice organization has a global infrastructure that supports high availability, redundancy, and disaster recovery.

DATA CENTERS

The subservice organization's data centers are located in the United States and are protected by physical and environmental controls aligned with industry standards (e.g., NIST 800-53, ISO 27001).

3. Software

PrePass software infrastructure is built on a secure, cloud-native architecture hosted within the subservice organization's environment, supporting scalable and resilient service delivery. The development of its online and mobile applications, including the PrePass app and INFORM™ analytics platform, is driven by a modern, multi-language technology stack.. These technologies enable robust backend processing, dynamic user interfaces, and secure data management across web and mobile environments. Development practices are aligned with NIST SP 800-53 standards and supported by CI/CD pipelines, infrastructure-as-code, and automated vulnerability scanning. Centralized monitoring, endpoint protection, configuration management, and security event detection capabilities further reinforce secure deployment, monitoring, and endpoint protection.

In addition to this, PrePass also uses the following software to support internal staff performing business functions and operational workflows:

Software	Description
Enterprise IT Service Management and Workflow Platform	IT Service Management (ITSM) tool used for DevOps integration, incident & change management.
Cloud-Based Network Edge Protection and Traffic Management Service	Monitoring tool used to detect and prevent malicious network traffic.
Web Application Security Testing and Vulnerability Assessment Tool	Tool used for vulnerability scanning and web application security testing.
Internal IT Service Management (ITSM) and Asset Management Platform	ITSM tool used for internal service desk, and asset management.

Software	Description
Enterprise Mobile Device and Endpoint Management System	Mobile Device Management (MDM) used for managing security policies, including anti-virus and malware protection on PCs and mobile devices.
Endpoint Protection and Threat Detection Platform	Anti-spyware program for endpoint, servers, office 365, cloud apps protection.
Security Information and Event Management (SIEM) Platform	Monitoring tool used for data collection, threat detection and investigation.
Managed Extended Detection and Response (MXDR) Security Service	Extended MXDR platform used to monitor security threats and performance issues 24x7x365.
Infrastructure Monitoring and Performance Management Platform	Monitoring tool used for monitoring database instances for CPU, memory, and disk space.
Endpoint Configuration, Asset Inventory, and Security Management Platform	Used for real-time endpoint management, vulnerability detection, and secure telemetry monitoring across PrePass infrastructure.
External Service Availability and Uptime Monitoring Tool	Website monitoring service used to alert PrePass if downtime or performance issues are detected.

4. People

- *Executive Leadership Team* – Provides strategic direction, oversight, and communication. Ensures alignment with compliance and risk management goals.
- *Legal and Compliance Team* – The Legal and Compliance Team ensures the organization adheres to applicable laws, regulations, and contractual obligations. Their main responsibilities include reviewing policies, supporting regulatory compliance efforts, managing legal risk, and collaborating with internal teams to align business practices with legal requirements.

- *Human Resources (HR) Team* – Responsible for managing the full employee lifecycle with a focus on supporting the organization's security and compliance objectives. This includes maintaining an up-to-date organizational chart and ensuring appropriate oversight from the parent organization. The HR team oversees the recruiting process conducting background checks, and ensuring all new hires complete required documentation such as Non-Disclosure Agreements (NDAs) and the Code of Conduct. As part of onboarding, employees receive security awareness training, which is also conducted annually to reinforce best practices. The HR team also manages ongoing employee development through regular performance reviews and ensures that all training completions, acknowledgements, and evaluations are properly documented and retained in accordance with internal policies and compliance requirements.
- *Accounting & Finance* – Manages the organization's financial operations, including budgeting, financial reporting, and billing. Their main responsibilities include ensuring the accuracy and integrity of financial data, support audit readiness, and help maintain compliance with financial regulations and contractual obligations.
- *Network Operations Center (NOC) Team* – Responsible for site systems maintenance, monitoring, and incident response.
- *Product Delivery Team* – Ensures the secure and reliable delivery of services and features to customers. Their main responsibilities include coordinating across engineering, QA, and operations to meet delivery timelines, maintain service quality, and follow the organization's change management process for all deployments.
- *Security and Risk Management Team* – Oversees the organization's adherence to regulatory and industry standards, including SOC 2. Their main responsibilities include conducting internal audits, managing risk assessments, maintaining security policies, coordinating with external auditors, and conducting disaster recovery testing.
- *IT Operations Team (IT)* – Responsible for maintaining system availability and supporting secure operations. Their duties include managing logical access, performing regular user access reviews, and responding to service tickets. They also support infrastructure maintenance, patching, monitoring, and participate in the change management process.
- *DevOps* – Responsible for building, deploying, and operating the organization's technology infrastructure. Their responsibilities include managing CI/CD pipelines, infrastructure as code, system monitoring, and automated deployments. In addition to supporting secure development practices, they perform system operations tasks such as environment provisioning, performance tuning, and incident support.
- *Customer Support and Enrollment Teams* – Responsible for managing customer onboarding, credential verification, and ongoing support.

5. Data

PrePass, LLC provides intelligent safety and tolling solutions for commercial fleets, processing sensitive operational data to streamline compliance and logistics. The system handles toll transaction records, GPS-based route data, weigh station bypass events, and driver identification information, all of which are used to optimize fleet performance and ensure regulatory adherence. These data types are managed through secure, integrated platforms that support real-time analytics, fraud detection, and dispute resolution, forming the backbone of PrePass commitment to confidentiality, integrity, and availability of customer information.

- *Customer Data* – Includes carrier credentials, bypass event logs, toll transactions, and safety performance metrics.

- *System Logs* – Capture authentication events, system changes, and security alerts for monitoring and audit purposes.
- *Third-Party Data* – Integrated from government and tolling authorities to support service delivery and compliance.

Customer and system data is encrypted at rest using Transparent Data Encryption (TDE) with AES-256 and in transit using TLS 1.2 or higher, ensuring protection against unauthorized access and data interception.

6. Processes and Procedures

PrePass management has developed policies and procedures and communicated them to all employees. These procedures cover the following key security areas:

- *Access* Control – Role-based access and multi-factor authentication are enforced across all systems.
- *Change Management* – Formal processes govern the development, testing, and deployment of system changes.
- *Incident Response* – Documented procedures guide the detection, reporting, and resolution of security and availability incidents.
- *Data Classification* – Classifying data based on its sensitivity and to provide guidelines for the appropriate handling and protection of each classification level.
- *DRP and BCP Policies* - Managing system availability and business resumption in the event of system disruptions, failures, and disasters.

B. Complementary Subservice Organization Controls

PrePass, LLC's controls related to the PrePass System cover only a portion of overall internal control for each user entity of PrePass, LLC. It is not feasible for the criteria related to the PrePass System to be achieved solely by PrePass, LLC. Therefore, each user entity's internal controls must be evaluated in conjunction with PrePass, LLC's controls, taking into account the types of controls expected to be implemented by the subservice organization as described below.

Complementary Subservice Organization Controls	
Subservice Organization	
1	The subservice organization is responsible for ensuring network protection for the cloud storage environment through the use of a firewall and security monitoring applications.
2	The subservice organization is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its Infrastructure as a Service (IaaS) cloud hosting services where PrePass systems reside.
3	The subservice organization is responsible for ensuring that devices accessing PrePass are patched, protected with anti-malware, and not jailbroken or rooted.
4	The subservice organization is responsible for environmental and physical security controls over data center facilities, backup media, and network hardware.

Complementary Subservice Organization Controls	
5	The subservice organization is responsible for ensuring that production media is securely decommissioned and physically destroyed prior to being removed from the data center.
6	The subservice organization is responsible for tracking backup failures to resolution.
7	The subservice organization is responsible for providing geo-redundant storage.

Attachment B – Principal Service Commitments and System Requirements

PREPASS INTERNAL SECURITY PRACTICES

PrePass maintains a comprehensive internal security program designed to protect the confidentiality, integrity, and availability of its systems and customer data. The program is aligned with industry best practices and is structured based on the NIST Special Publication 800-53 security and privacy control framework.

PrePass customers agree to a Master Service Agreement (MSA), which outlines the scope of service and obligations, terms of use, and security commitments. Third-party vendors are subject to nondisclosure agreements or other contractual confidentiality provisions, which define management's security commitments and requirements.

SECURITY MANAGEMENT

The organization’s security management program is structured based on the principles of NIST SP 800-53 and designed to protect the confidentiality, integrity, and availability of systems and data. Security governance is led by executive leadership and implemented through formal policies, procedures, and control activities.

Key elements of the security management program include:

- *Governance and Oversight* – Security roles and responsibilities are clearly defined and assigned. Senior leadership provides oversight through regular risk and compliance reviews.
- *Policy Framework* – Security policies are established, approved by management, and communicated to all personnel. Policies are reviewed and updated regularly to reflect changes in the threat landscape and regulatory requirements.
- *Risk Management* – A formal risk management process is in place to identify, assess, and mitigate risks. Risk assessments are conducted periodically and in response to significant changes. Control Implementation – Technical and administrative controls are implemented control families, including access control (AC), audit and accountability (AU), system and communications protection (SC), and incident response (IR).
- *Monitoring and Continuous Improvement* – Security controls are monitored for effectiveness, and findings from audits, assessments, and incidents are used to drive continuous improvement.