



A-LIGN.com

# SOC 3

Prepared for:  
Private Eyes Screening  
Group, Inc.

Year:  
2026



# **SOC 3 FOR SERVICE ORGANIZATIONS REPORT**

**August 1, 2025 to June 30, 2026**

## Table of Contents

|                                                                                                                                                                          |          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| <b>SECTION 1 ASSERTION OF PRIVATE EYES SCREENING GROUP, INC. MANAGEMENT ..</b>                                                                                           | <b>1</b> |
| <b>SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT .....</b>                                                                                                              | <b>3</b> |
| <b>SECTION 3 PRIVATE EYES SCREENING GROUP, INC.'S DESCRIPTION OF ITS IT SERVICES AND IT CONSULTING SYSTEM THROUGHOUT THE PERIOD AUGUST 1, 2025 TO JUNE 30, 2026.....</b> | <b>6</b> |
| OVERVIEW OF OPERATIONS.....                                                                                                                                              | 7        |
| Company Background .....                                                                                                                                                 | 7        |
| Description of Services Provided .....                                                                                                                                   | 7        |
| Principal Service Commitments and System Requirements.....                                                                                                               | 7        |
| Components of the System.....                                                                                                                                            | 8        |
| Boundaries of the System.....                                                                                                                                            | 14       |
| Changes to the System in the Last 11 Months.....                                                                                                                         | 14       |
| Incidents in the Last 11 Months .....                                                                                                                                    | 15       |
| Criteria Not Applicable to the System .....                                                                                                                              | 15       |
| Subservice Organizations .....                                                                                                                                           | 15       |
| COMPLEMENTARY USER ENTITY CONTROLS.....                                                                                                                                  | 16       |

## **SECTION 1**

### **ASSERTION OF PRIVATE EYES SCREENING GROUP, INC. MANAGEMENT**

## ASSERTION OF PRIVATE EYES SCREENING GROUP, INC. MANAGEMENT

July 10, 2026

We are responsible for designing, implementing, operating, and maintaining effective controls within Private Eyes Screening Group, Inc.'s ('Private Eyes' or 'PESG' or 'the Company') IT Services and IT Consulting System throughout the period August 1, 2025 to June 30, 2026, to provide reasonable assurance that PESG'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*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Private Eyes Screening Group, Inc.'s Description of Its IT Services and IT Consulting System throughout the period August 1, 2025 to June 30, 2026" 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 August 1, 2025 to June 30, 2026, to provide reasonable assurance that PESG's service commitments and system requirements were achieved based on the trust services criteria. PESG'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 "Private Eyes Screening Group, Inc.'s Description of Its IT Services and IT Consulting System throughout the period August 1, 2025 to June 30, 2026".

PESG uses Microsoft Azure ('Azure') to provide cloud hosting services, Synoverge Technologies Pvt. Ltd. ('Synoverge') to provide managed IT services, and Axile Tech, LLC ('AtQor') to provide IT support services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at PESG, to achieve PESG's service commitments and system requirements based on the applicable trust services criteria. The description presents PESG's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of PESG's controls. The description does not disclose the actual controls at the subservice organizations.

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

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 August 1, 2025 to June 30, 2026 to provide reasonable assurance that PESG's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of PESG's controls operated effectively throughout that period.

  
Sandra James  
CEO  
Private Eyes Screening Group, Inc.

**SECTION 2**

**INDEPENDENT SERVICE AUDITOR'S REPORT**



## INDEPENDENT SERVICE AUDITOR'S REPORT

To Private Eyes Screening Group, Inc.:

### *Scope*

We have examined Private Eyes Screening Group, Inc.'s ('PESG' or 'the Company') accompanying assertion titled "Assertion of Private Eyes Screening Group, Inc. Management" (assertion) that the controls within PESG's IT Services and IT Consulting System were effective throughout the period August 1, 2025 to June 30, 2026, to provide reasonable assurance that PESG'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*, in AICPA Trust Services Criteria.

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

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at PESG, to achieve PESG's service commitments and system requirements based on the applicable trust services criteria. The description presents PESG's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of PESG's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

### *Service Organization's Responsibilities*

PESG 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 PESG's service commitments and system requirements were achieved. PESG has also provided the accompanying assertion (PESG assertion) about the effectiveness of controls within the system. When preparing its assertion, PESG 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.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements

- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

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

#### *Independence and Ethical Responsibilities*

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination 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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

#### *Opinion*

In our opinion, management's assertion that the controls within PESG's IT Services and IT Consulting System were suitably designed and operating effectively throughout the period August 1, 2025 to June 30, 2026, to provide reasonable assurance that PESG's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of PESG's controls operated effectively throughout that period.

The SOC logo for Service Organizations on PESG's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

A-ALIGN ASSURANCE  
Tampa, Florida  
July 10, 2026

### **SECTION 3**

#### **PRIVATE EYES SCREENING GROUP, INC.'S DESCRIPTION OF ITS IT SERVICES AND IT CONSULTING SYSTEM THROUGHOUT THE PERIOD AUGUST 1, 2025 TO JUNE 30, 2026**

## **OVERVIEW OF OPERATIONS**

### **Company Background**

Private Eyes Screening Group Inc. (commonly referred to as 'PESG' or 'Private Eyes') was founded in September 1999 by Sandra James, Founder and Chief Executive Officer (CEO) with the objective of providing fast and accurate Pre and Post Employment Background Screening, Drug and Health Screening reports.

PESG is a women-owned corporation and has been accredited through the Professional Background Screening Association (PBSA) since 2016.

Industries served by PESG include Financial Services, Staffing Agencies, Healthcare, Legal Services, Advertising, Manufacturing, Retail, Educational institutions, Hospitality and Transportation and Logistics.

### **Description of Services Provided**

PESG provides pre- and post-employment background checks, Drug Screens, and health Screening services throughout the United States and in 193 countries worldwide. The Company was founded in 1999 to provide Background Check services to diverse industries.

PESG's Core application is background checks, and provides a multi-user, transaction-based application suite that enables the processing and delivery of pre- and post-employment background check services. The PESG PEEK platform enables processing of the following services related to Background Checks:

- Capturing data for the purpose of background screening
- Providing the required compliance forms necessary for the background check process to ensure clients' compliance with local, state, and federal requirements
- Providing record-keeping of background checks
- Providing an online, easy-to-use, secure portal to initiate and retrieve background checks
- Providing data reporting in a variety of formats

### **Principal Service Commitments and System Requirements**

PESG designs its processes and procedures related to Background checks to meet its objectives for its Background Check and Drug and Health Screen services. Those objectives are based on the service commitments that PESG makes to its customers (also referred to as user entities), the laws and regulations that govern the provision of Background Check services, and the financial, operational, and compliance requirements that PESG has established for the services. The Background Check services of PESG are subject to the security and privacy requirements of the Fair Credit Reporting Act (FCRA), as amended, including relevant regulations, as well as state privacy and security laws and regulations in the jurisdictions in which PESG operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offered provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Background Check that are designed to permit system users to access the information they need based on their role in the system, while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.

PESG establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. PESG has a due diligence process that all vendors and partners must complete in order to work with the company. PESG monitors on a quarterly basis, depending on the service provided. Such requirements are communicated in PESG's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Background check.

## Components of the System

### Infrastructure

Primary infrastructure used to provide PESG's IT Services and IT Consulting System includes the following:

| Primary Infrastructure   |                              |                                                                                                                                                                                                           |
|--------------------------|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hardware                 | Type                         | Purpose                                                                                                                                                                                                   |
| Azure Disk               | Azure                        | This is attached with windows server for high-performance, durable block storage for mission and business-critical applications                                                                           |
| Flow Log                 | Azure                        | Allows logging information about Internet Protocol (IP) traffic flowing through a network security group (NSG)                                                                                            |
| Analytics                | Azure                        | A logical storage unit utilized for storing, retaining, and querying data collected for Defender for cloud security resources that have been monitored in Azure to provide valuable insights for the same |
| Network Interface        | Azure                        | Provides an additional network interface on a device without the need for a physical network interface card (NIC)                                                                                         |
| Network Security Group   | Azure                        | Allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources                                                                                              |
| Network Watcher          | Azure                        | Provides the ability to diagnose the most common Virtual Private Network (VPN) Gateway and Connections issues                                                                                             |
| Public IP Address        | Azure                        | Allow Internet resources to communicate inbound to Azure resources                                                                                                                                        |
| VPN Gateway - IP         | Azure                        | A public IP address is used as the external connection point of the VPN                                                                                                                                   |
| Recovery Services Vault  | Azure                        | Stores recovery points that are created over time, and it provides an interface to perform backup-related operations                                                                                      |
| Restore Point Collection | Azure                        | Contains the restore points for a specific Virtual Machine (VM) which is configured in Backup service                                                                                                     |
| SendGrid                 | Software as a Service (SaaS) | SaaS for SendGrid (allows sending of e-mails without having to maintain e-mail servers)                                                                                                                   |

| Primary Infrastructure                          |       |                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hardware                                        | Type  | Purpose                                                                                                                                                                                                                                                                                          |
| Structured Query Language (SQL) virtual machine | Azure | Enables the use of full versions of SQL Server in the Azure cloud without having to manage any on-premises hardware                                                                                                                                                                              |
| Storage account                                 | Azure | Provides the flexibility of choosing the shell experience that best suits the work, either Bash or PowerShell. Cloud Shell runs on a temporary host provided on a per-session, per-user basis containing all Azure Storage data objects, including blobs, file shares, queues, tables, and disks |
| Traffic Manager Profile                         | Azure | Uses Domain Name System (DNS) to direct client requests to the appropriate service endpoint based on a traffic-routing method                                                                                                                                                                    |
| Virtual machine                                 | Azure | Gives the flexibility of virtualization without having to buy and maintain the physical hardware that runs it                                                                                                                                                                                    |
| Virtual machine                                 | Azure | Enables communication between multiple computers, virtual machines (VMs), virtual servers, or other devices across different office and data center locations                                                                                                                                    |
| Virtual Network Gateway                         | Azure | Azure VPN Gateway is a service that uses a specific type of virtual network gateway to send encrypted traffic between an Azure virtual network and on-premises locations over the public Internet                                                                                                |
| Azure Web Application Firewall (WAF)            | Azure | Azure WAF monitors the network traffic                                                                                                                                                                                                                                                           |

### Software

Primary software used to provide PESG' IT Services and IT Consulting System includes the following:

| Primary Software                        |                  |                                                                             |
|-----------------------------------------|------------------|-----------------------------------------------------------------------------|
| Software                                | Operating System | Purpose                                                                     |
| Visual Studio 2022                      | Windows          | Integrated Development Environment (IDE) Developer tool                     |
| SQL Server Management Studio            | Windows          | Integrated environment for managing any SQL infrastructure (database)       |
| IIS                                     | Windows          | Exchange static and dynamic web content with internet users                 |
| Azure Intrusion Prevention System (IPS) | N/A              | Intrusion detection and prevention system enabled along with Azure Firewall |
| Azure DevOps                            | N/A              | Tickets System/Manage code history                                          |
| Azure VPN                               | N/A              | VPN for access to production                                                |
| Source Tree                             | Windows          | Version control                                                             |

| Primary Software |                                        |              |
|------------------|----------------------------------------|--------------|
| Software         | Operating System                       | Purpose      |
| Windows 10+      | Windows                                | Workstations |
| Zoho             | Customer Relationship Management (CRM) | CRM Tool     |

### People

PESG has a staff of approximately 38 employees organized in the following functional areas:

- **Corporate.** Executives, senior operations staff, and company administrative support staff, such as legal, compliance, internal audit, training, contracting, accounting, finance, human resources, and transportation provider relations. These individuals use the PEEK Platform primarily as a tool to measure performance at an overall corporate level. This includes reporting done for internal metrics as well as for PESG' user entities.
- **Operations.** Staff performs the background checks and administers the scheduling and administration of drug screens and health screens on a day-to-day basis.
- Customer service representatives take phone calls directly from clients, assist clients with any questions or make updates to background checks in process.
- Verifiers - verify the employment, education, references, and professional license that applicants provide on their application.
- Quality assurance employees review and audit the background check reports for Quality, validity, and accuracy before the final report is sent to the client.
- The admin staff manages the facility and supports the production staff.
- **IT.** Help desk, IT infrastructure, IT networking, IT system administration, software systems development and application support, information security, and IT operations personnel managing electronic interfaces and business implementation support and telecom:
  - The help desk group provides technical assistance to the users.
  - The infrastructure, networking, and systems administration staff typically support the Company's IT infrastructure, which is used by the software. A systems administrator will deploy the releases of the PEEK platform and other software into the production environment.
  - The software development staff develops and maintains the custom software for PESG. This includes supporting utilities, and the external websites that interact with the Background check process. The staff include software developers, database administration, software quality assurance, and technical writers.
  - The information security staff supports the Peek platform indirectly by monitoring internal and external security threats and maintaining current antivirus software.
  - The information security staff maintains the inventory of IT assets.
  - IT operations manage the user interfaces for the PEEK platform. This includes processing user entity-supplied membership and eligibility files, producing encounter claims files, and other user-oriented data (capitation files, error reports, remittance advice, and so on).
  - Telecom personnel maintain the voice communications environment, provide user support to PESG, and resolve communication problems.

AtQor's is Microsoft service provider for PESG. Private Eye purchases Microsoft products and licenses the products via AtQor. They also provide technical support during the implementation of any new products Private Eye purchases.

Synoverge is part of Private Eye's programming team and has assisted in writing the code for Private Eye's application. Private Eye uses Microsoft DevOps for making changes and follows SDLC, starting from Analysis and Design to Coding, Unit Testing, followed by User Access Testing (UAT), and finally moving the code into production. Please find below the responsibility matrix for tasks performed by Synoverge:

| Tasks                                                                           | PESG    | Synoverge |
|---------------------------------------------------------------------------------|---------|-----------|
| Arrange for key business users for Requirement Gathering Phase                  | Arrange |           |
| Requirement Analysis                                                            | Assist  | Perform   |
| Prepare Plan                                                                    |         | Perform   |
| Develop feature / Fix issues                                                    |         | Perform   |
| Create System Test Plans & System Testing                                       | Perform |           |
| Prepare Acceptance Test Cases                                                   | Perform |           |
| Prepare UAT and Production Environment                                          | Assist  | Perform   |
| UAT                                                                             | Perform | Assist    |
| Resolve / Close Defects                                                         |         | Perform   |
| Signoff Acceptance of application                                               | Perform |           |
| User Demo and Training                                                          | Perform |           |
| Code Merge Activity<br>(when different source code repositories are maintained) | Assist  | Perform   |
| Production Deployment                                                           | Assist  | Perform   |
| Go-Live                                                                         | Perform | Assist    |

### Data

All data is stored in MS SQL Server including master and transaction data. E-mail and Error logs are also stored in the same. Data comes to the database from portal (aka web interface), or external interfaces shared with vendor via secured authentication method. People having respective rights only can generate reports in Portable Document Format (PDF) or Excel format. Audit trail is maintained and stored in databases to keep track of user activities.

Data, as defined by PESG, constitutes the following:

- Applicant full name
- Applicant Address
- Applicant date of birth
- Applicant Social Security Number (SSN)
- Applicants' e-mail address
- Applicant phone number
- Consent forms

Transaction processing is initiated by the receipt of background check order request. This request typically comes directly from a client requestor initiated via website, e-mail, or it may arrive by fax from a client location. After the background checks are completed, the client will get automatic e-mail notification, and the report can be viewed or downloaded on the PESG web portal.

Output reports are available in electronic PDF, comma-delimited value file exports, or electronically from the PESG website. The availability of these reports is limited by job function. Reports delivered externally will only be sent using a secure method-encrypted e-mail.

## *Processes, Policies and Procedures*

Formal IT policies and procedures exist that describe logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the PESG policies and procedures that define how services should be delivered. These are located on the Company's shared folder and can be accessed by any PESG team member.

### Physical Security

PESG uses Azure for hosting their infrastructure and systems. As such, the responsibility for the physical protection of this equipment is the responsibility of Azure. For a list of controls implemented by Azure, please refer to the "Subservice Organizations" section, below.

### Logical Access

PESG uses a role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. In the event that incompatible responsibilities cannot be segregated, PESG implements monitoring of one or more of the responsibilities. Monitoring must be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing annual reviews of access by role.

VPN users are authenticated via multi-factor authentication using username, password, and Personal Identification Number (PIN) prior to being granted remote access to the system. Only employees are authorized to sign on to the PESG network using an Active Directory user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Active Directory. Passwords must conform to defined password standards and are enforced through parameter settings in the Active Directory. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Customer employees' access PESG background check services through the Internet using their valid user ID and password to gain access to customer cloud resources. Passwords must conform to password configuration requirements configured on the virtual devices using the virtual server administration account. Virtual devices are initially configured in accordance with PESG's configuration standards, but these configuration parameters may be changed by the virtual server administration account.

Upon hire, employees are assigned to a position in the HR management system. Two days prior to the employees' start date, the hiring manager will request that user IDs be created and access be granted in writing to the IT team.

On an annual basis, access rules for each role are reviewed by a working group composed of security help desk, data center, customer service, and Human Resources (HR) personnel. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access. Completed rules are reviewed and approved by the Chief Information Security Officer (CISO). As part of this process, the CISO reviews access by privileged roles and requests modifications based on this review.

The HR system generates a list of terminated employees on a quarterly basis. This report is used by the security help desk to delete employee access. On an annual basis, HR runs a list of active employees. The security help desk uses this list to suspend user IDs and delete all access roles from IDs belonging to terminated employees.

### Computer Operations - Backups

PESG data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job depending on customer indicated preference within the documented work instructions. Backup infrastructure and on-site backup tape media are physically secured in locked cabinets. The backup infrastructure resides private networks logically secured from other networks.

### Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

PESG monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. PESG evaluates the need for additional infrastructure capacity in response to the growth of existing customers and the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Server Room space, power and cooling
- Disk storage
- Network bandwidth

PESG has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor-recommended operating system patches. Customers and PESG system owners review proposed operating system patches to determine whether the patches are applied. PESG systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. PESG staff validate that all patches have been installed, and if applicable, that reboots have been completed.

### Change Control

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

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

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

PESG has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. PESG system owners review proposed operating system patches to determine whether the patches are applied. PESG systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. PESG staff validate that all patches have been installed and if applicable that reboots have been completed.

PESG uses Synoverge and AtQor for making changes to their infrastructure and systems. As such, the responsibility for change management processes is the responsibility of Synoverge and AtQor. For a list of controls implemented by Synoverge and AtQor, please refer to the “Subservice Organizations” section, below.

### Data Communications

Microsoft Azure Firewall systems are in place to filter unauthorized inbound and outbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees. The PESG internal and external traffic is restricted (subnets: Public) is configured and is established to limit inbound and outbound traffic.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted on an annual basis to measure the security posture of a target system or environment. The third-party vendor TPX uses an accepted industry standard penetration testing methodology specified by PESG. The third-party vendor’s approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled insider or an attacker who has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by a third-party vendor on a quarterly basis in accordance with PESG. The third-party vendor Sysnet uses industry-standard scanning technologies and a formal methodology specified by PESG. These technologies are customized to test the organization’s infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as-needed basis. Scans are performed during non-peak windows. Tools requiring installation in PESG’s system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

### **Boundaries of the System**

The scope of this report includes the IT Services and IT Consulting System performed remotely.

This report does not include the cloud hosting services provided by Azure performed remotely.

This report does not include the managed IT services provided by Synoverge Technologies Pvt. Ltd. performed remotely.

This report does not include the IT support services provided by Axile Tech, LLC (“AtQor”) performed remotely.

### **Changes to the System in the Last 11 Months**

No significant changes have occurred to the services provided to user entities in the 11 months preceding the end of the review period.

## Incidents in the Last 11 Months

No significant incidents have occurred to the services provided to user entities in the 11 months preceding the end of the review period.

## Criteria Not Applicable to the System

All Common Criteria/Security criteria were applicable to PESG's IT Services and IT Consulting System.

## Subservice Organizations

This report does not include the cloud hosting services provided by Azure performed remotely.

This report does not include the managed IT services provided by Synoverge Technologies Pvt. Ltd. performed remotely.

This report does not include the IT support services provided by Axile Tech, LLC performed remotely.

### *Subservice Description of Services*

PESG relies on Azure for cloud hosting services to support in-scope infrastructure and systems.

PESG relies on Synoverge for development of the in-scope application.

PESG relies on AtQor's for managing Azure services. Private Eye purchases Microsoft products and licenses the products via AtQor. They also provide technical support during the implementation of any new products Private Eye purchases.

### *Complementary Subservice Organization Controls*

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

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

| Subservice Organization - Azure |              |                                                                                                                                                                 |
|---------------------------------|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Category                        | Criteria     | Control                                                                                                                                                         |
| Common Criteria / Security      | CC6.4, CC7.2 | Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors.                     |
|                                 |              | Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors. |
|                                 |              | Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.                                                         |

| Subservice Organization - Azure |          |                                                                                                                                                                                                                 |
|---------------------------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Category                        | Criteria | Control                                                                                                                                                                                                         |
|                                 |          | Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals. |
|                                 |          | The datacenter facility is monitored 24x7 by security personnel.                                                                                                                                                |

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

| Subservice Organization - Synoverge |          |                                                                            |
|-------------------------------------|----------|----------------------------------------------------------------------------|
| Category                            | Criteria | Control                                                                    |
| Common Criteria / Security          | CC8.1    | Changes are developed and deployed as per the guidelines provided by PESG. |

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

| Subservice Organization - AtQor |          |                                                                            |
|---------------------------------|----------|----------------------------------------------------------------------------|
| Category                        | Criteria | Control                                                                    |
| Common Criteria / Security      | CC8.1    | Changes are developed and deployed as per the guidelines provided by PESG. |

PESG's management, along with the subservice organizations, 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, PESG performs monitoring of the subservice organizations' controls, including the following procedures:

- Holding 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 subservice organizations.

## COMPLEMENTARY USER ENTITY CONTROLS

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

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

1. User entities are responsible for understanding and complying with their contractual obligations to PESG.

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