PROCAS®

ACCOUNTING SOFTWARE
FOR GOVERNMENT CONTRACTORS

Service Auditors' Report on System and Organization Controls (SOC 3)

Relevant to Security and Availability

For the Period November 1, 2021 to October 31, 2022

SC&H
ATTEST SERVICES

INDEPENDENT SERVICE AUDITORS' REPORT

To the Management of PROCAS, LLC.:

Scope

We have examined PROCAS, LLC's ("PROCAS'" or the "Company's") accompanying assertion titled "Assertion by Management of PROCAS, LLC" (assertion) that the controls within PROCAS' accounting solutions system (system) were effective throughout the period November 1, 2021 to October 31, 2022, to provide reasonable assurance that PROCAS' service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (*AICPA, *Trust Services Criteria*).

PROCAS used subservice organizations during the period under audit to provide hosting services, including all of its physical and environmental security functions services, and other cloud hosting services. 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 PROCAS, to achieve PROCAS' service commitments and system requirements based on the applicable trust services criteria. 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

PROCAS 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 PROCAS' service commitments and system requirements were achieved. PROCAS has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, PROCAS 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 Auditors' 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 November 1, 2021 to October 31, 2022 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 American Institute of Certified Public Accountants. 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 to achieve PROCAS' 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 PROCAS' 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 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 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 PROCAS' system were effective throughout the period November 1, 2021 to October 31, 2022, to provide reasonable assurance that PROCAS' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

SC+H Attest Services, P.C.

SC&H Attest Services, P.C.
Sparks, Maryland
December 16, 2022

PROCAS®
ACCOUNTING SOFTWARE
FOR GOVERNMENT CONTRACTORS

Assertion by Management of PROCAS, LLC

We, as management of PROCAS, LLC ("PROCAS" or the "Company"), are responsible for designing, implementing, operating, and maintaining effective controls within PROCAS' accounting solutions system (system) throughout the period November 1, 2021 to October 31, 2022, to provide reasonable assurance that PROCAS' service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (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 attached description of the boundaries of the system 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 November 1, 2021 to October 31, 2022, to provide reasonable assurance that PROCAS' service commitments and system requirements were achieved based on the applicable trust services criteria. PROCAS' 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 within the attached 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 November 1, 2021 to October 31, 2022, to provide reasonable assurance that PROCAS' service commitments and system requirements were achieved based on the applicable trust services criteria.

James E Wesloh
President

Introduction

Company Overview

PROCAS, LLC ("PROCAS" or the "Company") was founded in 1997 on the idea that government contracting accounting could be simplified by aligning the way software functions with the way people work in a government contracting environment. PROCAS is based in Columbia, Maryland.

Description of Services Provided

PROCAS provides its clients with an integrated financial and project accounting system. Additional offerings include timekeeping, expense reporting, management reporting, and a Web Application Programming Interface (WebAPI), all of which are integrated with the PROCAS accounting system. In 2021, PROCAS' WebAPI was released, and allows clients to download their data for their in-depth analysis and/or creation of custom dashboards and reports specific to their requirements. The Company also provides on-going support by PROCAS consultants and dedicated support staff.

Principal Service Commitments and System Requirements

PROCAS has implemented a secure infrastructure supported by industry specialists. Data is protected with server, firewall, network, and power redundancies; continuous replication; dedicated monitoring and management infrastructure; encrypted connections to servers; client data and backups are stored on encrypted media, and authentication credentials. Physical access to the Company's own facilities as well as its contracted colocation facilities are controlled by robust policies and procedures to gain access.

Organizational Structure

PROCAS' organizational structure provides the overall framework for planning, directing, and controlling operations. Personnel and business functions are separated into departments according to job function. The structure provides for clearly defined responsibilities and lines of authority for reporting and communication. The Company's client-facing activities areas are divided into three distinct departments: Information Technology (IT), Development, and Client Services. The Client Services department includes consulting, client application support, administration, and sales teams. Each department is managed by employees with exceptional experience and education in their respective fields. Duties are segregated to ensure adequate financial and operational controls.

Executive Management

The PROCAS executive management team provides the overall direction for the Company. All members of the PROCAS management team are actively engaged in the review, approval, and administration of those policies and procedures associated with business operations and the applications supported by the Company.

PROCAS' management consist of the President, Chief Operating Officer, Chief Information Officer, and Chief Product Officer. They have the ultimate responsibility for all PROCAS activities, including the internal control system, the assignment of authority and responsibility for operational activities, and the establishment of reporting relationships and authorization protocols. The management team meets periodically, formally on at least an annual basis, and is responsible for establishing a strategic plan and all aspects of PROCAS' operational and financial management.

Relevant Aspects of the Control Environment, Risk Management, Information and Communication, and Monitoring

PROCAS' internal control environment consists of five interrelated components:

Control Environment: This sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

Risk Management: This is the entity's identification and analysis of risks relevant to the achievement of its objectives, forming a basis for determining how the risks should be managed.

Information and Communication: Surrounding these activities are information and communication systems. These enable the entity's people to capture and exchange information needed to conduct and control the entity's operations.

Monitoring: The entire internal control process must be monitored, and modifications are made, as necessary. To support the modification, the systems react dynamically and change as conditions warrant.

Control Activities: Control policies and procedures must be established and executed to help ensure that the actions identified by management are completed as necessary to address risks for achievement of the entity's control objectives.

Set out below is a description of the components of internal control related to the services that may be relevant to customers.

Control Environment

The objectives of internal control as it relates to PROCAS are to provide reasonable, but not absolute, assurance that controls are suitably designed and implemented to meet the relevant trust services criteria, that assets are protected from unauthorized use or disposition, and that processes and procedures are executed in accordance with management's authorization and client instructions.

The control environment reflects the overall attitude and awareness of management and personnel considering the importance of controls and the emphasis given to controls in PROCAS' policies, procedures, and actions. Management has established and maintains controls designed to monitor compliance with established policies and procedures. The remainder of this subsection discusses the tone at the top as set by management, the integrity, ethical values, and competence of PROCAS employees, the roles of significant control groups, policies and procedures, the risk management process and monitoring. The internal control structure is established and refreshed based on PROCAS' assessment of risks facing the organization.

Risk Management

The process of identifying, assessing, and managing risks is a critical component of PROCAS' internal control system. The purpose of PROCAS' risk assessment process is to identify, assess, and manage risks that affect the Company's ability to achieve its objectives. The management of PROCAS also monitors controls to consider whether they are operating as intended, and whether they are modified as appropriate for changes in conditions or risks facing the organization.

Ongoing monitoring procedures are built into the normal recurring activities of PROCAS and include regular management and supervisory activities. Managers of the various organizational units are in regular communication with personnel and may question the accuracy of information that differs significantly from their knowledge of operations.

In conjunction with the strategic planning, management evaluates the organizational structure, including reporting lines, and completes an annual risk assessment to evaluate the threats to PROCAS business objectives and operations, including but not limited to relationships with vendors, business partners, and other parties as well as environmental, regulatory, technological, and fraud threats to the system's security. The risk assessment is based on the objectives established by management and defined within the Risk Management Policy. Based on discussions, the Company determines a risk mitigation strategy to reduce risk to an acceptable level, including the need for new controls.

All major enhancements, upgrades, and related changes associated with the system are reviewed and approved by appropriate management prior to implementation.

Information and Communication

Information and communication are an integral component of PROCAS' 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. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At PROCAS, information is identified, captured, processed, and reported by various information systems.

PROCAS has various information security policies to help ensure that employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of email to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems.

Contractual agreements provide a mechanism for communicating the terms of service within the Company and between the Company, clients, and users. Contractual agreements outline terms and payment for services, use of services, and enforcement. Management reviews and approves each contractual agreement. Any changes are reviewed by management and sent to the necessary teams for execution of the changes. Clients are notified of any changes. PROCAS maintains a repository of client contract terms.

Management has made contact information available to clients, consumers, external auditors, regulators, vendors, and others on the Company website and executed contracts.

Monitoring

Monitoring is an integral part of PROCAS' internal control framework. PROCAS' monitoring activities consist of assessments and the quality control process, which monitor changes in the industry as well as internal controls.
PROCAS' management conducts periodic reviews of activities within all related departments. Related department reviews include tests and review of policies and procedures including logical access, physical access, software network monitoring, change management, incident response, and backups.

PROCAS is responsible for designing and implementing security policies. PROCAS reviews all Company policies prior to release to verify they don't raise any security concerns and to confirm that they do not conflict with any of the existing security policies. The team monitors security best practices and trains staff on their use.

Furthermore, PROCAS is responsible for ensuring that the environment is equipped with security products, as necessary, and is responsible for keeping up to date with mitigations and countermeasures against exploits and vulnerabilities. The Company completes monthly internal vulnerability scans and annual external vulnerability scans in order to facilitate the security and availability of the system. Any high-risk vulnerabilities identified are tracked through resolution. PROCAS will review, as necessary, any new or existing instances where there are security questions.

Each PROCAS team member is accountable for keeping up to date with applicable regulatory and/or industry-specific compliance concerns. PROCAS meets on an as-needed basis to address security and availability concerns and is responsible for formalized, annual review of security policies to update any items which require attention.

Subservice Organizations

The Company uses subservice organizations to provide various services. The scope of this report does not include the controls at the applicable subservice organizations. The following is a description of the services each subservice organization provides:

Subservice Organization	Service Provided
Expedient	Provides colocation facilities that provide a hosting environment for servers that maintain client data, internet access, environmental protections, and physical security.
Microsoft Office 365	Provides Office applications, email, and Client Relationship Management systems for office productivity.
Mimecast	Provides inbound and outbound email security, including impersonation protection, malware protection, attachment protection, and long-term retention. Provides the company with an alternate email portal.

The Company has identified the following control to help monitor the subservice organizations:

- The Company obtains and inspects the latest applicable SOC report(s) to ensure an unqualified opinion, appropriate coverage over the time period under audit, implementation of relevant complementary subservice organizational controls, and that noted exceptions are appropriately reviewed by a member of management for potential impact.

Complementary User Entity Controls

PROCAS has contemplated that certain complementary user entity controls should be implemented by user organizations to achieve certain criteria included in this report. The complementary user entity controls are listed below.

The list of complementary user entity controls presented below should not be regarded as a comprehensive list of all controls that should be employed by the client. There may be additional controls that would be deemed appropriate that are not identified in this report.

Complementary User Entity Control
User organizations are responsible for managing access rights, including changes on a timely basis and monitoring user access to ensure that only authorized users maintain active access privileges.
User organizations are responsible for establishing physical and logical security protection over all workstations, servers, and communication hardware that interface with their environment and that are housed in their facilities or other locations under their control or supervision.
User organizations are responsible for reporting to PROCAS any application problems, including unauthorized use of any password or account or any other known or suspected breach of security encountered with PROCAS services and to provide such assistance as is necessary to permit problem resolution.
User organizations are responsible for managing the application's password change frequency and ensuring password change occurs.