AAR 360

Assurance | Advisory
Risk | Compliance

ProfitWell
Independent Service Auditor's Report on Controls at a Service Organization Relevant to Security (SOC 2 Type 1)

As of November 30, 2020

www.AARC-360.com

Table of Contents

SECTION 1 – INDEPENDENT SERVICE AUDITOR’S REPORT

Independent Service Auditor's Report

To: ProfitWell

Scope

We have examined ProfitWell's ('the Company', or 'the Service Organization') accompanying description of its Business Intelligence Platform for Subscription Companies titled "ProfitWell's Description of its Business Intelligence Platform for Subscription Companies" as of November 30, 2020, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design of controls stated in the description as of November 30, 2020, to provide reasonable assurance that ProfitWell'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* (AICPA, *Trust Services Criteria*).

ProfitWell uses Amazon Web Services ('AWS', or the 'Subservice Organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ProfitWell, to achieve ProfitWell's service commitments and system requirements based on the applicable trust services criteria. The description presents ProfitWell's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ProfitWell'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.

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

ProfitWell is responsible for its service commitments and system requirements and for designing and implementing, controls within the system to provide reasonable assurance that ProfitWell's service commitments and system requirements were achieved. ProfitWell has provided the accompanying assertion titled "Assertion of ProfitWell Management" (assertion) about the description and the suitability of design of controls stated therein. ProfitWell is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the Service Organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination. 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, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design of controls involves the following:

- 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
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- 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
- Evaluating the overall presentation of the description

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. 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 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.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects,

a. the description presents ProfitWell's Business Intelligence Platform for Subscription Companies that was designed and implemented as of November 30, 2020, in accordance with the description criteria.

b. the controls stated in the description were suitably designed as of November 30, 2020, to provide reasonable assurance that ProfitWell's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of November 30, 2020 and if the Subservice Organization and user entities applied the complementary controls assumed in the design of ProfitWell's controls as of November 30, 2020.

Restricted Use

This report is intended solely for the information and use of ProfitWell, user entities of ProfitWell's Business Intelligence Platform for Subscription Companies as of November 30, 2020, business partners of ProfitWell subject to risks arising from interactions with the Business Intelligence Platform for Subscription Companies, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the Service Organization
- How the Service Organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the Service Organization to achieve the Service Organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the Service Organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the Service Organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

AARC-360

Alpharetta, Georgia
December 18, 2020

SECTION 2 – ASSERTION OF PROFITWELL MANAGEMENT

Assertion of ProfitWell Management

December 18, 2020

We have prepared the accompanying description of ProfitWell's ('the Company', or 'the Service Organization') Business Intelligence Platform for Subscription Companies titled "ProfitWell's Description of its Business Intelligence Platform for Subscription Companies" as of November 30, 2020, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, Description Criteria) (description criteria). The description is intended to provide report users with information about the Business Intelligence Platform for Subscription Companies that may be useful when assessing the risks arising from interactions with ProfitWell's system, particularly information about system controls that ProfitWell has designed and implemented to provide reasonable assurance that its 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*, (AICPA, Trust Services Criteria).

ProfitWell uses Amazon Web Services ('AWS', or the 'Subservice Organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ProfitWell, to achieve ProfitWell's service commitments and system requirements based on the applicable trust services criteria. The description presents ProfitWell's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ProfitWell's controls. The description does not disclose the actual controls at the Subservice Organization.

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

We confirm, to the best of our knowledge and belief, that

a. the description presents ProfitWell's Business Intelligence Platform for Subscription Companies that was designed and implemented as of November 30, 2020, in accordance with the description criteria.

b. the controls stated in the description were suitably designed as of November 30, 2020, to provide reasonable assurance that ProfitWell's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of November 30, 2020, and if the Subservice Organization and user entities applied the complementary controls assumed in the design of ProfitWell's controls as of November 30, 2020.

Patrick Campbell

Patrick Campbell
Chief Executive Officer
ProfitWell

SECTION 3 – PROFITWELL’S DESCRIPTION OF ITS BUSINESS INTELLIGENCE PLATFORM FOR SUBSCRIPTION COMPANIES

ProfitWell’s Description of Its Business Intelligence Platform for Subscription Companies as of November 30, 2020

ProfitWell’s Services Overview

Founded in 2012 and headquartered in Boston, MA, ProfitWell provides Business Intelligence Platform for Subscription Companies that reduce churn, optimize pricing, and give companies accurate, free revenue reporting.

ProfitWell’s customers consist of subscription-as-a-service (SaaS) and direct-to-consumer (DTC) companies across a variety of industries.

Products and Services

ProfitWell’s core application is a multi-user application that provides the following services:

- Captures data from 3rd party subscription management and billing systems
- Calculates analytics on that data on a per-customer basis such as monthly recurring revenue (MRR), customer lifetime value (LTV) and other revenue metrics
- Provides a secure website where users can see metrics over time for their business, such as growth and churn rates
- Determine churn risk for customers, and proactively reaches out to those who are at risk of cancelling their subscriptions to prevent loss of revenue for the company

Subscription data is ingested into the ProfitWell application on a periodic basis from the billing systems which act as a system of record for the data. This includes information such as which plan each subscriber is on, invoices those customers have been issued, and payments made against those invoices. Calculated metrics are shown through the application’s secure web interface.

Principal Service Commitments and System Requirements

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 offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the ProfitWell application are designed to permit system users to access the information they need, while restricting them from accessing to those not authorized
- Use of encryption technologies to protect customer data both at rest and in transit

ProfitWell establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in ProfitWell’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 application.

Components of the System Used to Provide the Services

Infrastructure

The application runs on Linux containers running in Kubernetes at Amazon Web Services (AWS)

Employees access the cloud network through their desktop on company-supplied computers through an encrypted OpenVPN gateway using Advanced Encryption Standard 256-bit encryption to protect data and communications.

The application uses a MySQL relational database management system. These database servers are housed in ProfitWell's secure Virtual Private Cloud (VPC) at AWS.

Software

The application is a web application written in the python programming language for backend processes and TypeScript for the user interface. It is developed and maintained by ProfitWell's in-house software engineering group. The software engineering group enhances and maintains the application to provide service for the company's customers.

The application connects to 3rd party billing providers using OAuth authentication with credentials provided to the application during the signup process. The ProfitWell application integrates with the following data providers:

- Stripe
- Zuora
- Braintree
- Recurly
- Chargify
- Chargebee
- ReCharge

The application ingests data from the selected data provider for each company on a periodic basis, at a minimum of four (4) times per day, and as often as several times per hour. The data is stored in the database at which point processes are started to run various calculations and analytical operations on the data. The raw data is not exposed to the end user, but rather the results of the calculations performed. Customers can login to the web interface to see a variety of business analytics and insights about revenue growth, churn rates, and more.

For customers signed up for ProfitWell Retain, additional steps are taken with the data to determine additional attributes about a customer such as churn risk. Depending on the results of the analysis, automated emails may be sent to the customer, or in-app notifications presented to the end user the next time they login the web interface.

ProfitWell has a staff of approximately 60 employees organized in the following functional areas:

- *Corporate.* Executives, and company administrative support staff, such as Accounting and Human Resources. This group uses the ProfitWell application mostly as an end-user to monitor revenue metrics for ProfitWell itself.

- *Product.* Software systems development and application support personnel manage electronic interfaces and define new features for the product.

Data

Data, as defined by ProfitWell, constitutes the following:

- Customer lists
- Invoices
- Charges
- Subscription Histories
- Output reports
- Error logs

Data processing is initiated by ProfitWell on a periodic basis. Data is pulled directly from the system of record, which will include customer lists and associated subscription data for each customer. Data may also be added through ProfitWell's API, both customer lists and subscription histories, as well as additional metadata as needed.

Output reports are available in electronic comma-delimited value file exports, or electronically from the various websites. The availability of these reports is limited by job function. Reports delivered externally are sent via the ProfitWell application over connections secured by trusted security certificates.

Processes and Procedures

Management has developed and communicated procedures to restrict logical access to the application. Changes to these procedures are performed annually and authorized by senior management. These procedures cover the following key security life cycle areas:

- Data classification (data at rest, in motion, and output)
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, super user functionality, master passwords, powerful utilities, and security devices (for example, firewalls)

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

The security category and applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Security criteria and controls designed, implemented, and operated to meet them ensure that the system is protected against unauthorized access (both physical and logical). The controls supporting the applicable trust services security criteria are included in Section 4 of this report. Although the applicable trust services criteria and related controls are included in Section 4, they are an integral part of ProfitWell's description of the application.

Control Environment

Management Philosophy

ProfitWell's control environment reflects the philosophy of senior management concerning the importance of security of financial data and information. ProfitWell's Security Steering Committee meets quarterly. The committee, under the direction of the CEO, oversees the security activities of ProfitWell. The committee members are made up of the executive management team plus the Head of Finance and Director of Engineering. The committee is charged with establishing overall security policies and procedures for ProfitWell. The importance of security is emphasized within ProfitWell through establishing and communicating policies and procedures and is supported by investing in resources and people to carry out the policies. In designing its controls, ProfitWell has considered the relevance of controls to meet the relevant trust criteria.

Security Management

ProfitWell has an Ops team as part of the Engineering organization which is responsible for management of information security throughout the organization. As the information security team maintains security, it monitors known incidents and patches as well as results from recent vulnerability assessments and addresses necessary changes to the policies and procedures. Such changes can include a reclassification of data, a reassessment of risk, changes in incident response plans, and a verification of responsibilities for authorizing and monitoring accesses. Changes are reviewed and communicated during weekly IT maintenance meetings or through system alerts.

During annual security training and awareness programs, management ensures communication of the latest security policies.

Additionally, management is responsible for ensuring business associate agreements are current for third parties and for updating the annual IT risk assessment.

Security Policies

The following security policies and related processes are in place for the ProfitWell application:

- Data classification and business impact assessment
- Selection, documentation, and implementation of security controls
- Assessment of security controls
- User access authorization and provisioning
- Removal of user access
- Monitoring of security controls
- Security management

ProfitWell's information security policies and procedures contain formal usage guidelines that define appropriate IT resource usage to help ensure that information is utilized and maintained in a manner that ensures that such information remains secure. Access to the production applications is restricted to authorized personnel. Former employees' access to applications is removed promptly upon the employee leaving ProfitWell.

ProfitWell restricts access to system configurations, super-user functionality, master passwords, and security devices by implementing logical access controls. User access provisioning procedures exist to grant and revoke user access upon employee / contractor hire and termination, respectively. Access reviews are conducted annually to help ensure that current application users were authorized to access the applications and that their access rights were appropriate. User passwords are defined and enforced in accordance with the information security policy. Access to the firewall is restricted to authorized personnel. Further, administrative access to configure firewall access control rules is restricted to authorized individuals.

ProfitWell protects against unauthorized access to production system resources by restricting remote connectivity to authorized users. Administrator access is restricted to authorized users. Critical information system components require a separate password to gain access, and rights are limited to administrators

ProfitWell utilizes industry standard encryption techniques to protect user authentication information and the corresponding communication session transmitted over the Internet or other public networks. Transmission-level SSL security is implemented when information is being transmitted over public networks.

Personnel Security

Background checks are performed on new employees, who are also required to review and acknowledge their receipt of relevant security policies. The new positions are supported by job descriptions. Once employed, employees are subject to ProfitWell's procedures for accessing systems and sanctions for violating ProfitWell's information security policy. Employees are instructed to report potential security incidents to the security hotline via email or Slack.

ProfitWell's business associate agreement instructs user entities and transportation providers to notify their respective account representative if they become aware of a possible security breach.

Physical Security and Environmental Controls

The ProfitWell application is located at Amazon Web Services. AWS access is monitored by video surveillance and on-site personnel, and it is controlled through the use of card reader systems. Physical access to AWS data centers is not granted to employees of ProfitWell or any other outside team.

AWS employs UPS power systems, air conditioning systems, fire detection and suppression systems, and environmental monitoring and alert notification systems.

Change Management

ProfitWell has a formalized change management process in place, which requires identification and recording of significant changes, assessment of risk and potential effect of such changes, approval of proposed changes, and testing of changes to verify operational functionality. Proposed changes are evaluated to determine if they present a security risk and what mitigating actions, including employee and user entity notifications, must be performed. The software engineering and product teams meet weekly to review and schedule changes to the software environment.

Emergency changes follow the formalized change management process, but at an accelerated timeline. Prior to initiating an emergency change, necessary approvals are obtained and documented.

Changes to infrastructure and software are developed and tested in a separate development or test environment before implementation. Additionally, developers do not have the ability to migrate changes into production environments without sign off from at least one other member of the software engineering team.

ProfitWell has a formalized security and systems development methodology that includes project planning, design, testing, implementation, maintenance, and disposal or decommissioning.

ProfitWell uses a standardized server build checklist to help secure its servers, and it conducts quarterly vulnerability assessments to identify potential system vulnerabilities. Patches are applied regularly in accordance with ProfitWell's patch management process.

ProfitWell has implemented change control procedures to help ensure the integrity of network devices, programs, and data. Change control procedures are necessary to establish adequate testing and recovery plans. Change management processes include properly authorizing, testing, approving, implementing, documenting, and maintaining system applications and security patches. The senior leadership of the engineering team oversees the change management process to help ensure that all changes are authorized, tested, and approved prior to migration to the production environment.

The leadership of the engineering team is responsible and accountable for:

- Oversight of the Change Management Policy
- Authorization of work performed by third-party providers
- Monitoring the status of all system testing and implementation
- Oversight of the implementation of appropriate controls for new network applications, servers, and related equipment
- Oversight of fundamental change requests to the company’s network infrastructure
- Ensuring all users receive appropriate training on changes

Change Management Guidelines

The Change Management Policy covers the following types of system configurations:

- Installation of new servers
- Installation of new network software applications/parameter changes
- New or updated operating systems
- Installation of routine security patches and updates
- New policies, procedures, and standards
- Ensuring that all network systems are properly backed up prior to the implementation of significant system updates or changes
- Testing changes prior to introduction into the production environment

Systems Operations

Incident reporting and incident response are documented within the Incident Response Policy and Procedures and tracked by management until resolution. Employees are encouraged to bring forth any concerns over information security. If employees have concerns over a potential loss of data or breach, they are to notify ProfitWell’s Management immediately and the Incident Response Policy and Procedures are followed.

For the purpose of protecting and securing vital data and related business information, ProfitWell has configured backups to run on a daily basis. Backups are monitored for failure using an automated system.

System Monitoring

The Ops team uses a variety of security utilities to identify and detect possible security threats and incidents. These utilities include, but are not limited to, firewall notifications, intrusion detection system (IDS) or intrusion prevention system (IPS) alerts, vulnerability assessment reports, and operating system event logs. These alerts and notifications are reviewed daily by the Ops team using in-house monitoring tools. Additionally, the Ops team has developed and will review the following reports:

- Failed object level access
- Daily IDS or IPS attacks
- Critical IDS or IPS alerts
- Failed login detail
- Firewall configuration changes

Security events requiring further investigation are tracked using a help desk ticket and monitored until resolved.

Problem Management

Security incidents and other IT-related problems are reported using the company’s ticketing system. Issues are tracked using a change request ticket and monitored until resolved.

Data Backup and Recovery

ProfitWell uses services provided by AWS to back up its data files and software. Access to backup devices, scheduling utilities, systems, and media is restricted to authorized personnel.

System Account Management

ProfitWell has implemented role-based security to limit and control access within the production application. Employees are granted logical access to in-scope systems based on documented approvals by appropriate management personnel. The ability to create or modify user access accounts and user access privileges is limited to authorized personnel. User access is reviewed quarterly to verify whether individuals' access is necessary for their job functions and to identify the existence of inappropriate accounts.

The Human Resources Department provides IT personnel with an employee termination report on the day of employee termination. IT reconciles the termination report with current access privileges to determine if access has been appropriately removed or disabled.

Administrative access to ProfitWell servers and databases is restricted to authorized employees.

Unique user identification numbers, names, and passwords are required to authenticate all users to the application. Passwords must be complex.

Risk Mitigation

ProfitWell has implemented risk mitigation strategies to reduce the organization's exposure to the risk.

Vendor Management

ProfitWell monitors commitments provided by their vendors and where applicable independent auditor's reports from the third parties are obtained as an aspect of monitoring vendor SLAs. ProfitWell has assigned senior personnel to assess compliance by vendors.

Insurance coverage

Inadequate insurance coverage could result in severe financial loss for ProfitWell as well as loss of reputation and increased liability**.** The overall integrity of ProfitWell could be compromised by such inadequate coverage. ProfitWell has arranged for insurance coverage by reputable institutions in order to complement an effective system of controls.

Risk Assessment Process

ProfitWell regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to security based on the applicable trust services criteria set forth in TSP section 100, *2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

ProfitWell assesses security risks on an ongoing basis. This is done through regular management meetings with the engineering team, reviewing and acting upon security event logs, performing vulnerability assessments, and conducting a formal annual IT risk assessment in conjunction with the company-wide risk assessment.

Senior management, as part of its annual information security policy review, considers developments in technology and the impact of applicable laws and regulations on ProfitWell's security policies.

Changes in security threats and risks are reviewed by ProfitWell, and updates to existing control activities and information security policies are performed, as necessary.

ProfitWell performs risk assessments to determine the adequacy and implementation of technical, operational, and security controls to mitigate the potential risks and vulnerabilities to the security of information. ProfitWell has completed a risk assessment which identifies threats to its information and assets. This risk assessment is reviewed and updated periodically to include new assets, threats, and controls. Security processes and procedures are revised by ProfitWell management based on the assessed threats identified during the risk assessment process. ProfitWell's system security is periodically evaluated and compared with the procedures defined in the Information Security policies and procedures.

Information and Communication Systems

ProfitWell has an information security policy 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 Slack to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems.

A formally documented Incident Response Program exists that defines the process whereby ProfitWell reports security incidents and breaches. The policy addresses breach notification and escalation processes. Changes that may affect system security are communicated in writing to affected customers under the provisions of the service level agreements. External users have the ability to communicate security incidents or concerns to ProfitWell.

Monitoring Controls

ProfitWell has an Incident Response Program to identify, report, and act upon system security breaches and other incidents. Incidents are initially documented and escalated as needed based on severity. Incident response is broken down into six (6) main categories which include the following:

- Identification of the Incident
- Assessment of the Incident
- Containing and Controlling the Incident
- Notification of Federal Regulators and Law Enforcement
- Customer Notification
- Post-Incident Assessment

ProfitWell uses an industry standard centrally-managed monitoring software that is configured to monitor server events and data backup status. All relevant events are logged, and thresholds are defined to alert administrators of significant events.

Changes to the System During the Past 90 Days

There were no changes that are likely to affect report users' understanding of how the application is used to provide the service during the past 90 days.

Complementary Subservice Organization Controls (CSOCs)

ProfitWell utilizes a subservice organization to perform certain key operating functions for the ProfitWell application. The accompanying description of controls includes only those policies, procedures and controls at ProfitWell, and does not extend to policies, procedures and controls at the Subservice Organization.

ProfitWell uses AWS to provide cloud hosting services in support of its application and the following table presents the applicable Trust Services criteria that are intended to be met by controls at the subservice provider, alone or in combination with controls at ProfitWell, and the types of controls expected to be implemented at the subservice provider to meet those criteria.

Subservice Organizations

The ProfitWell is built on top of Amazon Web Services (AWS) infrastructure as a service (IAAS) and platform as a service (PaaS) products. AWS undergoes its own rigorous audit processes to include an annual AICPA based SOC 2 audit and is examined annually by ProfitWell. It is expected that each Subservice Organization has implemented the following types of controls to support the associated criteria.

	Complementary Subservice Organization Controls (CSOCs)	Related Criteria
1.	AWS is responsible for maintaining logical security over the servers and other hardware devices upon which the ProfitWell application is hosted.	CC6
2.	AWS is responsible for notifying ProfitWell of any security incidents related to security over the servers and other hardware devices upon which the ProfitWell application is hosted.	CC7
3.	AWS is responsible for maintaining physical security over its data center in which the servers used to host the application are housed.	CC6

Trust Services Criteria and Related Controls

CC1.0 – Common Criteria Related to Control Environment

No.	Criteria	Control Activity Specified by the Service Organization
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The strategic direction and oversight of the Company is conducted by Senior Management and the Board of Directors.
		An Employee Handbook is documented by the Company and distributed to all employees.
		Management communicates and oversees the implementation of the Code of Conduct, Integrity, and Ethics to new and current employees.
		Procedures are in place for employee evaluations to be performed against individual objectives derived from the Company’s goals, established standards, and specific job responsibilities.
		The Company’s policies include disciplinary actions and termination as potential sanctions for employee misconduct.

No.	Criteria	Control Activity Specified by the Service Organization
		Contracted employees are required to read and accept the contractor non-disclosure agreement prior to hiring.
CC1.2	The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The Company's Board of Directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.
		The Board of Directors defines, maintains, and periodically evaluates the skills and expertise needed among its members.
		The Company's Board of Directors have sufficient members who are independent from management and objective in evaluations and decision making.
		The Board of Directors supplements its expertise relevant to security as needed, through the use of a subcommittee or consultants.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Organizational charts are in place to communicate the defined key areas of authority, responsibility and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. These charts are communicated to employees and updated as needed.
		Reporting relationships and the organizational structure is reviewed by management as part of organizational planning and adjusted as needed based on changing commitments and requirements.
		Documented job descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
		Job descriptions are inspected annually for needed changes and updated if such changes are identified.
		Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors taking into consideration segregation of duties as necessary at the various levels of the Company and requirements relevant to security.
		The Company has assigned senior level executives the responsibility of handling their primary vendors.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Job requirements are documented in the job descriptions, and active employees' abilities to meet these requirements are evaluated as part of the performance review process.
		New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the employee checklists.
		Personnel with responsibilities for system configurations stay knowledgeable of appropriate ways to securely configure the Company's systems.

No.	Criteria	Control Activity Specified by the Service Organization
		The Company has developed contingency plans for assignments of responsibility important for internal control.
		Background checks are performed on all employees and standards are documented in policy.
		Hiring and termination policies and procedures are documented by the Company.
		Training programs are implemented by the Company.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Employee evaluations are performed against individual objectives derived from the Company’s goals, established standards, and specific job responsibilities.
		The Company's Management establishes performance measures for responsibilities at all levels of the Company, reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and longer-term objectives.
		Management and the Board of Directors establish measurable goals and performance evaluation criteria, including, incentives, and other rewards, and sanctions appropriate for responsibilities at all levels of the Company, considering the achievement of both short-term and longer-term objectives.
		Management and the board of directors establish measurable goals and performance evaluation criteria, taking into consideration pressures associated with the achievement of objectives.
		Monitoring activities are performed by management to ensure operational quality and control.

CC2.0 – Common Criteria Related to Communication and Information

No.	Criteria	Control Activity Specified by the Service Organization
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The Company implements technical controls to protect sensitive data within the Company and has documented information security policies and procedures.
		Information systems process and transform relevant data into information.
		Management performs monitoring activities to ensure operational quality and control.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the	Policy and procedures documents for significant processes are available on the Company’s shared internal drive.

No.	Criteria	Control Activity Specified by the Service Organization
	functioning of internal control.	Management’s communication sets the tone and direction for the entire organization.
		Employees can communicate confidential information when normal channels are not effective.
		Management selects the methods of internal communication to inform internal parties of information in a timely manner.
		Personnel with responsibility for designing, developing, implementing, operating, maintaining, or monitoring system controls receive communications about their responsibilities.
		The Company has documented incident response policies and procedures.
		System changes are communicated to internal users.
		The Company provides security training to employees to communicate security policies and procedures.
		The Company has prepared an objective description of the system and its boundaries and communicated such description to authorized users.
		Policy and procedures documents for significant processes are available on the Company’s shared internal drive.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Customer's service agreements include documented external user responsibilities.
		Open communication channels allow input from customers providing management and the Board of Directors with relevant information.
		Relevant information resulting from assessments conducted by external parties is communicated to management and Board of Directors.
		Clients are provided guidance in regard to best practices when utilizing the Company’s services.
		The Company communicates its system objectives to appropriate external users.
		Terms of Service clearly delineate user responsibilities relative to system controls and applicable communications.

No.	Criteria	Control Activity Specified by the Service Organization
		Internal and external users are provided escalation procedures for reporting security incidents such as reporting failures, incidents, concerns, and other complaints.

CC3.0 – Common Criteria Related to Risk Assessment

No.	Criteria	Control Activity Specified by the Service Organization
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The Company has defined a formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.
		The Company management considers the acceptable levels of risk relative to the achievement of operations objectives.
		Internal reporting provides management with accurate and complete information regarding management's choices and information needed in managing the Company.
		The Company reflects the required level of precision and accuracy suitable for user needs in nonfinancial reporting objectives and materiality within financial reporting objectives.
		Management considers the acceptable levels of variation relative to the achievement of operations objectives.
		Privacy policies are implemented for handling personal information in accordance with relevant legislation and regulations.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Risks to the Company are evaluated and mitigation procedures are implemented based on risk evaluations.
		Risk identification considers both internal and external factors and their impact on the achievement of objectives.
		The Company risk management strategy involves appropriate levels of management.
		Identified risks are analyzed through a process that includes estimating the potential significance of the risk.
		The risk assessment policy includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.
		During the risk assessment and management process, management identifies changes to the production servers, network infrastructure, and production software that potentially threaten the achievement of business objectives and update the potential threats to system objectives.

No.	Criteria	Control Activity Specified by the Service Organization
		The Company's risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the Company's information systems.
		The Company's identified risks includes (1) determining the criticality of identified assets in meeting objectives; (2) assessing the impact of identified threats and vulnerabilities in meeting objectives; (3) assessing the likelihood of identified threats; and (4) determining the risk associated with assets based on asset criticality, threat impact, and likelihood.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Not applicable - Based on the nature of the services provided by ProfitWell, management has, while assessing risks to the achievement of objectives, considered the potential for fraud to be not relevant.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The risk identification process considers changes to the physical environment in which the Company operates.
		The Company assesses changes in the business model while considering the potential impacts of new business lines.
		Risk assessment assesses changes in the systems and their potential impact.

CC4.0 – Common Criteria Related to Monitoring Activities

No.	Criteria	Control Activity Specified by the Service Organization
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The Company uses an industry standard, centrally managed, monitoring software that is configured to monitor server events, data backup status, and anti-virus statistics. All relevant events are logged, and thresholds are defined to alert administrators of significant events. Procedures are in place to review system monitoring software configurations on a periodic basis.
		Changes to the business environment are monitored and appropriately documented.
		The design and current state of the internal control system are used to establish a baseline for ongoing and separate evaluations.
		Senior Management possess adequate knowledge and skills to perform the control evaluation accurately.
		The feedback received from the control evaluations is integrated into the business and IT processes on an ongoing basis and subject to the changing business conditions.

No.	Criteria	Control Activity Specified by the Service Organization
		The management adjusts the scope and frequency of separate evaluations based on the identified or perceived risks.
		Daily operational security procedures are performed by the Company in relation to their internal security processes.
		A penetration test is performed annually to meet changing commitments and requirements.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the Board of Directors, as appropriate.	The Company's management assesses results of the periodic and separate control evaluations regularly and review the corrective actions in regard to the identified deficiencies.
		The Company identifies deficiencies to the respective parties to take corrective actions and to the Senior Management as needed.
		Management tracks whether deficiencies are remedied on a timely basis.

CC5.0 – Common Criteria Related to Control Activities

No.	Criteria	Control Activity Specified by the Service Organization
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The Company has a risk management and risk assessment strategy to help ensure that controls and mitigation strategies are selected, developed, and deployed adequately to mitigate risks.
		Management takes into account the business and IT environment, complexity, nature, scope of the business operations, and the specific characteristics of the Company while selecting and developing the control activities.
		Management selects the business processes for applying the control activities based on their relevance.
		The Company applies a mix of control activity types including manual and automated, preventive and detective to mitigate the risks.
		The Company management applies control activities across various levels in the Company.
		Organizational segregation of duties is defined and documented for all personnel.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	As part of the IT strategic plan, strategic IT risks affecting the Company and recommended courses of action are identified and discussed.
		Selected control activities help ensure the completeness, accuracy, and availability of technology processing.

No.	Criteria	Control Activity Specified by the Service Organization
		Management selects and implements control activities that restrict technology access rights to authorized users commensurate with their job responsibilities and protect the Company’s assets from external threats.
		The Company has control activities in place over the acquisition, development, and maintenance of current IT systems and its infrastructure to achieve management’s objectives.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Management implements control activities integrated with the business processes and employees’ day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.
		The Company management assigns ownership and accountability for control activities to management of the business unit or function in which the relevant risks reside.
		Procedures are in place to guide responsible personnel in performing their control activities in a timely manner and as defined by the policies and procedures.
		Responsible personnel research and take action on matters identified as a result of executing control activities.
		The personnel performing control activities are competent for their role and perform the activity with diligence and continuing focus.
		A revision history is included within the Company’s information security policy and is used to track reviews and updates to the policy.

CC6.0 – Common Criteria Related to Logical and Physical Access Controls

No.	Criteria	Control Activity Specified by the Service Organization
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	An inventory of all hardware and software within the scope of services are maintained and reviewed on at least an annual basis during the risk assessment process.
		Logical access control systems are utilized by the Company to control permissions and privileges.
		Unique user IDs are required to be used within the Company’s systems.
		Password configurations are enforced through the Company’s logical access control systems.

No.	Criteria	Control Activity Specified by the Service Organization
		Encrypted VPNs are used to help ensure the security and integrity of the data passing over the public network.
		The Company's virtual systems are segmented to permit unrelated portions of the information system to be isolated from each other.
		A firewall is deployed to monitor and restrict inbound Internet traffic.
		Web-based traffic is protected by industry standard encryption protocols. Remote connections to the Company's applications are provided through an SSL-based connection.
		Role based access control is in place to ensure principle of least privilege is followed and user rights are commensurate with job roles.
		New internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed, and access is disabled when access is no longer required, or the infrastructure and software are no longer in use.
		The Company stores data at rest on encrypted databases or backups.
		The Company uses a key management system to manage entire lifecycle of encryption keys.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	User IDs are authorized and implemented by the Company.
		Users are authorized and approved prior to gaining access to the Company's systems.
		Access is revoked for any terminated and separated employees.
		User access reviews are conducted on a semi-annual basis to help ensure user identities are not compromised.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Access rights and privileges granted to user IDs are defined through policy.
		Access is revoked for any terminated and separated employees.
		Access control procedures are utilized to grant access to the online application and access is granted based on the users' job function.

No.	Criteria	Control Activity Specified by the Service Organization
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Not applicable - The company stores sensitive data within AWS cloud.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Equipment and media destruction policies and procedures are implemented and documented by the Company.
		Decommissioned hardware containing potentially sensitive data is erased using 3rd party software.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Encrypted VPNs are required for remote access to help ensure the security and integrity of the data passing over the public network.
		Identification and authentication credentials are protected during transmission outside its system boundaries.
		Multi-factor authentication is required for remote network access by employees, administrators, and third parties.
		Firewall and an intrusion detection system are used to log access events and is available for review by authorized personnel.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Firewall and router configuration and configuration files are documented by the Company.
		Web-based traffic is protected by industry standard encryption protocols. Remote connections to the Company's applications are provided through an SSL-based connection.
		The Company prohibits the transmission of sensitive information over the Internet or other public communications paths, unless it is encrypted.
		Procedures are in place to guide personnel in the use and protection of removable media.
		The Company employs full-device hard drive encryption to protect the confidentiality and integrity of information on approved mobile devices.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	File integrity monitoring is in place to detect and alert authorized personnel of any unauthorized changes to software and configuration parameters.
		The Company follows the change management process to deploy, maintain, and modify software.

No.	Criteria	Control Activity Specified by the Service Organization
		Antivirus is installed on the Company’s systems and are required to updated regularly.
		Procedures are in place to scan information assets that have been transferred or returned to the Company’s custody.

CC7.0 – Common Criteria Related to System Operations

No.	Criteria	Control Activity Specified by the Service Organization
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	System configuration standards are documented by the Company. The system configuration standards are reviewed and updated by the Company on an annual basis as part of the annual policy review.
		Network scanning and testing is performed by the Company on an at least annual basis.
		File Integrity Monitoring (FIM) is in place to detect unauthorized modifications of critical system files, configuration files, or content files.
		Procedures are in place to detect unauthorized modification to system records.
		The Company performs external vulnerability scans to maintain the on-going security posture and security level for the Company's application.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Incident response policies and procedures are documented by the Company.
		The Company utilizes system monitoring tools to identify and evaluate ongoing system performance, security threats, and unusual system activity.
		The monitoring software sends event alert ticket notifications to the Company's IT personnel to provide notification of significant events.
		Security incidents and alerts are documented and retained by the Company.
		The Company has implemented processes to monitor the effectiveness of detection tools.

No.	Criteria	Control Activity Specified by the Service Organization
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Policies and procedures are documented to guide personnel in identifying and mitigating security breaches and other incidents.
		Detected security events are communicated to and inspected by the individuals responsible for the management of the security program and actions are taken, if necessary.
		IT personnel follow defined protocols for resolving and escalating reported events.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are assigned.
		Policies and procedures are documented to guide personnel in identifying and mitigating security breaches and other incidents.
		Procedures are in place to mitigate the effects of ongoing security incidents.
		Procedures are in place to end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized access, and other remediation actions.
		IT Personnel utilize documented back-up and recovery procedures to help ensure that proper back-ups are performed. Weekly full-system and daily incremental backups are performed using an automated system. Backups are monitored for failure using an automated system and procedures are in place to invoke the incident management process on a timely basis. Backups are tested for integrity on an annual basis. The Company’s business continuity plans are tested on an annual basis.

No.	Criteria	Control Activity Specified by the Service Organization
		Protocols for communicating security incidents and actions taken to affected parties are developed and implemented.
		Procedures are in place to understand the nature of the incident and the severity.
		Procedures are in place to remediate vulnerabilities through the development and execution of remediation activities.
		Policies are documented and maintained which address remedial actions for lack of compliance with policies and procedures.
		The design of incident response activities is evaluated for effectiveness on a periodic basis.
		Management reviews incidents related to security and identifies the need for system changes based on incident patterns and root causes.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Procedures are in place to restore the affected environment to functional operation by rebuilding systems, updating software, installing patches, and changing configurations, as needed.
		Procedures are in place to communicate the nature of the incident, recovery actions taken, and activities required for the prevention of future security events are made to management and others as appropriate.
		Procedures are in place to analyze the root cause of an event.
		Procedures are in place to implement changes to preventive controls, detective controls, or both, to prevent and detect recurrences on a timely basis.
		Procedures are in place to analyze lessons learned and improve the business continuity plan and recovery procedures.
		Procedures are in place to test the incident response plan and business continuity plan on an annual basis.

CC8.0 – Common Criteria Related to Change Management

No.	Criteria	Control Activity Specified by the Service Organization
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The Company has a documented change control policies and procedures which defines the procedures for change management review, testing, and approval of scheduled software and hardware changes migrated into the production environment.
		System change requests are reviewed and approved by management prior to work commencing on the requested change.
		A process is in place to design and develop system changes.
		A process is in place to document system changes to support ongoing maintenance of the system and to support system users in performing their responsibilities.
		A change management tracking system is utilized to maintain and track application change requests.
		Industry-accepted hardening standards are used as a basis for the Company’s system configuration standards.
		Application quality assurance testing validates key processing for the application during the change management process.
		Change requests are authorized, tested, approved, documented, and appropriately moved into production.
		Change management policies and procedures are documented that outline that change management separation of duties such that authorization, testing and implementation are segmented functions within the process.
		The Company has adopted a formal systems development life cycle methodology that governs the development, implementation, and maintenance of computerized information systems and related technology.
		A baseline configuration of IT and control systems is created and maintained.
		A process is in place for authorizing, designing, testing, approving and implementing changes necessary in emergency situations.

CC9.0 – Common Criteria Related to Risk Mitigation

No.	Criteria	Control Activity Specified by the Service Organization
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	An annual risk assessment process is in place and performed by the Company.
		The risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the Company to meet its objectives.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Procedures are in place to establish specific requirements for a vendor and business partner engagement that includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels.
		Due diligence procedures are documented and performed prior to engaging with a new service provider.
		Senior management members have been assigned the responsibility and accountability for the management of risks associated with vendors and business partners.
		The Company establishes communication and resolution protocols for service or product issues related to vendors and business partners.
		The Company establishes exception handling procedures for service or product issues related to vendors and business partners.
		The Company implements procedures for addressing issues identified with vendor and business partner relationships.
		The Company implements procedures for terminating vendor and business partner relationships.

Complementary User Entity Controls

Certain criteria specified in the description can be achieved only if complementary user entity controls contemplated in the design of ProfitWell's controls are suitably designed and operating effectively, along with related controls at ProfitWell. Complementary User Entity Controls are specific user controls or issues each ProfitWell client organization should implement or address respectively in order to achieve the applicable criteria identified in this report. These considerations are not necessarily a comprehensive list of all internal controls that should be employed by user entities, nor do they represent procedures that may be necessary in all circumstances.

1. User entities are responsible for understanding and complying with their contractual obligations to ProfitWell.
2. User entities are responsible for notifying ProfitWell 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 ProfitWell's 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 ProfitWell's services.

6. User entities are responsible for ensuring that user IDs and passwords are assigned to only authorized individuals.
7. User entities are responsible for ensuring that data submitted to ProfitWell is complete, accurate, and timely.
8. Standards and processes are in place for user entities to follow for security and industry guidelines.

SECTION 4 – GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

Guidance Regarding Information Provided by the Service Auditor

AARC-360's examination of the controls of ProfitWell was limited to the Trust Services Criteria Category of Security and related criteria and controls specified by the management of ProfitWell and did not encompass all aspects of ProfitWell's operations or operations at the Subservice Organization and User Entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) the Statement on Standards for Attestation Engagements No. 18 (AT-C section 205, *Examination Engagements*).

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	AARC-360 made inquiries of ProfitWell personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	AARC-360 observed application of the control activities by client personnel.
Inspection	AARC-360 inspected among other items, documents, reports, or electronic files that contain evidence of the performance of the controls, such as system log files.

In determining whether the report meets the users' objectives, the users should perform the following procedures:

- Understand the aspects of ProfitWell's controls that may affect the processing of the User Entity's transactions;
- Understand the flow of significant transactions through ProfitWell; and
- Determine whether the criteria are relevant to the user's requirements.