360ADVANCED

SOC 1 (SSAE No. 16) Type 1 Report on Controls Placed in Operation for Tax Return and Financial Statement Portal Services

Stone Vault, LLC

January 31, 2013

STONEVAULT

AICPA Service Organization Control Reports
AICPA
SOC
aicpa.org/soc
Formerly SAS 70 Reports

STONE VAULT, LLC

Table of Contents

SECTION 1:

INDEPENDENT SERVICE AUDITORS' REPORT

INDEPENDENT SERVICE AUDITORS' REPORT ON THE DESCRIPTION OF THE SERVICE ORGANIZATION'S SYSTEM AND THE SUITABILITY OF THE DESIGN OF CONTROLS PLACED INTO OPERATION

To Stone Vault, LLC:

We have examined Stone Vault, LLC's ("StoneVault") description of its Tax Return and Financial Statement Portal Services system as of January 31, 2013 and the suitability of the design of StoneVault's controls to achieve the related control objectives stated in the description. The description indicates that certain complementary user entity controls must be suitably designed and implemented at user entities for related controls at the service organization to be considered suitably designed to achieve the related control objectives. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

StoneVault uses Amazon Web Services, Inc. ("AWS") and Rackspace Hosting, Inc. ("Rackspace"), sub-service organizations, for application hosting, backup and storage services and cloud server services, respectively. The description included in Section 3 of this report includes only the controls and related control objectives of StoneVault and excludes the control objectives and related controls of AWS and Rackspace. Our examination did not extend to the controls at AWS or Rackspace.

Within Section 2 of this report, StoneVault has provided an assertion about the fairness of the presentation of the description and suitability of the design of the controls to achieve the related control objectives stated in the description. StoneVault is responsible for preparing the description and for its assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination 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, in all material respects, about whether the description is fairly presented and the controls were suitably designed to achieve the related control objectives stated in the description as of January 31, 2013.

An examination of a description of a service organization's system and the suitability of the design of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description of the system and the suitability of the design of the controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed to achieve the related control objectives stated in the description. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described within StoneVault's assertion in Section 2 of this report. We did not perform any procedures regarding the operating effectiveness of the controls stated in the description and, accordingly, do not express an opinion thereon. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions for the Tax Return and Financial Statement Portal Services system. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or any conclusions about the suitability of the design of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become ineffective or fail.

In our opinion, in all material respects, based on the criteria described in StoneVault's assertion in the next section of this report:

a. the description fairly presents StoneVault's Tax Return and Financial Statement Portal Services system that was designed and implemented as of January 31, 2013, and

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively as of January 31, 2013.

This report is intended solely for the information and use of StoneVault, user entities of StoneVault's Tax Return and Financial Statement Portal Services system as of January 31, 2013, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when obtaining an understanding of user entities information and communication systems relevant to financial reporting. This report is not intended to be and should not be used by anyone other than these specified parties.

February 25, 2013
Tampa, Florida

SECTION 2:

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

February 25, 2013

We have prepared the description of Stone Vault, LLC's ("StoneVault") Tax Return and Financial Statement Portal Services system for user entities of the system as of January 31, 2013 and their user auditors who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when obtaining an understanding of user entities' information and communication systems relevant to financial reporting. We confirm, to the best of our knowledge and belief, that:

a. the description fairly presents the Tax Return and Financial Statement Portal Services system made available to user entities of the system as of January 31, 2013 for the Tax Return and Financial Statement Portal Services system. StoneVault uses Amazon Web Services, Inc. ("AWS") and Rackspace Hosting, Inc. ("Rackspace"), sub-service organizations, for application hosting, backup and storage services and cloud server services, respectively. The description included in Section 3 of this report includes only the controls and related control objectives of StoneVault and excludes the control objectives and related controls at AWS and Rackspace. The criteria we used in making this assertion were that the description

    i. presents how the system made available to user entities of the system was designed and implemented to process relevant transactions as they relate to our environment, including when applicable:

        1. the types of services provided;
        2. the procedures, within both automated and manual systems, by which those services are provided;
        3. how the system captures and addresses significant events and conditions, other than transactions;
        4. the process used to prepare reports or other information provided to user entities of the system;
        5. the specified control objectives and controls designed to achieve those objectives; and
        6. other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.

    ii. does not omit or distort information relevant to the scope of the Tax Return and Financial Statement Portal Services system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the Tax Return and Financial Statement Portal Services system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. the controls related to the control objectives stated in the description were suitably designed as of January 31, 2013 to achieve those control objectives. The criteria we used in making this assertion were that:

    i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management; and

ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

/s/ Stone Vault, LLC

Rick Jablonski – Chief Operating Officer

Dave Stanton – Chief Technology Officer

SECTION 3:

STONEVAULT'S DESCRIPTION OF CONTROLS

SCOPE OF REPORT

This description of the system of controls provided by Stone Vault, LLC ("StoneVault") management, as related to Statement on Standards for Attestation Engagements No. 16 '*Reporting on Controls at a Service Organization*' ("SSAE 16" or "SOC 1"), considers the direct and indirect impact of risks and controls that StoneVault management has determined are likely to be relevant to its user entities' internal controls over financial reporting. The scope of management's description of the system of controls covers the general computer controls supporting the Tax Return and Financial Statement Portal Services system, and considers the initiation, authorization, recording, processing and reporting of transactions within those supporting IT processes. The scope of management's description of the system of controls does not cover the processing of user entity transactions. StoneVault is responsible for identification of risks associated with the system of controls (defined as control objectives), and for the design and operation of controls intended to mitigate those risks. This includes the applicable information technology infrastructure and the supporting processes related to the Tax Return and Financial Statement Portal Services system. StoneVault does not maintain accountability for any user entity assets, liabilities, or equity.

As part of its overall SOC 1 program, StoneVault management sets and determines the scope and timing of each report. This report features the Tax Return and Financial Statement Portal Services system. This description of the system of controls has been prepared by StoneVault management to provide information on controls applicable to the Tax Return and Financial Statement Portal Services system at the Gainesville, Florida facility.

Sub-Service Organizations

StoneVault uses Amazon Web Services, Inc. ("AWS") and Rackspace Hosting, Inc. ("Rackspace"), sub-service organizations, for application hosting, backup and storage services and cloud server services, respectively. The description included in Section 3 of this report includes only the controls and related control objectives of StoneVault and excludes the control objectives and related controls of AWS and Rackspace. Our examination did not extend to controls the AWS or Rackspace.

Significant Changes During the Review Period

Management is not aware of any significant changes that occurred during the review period.

Subsequent Events

Management is not aware of any relevant events that occurred subsequent to the period covered by management's description included in Section 3 of this report through the date of the service auditor's report that would have a significant effect on management's assertion.

Using the Work of the Internal Audit Function

The service auditor did not utilize any work of an Internal Audit function in preparing this report.

OVERVIEW OF OPERATIONS

Company Background

StoneVault is a privately held company, founded in 2012, providing a software as a service (SaaS) solution to professionals in the accounting, banking and insurance industries. StoneVault is controlled by its original founding parties, remains solely self-funded, and has maintained the same stake holders since its inception. StoneVault currently operates with nine employees and has strategic growth plans in place for each department within the company.

StoneVault's web-based software is designed to improve the efficiency of financial document delivery and storage for CPAs, bankers and other financial professionals.

Overview of Tax Return and Financial Statement Portal Services

StoneVault.com is a SaaS product that allows financial professionals to upload documents to a cloud-based application reducing the need for client's to share documents via physical or email based delivery. Financial professional's clients can reach out through the system and connect with their other trusted financial partners like bankers, insurance agents and attorneys. Once the client approves access to multiple trusted financial partners, the financial professional can have conversations with those professionals directly in StoneVault while maintaining client-privacy compliance. The client maintains ownership of all documents stored within the application and is responsible for granting access to documents to authorized financial partners. The system features include maintaining an audit history for each document showing when revisions are made and by whom as well as a commenting tool to be able to communicate back and forth.

CONTROL ENVIRONMENT

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal controls, providing discipline and structure. Aspects of StoneVault's control environment that affect the services provided and / or the system of controls are identified in this section.

Integrity and Ethical Values

The effectiveness of controls is greatly influenced by the level of integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are important elements of StoneVault's control environment, affecting the design, administration, and monitoring of other components. The communication and implementation of ethical behavior throughout the organization is designed to reduce the likelihood of personnel to engage in dishonest, illegal, or unethical acts.

StoneVault's Executive Team openly acknowledges, both internally and externally, that its service is predicated on sharing and managing the data of its users and requires an operational environment of the utmost ethical standards. StoneVault clearly communicates the expectation of honesty and integrity and written company policies outline the expectations placed upon all employees. The operational platforms implemented by StoneVault create an environment of transparency, in which tasks and responsibilities are managed publicly across web-based forums and communications are conducted via virtual chat-rooms and can easily be monitored and / or reviewed by management.

Executive Team

StoneVault's control consciousness is influenced significantly by its Executive Team. The Executive Team is comprised of the Chief Executive Office (CEO) and the Chief Technology Officer (CTO). Attributes include the team's experience and stature of its members, the extent of its involvement and scrutiny of activities, the appropriateness of its actions, the degree to which difficult questions are raised and pursued with management, and its interaction with clients.

Commitment to Competence

Management has established qualifications for each role within the company, including the required education, experience and skills sets needed to perform each role to company standards. Job descriptions for each role are specific to the department in which they are hired, but may be more generalized in respect to their actual function within their respective department. StoneVault operates with a "team-first" approach and has avoided the development of highly specific roles, instead creating departments consisting of members who share skill sets and the ability to cross-perform tasks within their respective department. This approach broadens the knowledge-base of our teams and ensures that tasks can be managed without interruption, especially in relation to customer service and support. Employee candidates, along with the established qualifications, will also possess the ability to work well in an open and team-oriented environment.

Management's Philosophy and Operating Style

StoneVault's management philosophy is built upon the mission to operate within a team-oriented environment. Management strives to maintain open and transparent communications regarding operations and performance in order to prevent the isolation of any single department and / or employee from overall company vision and objectives. Within each department, tasks and responsibilities are never assigned or delegated by a manager, but are instead are acquired by team members via ownership. The department objectives are clearly laid out for team members, and each member takes ownership of the specific tasks and responsibilities that they will complete during that pre-determined time period. This operating style improves morale amongst team members as they most often accept tasks and roles that they know they can achieve, increases productivity by allowing team members most comfortable with the

task to take ownership of it, and encourages self-accountability by allowing other team members to know exactly where each stands on their respective tasks and responsibilities. Management roles are more efficient and are able to focus more time on supporting their teams and removing road-blocks rather than delegation and accountability. StoneVault's team operating style also allows for more transparency and makes monitoring each department's progress towards their respective objectives less time consuming as all work and individual assignments are continually made public.

Organizational Structure

StoneVault's executive team has developed a relatively flat organizational structure. The CEO has taken on a seldom active role and primary functions of the business are managed by two executive management roles. StoneVault's individual departments are managed centrally by these two roles, respectively, with the operating structure within each department being flat. Without adding additional layers of department heads and team managers, StoneVault is able to operate efficiently within its means of resources without the processes and redundancy of typical hierarchical structures. The team-managed environment within each department, as outlined previously, eliminates the need for an abundance of management or supervisory roles, and allows for each department to consist of team members who can perform tasks within several different departments. StoneVault's flat departmental structure and lack of overly-specialized roles ensures that all team members can perform department task and roles preventing company processes and services from being interrupted.

There are four basic components to the StoneVault business structure: Operations, Technology, Marketing, and Support. Operations handles clerical office functions as well as Human Resources tasks. The Director of Operations reports to the CTO. The Information Technology team handles all programming, code and systems regardless of internal or external objectives. The CTO reports to the CEO. Marketing handles content and collateral creation used for customer acquisition and support. The Director of Marketing reports to the Director of Support. Support handles customer acquisition, sales, customer billing and all support needs of customers. The Director of Support reports to the CEO.

Human Resource Policies and Practices

StoneVault maintains a written human resources guide and employee hand book. This guide outlines employee expectations as well as defining what is and is not acceptable within the StoneVault workplace. StoneVault's policies and process documents are posted in a web-based forum that is public to all employees. Such documents include, but are not limited to, training discipline and termination policies. Changes to policies and procedures are clearly communicated to all employees and management ensures that such communications are received and understood by all employees.

RISK ASSESSMENT

StoneVault's risk assessment process is designed to identify and consider the implications of external and internal risk factors concurrent with establishing unit-wide objectives and plans. The likelihood of occurrence and potential monetary impact (or publicity risk) has been evaluated to enhance the reliability of management transaction processes. Risks are categorized as tolerable or requiring action, and include the following considerations:

- **Changes in the operating environment** – a change in regulations may necessitate a revision of existing processing. Revisions of existing processing may create the need for additional or revised controls;
- **New personnel** – new personnel who are responsible for overseeing the IT controls may increase the risk that controls will not operate effectively;
- **New or revamped information systems** – new functions added into the system that could affect user entities;
- **Rapid growth** – a rapid increase in the number of new customers may affect the operating effectiveness of certain controls;
- **New technology** – implementation of new application platforms / technology may operate so differently that it affects user entities;
- **New business models, products, or activities** – the diversion of resources to new activities from existing activities could affect certain controls; and
- **Expand foreign operations** – the use of personnel in foreign locations to maintain programs used by domestic user entities may have difficulty responding to changes in user requirements.

StoneVault's recognition of risks that could affect the organization's ability to provide reliable transaction processing for its user entities is generally implicit, rather than explicit. Management's involvement in the daily operations allows them to learn about risks related to transaction processing through direct personal involvement with employees and outside parties, thus reducing the need for formalized and structured risk assessment processes.

MONITORING

StoneVault's management conducts internal monitoring activities largely through the transparency of its departmental operation methods. As previously outlined, the task assignments, processes and progress are continually made public by each team member. When a problem or concern arises, it is immediately clear what may be causing the problem and / or where it originates. In this respect, management is required to spend less time tracing the problem and its origin and can immediately begin addressing and correcting the problem. This process of monitoring works as effectively in regards to written customer service concerns. Such written concerns are submitted in writing and immediately become public and easily tracked as the problem is circulated, handled and resolved internally.

Management is proactive concerning external concerns, especially those involving customers. The support team manages regular customer retention campaigns and conducts frequent satisfaction checks and surveys with all customers. Results from such campaigns and surveys are analyzed, along with written support request records, and account management policies and processes are improved and / or developed accordingly. Support team members are not authorized to deviate from company policies regarding StoneVault's provided services and customer service procedures. Management is focused on responding to customer complaints in a timely manner and there is a high level of inter-departmental communication about these events maintaining internal transparency. Customer complaints and other issues are handled via an internal ticketing system and by personal contact by management staff. Major customer-facing issues are reported to the operations executive for discussion and approval of action.

StoneVault's management performs monitoring activities in order to assess the quality of internal control over time and monitors activities throughout the year and takes corrective actions to address deviations from company policy and procedures. Management utilizes a risk-based approach to monitor business units and other auditable entities throughout the organization, ensuring that enterprise-wide risks are prioritized and addressed in order of significance.

INFORMATION AND COMMUNICATION SYSTEMS

Information System

StoneVault's system refers to the guidelines and activities for providing transaction processing and other services to user entities and includes the infrastructure and software that support StoneVault's Tax Return and Financial Statement Portal Services system.

The following describes the in-scope components supporting the Tax Return and Financial Statement Portal Services system:

System / Application	Description	Infrastructure
StoneVault.com	Provides financial document delivery and storage	Ubuntu / PostgreSQL

Information Technology Processes

StoneVault is responsible for maintaining and implementing information technology general computer controls related to computer processing supporting the Tax Return and Financial Statement Portal Services. These controls provide the basis for reliance on information / data from the systems used by user entities for financial reporting.

Develop and Manage Applications

Changes to the StoneVault application originate through customer requests or internal strategic development initiatives. Management meets on a monthly basis to discuss the strategic road map for the application and determine what changes should be worked on for the next period. Changes are documented in a ticketing system within the code repository and include the type of change, the effect on the system, and the plans for development. Change requests are reviewed and authorized by the CTO prior to the initiation of development activities.

Developers work in separated development environments that are not connected to production or testing environment. Once the developer(s) has completed work and performed validation testing of the change is completed it is moved to the testing phase where a separate or second developer, that didn't perform work, or in some cases the majority of the work on the change is requested to perform QA testing. If the change appears to function as intended, the CTO will approve the code for migration into production. The CTO is responsible for scheduling the migration of code into production. Two code repositories are utilized to track development changes and secure the source code. The first code repository is used for development and the second is used to maintain for production. Only the CTO has write access to the production code repository.

Backups

A backup system has been implemented to back up files and data required to support the StoneVault application related to the services being provided. Files uploaded to the StoneVault application are stored on AWS S3 system. Amazon performs real-time replication of this data to multiple locations.

Rackspace Cloud Server is used to host and backup servers used for the StoneVault application. StoneVault has configured the Rackspace Cloud Server to perform full daily and weekly backups of production data.

Systems Availability

Production systems reside on third party infrastructure. Management reviews the SOC 1 reports for these third party providers to ensure availability controls are in place.

StoneVault utilizes an enterprise monitoring tool to monitor application the IT infrastructure. The tool is configured to notify management in the event predefined thresholds are exceeded.

A ticketing system is utilized to monitor and manage customer issues and escalation procedures are in place to guide personnel in resolving issues. The CTO receives notification on all new tickets that are created and reviews them to ensure issues are resolved timely.

Information Security

The CTO is responsible for developing standards, procedures and processes, implementing standards, and overseeing logical security for StoneVault. The CTO has developed configuration standards for each type of hardware and associated system software. Access to systems is role based and determined on a requirement for each job role. Only the CTO can authorize and provide access to the production systems.

StoneVault administers security at the server level through restricting ports and through the OS level where individual IDs are passwords are required to gain access to the application. Users are assigned unique user IDs and passwords are required to gain access at the server, application and DB levels. StoneVault has enabled logging of access attempts and reviews these logs on an as needed basis.

Data Communications

The StoneVault internal network is protected from public internet traffic via stateful inspection firewalls that are configured to deny all traffic and only allow specific services to a specific destination. Access to administer the firewall is restricted to the CTO.

Encrypted communications are utilized to protect remote internet sessions to the application and internal network. Encryption is used to ensure the privacy and integrity of the data being passed over the public network.

Communication System

Management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities. This includes the ability to provide necessary training to the extent that personnel understand how their daily activities and roles relate to the overall support of services. StoneVault management believes that open communication throughout the organization ensures that deviations from standards are identified, reported and appropriately addressed.

CONTROL OBJECTIVES AND RELATED CONTROLS

Develop and Manage Applications

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that application and system software is developed that effectively supports application reporting requirements, and that system changes are authorized and appropriately tested before being moved to production.

Tracking Controls

1.1 Management systems are utilized to maintain and track development requests and activities.

Initiation and Authorization

1.2 Changes are authorized by the CTO and assigned to developers to be worked.

Development

1.3 QA testing is performed on changes by authorized personnel prior to migration to the production code repository.

Testing

1.4 Testing occurs in environments separated from development environments.

1.5 QA testing is performed on changes by authorized personnel prior to migration to the production code repository.

Approval

1.6 The CTO reviews and approves application development changes including but not limited to:

- Bug fixes
- System patching
- Upgrades
- Emergency changes

Access to Production

1.7 Access to migrate changes to the production environment is limited to the CTO.

Source Code Controls

1.8 Version control software is used to manage access to source code and facilitate version control for the development process. Access to source code is restricted to:

- CTO
- Developers (3)

1.9 Changes to source code result in the creation of a new version of the application code. If necessary, changes can be rolled back to prior versions of the application code.

Backups

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that relevant programs, files and datasets are appropriately backed up or electronically vaulted, rotated or vaulted offsite and recoverable in the event of a disaster.

Backup Controls

2.1 Job scheduler(s) are configured to automate the backup process for the following systems:

- Database
- Web application

2.2 The job scheduler(s) are configured to perform full backups on a daily basis.

2.3 Access to recall backup media is restricted to the CTO.

Restoration Testing

2.4 Quarterly restore tests are performed by the CTO to test the ability to restore data from backup media.

Systems Availability

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that production systems are designed and maintained to ensure system availability.

Monitoring

3.1 Management has configured a tool to monitor the production system for outages.

3.2 Management has configured the monitoring tool to provide email alerts to the CTO in the case of an outage.

Helpdesk

3.3 A help desk system is in place to track and monitor client issues and incidents.

3.4 The help desk system is configured to notify the CTO when new help desk tickets are created. The CTO reviews the status of open tickets to ensure issues are being resolved and communicated to clients in a timely basis.

Information Security

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that logical access to relevant applications, data and system resources is restricted to properly authorized individuals and programs.

General Controls

4.1 Internal IT access requests are approved by the CTO prior to granting access to system accounts.

4.2 Accounts assigned to terminated employees are deactivated, disabled, or assigned a new password upon notification of termination.

O/S Authentication Controls

4.3 Operating systems can only be directly reached through Secure Shell (SSH).

4.4 Unique user ID's and RSA keys are used to authenticate to the servers via SSH.

O/S Access Controls

4.5 Administrative access to production servers is limited to a single user account. Knowledge of the password is restricted to the CTO.

Logging Controls

4.6 The system is configured to log successful and unsuccessful login attempts.

4.7 Access logs are maintained for a minimum of 60 days and available for review.

Application Authentication Controls

4.8 Users must authenticate to the application using a unique user ID and a password.

4.9 Application configurations require passwords to be 8 characters in length.

Application Access Controls

4.10 Administrative access to the application is restricted to the:

- CTO
- Developer
- President

Database Authentication Controls

4.11 Authentication to the production database is completed through the O/S layer security.

Database Access Controls

4.12 Administrative access to the production database server is restricted to two user IDs and passwords. Knowledge of the passwords is restricted to the CTO.

Data Communications

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and the service organization.

Firewall Administration Controls

5.1 Stateful inspections of firewalls are in place and configured to filter unauthorized inbound and network traffic from the Internet.

5.2 The firewalls are configured to deny traffic and allow only specific services to specific destinations.

5.3 Access to request changes to the firewall rulesets is restricted to the CTO.

5.4 External traffic must pass through a firewall to communicate with production application servers. No direct conversations originating from the Internet pass directly through to the internal network.

Remote Access Controls

5.5 Customer web sessions are encrypted using HTTPS protocol.

5.6 Encrypted communications using SSH are utilized by employees to obtain remote access to the StoneVault servers to ensure the privacy and integrity of the data passing over the public network.

USER ENTITY CONTROL CONSIDERATIONS

Transaction processing support for user entities as performed by StoneVault and the control activities at StoneVault cover only a portion of the overall internal control for each user entity. It is not feasible for the control objectives related to the Tax Return and Financial Statement Portal Services system to be solely achieved by StoneVault. StoneVault's controls over the systems and infrastructure supporting the Tax Return and Financial Statement Portal Services system were designed with the assumption that certain controls would be in place and in operation at user entities. User entity internal controls must be evaluated, taking into consideration StoneVault's controls and their own internal controls. StoneVault does not represent any responsibility or provide any assurance in regards to the services that it provides in relation to any such internal control or regulatory requirements for which the client must assess or comply.

This section describes some of the control considerations for user entities, or "complementary user entity controls", which should be in operation at user entities to complement the controls at the service organization. User auditors should determine whether user entities have established controls to ensure that control objectives within this report are met. The "complementary user entity controls" presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities. There may be additional control objectives and related controls that would be appropriate for the processing of user transactions that are not identified in this report.

Control Considerations for User Entities

1. User entities are responsible for informing StoneVault of any regulatory issues that may affect the services provided by StoneVault to the user entity.
2. User entities are responsible for understanding and complying with their contractual obligations to StoneVault.
3. User entities are responsible for notifying StoneVault, in a timely manner, when changes are made to technical, billing or administrative contact information.
4. User entities are responsible for developing their own disaster recovery and business continuity plans that address their inability to access or utilize StoneVault's services.
5. User entities are responsible for reporting systems availability issues in a timely manner.
6. User entities are responsible for ensuring the confidentiality of any user IDs and passwords assigned to them for use with StoneVault's systems.
7. User entities are responsible for administrating their user's access and enforcing password policies.
8. User entities are responsible for notifying StoneVault of any actual or suspected information security breaches or fraud, including compromised user accounts in a timely manner.
9. User entities are responsible for determining whether StoneVault's security infrastructure is appropriate for its needs and for notifying the service organization of any requested modifications.
10. User entities are responsible for developing policies and procedures to protect their systems from unauthorized or unintentional use, modification, addition or deletion.