## Proformex System Description

## Purpose and Scope of Report

This report describes the system and control structure of Proformex as it relates to Proformex’s Software Platform. It is intended to assist user organizations and their independent auditors in determining the adequacy of the internal controls that are outsourced to Proformex and are relevant to their internal control structures as they relate to security and confidentiality risks.

This description is intended to focus on the internal control structure of Proformex that is relevant to only users of Proformex’s Software Platform and does not encompass all aspects of the services provided or procedures followed by Proformex.

# System Description

## Company Overview and Services Provided

Proformex was founded to address the unique needs of life insurance owners, trustees, agents and beneficiaries. The founders set out to develop a powerful software tool for purposes of integrating, adding, managing, and monitoring data and information related to life insurance. The result is Proformex, a software platform which helps users understand and monitor the asset of life insurance.

Proformex delivers a product which assists life insurance agents and brokers in the monitoring of life insurance policies and annuities, allows them to access an extensive data base of all their life insurance policies- regardless of carrier, and provides an archive for storage of important life insurance and related documents. Life insurance owners, trustees and beneficiaries also use Proformex to make sure that their life insurance asset is periodically monitored and managed so they are aware of changes in variables such as cash value, death benefit, premiums required, lapse age or financial rating of the insurance carrier.

## 

## Infrastructure

The infrastructure supporting Proformex’s Software Platform is a multi-tier web application built on Rackspace’s cloud infrastructure as a service and with managed firewall services to separate their web application from other cloud environments on the Rackspace cloud services. Proformex has a replicated environment in the U.S.A. based cloud infrastructure of Rackspace. The production application is supported by the development, test, quality assurance and demo environments.

## Software

The following provides a summary of systems used to deliver Proformex’s Software Platform:

Proformex**:**

* Active Directory
* File servers
* Microsoft windows
* Microsoft office conversion tools
* Microsoft SQL server
* Linux

## People

People involved in the operation and use of the system are:

Proformex**:**

* The CEO/President, who is responsible for leading the Company, performing sales activities, and managing the day-to-day operations of Proformex.
* The CTO, who is responsible for oversight of all IT related hardware, software, configuration, and security. This position is also responsible for the coordination of policy and system features/functionality along with the Director of Operations and CEO.
* The Data Security Officer who is responsible for oversight of all client data in the system, ensuring the Data Protection policies are being followed and for reporting to the Board of Directors on Data Security.
* The Data Manager, who is responsible for any manual data entry into the system.
* The Client Manager, who is responsible for Client training and passcodes distribution and resets.

## Procedures

Executive and Operations Management personnel maintain documented automated and manual standard operating procedures involved in the operation of Proformex’s Software Platform that include:

* Responsibilities and oversight
* Physical and environmental security
* Personnel security
* Device build and configuration
* Application development
* Asset management
* Access control
* Network security
* Communications management
* Operations management
* Information security incident management
* Business continuity management
* Compliance
* Third party security

Control activities have been placed into operation to help ensure that actions are carried out properly and efficiently. Control procedures serve as mechanisms for managing the achievement of control activities, and are a part of the process by which Proformex strives to achieve its business objectives. Proformex has applied a risk management approach to the Company in order to select and develop control procedures. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed, and improved when necessary to meet the applicable trust services criteria and the overall objective of the Company.

Proformex’s Software Platform encrypts customer sessions through the use of a valid TLS certificate; access to customer portals is restricted using a login/password combination and the password is configurable by each client. Unauthorized access to system resources is restricted through the use of firewalls, network access controls, and performance of external vulnerability assessments at least annually to help identify potential weaknesses.

Incidents are formally logged, tracked, and resolved using Rackspace monitoring services. Customer-found bugs and other issues are handled by having the Client contact their Client Support Manager. Major customer-facing issues are reported to the CTO and/or CEO for discussion and further approval of responsive action.

Access to Proformex’s Software Platform production application and servers is restricted to appropriate IT personnel; access additions or modifications are required to be approved by IT Management prior to provisioning. Terminated employees are removed from all key servers and services upon notification.

PROFORMEX utilizes an automated backup system to schedule and perform daily and weekly backup activities. Backups are scheduled, monitored and have their integrity validated through daily automated validity checks that notify Management. Backup media is electronically stored in the redundant failover facility to ensure availability of offsite backup data.

PROFORMEX maintains their productions system through a continual evaluation of system development activities that includes a series of predefined software development procedures including new development, ongoing modification, and application support activities and bug management. From initial change requests to the deployment of changes, the entire Software Development Life Cycle (SDLC) process is documented in PROFORMEX’s JIRA change management system that links to code under development in the SVN. The SDLC requires formal business requirements, impact assessments, testing and authorization of deployment procedures.

PROFORMEX’s information security is governed by their corporate information security policies and procedures that are documented and communicated to personnel on a regular basis. Their policies are based on only permitting access as necessary to enable personnel to perform job responsibilities. The CTO is responsible for administrating and implementing user and system level security and for monitoring security to ensure policies are being adhered to.

The data flow of PROFORMEX’s networks is restricted to their wide area network that consists of their primary hosted production systems located within Rackspace cloud computing environments. Remote access and administration is restricted via VPN connections and restricted to internal personnel of PROFORMEX. Customers connect to their production site via SSL Web connection.

## Data

Access to customer data in Proformex’s Software Platform is restricted to appropriate IT personnel, approved customer personnel, and their clients. Although data from multiple customers is kept on the same server, each database has separate connections to the application. Proformex has a written Data Protection Policy which is reviewed annually.

## System Boundaries

System boundaries pertaining to collection, use, retention, disclosure, and disposal or anonymization or personalization of data, are governed by contract provisions in particular service engagements. Data is not utilized or disclosed to third parties outside of the scope allowed in such contracts and agreements.

## Subservice Organizations

Rackspace is the subservice organization utilized to assist in the delivery of the Proformex’s Software Platform:

Proformex uses Rackspace for data center services. Rackspace is responsible for the uptime and management of the infrastructure that supports the delivery of internet and the environmental conditions that provide power and cooling to their devices. This subservice organization is also responsible for providing physical security controls and all administration of their hardware equipment, and for reporting any physical security incidents.

The applicable trust services criteria that are intended to be met by controls at the subservice organizations, alone or in combination with controls at Proformex, and the types of control expected to be implemented at the subservice organizations to meet those criteria are described in the “applicable trust services criteria” intended to be met by Proformex section below:

|  |  |
| --- | --- |
| **Control Activity Expected to be Implemented by Subservice Organizations** | **Applicable Trust Services Criteria** |
| Subservice organizations are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | CC5.1, CC5.2, CC5.3, CC5.4, CC5.5 |
| Subservice organizations are responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment. | CC3.1, A1.1 |
| Subservice organizations are responsible for maintaining segregation of Proformex’s Virtual Machine (“VM”) environments. | CC5.6 |
| Subservice organizations are responsible for ensuring the availability of hardware and software services. | A1.1, A1.2, A1.3 |
| Subservice organizations are responsible for implementing changes that are requested from Proformex. | CC3.1 |

## Control Environment

The control environment is determined by the control consciousness of an organization, which sets the tone of an organization and the way personnel conduct their activities, influencing how they carry out their control functions.  This is the foundation for all other components of internal control, providing discipline and structure for the business operations.

The control environment at PROFORMEX begins with Management’s philosophy and operating style as well as the priorities and direction provided by the Proformex Board of Directors. PROFORMEX’s entire organization is dedicated to delivering the highest level of customer service. The Company has created a corporate culture that supports this mission. PROFORMEX’s stated objective for the control environment portion of the examination is that control activities provide reasonable assurance that discipline and structure are an integral part of the Company and influence the control consciousness of personnel.

### Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people, who create, administer and monitor them. Integrity and ethical values are essential elements of the control environment, affecting the design, administration and monitoring of other components. Integrity and ethical behavior are the products of the entity’s ethical and behavioral standards, how they are communicated and how they are reinforced in practice. They include Management’s actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct and by leadership’s example.

PROFORMEX has implemented, maintains and regularly communicates a code of conduct and other policies regarding acceptable business practices, guidance on conflicts of interest and expected standards of ethical and moral behavior. PROFORMEX’s Management conducts business dealings with employees, suppliers, customers, investors, creditors, competitors and auditors on a high ethical plane and insists others have similar business practices.

### Commitment to Competence

Competence is the knowledge and skills necessary to accomplish tasks that define the individual’s job. Commitment to competence includes Management’s consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.

PROFORMEX maintains job descriptions that contain requirements of knowledge and skills needed to adequately perform each job. PROFORMEX reinforces these requirements by providing hands-on training throughout the initial period of employment and continual hands-on training for new business processes or job requirements.

### Management’s Philosophy and Operating Style

Management’s philosophy and operating style encompass a broad range of characteristics. Such characteristics may include the following: Management’s approach to taking and monitoring business risk; Management’s attitude and actions toward financial reporting (conservative or aggressive selection of alternative accounting principles and which accounting estimates are developed); and Management’s attitudes toward information processing and accounting functions and personnel. PROFORMEX’s Management takes a relatively conservative approach to information processing and risk associated with new business ventures.

### Organizational Structure

An entity’s organizational structure provides the framework for how entity-wide objectives are planned, executed, controlled and monitored. A relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. An entity develops an organizational structure contingent, in part, on its size and nature of activities.

The responsibilities of key positions within PROFORMEX are clearly defined in documented job descriptions and communicated. Individuals that hold key positions are experienced and knowledgeable. PROFORMEX’s organizational structure supports communication of information both up to leadership as well as down to support staff. PROFORMEX’s organizational structure is comprised of three primary business units and several groups that work together when delivering their SaaS. The three business units consist of:

* The Management team or Proformex Board of Directors, is responsible for the oversight and monitoring of the Company’s strategic direction and for making final decisions that are pushed down to the leadership teams and ultimately to team members.
* Leadership team, which is responsible for the overall management, communications, direction and implementation of the Management team’s strategic direction. The leadership team is directly responsible for production and manages the quality of services.
* Team members, who are responsible for executing on Company tasks and managing the day-to-day service offerings of their respective departments.

### Assignment of Authority and Responsibility

Assignment of authority and responsibility includes delegation of authority to address organizational goals and objectives, operating functions and regulatory requirements, including responsibility for information systems and authorizations for changes. Policies are established relating to business practices, knowledge and experience of key personnel and the appropriate number of people to carry out duties. In addition, Management’s policies and communications are directed at ensuring that personnel understand the entity’s objectives, know how their individual actions interrelate and contribute to those objectives and recognize how and for what they will be held accountable.

As mentioned above, PROFORMEX has well defined job descriptions and clear communication channels to disseminate information within the Company; this enables PROFORMEX to react to market and regulation changes and to meet its goals and objectives. PROFORMEX is appropriately staffed to support its operations, particularly with respect to critical areas such as software development and information technology system support.

### Human Resource Policies and Practices

Human resource policies and practices relate to hiring, orientation, training, evaluating, counseling, promoting, compensating and remedial action. They also include adequacy of employee background checks, particularly with regard to prior actions or activities considered to be unacceptable by the entity.

Standards for hiring the most qualified individuals with emphasis on educational background, prior work experience, past accomplishments and evidence of integrity and ethical behavior demonstrate Proformex’s commitment to competent and trustworthy people. Training policies created by Proformex communicate personnel roles and responsibilities and include practices such as regular training programs to illustrate expected level of performance, information technology practices and employee behavior. Personnel career growth and the reward of meeting expectations are driven by periodic performance appraisals and demonstrate Proformex’s commitment to advancing qualified personnel to higher levels of responsibility. Personnel who work for Proformex are required to read and acknowledge the Company’s internal policies and confidentiality requirements as well as the confidentiality of customer managed information.

## Risk Assessment

Proformex’s Leadership Team performs periodic risk assessments, which allows Proformex’s Board of Directors to identify risks in its areas of responsibility and to implement appropriate measures to address those risks. Proformex reevaluates the risk assessment at least annually to both update the previous results and to identify any new potential areas of concern.

The risk assessment process consists of the following phases:

* Identifying – The identification phase includes listing out risks (including threats and vulnerabilities) that exist in the environment. This phase provides a basis for all other risk management activities.
* Assessing – The assessment phase considers the potential impact(s) of identified risks to the service organization and their likelihood of occurrence.
* Mitigating – The mitigation phase includes putting controls, processes, and other physical and virtual safeguards in place to prevent and detect both identified and assessed risks.
* Reporting – The reporting phase results in risk reports provided to managers with the necessary data to make effective business decisions and to comply with internal policies and any applicable regulations.
* Monitoring – The monitoring phase includes the performance of monitoring activities by Proformex’s Management team to evaluate whether the processes, initiatives, functions and/or activities are mitigating the risk as designed.

## In-Scope Trust Service Principles

The table below provides TSP within the scope of this report. The controls designed and implemented to meet the applicable TSP criteria have been included in section 4.

|  |  |
| --- | --- |
| **Trust Services Principles** | **Definition** |
| Security | The system is protected against unauthorized access (both physical and logical). |
| Availability | The system is available for operation and use as committed or agreed. |

### Security

The security principle refers to the protection of the system from unauthorized access, both logical and physical. Limiting access to the system helps prevent potential abuse of the system, theft of resources, misuse of software, and improper access to, or the use, alteration, destruction, or disclosure of information. Key elements for the protection of the system include permitting authorized access based on relevant needs and preventing unauthorized access to the system in all other instances.

### Availability

The availability principle refers to the accessibility to the system, products, or services as advertised or committed by contract, service level, or other agreements. It should be noted that this principle does not, in and of itself, set a minimum acceptable performance level for system availability. The minimum performance level is established through commitments that are mutually agreed to in writing between two parties.

Although there is a connection between system availability, system functionality, and system usability, the availability principle does not address system functionality – the specific functions a system performs – and system usability – the ability of users to apply system functions to specific tasks or problems. It does, however, address system availability, which relates to whether the system is accessible for processing, monitoring, and maintenance.

## Trust Service Principles and Related Control Activities

### Integration with Risk Assessment

Along with assessing risks, Proformex’s Management has identified and put into effect the necessary actions to address those risks. In order to address these risks, control activities have been placed into operation to help ensure that the actions are carried out in a competent and efficient manner. Control activities serve as various mechanisms for managing the achievement of the security, availability and confidentiality principles and applicable criteria.

### Selection and Development of Control Activities

The applicable trust criteria and related control activities are included in the testing matrices, within section 4 of this report, to eliminate the redundancy that would result from listing the items in this section as well. Although the control activities are included in the testing matrices set forth below in section 4, they are, nevertheless, an integral part of Proformex’s description of its Software Platform. Any applicable trust services criteria that are not addressed by control activities at Proformex are also described within the testing matrices.

The description of the service auditor’s tests of operating effectiveness and the corresponding results are also presented in the testing matrices, adjacent to the service organization’s control procedures. The description and results of such tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

## Information and Communication

### Information Systems

A custom built multi-tier architecture is in place to support PROFORMEX’s application services. The PROFORMEX production system is a complex environment with several operating systems, databases and information systems. The service-oriented architecture reduces the complex relations between systems and solves data consistency problems among databases. The distributed architecture of PROFORMEX’s production system provides a stable environment for reasonable system performance. This is a high availability application, with built in redundancies, that is customized for user functionality and special security features, including role access permissions.

The SaaS system is managed by PROFORMEX; however the infrastructure that is used to deploy the production systems is maintained at a third party cloud computing environment managed by Rackspace. The managed third party data center provides the network, routers, firewalls, operating systems and databases used to deploy their SaaS solutions. The SaaS system is deployed in separate and redundant data centers located in geographically different areas in the United States.

PROFORMEX provides application development, system administration and monitoring of their SaaS. Proformex’s suite of software services is designed to provide and facilitate monitoring and management of Client’s life insurance and annuity portfolio. PROFORMEX provides the software and administration of the system to ensure that the system processing operates as designed. Clients that utilize PROFORMEX’s SaaS solutions are responsible for any manual data entry and/or document upload and determination of any custom configuration settings.

The SaaS solutions are deployed via the various business units within PROFORMEX. The day-to- day direct interactions with customers are delivered through PROFORMEX’s Product Management Team who is responsible for the end user testing and help desk support to clients. The Product Management Team members work directly with clients on the custom configuration setting and report design; the Product Development Team is responsible for determining the feasibility and managing the development of various Client requirements. The Infrastructure and Security Departments are responsible for maintaining the networks, operating systems and databases for their internally managed and hosted cloud computing environments.

### Communication

Throughout the Company, Proformex conducts daily, weekly, monthly, quarterly and annual meetings to identify and address significant issues affecting the Company’s operations. Defined agendas, meeting minutes and a corporate information system are established vehicles used for addressing and monitoring activities, accomplishments and issues. As annual business development plans are established, meetings are held throughout the Company to communicate defined goals and report results achieved. Monthly Management meetings provide the vehicle for Management to communicate and respond to operational tasks and issues. At all corporate levels, the Company has established communication channels to promote and distribute information up and down the defined Management structure.

## Monitoring

An effective monitoring foundation is dependent upon establishing an effective “tone at the top” of the Company and placing a high priority on maintaining effective internal controls. This requires that the top members of the Leadership Team, including the Data Security Officer are involved in the evaluation process. Monitoring internal controls is dependent on the selection and utilization of evaluators that have a solid baseline understanding of internal controls. They also need to have suitable capabilities, resources and authority to conduct a meaningful assessment of internal controls.

Proformex’s monitoring of internal controls is performed through application of both periodic and separate evaluations. These evaluations ascertain whether the components of their internal controls over services provided continue to function as designed and intended. In addition, these evaluations facilitate identification of internal control deficiencies and evaluators communicate findings to appropriate officials responsible for taking corrective action. Proformex has continuous internal reporting, monitoring and evaluation procedures in place to identify deviations from internal controls to effectively report these deficiencies to appropriate departments.

Monitoring is a process of assessing risks linked to achieving operational objectives. This requires establishing a monitoring foundation consisting of procedures for evaluating risks to Proformex’s clients. Monitoring activities include assessment of controls and reporting the results of the assessment together with any required corrective action steps.

Proformex’s monitoring procedures include:

* Analysis of, and appropriate follow-up on, operating reports or metrics that might identify anomalies indicative of a control failure
* Supervisory reviews of controls, such as reconciliation reviews as a normal part of processing
* Self-assessments of Management regarding the tone they set in the Company and the effectiveness of their oversight functions
* Inquiries of internal and external auditors by Management

## Additional Disclosures

## User Entity Controls

The control activities performed by Proformex cover only a portion of the overall internal control structure of Proformex’s user organizations. Therefore, each customer’s internal control structure must be evaluated in conjunction with Proformex’s control policies and procedures described in this report. Proformex’s controls over its Software Platform were designed with the understanding that certain user organization controls were in place and operating effectively.

| **Complementary User Entity Controls** | **Related Applicable Trust Principle** | **Related Applicable Trust Criteria** |
| --- | --- | --- |
| User organizations are responsible for management of user access requests through the use of the administrative user account for their entity to ensure appropriate individuals have access to their instance of the Proformex system. | Security | 3.2 |
| User organizations are responsible for ensuring that user IDs and passwords are assigned only to authorized individuals and that the roles assigned to the user account are appropriate. | Security | 3.2 |
| User organizations are responsible for ensuring the confidentiality of any user accounts and passwords assigned to them for use with Proformex’s Software Platform. | Security | 3.2 |
| User organizations are responsible for the setup, configuration, and loading of documentation into their instance of Proformex’s Software Platform, unless assistance of Proformex is requested. | Security | 3.2 |
| User entities are responsible for notifying Proformex of any approved contact modifications. | Security | 3.3 |
| User entities are responsible for defining the communications method utilized to connect to their systems (e.g., direct connections, over public networks, etc.). | Security | 3.6 |
| User organizations are responsible for immediately notifying Proformex of any actual or suspected information security breaches, including compromised user accounts. | Security | 3.7 |
| User organizations are responsible for performance of appropriate change management procedures as they relate to Proformex’s Software Platform upon deployment. | Security | 3.12 – 3.14 |
|  |  |  |