smartsimple

SmartSimple Software Inc.

SOC 3 Report

Report on SmartSimple Software Inc.’s Description of its System and on the Suitability of the Design and Operating Effectiveness of its Controls Relevant for Security, Availability and Processing Integrity (SOC 3) throughout the Period May 1, 2024, to April 30, 2025

Table of contents

This report is intended solely for use by the management of SmartSimple Software Inc., user entities, prospective user entities, and the independent auditors and practitioners providing services to such entities, and regulators. This report is not intended to be, and should not be, used by anyone other than those specified.

Deloitte.

Section 1 – Independent Service Auditors’ Report

To: SmartSimple Software Inc. (“the company,” “SmartSimple”).

Scope

We have been engaged to report on SmartSimple Software Inc.’s (SmartSimple) accompanying description of its application development, application management, operations support and monitoring services (application services) system titled “SmartSimple’s Description of its System” (description) throughout the period May 1, 2024, to April 30, 2025 to provide reasonable assurance that SmartSimple’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and processing integrity (“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*).

SmartSimple uses Amazon Web Services (AWS) (sub-service organization) to perform cloud computing services and Microsoft Corporation (Microsoft) for authentication and rights management services. The accompanying statement titled “Management’s Statement on System of Internal Control" and the Description of the Boundaries of the SmartSimple System indicate that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at SmartSimple, to achieve SmartSimple’s service commitments and system requirements based on the applicable trust services criteria. The Description of the Boundaries presents the complementary subservice organization controls assumed in the design of SmartSimple’s controls. The description does not disclose the actual controls at the subservice organization. Our engagement did not include such complementary subservice organization controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

The accompanying statement titled “Management’s Statement on System of Internal Control" and the Description of the Boundaries of the SmartSimple System indicate that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at SmartSimple, to achieve SmartSimple Software Inc’s service commitments and system requirements based on the applicable trust services criteria. The Description of the Boundaries of the SmartSimple System presents the complementary user entity controls assumed in the design of SmartSimple’s controls. Our engagement did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

This report is intended solely for use by the management of SmartSimple Software Inc., user entities, prospective user entities, and the independent auditors and practitioners providing services to such entities, and regulators. This report is not intended to be, and should not be, used by anyone other than those specified.

Service Organization's Responsibilities

SmartSimple is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that SmartSimple's service commitments and system requirements were achieved. SmartSimple has also provided the accompanying statement "Management's Statement on System of Internal Control " ("statement") about the effectiveness of controls stated therein. When preparing its statement, of SmartSimple Software Inc. is responsible for selecting and identifying in its statement, the applicable trust service criteria and for having a reasonable basis for its statement by performing an assessment of the effectiveness of the controls within the system.

Our Independence and Quality Management

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies Canadian Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements*, and accordingly maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service Auditors' Responsibilities

Our responsibility, under this engagement, is to express an opinion, based on the evidence we have obtained, on whether management's statement that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Our engagement was conducted in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information*, set out in the CPA Canada Handbook – Assurance. This standard requires that we plan and perform our engagement to obtain reasonable assurance about whether management's statement is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our reasonable assurance engagement included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that controls were not effective to achieve SmartSimple's service commitments and system requirements based on the applicable trust services criteria.

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve SmartSimple's service commitments and system requirements based on the applicable trust services criteria
- Performing such other procedures as we considered necessary in the circumstances.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become ineffective because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

Opinion

In our opinion, management's statement that the controls within SmartSimple Software Inc.'s system were effective throughout the period May 1, 2024, to April 30, 2025, if complementary user entity controls assumed in the design of SmartSimple Software Inc.'s controls operated effectively, to provide reasonable assurance that SmartSimple Software Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Deloitte LLP

Chartered Professional Accountants
July 30, 2025
Toronto, Canada

This report is intended solely for use by the management of SmartSimple Software Inc., user entities, prospective user entities, and the independent auditors and practitioners providing services to such entities, and regulators. This report is not intended to be, and should not be, used by anyone other than those specified.

Section 2 – Management's Statement on System of Internal Control

We have prepared the accompanying description of SmartSimple Software Inc.'s (the "Service organization" or "SmartSimple") application development, application management, operations support and monitoring services (application services) system included in Section 3, "SmartSimple's Description of its System" throughout the period May 1, 2024, to April 30, 2025, to provide reasonable assurance that SmartSimple's service commitments and system requirements relevant to security, availability, and processing integrity were achieved based on the trust services criteria relevant to security, availability, and processing integrity (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). Our description of the boundaries of the system is presented in Section 3 and identifies the aspects of the system covered by our statement.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period May 1, 2024, to April 30, 2025, to provide reasonable assurance that SmartSimple Software Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria. SmartSimple Software Inc.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section 3.

This management statement and the Description of the Boundaries of the SmartSimple System indicate that complementary user entity controls and complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at SmartSimple, to achieve SmartSimple Software Inc.'s service commitments and system requirements based on the applicable trust services criteria. The Description of the Boundaries of the SmartSimple System presents the complementary user entity controls and complementary subservice organization controls assumed in the design of SmartSimple Software Inc.'s controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We confirm that the controls within the system were effective throughout the period May 1, 2024, to April 30, 2025, to provide reasonable assurance that SmartSimple Software Inc.’s service commitments and system requirements were achieved based on the applicable trust services criteria.

SmartSimple Software Inc.

Section 3 – SmartSimple's Description of the Boundaries of its System

Organization Background and Services

SmartSimple Software Inc., or the "Company", was founded in 2002, and headquartered in Ontario, Canada. The company provides cloud-based and collaboration solutions supporting grantmaking foundations, research institutions, higher education, and government in driving efficiency and impact. SmartSimple Software Inc. announced its merger with Foundant Technologies on August 13, 2024, which is another leading provider of grant and philanthropic management software.

SmartSimple's cloud-based process automation platform was developed in 2003 and since then has been continuously enhanced. It is used by clients in multiple vertical markets to:

- Create an engagement framework between an organization and its multiple stakeholder communities.
- Automate business processes around these types of engagements.
- Gather and manage organization specific information related to these engagements.
- Report on outcomes from these engagements.

Each engagement framework is specific to the various vertical markets in which SmartSimple currently operates: philanthropy (government, corporate, community and family based), research grants and related research project management and medical case management. The system content and process models are fully configurable by the client without the need for programming.

Description of Services

SmartSimple and technical partners work with clients to provide business process automation, fast prototyping, system configuration, custom training, and ongoing support.

All clients operate on the same version of the platform. The platform is configured to reflect a client's organization-specific information, specific process needs, and outcomes. The platform can be configured for different use cases such as:

- **Corporate Giving Management**: An enterprise solution to support corporate giving programs and philanthropic impact.

- **Employee Giving Management**: A solution that supports corporate volunteering, donation, and matching programs.
- **Government Grants Management**: A solution to support US municipal and state agencies with grants management that enables transparency and visibility through the state granting processes by tracking spending from funding source to grant.
- **Arts Grants Management**: A solution for arts and culture funding agencies to collect applications, manage reviews, communicate, and report.
- **Research Grants Management**: A solution that **enables** research foundations, institutions, and government agencies funding research, to manage research programs and research grants from a single system.
- **Committee Management:** A configuration of the SmartSimple platform that supports the grant review process for funders, helping to improve the effectiveness of review meetings. The solution supports reviewer assignments, conflict of interest checks, and live meeting results.
- **Community Foundation Grants Management**: A configuration of the SmartSimple platform that accommodates the needs of community foundation programs through enabling collaboration, engagement, and reporting.
- **Private/Family Grants Management**: A configuration of the SmartSimple platform designed to manage the grants lifecycle, from application intake to post-award monitoring.
- **Medical Case Management**: A configuration of the SmartSimple platform that provides insurers and health care providers, employment services providers and structured settlement providers with a solution to securely share "need to know information" while following their existing business models and processes.
- **Interest on Lawyer Trust Accounts (IOLTA) 360°**: A configuration of the SmartSimple platform that helps IOLTA organizations go paperless, and automates manual tasks involved in the collection and fund allocation process through a centralized, online system.

Principal Service Commitments and System Requirements

SmartSimple designs its processes and procedures to meet its objectives for its services relevant to security, availability, and processing integrity. Those objectives are based on the service commitments that SmartSimple makes to user entities, the laws and regulations that govern the provision of services, and the operational and compliance requirements that SmartSimple has established for the services. SmartSimple communicates service commitments to user entities in the form of Service Level Agreements (SLAs), customer agreements and through the description of the service offerings provided online at the SmartSimple website.

Category	Service Commitment	System Requirements
Security	Systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability and integrity of information or systems.	• Logical access to systems is restricted to authorized personnel. • Systems are configured to identify and authenticate users to validate their entitlement to the systems. • Changes (including emergency/non-routine and configuration) to IT resources are logged, authorized, tested, and approved.
Availability	SmartSimple, within its control, makes commercially reasonable efforts to ensure that the platform is available for operation and use to meet contractual commitments.	• SmartSimple uses a hosting provider that provides on-demand computing capacity, and geographic redundancy. • Production data is backed up frequently in a cloud environment. • Business continuity plans are established, tested, and updated, at least annually.
Processing Integrity	System processing is complete, valid, accurate, timely, and authorized.	• Data integrity is maintained through all phases including transmission, storage, and processing.

SmartSimple is committed to designing and operating a system of internal control procedures that is appropriate to the needs of the business and to ensure client data is securely processed and professionally managed. Management has established internal control policies and procedures according to the key control objectives relevant to the service provided. It is management's responsibility to ensure the designed control procedures operate effectively on a continuous basis.

In order to provide its clients and their auditors with information regarding the management and control procedures in place at SmartSimple, SmartSimple has documented the internal controls it has implemented. The control procedures are organized according to a series of internal control objectives for each aspect of SmartSimple's services and for the specific computer environments included in the scope of this audit. For each internal control objective, the design, implementation, and operating effectiveness of the control procedures to achieve the objective have been audited by Deloitte.

Components of the System used to Provide the Service

Infrastructure and Software

SmartSimple's platform is hosted on the infrastructure provided by Amazon Web Services (AWS) data centers, utilizing AWS's Infrastructure-as-a-Service (IaaS) offering. By leveraging AWS, SmartSimple benefits from a highly scalable, secure, and reliable cloud environment without the need to manage physical hardware directly.

AWS is responsible for the provisioning and maintenance of the underlying physical servers, networking, storage, and other foundational IT resources. This includes ensuring the security, availability, and operational integrity of the data centers where the SmartSimple platform resides.

The operating system and database environments that support SmartSimple are also managed within the AWS ecosystem. This means that tasks such as patching, updates, backups, and system monitoring are handled using AWS tools and best practices, contributing to high system uptime and data resilience.

By relying on AWS's global infrastructure, SmartSimple can offer clients enhanced performance, disaster recovery capabilities, and compliance with various industry standards and certifications. This partnership allows SmartSimple to focus on delivering application-level features and support, while AWS ensures the robust operation, maintenance, and security of the underlying infrastructure.

People

SmartSimple's team is composed of a diverse group of professionals with expertise in software development, cloud technology, client support, implementation, project management, and business analysis. Their collective experience enables SmartSimple to deliver robust, configurable solutions tailored to the unique needs of organizations across various industries, including grants management, research funding, and corporate social responsibility.

SmartSimple places a strong emphasis on collaboration, both internally and with clients. The company fosters a culture of continuous learning and professional development, encouraging employees to stay abreast of the latest technological advancements and industry best practices. This commitment ensures that the team can provide informed guidance and innovative solutions to clients.

Client success managers, technical support specialists, and solution consultants work closely with clients throughout the entire lifecycle of their engagement with SmartSimple—from initial onboarding and system configuration to ongoing support and optimization. This hands-on approach helps build lasting relationships and ensures that clients receive responsive, personalized service.

Procedures

Formal IT policies and procedures have been established to govern and document all significant operational processes within the organization. These policies cover critical areas such as change management, service incident response, user access controls, network configuration and maintenance, as well as data backup procedures. The following are the key policies that have been implemented:

- Human resources security policy
- Access control policy
- Development security policy and procedures
- Change management policy
- Cryptography policy
- Physical and environmental security policy
- Operations security policy
- Communications security policy
- System acquisition, development and maintenance policy
- Vendor Management Policy
- Supplier relationship policy
- Incident management policy
- Business continuity and Disaster Recovery policy
- Infrastructure security policy and procedures
- Information classification and handling policy.
- Information security policy
- Data protection policy
- Backup policy
- Information security risk management policy and procedures
- Clear desk policy

Data

SmartSimple hosts separate instances of its platform each configured for the specific client that licenses the service. Clients are provided access to the environment in which their instance of the platform resides and SmartSimple provides configuration support, operations support, storage, backup and recovery.

SmartSimple deploys its services to its clients using three different models:

Public Cloud Hosting: Client instance is hosted along with other SmartSimple clients in a shared multi-tenant infrastructure.

- Data within client instances are separated logically through a proprietary software abstraction layer built into the platform.
- The geographical hosting location is based on the client's selection of jurisdiction.

Private Cloud: Client instance is hosted alone in a dedicated single-tenant infrastructure.

- The geographical hosting location is based on the client's selection of jurisdiction.

Enterprise Installation (on-premises installation): Client instance is hosted alone in a dedicated single-tenant infrastructure provisioned and managed by the client.

- The SmartSimple platform is installed on infrastructure that is hosted, managed, and owned by the client.
- The client owns that server and copy of the SmartSimple platform.

Identified System Incidents

SmartSimple has not experienced any system incidents within the period of coverage in this SOC 3 report that would be the result of an inappropriately designed and/or ineffective control(s).

Subservice organizations

SmartSimple uses certain subservice organizations to supplement its internal processes and procedures supporting the security and avaiability of the technology underlying business operations. SmartSimple adheres to internal policies and procedures and other applicable regulations in choosing subservice organizations. SmartSimple uses the following subservice organizations in this regard:

- **Amazon Web Services:** Amazon Web Services (AWS) provide on-demand cloud computing services to SmartSimple with regards to network & content delivery, storage, database services, and security & identity compliance. SmartSimple is responsible for maintaining server software and AWS is responsible for equipment, physical security and environment protection.

- **Microsoft Corporation:** Microsoft Corporation (Microsoft) services provides a combination of Microsoft Datacenters Infrastructure as a Service (IaaS) and Azure's IaaS and Platform as a Service (PaaS). SmartSimple uses M365 products, including the Microsoft Online Directory Services, Microsoft Organization ID, and Microsoft Entra ID (formerly Azure Active Directory). SmartSimple is responsible for managing user identities, assigning appropriate roles and permissions, and promptly removing access for terminated users and Microsoft Corporation is responsible for its hosting of physical and virtual servers, network management, data protection and storage services.

The subservice organizations listed above and their corresponding controls, processes, systems, and applications are not within the scope of this report. Users should consider obtaining the service auditor's reports for these subservice organizations, if available.

Subservice organizations and related criteria

The table below reflects controls at subservice organizations upon which SmartSimple relies for certain functions and controls that are relevant to the applicable criteria.

AWS

Trust services criteria intended to be met by the controls of the subservice organization	Controls expected to be implemented at the subservice 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.	**Logical access** • AWS has implemented effective authentication mechanisms. • Access for AWS system administrators to the environment(s) supporting SmartSimple's systems, is reviewed on a periodic basis. • New access for AWS system administrators to the environment(s) supporting SmartSimple's systems, is approved prior to granting access. • Access for AWS system administrators who no longer require access to the environment(s) supporting SmartSimple's systems, is removed within a timely manner. • Databases that SmartSimple has requested to be encrypted have appropriate encryption controls in place.
CC6.4 — The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	**Physical Security Controls** • Physical security devices are used for controlling accessing to highly sensitive facilities. • Requests for access to and removal from the data center are documented and approved by data center management. • Data center management review the list of names and roles of those granted physical access to their areas on a periodic basis to check for continued business need. • Appropriate controls are in place to manage vendor and contractor access, including approvals and monitoring of vendor and contractor access.

Trust services criteria intended to be met by the controls of the subservice organization	Controls expected to be implemented at the subservice organization
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	**System and network security** • AWS has implemented processes and tools to protect systems and networks from external attacks.
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.	**Data Segregation** • AWS maintains adequate separation of SmartSimple systems and data from other AWS customers.
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.	**Vulnerability Management** • Systems used to authenticate SmartSimple's access to AWS are free from exploitable security vulnerabilities.

Trust services criteria intended to be met by the controls of the subservice organization	Controls expected to be implemented at the subservice 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. 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.	**Incident management** • SmartSimple is notified of all security breaches or incidents which may impact the systems hosted at the subservice organization. **Backups** • SmartSimple is promptly notified of events that may prohibit the complete, accurate, and timely completion of processing and backups including, but not limited to, problems with system functionality, performance/response, and telecommunications. • Procedures are in place to safeguard primary and backup media related to SmartSimple data from accidental destruction or deletion.
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.	**Change management** • Changes to the environment(s) supporting SmartSimple's systems, are tested and approved prior to deploying to systems and infrastructure.
A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	**Capacity management** • The subservice organization has controls in place to monitor and manage capacity demand and to enable the implementation of additional capacity.

Trust services criteria intended to be met by the controls of the subservice organization	Controls expected to be implemented at the subservice organization
A1.2 — The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	**Incident Management** • When a potential incident is detected by the subservice organization related to its systems, a defined incident management process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures. **High availability** • AWS maintains reliable connections between data centers in geographically diverse availability zones and associated tooling, to facilitate reliable backup and restoration of systems into another region should an incident or outage occur.
A1.2 — The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. PI1.1 — The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.	**Environmental Protection and Systems Operations** • Environmental protections have been installed including but not limited to the following: temperature and humidity monitoring systems, cooling systems, backup power systems in the event of power failure, and redundant communications lines. • Operations personnel monitor the status of environmental protections on a continuous basis. • Environmental protections receive maintenance on at least an annual basis. • When a potential incident is detected, a defined incident management process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures.

This report is intended solely for use by the management of SmartSimple Software Inc., user entities, prospective user entities, and the independent auditors and practitioners providing services to such entities, and regulators. This report is not intended to be, and should not be, used by anyone other than those specified.

Microsoft Corporation (Microsoft)

Trust services criteria intended to be met by the controls of the subservice organization	Controls expected to be implemented at the subservice organization
CC 6.1 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. CC 6.2 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.	**Logical access** • Microsoft is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning, to the platform services supporting M365. • Microsoft is responsible for maintaining controls over protection of the network environment, including perimeter firewalls, restricting access to network devices for compliance with security standards.
CC 6.3 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.	**Logical access** • Microsoft is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning, to the platform services supporting M365. • Microsoft is responsible for maintaining controls over protection of the network environment, including perimeter firewalls, restricting access to network devices for compliance with security standards.

Trust services criteria intended to be met by the controls of the subservice organization	Controls expected to be implemented at the subservice organization
CC 6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	**Physical Security Controls** • Microsoft is responsible for maintaining controls over protection for the network environment, including perimeter firewalls, restricting access to network devices for compliance with security standards. • Microsoft is responsible for maintaining controls over physical access to the facilities, including data centers, supporting M365. Additionally, Microsoft Datacenters is responsible for maintaining controls for M365 that address environmental threats including natural disasters and man-made threats. • Microsoft is responsible for maintaining controls over physical data storage, protection and disposal services supporting M365.
CC 6.5 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.	**Logical and Physical Security Controls** • Microsoft is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning, to the platform services supporting M365. • Microsoft is responsible for maintaining controls over physical data storage, protections, and disposal services supporting M365.

This report is intended solely for use by the management of SmartSimple Software Inc., user entities, prospective user entities, and the independent auditors and practitioners providing services to such entities, and regulators. This report is not intended to be, and should not be, used by anyone other than those specified.

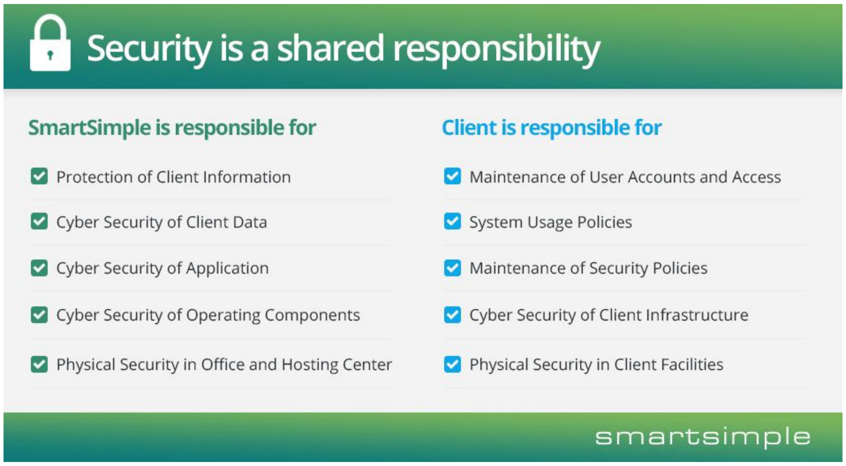
Trust services criteria intended to be met by the controls of the subservice organization	Controls expected to be implemented at the subservice organization
CC 6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries	**System and Network Security** • Microsoft is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning, to the platform services supporting M365. • Microsoft is responsible for maintaining controls over protection of the network environment, including perimeter firewalls, restricting access to network devices for compliance with security standards.
CC 6.7 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.	**Data Segregation** • Microsoft is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning, to the platform services supporting M365. • Microsoft is responsible for maintaining controls over data encryption for data at rest and in motion to the platform services supporting M365. • Microsoft is responsible for maintaining controls over protection of the network environment, including perimeter firewalls, restricting access to network devices for compliance with security standards.

Trust services criteria intended to be met by the controls of the subservice organization	Controls expected to be implemented at the subservice organization
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.	**System Security** • Microsoft is responsible for maintaining controls over protection of the network environment, including perimeter firewalls, restricting access to network devices for compliance with security standards.
CC 7.1 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.	**Vulnerability management** • Microsoft is responsible for maintaining controls over security and incident management, including incident identification and remediation, server vulnerability scanning, and patch management for M365 services hosted on Azure platform. • Microsoft is responsible for maintaining controls over protection of the network environment, including perimeter firewalls, restricting access to network devices for compliance with security standards.

Trust services criteria intended to be met by the controls of the subservice organization	Controls expected to be implemented at the subservice organization
CC 7.2 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. CC 7.3 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. CC 7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. CC 7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.	**Incident Management** • Microsoft is responsible for maintaining controls over data encryption for data at rest and in motion to the platform services supporting M365. • Microsoft is responsible for maintaining controls over security and incident management, including incident identification and remediation, server vulnerability scanning, and patch management for M365 services hosted on Azure platform. • Microsoft is responsible for maintaining controls over protection of the network environment, including perimeter firewalls, restricting access to network devices for compliance with security standards.
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.	**System Availability** • Microsoft is responsible for maintaining controls over data replication and redundancy to the platform services supporting M365. • Microsoft is responsible for maintaining controls over physical access to the facilities, including data centres, supporting M365, including maintaining controls for M365 that address environmental threats.

Shared responsibility model

SmartSimple follows a shared responsibility model with its clients. SmartSimple controls the operation, management and the components of the services and the platform. In turn, the clients assume responsibility and management of the use of and their unique configuration of the system.



Security is a shared responsibility

SmartSimple is responsible for

- ☑ Protection of Client Information
- ☑ Cyber Security of Client Data
- ☑ Cyber Security of Application
- ☑ Cyber Security of Operating Components
- ☑ Physical Security in Office and Hosting Center

Client is responsible for

- ☑ Maintenance of User Accounts and Access
- ☑ System Usage Policies
- ☑ Maintenance of Security Policies
- ☑ Cyber Security of Client Infrastructure
- ☑ Physical Security in Client Facilities

smartsimple

Complementary user entity controls

The effectiveness of the controls described in this report relies on the internal control structures in place at the user entity's locations that use SmartSimple's services. Refer to the Shared Responsibility Model described above. At a minimum, procedures should exist at each SmartSimple user entity as listed below:

Complementary user entity control	Related Trust Services Criteria
1. User entity is responsible for informing SmartSimple of any changes to the individuals authorized to act on behalf of the user entity.	CC 6.1 *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.* CC 6.2 *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.*

Complementary user entity control	Related Trust Services Criteria
2. User entity is responsible for approving the nature and extent of user-access privileges for new and modified user entity personnel's user access within user entity's SmartSimple instance, including standard application profiles/roles, financial reporting transactions, and segregation of duties.	CC 6.1 *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.* CC 6.2 *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.*
3. User entity is responsible for ensuring access for terminated and/or transferred user entity personnel is removed or modified from the user entity's SmartSimple instance in a timely manner.	CC 6.2 *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.*
4. User entity is responsible for reviewing its user profiles on a periodic basis and amending the access changes in a timely manner and/or communicating any changes to SmartSimple in a timely manner.	CC 6.1 *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.* CC 6.2 *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.*

Complementary user entity control	Related Trust Services Criteria
5. User entity is responsible for configuring its instance of SmartSimple with a role-based access security control system to provision access on a need to know and least privilege basis.	CC 6.1 *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.* CC 6.2 *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.*
6. User entity is responsible for configuring their application with appropriate password controls, such as complex passwords, minimum length, password expiration, and failed logon attempts.	CC 6.1 *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.*
7. User entity is responsible for configuring their screen time-out for their SmartSimple application instance.	CC 6.1 *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.*
8. User entity is responsible for enforcing privacy, data protection and information security policies in place which outline the commitments to information and data security, data storage, and privacy of data inputted into their SmartSimple system	CC 6.1 *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.*

Complementary user entity control	Related Trust Services Criteria
9. User entity is responsible for reviewing changes made to application systems on behalf of the user entity and having appropriate user entity personnel approve and authorize SmartSimple to implement the changes.	CC 8.1 *The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.*
10. User entity is responsible for reviewing and checking reports received from SmartSimple and providing timely communications if discrepancies are identified.	PI 1.2 *The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity’s objectives.*
11. User entity is responsible to define data input control, workflow configuration, unique and sequential identifiers, audit trails, and role-based access features in their SmartSimple application instance.	PI 1.2 *The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity’s objectives.*

Overview of Internal Control

Below is the relevant aspects of the Control Environment, Risk Assessment Process, information and Communication and Monitoring

Control environment

SmartSimple’s control environment includes the attitudes, awareness, and actions of management and of employees charged with governance concerning the Company’s internal controls and their significance. The control environment also includes governance and management functions, as well as influences the control awareness of its employees. The collective control environment encompasses management and employee efforts to establish and maintain an environment which supports the effectiveness of specific controls.

The control environment encompasses the following elements:

a. Commitment to integrity and ethical values

The control environment at SmartSimple begins at the highest level of the Company. Executive and senior leadership play important roles in establishing the Company's tone at the top and core values. Every employee is provided with the Company's Code of Conduct and Ethical Practices, Confidentiality Agreements, and sets guiding principles.

The integrity and ethical values of SmartSimple are essential to the Company's control environment and influence the effectiveness of design, implementation, operation, administration, and monitoring of internal controls. SmartSimple screens all new hires through the use of background, credit, and employment verification checks. SmartSimple's Code of Conduct and Ethical Practices identifies examples of misconduct as it pertains to the unethical, dishonest, and illegal acts and the corrective action that will be taken in the event of any occurrence of misconduct. These policy statements and the Code of Conduct outline the expected professional standards of SmartSimple employees.

SmartSimple also fosters a culture that emphasizes the importance of integrity and ethical behavior through oral communication and by Management example. SmartSimple has implemented a third party facilitated ethics hotline, to monitor ethical concerns.

b. Board oversight

The Board of Directors (the Board) maintains oversight of the Company's strategic directions, operational performance, and internal controls. The Board consists of internal and external advisors who bring experience and expertise needed to direct the company. The Board stays abreast of needs and challenges facing the Company through their involvement in day-to-day operations. Quarterly, the Board meets to review SmartSimple's Technologies' services, business strategy, financial information, security, and other items that are related to the Company as a whole. The Board plays an important role in the oversight and governance of the Company. The also help monitor that the Company is operating within established parameters and is complying with business practises.

c. Management philosophy and Operating Style

Management's philosophy and operating style is collaborative, team oriented and consensus driven. Decisions relating to operations, business risk, information processing, and financial reporting are discussed as a group in order to reach an accord among the team. The Management Team meets regularly to discuss open issues and review the daily operations of the Company. The Management Team is composed of strategic employees charged with governance of specific departments of the Company.

d. Organizational structure and assignment of authority and responsibility

SmartSimple's organizational structure provides a framework for planning, executing and controlling business operations. The Company is divided into departments that promote adequate staffing, efficiency of operations, segregation of duties, and responsibility for specific functions within the organization. Management has also established authority and appropriate lines of reporting for key staff. The Management Team, in conjunction with the Team Leads, review team member's performance based on their contribution to the overall team objectives. Reporting relationships are reviewed periodically by senior management and adjusted as needed based on changing business commitments and requirements.

e. Commitment to competence

SmartSimple follows a comprehensive and consistent hiring policy, which includes a multi-step screening process. Job descriptions for open positions at SmartSimple outline in detail the specific skills and behavioral dispositions required to accomplish the required tasks. The applicant's skill level and competency are screened during the interview process to determine whether their levels translate into requisite skills and knowledge.

New hires at SmartSimple must undergo a three-month probationary period; in this period, new hires are reviewed to assess their performance.

SmartSimple has implemented various training platforms to ensure that employees understand and perform their individual roles and responsibilities, including onboarding, e-learning, and on-the-job training. Training and professional development needs are identified on an ongoing basis as well as through the annual review process, which is a collaborative process for individuals and their managers to discuss performance and development. SmartSimple also provides a sponsored education program for employees to access and be reimbursed for courses and professional certifications.

f. Accountability for internal control responsibilities

All employees are expected to set and complete personal development objectives. SmartSimple employees (excluding contractors) meet with their managers annually to review and assess their development. The purpose of this resource management is to ensure that employees continue to develop their skills and knowledge as it pertains to their job and the growth of the Company. The Company's organizational structure and tone at the top also help establish and enforce individual accountability for performance of internal control responsibilities.

Risk management

SmartSimple maintains a risk management process to continually identify, assess, mitigate, report, and monitor risks. Management reviews and evaluates the risks identified in the risk management process at least annually. The risk management process encompasses the following phases:

- Identify – These efforts identify technical and business risks to the organization and operations.
- Assess – The assessment phase considers the potential impact(s) of identified risks to the business, their likelihood of occurrence and includes an evaluation of internal control effectiveness.
- Mitigate – The mitigation phase involves putting controls, processes, and other physical and virtual safeguards in place to prevent and detect identified and assessed risks.
- Report and Monitor – The monitoring phase includes SmartSimple performing various monitoring activities to evaluate whether processes, initiatives, functions and/or activities are mitigating the risk as designed. The risks are reported to managers with the data they need to make effective business decisions and to comply with internal policies and applicable regulations.

Information risk management, in particular the risks related specifically to system security, availability, and processing integrity, is carried out by the Information Security Committee. Risks are identified against achieving information security objectives and mitigation strategies are developed. The Information Security Committee reviews these specific risks periodically.

SmartSimple's risk management framework is impacted by its corporate vision and strategic objectives, whereby risks to achieving the objectives will be captured and assessed against impact and likelihood. Appropriate ownership is assigned to each risk and owners are responsible for the continual management and mitigation of these risks. Risk management is an ongoing process and as such, if and when there are changes or additions to business objectives, new risks may be identified and subjected to the above process.

Information and communication

Internal communication

SmartSimple has implemented various methods of internal communication at a business wide level to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner. These methods include orientation and training programs for newly hired employees; ongoing training programs tailored based on employee roles and responsibilities, including Security Awareness training; regular management meetings for updates on business performance and other matters; and regular all-hands meetings.

Regular communication media are used such as email, video conferencing, and internal messaging tools. Key internal information is posted via the SmartSimple intranet with information on topics such as department policies, HR procedures, and operational processes.

SmartSimple also maintains custom developed platforms such as Support Center and Compliance Tracker to manage, assign, and communicate internal control activities to specific control owners, ranging from operational duties to compliance activities.

External communication

At the client level, SmartSimple has also implemented various methods of external communication to support its client base and the community. System descriptions are communicated both through the general system description, policies, as well as the detailed and client-specific Statement of Work documents which form the basis of the technical specifications agreed upon by SmartSimple and the client. Client training sessions also form an integral part of communication and information transfer. Mechanisms are in place to allow the client support team to be notified and to notify clients of potential operational issues that could impact the client experience. SmartSimple has developed a Community Portal, which allows clients to interact with the client support team to report incidents and access external knowledge tools and community news. SmartSimple also maintains an external wiki, which includes information around technical system functions, upgrade details and general system best practices. A dashboard is also maintained by the Community Support team to monitor for potential breaches of the Service Level Policy. Clients can also subscribe to Premium Support offerings that include direct communication with their designated client support representative and proactive alerts for any client impacting issues.

SmartSimple has implemented its own instance of the platform to track and monitor incidents, problems, errors, and client inquiries. SmartSimple follows a Service Level Agreement which outlines a 4-tier classification of issues for platform and configuration incidents. An escalation procedure is in place, using an emergency email and phone number, for critical issues to alert subject matter experts, executive management, and key development teams.

Control Activities

Organization

Defined policies and procedures exist to ensure that appropriate controls have been established and implemented to address the employee lifecycle. Policies have been established and are monitored by SmartSimple's senior management. A formal process exists for drafting, approving, and revising policies. The SmartSimple control environment is subject to various internal and external risk assessments. The SmartSimple Security Committee has established an information security framework and regularly reviews and updates the ISMS policies, ensures security training is being delivered to employees and conducts security assessments. These reviews assess the availability, security, and integrity of data, as well as conformance to the information security policy.

SmartSimple utilizes Amazon Web Services as its hosting service provider. SmartSimple regularly reviews the third-party service audit reports made available by each provider and assesses any exceptions identified in these audit reports.

Human resources

SmartSimple establishes standard job descriptions for all technical and non-technical roles. The HR Manager may, as informed by the Management Team, create new or revise existing job descriptions as the needs arise within the organization. The job description is then reviewed by the Management Team before it is considered fit for use. SmartSimple has also developed a job skills matrix to define all required skills for any role in the Company. This ensures consistency across job roles and hiring. SmartSimple follows a comprehensive hiring procedure, including appropriate candidate screening and hiring decision making. Prospective candidates are screened through a rigorous interview process, with the expectation of evaluating their business and technical skills as required by the job description. Candidates are hired based on the criteria defined in the job posting and evaluations during interviews. Requests for new hires are authorized by the respective manager and subsequently reviewed and approved by senior management as well. Candidates are subject to a criminal background check, credit check, and employment history check.

All SmartSimple employees and contractors must sign a standard employment contract. SmartSimple's Code of Conduct addresses administrative policies and procedures related to recruitment, the employee development process, compensation and benefits, time away from work, professional conduct and maintaining workplace security. Employees and contractors are required to read and acknowledge they have read the Code of Conduct upon hire. SmartSimple has a defined Employee Confidentiality Agreement to make employees and contractors aware of the confidentiality of client confidential information; employees and contractors are required to sign this document when they are hired, acknowledging that they will keep client information confidential throughout and after their employment with SmartSimple.

The Company follows a structured onboarding process to assist new employees as they become familiar with SmartSimple tools, processes, systems, policies, and procedures. A new hire checklist is completed to ensure that required activities are completed for the onboarding of new employees and contractors. These activities include notifying network administrators to enable logical access from information systems, and enabling physical access and assets, such as keys and key fobs, and laptops.

Employee goals and objectives are defined annually and include training plans for each employee. A performance review is performed on an annual basis to review the employee's progress in meeting defined goals and objectives. Annual performance reviews are limited to SmartSimple's internal employees and does not extend to contractors.

A termination checklist is completed to ensure that required activities are completed for terminated employees and contractors. These activities include notifying network administrators to remove logical access from information systems, and removing physical access and assets, such as retrieving keys and key fobs, and laptops.

Logical security

Staff within the Infrastructure group of SmartSimple are responsible for administering and maintaining logical security for SmartSimple's client production and development environments.

SmartSimple has Information Security Management System (ISMS) policies that define logical security requirements and procedures, such as platform security architecture, use of virtualized servers, secure protocols, audit trails, and access and authentication methods. The ISMS policies also define requirements for logging and monitoring of events. SmartSimple has an established security incident response process.

SmartSimple maintains separate environments for production and non-production instances; these environments are logically and physically segregated. Data is also encrypted at rest and in motion.

To prevent unauthorized access, authorized users are assigned a user-ID, password, and a privilege level (role), which allows the user to sign on and use the system. The responsibility for provisioning employee or contractor access is shared between Human Resources, the Executive Team, and the Internal Support staff. A standard account with privileges is enabled until the hiring manager submits a request and is validated by a member of the Executive Team. The request includes the employee's roles and access privileges for the logical and physical access. Request for changes in access are captured in the SmartSimple permissions tool and audit log. When changes in an employee's job function occur, continued access must be explicitly approved by the Executive Team and documented in the Compliance Tracker. User access and privileges are reviewed on a regular basis by a member of the Executive team.

In addition, password complexity settings for user authentication are managed in compliance with SmartSimple's corporate password policy. SmartSimple uses Microsoft Entra ID (formerly Azure Active Directory (AAD)) for authentication to SmartSimple's network and access to applications that are integrated to M365 suite.

The SmartSimple Platform was developed using Role-Based Access Control (RBAC). All users who interact with the system are assigned roles in order to see/modify/delete data. All functions – including user interface – are controlled by the user's role.

Information systems operations

Information systems operation encompasses monitoring system performance, incident and problem management, and backup and recovery.

SmartSimple utilizes automated monitoring systems and tools to provide and manage service performance and availability. SmartSimple's servers are proactively remotely monitored using a third-party software tool, Pingdom, available for internal and external use. It allows for automated notifications and incident management of server performance. Pingdom alerts SmartSimple support staff if certain pre-established criteria are met.

SmartSimple manages incident and problem management using an instance of the SmartSimple platform, referred to as Support Center. SmartSimple clients can open operations-related problem tickets via phone call, web, or email. These tickets are logged into Support Center, and incident investigation and resolution are tracked in the ticket. SmartSimple personnel can also log tickets within Support Center. Support Center supports reporting to SmartSimple management on the status of problems and incidents.

Documentation is maintained to aid and inform staff in handling incidents or issues. The Support Center Tool is used to support communication, progress updates, and logging capabilities between teams. Root cause analysis is conducted for any significant operational issue (Emergency/Critical severity incident).

Backups are performed on a daily basis; backup jobs have been established whereby instances are backed up to a secure alternative location.

Application system development and maintenance

At SmartSimple, application systems development and maintenance controls are designed to provide reasonable assurance that systems development and maintenance activities are authorized, tested, and implemented. SmartSimple has documented policies that address these requirements. SmartSimple uses Support Center, to manage enhancement requests for new platform functionality.

A separate tool is used to manage the regression scripts for the QA process. Both of these tools validate that the development process is followed, and all changes are documented.

SmartSimple performs regular system upgrades comprised of newly developed features following the development roadmap and the enhancement requested by staff or clients. New code is subject to a peer review, plus automated testing for security vulnerabilities. Once the team determines that the functionality of the code is satisfactory, the code is then passed to a second developer for a detailed code review. After manual peer code review and testing the code is then subject to automated testing using a third-party security testing tool.

After testing, the scripts/code are migrated from the testing environment to the pre-production environment. After the code has been migrated, the QA team are notified that the new code is now in pre-production server for testing. Following successful testing of the new code in the pre-production environment, new code is built as a package. The QA team performs application regression testing to ensure the new package is ready for promotion. Once the QA team completes application regression testing, the package is migrated to the production environment by authorized staff.

Scheduled and non-scheduled changes to the SmartSimple platform are approved by the QA Manager (not development) with each step of the process being logged, tested, approved, and documented in accordance with the platform change policy.

SmartSimple communicates with clients via email broadcast, social media, and the external wiki when platform changes occur or when service use may be affected.

Vendor management

A vendor risk assessment is performed for all significant new vendors that have access to confidential data or impact the security of the system. Additionally, SmartSimple performs a periodic review of third-party service audit reports. A comprehensive information security risk questionnaire is performed for vendors, which provides an in-depth look at the security settings and standards that the vendor adheres to. Once the Comprehensive Information Security Risk Questionnaire is completed, it is reviewed by a senior member of the Information Security Team. Deficiencies are highlighted and reported on to the Risk Acceptance Authority.

Application processing integrity

The SmartSimple platform permits extensive configuration. There are multiple aspects of this configurable functionality that provide internal control features that can be utilized when the platform is configured for a given organization's functionality needs.

The platform architecture is built on a role-based model. This provides for the platform to be configured in such a way that user access controls and privilege management are not an afterthought, but a necessary starting point during the design of an application. Specific features related to role-based access include:

- The naming of various roles such as Admin, Manager, and User as needed by the organization
- An administrator interface that allows definition of an Admin role and assign various special privileges to this role
- Ability to associate all system objects such as fields, forms, menus, and other application components to each defined role

SmartSimple's platform model, provides for each data element to be configured as required by the client. As such, any data field included in the custom application built can be configured to implement data input controls or business rules. SmartSimple's architecture prompts for definition of such controls when a data model is established.

The workflow component of the platform supports the definition of sequential and branching logic and related controls that allow implementation of segregation of duties, forced flow of a transaction or output to specific individuals and such other business rules.

SmartSimple's platform provide for ongoing integrity of configured applications by virtue of its upgradeability without the loss of any configured features. The data associated with configuration (i.e., user defined field names) are stored external to the core application so that for each new version of the core application, the previous configuration changes are automatically available in the new version. This allows continued integrity of control features implemented/customized over the life of the application.

Availability

SmartSimple's contingency plans, risk assessment document and disaster recovery documents are maintained and updated to reflect emerging risks and lessons learned from past incidents. Disaster recovery plans are tested, and disaster recovery policies are reviewed on an annual basis by the Management Team.

SmartSimple has identified critical components required to maintain the availability of the system and recover service in the event of an outage. Critical system components are backed up to a secondary environment on its own physically distinct, independent infrastructure, and is engineered to be highly reliable.

SmartSimple continuously monitors service usage to project infrastructure needs to support availability commitments and requirements. SmartSimple maintains a capacity planning model to assess infrastructure usage and demands on a regular basis. In addition, capacity planning supports the planning of future demands to acquire and implement additional resources based on forecasted requirements and delivered by the hosting services providers.

Monitoring of controls

SmartSimple’s Management Team is committed to establishing and maintaining an effective internal control environment on an ongoing basis. With monthly ISMS management meetings, the Management Team is able to review the progress of the Company’s strategic, operational, financial, and human resources development. Through discussion and consensus, Management implements corrective action and changes on an as needed basis.

From a department perspective, SmartSimple department leads assess and monitor their departmental operations on an ongoing basis. This includes their department’s ability to meet objectives, the development of projects tasked to their department and the professional development of their employees. SmartSimple’s Management Team expects feedback from the department leads on the progress of their team and the corrective actions planned to remediate any discrepancies in accordance with the internal control policies.

SmartSimple’s information system relevant to its application hosting services consists of the systems to deliver services to its clients. Server performance is monitored and customized alerts are sent to escalation contacts.

SmartSimple has implemented in its own instance of the platform to track and monitor its compliance with internal controls policies. Referred to as the Compliance Tracker, the platform is populated with SmartSimple’s control points and control activities. Key control activities are assigned an owner, who is required to log into the platform and confirm that the control activity was performed as required. The Compliance Tracker is reviewed regularly to monitor that controls are being performed appropriately. SmartSimple management is informed of areas of non-compliance, to facilitate resolution and to restore compliance.

SmartSimple monitors resourcing and staffing through ongoing discussion and Management HR meetings. Annual performance reviews are performed to formally evaluate, discuss, and recognize performance over the last year and set goals and priorities for the next year. Also included as part of these discussions are employee roles and responsibilities and how they align with operational plans and goals for the coming period.

No significant changes to SmartSimple’s internal controls were performed within the period of coverage in this report.