SOC2 Type2 Report

Independent Service Auditors Report on Management's Description of a Service Organization's System Relevant to Security, Availability, Processing, Integrity, Confidentiality and Privacy and the Suitability of the Design and Operating Effectiveness of Controls For the period, March 1, 2024, to September 30, 2024, for SpinifexIT.

An Independent Service Auditor
Report issued by Ingressum

Confidential

Table of Contents

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

Independent Service Auditor's Report

To : Management of SpinifexIT

Scope

We have examined the attached SpinifexIT's description of the system titled "**SpinifexIT Applications" (**description) throughout the period, March 1, 2024 to September 30, 2024, included in Section 3, based on the criteria set forth in the Description Criteria DC Section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (description criteria) and the suitability of the design and operating effectiveness of controls included in the description throughout the March 1, 2024 to September 30, 2024, to provide reasonable assurance that SpinifexIT's service commitments and system requirements would be achieved based on the trust service criteria set forth in TSP Section 100, 2017 Trust Services Principles and Criteria for Security *Availability, Processing Integrity, Confidentiality and Privacy* (applicable trust services criteria).

The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of SpinifexIT's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls

As indicated in the description, SpinifexIT does not use any subservice organizations.

Service Organization's Responsibilities

SpinifexIT is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the system to provide reasonable assurance that the service commitments and system requirements were achieved.

SpinifexIT has provided the accompanying assertion titled, Management of SpinifexIT's Assertion (Assertion) about the presentation of the Description based on the Description Criteria and suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirement would be achieved based on the applicable trust services criteria if operating effectively. SpinifexIT is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and (5) designing, implementing and documenting controls that are suitably designed and operating effectively to meet the applicable trust services criteria stated in the Description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the presentation of the description based on the description criteria set forth in SpinifexIT's assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is presented in accordance with the description criteria and (2) the controls are suitably designed and operating effectively to meet the applicable trust services criteria stated in the description throughout the period March 1, 2024 to September 30, 2024.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness

of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs. Because of their nature, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, conclusions about the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria are subject to the risks that the system may change or that controls at a service organization may become ineffective.

Opinion

In our opinion, in all material respects, based on the description criteria described in SpinifexIT' s assertion and the applicable trust services criteria :

a. The description presents the system that was designed and implemented throughout the period March 1, 2024, to September 30, 2024.

b. The controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period March 1, 2024, to September 30, 2024, and the subservice organization and user entities applied the controls contemplated in the design of SpinifexIT' s controls throughout the period March 1, 2024 to September 30, 2024.

c. The controls operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period March 1, 2024, to September 30, 2024, and user entities applied the controls contemplated in the design of SpinifexIT's controls, and those controls operated effectively throughout the period March 1, 2024 to September 30, 2024

Description of Test of Controls

The specific controls we tested, and the nature, timing, and results of our tests are presented in section 4 of our report titled "Independent Service Auditors' Description of Test of Controls and Results"

Restricted Use

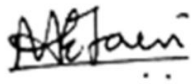
This report, including the description of controls and results thereof in Section 4 of this report, is intended solely for the information and use of SpinifexIT; user entities of SpinifexIT's systems during some or all of the period March 1, 2024 to September 30, 2024; and those prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following :

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, or other parties
- Internal control and its limitations

- User entity responsibilities, Complementary user-entity controls, and how they interact with related controls at the service organization to meet the applicable trust services criteria
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

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

Manoj Jain, CPA



November 5, 2024

SECTION 2

Management of SpinifexIT's assertion

Management of SpinifexIT's Assertion

October 28, 2024

Management of SpinifexIT's Assertion

We have prepared the accompanying description of SpinifexIT entitled "**SpinifexIT Applications**" throughout the period March 1, 2024, to September 30, 2024 (description), based on the criteria set forth in the Description Criteria DC Section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (description criteria).

The description is intended to provide users with information about the system that may be useful when assessing the risks arising from interactions with system throughout the period March 1, 2024 to September 30, 2024, particularly information about system controls that SpinifexIT has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for security, availability, and confidentiality set forth in TSP Section 100, 2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (applicable trust services criteria).

The description also indicates that certain trust services criteria specified in the description can be met only if complementary user entity controls contemplated in the design of SpinifexIT's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of user entities.

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

a. The description presents the system that was designed and implemented throughout the period March 1, 2024 to September 30, 2024 in accordance with the description criteria :

b. The controls stated in the description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated as described and if the subservice organizations and user organizations applied the controls assumed in the design of SpinifexIT's controls throughout the period March 1, 2024, to September 30, 2024

c. SpinifexIT's controls stated in the description operated effectively throughout the period March 1, 2024, to September 30, 2024, to achieve the service commitments and system requirements based on the applicable trust services criteria, if the subservice organizations and user organizations applied the controls assumed in the design of SpinifexIT's controls throughout the period March 1, 2024 to September 30, 2024

Gregory Tutt
Product Chief Technology Officer
SpinifexIT

SECTION 3

Description of SpinifexIT Applications

THROUGHOUT THE PERIOD MARCH 1, 2024, TO SEPTEMBER 30, 2024

Description of SpinifexIT's applications

Background and Overview of Services

SpinifexIT Application overview - On-premises applications

Payroll Optimization	**Easy Reporter**	Powerful and easy-to-use reporting for SAP and SAP SuccessFactors HCM. Easy Reporter is the only SAP-certified reporting solution that combines real-time access to SAP HCM and payroll data with access to SAP SuccessFactors Employee Central, Recruiting, third party data and more. Easy Reporter's drag-and-drop interface allows users to easily access HR and payroll data and results that other query tools don't – without custom programming or integration.
	Easy HelpDesk	Time-saving processes that reduce Payroll and HCM shared service center efforts by 80%. Easy Help Desk radically simplifies SAP HCM and Payroll shared service processes by allowing users to quickly research and resolve employee payroll queries from a single screen inside of SAP. Easy Help Desk empowers the first tier of payroll support to answer more questions, allowing more skilled support personnel to spend time resolving your most difficult challenges.
	Easy Balance (US and Canada)	Simplify US and Canadian payroll and tax reconciliation and improved accuracy of data and reports.
	Easy Single Touch Payroll (Australia)	A comprehensive suite of processes and tools that streamline Australian payroll reconciliation. Easy Single Touch Payroll is SpinifexIT's newest solution which reports the earning details of employees on a per Pay Period cycle. It is the digitization of payment summaries to a continuous, and ongoing process with up to date and year to date figures by employee. Easy Payment Summaries is the industry standard in Australia for SAP Payroll reconciliation processes, reports and tasks. Easy Payment Summaries eliminates many time-consuming reconciliation activities by providing reports that easily reconcile the results and data reported on the payment summary.
Data Cloning and Migration	**Easy Clone**	A Fast, Secure Way to Copy SAP HCM and Payroll Data and Results. SpinifexIT's Easy Clone allows users to copy current and historical employee data and results between systems in just seconds to support testing and troubleshooting. Users control exactly which records to copy, and which sensitive data fields like salary, personnel number, or social security/social insurance number to scramble, to protect data integrity.
	Easy Migration	The Easy Migration integrated solution copies your payroll configuration from your existing SAP system, helps you copy Payroll and Employee data to complete your Payroll testing activities, and runs reports between your legacy system and test system to validate your completed payroll configuration before going live.
	Easy Go Live	Speed up your Payroll Implementation with tools for Parallel Run Testing, Employee Investigation, loading data into Employee Central and ECP Production, as well as Cloning Employees.

Document Generation	**Easy Documents**	Innovative and time-saving employee documents for SAP and SAP SuccessFactors. Easy Documents allows to produce custom employee documents, letters, statements and reports containing data from SAP HCM, SAP SuccessFactors Recruiting, Employee Central and third-party data sources. Easy Documents uses conditional logic to generate documents based on pre-determined conditions, saving users time and improving validity of the output. You can even pre-populate regulatory, employment or benefits forms to save employees time and increase data accuracy.
Connectors	**Easy Payroll Control Center (PCC)**	Validate and reconcile your organization's Payroll results and support your Payroll processes with SpinifexIT's Easy Payroll Control Center Integrated Solution. Ensure the integrity of your organization's payroll results with our pre-defined set of validation and reconciliation content that seamlessly integrates with the Payroll Control Center solution.
	Easy Payroll Control Center (PCC)	Activating the Easy SF Connector enables you to report on both Employee Central Payroll (ECP) and SAP SuccessFactors Employee Central information together in real time. With your current EC and ECP data easily available, your team can quickly provide operational reporting to the HR or Payroll team, your organization's key decision makers or directly to your employees. This can be easily run directly from SuccessFactors without any technical knowledge or the need to do risky manual data extraction and manipulation.

SpinifexIT Application overview - Cloud applications

Solution Type	Product Name	Description
Smart Document Automation	**Strato**	Strato Smart Document Automation is a cloud-based solution that streamlines and automates the generation, management, and delivery of HR and payroll documents within SAP SuccessFactors, improving efficiency and accuracy for HR teams..
Strato Employee Document Management	**Strato**	Strato Employee Document Management is a secure, cloud-based solution that empowers HR teams to efficiently organize, store, and manage employee documents within SAP SuccessFactors, offering seamless access, compliance support, and enhanced data security across the document lifecycle.

Monitoring of Subservice Organizations

SpinifexIT outsources data center facility management from professional data center operating companies (subservice organizations). Section IV of this report and the description of the system only cover the Security, Availability, Processing, Integrity, Confidentiality and Privacy Trust Services Criteria relevant to SpinifexIT and exclude the related controls of the subservice organizations. Through the review of the subservice organizations' SOC 2 or other security policies, processes, and reports, SpinifexIT ensures that all subservice organizations have sufficient controls in place and monitor adherence to processes and procedures.

Data Center Facility Provider

SpinifexIT's data center service provider AWS offers geographic diversity in conjunction with state-of-the-art facilities. Designed and built with reliability, security, and resiliency in mind, they provide fully redundant high-density power and cooling capacities, fully integrated UPS systems, site-wide security and fire protection systems, and access control through customer portals.

Principal Service Commitments and System Requirements

SpinifexIT designs its processes and procedures related to the System to meet its objectives. Those objectives are based on the service commitments that SpinifexIT makes to user entities, the laws and regulations that govern the provision of products and services to its clients, and the financial, operational, and compliance requirements that SpinifexIT has established for the services. Security commitments to user entities are documented and communicated in customer agreements, as well as in the description of the service offering provided online.

SpinifexIT establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in SpinifexIT's system policies and procedures, system design documentation, and contracts with customers.

Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the System.

Components of the System

The System is comprised of the following components :

- Infrastructure including the physical structures, information technology (IT), and other hardware,
- Software includes application programs and IT system software that support application programs,
- People including executives, sales and marketing, client services, product support, information processing, software development, IT,
- Procedures (automated and manual), and
- Data includes transaction streams, files, databases, tables, and output used or processed by the system.

The System boundaries include the applications, databases, and infrastructure required to directly support the services provided to SpinifexIT's clients. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to SpinifexIT's customers are not included within the boundaries of its system.

Boundaries of the System

The specific products and services and locations included in the scope of the report are given below. All other products, services, and locations are not included.

Products and Services in Scope
Products / Application SpinifexIT applications are made up of on premises applications, namely: Easy Suite solutions such as Easy Reporter/Web Reporting, Easy Clone, Easy Helpdesk, Easy STP, Easy Balance US & Canada, Easy Documents, Easy PCC, Easy Migration, Easy GoLive and Cloud based application Strato Suite solutions that include Strato Documents, Strato Signature/Automate, Strato Forms and Strato Storage. **Services** • Support Functions

Scope Exclusions
• None • Only the employees and contract staff who are directly working in the scoped applications are part of this system description

Geographic Locations in Scope

Legal Entity for location	Address
Spinifex IT Group Holdings Pty Ltd Spinifex IT Holdings Pty Ltd Spinifex IT Global Pty Ltd	Suite 757, Waterman Chadstone, UL40, Level 2, 1341 Dandenong Road, Chadstone, Victoria 3148, Australia.
SpinifexIT Philippines, Inc.	Unit 1107, Trade and Financial Tower, 32nd Street 7th Avenue, Bonifacio Global City, 1634 Taguig City, Metro Manila, Philippines.
SpinifexIT North America, Inc.	Louisville Post Office #313 2948 Topside Road Louisville, TN 37777-9998, United States of America.
SpinifexIT Deutschland GmbH	Muskatellerweg 374226 Nordheim.
SpinifexIT Solutions UK Limited	E10 John Street, Bloomsbury, London WC1N 2EBd,United Kingdom
SpinifexIT Singapore Pte. Ltd.	16 Raffles Quay #16-02 Hong Leong Building, Singapore
SpinifexIT Canada Inc.	100 King Street West, Suite 5700, Toronto ON M5X 1C7, Canada

Subsequent Events

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

4. Description of Control Environment, Control Activities, Risk Assessment, Monitoring and Information, and Communication

Control Environment

SpinifexIT's internal control environment reflects the overall attitude, awareness, and actions of management concerning the importance of controls, and the emphasis given to controls in the Company's policies, procedures, methods, and organizational structure.

The Chief Executive Officer, the Senior Management Team, and all employees are committed to establishing and operating an effective Information Security Management System in accordance with its strategic business objectives. The Management at SpinifexIT is committed to the Information Security Management System and ensures that IT policies are communicated, understood, implemented, and maintained at all levels of the organization and regularly reviewed for continual suitability.

Integrity and Ethical Values

SpinifexIT requires directors, officers, and employees to observe high standards of business and personal ethics in conducting their duties and responsibilities. Honesty and integrity are the core principles of the company, and all employees are expected to fulfill their responsibilities based on these principles and comply with all applicable laws and regulations. SpinifexIT promotes an environment of open communication and has created an environment where employees are protected from any kind of retaliation should a good faith report of an ethics violation occur. Executive management has the exclusive responsibility of investigating all reported violations and to take corrective action when warranted.

Board of Directors

Business activities at SpinifexIT are under the direction of the Board of Directors. The company is governed by its Board of Directors headed by its Chairman Victor Allis and Founder/CEO Darren Pithie who oversees the company's Global operations playing a key role in strategy and client management.

Management's Philosophy and Operating Style

The Executive Management team at SpinifexIT assesses risks before venturing into business ventures and relationships. The size of SpinifexIT enables the executive management team to interact with operating management daily.

Risk Management and Risk Assessment

The application of protection measures is based on the risk associated with information assets and the importance of those assets to the organization. As part of this process, security threats are identified and the risk from these threats is formally assessed.

SpinifexIT has placed into operation a risk assessment process to identify and manage risks that could adversely affect their ability to provide reliable processing for User Organizations. This process consists of management identifying significant risks in their areas of responsibility and implementing appropriate measures to address those risks. The senior Management team is members of forums and core working groups in industry forums that discuss recent developments.

Pandemic /COVID Risks

SpinifexIT has reassessed its risk concerning Pandemic risk / COVID risks. Appropriate short-term and long-term changes have been made to impact controls.

Information Security Policies

SpinifexIT has developed an organization-wide SpinifexIT Information Security Policies.

Relevant and important Security Policies (IS Policies) are made available to all employees via Company Intranet or as hard copy policies to new employees. Changes to the Information Security Policies are reviewed and approved before

implementation.

Control Monitoring

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changes in business conditions. SpinifexIT management and Information Security personnel monitor the quality of internal control performance as a routine part of their activities.

Production systems and infrastructure are monitored through service-level monitoring tools which monitor compliance with service level commitments and agreements. Reports are shared with applicable personnel and customers, and actions are taken and communicated to relevant parties, including customers, when such commitments and agreements are not met. In addition, a self-assessment scan of vulnerabilities is performed using end point software. Vulnerabilities are evaluated and remediation actions monitored and completed. Results and recommendations for improvement are reported to management.

Information and Communication

SpinifexIT has documented procedures covering significant functions and operations for each major workgroup. Policies and procedures are reviewed and updated based upon changes and approval by management. Departmental managers monitor adherence to SpinifexIT policies and procedures as part of their daily activities.

SpinifexIT management holds departmental status meetings, along with strategic planning meetings, to identify and address application development, management, service issues, customer problems, and project management concerns. For each environment – Cloud hosted and on premises, there is a selected manager who is the focal point for communication regarding the environmental activity. Additionally, there are personnel that has been designated to interface with the customer if processing or systems development issues affect customer organizations. Electronic messaging has been incorporated into all of SpinifexIT's processes to provide timely information to employees regarding daily operating activities and to expedite management's ability to communicate with SpinifexIT employees.

Communication with Customer Organizations and project teams is conducted through email. Important corporate events, employee news, and cultural updates are some of the messages communicated using corporate internal messaging platform (Slack). Email & Slack is also a means to draw the attention of employees towards adherence to specific procedural requirements.

5. Description of system components and controls

People

Organizational Structure

The organizational structure of SpinifexIT provides the overall framework for planning, directing, and controlling operations. It has segregated personnel and business functions into functional groups according to job responsibilities. This approach helps enable the organization to define responsibilities, lines of reporting, and communication, and helps facilitate employees to focus on the specific business issues impacting SpinifexIT clients.

The CEO – Darren Pithie is responsible for the oversight of SpinifexIT. The SpinifexIT site is locally managed by the following individuals/teams :

- Engineering
- Finance
- Marketing
- Sales
- Quality Assurance
- Product Delivery
- Information Technology
- Compliance and Audit
- Administration
- Human Resources
- Business Development

The management team meets periodically to review business unit plans and performances. Weekly, monthly meetings and calls with senior management, and department heads are held to review operational, security, and business issues, and plans for the future.

SpinifexIT's Information Security policies define and assign responsibilities/accountabilities for information security. Regular management meetings are held to discuss the security level, changes, technological trends, occurrence of incidents, and security initiatives.

SpinifexIT Organization Chart

Commitment to competence

SpinifexIT's formal job descriptions outline the responsibilities and qualifications required for each position in the company. Training needs are identified on an ongoing basis and are determined by the current and anticipated needs of the Business. Employees are evaluated on an annual basis to document performance levels and to identify specific skill training needs

Assignment of Authority and Responsibility

Management is responsible for the assignment of responsibility and delegation of authority within SpinifexIT.

Human Resources Policies and Procedures

SpinifexIT maintains written Human Resources Policies and Procedures. The policies and procedures describe SpinifexIT practices relating to hiring, training and development, performance appraisal and advancement, and termination. Human Resource ('HR') policies and practices are intended to inform employees on topics such as expected levels of integrity, ethical behavior, and competence.

The Human Resources department reviews these policies and procedures periodically to ensure they are updated to reflect changes in the organization and the operating environment. Employees are informed of these policies and procedures upon their hiring and sign an acknowledgment form confirming their receipt. Personnel policies and procedures are documented in the SpinifexIT Human Resources Policy.

New Hire Procedures

New employees are required to read SpinifexIT's' corporate policies and procedures and sign an acknowledgment form stating that they have read and understood them. Hiring procedures require that the proper educational levels have been attained along with required job-related certifications, if applicable, and industry experience. If a candidate is qualified, interviews are conducted with various levels of management and staff.

Background and reference checks are completed for prospective employees before employment over the phone. Employees are required to sign Employee Confidentiality Agreement and are on file for employees. Discrepancies noted in background investigations are documented and investigated by the Human Resources Department in conjunction

with a third-party verification agency. Any discrepancies found in background investigations result in disciplinary actions, up to and including employee termination.

Training and Development

On an ongoing basis, SpinifexIT examines its training and development needs from a business standpoint, both in terms of current needs either internal or customer driven. SpinifexIT compares these needs to the current skills held by its employees. On an as-needed basis, SpinifexIT may select certain employees to receive additional training to meet the current and anticipated needs of the organization. SpinifexIT also offers regular training prepared in-house to undertake training periodically on relevant topics. These trainings are attended by all technical employees of the specific department the training belongs to.

Performance Evaluation

SpinifexIT has a performance review and evaluation program to recognize employees for performance and contributions. SpinifexIT performance evaluation process is also used to help employees improve their performance and skill levels. Employees' performance reviews, promotions, and compensation adjustments are performed every 12 months. The performance evaluation is reviewed with the employee and signed by the employee, their manager.

New Employee Training

HR coordinates to provide information security awareness program to all employees as part of induction. HR maintains the records of information security awareness training namely attendance sheets and feedback forms from employees. Employees undergo security awareness training regularly.

Employee Terminations

Termination or change in employment is being processed as per SpinifexIT HR-related procedures. There are identified and assigned responsibilities about termination or change in employment.

All employees, contractors, and third-party personnel are required to return physical and digital Identification/access tokens provided to them by SpinifexIT or its clients on their termination of employment or contract.

Access privileges are revoked upon termination of employment, contract, or agreement. In case of change of employment /role, rights associated with the prior roles are removed and new access privileges are created as appropriate for the current job roles and responsibilities.

Ethical Practices

SpinifexIT reinforces the importance of the integrity message, and the tone starts at the top. Every employee, manager, and director consistently maintain an ethical stance and supports ethical behavior. Employees at SpinifexIT encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

Code of Conduct and Disciplinary Action

SpinifexIT has put forward the Code of Conduct and Disciplinary Process to encourage and maintain standards of conduct and ensure consistent and fair treatment for all. SpinifexIT employee whose conduct does not comply with an element of the code of conduct and has been found to have breached the Code is prosecuted as per defined process.

Infrastructure

Infrastructure is deployed entirely within the AWS Platform utilizing Cloud Compute and Regional Persistent disks, Regional Snapshots, Encryption at Rest, Virtual Private Clouds isolated by application region with restricted access, minimized port exposure and network isolation only reachable via a secure gateway. Physical access to servers is managed entirely by AWS's data center security procedures. Multiple AWS data centers are utilized based on the region of the nearest AWS business unit.

Commitments and System Requirements

Commitments

Commitments are declarations made by management to customers within a combination of the Terms of Service, Privacy Policy and Data Processing Addendum. Commitments are communicated and made publicly available on the SpinifexIT website.

System Requirements

System requirements are specifications regarding how the infrastructure should function to meet the Company's commitments to Partners. Requirements are specified in the Company's policies and procedures, which are available to all employees. The Company's system requirements include the following:

- Change control
- Logical security
- Physical security – Managed by AWS
- Availability
- Privacy

Changes to the System

The SpinifexIT Software Development Life Cycle (SDLC) follows the Continuous Delivery (CD) development flow and strives to best meet the Continuous Delivery Pipeline ideals. SpinifexIT uses JIRA as its main communication platform for all development related activities.

The philosophy can be summarized as "test automatically, deploy small, deploy often." The goal is to maximize the flow of value delivery in the safest way possible, by deploying single changes in isolation which will allow any unexpected side effects to be quickly reverted and traced back to a more easily identifiable piece of code.

This differs from more traditional request processes, where deployments are scheduled at a cadence and may involve many changes to the code base simultaneously. In the event of any issues, the ability to revert is compromised and the cause of the issue is potentially attributable to any of the combined code that has shipped. These problems grow with the size of the code base and the development team.

The CD process begins with local software development on a virtual machine, designed to mimic the production environment as much as possible.

Code is version controlled using Bitbucket with the central repository managed within SpinifexIT's private account. Developers will follow the Bitbucket Branching Strategy guidelines to create a branch for the related work, and regularly check in their updates.

Once code is ready to be reviewed by other members of the team, a Merge Request (MR) is created to allow other members of the team to review and approve the code changes. The Continuous Integration system runs a growing assortment of tests to ensure the integrity of the code base, including manually written tests by the development team (such as Unit tests among others), security tests, vulnerability checks against 3rd party libraries, code structure and

error checks. The Continuous Integration (CI) system will record the results of these tests within the Merge Request where the reviewers may easily access the results.

On a daily basis, developers have the opportunity to have their merge requests reviewed by the team during daily standups. Some MRs may require a dedicated meeting for review. Merge Request reviews may continue for some time as different members of the team review, comment and make suggestions according to the team's Code Review Guidelines.

In some circumstances, long running manual test environments may be necessary to test certain features. The Lab environments may be requested by any development team and will be provisioned by the Operations team. These lab environments are full production clones (minus data) and accessible to other members of the company as needed.

When a Merge Request is approved and testing is completed, code is deployed to production using automated deployment scripts. In the event of any issues on deployment, the changes are rolled back immediately, and the issues investigated until resolved.

Physical Structures and Physical Access

Physical Access

SpinifexIT development center is in Manila, BGC area, Philippines The entrance for in-scope SpinifexIT's physical office is secured by a security person, physical access control system, and CCTV surveillance. Physical and Environmental Security of SpinifexIT is controlled and governed by SpinifexIT ISMS Policy.

Entry to the SpinifexIT offices is restricted to authorized personnel and a physical access control system is installed at all entrances. All employees are provided with access cards / biometric access. All visitors have to sign the visitor's register and are given an inactive visitor card.

Employees are subjected to show their ID cards at the Security entrance and swipe in/thumbprint the access management system. Employees are granted access only to those areas which they require to access. Some members of the IT Support Team & Administration team have access to the entire facility. The management team has access to all areas except the server rooms. Employees are required to always wear their access cards/employee identification cards while within the facility.

CCTV is implemented to monitor the activities in the server room and main entrance and other security zones. Admin Team monitors the CCTV recordings. Logs are generated and communicated to the management periodically. Backup of recordings are retained as per the retention period.

ID cards are issued to new employees based on an access requisition initiated by the Human Resource (HR) group. The HR group creates a ticket in the helpdesk ticketing application requesting the IT team and Administration / Facilities team to issue an access card to the new employee. The IT / Administration team ensures that the access card/biometric controls are configured with the appropriate access rights, and then issues the same to the employee.

On separation of an employee from the organization, the HR group initiates the 'Exit Process' and circulates it to all the concerned groups. Based on this, the employee's privileges in the access control system are revoked.

Access by visitors, contractors, and/or third-party support service personnel's both entry and exit are monitored by security personnel.

SpinifexIT allows its employees a high breed working environment, which allows an employee to work from home and office. Employees are required to work 3 days a week in the office.

Environmental Controls

SpinifexIT's power systems are designed to provide uninterrupted power, regardless of the availability of power from the local public utilities supplying the office premises. Backup UPS units and backup generators supply (owned or provided by Building Maintenance) power to the center in the event of a power failure. All components are covered by maintenance contracts and tested regularly.

Fire Extinguishers and smoke detectors are installed at all sensitive points. Regular check on the working condition is done, warranty is checked and AMC is entered on completion of Warranty. Yearly fire drills are conducted in coordination with Admin and HR personnel. The fire drills reports are collected, and analysis made upon them.

SpinifexIT Applications

SpinifexIT on-premises applications are developed using SAP SDK . Cloud applications are developed by a separate team utilizing S3 bucket, Elastic Beanstalk, Java, Tomcat, Docker, API, OAuth, Lambda, React, S3, DynamoDB, SNS components. The in-house Continuous Delivery development process involves automated testing, code reviews, automated security testing of the core code base and third-party libraries, vulnerability scans of the servers and combined intrusion detection systems, supplemented by an automated deployment process. Application infrastructure and code are monitored in production for performance, errors and security with alerting systems in place to notify SpinifexIT personnel immediately of any potential concerns. Additional supplements are in place for both abuse protection and rate limits.

Logical Security

Logical access to infrastructure is extensively restricted, network isolated, regionally segmented and accessible only via a secure central entry point. Access to SpinifexIT information systems and services is limited to those individuals who have a need-to-know. This standard is based on the principle of least privilege which states that users are only granted access necessary to complete required tasks. SpinifexIT employees are granted access to various systems based on current job responsibilities and no more. SpinifexIT employees are granted access to various systems to meet job responsibilities and no more. User access reviews are performed on a regular basis by the IT team.

Procedures exist for provisioning access to new personnel, changing access, and revoking access to all SpinifexIT information systems. The access provisioning process begins with the submission of a user access request form by the requestor or the hiring Manager. Upon receipt, the IT department will confirm access approval from the appropriate department, provision the appropriate level of access by assigning a unique user ID and password. Access confirmations will then be communicated with the requestor. Access revocations are initiated by the Human Resources department. Notifications are communicated to appropriate personnel to ensure all access to SpinifexIT' s systems are removed in a timely manner.

SpinifexIT utilizes Transport Layer Security (TLS) encryption to secure data in transit. Remote access to production systems is granted to authorized employees and controlled through the use of a Secure Shell (SSH) tunnel proxy over a secure gateway, which requires a unique user ID/password and Multi Factor for authentication.

Security Monitoring

SpinifexIT has devised and implemented adequate monitoring controls to detect unauthorized information processing activities. Critical servers and systems are configured to log user activities, exceptions, and information security events. System administrator and system operator activities are logged and reviewed periodically.

Capacity management controls are put in place to make certain SpinifexIT's resources are monitored, tuned and projections are made to ensure system performance meets the expected service levels and to minimize the risk of systems failure and capacity-related issues. The addition of new information systems and facilities, upgrades, new versions, and changes are subject to formal system analysis, testing and approval before acceptance.

Network & endpoint protection / monitoring

Access to Internet services from any company computing device (laptop, workstation, server, etc.) or any company address designation should be made through the company's approved perimeter security mechanisms. External connections to company servers are not permitted.

To stop any malware from affecting the security of the customer and organizational data, SpinifexIT uses daily Endpoint Protection vulnerability scans. IT team ensures that all the endpoints in organizations are scanned for any vulnerabilities, including public IPs and services hosted on AWS Data Center, and that any malware is dealt with efficiently and promptly.

Patch Management

All security patches are tested for stability before applying to the production environment. The patches are applied regularly or as required to ensure the efficient operation of the servers, endpoints, and network devices. Operating system patches are managed and applied as they become available.

Vulnerability Scans & Intrusion Detection/Intrusion Prevention

AWS Inspector is utilized to perform periodic vulnerability scans and to monitor any potential host-based intrusion events. The SpinifexIT operations team manages all systems through a configuration management system to automate, centralize, version control and review that infrastructure. Endpoint Protection is installed with the feature of scanning the device automatically and log reports are reviewed by the System Admin.

Anti-virus software has been installed on all desktops & laptops within the scope. Updates to the virus definition files are managed and downloaded by the software itself daily from the vendor website at specific intervals.

All inbound and outbound emails are scanned for viruses and are cleaned automatically as organization utilizes Google for its emails. Anti-malware and security practices are in accordance with the SpinifexIT Malware Protection Policy.

Procedures

IT policies and operating instructions are documented. Procedures described cover server management, server hardening, workstation security system, network management, security patch management, user creation, system audit, ID card activation, etc. Additionally, production and training standard operating procedures are available.

IT Help Desk

SpinifexIT has put in place a helpdesk function that functions out of the IT Department and an integrated helpdesk to handle problems and support requirements of users, support users in case of incidents, and manage them without disruption to SpinifexIT's business and ensures that changes to any component of SpinifexIT's information assets and infrastructure are controlled and managed in a structured manner.

All requests received at the Help Desk are classified as to their criticality and resolved within the maximum resolution time as detailed in the SpinifexIT Help Desk, Change Management, and Incident Response Procedure.

Change Management

SpinifexIT has implemented a well-defined Change management process to ensure that all changes to the information processing facilities, including equipment, supporting facilities and utilities, networks, application software, systems software, and security devices are managed and controlled. The Change Management process describes a methodical approach to handle the changes that are to be made to any work product. All the changes need to be subjected to a formal Change Management process.

Incident Response and Management

Procedures for the incident response including identification and escalation of security breaches and other incidents are included in the policy. Users or any other person log all incidents to the Helpdesk. The help desk personnel study

and escalate all security incidents to the designated team for further escalation/resolution. Any event related to the security of Information assets including facilities and people is termed an Incident.

When an incident is detected or reported, a defined incident response process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures. Root-cause analyses of all the incidents are performed and the root cause identified shall remedy and reported. The actions proposed from the root-cause analyses are reviewed and approved.

The types of information that are logged include:

- Report Date
- Location of Incident
- Incident Start Date
- Incident Notification Date
- Identified issue
- Remediation Steps
- Recommendations
- Preventive measures
- Action Items

There was no security incidents identified throughout the reporting period.

Logical Access

Security Authorization and Administration

Email is sent from HR to IT helpdesk for all new employees for a new workstation configured with minimum default access to company resources/applications required by an employee to perform the job duty. Any additional access is recommended by the line manager. The company has a standard configuration that is implemented across Desktops & laptops individually.

Only the IT team has access to change user profiles or give higher access. Other employees do not have local admin privileges on their desktops, only the IT team has access to install software on employees' machines. The ability to create or modify users and user access privileges is limited to the IT team.

User Access and review

Access to resources is granted to an authenticated user based on the user's identity through a unique login ID that is authenticated by an associated password. Assets are assigned owners who are responsible for evaluating the appropriateness of access based on job roles. This is documented in Access Control Matrix.

Roles are periodically reviewed and updated by asset owners regularly. Privileged access to sensitive resources is restricted to the IT team. Access to storage, backup data, systems, and media is limited to the IT team through the use of physical and logical access controls.

User access rights are currently not reviewed by IT Team members periodically to ensure the level of access is appropriate. This will be initiated going forward. Any access, which is deemed to be no longer required, will be identified and disabled.

Security Configuration

Employees establish their identity to the network and remote systems through the use of a valid unique user ID that is authenticated by an associated password.

Passwords are controlled through Password policy and include periodic forced changes, password expiry, and complexity requirements. User accounts are disabled after a limited number of unsuccessful login attempts; the user is

required to contact the IT Support team to reset the password. Local users do not have access to modify password rules. Guest and anonymous logins are not allowed on any machines.

Additional IT Infra security controls

- The use of encrypted VPN channels helps to ensure that only valid users gain access to IT components.
- Unattended desktops are locked within a time of inactivity. Users are required to provide their password to unlock the desktop.
- Administrative rights and access to administrative accounts are granted to individuals that require that level of access to perform their jobs. All administrative level access, other than to the IT team, must be justified and approved.

Confidentiality

SpinifexIT has implemented a data retention policy to ensure the confidentiality of client data. All agreements with related parties and vendors include confidentiality commitments consistent with the company's confidentiality policy (as described in IT and Security Policies).

Secure procedures are established to ensure the safe and secure disposal of media when no longer required. The level of destruction or disposal of media would depend on the information or data stored in the media and the criticality of the information as per the information classification guideline.

Additional Controls relating to confidentiality

- Access to data is restricted to applications through the access control system.
- Access to data is restricted through password-controlled folders.

Availability

Backup and Recovery of Data

SpinifexIT has developed a Backup policy, and suitable backups are taken and maintained. SpinifexIT has put in place backup processes that define the type of information to be backed up, backup cycles, and the methods of performing a backup.

The backup processes are approved by the business owners and comply with the requirements for business continuity, and legal & regulatory requirements. All backup and restoration logs are maintained for retention periods as defined in the backup procedures.

All backup copies are tested periodically to ensure that the data and information are securely retrievable in the event of an emergency without any loss of information. Users are made aware through adequate training of their responsibilities for ensuring backup of required data and information.

The backup media are tested for restoration periodically to ensure the effectiveness and integrity of the backup. Restoration is done in two cases – the primary case is when an SpinifexIT member requests to recover some data that they might have lost. The other case when a restoration test is done is during regular DR test. The relevant IT personnel (i.e., the backup administrator) ensure that the data is restored appropriately.

Privacy

SpinifexIT follows industry standard privacy practices. Privacy obligations are outlined in SpinifexIT's Privacy Policy and Terms of Service, both of which are available on the SpinifexIT website for all customers.

At any point the Privacy Policy is updated, current customers are notified through the email account associated with the user while a banner may be displayed within the application or under customer notifications. All policies are reviewed at least yearly.

SpinifexIT limits the type and amount of information collected to only what is needed to deliver service. SpinifexIT collects the following minimal amount of information in order to fulfill objectives: Cookies, User-submitted content, IP Address information, email address, and email communications.

Third party sharing is limited to only as needed to support SpinifexIT's services and align with legal requirements outlined within the Electronic Communications Privacy Act (ECPA) and General Data Protection Regulation (GDPR). Any vendor that has access to information that SpinifexIT constitutes as "sensitive or confidential" must maintain a current and acceptable SOC 2 report and sign a Data Processing Addendum (DPA).

All privacy incidents are mitigated according to our Privacy Breach Complaint Policy and Procedures with oversight of the DPO in a timeframe consistent with GDPR standards.

Applicable Trust Services Criteria and related Controls

The Security, Availability, Processing, Integrity, Confidentiality and Privacy trust services categories and SpinifexIT related controls are included in section 4 of this report, "Independent Service Auditor's Description of Tests of Controls and Results".

User- Entity Control Considerations for on premises applications

On premises application provided by SpinifexIT to user entities and the controls of SpinifexIT cover only a portion of the overall controls of each user entity. SpinifexIT controls were designed with the assumption that certain controls would be inherited by user entities SAP infrastructure. This section highlights those internal control responsibilities that SpinifexIT believes should be present for each user entity and has considered in developing the controls described in the report. This list does not purport to be and should not be considered a complete listing of the controls relevant to user entities. Other controls may be required at user entities.

- **Contractual Arrangements**
    - User organizations are responsible for understanding and complying with their contractual obligations to SpinifexIT such as providing input information, reviewing and approval of processed output, and releasing any instructions.

- **Other Controls**
    - User Organizations are responsible for ensuring end customer privacy.
    - User Organizations are responsible for ensuring that complete, accurate, and timely information is provided to SpinifexIT for processing.
    - User Organizations are responsible for their network security policy and access management for their networks, application & data.
    - User Organizations are responsible for working with SpinifexIT to jointly establish service levels and revise the same based on changes in business conditions
    - User Organizations are responsible for implementing sound and consistent internal controls regarding general IT system access and system usage.
    - User Organizations are responsible for implementing controls to remove user access for terminated users and those who were involved in services associated with SpinifexIT application.

- User Organizations are responsible for implementing controls necessary to ensure that transactions relating to SpinifexIT application are appropriately authorized, timely, and complete.
- User Organizations are responsible for ensuring that any data sent to SpinifexIT should be protected by methods to ensure confidentiality, privacy, integrity, availability.
- User Organizations are responsible for logging any complaint, service disruption, or security incident with SpinifexIT
- User Organizations are responsible for reviewing specific SLA reports and hold meetings jointly with SpinifexIT
- User Organizations are responsible for ensuring restricted access control to SpinifexIT applications and systems.
- User Organizations are responsible for ensuring that input data is provided by them as per the process agreed with SpinifexIT and using the secure HTTPS or other secure connections and mechanisms.
- User Organizations are responsible for ensuring that clear instructions are provided to SpinifexIT as part of the onboarding process and project setup.

SECTION 4

Independent service auditor's description of tests of controls and results

Audit Methodology

Introduction

This section presents the Control Objectives (or Criteria/Trust Principles in case of a SOC 2 audit) specified by the management along with the related controls that have been implemented to meet those control objectives.

We have included our description of the test procedures performed to determine the operating effectiveness of these controls.

Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

When using information produced (or provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

When IPE was used for sampling purposes, (such as HR population, lists of change requests, incidents, etc) we performed the following procedures to ensure completeness, the accuracy of the data/reports, and lists provided.

- Inquiry with management that the list is complete and covers all in-scope products, services, and people.
- Review of the sequences, Employee ID, and other transaction numbers for completeness.
- Reasonable checks against other data provided including last year's data.
- Requesting clients to generate the population and reports from the source systems in our presence, where feasible.

Testing Methodology

Section 4 outlines the controls in place by SpinifexIT and describes the tests of their effectiveness performed by the independent service auditor. The following methodologies were used in testing the suitability of the design and operating effectiveness of SpinifexIT's controls :

Test Methodology	Description
Inquiry	The auditor inquired relevant personnel to corroborate control placement or activity.
Inspection	The auditor obtained and read relevant documentation or read the screenshots provided.
Observation	The auditor directly witnessed control placement or activity or evidence thereof.

The tables on the following pages outline the control objectives, controls in place, and independent testing relevant to the independent assessment of SpinifexIT' s control environment throughout the audit period.

Materiality

We report all deviations which have been identified during the test of controls. User entities should determine the materiality of these deviations in respect to their contract with the service organization.

6. Independent Service Auditor's Description of Tests of Controls and Results

Criteria Group 1: Common Criteria Related to Control Environment

CC 1.0 Common Criteria Related to Control Environment			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.1	**The entity demonstrates a commitment to integrity and ethical values.**		
1.1.1	A code of business conduct and ethical standards is reviewed, updated if applicable, and approved by senior management annually. This is achieved via an Employee Handbook that is provided to every new employee.	Inspected the code of business conduct and ethical standards to determine whether it outlines the service organization's commitments to integrity and ethical values and if the conduct and standards were updated and approved by senior management within the examination period. For a selection of new hires, the code of business conduct and ethical standards inspected to determine whether the conduct and the standards were acknowledged by each new hire selected.	No exceptions noted.
1.1.2	Personnel are required to read and accept the code of business conduct and ethical standards upon their hire.	For a selection of new hires, the code of business conduct and ethical standards inspected to determine whether the conduct and the standards were acknowledged by each new hire selected.	No exceptions noted.
1.1.3	Agreements are established with services providers and that include clearly defined terms, conditions, and responsibilities for service providers.	For a selection of agreements with the service providers, we inspected the agreements to determine whether the agreement outlined the Company's requirements, including terms, conditions, and responsibilities for the service providers.	No exceptions noted.

CC 1.0 Common Criteria Related to Control Environment			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.1	**The entity demonstrates a commitment to integrity and ethical values.**		
1.1.4	Prior to employment, personnel are verified against regulatory screening databases, including criminal and employment checks.	For a selection of new hires, inspected the background checks to determine whether selected personnel successfully completed background checks including criminal and employment checks prior to being hired by SpinfexIT.	No exceptions noted.
1.1.5	Before a third-party is engaged by the Company, the third-party personnel undergo background screening. A background check includes criminal and employment checks.	For a selection of third-party personnel engaged by SpinfexIT, inspected the background checks to determine whether selected third-party personnel successfully completed background checks including criminal and employment checks prior to being engaged by SpinfexIT.	No exceptions noted.
CC 1.3	**Management establishes, with Board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.**		
1.3.1	The Steering Committee meets annually to evaluate the Company's security and privacy controls, policies, and risk assessments. The Steering Committee reports regularly to executive management.	Inspected a sample agenda from a Steering Committee meeting to determine security and privacy controls, policies and risk assessments are discussed on a regular basis.	No exceptions noted.
1.3.2	Reporting relationships and organizational structures are in place to align authority and responsibility to appropriate personnel and responsibilities and flow of information to manage the activities of the Company.	Inspected the organization chart to determine whether reporting relationships and organization structure are in place.	No exceptions noted.

CC 1.0 Common Criteria Related to Control Environment			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.3	**Management establishes, with Board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.**		
1.3.3	The security commitments and obligations of user entities are posted on the Company's websites and the web interface and included in business agreements.	Inspected the Terms of Service and Data Processing Addendum contained on the SpinfexIT website to determine that security commitments and obligations are communicated to user entities.	No exceptions noted.
CC 1.4	**The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.**		
1.4.1	The organization has documented HR Policies and procedures including recruitment, training and exit procedures.	Inspected and observed the HR Policies and procedures mentioned in it which include recruitment ,training and exit procedure	No exceptions noted.
1.4.2	SpinfexIT provides continued training about its commitments and requirements for personnel.	Inspected required training records for a sample of employees to determine if training is required annually.	No exceptions noted.
1.4.3	During its ongoing and periodic business planning, business continuity planning and budgeting process, management evaluates the need for additional tools and resources to achieve business objectives including contingency plans for assignments of responsibility important for internal control.	Inspected technology documentation and the Disaster Recovery Plan to determine whether the Company continually evaluates its need for additional tools and resources as well as contingency plans for assignments of responsibility important for internal control.	No exceptions noted.

CC 1.0 Common Criteria Related to Control Environment			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.5	**The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.**		
1.5.1	Departmental meetings are held on a periodic basis to monitor and manage the respective department's progress or lack thereof as it relates to their achievement of the department's responsibilities.	Inspected departmental meeting agendas to determine whether departments periodically meet and whether progress is monitored and measured by respective department heads, including escalation or taking of corrective action as necessary.	No exceptions noted.

Criteria Group 2: Common Criteria Related to Information and Communication

CC 2.0 Common Criteria Related to Information and Communication			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.1	**The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.**		
2.1.1	A risk assessment is performed at least annually to identify risks to the organization that would impact the achievement of service commitments and system requirements.	Inspected the annual risk assessment to determine whether it identifies the information required to support internal controls and the achievement of the Company's service commitments and system requirements.	No exceptions noted.
2.1.2	A risk assessment is performed at least annually to identify key information system processes that process relevant data into information to support the internal control and the achievement of service commitments and system requirements.	Inspected the annual risk assessment to determine whether it identifies the key information system processes that process relevant data into information to support internal controls and the achievement of the Company's service commitments and system requirements.	No exceptions noted.
2.1.3	Policies and procedures relevant to security have been implemented to produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained.	Inspected the Company's documented policies and procedures as they relate to security to determine whether internal controls for producing timely, current, accurate, complete, accessible, protected, verifiable and retained information have been documented.	No exceptions noted.
2.1.4	Daily backup snapshots are performed using an automated system.	Inspected the backup frequency configurations to determine whether backups are performed routinely.	No exceptions noted.

CC 2.0 Common Criteria Related to Information and Communication			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.2	**The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.**		
2.2.1	The intranet is used to communicate to personnel regarding their responsibilities for the design, development, implementation, maintenance, and oversight controls, relevant to the security of the system	Inspected the SpinfexIT intranet to determine whether documented policies and procedures addressing internal controls, relevant to the security of the system are available to internal personnel.	No exceptions noted.
2.2.2	The steering committee meets annually to communicate information needed to fulfill their roles with respect to the achievement of the Company's service commitments and systems requirements.	Inspected the steering committee meeting agendas to determine whether the steering meeting discussions address key items with respect to the achievement of the Company's service commitments and system requirements, including progress, delays, risks, and challenges related to those key items as applicable.	No exceptions noted.
2.2.3	Slack is available to internal users to communicate issues and/or concerns to management.	Observation performed within Slack to determine whether a communication channel is available to internal users for potential concerns.	No exceptions noted.
2.2.4	SpinfexIT's security commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.	Inspected the Terms and Conditions to determine whether documented responsibilities, policies and procedures as they relate to security commitments and responsibilities are available to external users. Inspected the SpinfexIT intranet to determine whether SpinfexIT personnel (internal users) have access to current policies and procedures.	No exceptions noted.

CC 2.0 Common Criteria Related to Information and Communication			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.2	**The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.**		
2.2.5	Policies and procedures are reviewed and updated no less than annually.	Inspected a sample of policies and procedures to determine whether a history of changes with the date of change was properly documented.	No exceptions noted.
2.2.6	Changes to SpinfexIT's commitments and system requirements are communicated to internal and external users.	Inspected the SpinfexIT intranet to determine whether changes to internal commitments and system requirements are communicated to internal personnel.	No exceptions noted.
		Inspected the Terms and Conditions to determine whether changes to SpinfexIT commitments and system requirements are communicated to external users.	
2.2.7	SpinfexIT posts a description of its system, system boundaries, and system processes that include infrastructure, software, people, processes and procedures, and data on the internet for internal users and external users.	Inspected the SpinfexIT website to determine a current system description is available to internal and external users.	No exceptions noted.
2.2.8	Planned changes to application components are communicated to external users	Inspected SpinfexIT's communication method to notify of planned changes to the external users	No exceptions noted.

CC 2.0 Common Criteria Related to Information and Communication			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.3	**The entity communicates with external parties regarding matters affecting the functioning of internal control.**		
2.3.1	Incident response policies and procedures are in place that include an escalation plan based on the nature and severity of the incident.	Inspected the Company's documented Incident Response policies and procedures to determine whether they include an escalation tree and communication plans depending on the nature of the incident.	No exceptions noted.
2.3.2	Contact email addresses are made available on the Company's websites. Management monitors customer and workforce member complaints reported.	Inspected the Company's website to determine whether contact email addresses and phone numbers are available to customers and external users.	No exceptions noted.
2.3.3	System boundaries and system processes are defined and made available to external users.	Inspected the SpinfexIT website to determine a current system description is available to external users.	No exceptions noted.

Criteria Group 3: Common Criteria Related to Risk Assessment

CC 3.0 Common Criteria Related to Risk Assessment			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 3.1	**The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.**		
3.1.1	Management performs a risk assessment annually. The risk assessment is based on the objectives established by management. The objectives incorporate the service commitments and system requirements. Assessed risks are reviewed on a continuous basis to identify changes in underlying threats or in the environment that would require an update to assessed risks.	Inspected risk assessment documentation to determine whether a risk assessment was conducted on a continuous basis to identify potential threats, rate the significance of the risk associated with the threats, and document mitigation strategies for those risks. Inspected documentation for the annual reviews of the risk assessment to determine whether the reviews included evaluation of identified changes in laws and regulations and changes to contractual commitments.	No exceptions noted.
3.1.2	Updates of or modifications to standard contractual terms and commitments are approved by the management prior to contract approval.	Inquired to determine that the management must approve any updates/modifications to the Data Processing Addendum (DPA). Inspected the Data Processing Addendum (DPA) to determine whether a standard Services Agreement is in place with standardized contractual language and if any changes to that language is tracked and documented.	No exceptions noted.

CC 3.0 Common Criteria Related to Risk Assessment			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 3.2	**The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.**		
3.2.1	Regular management meetings are held to discuss strategy and operations, risk considerations, and other factors critical to the business.	Inspected a sample of meetings to determine whether meetings are held where organizational strategy and operations, and risk considerations critical to the business were discussed.	No exceptions noted.
3.2.2	A risk assessment is performed to identify risks arising from external and internal sources and the effectiveness of these controls are shared with executive management.	Inspected the risk assessment to determine whether risks arising from external and internal sources and effectiveness of controls to mitigate those risks were identified and communicated.	No exceptions noted.
3.2.3	The information security team assesses and responds to security risks on an ongoing basis through regular management meetings with IT personnel.	Inspected a sample of Security Review meeting agendas from quarterly information security team meetings to determine whether security risks and vulnerabilities were identified, assessed, and analyzed by management.	No exceptions noted.
3.2.4	The Company has a defined information classification scheme for the labeling and handling of data.	Inspected the data classification policy to determine whether there is a documented classification scheme for labeling and handling data.	No exceptions noted.

CC 3.0 Common Criteria Related to Risk Assessment			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 3.3	**The entity considers the potential for fraud in assessing risks to the achievement of objectives.**		
3.3.1	Policies and procedures related to risk management are developed, implemented, and communicated to personnel.	Inspected Risk Assessment policy and process to determine that the organization has a defined and documented risk assessment process. .	No exceptions noted.
3.3.2	Management performs an annual access review for the in-scope system components to ensure that access is restricted appropriately. Tasks are created to remove access as necessary in a timely manner.	Inspected annual access review documentation to determine whether an access review was performed for in-scope system components and if tasks were created to remove inappropriate access.	No exceptions noted.
CC 3.4	**The entity identifies and assesses changes that could significantly impact the system of internal control.**		
3.4.1	Management meets on a periodic basis to discuss strategy and operations, risk considerations, and other factors critical to the business.	Inspected a sample of meetings to determine whether meetings are held where organizational strategy and operations, and risk considerations critical to the business were discussed.	No exceptions noted.
3.4.2	A risk assessment is performed to identify the information required and expected to support the internal control and the achievement of service commitments and system requirements.	Inspected the annual risk assessment documentation to determine whether the risk assessment process included consideration of the service commitments and system requirements.	No exceptions noted.

Criteria Group 4: Common Criteria Related to Monitoring Activities

CC 4.0 Common Criteria Related to Monitoring Activities			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 4.1	**The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.**		
4.1.1	Management performs assessments on a regular basis and communicates results to management for monitoring of corrective actions.	Inspected documentation for the annual reviews of the risk assessment to determine whether the reviews included evaluation of identified changes in laws and regulations and changes to contractual commitments.	No exceptions noted.
4.1.2	The internal audit function conducts system security reviews quarterly. Results and	Inspected Internal audits were conducted as per the established schedule. Documentation indicates that	No exceptions noted.

	recommendations for improvement are reported to management	corrective actions were effectively tracked and reported to management	
4.1.3	On-going evaluation of internal controls are performed, and necessary remediation is performed.	Inspected a sample of vulnerability scans performed and inspected the vulnerability remediation tracking documentation to determine exceptions are addressed as deficiencies are identified.	No exceptions noted.
		Inspected documentation for the annual risk assessment to determine whether potential risks and threats to the internal control environment are evaluated.	

CC 4.0 Common Criteria Related to Monitoring Activities			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 4.2	**The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.**		
4.2.1	Management performs risk assessments on a regular basis and communicates results to management for monitoring of corrective actions.	Inspected documentation of the annual risk assessment to determine whether potential risks and threats to the internal control environment are evaluated on an annual basis.	No exceptions noted.
		Inspected documentation for the annual reviews of the risk assessment to determine whether the results were communicated to management and corrective actions are evaluated.	
4.2.2	Deficiencies are risk rated and reported to senior management, as needed.	Inquired of management to determine whether management meets periodically to discuss planned assessments, identified risks, and on-going remediation.	No exceptions noted.
		Inspected applicable meeting agendas to determine whether risks are reported to senior management.	
4.2.3	Management tracks the status of all deficiencies until satisfactorily resolved.	Inspected the risk register to determine whether management tracks and monitors the deficiencies resulting from ongoing assessments.	No exceptions noted.
		Inspected applicable meeting agendas to determine whether risks are reported to senior management.	

Criteria Group 5: Common Criteria Related to Control Activities

CC 5.0 Common Criteria Related to Control Activities			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 5.1	**The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.**		
5.1.1	As part of its annual risk assessment, management linked the identified risks to controls that have been designed and operated to address them.	Inspected the annual risk assessment documentation to determine whether new controls were implemented for any risks not adequately addressed by existing controls.	No exceptions noted.
5.1.2	When management identifies the need for new controls, management considers a mix of control activities, including both manual and automated controls and preventive and detective controls.	Inspected the risk assessment documentation to determine whether management considered a mix of control activities to mitigate the identified risks.	No exceptions noted.
5.1.3	The Company has designed application-enforced segregation of duties to define what privileges are assigned to users within applications.	Inspected information security policies to determine whether application controls were designed to enforce segregation of duties to users within applications.	No exceptions noted.
CC 5.2	**The entity also selects and develops general control activities over technology to support the achievement of objectives.**		
5.2.1	When management identifies the need for new controls, management considers a mix of control activities, including both manual and automated controls and preventive and detective controls.	Inspected the risk assessment documentation to determine whether management considered a mix of control activities to mitigate the identified risks.	No exceptions noted.
CC 5.3	**The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.**		
5.3.1	Policy and procedure manuals address controls over significant aspects of operations. A comprehensive program is in place that addresses key components of IT operations.	Inspected the policy and procedures to determine whether they included section headings that addressed controls over the significant aspects of system operations.	No exceptions noted.
CC 5.0 Common Criteria Related to Control Activities			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 5.3	**The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.**		
5.3.2	Senior management establishes, maintains, and enforces information security policies and procedures.	Inspected policies and procedures to determine whether ownership, review, and approval is properly documented	No exceptions noted.

		within the Company's IT policies and procedures.	
5.3.3	Policy and procedure manuals are reviewed annually by senior management for consistency with the organization's risk mitigation strategy and updated as necessary for changes in the strategy.	Inspected the policy and procedure manuals to determine whether policies and procedures had been updated for changed in the risk mitigation strategy. Inspected documentation of the annual review of the policy and procedure's manuals by senior management.	No exceptions noted.

Criteria Group 6: Common Criteria Related to Logical and Physical Access Controls

CC 6.0 Common Criteria Related to Logical and Physical Access Controls			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
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.**		
6.1.1	System components are tracked through an asset inventory listing to log, track, and maintain all inventory components.	Inspected the asset inventory listing to determine whether a listing is in place to track system components.	No exceptions noted.
6.1.2	Organization has documented procedure for logical access controls	All policies are clear and detailed, effectively demonstrating the organization's commitment to logical access security. The control measures are robust, aiming to prevent unauthorized access.	No exceptions noted.
6.1.3	Access is granted on a least privileges basis as default and any additional access needs to be approved.	Inspected access control procedure document and determined that access is granted on least privileges basis as default and any additional access needs to be approved.	No exceptions noted.
6.1.4	Management performs an annual access review for the in-scope system components to ensure that access is restricted appropriately. Tasks are created to remove access as necessary in a timely manner.	Inspected the annual access review documentation to determine whether an access review was performed for in-scope system components and if tasks were created to remove inappropriate access.	No exceptions noted.
6.1.5	A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the data classification policy to determine if procedures exist around classifying and protecting confidential information.	No exceptions noted.
6.1.6	Passwords for in-scope system components are configured in accordance with industry standards.	Inspected in-scope system components to determine whether passwords are configured according to Company policy.	No exceptions noted.

CC 6.0 Common Criteria Related to Logical and Physical Access Controls			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
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.**		
6.1.1	System components are tracked through an asset inventory listing to log, track, and maintain all inventory components.	Inspected the asset inventory listing to determine whether a listing is in place to track system components.	No exceptions noted.
6.1.2	Organization has documented procedure for logical access controls	All policies are clear and detailed, effectively demonstrating the organization's commitment to logical access security. The control measures are robust, aiming to prevent unauthorized access.	No exceptions noted.
6.1.3	Access is granted on a least privileges basis as default and any additional access needs to be approved.	Inspected access control procedure document and determined that access is granted on least privileges basis as default and any additional access needs to be approved.	No exceptions noted.
6.1.4	Management performs an annual access review for the in-scope system components to ensure that access is restricted appropriately. Tasks are created to remove access as necessary in a timely manner.	Inspected the annual access review documentation to determine whether an access review was performed for in-scope system components and if tasks were created to remove inappropriate access.	No exceptions noted.
6.1.5	A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the data classification policy to determine if procedures exist around classifying and protecting confidential information.	No exceptions noted.
6.1.6	Passwords for in-scope system components are configured in accordance with industry standards.	Inspected in-scope system components to determine whether passwords are configured according to Company policy.	No exceptions noted.

CC 6.0 Common Criteria Related to Logical and Physical Access Controls			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
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.**		
6.1.7	A configuration management tool is in place to ensure that all system changes undergo formal documentation, review, and authorization.	Inspected the configuration management policy to determine whether all changes to the system are to be configuration controlled and approved.	No exceptions noted.
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.**		
6.2.1	Access to in-scope system components requires a documented access request form and manager approval prior to access being provisioned.	Inspected access request email for a sample of new hires that received access to the in-scope system components to determine whether an access provisioning request was properly approved prior to access being provisioned.	No exceptions noted.
6.2.2	A termination process is in place and initiated by the Human Resources department and access is revoked for employees within a timely manner as part of the termination process.	Inspected a listing of terminated employees and compared the listing to the active user listing to determine whether terminated employees retained access to the in-scope system and platforms after their separation.	No exceptions noted.
6.2.3	Management performs an annual access review for the in-scope system components to ensure that access is restricted appropriately. Tasks are created to remove access as necessary in a timely manner.	Inspected the annual access review documentation to determine whether an access review was performed for in-scope system components and if tasks were created to remove inappropriate access.	No exceptions noted.

CC 6.0 Common Criteria Related to Logical and Physical Access Controls			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
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.**		
6.3.1	Asset owners periodically review access to ensure continued appropriateness. Individuals are assigned to appropriate groups within the AWS environment.	Interviewed asset owners and inspected documentation to determine whether appropriate procedures are in place to remove or modify application access as needed.	No exceptions noted.
		Inspected the annual access review documentation to determine whether an access review was performed for in-scope system components and if tasks were created to remove inappropriate access.	
6.3.2	A termination process is in place and initiated by the Human Resources department and access is revoked for employees within a timely manner as part of the termination process.	Inspected a listing of terminated employees and compared the listing to the active user listing to determine whether terminated employees retained access to the in-scope system and platforms after their separation.	No exceptions noted.
6.3.3	The Company establishes and administers privileged user accounts in accordance with a role-based access scheme that organized information system and network privileges into roles.	Inspected the access control policy to determine whether a role-based access scheme was employed to organize information system and network privileges into roles.	No exceptions noted.
		Inspected evidence of administrators with access to the in-scope systems to determine whether privileged user accounts administered in accordance with a role-based access scheme.	

CC 6.0 Common Criteria Related to Logical and Physical Access Controls			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
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.**		
6.5.1	Formal data retention and disposal procedures are in place to guide the secure disposal of the Company's and customers' data.	Inspected data retention and disposal procedures to determine whether procedures are in place.	No exceptions noted.
CC 6.6	**The entity implements logical access security measures to protect against threats from sources outside its system boundaries.**		
6.6.1	Firewalls are configured to limit unnecessary ports, protocols and services. The only ports open into the environment are defined.	Inspected the firewall configurations and rulesets employed within the environment to determine whether the permit rules align with the specified networking protocols permitted for inbound network traffic.	No exceptions noted.
6.6.2	The company has deployed Transport Layer Security (TLS) for transmission of confidential and/or sensitive information over public networks.	Inspected TLS settings to determine whether transmission of confidential and/or sensitive information over public networks is encrypted.	No exceptions noted.
6.6.3	Remote access to production systems is restricted to authorized employees through industry authentication standard.	All remote access to production systems is restricted to authorized employees through MFA	No exceptions noted.
6.6.4	Intrusion detection systems are used to provide continuous monitoring of the network and prevention of potential security breaches.	Inspected AWS based intrusion detection system configurations to determine whether continuous monitoring of the network and early prevention of potential security breaches are in place.	No exceptions noted.

CC 6.0 Common Criteria Related to Logical and Physical Access Controls			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
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.**		
6.7.1	Company policies prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted.	Inspected the information security policies to determine that transmission of sensitive information over the internet happens only when the information is encrypted via AWS and JIRA.	No exceptions noted.
6.7.2	Google drive is used for the transmission of sensitive information.	Inspected available Google Drive configurations to determine whether data in transit is appropriately secured.	No exceptions noted.
6.7.3	Storage for workstations and laptops is encrypted using bitlocker.	Observed during walkthrough that user endpoint is encrypted through bit locker.	No exceptions noted.
CC 6.8	**The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.**		
6.8.1	Only authorized system administrators are able to install software on system devices. Unauthorized use or installation of software is explicitly covered in the acceptable usage policy.	Inspected the acceptable usage policy to determine whether the policies prohibit installation of software by users, and installation is limited to system administrators.	No exceptions noted.
6.8.2	An IT monitoring system logs and alerts system administrators of software installation or attempted software installation.	Action1 provides compliance reports about non-updated machines.	No exceptions noted.

CC 6.0 Common Criteria Related to Logical and Physical Access Controls			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.8	**The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.**		
6.8.3	Continuous Delivery procedures are in place to govern the modification and maintenance of production systems and address security and availability requirements.	Inspected the continuous delivery procedures to determine whether procedures are in place to govern the modification and maintenance of production systems and address security and availability requirements.	No exceptions noted.
6.8.4	Tools are in place to detect instances of malicious applications and vulnerabilities within the SpinfexIT AWS environment.	Inspected a sample of AWS vulnerability scans performed to determine whether monitoring solutions are in place to detect potential vulnerabilities and malicious applications.	No exceptions noted.
6.8.5	Logging and monitoring software is used to collect data from system infrastructure components and endpoint systems and used to monitor system performance, potential security threats and vulnerabilities, resources utilization, and to detect unusual system activity or service requests.	Inspected installed software for use of logging and monitoring software to determine whether the monitoring software is operational.	No exceptions noted.

Criteria Group 7: Common Criteria Related to System Operations

CC 7.0 Common Criteria Related to System Operations			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
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.**		
7.1.1	Baseline configurations for servers are retained within the configuration manager tool for roll back capability anytime an approved configuration change is made.	Inspected the hardening and configuration checklists to determine whether baseline configurations are retained and up to date for applicable system changes.	No exceptions noted.
7.1.2	An IT infrastructure monitoring tool is utilized to monitor IT infrastructure availability and performance and generates alerts when specific predefined thresholds are met.	Inspected IT infrastructure monitoring tool configurations and a sample notification to determine whether IT infrastructure monitoring tools are utilized to monitor IT infrastructure availability and performance and generates alerts when specific predefined thresholds were met.	No exceptions noted.
7.1.3	A configuration monitoring tool is utilized that notifies management of changes to the production system.	Inspected alert configurations settings and a sample alert to determine whether a configuration monitoring tool monitored and alerted management of changes to production in a timely manner.	No exceptions noted.
7.1.4	Automated mechanisms are used to continuously detect the addition of unauthorized components/devices into the system.	Inspected configuration settings for the monitoring tool and a sample alert to determine whether a configuration monitoring tool monitors and alerts management of any unauthorized components.	No exceptions noted.

CC 7.0 Common Criteria Related to System Operations			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
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.**		
7.1.5	Internal and external network vulnerability scans are performed on a periodic basis. A remediation plan is developed, and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected a sample of internal and external vulnerability scans to determine whether internal and external vulnerability scans were performed, and remediation plans were developed to remediate all critical and high vulnerabilities.	No exceptions noted.
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.**		
7.2.1	User entities are provided with instructions for communicating potential security breaches to the information security team.	Inspected the instructions provided to user entities to determine whether they include protocols for communicating potential security breaches.	No exceptions noted.
7.2.2	When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures.	Inspected the written incident management procedures to determine whether the procedures include a process for handling security incidents.	No exceptions noted.

CC 7.0 Common Criteria Related to System Operations			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
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.**		
7.2.3	Security incidents are reported to the help desk and tracked through to resolution. Incidents that may affect security compliance are reported to the security compliance officer.	Selected a sample of security incidents logged in the incident tracking system and inspected documentation to determine whether the incident was tracked within a help desk ticket until resolution. Inspected a sample of security incidents logged in the incident tracking system and associated communications to the security officer that may affect security compliance to determine whether the incidents were reported to the security officer.	No security incidents were identified and, therefore, the control did not operate during the examination period.
7.2.4	Intrusion detection systems are used to provide continuous monitoring of the Company's network and prevention of potential security breaches.	Inspected intrusion detection system configurations to determine whether continuous monitoring of the Company's network and early prevention of potential security breaches are in place.	No exceptions noted.
7.2.5	All incidents related to security are logged, tracked, and communicated to affected parties by management until resolved.	Inspected a sample of IT security incident tickets to determine whether an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No security incidents were identified and therefore, the control did not operate during the examination period.

CC 7.0 Common Criteria Related to System Operations			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
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.**		
7.2.6	A risk assessment is performed on at least an annual basis. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments, policies, and procedures are identified and the risks are formally assessed.	Inspected the most recent risk assessment to determine whether threats and changes were formally identified and assessed on an annual basis.	No exceptions noted.
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.**		
7.3.1	Security incident response policies and procedures have been developed that are communicated to authorized users.	Inspected incident response policies and procedures to determine whether an incident response plan is properly documented and has been communicated to authorized users.	No exceptions noted.
7.3.2	All incidents related to the security of the system are logged, tracked, and communicated to affected parties by management until resolved.	Inspected a sample of IT security incident tickets to determine whether an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No security incidents were identified and therefore, the control did not operate during the examination period.
7.3.3	Security incidents are analyzed including what specific attack occurred, which system(s) were affected and what happened during the attack. A root cause analysis is performed to determine the classification and impact of the event.	Inspected the documentation of root cause analysis for a sample of IT security incidents to determine whether a root cause analysis was performed to determine the classification and impact of the event.	No security incidents were identified and therefore, the control did not operate during the examination period.

CC 7.0 Common Criteria Related to System Operations			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
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.**		
7.4.1	Management has established defined roles and responsibilities to oversee implementation of information security policies including incident response.	Inspected security policies to determine whether the Company has established defined roles and responsibilities to oversee implementation of the incident response plan.	No exceptions noted.
7.4.2	After an incident has been confirmed, specific personnel are engaged in the containment process to reduce the magnitude of the incident.	Inspected a sample of IT security incident tickets to determine whether an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No security incidents were identified and therefore, the control did not operate during the examination period.
7.4.3	The containment phase ensures that all other interconnections to the system were not affected by the security incident.	Inspected a sample of IT security incident tickets to determine whether an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No security incidents were identified and therefore, the control did not operate during the examination period.
7.4.4	An assessment of the incident response to better handle future incidents is performed through an analysis of after-action reports or the mitigation of exploited vulnerabilities to prevent similar incidents in the future.	Inspected a sample of IT security incident tickets to determine whether an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No security incidents were identified and therefore, the control did not operate during the examination period.

CC 7.0 Common Criteria Related to System Operations			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
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.**		
7.4.5	Daily backups are configured for the databases.	Observed backup configurations to determine whether daily disk snapshots are configured for the databases.	No exceptions noted.
7.4.6	All incidents related to the security of the system are logged, tracked, and communicated to affected parties by management until resolved.	Inspected a sample of IT security incident tickets to determine whether an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No security incidents were identified and therefore, the control did not operate during the examination period.
7.4.7	Internal and external network vulnerability scans are performed on a periodic basis. A remediation plan is developed, and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected a sample of internal and external vulnerability scans to determine whether internal and external vulnerability scans were performed, and remediation plans were developed to remediate all critical and high vulnerabilities.	No exceptions noted.
CC 7.5	**The entity identifies, develops, and implements activities to recover from identified security incidents.**		
7.5.1	All software updates and patches are tested prior to implementation. An ability to rollback is implemented during software updates and/or patching.	Inspected a sample of updates and patches to determine whether each change was tested in accordance with the change management policy prior to being placed into production.	No exceptions noted.

CC 7.0 Common Criteria Related to System Operations			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.5	**The entity identifies, develops, and implements activities to recover from identified security incidents.**		
7.5.2	All incidents related to the security of the system are logged, tracked, and communicated to affected parties by management until resolved.	Inspected a sample of IT security incident tickets to determine whether an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No security incidents were identified and therefore, the control did not operate during the examination period.
7.5.3	Security incidents are analyzed including what specific attack occurred, which system(s) were affected and what happened during the attack. A root cause analysis is performed to determine the classification and impact of the event.	Inspected the documentation of root cause analysis for a sample of IT security incidents to determine whether a root cause analysis was performed to determine the classification and impact of the event.	No security incidents were identified and therefore, the control did not operate during the examination period.

Criteria Group 8: Common Criteria Related to Change Management

CC 8.0 Common Criteria Related to Change Management			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
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.**		
8.1.1	Systems development life cycle (SDLC) methodology is in place to govern the development, acquisition, implementation, and maintenance of computerized information systems and related technology requirements.	Inspected the systems development life cycle (SDLC) methodology to determine whether it governed the development, acquisition, implementation, and maintenance of computerized information systems and related technology requirements.	No exceptions noted.
8.1.2	The software change management process requires that change requests are: Authorized Formally documented Tested prior to migration to production Reviewed and approved	Inspected a sample of change requests (Merge Requests) within Bitbucket for code reviews to determine whether changes were: ● Authorized ● Formally documented ● Tested prior to migration to production ● Reviewed and approved	No exceptions noted.
8.1.3	Change management procedures are in place to govern the modification of production systems and address security and availability requirements.	Inspected the change management procedures to determine whether proper procedures were in place to govern the modification and maintenance of production systems and addressed security and availability requirements.	No exceptions noted.

CC 8.0 Common Criteria Related to Change Management			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
8.1.4	A process is in place to document system changes to support ongoing maintenance of the system and to support system users in performing their responsibilities.	Inspected change documentation from a system-generated list of program changes for a sample of emergency changes to determine whether the changes were properly approved.	No emergency changes were implemented and therefore, the control did not operate during the examination period.
8.1.5	A process is in place to track system changes prior to implementation.	Inspected the change management procedure whether it tracks system changes prior to implementation.	No exceptions noted.
8.1.6	A process is in place to select and implement the configuration parameters used to control the functionality of software.	Inspected and reviewed the current software development lifecycle policies and processes	No exceptions noted.
8.1.7	A process is in place to test system changes prior to implementation.	Inspected the QA testing process	No exceptions noted.
8.1.8	A process is in place to approve system changes prior to implementation.	Inspected the processes to verify all change requests are authorized, tested, approved, and documented	No exceptions noted.
8.1.9	A process is in place to implement system changes.	Inspected a list of authorized personnel for software and system changes to the production environment	No exceptions noted.
8.1.10	Objectives affected by system changes are identified, and the ability of the modified system to meet the objectives is evaluated throughout the system development life cycle.	Inspected and reviewed the change management and system development policies, procedures, and process	No exceptions noted.

8.1.11	Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents: Changes in infrastructure, data, software, and procedures required to remediate incidents to continue to meet objectives are identified, and the change process is initiated upon identification.	Inspected and reviewed the change management and system development policies, procedures, and process	No exceptions noted.
8.1.12	A baseline configuration of IT and control systems is created and maintained.	Inspected baseline checklist for IT	No exceptions noted.
8.1.13	A process is in place for authorizing, designing, testing, approving and implementing changes necessary in emergency situations.	Inspected change documentation from a system-generated list of program changes for a sample of emergency changes to determine whether the changes were properly approved.	No emergency changes were implemented and therefore, the control did not operate during the examination period.
8.1.14	The organization protects confidential information during system design, development, testing, implementation, and change processes to meet the organization's objectives related to confidentiality.	Separate environments for production, testing, and development are in use	No exceptions noted.
8.1.15	The organization protects personal information during system design, development, testing, implementation, and change processes to meet the organization's objectives related to privacy.	Inspected system-generated list of user and admins with access to development, testing, and production environments.	No exceptions noted.

Criteria Group 9: Common Criteria Related to Risk Mitigation

CC 9.0 Common Criteria Related to Risk Mitigation			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 9.1	**The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.**		
9.1.1	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and migration strategies for those risks.	Inspected the risk management policy to determine whether a program has been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
9.1.2	Cyber insurance is in place to minimize the financial impact of any loss events.	Inspected applicable insurance documentation to determine whether cyber insurance is in place for potential loss events.	No exceptions noted.
CC 9.2	**The entity assesses and manages risks associated with vendors and business partners.**		
9.2.1	The risk management program includes vendors and business partners to minimize any loss in an event.	Inspected the risk management policy to determine whether the program includes vendors and business partners to minimize any loss in an event.	No exceptions noted.
9.2.2	A vendor risk assessment is performed for all vendors on an annual basis that have access to confidential data or impact the security of the system.	Inspected vendor risk assessment documentation for a sample of vendors to determine whether a risk assessment was performed within the past year.	No exceptions noted.

CC 9.0 Common Criteria Related to Risk Mitigation			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 9.2	**The entity assesses and manages risks associated with vendors and business partners.**		
9.2.3	Management has established defined roles and responsibilities to oversee implementation of information security policies.	Inspected documentation to determine whether the Company has established defined roles and responsibilities to oversee implementation of information security policies.	No exceptions noted.
9.2.4	SpinfexIT has documented and communicated security policies that define the information security rules and requirements for the service environment.	Inspected the security policies to determine whether they address applicable information security requirements including communication of service issues.	No exceptions noted.
9.2.5	SpinfexIT has clauses in its agreements with vendors and business partners to terminate relationships when necessary. Vendor and business partner access is removed upon termination through a termination checklist and access is revoked within 24 hours as part of the termination process.	Inspected a listing of terminated vendors and compared the vendor employee listing to the active user listing to determine whether terminated vendor employees retained access to the in-scope system and platforms after their separation.	No exceptions noted.
		For a selection of agreements with the service providers, inspected the agreements to determine whether the agreement included termination clauses.	

Additional Criteria Group A1: Additional Criteria Related to Availability

Additional Criteria Group A1.0 – Additional Criteria Related to Availability			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
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.**		
A1.1.1	Processing capacity is monitored on an ongoing basis.	Inspected documentation of the capacity and availability tool to determine if processing capacity is monitored on an ongoing basis.	No exceptions noted.
A1.1.2	Future processing demand is forecasted and compared to scheduled capacity on an ongoing basis. Forecasts are reviewed and approved by management.	Inspected documentation of management's monthly service provider account review to determine whether forecasting of future processing demand and scheduled capacity is performed on an ongoing basis.	No exceptions noted.
A1.2	**The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.**		
A1.2.1	Daily backups are performed using an automated system.	Inspected the backup frequency configurations to determine whether daily and hourly disk snapshots are performed.	No exceptions noted.
A1.2.2	Backups are monitored for failure and the incident management process is automatically invoked.	Inspected the backup alert configurations to determine if backup monitoring is in place.	No exceptions noted.
A1.2.3	Backups are stored offsite by a third-party storage provider.	Inspected the offsite replication configurations to determine whether backups are securely stored offsite within the third-party media vault.	No exceptions noted.

Additional Criteria Group A1.0 – Additional Criteria Related to Availability			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
A1.2	**The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.**		
A1.2.4	Business continuity and disaster recovery plans have been developed and updated annually.	Inspected the most recent Business Continuity and Disaster Recovery Plan to determine whether the Company has a plan in place which outlines the strategy to resume operations in the case of a disruption of operations including tasks and communication protocols.	No exceptions noted.
A1.3	**The entity tests recovery plan procedures supporting system recovery to meet its objectives.**		
A1.3.1	Business continuity and disaster recovery plans, including restoration of backups, are tested annually.	Inspected test results to determine if the business continuity and disaster recovery plans, including restoration of backups, are tested annually.	No exceptions noted.
A1.3.2	Test results are reviewed and utilized to improve the business continuity and disaster recovery plans	Inspected evidence of the business continuity and disaster recovery test results communicated to management to determine whether test results are properly reviewed.	No exceptions noted.

Additional Criteria Group P1: Privacy Criteria Related to Notice and Communication of Objectives

Additional Criteria Group P1.0 – Privacy Criteria Related to Notice and Communication of Objectives			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
P1.1	**The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.**		
P1.1.1	The entity provides notice of its privacy practices to data subjects of the system. The notice is readily accessible and made available when personal information is first collected from the data subject.	Inspected applicable public privacy notices on SpinfexIT's website to determine whether they are readily accessible before the time personal information is collected.	No exceptions noted.
P1.1.2	The entity provides notice of its privacy practices to data subjects of the system. The Data Privacy Officer (DPO) is responsible for ensuring that the notice includes the following disclosures: ● Notification of a mechanism to opt-out of the collection and use of their personal information upon collection and upon changes to the purpose and use of personal information ● Policies regarding retention, sharing, disclosure, and disposal of their personal information ● The mechanism(s) to access, make changes to, or make inquiries regarding their personal information	Inspected the Privacy Policy, Terms of Service and Data Processing Addendum contained on the SpinfexIT website to determine that notice of privacy practices are communicated to data subjects and contain the applicable disclosures.	No exceptions noted.

Additional Criteria Group P2: Privacy Criteria Related to Choice and Consent

Additional Criteria Group P2.0 – Privacy Criteria Related to Choice and Consent			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
P2.1	**The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.**		
P2.1.1	Privacy notices containing information about choice and consent options include the following: ● Consent is obtained before the personal information is processed or handled. ● To ensure that consent is freely given, requests for consent are designed not to be deceptive intimidating or imply that failure to provide consent will result in significant negative consequences. ● Implicit consent has clear actions on how a data subject opts out. ● Action by a data subject to constitute valid consent.	Inspected the privacy notice process on SpinfexIT's website to determine whether choice and consent considerations are included.	No exceptions noted.
P2.1.2	The privacy notices are clear, comprehensive, and visible to users and it includes the purpose and intended use of the collected personal information, encompassing detailed use, consent, authorization, sharing, disclosure, access, security, retention, and disposal of personal information.	Inspected the Privacy Policy, Terms of Service and Data Processing Addendum publicly available on the SpinfexIT website to determine that the notice is clear and comprehensive.	No exceptions noted.

Additional Criteria Group P2.0 – Privacy Criteria Related to Choice and Consent			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
P2.1	**The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.**		
P2.1.3	The privacy staff meets periodically to discuss relevant privacy laws and regulations to determine whether they require the entity to obtain consent and reviews and updates the entity's policies for conformity to the requirements.	Inspected a sample of privacy meeting agendas to determine whether privacy laws and regulations are reviewed by privacy staff on a regular basis.	No exceptions noted.
P2.1.4	On an annual basis, the DPO reviews its policies to ensure the definition of "sensitive" personal information is properly delineated and communicated to personnel.	Inspected applicable policies and procedures to determine whether the DPO reviews privacy policies on an annual basis.	No exceptions noted.
P2.1.5	The entity provides updated training and awareness to personnel that includes defining what constitutes personal information and what personal information is considered sensitive.	Inspected training materials to determine whether information contains obligations related to personal information and what personal information is considered "sensitive."	No exceptions noted.

Additional Criteria Group P3: Privacy Criteria Related to Collection

Additional Criteria Group P3.0 – Privacy Criteria Related to Collection			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
P3.1	**Personal information is collected consistent with the entity's objectives related to privacy.**		
P3.1.1	Privacy-related complaints are investigated monthly to identify whether there were incidents of unfair or unlawful practices.	Inspected the data subject complaint process to ensure support personnel responded in a timely manner.	No privacy complaints were received by SpinfexIT and therefore, the control did not operate during the examination period.
P3.1.2	Members of the privacy staff determine whether personal information is collected only for the purposes identified in the terms of service agreement.	Inspected the terms of service agreement to determine if collection of information is defined and identified by SpinfexIT. Inquired of management to determine whether reviews of system change requests, privacy policies, and contracts are conducted on a routine basis to ensure personal information is not collected in excess of the necessary minimum.	No exceptions noted.
P3.1.3	Risk assessments are conducted to assess privacy related issues and implications of system changes.	Inspected the most recent risk assessment to determine whether changes are assessed for privacy implications to ensure the collection of information is consistent with privacy commitments.	No exceptions noted.

Additional Criteria Group P4: Privacy Criteria Related to Use, Retention, and Disposal

Additional Criteria Group P4.0 – Privacy Criteria Related to Use, Retention, and Disposal			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
P4.1	**The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.**		
P4.1.1	Privacy notices are reviewed periodically during privacy meetings to ensure that personal information is used in conformity with the privacy notice, consent received from the data subject, and applicable laws and regulations.	Inspected a sample of privacy meeting agendas to determine that privacy notices are being reviewed on a periodic basis.	No exceptions noted.
P1.1.2	The entity provides notice of its privacy practices to data subjects of the system. The Data Privacy Officer (DPO) is responsible for ensuring that the notice includes the following disclosures: ● Notification of a mechanism to opt-out of the collection and use of their personal information upon collection and upon changes to the purpose and use of personal information ● Policies regarding retention, sharing, disclosure, and disposal of their personal information ● The mechanism(s) to access, make changes to, or make inquiries regarding their personal information	Inspected the Privacy Policy, Terms of Service and Data Processing Addendum contained on the SpinfexIT website to determine that notice of privacy practices are communicated to data subjects and contain the applicable disclosures.	No exceptions noted.

Additional Criteria Group P4.0 – Privacy Criteria Related to Use, Retention, and Disposal			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
P4.2	**The entity retains personal information consistent with the entity's objectives related to privacy.**		
P4.2.1	Policies establish retention periods for information maintained by the organization.	Inspected the Data Processing Addendum to determine that retention periods are specified for all information maintained, and whether deleted information follows a procedure consistent with privacy commitments.	No exceptions noted.

Additional Criteria Group P5: Privacy Criteria Related to Access

Additional Criteria Group P5.0 – Privacy Criteria Related to Access			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
P5.1	**The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.**		
P5.1.1	Minimum password configuration requirements are established for all registered users of the Company's web application.	Inspected the password parameters required for registered users to authenticate to the SpinfexIT applications to determine whether the following password parameters have been established for the following attributes: • Minimum password length • Password complexity	No exceptions noted.
P5.1.2	When a registered user fails to enter an appropriate username and password access is denied to the system.	Performed a walkthrough, using a test account, of the authentication process for registered users of the SpinfexIT website to determine that if an incorrect username and password is entered, users will not be granted access to the system.	No exceptions noted.

Additional Criteria Group P6: Privacy Criteria Related to Disclosure and Notification

Additional Criteria Group P6.0 – Privacy Criteria Related to Disclosure and Notification			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
P6.1	**The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.**		
P6.1.1	The entity's application(s) provide for user interface (UI) screens that have a click button that captures and records a data subject's consent which encompasses the acknowledgement of sub-processors used by the entity.	Performed a walkthrough to determine data subjects are required to consent to SpinfexIT's Privacy Policy, Terms of Service, Cookie Policy and GDPR.	No exceptions noted.
P6.3	**The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.**		
P6.3.1	All incidents are logged, tracked, and communicated to affected parties by management until resolved.	Inspected a sample of IT security incident tickets to determine whether an incident response plan was initiated by authorized personnel, threats are mitigated, corrective action plans were documented, incidents were tracked until resolved, and an after-action report was prepared.	No security incidents were identified and therefore, the control did not operate during the examination period.
P6.3.2	Incident management procedures include instructions on how to escalate a suspected incident to the incident response team. The entity has a standard incident report template that must be completed for each incident.	Inspected the Incident Reporting Guidelines to determine whether there are procedures in place for when to contact the incident response team members. Inspected the Incident Reporting Guidelines to determine whether there is a standard incident report template that must be completed.	No exceptions noted.

Additional Criteria Group P6.0 – Privacy Criteria Related to Disclosure and Notification			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
P6.4	**The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.**		
P6.4.1	Contracts with vendors or other third parties are required in order to set up a vendor or other third party in the accounts payable system.	Inspected a sample of contracts with vendors or third parties from a list of those in the system to determine whether contracts are required before being set up in the system.	No exceptions noted.
P6.4.2	Vendors or other third parties are required to undergo a privacy and security assessment before the Company enters into a contract with those parties, and routinely thereafter, to confirm that control environments are consistent with the Company's commitments and system requirements and are in place.	Inspected the Vendor Management Program to determine whether privacy and security assessments are required before entering into contract with vendors.	No exceptions noted.
P6.5	**The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.**		
P6.5.1	Standard contractual templates are used for contracts involving personal information containing the requirement for an independent third-party assessment or the right to audit the vendor or third party.	Inspected the standard contract template for contracts involving personal information to determine whether there is a requirement for a third-party assessment or the right to audit the vendor.	No exceptions noted.

Additional Criteria Group P6.0 – Privacy Criteria Related to Disclosure and Notification			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
P6.5	**The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.**		
P6.5.2	Prior to contracting with vendors and other third parties, vendors and other third parties are required to sign a Data Processing Agreement. The agreement will outline specific instructions to the vendor and other third parties on who should be contacted in the event of a privacy or security incident as well as the timeframe in which the notification must occur.	Inspected a sample of executed Data Processing Agreements signed by third parties to determine whether vendors are required to notify SpinfexIT in the event of a privacy or security incident.	No exceptions noted.
P6.6	**The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.**		
P6.6.1	An incident identification and breach response procedure is documented that provides guidelines to determine whether an incident constitutes a breach. The procedure is communicated to personnel who handle personal information.	Inspected SpinfexIT's incident reporting guidelines to determine whether they detail what constitutes a breach, and how to respond to ensure procedures are in place.	No exceptions noted.
P6.6.2	Unauthorized uses and disclosures are documented and assessed by privacy staff.	Inspected a sample of incidents to determine whether incidents are tracked by management until resolved and closed incidents are reviewed by management for appropriate resolution.	No instances of unauthorized use or disclosure of client data were identified and therefore, the control did not operate during the examination period.

Additional Criteria Group P6.0 – Privacy Criteria Related to Disclosure and Notification			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
P6.6	**The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.**		
P6.6.3	Incident response procedures are reviewed on an annual basis to determine the procedures align with commitments and system requirements.	Inspected SpinifexIT's incident reporting guidelines to determine the procedures are reviewed periodically to ensure they are aligned with system requirements.	No exceptions noted.

Additional Criteria Group P7: Privacy Criteria Related to Quality

Additional Criteria Group P7.0 – Privacy Criteria Related to Quality			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
P7.1	**The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.**		
P7.1.1	Management performs an annual access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner.	Inspected the annual access review documentation to determine whether an access review was performed for in-scope system components and if tickets were created to remove inappropriate access.	No exceptions noted.
P7.1.2	A change request log exists to identify and provide notification within SpinfexIT when personal information within the IT systems is altered. Such alterations must be reviewed and approved by operations personnel prior to finalization of the records.	Inspected a sample of personal information alteration notifications to determine whether they were reviewed and approved before finalization of the record.	No instances of personal information alteration requests of client data were identified and therefore, the control did not operate during the examination period.

Additional Criteria Group P8: Privacy Criteria Related to Monitoring and Enforcement

Additional Criteria Group P8.0 – Privacy Criteria Related to Monitoring and Enforcement			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
P8.1	**The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.**		
P8.1.1	A process is in place to contact SpinfexIT with inquiries, complaints, and disputes.	Performed a walkthrough of the data subject complaint process to ensure support personnel responded in a timely manner.	No exceptions noted.
P8.1.2	Privacy complaints are documented and resolved in a timely manner.	Inspected a sample of customer privacy complaints to determine whether SpinfexIT reports and tracks all privacy related concerns.	No privacy complaints were received by SpinfexIT and therefore, the control did not operate during the examination period.
P8.1.3	The Steering Committee is responsible for evaluating customer privacy concerns and complaints, determining whether urgent reporting or remediation actions are required, and directly responding to customers on actions taken to address such concerns and complaints.	Inquired of management to determine whether SpinfexIT employees have been assigned responsibility of monitoring privacy, including concerns and complaints. Inspected a sample agenda from a Steering Committee meeting to determine whether privacy concerns are being evaluated.	No exceptions noted.
P8.1.4	Management maintains reports summarizing incidents, cause of incidents, and corrective actions plans.	Inspected a sample of incidents, incident response evaluations, and corrective action plans to determine an incident response procedure is in place and documents remediation of incidents.	No security incidents were identified and therefore, the control did not operate during the examination period.

Additional Criteria Group P8.0 – Privacy Criteria Related to Monitoring and Enforcement			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
P8.1	**The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.**		
P8.1.5	Policies and procedures are in place to monitor privacy controls and compliance with laws, regulations, and other requirements. Privacy staff monitor privacy developments to ensure compliance.	Inspected applicable privacy policies to determine whether procedures are in place to monitor privacy controls for compliance with privacy commitments.	No exceptions noted.
		Inspected a sample agenda from a Steering Committee meeting to determine whether privacy developments are evaluated.	

End of Report