System and Organization Controls (SOC) 2 Type I
Report on Management's Description of its

Internal Infrastructure

And the Suitability of Design of Controls Relevant to the Trust Services Criteria for Security

As of May 16, 2022

Together with
Independent Service Auditors' Report

SpearMC

We Support Our
Healthcare Professionals

Table of Contents

I. Independent Service Auditors' Report

Independent Service Auditors' Report

To the Management of SpearMC, Inc. (SpearMC)

Scope

We have examined SpearMC's accompanying description of its Internal Infrastructure titled "Description of SpearMC's Internal Infrastructure" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design of controls stated in the description as of May 16, 2022, to provide reasonable assurance that SpearMC's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

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

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

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

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other Matter

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

Opinion

In our opinion, in all material respects,

a. The description presents SpearMC's Internal Infrastructure that was designed and implemented as of May 16, 2022, in accordance with the description criteria.
b. The controls stated in the description were suitably designed as of May 16, 2022, to provide reasonable assurance that SpearMC service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date.

Restricted Use

This report is intended solely for the information and use of SpearMC, user entities of SpearMC's Internal Infrastructure as of May 16, 2022, business partners of SpearMC subject to risks arising from interactions with the Internal Infrastructure, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

San Jose, California
July 5, 2022

II. Assertion of SpearMC Management

Assertion of SpearMC Management

We have prepared the accompanying description of SpearMC's Internal Infrastructure system titled *"Description of SpearMC's Internal Infrastructure*" as of May 16, 2022, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the Internal Infrastructure system that may be useful when assessing the risks arising from interactions with SpearMC's system, particularly information about system controls that SpearMC has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

a. The description presents SpearMC's Internal Infrastructure system that was designed and implemented as of May 16, 2022, in accordance with the description criteria.

b. The controls stated in the description were suitably designed as of May 16, 2022, to provide reasonable assurance that SpearMC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date.

Signed by SpearMC Management

July 5, 2022

III. Description of SpearMC's Internal Infrastructure

Description of SpearMC's Internal Infrastructure

Company Background

SpearMC was founded in 2004, with the objective of being the thought leader, expert content provider and trusted advisor in combining business and technology competence to drive organizational performance. SpearMC is a technology and professional services firm that specializes in Oracle-PeopleSoft implementations, upgrades, optimization, and training.

SpearMC serves all industries.

SpearMC follows a balanced employee/contractor model to provide the specific skills and experience required by its clients. Its consulting specialists and vast network of business analysts, technical leads, and project managers, combine technical expertise, industry competence, and operations improvement that SpearMC leverages to custom-tailor solutions for each client. This model has allowed the company to quickly grow its revenue and asset base, while adhering to a strict cost structure. The company is based in California with satellite offices throughout the U.S.

SpearMC is an Oracle Partner, making it eligible to resell Oracle products. The company is Gartner Recognized in the 2022 Market Guide for Oracle Cloud Infrastructure Professional and Managed Services and has been ranked in both Inc. Magazine and the San Francisco Business Times as one of the fastest growing private companies in America.

Services Provided

SpearMC primarily provides services to its clients that include technology and management consulting, applications development, and technical training. SpearMC also designs and develops proprietary standard and custom-tailored training materials.

SpearMC's specific lines of business include:

- IT Consulting services
- IT Training services
- IT Managed services
- Software Resale

Products and services offered utilize the individual client's environment, not a SpearMC platform.

SpearMC will integrate client data, processes, and applications, in the client environment, to deliver fully functional solutions tailored to meet the client's business needs. Functional areas of expertise include:

- Human Capital Management – HCM
- Financial Management Systems – FMS
- Supply Chain Management – SCM
- Campus Solutions - CS
- Business Intelligence – BI

SpearMC works with its clients to understand the unique needs and requirements for their system to add efficiencies, improve system automation, eliminate redundant activities, improve operational performance, and often enhance customer service. SpearMC provides these services by accessing and working within the client environments and following all security protocols dictated by the client.

Client data is only accessed directly thru the client-controlled environment via client secured support tools and websites.

SpearMC communicates with clients via email.

Principal Service Commitments and System Requirements

SpearMC designs its processes and procedures, related to its services, to meet its objectives for its clients. Those objectives are based on the service commitments that SpearMC makes to its clients, the laws and regulations that govern the provision of SpearMC services, and the financial, operational, and compliance requirements that SpearMC has established for the services.

The technology and management consulting, applications development, and technical training services of SpearMC are subject to the security, confidentiality and privacy requirements as outlined in the individual client's-Confidentiality and Mutual Non-Disclosure Agreement(s) and/or as documented and communicated in Master Service Agreements (MSA) / Statement of Work (SOW) and other supplemental client agreements.

Security commitments, for client environments, are outlined and agreed upon by executing client specific compliance forms. Security commitments, internal to SpearMC, are governed by company's respective Information Security Policies for which both employees and contracted resources must adhere to.

SpearMC is a professional services firm that does not provide any equipment or software to its clients. SpearMC resources are granted remote access to client environments, generally following client specified incident management processes. Background checks are performed on all employees and sub-contractors (if required by client). Additionally, all resources are required to have their own client issued lap-tops in their possession.

SpearMC is an Oracle License Reseller and predominately relies on Oracle, Inc. to maintain their own vendor software. There is no internal change management, no vendor hosting, nor does any data flow through any SpearMC system(s). SpearMC does not transmit or store any client sensitive data. The software end user, or client, typically signs any security agreements directly with the software vendor.

SpearMC does not utilize any "on-premise" systems for its own business operations. All internal software, used for company business operations, is Software-as-a-Service "SaaS" based. Except for the Microsoft Windows operating system running on individual resource laptops, the Company does not deploy any networks for its internal business operations. SpearMC's software vendor(s) (i.e., Microsoft Office 365) hosts and maintains the servers, database, and code that make up the applications utilized by SpearMC. All software is accessed through ISP via web browser. Each employee has unique login credentials.

SpearMC requires Cyber security training, detailing, the handling of sensitive information and risks associate with connectivity to external networks, of its employees and long term contracted resources. Since SpearMC resources are given access to client environments, SpearMC resources will periodically go through security training, specific to the client and provided by the client.

SpearMC establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other procedural requirements, if and where applicable. Such requirements are communicated in SpearMC's company policies and procedures and contracts with clients. Information security policies define an organization-wide approach to how data is protected. These include policies and procedures around how services are delivered, how the internal business applications 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 internal processes required in the operation of SpearMC's Technology and Professional Services.

Components of the System

Infrastructure

Primary systems used for carrying out SpearMC's services includes the following:

Primary Systems		
Hardware	Type	Purpose
Laptops	Windows OS	SpearMC is a professional services firm. All resources have their own laptops. Resources are granted remote access to client environments such that access is managed by SpearMC's clients.

Software

Primary software used for carrying out SpearMC's services includes the following:

Primary Software		
Software	Operating System	Purpose
Office 365		SpearMC is a professional services firm. All resources use Office 365 applications on their laptops to communicate with their colleagues and clients.
Sage - Intacct		SaaS based internal software, used by accounting, for business operations, specifically financial and management reporting
ADP		SaaS based internal software, used by accounting, for business operations, specifically payroll data.
Nexonia		SaaS based internal software, used by accounting, for business operations, specifically time & expense reporting.
OCI "Demo" Grounds		Oracle "Demo" Environment hosted by Oracle used by SpearMC for demonstration purposes. "SaaS" solution provided by Oracle.
Jira		SaaS based application used for tracking and project management of issues for client projects.

Primary Software		
Software	Operating System	Purpose
Box.com		Box.com is a secure cloud content management and file sharing service used by SpearMC to create, store, share, edit, etc. company files.

People

SpearMC has 26 employees and has been in business for 17 years.

- Operations: Executives, managing directors, and company administrative support staff, including accounting and human resources. Performance reviews normally occur on an annual basis. Employees conduct a self-evaluation and then submit the completed form to their supervisor for his/her input. Pay adjustments are based on Company financial results and individual performance.
    - SpearMC evaluates candidates for relevant experience, skills, knowledge, qualifications, and education to ensure a proper fit with the job profile.
    - An interview is held with at least one SpearMC employee, to further determine fit of experience, skills, etc.
    - Subsequent verification process is comprised of three parts:
        - Background check
        - Reference check(s)
        - Corporate verification(s)

Sales/Delivery: SpearMC has a network of experienced consultants, who provide the specific skills and experience required by clients to manage their systems.

- SpearMC evaluates candidates for relevant experience, skills, knowledge, qualifications, and education to ensure a proper fit with the job profile.
- SpearMC will often vet the qualified applicant by key contacts within its network to assess reputation, competence, and soft skills.

- Part of this process is conducting a phone interview with at least one SpearMC representative to further determine fit of experience, skills, etc. and to identify what the candidate is looking for, their availability and rate.
- Once a candidate has been evaluated favorably, their resume is converted into SpearMC's format and submitted for client review.
- SpearMC coordinates the on-site interview and all related communications once selected by the client.
- Subsequent verification process is comprised of three parts:
  - Background check
  - Reference check(s)
  - Corporate verification(s)

- SpearMC follows a strict onboarding / offboarding checklist for all employee or contract resources.

Data

Internal SpearMC Systems – As noted above, SpearMC is a professional services firm and an Oracle License Reseller. The company predominately relies on Oracle, Inc. to maintain their own vendor software. There is no internal change management, no vendor hosting, nor does any client data flow through any SpearMC system(s)/network(s). SpearMC does not transmit, store, process or produce any client sensitive data within SpearMC internal environments. All internal SpearMC sensitive HR data is contained in ADP system. Only authorized SpearMC employees can access the ADP system.

Client Environments:
SpearMC is a professional services firm that does not provide any equipment or software to its clients. SpearMC resources are granted remote access to client environments, generally following client specified incident management processes. All client sensitive data remains in the client environment that is governed by client specific security protocols.

Processes, Policies and Procedures

There are limited formal IT policies and procedures, with respect to the physical security, logical access, computer operations, change control, and data communication as there are no SpearMC system/networks to physically secure, access, or operate.

Physical Security

SpearMC Headquarters: Key card entry is required at the company's headquarters in California, although the majority of SpearMC employees work from home. Except for individual laptops, which resources are required to always have in their possession, SpearMC does not have any on-premises facilities/systems/networks to physically secure.

SpearMC Resource Remote Locations: Each resource has unique login credentials and is required to always have their laptop in their possession. SpearMC utilizes a web-based model for its own business operations. The Company does not deploy any networks for its internal business operations. SpearMC's software vendor, Microsoft, hosts and maintains the servers, database, and code that make up the applications (i.e., Office 365) utilized by SpearMC. All software is accessed through ISP via web browser.

SpearMC requires two weeks' notice, from its employees, to allow for an orderly transition. Human Resources schedules an exit interview to collect any company property, review benefits information, and give a final paycheck. All company-owned property, including equipment, credit cards and/or client issued pass cards, must be returned immediately upon termination of employment. All unique login credentials, access to SpearMC email, as well as access to the company BOX.com account is disabled upon termination.

Client Site/Protocols: Physical access to client equipment and systems is managed according to the individual client's specified procedures and processes.

Logical Access

SpearMC Headquarters: Except for individual laptops, SpearMC does not have any on-premises facilities/networks/systems to protect via logical access controls.

SpearMC Resource Remote Locations: SpearMC utilizes a web-based model for its own business operations. All internal software, used for company business operations, is Software-as-a-Service "SaaS" based. Access to SpearMC's internal software is restricted by internal operations staff, depending on pre-defined roles, thru respective login permissions.

Except for the Microsoft /Windows operating system running on individual employee laptops, SpearMC does not have any on-premises software. The Company does not deploy any networks for its internal business operations. SpearMC's software vendor, Microsoft, hosts and maintains the servers, database, and code that make up the applications (i.e., Office 365) utilized by SpearMC. All software is accessed through ISP via web browser. Each employee and/or resource has unique login credentials.

SpearMC requires two weeks' notice, from its employees, to allow for an orderly transition. Human Resources schedules an exit interview to collect any company property, review benefits information, and

give a final paycheck. All company-owned property, including equipment, credit cards and/or client issued pass cards, must be returned immediately upon termination of employment. All unique login credentials, access to SpearMC email, as well as access to the company Box.com account is disabled upon termination.

Client Site/Protocols: Logical access to client equipment and systems is managed according to the individual client's specified procedures and processes. How resources access their client systems (i.e., through the use and authentication of VPN technology, etc.) is dependent on the individual client.

Computer Operations – Backups

SpearMC Headquarters:

SpearMC is an Oracle License Reseller and predominately relies on Oracle, Inc. to maintain their own vendor software. There is no internal change management, no vendor hosting, nor does any client data flow through any SpearMC system(s)/network(s). SpearMC does not transmit or store any client sensitive data, therefore there is no data to backup and/or trouble shoot.

SpearMC Resource Remote Locations: All SpearMC company files are maintained within SaaS applications. The individual third-party software vendors are responsible for backup management.

Client Site/Protocols: Client data is only accessed directly thru the client-controlled environment via client secured support tools and websites. Backup infrastructure would be maintained at the client, with physical access restricted according to applicable client policies.

Computer Operations – Availability

SpearMC Headquarters:

SpearMC is an Oracle License Reseller and predominately relies on Oracle, Inc. to maintain their own vendor software. There is no internal change management, no vendor hosting, nor is any client data stored or flowing through any SpearMC system(s) or network(s).

SpearMC Resource Remote Locations: All SpearMC company files are maintained within SaaS applications. The individual third-party software vendors are responsible for incident management.

Client Site/Protocols: SpearMC resources are guided by the individual client's specified incident response policies and procedures with respect to identifying, responding, and reporting to information technology incidents. System and/or infrastructure security breaches and other incidents are limited to the client site.

Change Control

SpearMC Headquarters: SpearMC is an Oracle License Reseller and predominately relies on Oracle, Inc. to maintain their own vendor software. There is no internal change management, no vendor hosting, nor is any client data stored or flowing through any SpearMC system(s) or network(s).

SpearMC Resource Remote Locations: All SpearMC company files are maintained within SaaS applications. The individual third-party software vendors are responsible for change control.

Client Site/Protocols: SpearMC employees and/or resources are guided by the individual client's specified change control policies and procedures.

Data Communications

SpearMC Headquarters: SpearMC is an Oracle License Reseller and predominately relies on Oracle, Inc. to maintain their own vendor software. There is no internal change management, no vendor hosting, nor is any client data stored or flowing through any SpearMC system(s) or network(s). Therefore, firewall or redundancy systems are not applicable.

SpearMC Resource Remote Locations: Not Applicable

SpearMC utilizes a web-based model for its own business operations. All internal software, used for company business operations, is Software-as-a-Service "SaaS" based. Access to SpearMC's internal software is restricted by internal operations staff, depending on pre-defined roles, thru respective login permissions.

Except for the Microsoft /Windows operating system running on individual employee laptops, SpearMC does not have any on-premises software. The Company does not deploy any networks for its internal business operations. SpearMC's software vendor, Microsoft, hosts and maintains the servers, database, and code that make up the applications (i.e., Office 365) utilized by SpearMC. All software is accessed through ISP via web browser. Each employee and/or resource has unique login credentials

Client Site/Protocols: SpearMC employees and/or resources are authorized to access the client system(s) following the individual client's authentication specified policies and procedures.

The applicable trust services criteria and the related controls

Common Criteria (Security)
Security refers to the protection of information during its collection or creation, use, processing, transmission, and storage and systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Control Environment

Integrity and Ethical Values

As trusted advisors to its clients, integrity and ethical values are essential elements of SpearMC's control environment. Integrity and ethical behavior are the product of SpearMC's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. This includes management's actions to reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. This includes the communication of Company values and behavioral standards to personnel through policy statement(s) and codes of conduct, as well as setting good examples.

Specific control activities that SpearMC has implemented in this area are described below:
Employees:

- Formally, documented organizational policy statement(s) including an information security policy and code of conduct that communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
- Background checks, reference checks, and corporate verifications are performed as a component of the hiring process that may also require drug testing.

Commitment to Competence

SpearMC's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' and contractors' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for various jobs and how those levels translate into skills and knowledge.

Specific control activities that SpearMC has implemented in this area are described below:

- Management has considered the competence levels for jobs and translated required skills and knowledge levels into written position requirements.
- SpearMC evaluates candidates for relevant experience, skills, knowledge, qualifications, and education to ensure a fit with the job profile.
- Employees and contractors are encouraged to, and do, regularly attend training seminars to both maintain and grow their knowledge and skillsets.
- Management, via bonus opportunities, encourages employees to present at conferences, webinars, user group, etc., and earn Oracle certifications.

Management's Philosophy and Operating Style

SpearMC's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing accounting functions, and personnel.

Specific control activities that SpearMC has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held on a weekly basis to discuss major initiatives and issues that affect the business.
- Firm-wide meetings are held monthly to discuss major initiatives and issues that affect the business.

Organizational Structure and Assignment of Authority and Responsibility

SpearMC's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility.

An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its smaller size and the nature of its activities.

SpearMC's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- A Business Operations Manual (BOM) designed to provide an understanding of SpearMC's operation structure and back-office processes.
- BOM is a living document whose content is reviewed and updated accordingly, on an annual basis by the Operations team to remain current with organizational changes and business processes.
- An organizational chart is in place to communicate key areas of authority and responsibility.

Human Resource Policies and Practices

SpearMC's human resource policies and practices relate to both employee and outsourcing/contractor hiring, orientation, training, evaluation, and compensation. SpearMC's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel to support internal operations and our clients.

Employees: Executives, directors, managers, consultants and administrative staff.

Contractors: Large network of experienced consultants, specialists, and subject matter experts. This is the foundation of SpearMC's sourcing and delivery efforts and successes. Speed of staffing is exceptionally fast while maintaining a high level of quality.

Specific control activities that the service organization has implemented in this area are described below:

Employees:

- Candidates are evaluated for relevant experience, skills, knowledge, qualifications, and education to ensure a proper fit with the job profile.
- Subsequent verification process is comprised of three parts:
    - Background check
    - Reference checks
    - Corporate verifications
- New employees are required to sign acknowledgement forms for the employee handbook (includes code of conduct) and a confidentiality agreement following new hire orientation on their first day of employment.
- Performance evaluations and compensation review for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in an off-boarding checklist.

Contractors:

- Candidates are evaluated for relevant experience, skills, knowledge, qualifications, and education to ensure a proper fit with the job profile.
- Candidates are vetted by key contacts within SpearMC's network to assess reputation, competence and skills including a phone interview with at least one SpearMC.
- Subsequent verification process is comprised of three parts:
    - Background check
    - Reference checks
    - Corporate verifications
- Contractors are required to sign acknowledgement forms including a code of conduct and a confidentiality agreement on their first day of employment.
- Contractor termination procedures are in place to guide the termination process and are documented in an off-boarding checklist.

Risk Assessment Process

This process has identified risks resulting from the nature of the services provided by SpearMC. SpearMC's risk assessment process identifies and manages risks that could potentially affect SpearMC's ability to provide reliable services to clients. This ongoing process requires that management identify significant risks, inherent in services, as they oversee their areas of responsibility.

Management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk – changes in the environment, management, and SpearMC's network of consultants, specialists and subject matter experts utilized for outsourcing.
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance – legal and regulatory changes

SpearMC has hired a Risk and Compliance Manager who is responsible for assisting management in identify potential risks to the company and monitoring the operation of SpearMC's internal controls. The role is intended to align the company's strategy more closely with its key stakeholders and maximize opportunities in the rapidly changing market environment. SpearMC attempts to actively identify and mitigate significant risks through the continuous communication between its directors and executives.

<u>Integration with Risk Assessment</u>

The environment in which the Company operates; the commitments, agreements, and responsibilities of SpearMC's Technology and Professional Services Firm; as well as the nature of the components of the Firm result in risks that the criteria will not be met. SpearMC addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because every company, and the environment in which it operates is unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the firm, SpearMC's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication is an integral component of SpearMC's internal control system. It is the process of identifying and exchanging information in the form and time frame necessary to conduct, manage, and control the company's operations.

This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, staffing, tracking, and monitoring individual client projects, or project management. At SpearMC, information is identified and communicated thru conversations with clients, vendors and employees.

Monthly calls are held to discuss and disseminate any new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, company-wide outings, as well as a more formal, quarterly, and annual company-wide gathering, are held in various geographic locations to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the gatherings with information gathered from various industry seminars and external informational databases as well as well conversations with various internal and external colleagues. General updates to company-wide security policies and procedures are usually communicated to the appropriate SpearMC personnel via e-mail messages.

Specific information is used to support SpearMC's Information and Technology Firm are described in the Description of Services section above.

Monitoring Controls

Operation Management team monitors operational controls to ensure that they are operating as intended and that controls are modified as conditions change. Employee activity and adherence to company policies and procedures is also monitored. Necessary corrective actions are taken, as required, to correct deviations from company policies and procedures. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

<u>On-Going Monitoring</u>

SpearMC's management will initiate corrective action through company meetings, internal conference calls, and informal notifications.

Management's close involvement in SpearMC's operations helps to identify variances from expectations regarding internal controls. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of SpearMC's employees and contractors.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Criteria Not Applicable to the System

All relevant trust services criteria were applicable to SpearMC's Internal Infrastructure.

Subservice Organizations

SpearMC, Inc.'s services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to SpearMC's services to be solely achieved by SpearMC's control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of SpearMC.

The following subservice organization controls should be implemented by Microsoft to provide additional assurance that the trust services criteria described within this report are met.

Subservice Organization – Microsoft O365 & Azure		
Category	Criteria	Control
Common Criteria / Security	CC6.4	Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established.
		Security verification and check-in for personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors, are required.
		Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		The datacenter facility is monitored 24x7 by security personnel.

Subservice Organization – Microsoft O365 & Azure		
Category	Criteria	Control
Common Criteria / Security	CC6.7	Data in motion is encrypted when transmitting data between the customer and the data center and between data centers.
Common Criteria / Security	CC7.2	Each Service team has on-call personnel who respond to potential Security, Availability, Confidentiality, and Processing Integrity incidents. If an incident is assigned a high severity, the O365 Security team will track and address the issues to resolution.
Common Criteria / Security	CC7.2	Security events escalated to the Security team are reviewed by the Security Incident Response Team and action is taken in accordance with the established incident response program procedures.

SpearMC, Inc. management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, SpearMC, Inc. performs monitoring of the subservice organization controls, including the following procedures

- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

Complementary User Entity Controls

SpearMC's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the SOC 2 Criteria related to SpearMC's services to be solely achieved by SpearMC's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of SpearMC's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the SOC 2 Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to SpearMC.
2. User entities are responsible for notifying SpearMC of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of SpearMC services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize SpearMC services.
6. User entities are responsible for providing SpearMC with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying SpearMC of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

IV. Description of Design of Controls and Results Thereof

Description of Design of Controls and Results Thereof

Relevant trust services criteria and SpearMC related controls are an integral part of management's system description and are included in this section. Sensiba San Filippo LLP performed testing to determine if SpearMC controls were suitably designed to achieve the specified criteria for the Security set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria)*, as of May 16, 2022.

Control Number	Description of SpearMC Controls	Results
CC1.0 - Control Environment		
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.		
CC1.1.1	Entity has a documented code of conduct with defined sanctions for violations and all personnel, including contract employees, are required to read and acknowledge upon hire.	Controls is suitably designed.
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
CC1.2.1	The company demonstrates a commitment to integrity and ethical values by completing an annual review of ethical management and hiring practices.	Control is suitably designed
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
CC1.3.1	Management evaluates its organizational structure, delegates authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties, as necessary, at the various levels of the organization.	Control is suitably designed

Control Number	Description of SpearMC Controls	Results
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
CC1.4.1	The entity considers the technical competency of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.	Control is suitably designed
CC1.4.2	Background checks are performed on new hires before the new hire's start date, as permitted by local laws. The results are reviewed by HR and appropriate action is taken if deemed necessary.	Control is suitably designed
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
CC1.5.1	Management has established a privacy and information security policy to help employees understand their obligations and responsibilities to comply with the Company's security policies and procedures, including the identification and reporting of incidents requiring signature for acknowledgement for full-time employees and contractors (where applicable).	Control is suitably designed
CC1.5.2	Management performs annual performance reviews for all employees to communicate responsibilities and accountability and to provide incentives, rewards and to implement corrective measures as necessary.	Control is suitably designed
CC2.0 - Communication and Information		
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
CC2.1.1	Entity's internal software applications produces data that is accurate, complete, accessible, protected and retained.	N/A - The control is carved out and the responsibility of subservice organization.

Control Number	Description of SpearMC Controls	Results
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
CC2.2.1	Entity has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki or Intranet, and accessible to all employees.	Control is suitably designed
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.		
CC2.3.1	Entity maintains a Privacy Policy that is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments.	Control is suitably designed
CC2.3.2	Entity maintains a Terms of Service that is available to all contracted clients and internal employees, and the terms detail the company's security commitments.	Control is suitably designed
CC3.0 - Risk Assessment		
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
CC3.1.1	The entity has defined and implemented a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances	Control is suitably designed
CC3.2 - COSO Principle 7: 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.		
CC3.2.1	The entity maintains a risk register that continuously documents risks facing the company and in-progress remediation programs to address those risks.	Control is suitably designed

Control Number	Description of SpearMC Controls	Results
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
CC3.3.1	As part of its ongoing risk assessment, entity considers and addresses potential fraud activity (e.g., fraudulent reporting, loss of assets, unauthorized acquisitions, etc.)	Control is suitably designed
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.		
CC3.4.1	As part of its ongoing risk assessment, entity considers potential impacts of new business lines, altered business lines, acquisitions or divested operations on the system of internal control.	Control is suitably designed
CC4.0 - Monitoring Activities		
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
CC4.1.1	Management requires malware detection software on all endpoint devices that can access company systems and resources and is configured to perform daily scans and update virus signatures regularly.	Control is suitably designed
CC4.1.2	Management holds formal, monthly meetings, to discuss any incidents, root causes of incidents, and corrective action plans. Management follows-up for completion of corrective action plans, when applicable.	Control is suitably designed
CC4.2 - COSO Principle 17: 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.		
CC4.2.1	Management holds formal, monthly meetings, to discuss any incidents, root causes of incidents, and corrective action plans. Management follows-up for completion of corrective action plans, when applicable.	Control is suitably designed

Control Number	Description of SpearMC Controls	Results
CC5.0 - Control Activities		
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
CC5.1.1	The entity maintains a risk register that continuously documents risks facing the company and in-progress remediation programs to address those risks.	Control is suitably designed
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.		
CC5.2.1	As part of its ongoing risk assessment, entity considers potential impacts of new business lines, altered business lines, acquisitions or divested operations on the system of internal control.	Control is suitably designed
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
CC5.3.1	The entity has defined and implemented a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances	Control is suitably designed
CC5.3.2	Management has established a privacy and information security policy to help employees understand their obligations and responsibilities to comply with the Company's security policies and procedures, including the identification and reporting of incidents requiring signature for acknowledgement for full-time employees and contractors (where applicable).	Control is suitably designed

Control Number	Description of SpearMC Controls	Results
CC6.0 - Logical and Physical Access Controls		
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
CC6.1.1	Access to company resources and software is limited to appropriate personnel and based on role.	Control is suitably designed
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
CC6.2.1	New hire checklist are formally documented and approved by appropriate personnel, prior to access being granted.	Control is suitably designed
CC6.2.2	Terminated user checklist are formally documented to ensure that access revocation occurs in a timely manner.	Control is suitably designed
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
CC6.3.1	Access to company resources and software is limited to appropriate personnel and based on role.	Control is suitably designed
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
CC6.4.1	The Company relies on subservice organizations physical and environmental controls, as defined and tested within their SOC 2 efforts.	N/A - The control is carved out and the responsibility of subservice organization.

Control Number	Description of SpearMC Controls	Results
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.		
CC6.5.1	Procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.	Control is suitably designed
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
CC6.6.1	Access to company resources and software is limited to appropriate personnel and based on role.	Control is suitably designed
CC6.6.2	All personnel are required to access systems and resources with a unique ID & password. Password configurations and complexity are specified by management.	Control is suitably designed
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		
CC6.7.1	SpearMC leverages subservice organizations data in transit standards as defined and tested within their SOC 2 efforts.	N/A - The control is carved out and the responsibility of subservice organization.
CC6.7.2	Procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.	Control is suitably designed
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
CC6.8.1	Management requires malware detection software on all endpoint devices that can access company systems and resources and is configured to perform daily scans and update virus signatures regularly.	Control is suitably designed

Control Number	Description of SpearMC Controls	Results
CC7.0 - System Operations		
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		
CC7.1.1	Management requires malware detection software on all endpoint devices that can access company systems and resources and is configured to perform daily scans and update virus signatures regularly.	Control is suitably designed
CC7.1.2	Incident response procedures are in place to guide personnel when a potential breach or suspicious activities are detected. Identified security incidents are reported and acted upon by appropriate personnel.	Control is suitably designed
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
CC7.2.1	Management requires malware detection software on all endpoint devices that can access company systems and resources and is configured to perform daily scans and update virus signatures regularly.	Control is suitably designed
CC7.2.2	Incident response procedures are in place to guide personnel when a potential breach or suspicious activities are detected. Identified security incidents are reported and acted upon by appropriate personnel.	Control is suitably designed
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		
CC7.3.1	Security personnel review identified security events to determine impact and to recommend remediation, if necessary.	N/A - The control is carved out and the responsibility of subservice organization.

Control Number	Description of SpearMC Controls	Results
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		
CC7.3.2	Incident response procedures are in place to guide personnel when a potential breach or suspicious activities are detected. Identified security incidents are reported and acted upon by appropriate personnel.	Control is suitably designed
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
CC7.4.1	Incident response procedures are in place to guide personnel when a potential breach or suspicious activities are detected. Identified security incidents are reported and acted upon by appropriate personnel.	Control is suitably designed
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.		
CC7.5.1	As part of its incident response plan, procedures are in place to recover from security incidents, including restoring any affected software or systems, as needed.	N/A - The control is carved out and the responsibility of subservice organization.
CC8.0 - Change Management		
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		
CC8.1.1	SpearMC uses manufacturer auto-update configurations for assets to ensure patches are applied timely.	Control is suitably designed

Control Number	Description of SpearMC Controls	Results
CC9.0 - Risk Mitigation		
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
CC9.1.1	As part of its risk management process, entity has developed a written business continuity plan with procedures to follow to limit potential business disruptions.	Control is suitably designed
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.		
CC9.2.1	As part of its risk assessment process, management reviews the annual SOC report for its primary vendor to confirm that outsourced controls are appropriately designed and operating effectively.	Control is suitably designed
CC9.2.2	The company has a formally documented Vendor Management Policy that outlines procedures for managing vendor relationships.	Control is suitably designed