# System and Organization Controls 2 (SOC 2) Type II Report

Description of *"NeoNiche Integrated Solutions Pvt Ltd - Event Management Company"* relevant to Security, Availability, Processing Integrity Privacy and Confidentiality
As of July 20th, 2024

# (SSAE 21 – SOC 2 Type II Report)

# Section I
# Management Assertion Letter

We have prepared the accompanying description of *NeoNiche Integrated Solutions Pvt. Ltd.'s* system; titled ***"Event Management, Brand Activation, Creative Services, Integrated Marketing, Digital Marketing, MICE, Technical Solutions & Production Management"*** As on July 20th, 2024 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 Type II Report*** (AICPA, Description Criteria)

The description is intended to provide report users with information about the ***"Event Management, Brand Activation, Creative Services , Integrated Marketing, Digital Marketing , MICE , Technical Solutions & Production Management"*** that may be useful when assessing the risks arising from interactions with, particularly information about the system controls that *NeoNiche Integrated Solutions Pvt. Ltd  has* designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved. These are based on the trust services criteria relevant to Confidentiality, Integrity and Availability as set forth in TSP section 100, ***2017*** AICPA, Trust Services Criteria.

The description includes only the controls of ***NeoNiche Integrated Solutions Pvt. Ltd.*** And excludes controls of the subservice organizations. The description also indicates that certain trust services criteria specified therein can be met only if the subservice organizations' controls contemplated in the design of ***NeoNiche Integrated Solutions Pvt. Ltd.*** controls are suitably designed and operating effectively, along with related controls at ***NeoNiche Integrated Solutions Pvt. Ltd.***

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ***NeoNiche Integrated Solutions Pvt. Ltd.,*** to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents ***NeoNiche Integrated Solutions Pvt. Ltd.'s*** *c*ontrols, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ***NeoNiche Integrated Solutions Pvt. Ltd.'s*** controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at ***NeoNiche Integrated Solutions Pvt. Ltd.***, to achieve ***NeoNiche Integrated Solutions Pvt. Ltd.'s*** service commitments and system requirements based on the applicable trust services criteria. The description presents ***NeoNiche Integrated***

***Solutions Pvt. Ltd.'s*** controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of ***NeoNiche Integrated Solutions Pvt. Ltd.'s*** controls.

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

A. The description fairly presents the ***"Event Management, Brand Activation, Creative Services, Integrated Marketing, Digital Marketing, MICE, Technical Solutions & Production Management"*** throughout the period as on July 20th, 2024 based on the following description criteria:

The description contains the following information:

1. The types of services provided:
2. The principal service commitments and system requirements:
3. The components of the system used to provide the services, which are as follows:

a. **Infrastructure**. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks).
b. **Software**. The application programs and IT system software that support application programs (operating systems, middleware, and utilities).
c. **People**. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
d. **Procedures**. The automated and manual procedures in the operation of a system.
e. **Data**. The information used and supported by a system (Transaction streams, files, databases, tables, and output used or processed by the system).

4. For identified system incidents that (a) were the result of controls that were not suitably designed or operating effectively or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements, as of the date of the description the following information:

a. Nature of each incident
b. Timing surrounding the incident
c. Extent (or effect) of the incident and its disposition

5. The applicable trust services criteria and the related controls designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.

6. If service organization management assumed, in the design of the service organization's system, that certain controls would be implemented by user entities, and those controls are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved, those complementary user entity controls (CUECs)
7. If the service organization uses a subservice organization and the controls at the subservice organization are necessary, in combination with controls at the service organization, to provide
8. trust services criteria that are intended to be met by controls at reasonable assurance that the service organization's service commitments and system requirements are achieved, the following:

a. The nature of the service provided by the subservice organization
b. Each of the applicable the subservice organization
c. The types of controls that service organization management assumed, in the design of the service organization's system, would be implemented by the subservice organization that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved (commonly referred to as complementary subservice organization controls or CSOCs)

9. Any specific criterion of the applicable trust services criteria that is not relevant to the system and the reasons it is not relevant.
10. There were no significant effects of COVID-19 epidemic spate on the ***NeoNiche Integrated Solutions Pvt. Ltd.***, its operations and the technologies used. In fact, there have not been any significant changes in the business process execution as well. The technologies that were used before the pandemic period have been extended and applied to all the operating staff irrespective of the fact whether they work on the client's environment using client's resources or ***NeoNiche Integrated Solutions Pvt. Ltd.'s*** systems and resources. With the advent in technology, physical presence of operating staff has not been a cause for concern while performing the operations efficiently and effectively by allowing them to work remotely.
11. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and not, therefore, include every aspect of the system that each individual user considers important to his or her own particular needs.

B. The controls stated in the description were suitably designed as on July 20th, 2024 to provide reasonable assurance that ***NeoNiche Integrated Solutions Pvt. Ltd.'s*** service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as on July 20th, 2024 and if the subservice organization and user entities applied the complementary controls assumed in the design of ***NeoNiche Integrated Solutions Pvt. Ltd.'s*** controls as on July 20th, 2024.

C. ***NeoNiche Integrated Solutions Pvt. Ltd.*** **Controls** stated in the description were operated effectively as on July 20th, 2024 to achieve ***NeoNiche Integrated Solutions Pvt. Ltd.'s*** service commitments and system requirements based on the applicable trust services criteria, if its controls operated effectively as on July 20th, 2024 and if the subservice organization and user entities applied the complementary controls assumed in the design of ***NeoNiche Integrated Solutions Pvt. Ltd.'s*** controls as on July 20th, 2024.

VALAY
JIGNESH
LAKDAWALA

Digitally signed by
VALAY JIGNESH
LAKDAWALA
Date: 2024.09.02
18:33:11 +05'30'

***Name : Valay Lakdawala***
***Title : Co Founder & Director***
***NeoNiche Integrated Solutions Pvt. Ltd .***
***Date: 15th July 2024***

CYBORGENIC

# Section II

# Independent Service Auditor’s Report

**To,**
**Prateek N Kumar**
**Founder & CEO**
**NeoNiche Integrated Solutions Pvt. Ltd.**

***Scope***

We have examined ***NEONICHE's*** accompanying description in ***Section III*** titled " ***Event Management, Brand Activation, Creative Services , Integrated Marketing, Digital Marketing , MICE , Technical Solutions & Production Management***" as on 20th July 2024, 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* and the suitability of the design and operating effectiveness of controls stated in the description throughout the as on 20th July 2024 to provide reasonable assurance that ***NEONICHE'S*** service commitments and system requirements were achieved based on the trust services criteria relevant to ***Security, Availability, Confidentiality , Privacy and Processing Integrity*** ( applicable trust services criteria) set forth in **TSP Section 100, 2017** as per AICPA, Trust Services Criteria.

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ***NEONICHE***, to achieve ***NEONICHE'S*** service commitments and system requirements based on the applicable trust services criteria. The description presents ***NEONICHE'S*** controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ***NEONICHE'S*** controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at ***NEONICHE***, to achieve ***NEONICHE'S*** service commitments and system requirements based on the applicable trust services criteria. The description presents ***NEONICHE'S*** controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of ***NEONICHE'S*** controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

The information included in ***Section V, "Other Information Provided by NEONICHE"*** that is not covered by this Auditor's Report, is presented by ***NEONICHE'S*** management to provide additional information and is not a part of ***NEONICHE'S*** description. Information about ***NEONICHE'S*** management responses to exceptions identified in the report and glossary of terms has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve ***NEONICHE'S*** service commitments and system requirements based on the applicable trust services criteria and accordingly, we express no opinion on it.

**Service Organization's responsibilities**

***NEONICHE*** 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 ***NEONICHE'S*** service commitments and system requirements were achieved. In ***Section II***, ***NEONICHE*** has provided its assertion titled ***"Assertion of NEONICHE Management"*** about the description and the suitability of design and operating effectiveness of controls stated therein. ***NEONICHE*** 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 auditor's responsibilities**

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness 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 and operated effectively 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 and operating effectiveness 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 or did not operate effectively;
- 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 the applicable trust services criteria if those controls operated effectively;
- Testing the operating effectiveness of controls stated in the description 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.

**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 each individual report user may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

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

The physical distancing and restriction on interstate movement due to COVID-19 epidemic has posed a real threat and challenge as the data collection, correspondence, interviewing the auditee, presentations etc., being done virtually. Lack of personal interaction with the attendee and not making physical visits to the premise could potentially limit the scope of audit. We were unable to determine whether changes in the system processes and resources might have been warranted in respect of effectiveness and efficiency of system of internal controls.

**Description of tests of controls**

The specific controls we tested, and the nature, timing, and results of those tests are presented in ***Section IV***, ***"Trust Services Security Criteria, Related Controls, and Tests of Controls,"*** of this report in columns 2***, 3, and 4*** respectively.

**Opinion**

In our opinion, in all material respects,

a. the description presents ***NEONICHE'S*** **"Content Management, Data Collection & Analytics and Machine Learning Services"** that was designed and implemented as on 20th July 2024, in accordance with the description criteria.

b. the controls stated in the description were suitably designed as on 20th July 2024, to provide reasonable assurance that ***NEONICHE'S*** service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of ***NEONICHE'S*** controls throughout that period.

c. the controls stated in the description operated effectively as on 20th July 2024, to provide reasonable assurance that ***NEONICHE'S*** service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of ***NEONICHE'S*** controls operated effectively throughout that period.

**Restricted Use**

This report, including the description of tests of controls and results thereof in ***Section IV,*** is intended solely for the information and use of ***NEONICHE***, user entities of ***NEONICHE'S*** **"Content Management, Data Collection & Analytics and Machine Learning Services"** during some or all of the period as on 20th July 2024 business partners of ***NEONICHE*** that were subject to risks arising from interactions with the ***NEONICHE'S*** **"Event Management, Brand Activation, Creative Services Integrated Marketing, Digital Marketing , MICE , Technical Solutions & Production Management"**, 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; and
- 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.

CPA Name: - Mr. Jay Maru

License No.: - 41401

Jay Dhiraj Maru

Digitally signed by Jay Dhiraj Maru
Date: 2024.09.03
11:37:39 -04'00'

July 20th, 2024

Mumbai, India.

# Section III

# Description of the NeoNiche Integrated Solutions Pvt Ltd - Event Management Company.

***"Event Management, Brand Activation, Creative Services Integrated Marketing, Digital Marketing, MICE, Technical Solutions & Production Management"***

As of July 20th, 2024

## A. Background and Overview of Services

NEONICHE's intuitive, modular platform uses 21st-century paradigms. This way, you can avoid making expensive errors and monitor the overall Evet management situation. The platform offers a complete solution for managing the *Event Management, Brand Activation, Creative Services, Integrated Marketing, Digital Marketing, MICE, Technical Solutions & Production Management Services*.

NEONICHE was established with the sole intention of providing every organisation with tools at a reasonable cost. Their aim to make sure that every organisation has access to the technology they need to succeed. And they will here to give them those resources.

Their products and services assist businesses in reducing tedious, time-consuming chores and freeing up important resources. Client teams may automate time-consuming operations like data entry to save time and effort while achieving more.

NEONICHE is in the business of providing *Event Management, Brand Activation, Creative Services, Integrated Marketing, Digital Marketing, MICE, Technical Solutions & Production Management Services*.

### A.1.Subservice Organizations

Subservice providers used by NEONICHE are not covered by the purview of this analysis.

**AWS Server:**

**GoDaddy:**

**Big Rock**

**INfiflex**

**Outsourced tech partners and vendors:** to offer services and assistance for software development

### A.2. Boundaries of the System

The list that follows contains the precise goods, services, and areas that fall under the report's purview. Not included are any additional goods, services, or places.

<table>
<tr><th colspan="2">Products and Services in Scope</th></tr>
<tr><td colspan="2">The scope of this report is limited to <i>Event Management, Brand Activation, Creative Services, Integrated Marketing, Digital Marketing, MICE, Technical Solutions &amp; Production Management</i> Products<br><b>Services</b><br><i>Event Management, Brand Activation, Creative Services, Integrated Marketing, Digital Marketing, MICE, Technical Solutions &amp; Production Management</i></td></tr>
<tr><th colspan="2">Geographic Locations in Scope</th></tr>
<tr><td><b>Office Location</b></td><td><b>Registered Address</b></td></tr>
<tr><td>Mumbai</td><td>101A, 1st floor DTC Building, Sitaram Mills Compound, NM Joshi Marg, Lower Parel, Mumbai, Maharashtra 400011</td></tr>
</table>

The report excludes all processes and activities that are executed outside above locations. Unless otherwise mentioned, the description and related controls apply to locations covered by the report.

### A.3. Control Environment

The internal control environment at NEONICHE reflects management's overall perspective on the value of controls, as well as their understanding of that value and actions. It also shows how controls are prioritised within the organization's policies, practises, and methodologies.

In accordance with its strategic business goals, the Chief Executive Officer, Senior Management Team, and all employees are committed to building and running a successful information security management system. The management of NEONICHE is dedicated to the Information Security Management System and makes sure that IT policies are communicated, understood, upheld, and maintained at all organisational levels. They also conduct frequent reviews to ensure that they remain appropriate.

## A.4. Integrity and Ethical Values

Directors, officers, and employees of NEONICHE are expected to uphold high standards of professional and personal ethics when performing their jobs and fulfilling their responsibilities. The company's guiding principles are honesty and integrity, and all workers are required to carry out their duties in accordance with these principles and adhere to all relevant laws and regulations. When an ethics violation occurs, NEONICHE encourages open discussion and has established a setting where employees are shielded from any form of retaliation. Investigations into all reported infractions and, when necessary, corrective action are the sole purview of executive management.

### A.4.1. Board of Directors

The Board of Directors oversees all business operations at NEONICHE. Prateek N Kumar, the company's Founder, serves as CEO, and VALAY LAKDAWALA & ASHISH SEDANI, Co-Founder, are on the Board of Directors.

## A.5.Management’s Philosophy and Operating Style

The NEONICHE Executive Management team evaluates risks before starting new commercial ties and collaborations and is responsible for the day-to-day operations of the organization and is committed for providing quality, accurate and timely service to its clients. Employees follow workflow practices and internal control procedures in order to achieve the highest standards of client satisfaction. The management oversees and guides the organization and its business. The basic responsibility of the management is to exercise business judgment to act in what will be reasonably in the best interests of the organization. The management also considers the organization’s ethical behaviour and the interests of the organization clients, employees, and communities in which it functions.

## B. Risk Management and Risk Assessment

NEONICHE recognizes that risk assessment is a critical component of its operations which helps to ensure that its clients are properly served and corporate assets are properly managed. The foundation of this process is management’s knowledge of its operations, its close working relationship with its clients, and its understanding of the industry in which it operates.

At NEONICHE, the ability to identify, measure, and manage risk is embedded in the security management framework, control systems and reporting mechanisms. The risk management practices implemented by NEONICHE consist of internal controls derived from its policies, processes, personnel, and systems.

The CISO, Operations Head and IT Manager are responsible for monitoring risk levels on various parameters and the management ensures implementation of risk mitigation measures. Formal reporting and control mechanisms are in place to provide timely information and to facilitate proactive risk management. For any significant risks identified, NEONICHE management is responsible for implementing appropriate measures to monitor and manage these risks (e.g., implementing/revising control procedures).

### *Information Security Policies*

A company-wide set of NEONICHE information security policies has been created.

All employees have access to pertinent and crucial Security Policies (IS Policies) via the shared network or shared drive. Before being put into effect, changes to the information security policies are reviewed by the head of operations and approved by the director or CISO.

## C. Monitoring

Internal control monitoring is crucial to determining whether their controls are working as intended and whether they have been changed appropriately to account for changes in the environment in which their business is operated. Monitoring their effectiveness of internal controls is a regular task for management and information security staff at NEONICHE. NEONICHE employs a variety of monitoring technologies, such as Uptime Robot for application and website uptime, as well as inbuilt real-time monitoring tools for the many sub-services (AWS, Git, MongoDB, Auth0, SendGrid, mail services) utilised for the application.

## D. Information and Communication

For each main work group, NEONICHE has processes in writing that encompass the key duties and activities. Policies and procedures are evaluated and changed in response to modifications and management approval. As part of their routine duties, departmental managers check that NEONICHE policies and procedures are being followed.

To detect and handle service issues, customer difficulties, and project management issues, NEONICHE management holds departmental status meetings in addition to strategic planning meetings. Each service has a designated service manager who serves as the main point of contact for communications pertaining to service activities. If processing or system development issues have an impact on client organisations, there are also individuals who have been designated to interface with the customer. To deliver timely information, electronic messaging has been included into several of NEONICHE's procedures.

### D.1. Internal & External Communication

NEONICHE’s management has established an organizational structure and an established communication mechanism using different modes of communication such as e-mail and trainings to help facilitate the communication of important business information with all its employees on a timely basis.

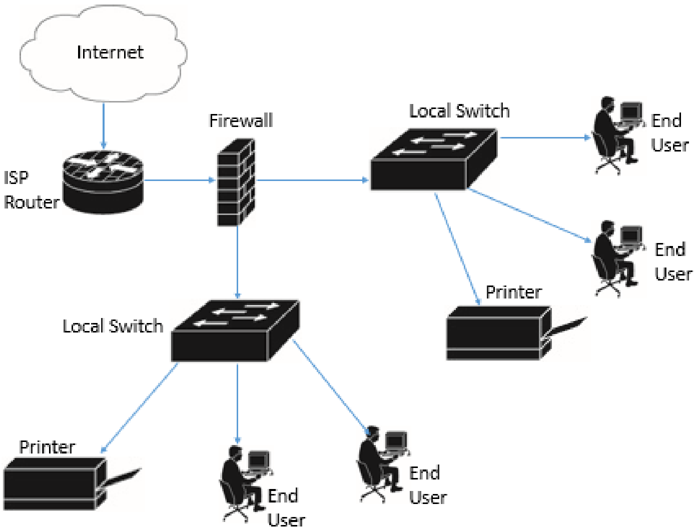
The organization has developed an induction program for new employees, through which they communicate the client business operation processes to be followed for service delivery aspects, confidentiality requirement, HR policies, IT policies, administrative policies and organization security policies and practices. All employees and contractors are required to accept the organization policies and procedures by signing an undertaking. There exists a formal client business operation process for delivering services to its clients, which includes allocation, monitoring, reviewing and tracking the request. The request status is monitored and reviewed by the Operations Head/ team lead and information is communicated to its clients for any issues and foreseeable delays.

## E. Components of the System

**E.1. Infrastructure:** The infrastructure consists of the System's physical and hardware elements, such as its computing devices, tools, and networks.

E.1.1. Network Segmentation Overview. Their newest hardware, software, and networking setups are available at NEONICHE.

**NETWORK DIAGRAM**



### E.1.3. **Physical Control Access**

NeoNiche Integrated Solutions Pvt. Ltd has implemented the biometric figure print and entrance. Biomatrix device is used for access control. every access and denial are monitored in the system. access adding and removing by the request of management and done by HR & Admin team.

#### E.1.4. **Access to the Server Room**

NEONICHE have an access restricted server. firewall, core switch. patch panel is in room. all the product related to NeoNiche is separated and locked in Room.

#### E.1.5. **Electric Backup**

NeoNiche Integrated Solutions Pvt. Ltd has stabilizer for controlling power fluctuation.

## F. Software

F.1. **Firewalls** NEONICHE makes use of an AWS security group along with Fortinet firewall, and certain ports that are necessary for accessing their web application and RDP port from particular networks are permitted. Custom TCP and RDP ports are the only ports that NEONICHE has defined as authorised in security groups.

F.2. **Security Monitoring** DLP setting is carried out on Antivirus, where NEONICHE has disabled USB, and each email or file upload with a certain set of contents notifies the designated staff members in charge of network security via email.
Any company computing device (laptop, workstation, server, etc.) or company address designation should only be able to access Internet services through the perimeter security measures that have been approved by the company.

NEONICHE employs use Endpoint Protection and system vulnerability scans to prevent malware from impairing the security of customer and organisational data. The IT team ensures that all endpoints in businesses, including services hosted on Amazon Web Services (AWS), are inspected for vulnerabilities and that any malware is removed effectively and promptly.

Monitoring is a crucial component of internal control in determining if the controls are working as intended and whether they have been changed appropriately to account for shifts in their business environment. NEONICHE management and information security staff routinely check their effectiveness of internal control performance as part of their duties. NEONICHE uses a variety of monitoring tools, such as Uptime Robot for application and website uptime, as well as built-in real-time monitoring tools for all the sub-services (AWS, big rock, GCP, Azure, Google mail utilised for the application.

In order to find illegal information processing activities, NEONICHE has designed and put in place suitable monitoring controls. Users' actions, exceptions, and information security events are logged on critical servers and systems. Activity logs are maintained for system operators and administrators.

To ensure that system performance achieves the anticipated service levels and to reduce their risk of system failure and capacity-related problems, capacity management controls are put in place for NEONICHE's resources. These controls ensure that resources are monitored, tuned, and projections are made. Prior to acceptance, formal system analysis, testing, and approval are required for their addition of new information systems and facilities, upgrades, new versions, and changes.

F.3 **Patch Management:** The IT team makes sure that all updates to their operating systems of servers and network devices are evaluated for stability and any concerns with availability before being applied to their production environment. Any patches are tested and deployed prior to being released. To guarantee that servers, desktops, and important network devices operate effectively, their patch management activity is carried out on a regular basis or as and when any critical event occurs. Operating system patches are monitored and installed as they become available.

The IT team at NEONICHE updates patches manually on multiple systems because there is no centralized patch management server.

## G. Vulnerability Scans & Intrusion Detection/Intrusion Prevention

At the moment, NEONICHE has carried out a VAPT through 3rd party service provider Cyborgenic in Q2 2024.

## H. People

The NEONICHE INTEGRATED SOLUTIONS PVT. LTD organisational structure offers a comprehensive framework for organising, leading, and managing operations. It has divided employees and corporate operations into functional groupings based on duties. This strategy makes it easier for their company to identify roles, reporting structures, and channels of communication while allowing staff to concentrate on the business concerns affecting NEONICHE INTEGRATED SOLUTIONS PVT. LTD clients.

Their management team meets on a regular basis to discuss their plans and operations of the business units. To assess operational, security, and business challenges as well as future goals, senior management and department heads participate in weekly and monthly meetings and calls.

The information security policies of NEONICHE INTEGRATED SOLUTIONS PVT. LTD outline and allocate duties and accountability for information security. The level of security, changes, technological trends, the frequency of events, and security efforts are all topics that are covered at regular management meetings.

***Roles and Responsibilities***

### Chief Information Security Officer (CISO)

The Chief Information Security Officer (CISO) would be responsible for establishing, maintaining, implementing, administering, and interpreting organization-wide IT security policies, IT standards, guidelines, and procedures. The CISO is responsible for the following;

- Act as the organization's representative with respect to inquiries from customers, partners, and the general public regarding the organization's IT security strategy
- Act as the organization's representative when dealing with law enforcement agencies while pursuing the sources of network attacks and information theft by employees.
- Balance security needs with the organization's strategic business plan, identify risk factors, and determine solutions to both.
- Develop security policies and procedures that provide adequate business application protection without interfering with core business requirements.
- Plan and test responses to security breaches
- Oversee the selection testing, deployment, and maintenance of security hardware and software products as well as outsourced arrangements.
- Oversee a staff of employees responsible for organization's security, ranging from network technicians managing firewall devices to security guards.
- Defining technical and non-technical information security standards, procedures and guidelines;
- Collecting, analysing and commenting on information security metrics and incidents;
- Organizing a security awareness campaign for personnel to enhance the security culture and develop a broad understanding of the requirements of ISO/IEC 27001.
- Ensure Internal Audit & MRM are conducted at planned Interval

- reporting on the performance of the information security management system to top management.

### ISMS IA Team:

- Conduct information security internal audit as per plan and directions from CISO
- Prepare audit report and submit to CISO for further action
- Facilitate auditees in closing of audit findings.

### Manager- IT

The Manager IT is responsible for the following.

- Implement IT Security and Privacy Controls
- Responsible for Network Security Measures
- Investigate Network Security aspects of incidents.
- Actively promote the implementation of Information Security within Organization
- Capacity management in regards of information security

### Process Heads & Data Owners

Process Heads & data Owners are responsible for following;

- Appropriate classification and protection of the information assets;
- Authorizing access to information assets in accordance with the classification and business needs;
- Monitoring compliance with protection requirements affecting their assets.
- Complying with the principles and policies in the information security policy

### End User

End User shall be responsible for following:

- It is the responsibility of each end user to report any incidence which is observed /suspected to ISM.
- Users shall not test any existence of vulnerability in the information systems.

- Understand the IT laws and amendments.
- Avoid breaches of any law, statutory, regulatory and/ or contractual obligations as well as security requirements.

### H.1. Commitment to competence

The duties and qualities necessary for each position at NEONICHE are outlined in the official roles and responsibilities doc. The business's present and future needs affect their ongoing identification of training requirements. Employees are assessed annually to track their performance levels and pinpoint areas in which they need to improve their skills.

### H.2. Assignment of Authority and Responsibility

The delegation of authority and duty within NEONICHE is the responsibility of management.

### H.3. New Hire Procedures

Being a young, professional start-up, NEONICHE bases its hiring philosophy on the right people at the right time principle. Their hiring process at NEONICHE includes sourcing via recommendations, job boards, headhunting, and recruitment agencies; screening potential candidates and background checks; selecting the best candidates through interviews and/or tests; and an on boarding process that includes document verification and new employee data updating, as well as acceptance of a non-disclosure agreement, acceptable use policy, and code of conduct.

### H.4. Training and Development

NEONICHE's training and development program strives to continuously up-skill its personnel and offer them learning opportunities, enabling them to perform better in their present and future jobs. It mostly consists of training on specific domains, processes, quality, and information security issues. Depending on their needs and organizational requirements, employees are also encouraged to explore learning possibilities through external certificates.

### H.5. Performance Evaluation

NEONICHE follows an anniversary based formal performance evaluation process, wherein an employee is evaluated on the performance against various KRAs during the year. As a value-based organization, organization values are also a part of the appraisal process and have a 20% weightage on the overall evaluation score, with 80% weightage being distributed across various KRAs.

### H.6. New Employee Training

Each new hire goes through an orientation programmed designed to familiarize them with the organization, its goals, the background of their business, its mission, vision, values, and the cultural code of NEONICHE. Aspects of quality and information security, as well as HR policies and employee expectations with regard to organizational norms and principles, are also included.

### H.7. Employee Terminations

Employment changes or terminations are handled in accordance with NEONICHE HR-related procedures. Regarding termination or change in employment, there are clearly defined and allocated tasks.

Retirement, Notice Termination, or Termination with Cause (which could be used in cases of misconduct, indiscipline, violation of organisational norms, policies, and procedures, carelessness, or breach of confidentiality and non-compete norms and agreements) are the three ways that an employee's employment may be terminated.

Any documents, records, correspondence, and information (in whatever medium or format) pertaining to the business or affairs of the Company or any of its affiliates or its business contacts, as well as any other property of the Company or any of its affiliate, which is in the possession of any employee in such circumstances must be delivered immediately to the Company.

All access to business resources and communication channels is terminated if an employee quits.

Access to corporate systems is examined when there is a change in employment due to reassignment or a change in job or status, and any appropriate changes are made about access as needed. Exit procedures are documented in the HR manual.

### H.8. Administrative Level Access

Administrative rights and access to administrative accounts are granted to individuals that require that level of access in order to perform their jobs.  All administrative level access, other than to IT team, must be justified to and approved by CEO / Executive Director.

## IOutbound Communication

The NEONICHE Network provides access to NEONICHE Applications. External internet access is necessary for contact with the clients and file uploads. The NEONICHE application and encrypted channels are used for outgoing communication. Web and protocol filtering rules are periodically reviewed and updated by the IT team. After reviewing these suggestions, human resources decide whether any adjustments need to be made.

## J. Backup and Recovery of Data

NEONICHE keeps two different types of backups. 1) User data backup and 2) server data backup is both done on a real-time basis using Google Drive. Server data backup uses AWS for DB server backup and cloud storage (AWS), with a rolling 7-day retention period. Formal policies and practices for backing up and recovering data exist. Details regarding back-up are defined in the Backup Policy.

NEONICHE has established backup procedures that specify the kinds of data to be backed up, backup cycles, and backup techniques. The business owners have approved the backup procedures, and they abide by all legal and regulatory obligations as well as those for business continuity. All backup and restoration logs are kept for the duration of the "Backup Restore Procedure" retention periods.

All backup copies are periodically tested to make sure the data and information can be safely retrieved in the case of an emergency without any data loss. Users are properly trained so they are aware of their obligations to make sure the necessary data and information are backed up.

### K. Data Restoration Procedure

Restoration is carried out in two situations, the first being when a NEONICHE member requests the recovery of some lost data. A restoration test is also performed during a routine DR test. The backup administrator, who is the appropriate IT staff member, makes sure that the data is recovered correctly.

In addition to physical safeguards, NEONICHE has created protocols that guarantee business continuity in the event of a protracted interruption of service. Their system is built to switch automatically to an alternative database in the event of such an interruption. AWS backup is a practise at NEONICHE.

Based on a business impact study, their disaster recovery plan specifies the roles and duties and lists the essential operating systems, personnel, data files, and IT application programmes that must be available constantly.

neoniche

## Section IV

## Description of Criteria NeoNiche Integrated Solutions Pvt Ltd - Event Management Company.

# “Event Management, Brand Activation, Creative Services Integrated Marketing, Digital Marketing, MICE, Technical Solutions & Production Management”

As of 20th July 2024

## 4.1Trust Services Principles, Criteria, Control Activities, And Testing Performed

### CC1.0 – Common Criteria Related to Control Environment

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| CC1.1 | COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values. | The company maintains formally documented Information Security and Data Privacy policies and procedures and they are reviewed by IT Admin and approved by the Director of company | Inspected the information security and data privacy policies and procedures for the in- scope technology and locations. It was also noted that they are reviewed annually and approved by Top Management.<br>The last review was conducted by IT Admin and approved by Top Management. While communicated by HR on and policy exceptions are maintained in the document.<br>The policies and procedures are made available to all employees of the company through the shared drive folder | No exceptions noted. |
| | | Information security policies include classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements. | Inspected the security policies to ascertain they included the matters specified. | No exceptions noted. |
| | | The employees are required to acknowledge the Information security and Data privacy policies, procedures on an annual basis. | Inspected the email communication from IT Admin to all the employees in the company to determine that Information security and Data privacy policies and procedures were communicated from executive management to all employees.<br>Inspected the Information security policy hosted on company's shared folder and employee acknowledgements of sample employees to determine that | No exceptions noted. |

| | | | | |
|---|---|---|---|---|
| | | | personnel were required to acknowledge on an annual basis.<br>Interviewed sample of new hires- Aniska Singh (Joined on 01/07/2024), whether they are aware and abide to the Information Security policies of the organization. Also verified signed NDA copies at the time of joining. | |
| | | Employees must read and acknowledge the employee handbook and the non-Disclosure agreement (NDA) upon hire. | Inspected completed NDAs for a judgmental sample of employees hired during the review period to determine that the employees signed a confidentiality agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.<br>Inspected NDAs of Aniska Singh to ensure process is followed. | No exceptions noted. |
| | | A documented organizational chart is in place to communicate organizational structures, lines of reporting, and areas of authority. | Inspected the organizational chart to determine that a documented organizational chart was in place to communicate organizational structures, lines of reporting, and areas of authority. | No exceptions noted. |
| | | Employees who do not comply with Company policies and standards will be subject to disciplinary actions. | Inspected policies and procedures to ensure disciplinary actions for misconduct are included. | No exceptions noted. |

| Criteria | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|
| | The onboarding process includes background checks for all candidates extended a job offer. | Inspected Background verification reports of sample of new hires performed by HR Manager to verify background screening and consent, including past employment, criminal search, and address history was completed.<br>Background verification is regularly done for all employees. | No exceptions noted. |
| | HR policies, which include probation, suspension and termination, are in place for employee misconduct. | Inspected employee's Manual, code of conduct and HR policies to determine that HR policies, which include probation, suspension and termination, were in place for employee misconduct. | No exceptions noted. |
| | Employees are directed on how to report unethical behavior in a confidential manner. | Inspected HR Policies to verify all the requirements for unethical behavior | No exceptions noted. |
| | Company's Vision and Mission statement in place for its objective | Inspected Neoniche vision and mission statement along with measurability of objective progress. | No exceptions noted. |
| | Company's Whistle blower policy is in place on reporting of wrong doing or malpractice | Inspected whistle blower policy | No Exception Noted |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| CC1.2 | COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. | A documented organizational chart is in place to assign responsibility and delegate lines of authority to personnel.<br>A documented onboarding and offboarding tracker are in place to track the employee and their access status. | Inspected the organizational chart to determine that a documented organizational chart was in place to assign responsibility and delegate lines of authority to personnel. | No exceptions noted. |
| | | | Verified details of employees resigned or terminated from Neoniche with details of deactivation request date, deactivation related to id, activity log, access card, ID card of building entrance, and any other access related to Neoniche. | No exceptions noted. |
| | | A steering committee is built up to report the irregularities to the top management | Verified Onboarding process that details Emp id, start date, equipment and email address.<br>Steering committee verified with following members:<br>CEO<br>IT Admin<br>HR | No exceptions noted.<br>No exception Noted |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| CC1.3 | COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | The experience and training of candidates for employment or transfer are evaluated before they assign the responsibilities of their respective position. | Inspected job requirements listed within a sample of job descriptions to determine that the experience and training of candidates for employment or transfer were evaluated before they assigned the responsibilities of their respective position. | No exceptions noted. |
| | | Roles and responsibilities defined in written job descriptions consider and address specific requirements relevant to the system. | Inspected the written job description for a sample of roles to determine that roles and responsibilities defined in written job descriptions considered and addressed specific requirements relevant to the system. | No exceptions noted. |
| | | Job descriptions are created or updated as part of the hiring process. All new hires are required to have a written job description. | Inspected onboarding procedures to ensure written job descriptions are required to be updated or created for new hires. | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| CC1.4 | COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | The ability of candidates to meet the requirements documented in job descriptions is evaluated as part of the hiring process. | Inquired with management to ensure potential new hires' experience and qualifications are evaluated against the job requirements by the HR manager. | No exceptions noted. |
| | | The company evaluates the competencies and experience of candidates prior to hiring. | Inquired the HR regarding onboarding procedures to determine that the company evaluated the competencies and experience of candidates prior to hiring.<br>Inspected the process to determine that the person is evaluated for competencies and experience of candidates prior to hiring. | No exceptions noted. |
| | | Employees must read and acknowledge the employee handbook and the non-Disclosure agreement (NDA) upon hire. | Inspected completed NDA Aniska Singh, for a judgmental sample of employees hired during the review period to determine that the employees signed a confidentiality agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties. | No exceptions noted. |
| | | Employees are required to complete information security training upon hire and annually thereafter. Employees must complete and pass evaluation parameters after security awareness training. | Inspected the assigned security and compliance training programs through an awareness training program to ensure employees are required to be trained on information security topics and that an evaluation must be passed after the training. | No exceptions noted. |
| | | | Inspected evaluation results for a sample of new hires to ensure each sampled employee completed and passed the required evaluation exam. | No exceptions noted. |
| | | | Inspected the security awareness training presentation that is used to train Neoniche employees on security practices.<br>Inspected email trail from HR about training. | No exceptions noted. |

| | | | | |
|---|---|---|---|---|
| | | Employees must read and acknowledge the Policies and Procedures upon hire. | Inspected documented policies and procedures to ensure employees are required to read and accept the policies and procedures.<br>Policy adherence is confirmed through offer letter.<br>Inspected offer letter duly signed by for Aniska Singh. | |
| | | The onboarding process includes background checks for all candidates extended a job offer. | Inspected on boarding process vide onboarding policy and procedures. | No exceptions noted |
| CC1.5 | COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. | Employees who do not comply with company policies and standards will be subject to disciplinary actions. | Inspected code of conduct and HR policies to ensure disciplinary actions for misconduct are in place.<br>Inspected the HR records to determine the employee information is tracked and maintained. | No exceptions noted. |

## CC2.0 – Common Criteria Related to Communication and Information

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| CC2.1 | COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. | The Neoniche team is updated periodically by application development on the development and performance of internal controls. Any issues or concerns identified are reported up to the IT Admin. | Inquired with management to ensure the Neoniche team is updated periodically by application development and IT Admins on the development and performance of internal controls. Any issues or concerns identified are reported up to the IT Admin. | No exceptions noted. |
| | | | Inspected an example email correspondence to ensure the Neoniche team is updated periodically by application development and IT Admin on the development and performance of internal controls. | No exceptions noted. |
| | | Network Architecture diagrams are documented and maintained by management to identify the relevant internal and external information sources of the system. | Inspected the network architecture and data flow diagram to determine that diagrams were documented and maintained by management up to date to identify the relevant internal and external information sources of the system. | No exceptions noted. |
| | | Data flow diagrams are documented and maintained by management to identify the relevant internal and external information sources of the system. | Inspected the data flow diagram to determine that data flow diagrams were documented and maintained by management to identify the relevant internal and external information sources of the system. | No exceptions noted. |

| Criteria | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|
| | Data that entered into the system, processed by the system, and output from the system is protected from unauthorized access. | Inspected the Kaspersky, the SSL certificate cipher configuration, and the remote access authentication settings to determine that data that entered into the system, processed by the system, and output from the system was protected from unauthorized access. | No exceptions noted. |
| | Data is only retained for as long as required to perform the required system functionality, service or use. | Inspected the data disposal policy to determine that data was retained for only as long as required to perform the required system functionality, service or use. | No exceptions noted. |
| | A description of the system is posted onthe company's intranet and is available to the internal users. This description delineates the boundaries of the system. | Inspected the policy and procedure to determine that a description of the system was posted on the company's intranet and was available to the internal users. This description delineated the boundaries of the system. | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | 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. | Security and availability responsibilities are documented in internal policies and procedures. The company's internal policies and procedures are available to all employees on the company intranet. | Inspected the company's document repository, to ensure internal policies and procedures are made available to all employees.<br>Inspected policies and procedures. | No exceptions noted. |
| | | | Inspected policies and procedures to ensure security and availability responsibilities are documented. | No exceptions noted. |
| | | Security reminders are sent as necessary to educate employees on security issues or recommended practices. | Inspected an example security reminder to ensure employees are educated as necessary on security issues or recommended practices. | No exceptions noted. |
| | | The Password Policy includes procedures for creating, changing, and safeguarding passwords. | Inspected the password management policy to ensure it includes procedures for creating, changing, and safeguarding passwords. | No exceptions noted. |
| | | The incident management response plan details procedures for internal users to report security and availability incidents. | Inspected the incident management response plan to ensure it details procedures for internal users to report security and availability incidents. | No exceptions noted. |
| | | Employees must read and acknowledge the Policies and procedures upon hire. | Inspected documented policies and procedures to ensure employees are required to read and accept the policies and procedures. | No exceptions noted. |
| | | | Inspected signed NDAs to ensure a sample of new hires read and accepted the policies and procedures. | No exceptions noted. |
| | | Employees are required to complete information security training upon hire and annually thereafter. Employees must complete and pass a quiz after security awareness training. | Observed training materials to ensure employees are required to be trained on information security topics and that a quiz must be passed after the training. | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| | | | Inspected evaluation results for a sample of employees to ensure each sampled employee completed and passed the required evaluation. | No exception noted. |
| | | | Inspected the security awareness training presentation that is used to train Neoniche employees on security practices. | No exceptions noted. |
| | | | Inspected quiz results for a sample of new hires to ensure each sampled employee completed and passed the required quiz. | No exception noted. |
| CC2.3 | COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control. | Master service agreements between the company and customers detail responsibilities and commitments related to security. Availability responsibilities and commitments are documented in service level agreements (SLAs). | Inspected template customer agreements of client to ensure security and availability commitments for the company and customers are defined. | No exceptions noted. |
| | | The business continuity management and disaster recovery plan detail procedures for communicating availability incidents to external parties. | Inspected the business continuity management and disaster recovery plan to ensure it details procedures for communicating availability incidents to external parties. | No exceptions noted. |
| | | Users can send an email to the IT Admin or can call the organization to inform them of a security breach or complaint. | Email sent to the IT Admin is verified for a technical issue. | No exceptions noted. |

| Criteria | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|
|  | Major and minor releases are communicated to customers through email | Inspected email for a sample of releases to ensure releases are communicated to customers via email. | No exceptions noted. |
|  |  | Inspected a sample email that details about type of change, type of department, task type, description, owner, start/end time, duration and status.<br>Inspected a sample email communication to the key stakeholders mentioning the major features addressed as part of the release communication |  |
|  | Customer commitments, requirements and responsibilities are outlined and communicated through service agreements. | Inquired the IT Admin regarding procedures to ascertain they included the matters specified. | No exceptions noted. |
|  | Changes to commitments, requirements and responsibilities are communicated to third parties, external users, and customers via e-mail. | Inspected Mail regarding changes to commitments to determine that changes to commitments, requirements and responsibilities were communicated to third parties, external users and customers via e-mail.<br>Inspected the change Management policy to determine that changes to commitments, requirements and responsibilities were documented and communicated to third parties, external users and customers via e-mail. | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| | | | Inspected an example client communication, to determine that changes to commitments, requirements and responsibilities were communicated to third parties. | |
| | | The company’s information security policy addresses security responsibilities for all personnel. | Inspected the information security policy to verify that it addresses access control and the communication of information security responsibilities to all personnel. | No exceptions noted. |
| | | The organization maintains privacy policies that are communicated to internal and external users. | Inspected the Privacy Policy as published and email communication from IT Admin to verify they are communicated to all employees. | No exceptions noted. |

## CC3.0 – Common Criteria Related to Risk Assessment

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| CC3.1 | COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of | The methodology for the IT risk assessments details the need for identifying potential threats as well as assessing the likelihood and impact of the identified threats. | Inspected the methodology for the IT risk assessments to ensure it identifying potential threats and assessing the likelihood and impact of the threats.<br>Inspected Risk Management Policy as well as Risk Register | No exceptions noted. |

| | | | | |
|---|---|---|---|---|
| | risks relating to objectives. | The risk assessment methodology describes the company's requirements for the completion of the IT risk assessments and the handling of risk acceptance. | Inspected the risk assessment methodology to ensure it describes the requirements for the completion of the IT risk assessments and the handling of risk acceptance.<br>Inspected Risk Management Policy | No exceptions noted. |
| | | The third-party management policy defines expectations for identifying and risk rating all vendor relationships.<br>The risk ratings consider the nature of the information stored and transmitted and the criticality of the vendor to providing services. | Inspected the third-party management policy to ensure it defines expectations for identifying and risk rating all vendor relationships and risk ratings consider the nature of the information stored and transmitted and the criticality of the vendor to providing services. | No exceptions noted. |
| | | The company implements privacy regulatory measures. | Observed communication of corporate responsibility for and commitment to personal privacy, reference to applicable laws, principles and regulations, and contact information for concerns related to privacy issues to verify communication of privacy policies to internal and external users. | No exceptions noted. |
| | | Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure. | Inspected the documented key performance indicators to determine that executive management established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure. | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| CC3.2 | COSO Principle 7: The entity identifies risks to the achievement of its objectives | The methodology for the IT risk assessments details the need for identifying potential threats as well as assessing the likelihood and impact of the identified threats. | Inspected the methodology for the IT risk assessments to ensure it details identifying potential threats and assessing the likelihood and impact of the threats. | No exceptions noted. |

| | | | | |
|---|---|---|---|---|
| | across the entity and analyzes risks as a basis for determining how the risks should be managed. | | Inspected Risk Management Policy for Risk assessment and treatment | |
| | | The risk assessment methodology describes the company’s requirements for the completion of the IT risk assessments and the handling of risk acceptance. | Inspected the risk assessment methodology to ensure it describes the requirements for the completion of the IT risk assessments and the handling of risk acceptance. | No exceptions noted. |
| | | The IT risk assessments identify potential risks to the security and availability of the system and identifies mitigating controls for the risks. | Inspected the IT risk assessments and the risk register, to ensure potential risks and mitigating controls for the risks are identified. | No exceptions noted. |
| | | The third-party management policy defines expectations for identifying and risk rating all vendor relationships. The risk ratings consider the nature of the information stored and transmitted and the criticality of the vendor to providing services. | Inspected the third-party management policy to ensure it defines expectations for identifying and risk rating all vendor relationships and risk ratings consider the nature of the information stored and transmitted and the criticality of the vendor to providing services. | No exceptions noted. |
| | | The vendor risk assessment rates the inherent risk of a vendor based on the nature of the information that is stored and transmitted, cost, compliance, and quality of work. | Inspected the vendor risk assessment to ensure it rates the inherent risk of a vendor based on the nature of the information that is stored and transmitted, cost, compliance, and quality of work. | No exceptions noted. |
| | | The IT risk assessments are presented to management for approval. | Inspected the IT risk assessments to ensure the IT risk assessments are approved by management on an annual basis. | No exceptions noted. |

| | | | | |
|---|---|---|---|---|
| CC3.3 | COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives. | A risk assessment is conducted at least annually on all information technology assets. Environmental, regulatory, and technological changes are considered during this assessment. | Through inquiry of management, noted that company has implemented measures and procedures in order to identify potential threats of disruption to systems operation that would impair system security and availability, prevent and mitigate threats when commercially practicable and assess the risks associated with the identified threats.<br>Inspected the risk assessment documentation and identified evidence showing the assessment was performed during the examination period. | No exceptions noted. |
| | | The IT risk assessments considers fraudulent activities, including the likelihood and impact. | Inspected the IT risk assessments and the risk register, to ensure the assessment considers fraudulent activities, including the likelihood and impact.<br>Inspected the risk assessment procedures to verify that the risk assessment was required to be based on an industry- accepted risk assessment standard, the risk assessment process was required to be performed at least annually, and the risk assessment was also required to be performed following significant changes to the environment. | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| CC3.4 | COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control. | The organization has an annual risk assessment process in place. | Inspected the Risk Assessment Procedures to verify that the risk assessment was required to be based on an industry-accepted risk assessment standard, the risk assessment process was required to be performed at least annually, and the risk assessment was also required to be performed following significant changes to the environment.<br>Inspected the annual risk assessment document to verify it included identification of vulnerabilities, threats and risks, control analysis, correlation of risks and controls, analysis of likelihood and impact, risk determination, overall risk ratings and recommendations in alignment with the risk assessment procedures. | No exceptions noted. |
| | | The vendor selection process includes a review of materials to ensure the risks associated with the vendor relationship are understood. | Inspected the third-party management policy to ensure it details the requirements for the vendor selection process, including a review of materials to ensure the risks associated with the vendor relationship are understood. | No exceptions noted. |
| | | | Inspected the due diligence procedures followed to engage subservice organizations.<br>Inspected the vendor review performed for on an auto ensure the company has taken proactive steps in risk management. | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| | | The vendor risk assessment is updated by management on at least an annual basis. | Inspected the vendor risk assessment to ensure it was updated within the last year. | No exceptions noted. |
| | | The company has an annual risk assessment process in place. | Inspected the risk register document to verify it included identification of vulnerabilities, threats and risks, control analysis, correlation of risks and controls, analysis of likelihood and impact, risk determination, overall risk ratings and recommendations in alignment with the risk assessment procedures. | No exceptions noted. |

## CC4.0 – Common Criteria Related to Monitoring Activities

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| CC4.1 | COSO Principle 16*:* The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the | An availability monitoring solution is configured to monitor the core infrastructure and individual servers hosting the application. The solution is configured to alert when failures occur. | Inspected the audit logging and monitoring policy to ensure it details the availability monitoring process. | No exceptions noted. |
| | | | Inspected the Endpoint Protection on computers, Kaspersky Endpoint Protection is installed, to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. | No exceptions noted. |

| Criteria | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|
| components of internal control are present and functioning. | | Inspected an example alert from Kaspersky Endpoint Protection to ensure the availability monitoring solution alerts appropriate personnel when there is a failure. | No exceptions noted. |
| | A performance and availability monitoring solution are configured to monitor the core infrastructure and individual services hosted on Microsoft Office 365 Workspace. The solution is configured to alert when defined thresholds have been exceeded for memory, CPU, disk space, read/write usage, and unavailable endpoints/internal services. | Inspected the audit logging and monitoring policy to ensure it details the performance and availability monitoring process. | No exceptions noted. |
| | | Inspected the Service performance monitoring tool for performance and availability monitoring to ensure it monitors various availability metrics and alerts appropriate personnel when thresholds are exceeded. | No exceptions noted. |
| | Management obtains and reviews attestation reports of the third-party data center provider to evaluate the effectiveness of controls within the third-party's environment. | Inspected the completed attestation report for the third-party data center to determine that management obtained and reviewed attestation reports of the third-party data center provider to evaluate the effectiveness of controls within the third-party's environment. | No exceptions noted. |
| | Operations personnel review uptime monitors on a weekly basis to ensure the availability of the infrastructure after maintenance activities. | Inspected the reviews completed for a sample of weeks to ensure the uptime monitors are reviewed on a daily basis by the operations team. | No exceptions noted. |
| | Operations personnel review administrative activity and failed login report on a weekly basis. | Inspected the reviews completed for a sample of weeks to ensure administrator activity and failed logins were reviewed. | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| | | The production environment is monitored by a log management and analytics solution. Logs are reviewed on a monthly basis. | Inspected the configuration of the log management and analytics solution. Performance Monitoring Tool to ensure it logs activity in the production environment. | No exceptions noted. |
| | | | Inspected the reviews completed for a sample of months to ensure the logs are reviewed on a daily basis. | No exceptions noted. |
| | | IT Admin conducts a weekly staff meeting and includes topics for discussion like to review upcoming maintenance schedules or outage event on to share details and awareness. | Inspected meeting agendas for a sample of weeks to ensure the support team conducts a daily standup staff meeting and includes topics for discussion like to review upcoming maintenance schedules or outage event on to share details and awareness.<br>Weekly meeting record collected as well as maintenance plan is also found evident. | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| CC4.2 | COSO Principle 17: The entity evaluates and communicates internal control deficiencies in | Vulnerabilities, deviations and control gaps identified from the risk assessment are communicated to those parties responsible for taking corrective actions. | Inspected the vulnerability management policy, risk assessment methodology and the completed risk assessment to determine that vulnerabilities, deviations and control gaps identified from the risk assessment were communicated to those parties responsible for taking corrective actions. | No exceptions noted. |

| Criteria | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|
| a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate. | Vulnerabilities, deviations and control gaps identified from the risk assessment are documented, investigated, and addressed. | Inspected the risk register and the treatment related to resolution of identified vulnerabilities to determine that vulnerabilities, deviations and control gaps identified from the risk assessment were documented, investigated and addressed.<br>Inspected email of IT Admin regarding Risk Register | No exceptions noted. |
|  | Access to the production environment is reviewed on a quarterly basis to ensure it is restricted to authorized personnel who require access to perform their job functions. The access to production environment is also controlled by multifactor authentication. | Inspected the access control policy to ensure access to the production environment is reviewed on a quarterly basis. | No exceptions noted. |
|  | The production environment is monitored by a log management and analytics solution. Logs are reviewed on a monthly basis. | Inspected the configuration of the to ensure it logs activity in the office environment | No exceptions noted. |
|  |  | Inspected the reviews completed for a sample of months to ensure they are reviewed on a monthly basis. | No exceptions noted. |

## CC5.0 – Common Criteria Related to Control Activities

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| 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. | The company applies appropriate controls to lessen the likelihood and/or impact of identified risks. | Inspected the risk assessment methodology to ensure the company applies appropriate controls to lessen the likelihood and/or impact of identified risks. | No exceptions noted. |
| | | | Inspected the IT risk assessments and the treatment to ensure the company has identified and applied mitigating controls to reduce the risks presented to the system. | No exceptions noted. |
| | | Monitoring is performed of key controls to measure the success of the controls in addressing relevant risks. | Inspected the policies and procedures to ensure monitoring is performed of key controls to measure the success of the controls in addressing relevant risks. | No exceptions noted. |
| | | The business continuity management and disaster recovery plan describe the company's strategy for responding in the event of a disaster. | Inspected the business continuity management and disaster recovery plan to ensure the plan describes the company's strategy for responding in the event of a disaster. | No exceptions noted. |
| | | The company maintains a formally documented information security policy. | Inspected the information security policy to verify it includes requirements for authentication, identification, logical access control, secure data management, record handling, incident response, access control, compliance, surveillance, and supervision and control.<br>Inspected approval of policies bythe Top Management to verify procedures for review and update to the information security policy. | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| CC5.2 | COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives. | The company applies appropriate controls to lessen the likelihood and/or impact of identified risks. | Inspected the risk assessment methodology to ensure the company applies appropriate controls to lessen the likelihood and/or impact of identified risks. | No exceptions noted. |
| | | | Inspected the IT risk assessments to ensure the company has identified and applied mitigating controls to reduce the risks presented to the system. | No exceptions noted. |
| | | An availability monitoring solution is configured to monitor the core infrastructure and individual services at Microsoft Office 365. The solution is configured to alert when failures occur. | Inspected the audit logging and monitoring policy to ensure it details the availability monitoring process. | No exceptions noted. |
| | | | Inspected the configuration of the failure delivery mechanism to ensure the availability of the environment is monitored and appropriate personnel are notified of failures. | No exceptions noted. |
| | | | Inspected alert policies to ensure the availability monitoring solution alerts appropriate personnel when there is a failure. | No exceptions noted. |
| | | A performance and availability monitoring solution are configured to monitor the core infrastructure and Service Health<br>The solution is configured to alert when defined thresholds have been exceeded for memory, CPU, disk space, read/write usage, and unavailable endpoints/internal services. | Inspected the audit logging and monitoring policy to ensure it details the performance and availability monitoring process. | No exceptions noted. |
| | | | Inspected the configuration of the performance and availability monitoring by Service Health, which ensures a 99.9% uptime of services | No exceptions noted. |
| | | | Inspected example alerts to ensure the performance and availability monitoring solution alerts appropriate personnel when a threshold has been exceeded. | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| 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. | The company has documented policies and procedures for the system that detail implemented controls to maintain security and availability. | Inspected the company's documented policies and procedures to ensure documentation includes controls to maintain security, availability. | No exceptions noted. |
| | | Policies and procedures are reviewed at least annually. | Inspected the company's documented policies and procedures to ensure they are reviewed at least annually. | No exceptions noted. |
| | | The company holds daily standup meetings to ensure operational quality and control. | Observed an agenda for a change meeting that included a review of projects, changes, timelines, and capacity to verify monitoring for operational quality and control.<br>Observed an operations meeting about the discussion of infrastructure items coming through the following week, including maintenance window work, outstanding items, other planned maintenance, and potential impacts due to changes at a technical level. | No exceptions noted. |

## CC6.0 – Common Criteria Related to Logical and Physical Access Controls

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| CC6.1 | The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. | Logical access to the system is restricted to authorized individuals who need access to perform their job functions. | Inspected the access control policy to ensure they address the restriction of access to systems. | No exceptions noted. |
| | | | Inspected the Identity and access management to access profiles to the projects in production environment to ensure access is appropriate. | No exceptions noted. |
| | | End user systems are configured with Account and password Management controls. | Inspected the local system group policies of a sample systems to ensure password complexity and account management controls are configured.<br>Inspected the configuration of group policy deployment and noted the settings related to prohibit access to control panel, prevent windows from Storing LAN Manager Hash, control access to command prompt, disable forced system restarts, restrict software installations and disable guest account are enabled. | No exceptions noted. |
| | | All users are required to be assigned a unique user ID prior to being granted access to system components. | Inspected the access control policy to verify requirement for the use of non-repeated generic user IDs.<br>Access Management Solutions is applied to all user accounts that are created and managed directly. | No exceptions noted. |

| Criteria | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|
| | Passwords are enforced on the technologies supporting the infrastructure. The password settings enforced include minimum length, complexity requirements, and expiration. | Inspected the configuration of the password practices enforced to access the production environment to ensure they include password minimum length, complexity requirements and expiration.<br>Access control solutions for policies and noticed they are applied to all user accounts that are created and managed directly.<br>Inspected the group policy configured on the end user systems with the following options<br>• maximum password age 30 days<br>• minimum password length 12-28 characters 30 characters for Service Accounts<br>• users are prompted to change their password at logon 7 days before the existing one expires.<br>• passwords must contain at least three of the following five elements:<br>- numeric – (0-9)<br>- uppercase – (A-Z)<br>- lowercase – (a-z)<br>- special characters (? @, #, %, etc.) | No exceptions noted. |

| Criteria | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|
| | Multifactor authentication is required to access the technologies supporting infrastructure. | Inspected the authentication configurations for accessing environment to ensure multifactor authentication is required.<br>Verified implementation of MFA to access environment and noticed the account sign in has requested to approve request sent on the users mobile. | No exceptions noted. |
| | An inventory of system assets and components is maintained to classify and manage the information assets. | Inspected the inventory and asset owner listing to determine an inventory of system assets and components was maintained to classify and manage the information assets.<br>Verified Laptop issued to Aniska Singh Respective filled form is verified. | No exceptions noted. |
| | Microsoft audit logging settings are in place that include:<br>• Read/Write Events<br>Microsoft Office 365 audit logs are maintained and reviewed as needed. | Inspected the audit logging settings to determine that audit logging configurations were in place that included:<br>• Read/Write Events<br>Inspected sample audit log extract to determine that audit logs were maintained and reviewed as needed. | No exceptions noted. |
| | Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. | Inspected the information security policy to determine documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring. | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| 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. | Written authorization in the form of a ticket, email, or other documented methods is required to grant and remove access to the Microsoft Office 365<br>This process is documented within Policy. | Inspected the access control policy to verify requirements for authorization of users prior to granting access. | No exceptions noted. |
| | | | Inspected the dashboard to ensure access granted to the production environment is documented and reviewed. | No exceptions noted. |
| | | | Inspected the dashboard to ensure to ensure access removed from the production environment is documented and reviewed. | No exceptions noted. |
| | | Access to the production environment is reviewed on a quarterly basis to ensure it is restricted to authorized personnel who require access to perform their job functions. | Inspected the access control policy to ensure access to the production environment is reviewed on a periodic basis. | No exceptions noted. |
| | | | Inspected the dashboard which ensure user roles and access profiles to the projects in production environment to ensure user access to the production environment is reviewed for appropriateness. | No exceptions noted. |
| | | Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. | Inspected the information security policy to determine documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring. | No exceptions noted. |
| | | Documented incident response policies and procedures are in place to guide personnel in the event of an incident. | Inspected the incident response plan to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident. | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| | | All employees are responsible for reporting known or suspected information technology security incidents. All security incidents must be promptly reported to the team or IT Admin. | Through inquiry with management and corroboration with employees, confirmed the methods for reporting security incidents.<br>Inspected the documented policies and procedures related to reporting and documenting security incidents.<br>Inspected sample of security incidents reported during examination period to ensure these were reported to IT Admin | No exceptions noted. |
| 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. | Access to the production environment is reviewed on a quarterly basis to ensure it is restricted to authorized personnel who require access to perform their job functions. | Inspected the access control policy to ensure access to the production environment is reviewed on a periodic basis. | No exceptions noted. |
| | | | Inspected the dashboard to ensure roles and access profiles to the projects in production environment to ensure user access to the production environment is reviewed for appropriateness. | No exceptions noted. |
| | | Logical access to systems is revoked as a component of the termination process. | Inquired the IT Admin regarding logical access and the termination process to determine that logical access to systems was revoked for an employee as a component of the termination process.<br>Inspected the human resource policy to determine that logical access to systems was revoked for an employee as a component of the termination process. | No exceptions noted. |

| Criteria | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|
|  |  | Inspected the user access revocation email for a sample of terminated employees and the user listings to determine that logical access to systems was revoked for an employee as a component of the termination process. |  |
|  | Written authorization in the form of a ticket, email, or other documented methods is required to grant and remove access to the production environment. This process is documented within Policy. | Inspected the access control policy and the separation process to ensure they detail the written authorization process. | No exceptions noted. |
|  |  | Inspected the email for granting access to sample of new hires to ensure access granted to the production environment is documented. | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| | | | Inspected the email for revoking access to sample of terminations to ensure access removed from the production environment is documented. | No exceptions noted. |
| | | User access is restricted via role-based security privileges defined within the access control system. | Inspected the user roles and access profiles to the projects in production environment to ensure user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| CC6.4 | The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity’s objectives. | Physical access to the corporate office facilities is controlled by Biometric | Observed Biometric with facial recognition at the entrance of the facility.<br>Inspected a sample of face reader access log files of the main entry door for the examination period to ensure access is restricted to appropriate personnel. | No exceptions noted. |
| | | The corporate facility has video surveillance cameras installed. | Observed CCTV camera at entry to the office and inside the office covering the entire floor to verify use of video surveillance system. | No exceptions noted. |
| | | The corporate facility requires the asset movement register to be signed for inward/outward moment of assets. | Inspected the Asset movement register to verify the assets are being tracked for inward / outward moment in the corporate facility. It was noted that there was no asset movement during the examination period. | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| | | | Inspected assets register. | |
| | | The corporate facility requires that visitors sign a visitor log to gain access to the corporate facility. | Observed that visitor register for the examination period and noticed the register capture details of visitor's name, address, date, Time In/Out, and comments for purpose of visit. | No exceptions noted. |
| | | The corporate facility is equipped with fire extinguishers at multiple location. | Inspected the placement of fire extinguishers that are kept at various locations of office. It is also noted from Admin that all employees are trained annually. | No exceptions noted. |
| | | The data retention retrieval and secure disposal policy addresses the removal and destruction of data and hardware. | Inspected the data retention retrieval and secure disposal policy to ensure it addresses the removal and destruction of data and hardware. | No exceptions noted. |
| 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 | The data retention retrieval and secure disposal policy addresses the removal and destruction of data and hardware.<br>Data that is no longer required for business purposes is rendered unreadable. | Inspected the use of paper shredder for disposal of confidential or sensitive paper documents. | No exceptions noted. |
| | | | Inquired the IT Manager regarding data disposal to determine that data that was no longer required for business purposes was rendered unreadable. | No exceptions noted. |
| | | Data that is no longer required for business purposes is rendered unreadable. Controls relating to the destruction and disposal of hardware is administered by | Inspected the data retention retrieval and secure disposal policy to determine that data that was no longer required for business purposes was rendered | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| | assets has been diminished and is no longer required to meet the entity’s objectives. | the subservice organization Microsoft. See the subservice organization Controls above for additional details. | unreadable | |
| | | | Not Applicable | Not Applicable |
| | | A firewall is in place to filter unauthorized inbound network traffic from the internet. | FortiGate 100F Firewalls is used to deny unauthorized access to the organization. | No exceptions noted. |
| CC6.6 | The entity implements logical access security measures to protect against threats from sources outside its system boundaries. | The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. | FortiGate 100F Firewalls is used to deny unauthorized access to the organization. | No exceptions noted. |
| | | Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. | Inspected the Kaspersky Endpoint Protection to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software. | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| | | The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. | Inspected Kaspersky Endpoint Protection console to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available. | No exceptions noted. |
| | | Symantec Endpoint Security is installed on systems and is configured to scan for viruses weekly. | Inspected the inventory of the Kaspersky Endpoint Protection to ensure antivirus is installed on endpoints. | No exceptions noted. |
| 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. | Symantec Endpoint Security is installed on systems and is configured to scan for viruses weekly.<br>The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. | Inspected the configuration of Kaspersky Endpoint Protection to ensure scans are run on a weekly basis.<br>Kaspersky Endpoint Protection security profile settings in the dashboard and determined that the following settings has been enabled.<br>• File threat protection<br>• Mail threat protection<br>• Web threat protection<br>• Network threat protection<br>• Firewall<br>• Behavior detection, exploit prevention and remediation engine<br>• Cloud discovery<br>• Host intrusion prevention<br>• Device control<br>• Web Control<br>• Full disk encryption<br>• Vulnerability protection | No exceptions noted. |

| Criteria | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|
| | | • Inspected the Kaspersky Endpoint Protection console to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available. | No exceptions noted. |
| | The ability to migrate changes into the production environment is restricted to authorized and appropriate users. | Inquired IT Admin regarding access to production systems to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users. | No exceptions noted. |
| | | Inspected the list of users with the ability to implement changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users. | No exceptions noted. |
| | The production environment is monitored by a log management and analytics solution. Logs are reviewed on a monthly basis. | Inspected the configuration of the log management and analytics solution to ensure it logs activity in the production environment. | No exceptions noted. |
| | | Inspected the reviews completed for a sample of months to ensure the production logs are reviewed on a daily basis. | No exceptions noted. |
| | Servers are patched on a monthly basis. | Inspected the patch status report and email communication post patch deployments during examination period to ensure patching occurred. | No exceptions noted. |
| | The ability to migrate changes into the production or corporate office environment is restricted to authorized and appropriate users. | Inquired the IT Manager regarding access to production systems to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users. | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| | | | Inspected the change control register of corporate facility that details on updates and changes to network configurations with last updated record. | No exceptions noted. |

## CC7.0 – Common Criteria Related to System Operations

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| 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. | The organization maintains a formally documented Change Management Policy that outlines system configuration standards. | Inspected the Configuration Management Policy and the System Hardening Policy to verify that the policies were in place and reviewed and approved by management.<br>Inspected that configuration standards include baseline configurations, requirements for change management to implement changes, access restrictions for change, security impact analysis, and documentation of configurations used in the environment.<br>Inspected that the hardening standards include requirements for unnecessary software and services; changes to passwords and disabling of default credentials; settings for security parameters; permissions and shares; installation of patches and firmware updates; audit logging; implementation of account and password management policy; and specific hardening procedures. | No exceptions noted. |
| | | The production environment is monitored by a log management and analytics solution. Logs are reviewed on a monthly basis. | Inspected the configuration of monitoring solution to ensure it logs activity in the production environment. | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| | | | Inspected the reviews completed for a sample of months to ensure the logs are reviewed on a daily basis. | No exceptions noted. |
| 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. | The incident management response plan details procedures for detecting, assessing, investigating, containing, and mitigating security and availability incidents. | Inspected the incident management response plan to ensure it includes the mentioned procedures. | No exceptions noted. |
| | | The incident management response plan details procedures for internal users to report security and availability incidents. | Inspected the incident management response plan to ensure it details procedures for internal users to report security and availability incidents. | No exceptions noted. |
| | | An availability monitoring solution is configured to monitor the core infrastructure and individual services at Microsoft Office 365. The solution is configured to alert when failures occur. | Inspected the audit logging and monitoring policy to ensure it details the availability monitoring process. | No exceptions noted. |
| | | | Inspected the configuration of the availability monitoring solution to ensure the availability of the environment is monitored and appropriate personnel are notified of failures. | No exceptions noted. |
| | | A performance and availability monitoring solution are configured to monitor the core infrastructure and | Inspected the audit logging and monitoring policy to ensure it details the performance and availability monitoring process. | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| 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. | The business continuity management and disaster recovery plan details procedures for communicating availability incidents to external parties. | Inspected the business continuity management and disaster recovery plan to ensure it details procedures for communicating availability incidents to external parties. | No exceptions noted. |
| | | Security incidents are assessed to evaluate the exposure of an incident along with the amount of damage. | Inspected the incident management response plan to ensure incidents are assessed to evaluate the exposure along with the amount of damage. | No exceptions noted. |
| | | The incident management response plan details procedures for detecting, assessing, investigating, containing, and mitigating security and availability incidents. | Inspected the incident management response plan to ensure it includes the mentioned procedures. | No exceptions noted. |
| | | The actions taken to address identified security incidents are documented and communicated to affected parties. | Inquired IT Admin regarding security incidents to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.<br>Inspected a sample communication to the client done via email. | No exceptions noted. |
| | | Resolution of incidents are documented through email as a ticket and communicated to affected users. | Inquired IT Admin regarding security incidents to determine that resolution of incidents was documented within the email and communicated to affected users.<br>Inspected the incident response policy to determine that resolution of incidents was documented within the ticket and communicated to affected users. | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| | | Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented. | Inspected the incident management response plan to determine that roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program were defined and documented. | No exceptions noted. |
| | | The incident response and escalation procedures are reviewed at least annually for effectiveness. | Inspected the incident response policy to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness. | No exceptions noted. |
| | | Vulnerability assessments are completed on all releases prior to implementation in the production environment. All vulnerabilities are tracked to resolution. | Inspected vulnerability scan report to ensure external vulnerability assessments are completed on the production environment and all vulnerabilities are tracked to resolution. | No exceptions noted. |
| CC7.5 | The entity identifies, develops, and implements activities to recover from identified security incidents. | Change management requests are opened for incidents that require fixes. | Inspected the incident management response plan to determine that change management requests were required to be opened for incidents that required fixes. | No exceptions noted. |
| | | Data backup and restore procedures are in place to guide personnel in performing backup activities. | Inspected the business continuity management and disaster recovery plan to determine that data backup and restore procedures were in place to guide personnel in performing backup activities. | No exceptions noted. |

| | | | | |
|---|---|---|---|---|
| | | The company has a Patch Management policy in place. | Verified patch management done through Mange Engine Endpoint Protection.<br>Inspected the patch management policy to verify that vendors are listed within the policy, timeframes and sources are given for specific vendors, security patching procedures are listed to identify new security vulnerabilities, risk ranking procedures are addressed, and reputable vendors are listed to provide security vulnerability information.<br>Inspected a sample of end user systems to verify that their systems are up to with latest security patches and noted it is updated with Windows 10 Professional version and Windows 11 version<br>Operating System environment is a mix-up of Windows 10 and Windows 11 | No exceptions noted. |
| | | A business continuity and disaster recovery plan are documented to identify and reduce risks, limit theconsequences of damaging incidents, and ensure the timely resumption of essential operations. | Inspected the business continuity management and disaster recovery plan to determine that a business continuity and disaster recovery plan was documented to identify and reduce risks, limited the consequences of damaging incidents, and ensured the timely resumption of essential operations. | No exceptions noted. |
| | | Data backup and restore procedures are in place to guide personnel in performing backup activities. | Inspected the business continuity management and disaster recovery plan to determine that data backup and restore procedures were in place to guide personnel in performing backup activities. | No exceptions noted. |

| | | | | |
|---|---|---|---|---|
| | | Related party and vendor systems are subject to review as part of the vendor management process. Attestation reports (SOC 2 reports) are obtained and evaluated when available. Site visits or other procedures may be performed based on the company’s vendor guidelines. | See complementary subservice organization controls for the types ofcontrols expected to be implemented by the subservice organizations.<br>Inspected the company’s review of attestation reports for each of the critical third-party vendors identified by management. | No exceptions noted. |

## CC8.0 – Common Criteria Related to Change Management

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| 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. | The System Development Life Cycle addresses business requirements, scoping, design, development, code review, quality assurance, and implementation of system components. | Inspected SDLC (System Development Life Cycle) policy | No exceptions noted. |

### CC9.0 – Common Criteria Related to Risk Mitigation

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| CC9.1 | The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. | The business continuity management and disaster recovery plan addresses recovering connectivity and supporting systems to ensure customer obligations can be met. | Inspected the business continuity management and disaster recovery policy to ensure the plan addresses recovering connectivity and supporting systems so customer obligations can be met. | No exceptions noted. |
| | | Business continuity and disaster recovery testing is performed on an annual basis. | Inspected the business continuity management and disaster recovery policy to ensure they detail testing of the plans. | No exceptions noted. |
| | | Documented policies and procedures are in place to guide personnel in performing risk mitigation activities. | Inspected the risk assessment methodology to determine that documented policies and procedures were in place to guide personnel in performing risk mitigation activities. | No exceptions noted. |
| | | Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. | Inspected the risk assessment policy to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. | No exceptions noted. |
| | | A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. | Inspected the risk register to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. | No exceptions noted. |

| Criteria | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|
|  | Identified risks are rated using a risk evaluation process and ratings are approved by management. | Inspected the risk assessment methodology to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.<br>Inspected the completed risk register dated to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.<br>Inspected the completed risk register to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process. | No exceptions noted. |
|  | Management develops risk mitigation strategies to address risks identified during the risk assessment process. | Inspected the risk assessment policy to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.<br>Inspected the completed risk register dated to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process. | No exceptions noted. |

| Criteria | | Control Activity Specified by the service organization | Tests Performed | Results |
|---|---|---|---|---|
| CC9.2 | The entity assesses and manages risks associated with vendors and business partners. | Third-party agreements are required to include non-disclosure/confidentiality clauses. | Inspected the third-party management policy to ensure it details requirements for contract language in third-party agreements. | No exceptions noted. |
| | | | Inspected the agreements with in-scope subservice organizations supporting the system to ensure the agreements includes non-disclosure/confidentiality clauses. | No exceptions noted. |
| | | The third-party management policy defines expectations for identifying and risk rating all vendor relationships. The risk ratings consider the nature of the information stored and transmitted and the criticality of the vendor to providing services. | Inspected the third-party management policy to ensure it defines expectations for identifying and risk rating all vendor relationships and risk ratings consider the nature of the information stored and transmitted and the criticality of the vendor to providing services. | No exceptions noted. |
| | | The vendor risk assessment rates the inherent risk of a vendor based on the nature of the information that is stored and transmitted, cost, compliance, and quality of work. | Inspected the vendor risk assessment to ensure it rates the inherent risk of a vendor based on the nature of the information that is stored and transmitted, cost, compliance, and quality of work. | No exceptions noted. |
| | | The company has documented procedures for addressing issues identified with third parties. | Inspected the third-party management policy to determine that the entity documented procedures for addressing issues identified with third parties. | No exceptions noted. |

| | | | | |
|---|---|---|---|---|
| | | The company has documented procedures for terminating third-party relationships. | Inspected the third-party management policy to determine that the entity documented procedures for terminating third-party relationships. | No exceptions noted. |
| | | Management obtains and reviews attestation reports of the third-party data center provider, Microsoft office 365 to evaluate the effectiveness of controls within the third-party's environment. | Inquired the IT Admin regarding third- parties to determine that management obtained and reviewed attestation reports of the third-party data center provider to evaluate the effectiveness of controls within the third-party's environment.<br>Inspected the completed attestation report for the third-party data center, to determine that management obtained and reviewed attestation reports of the third-party data center provider to evaluate the effectiveness of controls within the third-party's environment. | No exceptions noted. |
| | | The organization conducts due diligence procedures prior to engaging with service providers and vendors. | Inspected the third-party management policy to verify that the requirements for management of critical third parties are documented and in place and the organization was required to conduct due diligence procedures prior to engaging with service providers and vendors. | No exceptions noted. |
| | | | Inspected vendor review performed by obtaining their Information Security policies before engagement. | No exceptions noted. |

| | | | | |
|---|---|---|---|---|
| | | | Inspected the vendor review performed for vendors, to ensure the review are performed on an annual basis. | No exceptions noted. |

# Section V

## Other Information Provided by NeoNiche Integrated Solutions Pvt Ltd - Event Management Company.

**"Event Management, Brand Activation, Creative Services Integrated Marketing, Digital Marketing, MICE, Technical Solutions & Production Management"**

As of July 20th, 2024

### L. Other Information Provided by NEONICHE

NEONICHE offers the data in this part only for informational purposes. There have been no audit processes carried out regarding this part by the Independent Auditor

## L.1. Disaster and Recovery Services

Business continuity planning, which includes disaster recovery, is a concept that addresses how an organisation mitigates future risks rather than actual controls that give user auditors a level of comfort regarding the processing of transactions, according to guidance published by the AICPA. As a result, a service organisation should not list any specific control processes that deal with disaster recovery planning in its description of controls. As a result, this section contains descriptions of the control methods from NEONICHE's disaster recovery plan.