iMocha Inc.

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

Description of iMocha platform relevant to the Trust Services Criteria of Security, Availability and Confidentiality

March 1, 2026 through May 31, 2026

STATEMENT OF CONFIDENTIALITY

This report, including the description of the system, the applicable trust services criteria, the related controls, and the results of testing, is intended solely for the use of the management of iMocha, user entities of iMocha platform during some or all of the period March 1, 2026 to May 31, 2026, business partners of iMocha subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and the independent auditors of such user entities, who have sufficient knowledge to consider it.

This report, and the information contained herein, is confidential and proprietary to iMocha and is intended only for the authorized recipients identified above. It is not intended to be, and should not be, used or relied upon by anyone other than these specified parties. Unauthorized use, reproduction or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

SECTION 1 - INDEPENDENT SERVICE AUDITORS' REPORT

1 INDEPENDENT SERVICE AUDITORS' REPORT

To the management of iMocha Inc.

Scope

We have examined the description of the system provided by Management of iMocha Inc. (the "Service Organization" or "iMocha") included in Section 3, "Description of Systems Provided by Service Organization" of its iMocha platform throughout the period March 1, 2026 to May 31, 2026 (the "Description") based on the criteria for a Description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, in AICPA Description Criteria, ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period March 1, 2026 to May 31, 2026, to provide reasonable assurance that iMocha's service commitments and system requirements would be achieved based on the trust services criteria relevant to Security, Availability and Confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria.

iMocha uses Microsoft Corporation (Microsoft Azure) (Subservice Organization) for cloud hosting services. The Description indicates that complementary Subservice Organization controls that are suitably designed and operating effectively are necessary, along with controls at iMocha, to achieve iMocha's service commitments and system requirements based on the applicable trust services criteria. The Description presents iMocha's controls, the applicable trust services criteria, and the types of complementary Subservice Organization controls assumed in the design of iMocha's controls. The Description does not disclose the actual controls at the Subservice Organizations. Our examination did not include the services provided by the Subservice Organizations, 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 iMocha, to achieve iMocha's service commitments and system requirements based on the applicable trust services criteria. The Description presents iMocha's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of iMocha's controls. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

Management of iMocha 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 iMocha service commitments and system requirements would be achieved. Management of iMocha has provided the accompanying assertion in Section 2 titled, "Management Assertion Provided by iMocha Inc." (the "Assertion") about the Description and the suitability of the design and operating effectiveness of controls stated therein. Management of iMocha 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 (AICPA). Those standards require that we plan and perform the 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 operating effectively to provide reasonable assurance that the iMocha's service commitments and system requirements would be 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 a Description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- 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 would achieve its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of those controls stated in the Description to provide reasonable assurance that iMocha 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.

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with the Code of Professional Conduct established by the AICPA. We have complied with those requirements. We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of report users and therefore may not include every aspect of the system that each individual report user may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls.

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 the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in Section 4, "Information Provided by the Service auditor: Test of controls".

Opinion

In our opinion, in all material respects:

a) The Description presents iMocha's system that was designed and implemented throughout the period March 1, 2026 to May 31, 2026, in accordance with the description criteria.

b) The controls stated in the Description were suitably designed throughout the period March 1, 2026 to May 31, 2026, to provide reasonable assurance that iMocha'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 iMocha's controls throughout that period.

c) The controls stated in the Description operated effectively throughout the period March 1, 2026 to May 31, 2026, to provide reasonable assurance that iMocha's service commitments and system requirements would be achieved based on the applicable trust services criteria, and if the Subservice Organizations and user entities applied the complementary controls assumed in the design of iMocha's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of management of iMocha, user entities of iMocha platform during some or all of the period March 1, 2026 to May 31, 2026, business partners of iMocha subject to risks arising from interactions with the iMocha's system, 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 iMocha.

- How iMocha's system interacts with user entities, business partners, Subservice Organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary Subservice Organization controls and how they interact with related controls at iMocha to achieve iMocha's commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use iMocha's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of iMocha'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.

Norvex CPA Inc.

Norvex CPA Inc.
License No.: PAC-FIRM-LIC-60389
Whitefish, Montana
Date: August 12, 2026

SECTION 2 - MANAGEMENT'S ASSERTION PROVIDED BY SERVICE ORGANIZATION

MANAGEMENT ASSERTION PROVIDED BY IMOCHA INC.

For the period from March 1, 2026 through May 31, 2026

We have prepared the accompanying System Description Provided by Service Organization (Description) of IMocha Inc. (the "Service Organization" or "IMocha") in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (Description Criteria). The Description is intended to provide report users with information about the IMocha platform (System) that may be useful when assessing the risks arising from interactions with the System throughout the period March 1, 2026 to May 31, 2026, particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability and Confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria.

iMocha uses Microsoft Corporation (Microsoft Azure) (Subservice Organization) for cloud hosting services. The description indicates that complementary Subservice Organization controls that are suitably designed and operating effectively are necessary, along with controls at IMocha, to achieve IMocha's service commitments and system requirements based on the applicable trust services criteria. The description presents IMocha's controls, the applicable trust services criteria, and the types of complementary Subservice Organization controls assumed in the design of IMocha controls. The description does not disclose the actual controls at the Subservice Organization. The description does not extend to controls of the Subservice Organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at IMocha, to achieve IMocha's service commitments and system requirements based on the applicable trust services criteria. The description presents IMocha's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of IMocha's controls. The description does not extend to controls of the user entities.

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

a) The description presents the System that was designed and implemented throughout the period March 1, 2026 to May 31, 2026 in accordance with the description Criteria.

b) The controls stated in the description were suitably designed throughout the period March 1, 2026 to May 31, 2026, to provide reasonable assurance that IMocha'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 Organization and user entities applied the complementary controls assumed in the design of IMocha's controls throughout that period.

c) The controls stated in the description operated effectively throughout the period March 1, 2026 to May 31, 2026, to provide reasonable assurance that IMocha's service commitments and system

requirements were achieved based on the applicable trust services criteria, if the Subservice Organization and user entities applied the complementary controls assumed in the design of IMocha's controls operated effectively throughout that period.

For IMocha Inc.

Name: Sujit Karpe
Title: CTO
Date: 12-08-2026

SECTION 3 – DESCRIPTION OF THE SYSTEM

3 DESCRIPTION OF SYSTEMS PROVIDED BY THE SERVICE ORGANIZATION

3.1 Overview of service organization and in-scope services

iMocha is a cloud-based SaaS company that provides an AI-powered skills assessment and skills intelligence platform for enterprise and mid-market organizations. The platform applies artificial intelligence, machine learning and agentic workflows to help customers assess candidate and employee skills through a library of assessments and AI-led interviews, build and maintain skill taxonomies and skill profiles, and derive workforce skills intelligence to support hiring, internal mobility, learning and workforce planning decisions. iMocha delivers its solutions through secure cloud technologies hosted on Microsoft Azure, enabling customers to operate skills-based talent programs at scale.

The scope of this report includes the systems, processes, people and technology supporting the iMocha platform, comprising the App Platform, the Test Platform, the Talent Portal, Talent Management and the customer-facing API, including the development, deployment and delivery of AI-powered solutions, customer-facing web applications, APIs and related services, together with the management, operation and security of the production environment, supporting infrastructure, software development lifecycle and information assets used to deliver these services to customers. Any other services provided by iMocha Inc. are outside the scope of this report.

The scope of this report includes the following locations from where in-scope services are provided:

- US - iMocha Inc.
- India - Tecknack Technologies Pvt. Ltd.

3.2 Principal Service Commitments and System Requirements

iMocha designs its processes and procedures to meet objectives for its software application. Those objectives are based on the service commitments that iMocha makes to customers and the compliance requirements that iMocha has established for their services.

Security commitments to user entities are documented and communicated in iMocha's customer agreements, as well as in the description of the service offering provided online. iMocha's security commitments are standardized and based on some common principles.

These principles include but are not limited to, the following:

- The fundamental design of iMocha's software application addresses security concerns such that system users can access the information based on their role in the system and are restricted from accessing information not needed for their role.
- iMocha implements various procedures and processes to control access to the production environment and the supporting infrastructure.
- Monitoring of key infrastructure components is in place to collect and generate alerts based on utilization metrics.

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit.
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties.
- Confidential information must be used only for the purposes explicitly stated in agreements between iMocha and user entities.

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components.
- Responding to customer requests in a reasonably timely manner.
- Business continuity and disaster recovery plans are tested on a periodic basis.
- Operational procedures supporting the achievement of availability commitments to user entities.

iMocha establishes operational requirements that support the achievement of security commitments and other system requirements. Such requirements are communicated in iMocha's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal networks are managed, and how staff is hired.

3.3 Components of the System used to provide services

Infrastructure & Network Architecture

The production infrastructure for the iMocha platform is hosted on Microsoft Azure, with the primary production region in East US and a secondary replicated region in North Europe. The iMocha platform uses a virtual and secure network environment on top of Cloud infrastructure to ensure that the software application is always protected. This is achieved by hosting the application inside a dedicated Azure Virtual Network (VNet), segmented into subnets by application tier, with Network Security Groups (NSGs) applied at subnet and network interface level. The iMocha platform ensures there are only specific authorized points of entry, and filters traffic to the private networks that support the application.

When a customer's client device connects to the application over the internet, their data is encrypted and secured over HTTPS using TLS 1.2. Traffic resolves through Cloudflare, which provides DNS, web application firewall and DDoS protection, and then passes through the Azure endpoint and API Management layer into the Virtual Network that:

- houses the entire application runtime
- protects the application runtime from any external networks

The network is protected by deny-by-default Network Security Groups and firewalls to ensure that only deliberately allowed traffic can pass through. Furthermore, network flow logs, DNS logs, and other cloud console events are continuously monitored by cloud monitoring tooling to spot malicious activity and unauthorized behavior.

Software

iMocha is responsible for managing the development and operation of the iMocha platform including infrastructure components such as servers, databases, and storage systems. The in-scope infrastructure and software components used by the iMocha platform are shown in the table below:

System/ Application	Business Function / Description
iMocha platform	Access to the iMocha platform SaaS application – comprising the App Platform, Test Platform, Talent Portal, Talent Management and the customer-facing API – is through a web interface or API and user authentication. The application tier runs on Azure App Services and the production database is hosted on an Azure SQL Managed Instance.
Microsoft Entra ID	Identity and access management service used to administer users, groups, roles and permissions for iMocha corporate and cloud resources, with multi-factor authentication enforced for all users.
Azure Network Security Groups, Azure API Management and Cloudflare	Front-end firewalls protect the network perimeter with rule-based ACLs and back-end firewalls segregate the database servers from internal traffic. Cloudflare provides DNS, web application firewall, bot and DDoS protection at the perimeter, and Azure API Management enforces API key validation and rate limiting.
Azure DevOps	Source code repository, version control system, work item tracking and build software.
Microsoft 365 (Exchange Online, OneDrive and SharePoint)	Identity and email provider for iMocha personnel.

People

iMocha's staff have been organized into various functions including Engineering, Product, Information Technology, Customer Success, Sales, Marketing, Human Resources and Finance. The personnel have also been assigned to the following key roles:

- **Senior Management:** Senior management carries the ultimate responsibility for achieving the mission and objectives of the organization. They ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the organization's mission. They also assess and incorporate the results of the risk assessment activity into the decision-making process. The senior management understands that their support and involvement is required in order to run an effective risk management program that assesses and mitigates IT-related mission risks.
- **Information Security Officer:** The Senior Management assigns the role of Information Security Officer to one of its staff members who is responsible for the performance of the information security program of the organization. Decisions made in these areas are based on an effective risk management program. The Information Security Officer is responsible for identifying risks, threats, and vulnerabilities, and adding controls to mitigate these risks. Additionally, they also

summarize remaining residual risks and report the same to Senior Management in a timely manner.

- **Compliance Program Manager:** The company assigns the role of Compliance Program Manager to a staff member who would be responsible for the smooth functioning of the Information Security Program. The Compliance Program Manager takes care of the effective and timely completion of tasks required for the functioning of all information security controls, across all functions/departments of the organization.
- **System Users:** The organization's staff members are the users of the IT systems. The organization understands that use of the IT systems and data according to an organization's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, staff members that access IT resources are provided with annual security awareness training.

Data

Data, as defined by iMocha, constitutes the following:

- Transaction data
- Electronic interface files
- Output reports
- Input reports
- System files
- Error logs

All data that is managed, processed and stored as a part of the iMocha platform is classified as per the Information Classification and Asset Management Procedure which establishes a framework for categorizing data based on its sensitivity, value, and criticality to achieving the objectives of the organization. All data is to be assigned one of the following sensitivity levels:

Data Sensitivity	Description	Examples
Customer confidential	Highly valuable and sensitive information where the level of protection is dictated internally through policy and externally by legal and/or contractual requirements. Access to confidential information is limited to authorized employees, contractors, and business partners with a specific need.	- Customer system and operating data - Customer PII - Anything subject to a confidentiality agreement with a customer
Company Confidential	Information that originated or is owned internally or was entrusted to iMocha by others. Company confidential information may be shared with authorized employees, contractors, and business partners but not released to the general	- iMocha's PII - Unpublished financial information - Documents and processes explicitly marked as confidential

Data Sensitivity	Description	Examples
		- Pricing/marketing and other undisclosed strategies
Public	Information that has been approved for release to the public and is freely shareable both internally and externally.	- Press releases - Public website

Further, all customer data is treated as confidential. The availability of this data is also limited by job function. All customer data storage and transmission follow industry-standard encryption. The data is also regularly backed up as documented in the Backup Policy / Procedure.

Procedures and Policies

Formal policies and procedures have been established to support the iMocha platform. These policies cover:

- Acceptable Usage Policy
- Access Control Policy
- Anonymization and Pseudonymization Policy
- Anti-Malware Policy
- Backup Policy/ Procedure
- Business Continuity and Disaster Recovery Procedure
- Change Management Procedure
- Code of Conduct Policy
- Cryptography Policy
- Data Breach Management Procedure
- Data Protection Impact Assessment (DPIA) Procedure
- Data Retention and Disposal Policy
- Data Subject Rights Procedure
- HR Disciplinary Procedure
- Information Classification and Asset Management Procedure
- Information Security (IS) Policy
- Information Security Incident Management Policy
- Privacy Policy
- Logging and Monitoring Policy
- Management Review Meeting Procedure
- Mobile Devices and Teleworking Policy

- Network Security Policy
- Password Management Policy
- Patch & Vulnerability Management Policy
- Risk Management Procedure
- Security Incident Response Plan
- Supplier Management Policy
- System Hardening Procedure
- Threat Intelligence Policy

All policies are made available to all existing and new staff members to provide direction regarding the staff members' responsibilities related to the functioning of internal control. All staff members are expected to adhere to the policies and procedures that define how services should be delivered. Specifically, staff members are required to acknowledge their understanding of these policies upon hiring and annually thereafter.

iMocha also provides information to clients and staff members on how to report failures, incidents, concerns, or complaints related to the services or systems provided by the iMocha platform, in the event there are problems, and takes actions within an appropriate timeframe as and when issues are raised.

3.4 Relevant aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

The applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. This section provides information about the five interrelated components of internal control at iMocha, including:

1. Control environment
2. Risk assessment
3. Control activities
4. Information and communication
5. Monitoring controls

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of iMocha's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of iMocha's ethical and behavioral standards, how they are

communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct.

iMocha and its management team has established the following controls to incorporate ethical values throughout the organization:

- A formally documented "Code of business conduct" communicates the organization's values and behavioral standards to staff members.
- Staff members are required to acknowledge (upon hiring and annually thereafter) comprehensive policies and procedures covering the areas of Information Security, Change Management, Incident Management, and Access Control. Staff Members also acknowledge that they understand their responsibility for adhering to the policies and procedures.
- All new employees go through background checks as a part of the hiring process.

Commitment to Competence

iMocha's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. The following controls have been established in order to incorporate the commitment to competence throughout the organization:

- Management outlines the roles and responsibilities of technical staff to ensure that they are clear about their responsibilities in the organization. These roles and responsibilities are reviewed annually by the senior management.
- Annual Security Awareness Training is provided to all staff which focuses on maintaining the security of the proprietary and customer-servicing systems and related data.
- Employees receive periodic reviews by their supervisors inclusive of discussing any deficiencies noted in the execution of their job responsibilities.
- Employees are evaluated for competence in performing their job responsibilities at the time of hiring.

Management Philosophy and Operating Style

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

iMocha's information security function, composed of senior management and the Information Security Officer, meets frequently and includes at least an annual meeting to review policies and procedures and set the information security program roadmap. The security function, under the direction of senior management, oversees the security activities and communication of its policies and procedures.

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

- Senior management meetings are held to discuss major initiatives and issues that affect the business as a whole.

- Senior management reviews the functioning of internal controls, vendor risk assessment, risk assessment and high severity security incidents annually.

Organizational Structure and Assignment of Authority and Responsibility

iMocha's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

The management is committed to maintaining and improving its framework for how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. This also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties.

In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are accessible to all employees of the company and are updated as required.

Human Resources

iMocha's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by the management's ability to hire and retain top-quality personnel who ensure the service organization is operating at maximum efficiency.

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

- Validation of identity, past performance, and other background checks are performed on new hires, who are evaluated for competence in performing their job responsibilities at the time of hiring.
- Job positions are supported by job descriptions.
- New employees are required to acknowledge company policy and confidentiality related agreements upon hire and annually thereafter.
- Upon hire and annually thereafter, all employees must complete training courses covering basic information security practices.
- Performance evaluations for each employee are performed on an annual basis.
- If an employee violates the Code of Conduct in the employee handbook or the company's policies or otherwise acts in a manner deemed contrary to the mission and objectives of the company, the employee is subject to sanctions up to and including termination of employment.
- When a person is relieved of duties from the company, access to critical systems is made inaccessible in a timely manner.

Risk Assessment

iMocha's risk assessment process identifies and manages risks that could potentially affect its ability to provide reliable services to its customers. The management is expected to identify significant risks inherent in products and services as they oversee their areas of responsibility. iMocha identifies the underlying sources of risk, measures the impact on the organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process identifies risks to the services provided by the iMocha platform, and the management has implemented various measures designed to manage these risks.

iMocha believes that effective risk management is based on the following principles:

- Senior management's commitment to the security of iMocha platform.
- The involvement, cooperation, and insight of all iMocha staff.
- Initiating risk assessments with discovery and identification of risks.
- A thorough analysis of identified risks.
- Commitment to the strategy and treatment of identified risks.
- Communicating all identified risks to the senior management.
- Encouraging all iMocha staff to report risks and threat vectors.

Scope

The Risk Assessment and Management program applies to all systems and data that are a part of the iMocha platform. The iMocha risk assessment exercise evaluates infrastructure such as computer infrastructure, containing networks, instances, databases, systems, storage, and services. The risk assessments also include an analysis of business/IT practices, procedures, and physical spaces as needed.

Risk assessments may be high-level or detailed to a specific organizational or technical change as the stakeholders and technologists see fit.

Overall, the execution, development, and implementation of risk assessment and remediation programs is the joint responsibility of iMocha's Information Security Officer and the department or individuals responsible for the area being assessed. All iMocha staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Staff is further expected to work with the risk assessment project lead in the development of a remediation plan per risk assessment performed.

Vendor Risk Assessment

iMocha uses a number of vendors to meet its business objectives. iMocha understands that risks exist when engaging with vendors and as a result, continuously assesses those risks that could potentially affect the Company's ability to meet its business objectives.

iMocha employs several activities to effectively manage their vendors. Firstly, the Information Security Officer performs an annual exercise of thoroughly examining the nature and extent of risks involved with each vendor relationship. For critical vendors, iMocha assesses vendor compliance commitments through the review of available information security assessment reports and determines whether compliance levels adequately support iMocha's commitments to its customers. If a critical vendor is unable to provide a third-party security report or assessment, iMocha management meets with such vendors periodically to assess their performance, security concerns, and their services. Any vendor risks identified are recorded in the risk assessment matrix, which is reviewed annually by the Senior Management of the company.

Integration with Risk Assessment

As part of the design and operation of the system, iMocha identifies the specific risks that service commitments may not be met, and designs control necessary to address those risks. iMocha's management performs an annual Risk Assessment Exercise to identify and evaluate internal and external risks to the Company, as well as their potential impacts, likelihood, severity, and mitigating action.

Information and Communication

iMocha maintains a company-wide Information Security Policy, supported by detailed standards and training to ensure that employees understand their individual roles and responsibilities regarding security and significant events.

iMocha also has additional policies and procedures that define access management, change management, and authentication requirements and procedures for critical systems. These policies and procedures are published and made available to internal staff.

Monitoring Controls

iMocha management monitors control to ensure that they are operating as intended and that the controls are modified as conditions change. Monitoring activities are undertaken to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Staff activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, independent evaluations, or a combination of the two.

Control Activities

iMocha's control activities are defined through its established policies and procedures which address individual risks associated with the achievement of the company's objectives. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions.

Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action.

Physical Security

The in-scope production system and supporting infrastructure are hosted by Microsoft Azure. As such, Microsoft is responsible for the physical and environmental security controls of the in-scope production system. iMocha reviews the independent assurance reports published by Microsoft in respect of the Azure platform on an annual basis to ensure that its controls are in accordance with the standards expected by the customers of the iMocha platform.

Logical Access Control

The iMocha platform uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. User access, which is role-based, is controlled in the software application and authenticates to the database.

iMocha has identified certain systems that are critical to meet its service commitments. All-access to critical systems is under the principle of least required privilege (wherein a staff member is granted the minimum necessary access to perform their function) and controlled by the role of the staff member as well as a role-based access matrix prior to being issued system credentials and granted the ability to access the system. When a person is relieved of duties from the company, access to critical systems is made inaccessible in a timely manner.

The Information Security Officer is responsible for performing quarterly reviews of everyone who has access to the system and assessing the appropriateness of the access and permission levels and making modifications based on the principle of least privilege, whenever necessary.

Access to critical systems requires multi-factor authentication (MFA), which is enforced through Microsoft Entra ID for company email, the version control tool and cloud infrastructure. Staff members must use complex passwords, wherever possible, for all of their accounts that have access to iMocha customer data. Password policy settings require a minimum length of eight characters and complexity, require unique credentials that are not reused elsewhere, and require that any shared account credentials be held only in an approved password manager. Password configuration settings are configured on each critical system. Additionally, company-owned endpoints are configured to auto-screen-lock after defined time of inactivity, and removable media is disabled on company-issued assets.

Change Management

A documented Change Management Procedure guides all staff members in documenting and implementing application and infrastructure changes. It outlines how changes to the iMocha system are reviewed, deployed, and managed. The policy covers all changes made to the iMocha platform, regardless of their size, scope, or potential impact.

The change management policy is designed to mitigate the risks of:

- Corrupted or destroyed information.
- Degraded or disrupted software application performance.
- Productivity loss.

- Introduction of software bugs, configuration errors, vulnerabilities, etc.

A change to the iMocha platform can be initiated by a staff member with an appropriate role. iMocha uses Azure DevOps as its version control and work item tracking system to manage and record activities related to the change management process.

The version control system maintains source code versions and migrates source code through the development and testing process to the production environment. The version control software maintains a history of code changes to support rollback capabilities. It also facilitates the code review process which is mandated for all changes.

To initiate a change, the developer first creates a feature branch with the updated code. Once the code change is ready for review, the developer submits the code for peer review and automated testing, known as a pull request. For all code changes, the reviewer must be different from the author. Once a pull request is approved, the change can be released to production.

The ability to implement changes in the production infrastructure is restricted to only those individuals who require the ability to implement changes as part of their responsibilities.

Incident Management

iMocha has an incident management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers. Customers are directed to contact iMocha via the support email address provided during onboarding to report failures, incidents, concerns, or other complaints in the event there were problems.

Incident response procedures and centralized tracking tools consist of different channels for reporting production system incidents and weaknesses. Production infrastructure is configured to generate audit events for actions of interest related to operations and security. Security alerts are tracked, reviewed, and analyzed for anomalous or suspicious activity.

Where required, security incidents are escalated to privacy, legal, customer, or senior management team(s) and assigned a severity rating. Operational events are automatically resolved by the self-healing system.

- Low severity incidents are those that do not require immediate remediation. These typically include a partial service of iMocha being unavailable (for which workarounds exist). These do not require someone to be paged or woken up beyond normal work hours.
- Medium severity incidents are similar to low but could include scenarios like suspicious emails or unusual activity on a staff laptop. Again, these do not require immediate remediation or trigger automatic calls outside work hours. Low and medium-severity incidents usually cover the large majority of incidents found.
- High severity incidents are problems an active security attack has not yet happened but is likely. This includes situations like backdoors, malware, and malicious access to business data (e.g., passwords, payment information, vulnerability data, etc.). In such cases, the information security team must be informed, and immediate remediation steps should begin.

- Critical severity incidents are those where a security attack was successful and something important was lost (or irreparable damage caused to production services). Again, in such cases, immediate actions need to be taken to limit the damage.

Post-mortem activities are conducted for incidents with critical severity ratings. Results of post- mortems may include updates to the security program or changes to systems required as a result of incidents.

Cryptography

User requests to iMocha's systems are encrypted using Transport Layer Security (TLS) using certificates from an established third-party certificate authority. Remote system administration access to iMocha web and application servers is available through cryptographic network protocols (i.e., SSH) or an encrypted virtual private network (VPN) connection. Data at rest is encrypted using Advanced Encryption Standard (AES) 256-bit.

Asset Management (Hardware and Software)

Assets used in the system are inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels, as appropriate, to help ensure assets are classified appropriately, patched, and tracked as part of configuration management. iMocha maintains an IT asset inventory recording asset ownership, make and model, serial number and the individual to whom the asset is assigned, which is reviewed periodically. This helps to ensure a complete and accurate inventory of technology assets with the potential to store or process information is maintained.

Vulnerability Management and Penetration Testing

Vulnerability assessment and penetration testing of the in-scope web applications is performed by an independent third-party service provider, and automated compliance and configuration monitoring is performed on a continuous basis through the compliance management platform. Automated software update tools are used to help ensure operating systems are running the most recent security updates provided by the software vendor. Vulnerabilities identified are risk-ranked to prioritize the remediation of discovered vulnerabilities and are tracked to closure through the risk register.

Endpoint Management

Endpoint management solutions are in place that includes policy enforcement on company-issued devices, as well as bring-your-own devices that could connect to or access data within the system boundaries. Centrally managed anti-malware protection is deployed across workstations and removable media is disabled on company-issued endpoints. Policies enforced on endpoints include but are not limited to enabling screen lock, OS updates, and encryption at rest on critical devices/ workstations.

Availability

iMocha has a documented Business Continuity and Disaster Recovery Procedure, and testing performed against the recovery time objectives (RTOs) and recovery point objectives (RPOs). The production database hosted on Azure SQL Managed Instance is backed up automatically, with full backups weekly,

differential backups every 12 to 24 hours and transaction log backups every 5 to 10 minutes, retained in geo-redundant storage with long-term retention configured. A failover group maintains continuous replication of the primary instance in East US to a secondary instance in North Europe. Backup restoration is tested as part of operational activities and is included as part of the BCP test plan.

Boundaries of the System

The scope of this report includes the iMocha platform. It also includes the people, processes, and IT systems that are required to achieve our service commitments toward the customers of this application.

iMocha depends on a number of vendors to achieve its objectives. The scope of this report does not include the processes and controls performed by the vendors. The management understands that risks exist when engaging with vendors and has formulated a process for managing such risks, as detailed in the Risk Assessment section of this document.

3.5 Significant Events, Conditions and Security incidents during the audit period

This section describes significant events and conditions, including significant changes to the system, and any security or system incidents that occurred during the period March 1, 2026 to May 31, 2026 that are likely to be relevant to report users' understanding of how the system is used to provide the services, or that affected, or could have affected, iMocha’s achievement of its service commitments and system requirements based on the applicable trust services criteria relevant to Security, Availability, and Confidentiality.

There were no security or system incidents identified during the period that (a) were the result of controls that were not suitably designed or were not operating effectively to achieve one or more of iMocha’s service commitments and system requirements, or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements based on the applicable trust services criteria relevant to Security, Availability, and Confidentiality.

This includes the absence of any identified personal data breach that resulted in a significant failure to achieve iMocha’s privacy commitments during the period.

3.6 Complementary User Entity Controls

iMocha’s controls were designed with the assumption that certain internal controls would be in place at customer organizations. The application of such internal controls by customer organizations is necessary to achieve certain trust services criteria identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for processing of transactions for iMocha customers.

For customers to rely on the information processed through the iMocha’s software application, each customer is expected to evaluate its own internal controls to ensure appropriate control activities are in place. The following general procedures and controls should be considered. They should not, however, be regarded as a comprehensive list of all controls that should be implemented by customer organizations.

Complementary Customer Control List	Related Criteria
Customers are responsible for managing their organization's iMocha platform account as well as establishing any customized security solutions or automated processes through the use of setup features	CC5.1, CC5.2, CC5.3, CC6.1
Customers are responsible for ensuring that authorized users are appointed as administrators for granting access to their iMocha platform account	CC5.2, CC6.3
Customers are responsible for notifying iMocha of any unauthorized use of any password or account or any other known or suspected breach of security related to the use of iMocha platform.	CC7.2, CC7.3, CC7.4
Customers are responsible for any changes made to user and organization data stored within the iMocha platform.	CC8.1
Customers are responsible for communicating relevant security and availability issues and incidents to iMocha through identified channels.	CC7.2, CC7.3, CC7.4

3.7 Complementary Subservice Organization Controls

The controls at iMocha, together with the complementary controls at user entities, related to the iMocha platform and relevant to the Security, Availability, and Confidentiality ("in-scope trust services criteria"), cover only a portion of the overall system of internal control relevant to those criteria. The applicable trust services criteria cannot be achieved by the controls at iMocha alone; achieving them also depends on the suitable design and operating effectiveness of controls at the Subservice Organizations that provide services supporting the services iMocha delivers to its user entities.

iMocha uses the carve-out method to present the Subservice Organizations referenced in this description. Accordingly, this description does not include the controls at the Subservice Organizations. The description presents only the types of complementary Subservice Organization controls that iMocha assumes have been implemented and that are necessary, in combination with iMocha's own controls, to achieve the applicable trust services criteria. The scope of this examination does not extend to the controls in operation at the Subservice Organizations.

The Subservice Organizations used by iMocha relevant to providing services related to iMocha platform is shown below:

Subservice Organization	Service Provided
Microsoft Azure	Cloud computing services

Control Activities expected to be implemented by Subservice Organization	Applicable Criteria
Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.	CC6.1, CC6.2, CC6.3, CC6.5, CC7.2
Physical access and security to the data center facility are restricted to authorized personnel.	CC6.4, CC6.5
Environmental protection, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control	CC6.4, A1.2

Control Activities expected to be implemented by Subservice Organization	Applicable Criteria
requirements.	
Encryption methods are used to protect data in transit and at rest.	CC6.1
Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically.	A1.3
Policies and procedures to document repairs and modifications to the physical components of a facility including, but not limited to, hardware, walls, doors, locks, and other physical security components.	A1.2
A defined Data Classification Policy specifies classification levels and control requirements to meet the company's commitments related to confidentiality.	C1.1
A defined process is in place to sanitize and destroy hard drives and back up media containing customer data prior to leaving company facilities.	C1.2

3.8 Trust services criteria and Description of Related Controls

TSC Ref. #	Criteria	Control Number	Control Activity as specified by iMocha
Control Environment			
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	GOV-08	Mechanisms exist to define the context of its business model and document the mission of the organization.
		HRS-03	Mechanisms exist to define cybersecurity responsibilities for all personnel.
		HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.
		HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and privacy governance controls.
		GOV-01.1	Mechanisms exist to coordinate cybersecurity, privacy and business alignment through a steering committee or advisory board, comprising of key cybersecurity, privacy and business executives, which meets formally and on a regular basis.

TSC Ref. #	Criteria	Control Number	Control Activity as specified by iMocha
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and privacy policies, standards and procedures.
		GOV-04	Mechanisms exist to assign a qualified individual with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.
		HRS-03	Mechanisms exist to define cybersecurity responsibilities for all personnel.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.
		HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.
		HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.
		PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and privacy requirements within business process planning for projects / initiatives.
		SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.
		SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including basic security awareness training, ongoing awareness training and specific-system training.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	CAP-04	Automated mechanisms exist to centrally-monitor and alert on the operating state and health status of critical systems, applications and services.
		HRS-03	Mechanisms exist to define cybersecurity responsibilities for all personnel.
		HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.
		HRS-08	Mechanisms exist to perform annual formal performance evaluation all the employee to

TSC Ref. #	Criteria	Control Number	Control Activity as specified by iMocha
			assesses the individual's job performance, adherence to their assigned internal control responsibilities and alignment with the entity's principles, values, and objectives.
Communication And Information			
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	GOV-01.1	Mechanisms exist to coordinate cybersecurity, privacy and business alignment through a steering committee or advisory board, comprising of key cybersecurity, privacy and business executives, which meets formally and on a regular basis.
		GOV-08	Mechanisms exist to define the context of its business model and document the mission of the organization.
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.	AST-04	Mechanisms exist to maintain network architecture diagrams that: ▪ Contain sufficient detail to assess the security of the network's architecture; ▪ Reflect the current architecture of the network environment; and ▪ Document all sensitive/regulated data flows.
		CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.
		CLD-06.1	Mechanisms exist to formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for controls between the Cloud Service Provider (CSP) and its customers.
		CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.
		GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and privacy policies, standards and procedures.
		HRS-03	Mechanisms exist to define cybersecurity responsibilities for all personnel.
		IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.

TSC Ref. #	Criteria	Control Number	Control Activity as specified by iMocha
		TPM-05	Mechanisms exist to identify, regularly review and document third-party confidentiality, Non-Disclosure Agreements (NDAs) and other contracts that reflect the organization's needs to protect systems and data.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	CAP-04	Automated mechanisms exist to centrally-monitor and alert on the operating state and health status of critical systems, applications and services.
		CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.
		CLD-06.1	Mechanisms exist to formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for controls between the Cloud Service Provider (CSP) and its customers.
		CPL-02	Mechanisms exist to provide a security & privacy controls oversight function that reports to the organization's executive leadership.
		HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.
		IRO-10	Mechanisms exist to timely-report incidents to applicable: ▪ Internal stakeholders; ▪ Affected clients & third-parties; and ▪ Regulatory authorities.
		SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.
		TPM-05	Mechanisms exist to identify, regularly review and document third-party confidentiality, Non-Disclosure Agreements (NDAs) and other contracts that reflect the organization's needs to protect systems and data.
Risk Assessment			
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and privacy requirements within business process planning for projects / initiatives.

TSC Ref. #	Criteria	Control Number	Control Activity as specified by iMocha
	assessment of risks relating to objectives.	RSK-01	Mechanisms exist to facilitate the implementation of risk management controls.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	RSK-01	Mechanisms exist to facilitate the implementation of risk management controls.
		RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.
		RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.
		RSK-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices.
		RSK-06	Mechanisms exist to remediate risks to an acceptable level.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	AST-02	Mechanisms exist to perform inventories of technology assets that: ▪ Accurately reflects the current systems, applications and services in use; ▪ Identifies authorized software products, including business justification details; ▪ Is at the level of granularity deemed necessary for tracking and reporting; ▪ Includes organization-defined information deemed necessary to achieve effective property accountability; and ▪ Is available for review and audit by designated organizational personnel.
		RSK-01	Mechanisms exist to facilitate the implementation of risk management controls.
		VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.
		RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.

TSC Ref. #	Criteria	Control Number	Control Activity as specified by iMocha
		TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.
Monitoring Activities			
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.
		CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate security policies, standards and other applicable requirements.
		IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.
		IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.
		IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.
		MON-03	Mechanisms exist to configure systems to produce audit records that contain sufficient information to, at a minimum: ▪ Establish what type of event occurred; ▪ When (date and time) the event occurred; ▪ Where the event occurred; ▪ The source of the event; ▪ The outcome (success or failure) of the event; and ▪ The identity of any user/subject associated with the event.
		VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.
		VPM-06.6	Mechanisms exist to perform quarterly external vulnerability scans (outside the organization's network looking inward) via a reputable vulnerability service provider, which include rescans until passing results are obtained or all

TSC Ref. #	Criteria	Control Number	Control Activity as specified by iMocha
			"high" vulnerabilities are resolved, as defined by the Common Vulnerability Scoring System (CVSS).
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.
		END-05	Mechanisms exist to utilize host-based firewall software, or a similar technology, on all information systems, where technically feasible.
		GOV-01.1	Mechanisms exist to coordinate cybersecurity, privacy and business alignment through a steering committee or advisory board, comprising of key cybersecurity, privacy and business executives, which meets formally and on a regular basis.
		GOV-03	Mechanisms exist to review the cybersecurity and privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
		VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.
		VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.
		WEB-03	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.
Control Activities			
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.
		HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.
CC5.2	COSO Principle 11: The entity also selects and	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior

TSC Ref. #	Criteria	Control Number	Control Activity as specified by iMocha
	develops general control activities over technology to support the achievement of objectives.		organization management with insights into the appropriateness of the organization's technology and information governance processes.
		RSK-01	Mechanisms exist to facilitate the implementation of risk management controls.
		VPM-06.6	Mechanisms exist to perform quarterly external vulnerability scans (outside the organization's network looking inward) via a reputable vulnerability service provider, which include rescans until passing results are obtained or all “high” vulnerabilities are resolved, as defined by the Common Vulnerability Scoring System (CVSS).
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.	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.
		GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and privacy policies, standards and procedures.
Logical and Physical Access Controls			
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	AST-02	Mechanisms exist to perform inventories of technology assets that: ▪ Accurately reflects the current systems, applications and services in use; ▪ Identifies authorized software products, including business justification details; ▪ Is at the level of granularity deemed necessary for tracking and reporting; ▪ Includes organization-defined information deemed necessary to achieve effective property accountability; and ▪ Is available for review and audit by designated organizational personnel.
		AST-02.7	Mechanisms exist to protect Intellectual Property (IP) rights with software licensing restrictions.
		AST-04	Mechanisms exist to maintain network architecture diagrams that: ▪ Contain sufficient detail to assess the security of the network's architecture; ▪ Reflect the current architecture of the network environment; and ▪ Document all sensitive/regulated data flows.

TSC Ref. #	Criteria	Control Number	Control Activity as specified by iMocha
		AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally owned devices in the workplace.
		CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platform that are consistent with industry-accepted system hardening standards.
		DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.
		IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: ▪ Remote network access; ▪ Third-party systems, applications and/or services; and/ or ▪ Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.
		IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.
		IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.
		IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.
		IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.
		IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.
		IAC-19	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.
		IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."
		IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned

TSC Ref. #	Criteria	Control Number	Control Activity as specified by iMocha
			tasks in accordance with organizational business functions.
		NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.
		VPM-06.6	Mechanisms exist to perform quarterly external vulnerability scans (outside the organization's network looking inward) via a reputable vulnerability service provider, which include rescans until passing results are obtained or all “high” vulnerabilities are resolved, as defined by the Common Vulnerability Scoring System (CVSS).
		WEB-03	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.
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.	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.
		IAC-07.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.
		IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to organization-defined personnel or roles without management approval.
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.	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.
		IAC-19	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.
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		Not applicable as all the applications and information are hosted on cloud services provided by Azure.

TSC Ref. #	Criteria	Control Number	Control Activity as specified by iMocha
	locations) to authorized personnel to meet the entity's objectives.		
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.
		DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	CRY-05.3	Mechanisms exist to ensure that database servers utilize encryption to protect the confidentiality of the data within the databases.
		DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.
		IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.
		MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.
		MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.
		NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).
		NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.
		NET-04	Mechanisms exist to design, implement and review firewall and router configurations to restrict connections between untrusted networks and internal systems.
		NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).

TSC Ref. #	Criteria	Control Number	Control Activity as specified by iMocha
		NET-08.1	Mechanisms exist to require De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.
		NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.
		WEB-03	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.
		CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.
		DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.
		DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.
		DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.
		DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.
		DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.
		MDM-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of mobile device management controls.
		NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.
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.	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.
		END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.
System Operations			
CC7.1	To meet its objectives, the entity uses detection and	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for

TSC Ref. #	Criteria	Control Number	Control Activity as specified by iMocha
	monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		technology platform that are consistent with industry-accepted system hardening standards.
		VPM-06.6	Mechanisms exist to perform quarterly external vulnerability scans (outside the organization's network looking inward) via a reputable vulnerability service provider, which include rescans until passing results are obtained or all “high” vulnerabilities are resolved, as defined by the Common Vulnerability Scoring System (CVSS).
		VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.
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.	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.
		MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.
		MON-16	Mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.
		NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and privacy-related incidents.
		IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.
		IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.
		IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.

TSC Ref. #	Criteria	Control Number	Control Activity as specified by iMocha
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.	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and privacy-related incidents.
		IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.
		IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.
		IRO-10	Mechanisms exist to timely-report incidents to applicable: ▪ Internal stakeholders; ▪ Affected clients & third-parties; and ▪ Regulatory authorities.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and privacy incidents to reduce the likelihood or impact of future incidents.
Change Management			
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.
		CHG-02	Mechanisms exist to govern the technical configuration change control processes.
		CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.
		PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.
		TDA-06	Mechanisms exist to develop applications based on secure coding principles.
Risk Mitigation			
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services.
CC9.2	The entity assesses and manages risks associated	CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented

TSC Ref. #	Criteria	Control Number	Control Activity as specified by iMocha
	with vendors and business partners.		procedures within their area of responsibility to adhere to appropriate security policies, standards and other applicable requirements.
		RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.
		TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.
		TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of Third-Party Service Providers (TSP) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.
		TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.
		TPM-05	Mechanisms exist to identify, regularly review and document third-party confidentiality, Non-Disclosure Agreements (NDAs) and other contracts that reflect the organization’s needs to protect systems and data.
		TPM-08	Mechanisms exist to monitor, regularly review and audit Third-Party Service Providers (TSP) for compliance with established contractual requirements for cybersecurity and privacy controls.
Additional Criteria for Availability			
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	BCD-11.7	Mechanisms exist to maintain a failover system, that is not collocated with the primary system, application and/or service, which can be activated with little-to-no loss of information or disruption to operations.
		CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.
		CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.

TSC Ref. #	Criteria	Control Number	Control Activity as specified by iMocha
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services.
		BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization’s readiness to execute the plan.
		RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks.
Additional Criteria for Confidentiality			
C1.1	The entity identifies and maintains confidential information to meet the entity’s objectives related to confidentiality.	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.
C1.2	The entity disposes of confidential information to meet the entity’s objectives related to confidentiality.	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.

SECTION 4 – INFORMATION PROVIDED BY THE SERVICE AUDITORS: TEST OF CONTROLS

4 INFORMATION PROVIDED BY INDEPENDENT SERVICE AUDITORS: TEST OF CONTROLS

4.1 Objective of Our Examination

This report, including the description of tests of controls and results thereof in this section are intended solely for the information and use of iMocha, user entities of the iMocha system related to iMocha platform during some or all of the period March 1, 2026 through May 31, 2026, business partners of iMocha subject to risks arising from interactions with iMocha's system, 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, Subservice Organizations, and other parties.
- internal control and its limitations.
- complementary user-entity controls and how they interact with related controls at the service Organization to meet the applicable trust services criteria;
- the applicable trust services criteria; and
- the risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

This section presents the following information provided by iMocha:

- The controls established and specified by iMocha to achieve the specified trust services criteria.

Also included in this section is the following information provided by auditors:

- A description of the tests performed by auditors to determine whether iMocha's controls were operating with sufficient effectiveness to achieve specified trust services criteria. Auditors determined the nature, timing, and extent of the testing performed.
- The results of tests of controls.

The examination was conducted in accordance with the criteria as set forth in DC Section 200. 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance-2022) ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period March 1, 2026 through May 31, 2026 to provide reasonable assurance that iMocha's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality ("applicable trust services criteria") set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus-2022), of the American Institute of Certified Public Accountants (AICPA), and the AICPA Statement on Standards for Attestation Engagements No. 18 (SSAE 18), as amended by Statement on Standards for Attestation Engagements No. 21 (SSAE 21). These attestation standards are inclusive of the following: (1) AT-C section 105, Concepts Common to All Attestation Engagements; and (2) AT-C section 205, Assertion-Based

Examination Engagements. Our testing of iMocha' controls was restricted to the controls identified by iMocha to meet the criteria related to Security, Availability, and Confidentiality listed in Section 1 of this report and was not extended to controls described in Section 3 but not included in Section 4, or to controls that may be in effect at user entities or subservice organizations.

It is each user's responsibility to evaluate the information included in this report in relation to internal control in place at individual user entities and Subservice Organizations to obtain an understanding and to assess control risk at the user entities. The controls at user entities, Subservice Organizations, and iMocha's controls should be evaluated together. If effective user entity or Subservice Organizations controls are not in place, iMocha's controls may not compensate for such weaknesses.

4.2 Control Environment Elements

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for other components of internal control, providing discipline and structure. In addition to the tests of design, implementation, and operating effectiveness of controls identified by iMocha our procedures included tests of the following relevant elements of the iMocha control environment:

1. Environment
2. Internal Risk Assessment
3. Information and Communication
4. Monitoring
5. Control Activities

Such tests included inquiry of the appropriate management, supervisory, and staff personnel; observation of iMocha activities and operations, inspection of iMocha documents and records, and re-performance of the application of iMocha controls. The results of these tests were considered in planning the nature, timing, and extent of our testing of the control activities described in this section.

4.3 Applicable Trust Services Criteria, Controls, Tests of Operating Effectiveness, and Results of Tests

Our tests were designed to examine the iMocha description of the system related to iMocha as well as the suitability of the design and operating effectiveness of controls for a representative number of samples throughout the period of March 1, 2026 to May 31, 2026.

In selecting particular tests of the operational effectiveness of controls, we considered the (a) nature of the items being tested, (b) the types of available evidential matter, (c) the nature of the trust services principles and criteria to be achieved and (d) the expected efficiency and effectiveness of the test.

Testing the accuracy and completeness of information provided by iMocha is also a component of the testing procedures performed. Information we are utilizing as evidence may include, but is not limited to:

1. Standard 'out of the box' reports as configured within the system.

2. Parameter-driven reports generated by iMocha systems.
3. Custom-developed reports that are not standard to the application such as scripts, report writers, and queries.
4. Spreadsheets that include relevant information utilized for the performance or testing of a control.
5. iMocha - prepared analyses, schedules, or other evidence manually prepared and utilized by the Company.

While these procedures are not specifically called out in the test procedures listed in this section, they are completed as a component of our testing to support the evaluation of whether or not the information is sufficiently precise and detailed for purposes of fully testing the controls identified by iMocha.

4.4 Description of Testing Procedures Performed

Our examination included inquiry of management, supervisory, and staff personnel; inspection of documents and records; observation of activities and operations; and re-performance of controls surrounding and provided by iMocha. Our tests of controls were performed on controls as they existed during the period of March 1, 2026 through May 31, 2026, and were applied to those controls relating to the trust services principles and criteria.

Tests performed of the operational effectiveness of controls are described below:

Test	Description
Inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the report period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.
Observation	Observed the performance of the control multiple times throughout the report period to evidence application of the specific control activity.
Examination of Documentation/Inspection	If the performance of the control is documented, inspected documents and reports indicating performance of the control.
Re-performance of Monitoring Activities or Manual Controls	Obtained documents used in the monitoring activity or manual control activity and independently re-performed the procedures. Compared any exception items identified with those identified by the responsible control owner.
Re-performance of Programmed Processing	Input test data, manually calculated expected results, and compared actual results of processing to expectations.

Reporting on Results of Testing

The concept of materiality is not applied when reporting the results of tests of controls for which deviations have been identified because the service auditor does not have the ability to determine whether a deviation will be relevant to a particular user entity. Consequently, the service auditor reports all deviations.

4.5 Testing Procedures Performed by Independent Service Auditor

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
CC1.1 CC2.1	GOV-08	Mechanisms exist to define the context of its business model and document the mission of the organization.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the mission statement to ascertain whether mechanisms exist to define the context of its business model and document the mission of the organization. Inspected the current approved version of the governance document evidencing an in-period review and version history, and the management / steering-committee meeting minutes at which the matter was reviewed during the period, to determine whether the control operated effectively throughout the period.	No exception noted.
CC1.1 CC1.3 CC1.5 CC2.2	HRS-03	Mechanisms exist to define cybersecurity responsibilities for all personnel.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected roles and responsibilities document to ascertain whether mechanisms exist to define cybersecurity responsibilities for all personnel.	No exception noted.
CC1.1 CC1.5	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Acceptable Use Policy to ascertain whether mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior. For a sample of employees, inspected the signed policy	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
			acknowledgements, to determine whether the control operated effectively throughout the period.	
CC1.1	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third parties.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the executed Non-Disclosure Agreement and employment agreement templates and, for a sample of personnel, the signed agreements on file. Noted that there were no new joiners during the audit period.	The operating effectiveness of the control could not be determined as there was no related activity during the audit period.
CC1.2	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and privacy governance controls.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Internal Privacy Policy to ascertain whether mechanisms exist to facilitate the implementation of cybersecurity and privacy governance controls. Inspected the current approved version of the governance document evidencing an in-period review and version history, and the management / steering-committee meeting minutes at which the matter was reviewed during the period, to determine whether the control operated effectively throughout the period.	No exception noted.
CC1.2 CC2.1 CC4.2	GOV-01.1	Mechanisms exist to coordinate cybersecurity, privacy and business alignment through a steering committee or advisory board, comprising of key cybersecurity, privacy and business executives,	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected management meeting minutes to ascertain whether mechanisms exist to coordinate cybersecurity, privacy and business alignment through a steering committee or advisory board, comprising of key	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
		which meets formally and on a regular basis.	cybersecurity, privacy and business executives, which meets formally and on a regular basis.	
CC1.3 CC2.2 CC5.3	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and privacy policies, standards and procedures.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Internal Privacy Policy to ascertain whether mechanisms exist to establish, maintain and disseminate cybersecurity and privacy policies, standards and procedures. Inspected the current approved version of the governance document evidencing an in-period review and version history, and the management / steering-committee meeting minutes at which the matter was reviewed during the period, to determine whether the control operated effectively throughout the period.	No exception noted.
CC1.3	GOV-04	Mechanisms exist to assign a qualified individual with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected Chief Information Security Officer Roles and Responsibilities document to ascertain whether mechanisms exist to assign a qualified individual with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program. Inspected the current approved version of the governance document evidencing an in-period review and version history, and the management / steering-committee meeting minutes at which the matter was reviewed during the	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
			period, to determine whether the control operated effectively throughout the period.	
CC1.4	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Human Resource Security Policy to ascertain whether mechanisms exist to facilitate the implementation of personnel security controls. For a sample of employees, inspected the signed policy acknowledgements, to determine whether the control operated effectively throughout the period.	No exception noted.
CC1.4 CC2.3	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the ISMS training completion records to ascertain whether mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	No exception noted.
CC1.4	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Noted that there were no new joiners during the audit period.	The operating effectiveness of the control could not be determined as there was no related activity during the audit period.
CC1.4 CC3.1	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and privacy requirements within business	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected Manpower Planning/Hiring Plan to ascertain whether mechanisms exist to identify and allocate resources	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
		process planning for projects / initiatives.	for management, operational, technical and privacy requirements within business process planning for projects / initiatives. Inspected the planning artefacts produced during the period and evidence of management review and approval, to determine whether the control operated effectively throughout the period.	
CC1.4	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Human Resource Security Policy and the Security & Privacy Awareness Training Report to ascertain whether mechanisms exist to facilitate the implementation of security workforce development and awareness controls. For a sample of employees and contractors, inspected the training-completion records and certificates evidencing completion of the assigned security and privacy awareness training during the period, to determine whether the control operated effectively throughout the period.	No exception noted.
CC1.4	SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including basic security awareness training, ongoing awareness training and specific-system training.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Security & Privacy Awareness Training Report to ascertain whether mechanisms exist to document, retain and monitor individual training activities, including basic security awareness training, ongoing awareness training and specific-system training. For a sample of employees and contractors, inspected the	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
			training-completion records and certificates evidencing completion of the assigned security and privacy awareness training during the period, to determine whether the control operated effectively throughout the period.	
CC1.5 CC2.3	CAP-04	Automated mechanisms exist to centrally-monitor and alert on the operating state and health status of critical systems, applications and services.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Logging and Monitoring Policy and the Capacity Monitoring Reports & Management Review to ascertain whether automated mechanisms exist to centrally-monitor and alert on the operating state and health status of critical systems, applications and services.	No exception noted.
CC1.5	HRS-08	Mechanisms exist to perform annual formal performance evaluation all the employee to assesses the individual's job performance, adherence to their assigned internal control responsibilities and alignment with the entity's principles, values, and objectives.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample employees, performance evaluation report to ascertain whether mechanisms exist to perform annual formal performance evaluation all the employee to assesses the individual's job performance, adherence to their assigned internal control responsibilities and alignment with the entity's principles, values, and objectives.	No exception noted.
CC2.1	CPL-04	Mechanisms exist to thoughtfully plan audits by including input from operational risk and compliance partners to minimize the impact of audit-related activities on business operations.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Internal Audit, Continual Improvement and Non-Conformity and Corrective Action Policy to ascertain whether mechanisms exist to thoughtfully plan audits by including input from operational risk and compliance partners to minimize the impact of audit-related activities on business operations.	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
			Inspected the compliance / audit calendar and the completed internal audit report for the period, together with evidence that resulting findings were tracked to closure, to determine whether the control operated effectively throughout the period.	
CC2.2 CC6.1	AST-04	Mechanisms exist to maintain network architecture diagrams that: ▪ Contain sufficient detail to assess the security of the network's architecture; ▪ Reflect the current architecture of the network environment; and ▪ Document all sensitive/regulated data flows.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Reviewed and Approved Network Diagram to ascertain whether mechanisms exist to maintain network architecture diagrams that: ▪ Contain sufficient detail to assess the security of the network's architecture; ▪ Reflect the current architecture of the network environment; and ▪ Document all sensitive/regulated data flows.	No exception noted.
CC2.2 CC2.3	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Change Management Procedure and, for a sample of changes, the change tickets to ascertain whether mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	No exception noted.
CC2.2 CC2.3	CLD-06.1	Mechanisms exist to formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for controls between the Cloud Service Provider (CSP) and its customers.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Information Security (IS) Policy to ascertain whether mechanisms exist to formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for controls between the Cloud Service Provider (CSP) and its customers.	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
			Inspected the cloud-service configuration and the Customer Responsibility Matrix in effect during the period, to determine whether the control operated effectively throughout the period.	
CC2.2	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Risk Register to ascertain whether mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. Inspected the compliance / audit calendar and the completed internal audit report for the period, together with evidence that resulting findings were tracked to closure, to determine whether the control operated effectively throughout the period.	No exception noted.
CC2.2 CC7.3 CC7.4	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Information Security Incident Management Policy to ascertain whether mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	No exception noted.
CC2.2 CC2.3 CC9.2	TPM-05	Mechanisms exist to identify, regularly review and document third-party confidentiality, Non-Disclosure Agreements (NDAs) and other contracts that reflect the organization's needs to protect systems and data.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Supplier Management Policy and the Processor Contract (DPA) to ascertain whether mechanisms exist to identify, regularly review and document third-party confidentiality, Non-Disclosure Agreements (NDAs) and	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
			other contracts that reflect the organization's needs to protect systems and data.	
CC2.3	CPL-02	Mechanisms exist to provide a security & privacy controls oversight function that reports to the organization's executive leadership.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Information Security Roles and Responsibilities document to ascertain whether mechanisms exist to provide a security & privacy controls oversight function that reports to the organization's executive leadership.	No exception noted.
CC2.3 CC7.4	IRO-10	Mechanisms exist to timely-report incidents to applicable: ▪ Internal stakeholders; ▪ Affected clients & third-parties; and ▪ Regulatory authorities.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Information Security Incident Management Policy and the Data Breach Management Procedure to ascertain whether mechanisms exist to timely-report incidents to applicable: ▪ Internal stakeholders; ▪ Affected clients & third-parties; and ▪ Regulatory authorities.	No exception noted.
CC2.3	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Security & Privacy Awareness Training Report to ascertain whether mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function. For a sample of employees and contractors, inspected the training-completion records, to determine whether the control operated effectively throughout the period.	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
CC3.1 CC3.2 CC3.3 CC5.2	RSK-01	Mechanisms exist to facilitate the implementation of risk management controls.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Risk Management Procedure to ascertain whether mechanisms exist to facilitate the implementation of risk management controls. Inspected the risk assessment performed during the period and the Risk Register evidencing in-period updates, assigned risk owners and treatment plans, and re-performed the traceability of a sample of risks to their treatment, to determine whether the control operated effectively throughout the period.	No exception noted.
CC3.2 CC3.4	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Risk Management Procedure and the Risk Register to ascertain whether mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data. Inspected the risk assessment performed during the period and the Risk Register evidencing in-period updates, assigned risk owners and treatment plans, and re-performed the traceability of a sample of risks to their treatment, to determine whether the control operated effectively throughout the period.	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
CC3.2	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Risk Register to ascertain whether mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	No exception noted.
CC3.2	RSK-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the risk register to ascertain whether mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices. Inspected the risk assessment performed during the period and the Risk Register evidencing in-period updates, assigned risk owners and treatment plans, and re-performed the traceability of a sample of risks to their treatment, to determine whether the control operated effectively throughout the period.	No exception noted.
CC3.2	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Risk Management Procedure and the Risk Register to ascertain whether mechanisms exist to remediate risks to an acceptable level. Inspected the risk assessment performed during the period and the Risk Register evidencing in-period updates, assigned risk owners and treatment plans, and re-performed the traceability of a sample of risks to their treatment, to	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
			determine whether the control operated effectively throughout the period.	
CC3.3 CC6.1	AST-02	Mechanisms exist to perform inventories of technology assets that: ▪ Accurately reflects the current systems, applications and services in use; ▪ Identifies authorized software products, including business justification details; ▪ Is at the level of granularity deemed necessary for tracking and reporting; ▪ Includes organization-defined information deemed necessary to achieve effective property accountability; and ▪ Is available for review and audit by designated organizational personnel.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Information Classification and Asset Management Procedure and the Documented Asset Inventory and Review Dates to ascertain whether mechanisms exist to perform inventories of technology assets that: ▪ Accurately reflects the current systems, applications and services in use; ▪ Identifies authorized software products, including business justification details; ▪ Is at the level of granularity deemed necessary for tracking and reporting; ▪ Includes organization-defined information deemed necessary to achieve effective property accountability; and ▪ Is available for review and audit by designated organizational personnel.	No exception noted.
CC3.3	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Patch & Vulnerability Management Policy and the Patch Management Records to ascertain whether mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware. Inspected the vulnerability scan during the period and, for a sample of findings, the remediation tickets evidencing resolution within the defined SLA, to determine whether the control operated effectively throughout the period.	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
CC3.4 CC9.2	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Supplier Management Policy and the Review of Vendor Audit Reports to ascertain whether mechanisms exist to periodically assess supply chain risks associated with systems, system components and services. Inspected the risk assessment performed during the period and the Risk Register evidencing in-period updates, assigned risk owners and treatment plans, and re-performed the traceability of a sample of risks to their treatment, to determine whether the control operated effectively throughout the period.	No exception noted.
CC3.4 CC9.2	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Supplier Management Policy to ascertain whether mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services. For a sample of active third parties, inspected the vendor due-diligence, risk-assessment and ongoing-monitoring records (including any SOC / assurance reports reviewed) during the period, to determine whether the control operated effectively throughout the period.	No exception noted.
CC4.1 CC4.2 CC5.1 CC5.2	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the compliance / audit calendar and the	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
CC5.3		insights into the appropriateness of the organization's technology and information governance processes.	completed internal audit report for the period, together with evidence that resulting findings were tracked to closure, to determine whether the control operated effectively throughout the period. Inspected Internal audit report to ascertain whether mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	
CC4.1 CC9.2	CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate security policies, standards and other applicable requirements.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Management Review Meeting Procedure and the minutes of monthly departmental meetings to ascertain whether mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate security policies, standards and other applicable requirements.	No exception noted.
CC4.1 CC6.1 CC6.2	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Access Control Policy to ascertain whether mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights. For a sample of personnel exiting during the period, inspected the exit clearance checklist and the confirmation of email and physical access deactivation on the last working	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
			day. No onboarding activity within the examination period was evidenced.	
CC4.1 CC6.1 CC6.3	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Access Control Policy and the Role Based Access on Production resources configuration to ascertain whether mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	No exception noted.
CC4.1	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Reports of User Access Reviews to ascertain whether mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary. Inspected the access request log and the role-based group membership listing for the production subscription, and enquired whether a periodic access review was performed and documented during the period.	No exception noted.
CC4.1	MON-03	Mechanisms exist to configure systems to produce audit records that contain sufficient information to, at a minimum: ▪ Establish what type of event occurred; ▪ When (date and time) the event occurred; ▪ Where the event occurred; ▪ The source of the event; ▪ The outcome	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Logging and Monitoring Policy to ascertain whether mechanisms exist to configure systems to produce audit records that contain sufficient information to, at a minimum: ▪ Establish what type of event occurred; ▪ When (date and time) the event occurred; ▪ Where the event	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
		(success or failure) of the event; and ▪ The identity of any user/subject associated with the event.	occurred; ▪ The source of the event; ▪ The outcome (success or failure) of the event; and ▪ The identity of any user/subject associated with the event.	
CC4.1 CC4.2	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected Patch & Vulnerability Management Policy and vulnerability scan report to ascertain whether mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	No exception noted.
CC4.1 CC5.2 CC6.1 CC7.1	VPM-06.6	Mechanisms exist to perform quarterly external vulnerability scans (outside the organization's network looking inward) via a reputable vulnerability service provider, which include rescans until passing results are obtained or all “high” vulnerabilities are resolved, as defined by the Common Vulnerability Scoring System (CVSS).	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Patch & Vulnerability Management Policy and the vulnerability assessment and penetration testing reports to ascertain whether mechanisms exist to perform quarterly external vulnerability scans via a vulnerability service provider, and determined the dates on which the scans were performed and the reports issued.	No exception noted.
CC4.2	END-05	Mechanisms exist to utilize host-based firewall software, or a similar technology, on all information systems, where technically feasible.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the System Hardening Procedure to ascertain whether mechanisms exist to utilize host-based firewall software, or a similar technology, on all information systems, where technically feasible.	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
			For a sample of production endpoints, inspected the endpoint agent / hardening status during the period, to determine whether the control operated effectively throughout the period.	
CC4.2	GOV-03	Mechanisms exist to review the cybersecurity and privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Management Review Meeting Procedure to ascertain whether mechanisms exist to review the cybersecurity and privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	No exception noted.
CC4.2	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Patch & Vulnerability Management Policy and the Patch Management Records to ascertain whether mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated. Inspected the vulnerability scan report issued during the period and, for a sample of findings, the remediation tickets evidencing resolution within the defined SLA, to determine whether the control operated effectively throughout the period.	No exception noted.
CC4.2 CC6.1 CC6.6	WEB-03	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Network Security Policy to ascertain whether mechanisms exist to deploy Web Application Firewalls	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
			(WAFs) to provide defense-in-depth protection for application-specific threats. Inspected the production web / network protection configuration and enforced rules in effect during the period, to determine whether the control operated effectively throughout the period.	
CC5.1	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Access Control Policy and the Separation of Development, Test and Production Environment configuration to ascertain whether mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	No exception noted.
CC6.1	AST-02.7	Mechanisms exist to protect Intellectual Property (IP) rights with software licensing restrictions.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Information Classification and Asset Management Procedure and the Documented Asset Inventory and Review Dates to ascertain whether mechanisms exist to protect Intellectual Property (IP) rights with software licensing restrictions. Inspected the asset inventory evidencing in-period updates, to determine whether the control operated effectively throughout the period.	No exception noted.
CC6.1	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk	Inquired with the management regarding the control activity to ascertain that the control operates as described.	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
		associated with personally owned devices in the workplace.	Inspected the Mobile Devices and Teleworking Policy to ascertain whether mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace. Inspected the asset inventory evidencing in-period updates and to determine whether the control operated effectively throughout the period.	
CC6.1 CC7.1	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platform that are consistent with industry-accepted system hardening standards.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the System Hardening Procedure and the System Hardening Procedure to ascertain whether mechanisms exist to develop, document and maintain secure baseline configurations for technology platform that are consistent with industry-accepted system hardening standards.	No exception noted.
CC6.1	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Information Classification and Asset Management Procedure to ascertain whether mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	No exception noted.
CC6.1	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: ▪ Remote network access; ▪ Third-party systems, applications and/or services; and/ or ▪ Non-console access to critical systems or	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Access Control Policy and the Password Configuration for All In-Scope Applications and Infrastructure to ascertain whether automated mechanisms	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
		systems that store, transmit and/or process sensitive/regulated data.	exist to enforce Multi-Factor Authentication (MFA) for: ▪ Remote network access; ▪ Third-party systems, applications and/or services; and/ or ▪ Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	
CC6.1	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Password Management Policy and the Password Configuration for All In-Scope Applications and Infrastructure to ascertain whether mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	No exception noted.
CC6.1	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Access Control Policy and access group mapping to ascertain whether mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	No exception noted.
CC6.1	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Access Control Policy and the Privilege Access Management records to ascertain whether mechanisms exist to restrict and control privileged access rights for users and services.	No exception noted.
CC6.1 CC6.3	IAC-19	Mechanisms exist to prevent the sharing of generic IDs, passwords or	Inquired with the management regarding the control activity to ascertain that the control operates as described.	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
		other generic authentication methods.	Inspected the Access Control Policy and list of active users to ascertain whether mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.	
CC6.1	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Access Control Policy and the Role Based Access on Production resources configuration to ascertain whether mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	No exception noted.
CC6.1	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Access Control Policy and the Privilege Access Management records to ascertain whether mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	No exception noted.
CC6.1 CC6.6	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Network Security Policy to ascertain whether mechanisms exist to define, control and review organization-approved, secure remote access methods.	No exception noted.
CC6.2	IAC-07.1	Mechanisms exist to revoke user access rights following changes in	Inquired with the management regarding the control activity to ascertain that the control operates as described.	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
		personnel roles and duties, if no longer necessary or permitted.	Inspected the Access Control Policy and, for a sample of terminated users, the Offboarding - Logical Access & Physical Access Revocation records to ascertain whether mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	
CC6.2	IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to organization-defined personnel or roles without management approval.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Access Control Policy and the Privilege Access Management records to ascertain whether mechanisms exist to restrict the assignment of privileged accounts to organization-defined personnel or roles without management approval.	No exception noted.
CC6.5	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Information Classification and Asset Management Procedure to ascertain whether mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components. Inspected the asset inventory, to determine whether the control operated effectively throughout the period.	No exception noted.
CC6.5	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Information Classification and Asset Management Procedure and the Personal Information	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
			Disposal records to ascertain whether mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	
CC6.6	CRY-05.3	Mechanisms exist to ensure that database servers utilize encryption to protect the confidentiality of the data within the databases.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Cryptography Policy and the Encryption for Data at Rest configuration to ascertain whether mechanisms exist to ensure that database servers utilize encryption to protect the confidentiality of the data within the databases.	No exception noted.
CC6.6 CC6.7	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Information Classification and Asset Management Procedure and the Removable Media Disabled for Servers, Laptops, and Desktops configuration to ascertain whether mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	No exception noted.
CC6.6	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Access Control Policy and the Password Configuration for All In-Scope Applications and Infrastructure to ascertain whether mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	No exception noted.
CC6.6 CC7.2	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to	Inquired with the management regarding the control activity to ascertain that the control operates as described.	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
		support the centralized collection of security-related event logs.	Inspected the Logging and Monitoring Policy to ascertain whether mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.	
CC6.6	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Logging and Monitoring Policy to ascertain whether mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	No exception noted.
CC6.6	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Network Security Policy to ascertain whether mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC). Inspected the production firewall and network-device rule-base configuration in effect during the period, and re-performed inspection of the rule base against the approved standard, to determine whether the control operated effectively throughout the period.	No exception noted.
CC6.6	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the firewall configuration and network architecture diagram to ascertain whether mechanisms exist to monitor and control communications at the external	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
			network boundary and at key internal boundaries within the network.	
CC6.6	NET-04	Mechanisms exist to design, implement and review firewall and router configurations to restrict connections between untrusted networks and internal systems.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the firewall configuration to ascertain whether mechanisms exist to design, implement and review firewall and router configurations to restrict connections between untrusted networks and internal systems.	No exception noted.
CC6.6	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the firewall configuration to ascertain whether mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception.	No exception noted.
CC6.6	NET-08.1	Mechanisms exist to require De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the network architecture diagram to ascertain whether mechanisms exist to require De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	No exception noted.
CC6.7	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the SSL Labs report and SSL/TLS certificate to ascertain whether cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
CC6.7	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the encryption configuration for production databases, servers, and cloud storage to ascertain whether cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	No exception noted.
CC6.7	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Information Security Policy and Internal Privacy Policy to ascertain whether mechanisms exist to facilitate the implementation of data protection controls. Inspected the system configuration enforcing the data-handling requirement in effect during the period (e.g., classification labelling, removable-media / DLP restriction or retention settings) to determine whether the control operated effectively throughout the period.	No exception noted.
CC6.7	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the removable media restriction configuration to ascertain whether mechanisms exist to restrict the use of types of digital media on systems or system components.	No exception noted.
CC6.7	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the removable media restriction configuration to ascertain whether mechanisms exist to restrict or prohibit	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
			the use of portable storage devices by users on external systems.	
CC6.7	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Information Classification and Asset Management Procedure and the Internal Privacy Policy to ascertain whether mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected. Inspected the system configuration enforcing the data-handling requirement in effect during the period (e.g., classification labelling, removable-media / DLP restriction or retention settings), to determine whether the control operated effectively throughout the period.	No exception noted.
CC6.7	MDM-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of mobile device management controls.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Mobile Devices and Teleworking Policy to ascertain whether mechanisms exist to develop, govern & update procedures to facilitate the implementation of mobile device management controls. For a sample of managed mobile / endpoint devices, inspected the enforced MDM configuration and enrolment status during the period, to determine whether the control operated effectively throughout the period.	No exception noted.
CC6.7 CC7.2	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive	Inquired with the management regarding the control activity to ascertain that the control operates as described.	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
		information as it is stored, transmitted and processed.	Inspected the Internal Privacy Policy to ascertain whether automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed. Inspected the production firewall and network-device rule-base configuration in effect during the period, and re-performed inspection of the rule base against the approved standard, to determine whether the control operated effectively throughout the period.	
CC6.8	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the System Hardening Procedure to ascertain whether automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	No exception noted.
CC6.8	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	Inquired with the management regarding the control activity to ascertain that the control operates as described. For a sample of production endpoints, inspected the endpoint agent / hardening status during the period, to determine whether the control operated effectively throughout the period. Inspected, for sample laptops, status of anti-malware solution to ascertain whether mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	No exception noted.
CC7.1	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	Inquired with the management regarding the control activity to ascertain that the control operates as described.	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
			Inspected the vulnerability assessment and penetration testing reports issued by the independent service provider and determined the dates on which the testing was performed.	
CC7.2	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Log Management and Monitoring Policy to ascertain whether mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	No exception noted.
CC7.2	MON-16	Mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Logging and Monitoring Policy to ascertain whether mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities. Inspected the logging and monitoring tooling configuration (e.g., Azure Monitor / the SIEM) and, for a sample of dates or generated alerts during the period, the underlying logs and evidence of review and follow-up, to determine whether the control operated effectively throughout the period.	No exception noted.
CC7.3 CC7.4	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Information Security Incident Management Policy to ascertain whether mechanisms exist to implement	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
		capability for cybersecurity and privacy-related incidents.	and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and privacy-related incidents. Inspected the incident register maintained during the period and, for a sample of incidents recorded, the records of triage, response and closure, to determine whether the control operated effectively throughout the period.	
CC7.3 CC7.4	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Information Security Incident Management Policy to ascertain whether mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	No exception noted.
CC7.3	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Information Security Incident Management Policy and the Security incident register to ascertain whether mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations. Noted that there were no security incidents during the audit period.	The operating effectiveness of the control could not be determined as there was no related activity during the audit period.
CC7.5	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and privacy	Inquired with the management regarding the control activity to ascertain that the control operates as described.	The operating effectiveness of the control could not be determined as there was

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
		incidents to reduce the likelihood or impact of future incidents.	Inspected the Information Security Incident Management Policy to ascertain whether mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and privacy incidents to reduce the likelihood or impact of future incidents. Noted that there were incidents related to cybersecurity and privacy during the audit period.	no related activity during the audit period.
CC8.1	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Change Management Procedure to ascertain whether mechanisms exist to facilitate the implementation of a change management program. For a sample of changes deployed to production during the period, inspected the change tickets evidencing request, testing, authorization and deployment, to determine whether the control operated effectively throughout the period.	No exception noted.
CC8.1	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample changes, change tickets to ascertain whether mechanisms exist to govern the technical configuration change control processes.	No exception noted.
CC8.1	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Change Management Procedure to ascertain whether mechanisms exist to appropriately test and	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
		implemented in a production environment.	document proposed changes in a non-production environment before changes are implemented in a production environment. For a sample of changes deployed to production during the period, inspected the change tickets evidencing request, testing, authorization and deployment to determine whether the control operated effectively throughout the period.	
CC8.1	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Change Management Procedure to ascertain whether mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	No exception noted.
CC8.1	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Change Management Procedure to ascertain whether mechanisms exist to develop applications based on secure coding principles. For a sample of releases or code changes during the period, inspected evidence of peer code review and application security testing performed, to determine whether the control operated effectively throughout the period.	No exception noted.
CC9.1 A1.3	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services.	Inquired with the management regarding the control activity to ascertain that the control operates as described.	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
			Inspected the Supplier Management Policy to ascertain whether mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services. Inspected the backup job execution logs, restoration test results and the most recent DR / BCP exercise results covering the period, to determine whether the control operated effectively throughout the period.	
CC9.2	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Supplier Management Policy to ascertain whether mechanisms exist to facilitate the implementation of third-party management controls. For a sample of active third parties, inspected the vendor due-diligence, risk-assessment and ongoing-monitoring records (including any SOC / assurance reports reviewed) during the period, to determine whether the control operated effectively throughout the period.	No exception noted.
CC9.2	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of Third-Party Service Providers (TSP) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Supplier Management Policy and Vendor Risk Register to ascertain whether mechanisms exist to maintain a current, accurate and complete list of Third-Party Service Providers (TSP) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
			For a sample of active third parties, inspected the vendor due-diligence, risk-assessment and ongoing-monitoring records (including any SOC / assurance reports reviewed) during the period, to determine whether the control operated effectively throughout the period.	
CC9.2	TPM-08	Mechanisms exist to monitor, regularly review and audit Third-Party Service Providers (TSP) for compliance with established contractual requirements for cybersecurity and privacy controls.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Supplier Management Policy to ascertain whether mechanisms exist to monitor, regularly review and audit Third-Party Service Providers (TSP) for compliance with established contractual requirements for cybersecurity and privacy controls.	No exception noted.
A1.1	BCD-11.7	Mechanisms exist to maintain a failover system, that is not collocated with the primary system, application and/or service, which can be activated with little-to-no loss of information or disruption to operations.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Multi-Availability Zone configuration to ascertain whether mechanisms exist to maintain a failover system, that is not collocated with the primary system, application and/or service, which can be activated with little-to-no loss of information or disruption to operations.	No exception noted.
A1.1	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected Azure Monitor and capacity monitoring dashboards showing utilisation monitoring and alerting for production App Service plans and the Azure SQL Managed Instance to ascertain whether mechanisms exist to facilitate the implementation of capacity management controls to	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
			ensure optimal system performance to meet expected and anticipated future capacity requirements.	
A1.1	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected Azure Monitor and capacity monitoring dashboards showing utilisation monitoring and alerting for production App Service plans and the Azure SQL Managed Instance to ascertain whether mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	No exception noted.
A1.2	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected backup configuration and scheduled backup evidence to ascertain whether mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	No exception noted.
A1.3	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization’s readiness to execute the plan.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Business Continuity and Disaster Recovery Procedure and the Disaster Recovery Test Report to ascertain whether mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization’s readiness to execute the plan, and	No exception noted.

TSC Ref. #	Control Number	Control Activity as specified by iMocha	Testing Performed	Results of Testing
			determined the date on which the most recent test was performed.	
A1.3	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Risk Register to ascertain whether mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks. Inspected the risk assessment performed during the period and the Risk Register evidencing in-period updates, assigned risk owners and treatment plans, and re-performed the traceability of a sample of risks to their treatment, to determine whether the control operated effectively throughout the period.	No exception noted.
C1.1 C1.2	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected the Data Retention and Disposal Policy to ascertain whether mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations. Inspected the system configuration enforcing the data-handling requirement in effect during the period (e.g., classification labelling, removable-media / DLP restriction or retention settings), to determine whether the control operated effectively throughout the period.	No exception noted.