SOC 2®-Type2 Report

Wellnomics Ltd

Examination Information	
Company name	Wellnomics Ltd
Trading name	
Client file no.	1141
ABN	NZBN: 9429038150791
Phone	
Address/audit sites	106 Wrights Road, Addington, Christchurch 8024, New Zealand
Contact person	Vladimir Zaporokha
Email	vladimir.zaporokha@wellnomics.com
Scope of Services	Software developer for ergonomics software. Creates a desktop application and server-based database with web access to users. Provides hosted server locations for global customers.
Service auditor team	Ankit Prashar (Information Security Auditor), Harry Khalili (CPA)
Examination standard	International Standard on Assurance Engagements (ISAE) No. 3000, Description Criteria section 200, Trust Services Criteria section 100
Report Type	☐ SOC 2®-Type1 ☒ SOC 2®-Type2 – For the period of 12 month, from 25/06/2024 25/06/2025 ☐ SOC 3®
Applicable Trust Service Criteria	☒ Security ☐ Availability ☐ Processing integrity ☐ Confidentiality ☐ Privacy
Examination period	Start Date: 03/07/2025 End Date: 31/07/2025
Examination planning and desktop review date	02/07/2025
Examination date	23/07/2025 -24/07/2025 and 28/07/2025
Report preparation date	05/08/2025

Your partner in building a
robust, safe, and sustainable business.

Head Office
Suite 402, 77 Pacific Highway
North Sydney, NSW 2060
www.gccertification.com

Examination participants

Name	Title	Opening meeting	Closing meeting
Vladimir Zaporokha	Information Security officer	☒	☒
Ankit Prashar	Lead Auditor	☒	☒
Harry Khalili	CPA	☒	☒

Disclaimer

Due to the sampling process and time available during the audit, some issues, non-compliances or required improvements within the organisation may not have been identified in this report. This is the organisation's responsibility to identify them through its internal audit system and to take the necessary actions to ensure the integrated management system implemented is effective and meets the standard, organisational and regulatory requirements.

Confidentiality statement

Based on the signed agreement, GCC, its employees, auditors and contractors, will keep all information relating to your organisation collected during this audit confidential, and will not disclose any such information to any third party, except that as required by legislation or relevant accreditation bodies.

Distribution

Global Compliance Certification/ Company's Representative / Audit team.

Note

The audit team would like to thank all the audit participants for their hospitality, coordination, openness throughout the audit and supporting the audit team to conduct the audit smoothly.

Contents

Section 1 — Assertion of Wellnomics Service Organization Management 5
Section 2 — Independent Service Auditor's Report 6
Section 3 — Wellnomics Service Organization's Description of the ergonomic software 9
Section 4 — Trust Services Category, Criteria, Related Controls, and Tests of Controls 20

Section 1 — Assertion of Wellnomics Service Organization Management

Assertion of Wellnomics Ltd Management

We have prepared the accompanying description in section 3 titled "Wellnomics Ltd Service Organization's Description" throughout the period June 25, 2024, to June 25, 2025, 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.

The description is intended to provide report users with information about the Wellnomics Ltd Processing System that may be useful when assessing the risks arising from interactions with Wellnomics Ltd Service Organization's (Wellnomics') system, particularly information about the system controls that Wellnomics Ltd 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, set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Wellnomics Ltd, to achieve Wellnomics' service commitments and system requirements based on the applicable trust service criteria. The description presents Wellnomics' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Wellnomics' controls.

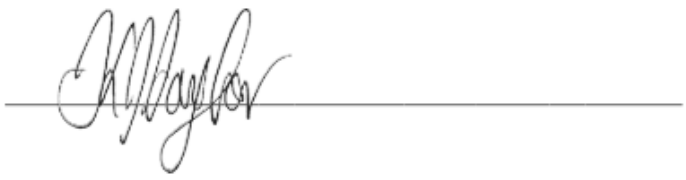
We confirm, to the best of our knowledge and belief, that:

a. the description presents Wellnomics' processing system as a service organization that was designed and implemented throughout the period June 25, 2024, to June 25, 2025, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period in a. above, to provide reasonable assurance that Wellnomics Ltd'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 user entities applied the complementary controls assumed in the design of Wellnomics' controls throughout that period.

c. the controls period in the description operated effectively throughout the period stated in a. above, to provide reasonable assurance that Wellnomics Ltd's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary user entity controls assumed in the design of Wellnomics Ltd's controls operated effectively throughout that period.

Signed by Wellnomics management, August 7, 2025



Section 2 — Independent Service Auditor's Report

To: Management of Wellnomic's LTD Service Organization

Scope

We have examined Wellnomics Service Organization's (ABC's) accompanying description of "Wellnomics Ergonomics software" throughout the period 25/06/2024 – 25/06/2025 (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 25/06/2024 – 25/06/2025, to provide reasonable assurance that Wellnomic's service commitments and system requirements were achieved based on the trust services criteria relevant to *security* set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria.*

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

Service Organization's Responsibilities

Wellnomics 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 Wellnomics's service commitments and system requirements were achieved. In section 1, Wellnomics has provided its assertion titled "Assertion of Wellnomics Service Organization Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Wellnomics 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 International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. That standard requires that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

An examination of the description of Wellnomic's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and Wellnomics 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 Wellnomics service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

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

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

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

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are presented in section 4, in a table format, "Trust Service Criteria categories, Related Service organization's Controls and Result of Test of Controls relevant to the security.

Opinion

In our opinion, in all material respects,

a. the description presents the Wellnomics System that was designed and implemented throughout the period 25/06/2024 – 25/06/2025, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the 25/06/2024 – 25/06/2025 to provide reasonable assurance that Wellnomic'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 applied the complementary controls assumed in the design of Wellnomic's controls throughout the period.**

c. the controls stated in the description operated effectively throughout the period 25/06/2024 – 25/06/2025, to provide reasonable assurance that Wellnomic's service commitments and system requirements were achieved

based on the applicable trust services criteria **if complementary subservice organization controls assumed in the design of Wellnomic'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 Wellnomics; user entities of the Wellnomics Processing System during some or all of the period 25/06/2024 – 25/06/2025; business partners of Wellnomics subject to risks arising from interactions with the Wellnomics Processing 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, business partners, subservice organizations, and other parties
- Internal control and its limitations

Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

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

Harry Khalili	**Ankit Prashar**	**Mousa Sharifi**
CA, AICPA International Associate	Information Security Lead Auditor	Director, AICPA Affiliate Member
Harry Khalili	A. Prashar	M. Sharifi
17/08/2025	05/08/2025	19/08/2025

Section 3 — Wellnomics Service Organization's Description of the ergonomic software

Company Background

Wellnomics is a pioneering company headquartered in New Zealand, deeply rooted in the mission of improving workplace health, safety, and productivity through innovative technology solutions. With a focus on ergonomic software, Wellnomics has established itself as a leader in developing and deploying tools designed to promote better health and well-being for computer users. Their product suite is renowned for its effectiveness in managing and mitigating the risks associated with repetitive strain injuries (RSIs) and other occupational hazards from prolonged computer use. By leveraging advanced analytics and personalised feedback mechanisms, Wellnomics empowers employees and organisations to adopt healthier work practices, fostering an environment that prioritises well-being alongside productivity. Over the years, Wellnomics has cemented its presence in New Zealand and expanded its reach globally, serving a diverse clientele that spans multiple industries and sectors. This expansion reflects the universal challenge of maintaining occupational health in the digital era and underscores Wellnomics' commitment to delivering solutions that are both innovative and accessible. The company's approach to ergonomics goes beyond software; it encompasses a holistic view of workplace health, advocating for a culture of awareness and proactive management of work-related health issues. Through continuous research and development, Wellnomics stays at the forefront of ergonomic trends, ensuring its products and services evolve in line with the latest scientific findings and workplace demands. This dedication to excellence and innovation makes Wellnomics a trusted partner for organisations aiming to enhance their health and safety protocols, ultimately leading to healthier, happier, and more productive workforces.

Description of services overview or services provided.

Wellnomics provides various services focused on improving workplace ergonomics and employee well-being.

Their offerings include:

1. **Sit-Stand Coaching**: Guidance on using sit-stand desks effectively.
2. **Stretch Break Reminders**: Notifications to take breaks and stretch.
3. **Office Ergonomics Training**: Online courses on ergonomic best practices.
4. **Workstation Assessments**: Evaluations of office setups to ensure ergonomic compliance.
5. **Wellness & Risk Reporting**: Tools for monitoring and reporting employee wellness and risks.

Principal service commitments and system requirements

Wellnomics Ltd designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Wellnomics Ltd makes to user entities, the laws and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Wellnomics Ltd has established for the services. The system services are subject to the security commitments established internally.

Security Commitments

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

- **Authorisation and Access Control:** System features and configuration settings designed to authorise user access while restricting unauthorised users from accessing information not needed for their role.
- **Intrusion Detection:** Use of intrusion detection systems to prevent and identify potential security attacks from users outside the system's boundaries.
- **Vulnerability Management:** Regular vulnerability scans over the system and network, and penetration tests over the production environment.
- **Incident Management:** Operational procedures for managing security incidents and breaches, including notification procedures.
- **Encryption:** Use of encryption technologies to protect customer data both at rest and in transit.

- **Data Retention and Disposal:** Data retention and data disposal policies are used to ensure data is kept securely and disposed of appropriately when no longer needed.
- **System Availability:** Commitment to maintaining high uptime availability of production systems.

System Requirements

To fulfil these service commitments, Wellnomics Ltd leverages various cloud-based solutions and tools, which include but are not limited to:

- **Azure:** Used for cloud services, including computing, storage, and databases.
- **Vulnerability Scanners:** Employed to identify and remediate security vulnerabilities within the system.
- **Confluence:** Used for document management, including policies and procedural documents.
- **Freshdesk:** Utilised for task management and tracking support requests.
- **HubSpot:** The CRM platform for managing customer relationships and access control.
- **Jira:** Employed for task management, including creation, tracking, and access control.
- **Microsoft Endpoint Manager:** Used for mobile device management (MDM) and inventory of computers.
- **Office 365:** Serves as an identity provider, managing access, groups, and people, and supports single sign-on functionality.

Security commitments

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

- System features and configuration settings are designed to authorise user access while restricting unauthorised users from accessing information not needed for their role.
- Use intrusion detection systems to prevent and identify potential security attacks from users outside the system's boundaries.
- Regular vulnerability scans over the system and network and penetration tests over the production environment.
- Operational procedures for managing security incidents and breaches, including notification procedures.
- Use encryption technologies to protect customer data at rest and in transit.
- Use of data retention and data disposal
- Uptime availability of production systems

Security commitments

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

- System features and configuration settings are designed to authorise user access while restricting unauthorised users from accessing information not needed for their role.
- Use intrusion detection systems to prevent and identify potential security attacks from users outside the system's boundaries.
- Regular vulnerability scans over the system and network and penetration tests over the production environment.
- Operational procedures for managing security incidents and breaches, including notification procedures.

- Use encryption technologies to protect customer data at rest and in transit.
- Use of data retention and data disposal
- Uptime availability of production systems

Components of the system

The System description is comprised of the following components:

- The System description is comprised of the following components:
- Software - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use mobile applications or desktop or laptop applications are.
- People - The personnel involved in a system's governance, operation, security, and use (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- Data – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- Procedures – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorised, performed, and delivered, as well as reports and other information prepared.

Infrastructure

Wellnomics Ltd maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents the device name, inventory type, description, and owner. To outline the topology of its network, the organisation maintains the following network diagram(s).

Current hosting architecture - Data Flow Topology

Hardware	Type	Purpose (optional)
Azure Platform	Azure	Managed cloud platform where services are hosted
Azure Virtual Machine	Azure	Virtual machine service for web hosting and backend service offerings
Azure Kubernetes	Azure	Container orchestration for deployment, scaling, and management
Azure Database	Azure	Transactional database with backups and redundancy

Software

Wellnomics Ltd is responsible for managing the development and operation, including infrastructure components such as servers, databases, and storage systems. The in-scope Wellnomics Ltd infrastructure and software components are shown in the table provided below:

System/Application	Operating System	Purpose
Azure SDK	N/A	The SDK is used to communicate with Microsoft azure web services
Confluence	N/A	Document management, including policies and procedural documents

System/Application	Operating System	Purpose
Cybermalls	N/A	Security management and monitoring
Freshdesk	N/A	Task management and tracking support requests
HubSpot	N/A	CRM platform for managing customer relationships and access control
Jira	N/A	Task management, including creation, tracking, and access control
Microsoft Azure	N/A	Cloud services, including computing, storage, and databases
Microsoft Endpoint Manager	N/A	Mobile device management (MDM) and inventory of computers
Office 365	N/A	Identity provider, managing access, groups, people, and supports single sign-on functionality
Vanta	N/A	Automated security and compliance monitoring

People

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

Wellnomics Ltd has a staff of approximately 151 organised in the following functional areas:

Management: Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment. This includes the CEO and Information Security Officer.

Operations: Responsible for maintaining the availability of production infrastructure and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.

Information Technology: Managed laptops, software, and other technology involved in employee productivity and business operations.

Product Development: Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

Data

Data as defined by Wellnomics Ltd, constitutes the following:

User and account data - this includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Data is categorised in the following major types of data used by Wellnomics Ltd.

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for Wellnomics Ltd.	• Press releases. • Public website
Internal	Access to internal information is approved by management and is protected from external access.	• Internal memos • Design documents. • Product specifications • Correspondences
Customer data	Information received from customers for processing or storage by Wellnomics Ltd. Wellnomics Ltd must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Customer operating data • Customer PII • Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by Wellnomics Ltd to operate the business. Wellnomics Ltd must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Legal documents • Contractual agreements • Employee PII • Employee salaries

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilised by the company in delivering its services.

All employees and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Wellnomics Ltd has policies and procedures in place to proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

Processes and procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorised by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

Physical security

Wellnomics Ltd.'s production servers are maintained by Microsoft Azure, which is responsible for the protection of physical and environmental security. Wellnomics Ltd reviews the attestation reports and performs a risk analysis of Microsoft Azure at least annually.

Logical access

Wellnomics Ltd provides employees and contractors access to infrastructure via a role-based access control system. This system ensures uniform, least-privilege access to identified users and maintains simple and reportable user provisioning and de-provisioning processes.

Access to these systems is divided into admin, user, and no-access roles. User access and roles are reviewed annually to ensure the least privileged access.

The Systems Administration and the IT team are responsible for providing access to the system based on the employee's role and performing a background check. The employee reviews Wellnomics Ltd.'s policies and completes security training. These steps must be completed within 14 days of hire.

When an employee is terminated, The Systems Administration, along with the IT team, is responsible for deprovisioning access to all in-scope systems within three business days.

Computer operations - backups

The Systems Administration, along with the IT team, backs up customer data and monitors it for completion and exceptions. If there is an exception, The Systems Administration, along with the IT team, will troubleshoot to identify the root cause and rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in Microsoft Azure, with physical access restricted according to policies. Backups are encrypted, and access is restricted to key personnel.

Computer operations - availability

Wellnomics Ltd. maintains an incident response plan to guide employees in reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting, and acting upon breaches or other incidents.

Wellnomics Ltd internally monitors all applications, including the web UI, databases, and cloud storage, to ensure service delivery meets SLA requirements.

Wellnomics Ltd utilises vulnerability scanning software that checks source code for common security issues and vulnerabilities identified in open-source dependencies and maintains an internal SLA to respond to those issues.

Change management.

Wellnomics Ltd maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilised to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilised to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data communications

Wellnomics Ltd has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the Wellnomics Ltd application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

The PaaS provider also automates the provisioning and de-provisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on the underlying hardware.

At Wellnomics, our vulnerability detection process leverages the robust capabilities of Microsoft Azure. We utilise Azure's advanced security tools and services to monitor and assess potential threats in real time. The process includes continuous scanning for vulnerabilities, automated risk assessments, and the generation of comprehensive security reports. Azure's machine learning algorithms help identify patterns and predict potential risks, ensuring proactive protection of your digital environment.

Boundaries of the system

The boundaries of the system are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the System.

This report does not include the Cloud Hosting Services provided by Azure at multiple facilities.

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 Wellnomics Ltd.'s control environment, affecting other components' design, administration, and monitoring. Integrity and ethical behaviour are the product of Wellnomics Ltd.'s ethical and behavioural standards, how they are communicated, and how they are reinforced in practice. 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 behavioural standards to personnel through policy statements and codes of conduct, as well as by example.

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

- Formally documented organisational policy statements and codes of conduct communicate entity values and behavioural standards to personnel.
- Policies and procedures require employees to sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to it.
- The employee handbook includes a confidentiality statement stating that the company will not disclose proprietary or confidential information, including client information, to unauthorised parties.
- Background checks are performed for employees as a component of the hiring process.

Commitment to competence

Wellnomics Ltd.'s management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes considering job competence levels and how those levels translate into the requisite skills and knowledge.

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

- Management has considered job competence levels and translated required skills and knowledge into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's philosophy and operating style

The Wellnomics Ltd management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way Wellnomics Ltd can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally, any regulatory changes that may require Wellnomics Ltd to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

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

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

Organisational structure and assignment of authority and responsibility

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

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

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

- Organisational charts are in place to communicate key areas of authority and responsibility.
- Organisational charts are communicated to employees and updated as needed.

HR policies and practices

Wellnomics Ltd.'s success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. This success is evidenced by its proven track record for hiring and retaining top quality personnel who ensure the service organisation is operating at maximum efficiency. Wellnomics Ltd.'s human resources policies and practices relating to employee hiring, orientation, training, evaluation, counselling, promotion, compensation, and disciplinary activities.

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

- New employees must sign acknowledgment forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

Risk assessment process.

Wellnomics Ltd.'s risk assessment process identifies and manages risks that could potentially affect Wellnomics Ltd.'s ability to provide reliable and secure services to our customers. As part of this process, Wellnomics Ltd maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is re-evaluated annually, and tasks are incorporated into the regular Wellnomics Ltd product development process so they can be dealt with predictably and iteratively.

Integration with risk assessment

The environment in which the system operates, the commitments, agreements, and responsibilities of Wellnomics Ltd.'s system, and the nature of the system components result in risks that the criteria will not be met. Wellnomics Ltd addresses these risks by implementing suitably designed controls to ensure the criteria are met reasonably. Because each system and the environment in which it operates are unique, the combination of risks to meet the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Wellnomics Ltd.'s management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and communication systems

Information and communication are integral to Wellnomics Ltd.'s internal control system. It is identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

Wellnomics Ltd. uses several information and communication channels internally to share information with management, employees, contractors, and customers. Chat systems and email are the primary internal and external communication channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, Wellnomics Ltd uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

Monitoring controls

Management monitors controls to ensure that they operate as intended and that controls are modified as conditions change. Wellnomics Ltd.'s management performs monitoring activities to assess the quality of internal control over time continuously. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-going monitoring

Wellnomics Ltd.'s management conducts quality assurance monitoring on a regular basis, and additional training is provided based on the results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Wellnomics Ltd.'s operations help to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximise the performance of Wellnomics Ltd.'s personnel.

Reporting deficiencies

Our internal risk management tracking tool is utilised to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the system (Type 1)

There have not been any significant changes impacting our business in the last three months. This includes no acquisitions, mergers, or major changes to the system environment.

Changes to the system (Type 2)

N/A

Incidents (Type 1)

There have not been any incidents.

Incidents (Type 2)

N/A

Criteria not applicable to the system

All Common Criteria/Security criteria were applicable to the Wellnomics system.

Subservice organisations.

This report does not include the Cloud Hosting Services provided by Azure at multiple facilities.

Subservice description of services

The Cloud Hosting Services provphiided by Azure support the physical infrastructure of the entity's services.

Complementary Subservice Organisation Controls

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

Microsoft Azure has implemented the following subservice organisation controls, which are included in this report to provide additional assurance that the trust services criteria are met.

Azure

Category	Criteria	Control
Security	CC 6.4	Procedures to restrict physical access to the datacentre to authorised employees, vendors, contractors, and visitors, have been established.
Security	CC 6.4	Security verification and check-in for personnel requiring temporary access to the interior of the datacentre facility, including tour groups or visitors, are required.
Security	CC 6.4	Physical access to the datacentre is reviewed quarterly and verified by the Datacentre Management team.
Security	CC 6.4	Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorised individuals.
Security	CC 6.4	The datacentre facility is monitored 24x7 by security personnel.
Availability	A 1.2	Datacentre Management team maintains, and tests data centre managed environmental equipment within the facility according to documented policy and maintenance procedures.
Availability	A 1.2	Environmental controls have been implemented to protect systems inside datacentre facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.

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

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organisation(s) ● Making regular site visits to vendor and subservice organisation(s') facilities
- Testing controls performed by vendors and subservice organisation(s)
- Reviewing attestation reports over services provided by vendors and subservice organisation(s)
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organisation

Complementary user entity controls

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

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

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

Section 4 — Trust Services Category, Criteria, Related Controls, and Tests of Controls

Wellnomics has designed and implemented controls to provide reasonable assurance that Wellnomic's service commitments and system requirements were achieved. These controls are presented below and are an integral part of Wellnomic's description of the Wellnomics Processing System throughout the period 25/06/2024 – 25/06/2025.Controls are mapped to each applicable trust services criteria and are organized by criteria area. Control numbers are unique identifiers designed to align with the relevant trust service criteria.

a. Security. Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to achieve its objectives.

Security refers to the protection of:

i. information during its collection or creation, use, processing, transmission, and storage

and

ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Trust service criteria for the applicable category	Description of service organization's controls	Service auditor test of controls	Test Controls Result
CONTROL ENVIRONMENT			
CC1.1: **COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.**	The organisation has established, communicated, and implemented the following policies and procedures to demonstrate its commitment to integrity and ethical values: a Code of Conduct, confidentiality requirements Background Checks, and Performance Evaluations.	Background checks were completed for employees who started during the observation period, including Ministry of Justice checks as required by the Human Security Policy. Confidentiality requirements were communicated to new employees through employment contracts, as confirmed by sample reviews. Sampled records also showed that employee performance was reviewed regularly, in line with top management's directives.	No exceptions noted.
CC1.2 **COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.**	As the organisation does not have a Board of Directors, the CEO is responsible for information security at Wellnomics. The CEO has allocated information security responsibilities to various roles within the organisation to ensure the implementation of internal controls.	Samples were reviewed, and it was noted that Wellnomics has allocated information security management responsibilities to the Information Security Officer, including risk management, framework implementation, communication, security operations and tool management, and vendor management. It was also noted that top management has formed an information security team collectively responsible for implementing technical and organisational controls. Samples confirmed that top management and information security officers were competent in analysing the performance of internal controls. Sampled management review meeting minutes confirmed that the performance of internal controls was reported to top management at regular intervals.	No exceptions noted.
CC1.3 **COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.**	The CEO has designated information security roles and responsibilities through formal documentation, and organisational structures have been established and communicated accordingly.	Wellnomics has assigned information security management responsibilities to the Information Security Officer, including risk management, framework implementation, communication, security operations and tool management, and vendor management. Additionally, top management has established an information security team that is collectively responsible for implementing technical and organisational controls. Samples confirmed that the Information Security Officer is responsible for briefing top management on performance, improvement requirements, and the achievement of organisational objectives.	No exceptions noted.
CC1.4 **COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in**	The organisation has communicated competency requirements for information security and critical roles. An information security awareness program has been developed to ensure employees are aware of best information security practices.	Samples were reviewed, and it was noted that the competency requirements for information security and critical roles were reviewed and updated within the observation period. Samples confirmed that employees hired to conduct allocated tasks met the required educational and competency requirements. It was also noted that the organisation conducted regular information security awareness sessions within	No exceptions noted.

Trust service criteria for the applicable category	Description of service organization's controls	Service auditor test of controls	Test Controls Result
alignment with objectives.		the observation period to ensure that employees were aware of the latest information security practices.	
CC1.5 **COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.**	The organisation has assigned information security responsibilities to appropriate roles and ensures accountability by conducting regular performance reviews.	Samples showed that the organisation regularly reviews employee performance through one-to-one catchups. These sessions offer an opportunity for employees to discuss their progress, receive constructive feedback, and set goals for personal and professional development.	No exceptions noted.
INFORMATION AND COMMUNICATION			
CC2.1 **COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.**	The organisation has established technical measures, including Vanta controls self-assessment, to monitor the effectiveness of internal controls. Additionally, further controls have been implemented to detect vulnerabilities, events, and incidents.	Samples were reviewed throughout the observation period, confirming that Vanta self-assessment controls were enabled to monitor the effectiveness of implemented controls. Logs were examined within the SIEM solution, and it was observed that all information assets listed in the service description were actively monitored and securely stored. Additionally, the Vanta vulnerabilities register was assessed, revealing that the organisation has deployed multiple tools to identify vulnerabilities across code, infrastructure, and endpoints. These tools were found to be consistently operational throughout the year.	No exceptions noted.
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.**	The organisation has established internal communication channels via Slack, an incident reporting mailbox, security awareness exercises, and policy distribution through Vanta.	Throughout the observation period, the organisation demonstrated effective implementation of internal communication and awareness mechanisms. Communication channels such as Slack and a dedicated incident reporting mailbox were actively used to facilitate timely reporting and collaboration. Security awareness exercises were conducted to reinforce staff understanding of key risks and responsibilities. Additionally, policies were consistently distributed and maintained via the Vanta platform, ensuring accessibility and alignment with organisational standards. These controls were found to be operational and effective in supporting the organisation's security posture.	No exceptions noted.
CC2.3 **COSO Principle 15: The entity communicates with external parties regarding matters affecting the**	The organisation uses Wellnomic's support page for external communication, provides a public log release page for product updates, and maintains a security page with relevant security information.	During the observation period, the organisation demonstrated effective use of external communication channels and transparency mechanisms. The Wellnomic support page was consistently available and served as a reliable platform for external stakeholders to seek assistance and report issues. The public log release page was actively maintained, providing	No exceptions noted.

Trust service criteria for the applicable category	Description of service organization's controls	Service auditor test of controls	Test Controls Result
functioning of internal control.		timely updates on product changes and enhancements. Additionally, the organisation's security page was regularly updated with relevant information, reinforcing its commitment to transparency and proactive security communication. These controls were found to be operational and effective in supporting stakeholder engagement and trust.	
RISK ASSESSMENT			
CC3.1 **COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.**	The organisation has established and disseminated a risk management policy and procedure that offers comprehensive guidance on identifying information security risks.	Throughout the observation period, the organisation demonstrated effective implementation of its risk management framework. A formal risk management policy and procedure was established and disseminated, providing comprehensive guidance for identifying and assessing information security risks. These documents were consistently referenced and applied across relevant operational activities, supporting proactive risk identification and mitigation. The controls were found to be operational and effective in promoting a structured and informed approach to risk management.	No exceptions noted
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.**	The organisation routinely conducts risk assessments to identify information security risks and determine appropriate management strategies.	Organisation The organisation has conducted regular risk assessments to identify information security risks and has consistently applied the guidance derived from the risk assessment process to determine how these risks should be managed. This approach demonstrates the organisation's commitment to proactively identifying, analysing, and addressing potential threats to its objectives, ensuring that appropriate risk management strategies are in place and operational.	No exceptions noted
CC3.3 **COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.**	The organisation has evaluated the potential for fraud originating from both internal and external parties in the process of identifying information security risks.	Throughout the observation period, the organisation demonstrated a proactive approach to fraud risk management as part of its broader information security risk assessment process. The organisation effectively evaluated the potential for fraud originating from both internal and external parties, incorporating this analysis into its approved risk identification procedures. These evaluations were conducted in accordance with established policies and were found to be operational and effective in supporting the organisation's ability to detect and mitigate fraud-related risks.	No exceptions noted

Trust service criteria for the applicable category	Description of service organization's controls	Service auditor test of controls	Test Controls Result
CC3.4 **COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.**	The organisation has assessed information security risks from changes to assets and external factors, including changes in the code and remediation of vulnerabilities.	Throughout the observation period, the organisation effectively assessed information security risks arising from changes to assets and external factors. This included evaluating risks associated with code modifications and the remediation of identified vulnerabilities. These assessments were conducted in accordance with the organisation's approved risk management procedures and were consistently applied to ensure that emerging risks were identified and addressed in a timely manner. The controls were found to be operational and effective in maintaining the organisation's security posture amid evolving technical and environmental conditions.	No exceptions noted
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.**	The organisation has engaged an external party to perform technical assessments, providing independent verification of its security controls and processes. In addition, the organisation conducts third-party risk assessments to ensure that vendors have appropriate controls in place and operating effectively, which may impact its internal control environment.	Throughout the observation period, the organisation demonstrated effective implementation of its external assurance and vendor risk management practices. An independent third party was engaged to perform technical assessments, providing objective verification of the organisation's security controls and processes. In parallel, the organisation conducted third-party risk assessments to evaluate the adequacy and operational effectiveness of controls implemented by its vendors. These activities were performed in accordance with the organisation's approved procedures and were found to be operational and effective in supporting the integrity of its internal control environment.	No exceptions noted
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.**	Scheduled meetings are conducted between information security personnel and senior management to report and resolve any identified information security deficiencies.	Throughout the observation period, the organisation demonstrated effective governance over its information security programme. Scheduled meetings were consistently conducted between information security personnel and senior management to report and address identified security deficiencies. These meetings facilitated timely escalation, decision-making, and resolution of issues, in alignment with the organisation's approved procedures. The controls were found to be operational and effective in maintaining oversight and responsiveness within the information security function.	No exceptions noted

Trust service criteria for the applicable category	Description of service organization's controls	Service auditor test of controls	Test Controls Result
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.**	The organisation has implemented information security measures to address identified information security risks.	Throughout the observation period, the organisation demonstrated effective implementation of information security measures to address identified risks. These measures included a comprehensive set of technical, organisational, human-related, and physical controls, all applied in accordance with the organisation's approved risk management procedures. The controls were tailored to mitigate specific threats to information assets and were found to be operational and effective in reducing exposure to known vulnerabilities while maintaining the organisation's overall security posture.	No exceptions noted
CC5.2 **COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.**	Organisation employs technologies such as Mobile Device Management (MDM), cloud hosting, and productivity applications. Security protocols are implemented through established policies to ensure the secure management of these technologies.	Throughout the observation period, the organisation demonstrated effective implementation of controls to manage and secure its technology environment. Technologies such as Mobile Device Management (MDM), cloud hosting platforms, and productivity applications were actively used and governed through established security policies. These policies ensured secure configuration, access management, and ongoing monitoring of the technologies in use. The implemented controls encompassed technical, organisational, human-related, and physical measures, and were found to be operational and effective in maintaining the confidentiality, integrity, and availability of information assets.	No exceptions noted
CC5.3 **COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.**	The organisation has clear information security policies in place to safeguard its operations.	Over the course of the observation period, the organisation demonstrated effective implementation of its information security policies designed to safeguard operations. These policies provided clear guidance and were consistently applied across the organisation's activities. The controls encompassed technical, organisational, human-related, and physical measures, ensuring a comprehensive approach to protecting information assets and maintaining the integrity of the control environment. The policies were found to be operational and effective in supporting the organisation's security objectives.	No exceptions noted

Trust service criteria for the applicable category	Description of service organization's controls	Service auditor test of controls	Test Controls Result
LOGICAL AND PHYSICAL 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.**	The organisation has implemented a policy to regulate access to its infrastructure, software, and systems.	During the observation period, the organisation effectively implemented its access control policy to regulate access to infrastructure, software, and systems. The policy provided clear guidance on authorisation procedures, access provisioning, and periodic reviews. These controls encompassed technical, organisational, human-related, and physical measures, and were consistently applied to ensure that only authorised personnel had access to critical resources. The controls were found to be operational and effective in safeguarding the organisation's information assets.	No exceptions noted
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.**	The organisation applies access controls, registers identities in an IAM system, and regularly reviews the access register.	During the observation period, the organisation effectively applied access control measures to safeguard its infrastructure and systems. Identities were consistently registered and managed through an established Identity and Access Management (IAM) system, ensuring appropriate authorisation and accountability. The access register was subject to regular review, supporting the timely identification and remediation of any access-related discrepancies. These controls included technical, organisational, human-related, and physical elements, and were found to be operational and effective in maintaining secure access to critical resources.	No exceptions noted
CC6.3 **The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.**	Access is granted using Role-Based Access Control (RBAC). Asset access is revoked through an offboarding checklist approved by top management.	During the observation period, the organisation demonstrated effective operation of its controls related to access authorisation, modification, and revocation. Access to data, software, functions, and other protected information assets was managed using Role-Based Access Control (RBAC), ensuring that permissions were aligned with users' roles and responsibilities in accordance with the principles of least privilege and segregation of duties. This approach helped ensure that only appropriately authorised individuals could access sensitive resources, supporting the organisation's objectives. When asset access was no longer required, a formal revocation process was followed. Access rights were revoked through an offboarding checklist, which required approval from top management. This process ensured that departing users' access was promptly and	No exceptions noted

Trust service criteria for the applicable category	Description of service organization's controls	Service auditor test of controls	Test Controls Result
		systematically removed, minimising the risk of unauthorised access to critical assets. Regular reviews and oversight were conducted to verify that these controls remained operational and effective. No exceptions were noted during the assessment period, indicating consistent and reliable application of the access management procedures.	
CC6.4 **The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.**	The organisation maintains a physical security policy and depends on cloud providers for the security of infrastructure, backup storage, and associated resources. Physical controls are in place for test infrastructure located at the headquarters.	During the observation period, the organisation effectively implemented controls to safeguard its infrastructure and associated resources. A formal physical security policy was maintained and applied to the organisation's test infrastructure located at headquarters, ensuring appropriate access restrictions and environmental protections. For broader infrastructure, backup storage, and related services, the organisation relied on cloud service providers, whose security capabilities were integrated into the organisation's control environment. These measures, encompassing technical, organisational, human-related, and physical controls, were found to be operational and effective in maintaining the confidentiality, integrity, and availability of information assets.	No exceptions noted
CC6.5 **The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.**	Organisation has established and enforced an access revocation process for infrastructure. Additionally, asset management controls are implemented to ensure that assets are retrieved upon termination.	During the observation period, the organisation effectively enforced its access revocation process to ensure timely removal of infrastructure access upon termination or role change. This process was consistently applied in accordance with approved procedures, supporting the protection of critical systems and data. In addition, asset management controls were implemented to ensure that organisational assets were retrieved upon termination. These controls, which included technical, organisational, human-related, and physical measures, were found to be operational and effective in maintaining the integrity of the organisation's control environment.	No exceptions noted
CC6.6 **The entity implements logical access security measures to protect against threats from sources outside its system boundaries.**	The organisation protects against external threats with MFA, firewalls, and data encryption both at rest and in transit.	During the observation period, the organisation effectively implemented security measures to protect against external threats. These included the use of Multi-Factor Authentication (MFA), firewalls, and data encryption protocols applied both at rest and in transit. The controls were supported by established security policies and procedures, and encompassed technical, organisational, human-related, and physical safeguards. These measures were found to be operational and effective in maintaining the	No exceptions noted

Trust service criteria for the applicable category	Description of service organization's controls	Service auditor test of controls	Test Controls Result
		confidentiality, integrity, and availability of the organisation's information assets.	
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.**	The organisation uses approved cryptography, data encryption, and access controls to secure the transmission of sensitive information.	During the observation period, the organisation effectively implemented controls to secure the transmission of sensitive information. Approved cryptographic methods, data encryption protocols, and access controls were consistently applied to protect data both in transit and at rest. These measures were governed by established security policies and encompassed technical, organisational, human-related, and physical safeguards. The controls were found to be operational and effective in maintaining the confidentiality and integrity of sensitive information throughout its lifecycle.	No exceptions noted
CC6.8 **The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.**	The organisation protects code and infrastructure by detecting malware and identifying vulnerabilities.	During the observation period, the organisation effectively implemented controls to safeguard its code and infrastructure against external threats. Malware detection mechanisms and vulnerability identification tools were actively used to monitor and respond to potential risks. These controls were supported by established security policies and encompassed technical, organisational, human-related, and physical measures. The controls were found to be operational and effective in maintaining the integrity and resilience of the organisation's technology environment.	No exceptions noted
SYSTEM OPERATIONS			
CC7.1 **To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.**	The organisation uses CI/CD pipelines for configuration changes and conducts regular code reviews to detect security flaws.	During the observation period, the organisation effectively implemented secure development practices through the use of Continuous Integration and Continuous Deployment (CI/CD) pipelines for managing configuration changes. These pipelines ensured consistent, automated, and auditable deployments. In addition, regular code reviews were conducted to identify and remediate potential security flaws prior to release. These practices were supported by technical, organisational, human-related, and physical controls, and were found to be operational and effective in maintaining the security and integrity of the organisation's codebase and infrastructure.	No exceptions noted

Trust service criteria for the applicable category	Description of service organization's controls	Service auditor test of controls	Test Controls Result
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.**	Organisation has established logging, vulnerability management, and infrastructure monitoring on system components to identify and address anomalies effectively.	During the observation period, the organisation effectively implemented logging, vulnerability management, and infrastructure monitoring across system components to detect and respond to anomalies. These controls were supported by established procedures and technologies that enabled timely identification and remediation of potential security issues.	No exceptions noted
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.**	The organisation maintains an incident response process to evaluate the severity of information security incidents.	During the observation period, the organisation effectively maintained and applied its incident response process to evaluate the severity of information security incidents. The process was consistently followed in accordance with established procedures, enabling timely assessment, classification, and escalation of incidents.	No exceptions noted
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.**	Organisation has established a comprehensive incident response process for effectively addressing information security incidents.	During the observation period, the organisation effectively maintained and enforced a comprehensive incident response process for addressing information security incidents. This process enabled timely identification, evaluation, and resolution of incidents in accordance with established procedures. Regular table top exercises were performed to ensure suitability of response plan.	No exceptions noted
CC7.5 **The entity identifies, develops, and implements activities to recover from identified security incidents.**	Wellnomics has established and communicated a business continuity and disaster recovery plan that helps organisations identify critical business systems that remain operational during disasters and outlines the steps for recovery.	Wellnomics Business Continuity and Disaster Recovery Plan (BCDRP) outlines key elements to ensure operations continue during disasters. These include alternative work facilities to maintain productivity, clear communication and escalation guidelines, prioritising critical services to minimise disruption, and defining acceptable downtime and data loss limits during recovery. Although no disasters occurred during the observation period, a tabletop exercise was conducted to test the plan. The exercise was	No exceptions noted

Trust service criteria for the applicable category	Description of service organization's controls	Service auditor test of controls	Test Controls Result
		successful, with no deviations observed, and the plan was deemed effective.	
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.**	Organisaiton manages infrastructure changes through defined change management procedures, deploying code Changes via the CI/CD pipeline.	During the observation period, the organisation demonstrated effective management of infrastructure changes through well-defined change management procedures. These procedures ensured that changes were properly documented, reviewed, and approved prior to implementation. Code changes were deployed using established Continuous Integration and Continuous Deployment (CI/CD) pipelines, which provided automation, consistency, and traceability across the deployment lifecycle. This approach supported controlled and auditable releases, reducing the likelihood of misconfigurations and enabling rapid remediation when necessary.	No exceptions noted
RISK MITIGATION			
CC9.1 **The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.**	Wellnomics developed a business continuity and disaster recovery plan to minimise disruption risks.	Wellnomics Business Continuity Plan (BCP) ensures operational resilience and addresses information security risks during disruptions. The plan identifies essential services and details procedures to maintain business operations in various scenarios, such as system failures, cyberattacks, or natural disasters. By safeguarding sensitive data and systems, the BCP helps reduce the risk of breaches, downtime, and other security incidents.	No exceptions noted
CC9.2 **The entity assesses and manages risks associated with vendors and business partners.**	Wellnomics evaluates vendors by impact level through vendor assessment and enforces risk controls with required compliance.	During the observation period, Wellnomics effectively implemented a structured vendor evaluation process based on impact levels. Vendor assessments were conducted to determine the potential risk posed by third-party relationships, and appropriate risk controls were enforced in line with required compliance standards. This process ensured that vendors with access to sensitive systems or data were subject to rigorous scrutiny and that their controls aligned with the organisation's security and compliance expectations. The controls were found to be operational and effective in managing third-party risk and maintaining the integrity of the organisation's control environment.	No exceptions noted