WiseTech Global CargoWise Application Hosted on CargoWise Cloud System and Organization Control (SOC) 3 Report

Relevant to Security and Availability

Report on WiseTech Global's CargoWise Application Hosted on CargoWise Cloud from 1 July 2022 to 31 December 2022

Prepared in Accordance with Standard on Assurance Engagements ISAE 3000 'Assurance Engagements on Controls'

Ernst & Young
200 George Street
Sydney NSW 2000 Australia
GPO Box 2646 Sydney NSW 2001

Tel: +61 2 9248 5555
Fax: +61 2 9248 5959
ey.com/au

Building a better working world

Section 1 - Report of Independent Accountants

To the Management of WiseTech Global,

Scope

We have examined management's assertion, contained within the accompanying "Managements Report of its Assertions on the Effectiveness of its controls over WiseTech Global's CargoWise Application Hosted on CargoWise Cloud - Based on the Trust Services Criteria for (Security and Availability)" (Assertion), that WiseTech Global's controls over the CargoWise (System) were effective throughout the period 1 July 2022 to 31 December 2022, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Management's Responsibilities

WiseTech Global's management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the System and describing the boundaries of the System
- Identifying the principal service commitments and system requirements and the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of the system
- Identifying, designing, implementing, operating, and monitoring effective controls over the CargoWise (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement

Our Responsibilities

Our responsibility is to express an opinion on the Assertion, 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 (IAASB). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of WiseTech Global's relevant security and availability policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating WiseTech Global's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (including

Ernst & Young
200 George Street
Sydney NSW 2000 Australia
GPO Box 2646 Sydney NSW 2001

Tel: +61 2 9248 5555
Fax: +61 2 9248 5959
ey.com/au

International Independence Standards), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

We apply International Standard on Quality Control I and accordingly maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Inherent limitations:

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve WiseTech Global's principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion:

In our opinion, WiseTech Global's controls over the system were effective throughout the period 1 July 2022 to 31 December 2022, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

Ernst & Young

14 November 2023

Section 2 - Management's Report of Its Assertions on the Effectiveness of Its Controls Over WiseTech Global CargoWise Application

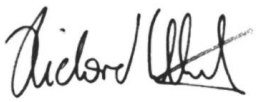
Based on the Trust Services Criteria for Security and Availability

14 November 2023

We, as management of, WiseTech Global are responsible for:

- Identifying the CargoWise Application (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and service requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirements
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the system were effective throughout the period of 1 July 2022 to 31 December 2022, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security and availability set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*



Richard White

Founder & CEO

Attachment A

CargoWise Application Hosted on CargoWise Cloud

CargoWise Application Hosted on CargoWise Cloud

About WiseTech Global

WiseTech Global (WTG) is a provider of software solutions to the logistics industry globally. Our mission is to create breakthrough products that enable and empower those that own and operate the supply chains of the world.

Founded in 1994, we are a global provider of software solutions across more than 165 countries. Our 18,000+ customers are logistics service providers in a highly fragmented industry and range from the world's largest multinational companies to small and medium-sized regional or domestic enterprises. 24 of the top 25 global freight forwarders are our customers[1].

Our people are innovators and visionaries. We challenge the status quo, think boldly, and build world-leading products. WiseTech Global has a long track record of innovating continuously and successfully.

Our flagship global platform, CargoWise, has deep functionality and integration to help our customers run their businesses more efficiently and profitably.

About CargoWise

CargoWise is a single source, deeply integrated, and truly global platform designed to meet the diverse needs of the logistics industry.

A highly flexible and feature-rich system, CargoWise delivers powerful productivity, extensive functionality, comprehensive integration, and deep international compliance capabilities.

[1] Armstrong & Associates: Top 50 Global Third-Party Logistics Providers List, ranked by 2020 logistics gross revenue/turnover. Armstrong & Associates: Top 25 Global Freight Forwarders List, ranked by 2020 logistics gross revenue/turnover and freight forwarding volumes.

Figure 1. Productivity Diagram

CargoWise is a cloud-based software platform that enables customers to execute highly complex logistics transactions and manage their operations on one database across multiple users, functions, offices, and countries.

Translated into 30 languages and operating across currencies, CargoWise offers truly global capabilities for a global industry.

CargoWise grows with your company, streamlining your processes, integrating your business with your customers and partners, and increasing your efficiency, visibility, and profitability at any size.

CargoWise Ecosystem

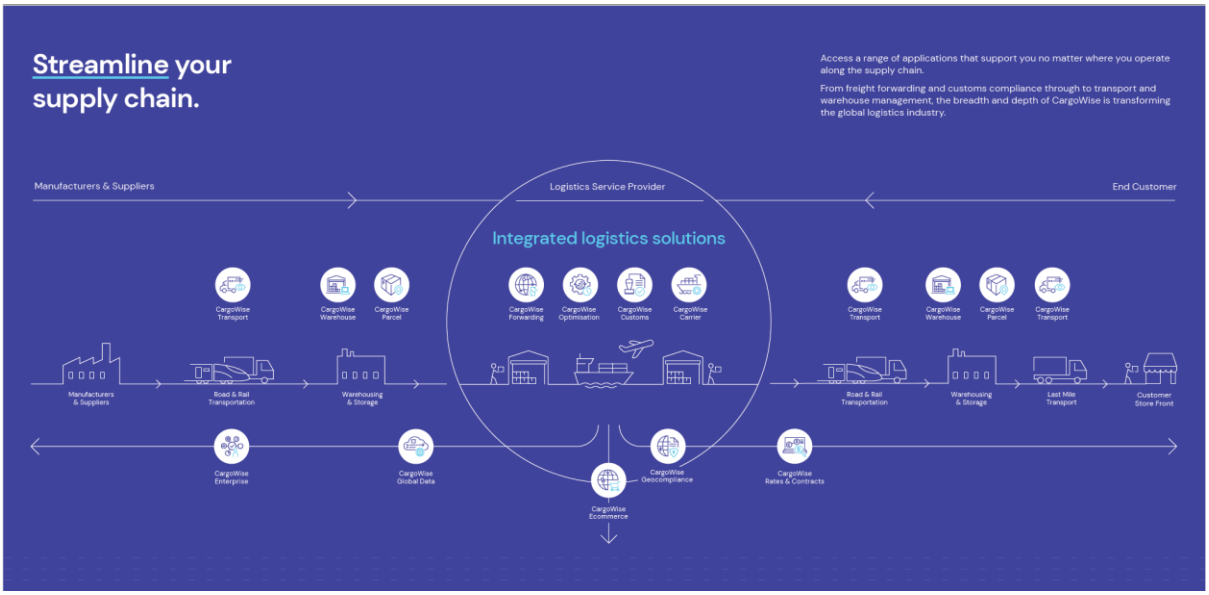
For ease of reference the CargoWise application and CargoWise Cloud together will be referred to in this document as the CargoWise “ecosystem”.

CargoWise application and associated modules are hosted on WiseTech’s CargoWise Cloud.

CargoWise Application Modules

From freight forwarding and customs compliance through to transport and warehouse management, CargoWise is transforming the global logistics industry. The following is a description of modules that make up CargoWise.

Figure 2. Supply Chain Diagram



- **CargoWise Forwarding:** Execute complex logistics transactions and manage your freight operations from a single, easy to use platform.
- **CargoWise Customs:** Meet customs challenges with confidence and unlock emerging trade opportunities. Create, manage and clear your import and export customs declarations in more than 30 countries.
- **CargoWise Optimization:** Automation and visibility tools help you and your customers improve decision-making capabilities and achieve supply chain transparency.
- **CargoWise Geo-compliance:** Comprehensive geo-compliance tools keep you connected with more countries and customs authorities, helping your shipments move without delay.
- **CargoWise Rates and Contracts:** Get the best rate for the origin, destination, commodity and quantity you want to ship with a comprehensive global database of ocean, road and air carrier rates and contracts.
- **CargoWise Carrier:** Seamlessly manage bookings and bills of lading with integrated sailing schedules, container control, automated data exchange and more.
- **CargoWise Global Data**: Master Data Validation tools help ensure data quality and remove the risks associated with incorrect or incomplete data.

- **CargoWise Enterprise:** Automate, consolidate and streamline core business processes including sales and marketing, accounting, human resources and more.
- **CargoWise Ecommerce:** An integrated solution from origin to final destination that delivers faster, safer and more reliable international ecommerce operations.
- **CargoWise Warehouse**: Manage and track the movement of your inventory with a comprehensive and flexible warehouse management system that gives you real-time control over inbound and outbound cargo.
- **CargoWise Transport**: Real-time, on-the-road data allows you to streamline your order-to-delivery process and proactively plan capacity, loads and routes.
- **CargoWise Parcel:** Automate routing, packing, rating, shipping, and tracking in your warehouses, stores, or your ecommerce site from one easy to use platform.

CargoWise Cloud

The CargoWise application is hosted on CargoWise Cloud, a global data network, including 24/7 global disaster recovery, upgrades and maintenance, backup, and continuity planning.

Locations that host the customer domain of the CargoWise application are:

- Sydney Data Center – WTG managed.
- Chicago Data Center – WTG managed.
- Germany Data Center – A Co-Location data center.
- China Cloud Instance – Hosted in China and segregated to meet China Cybersecurity Law.

Organizational Level Practices

Leadership

WTG leadership regularly reviews internal and external environments that may affect our business or our customers and establishes strategy and objectives accordingly. These include but are not limited to industry trends, legislative and regulatory changes, and new security challenges.

More information can be found on our website, see Corporate Governance.

Management Review and Continual Improvement

WiseTech Global have an established formal organization structure to define reporting lines, accountabilities, and responsibilities as they relate to information security commitments. Risks, audit findings and continual improvement objectives are reported to leaders at the appropriate level.

Risk Management

A structured approach has been adopted to manage enterprise and technology risks using consistent methods for assessment and treatment. This enterprise risk management process is founded upon the *ISO 31000 - Risk management - Principles and guidelines*.

Policy, Procedure and Awareness

An Information Security Framework and an Information Security Policy has been established. Policies are determined and issued by senior management. Policies are reviewed regularly or as changes/risks present themselves.

Security and compliance training is presented to all staff from the week they join WTG, with all new joiners required to take the following compliance training:

- Cyber Security Awareness
- Code of Conduct
- Market Disclosure and Communications Principles Training
- Modern Slavery
- Privacy and Data Protection

Where relevant, policy acknowledgement is also conducted via employee contracts and training modules. Policy deviations are reported and monitored, through incident management processes, whistle-blower reporting and Human Resource mechanisms.

Communication

WiseTech Global communicates with customers through a variety of channels:

- Links and information about CargoWise Updates, Wise Learning Updates and WiseNews are published on the home page of a customer's CargoWise application. This communication is designed to allow customers to quickly access relevant information about recent changes to the system, new functionality available, and significant industry news.

- All customers are provided with Update Notes, Guides, Technical Information and Learning Materials published on the MyAccount website. The MyAccount website is a repository of educational and instructional information for customers to learn how to utilize features of the CargoWise system, and to download the installation files required to access the hosted CargoWise environment.

- WiseTech Global has the ability to send email campaigns to designated customer technical or administrative contacts. WiseTech Global can elect to utilize this communication method for sending out significant company, industry or platform announcements.

- Complaints, inquiries and request processes are contained within the MLA, and also encouraged either directly or through lodging an incident request.

Other internal communication processes include:

- Disaster Recovery Plans – These plans detail the categories and requirements of communication among the Crisis and DR teams. These documents contain details on what, how and when to communicate to stakeholders, including our customers.

- Data Breaches – WTG has established a Data Breach Notification team who are notified in the cases of data breaches. This process also aligns to GDPR notifiable data breach requirements.

IT Operations

Human Resource Security

WTG human resources teams have security controls embedded in their practices and work closely with Information Security to ensure effective and efficient processes for onboarding and offboarding of staff.

Vendor Management

WiseTech Global conducts security risk assessments as set out by the Supplier Relationship Security Policy for critical suppliers. This process includes annual assessments for critical suppliers.

Asset Management

WiseTech has an IT Asset Management Policy established to guide staff on how assets should be identified, tracked, and disposed. Asset classes have an asset owner recorded in the Information Asset Register.

Incident Management

The WiseTech Incident Management Process has been prepared to govern the logging, monitoring, escalation and resolution of incidents and problems. Various incident management plans and playbooks have also been established.

Development and Change Management

WiseTech Global has an established and documented Systems Development Life Cycle (SDLC) methodology. Development of security assessments and controls to minimize risk are included in each stage of the SDLC.

The WiseTech Global Software Change Management Process has been implemented by WiseTech Global management for the documentation, approval, testing and deployment of coded CargoWise application software changes.

Changes to hardware and infrastructure are controlled via the WTG Information Services Change Management Procedure. Changes are categorized and measured against risk to ensure an adequate amount of oversight and review is performed. WTG Information Services department runs a Change Approval Board (CAB) for infrastructure changes. The CAB looks at the details of any high-risk changes, assists staff to prioritize those changes, and ensures there are no conflicts with competing changes. This all lends itself to continually providing service reliability as we manage and improve our solutions.

Access and Identity Management

WiseTech Global uses centralized domain management of accounts and computer objects. Access authentication via the use of passwords has been configured across the environment, and includes requirements for password length, complexity, and re-use.

Access to data and systems is dependent on the staff's job role/function. Requests for new access or changes in access to WiseTech managed customer systems and data are required to be approved by an appropriate level of management or authorized approver.

Privileged user access to WiseTech systems is restricted to authorized personnel only. The currency and appropriateness of accounts assigned privileged user access across the WiseTech environment is revalidated on a quarterly basis.

Access for departing personnel is removed on the employee or contractor's last date of employment.

Logging and Monitoring

Event logging is a valuable resource in identifying security breaches, assessing data and system damage in the instance of a breach, and providing unique insights and metrics into IT operations. Logs generated by multiple sources are forwarded to a centralized management system for storage, correlation and analysis as required.

Monitoring is also performed across the CargoWise application and underlying infrastructure for capacity, performance, and uptime thresholds.

Network Security

WTG utilizes firewalls and network segmentation to control boundaries between network segments where assets have a common function, risk, or role. Network security is monitored by the WiseTech Global Information Services Team through use of IDS/IPS, SIEM, and other console management solutions.

Performance and Capacity

Performance and capacity monitoring thresholds have been configured across both the internal infrastructure and customer environments to meet availability commitments. These thresholds are monitored by the relevant teams through use of a third-party automated monitoring tool.

Cryptography

Public key infrastructure encryption is used for all user sessions connecting to CargoWise application. These keys are stored in an encrypted key vault inside our corporate network, in a separate and isolated domain. Access to this domain is restricted to a small group of WTG senior engineering administrators.

Backups and Recovery

Full and incremental disk backups are scheduled and performed at each WiseTech location. Database logshipping is performed by an internally developed WiseTech logshipping replication tool as soon as backups become available. All production WiseTech customer data is stored at a minimum of two separate sites for the purposes of disaster recovery.

Disaster Recovery

WiseTech has established a Business Continuity Management program for CargoWise. This program, and associated plans and playbooks are reviewed and tested annually.

Cyber Security

Vulnerability Management

The WTG Information Services team operates a continuous Vulnerability Management program for discovering, prioritizing, and mitigating vulnerabilities. Assets are scanned either daily, by endpoint detection and response tools or weekly, by our vulnerability scanners. Anti-malware tools are used to protect systems and data from malicious software, and virus definition updates are automatically applied.

Where applicable, WTG uses automated patching processes to minimize effort and increase the efficiency and timeliness of updates.

Physical and Environmental Security

Physical and environmental controls are documented in the Physical & Environmental Security Policy for WTG managed sites. Periodic maintenance of all environmental protection devices, including sensors, alarm systems and generators, are performed by the vendor or third-party specialists. Results of maintenance reports are retained and audited on a regular basis.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments & System Requirements

WTG designs its processes and procedures to meet its objectives for the CargoWise ecosystem. WTG is committed to providing reliable and secure software solutions to the logistics industry globally and to protecting customer data in its possession.

WTG's Security and Availability commitments are communicated to external customers through use of Maintenance and License Agreements (MLAs). To achieve the service level and availability commitments as set out in the customer MLAs, WTG have implemented and operate Security and Risk management programs. Security and Availability commitments include, but are not limited to, the following:

- Detect and act on suspected security incidents or data breaches.
- Ensure recoverability of customer data.
- Meeting system availability uptime thresholds as set out in the MLA.
- Scheduled maintenance windows to minimize the impact of changes to services on customers.
- Communication channels and notifications to support customers with the processing of defects, incidents and data breaches.

WTG establishes operational requirements that support the achievement of security and availability commitments. These requirements are documented in policies and procedures, system design documentation, and customer agreements.

Security and availability commitments and associated system requirements are conveyed to internal personnel through a combination of IT security policies, on-the-job training, and weekly status meetings. IT security policies have been prepared by WTG management to define the responsibilities of individuals and to provide necessary information to those responsible for the design, implementation, operation, maintenance and monitoring of internal controls relevant to the security and availability of the CargoWise system. By the same token, information regarding processes for reporting security and availability incidents to appropriate personnel and third parties have been formalized and made available to internal users within the WiseTech Global Incident Management Procedure and Customer Service Team Enterprise Support Process documents.