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 October 2024 to 30 September 2025

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

Shape the future
with confidence

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

Section 1 - Independent Service Auditor’s Assurance Report

To: WiseTech Global Management

Scope

We have examined management’s statement, contained within the accompanying “Management’s Report of its Statements on the Effectiveness of Its Controls Over WiseTech Global CargoWise Application Based on the Trust Services Criteria for Security and Availability” (Statement), that WiseTech Global’s (WiseTech) controls over the CargoWise Application Hosted on CargoWise Cloud (System) were effective throughout the period 1 October 2024 to 30 September 2025, to provide reasonable assurance that WiseTech’s service commitments and system requirements were achieved based on the trust services 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*, in AICPA *Trust Services Criteria*.

WiseTech uses Equinix, Microsoft Azure, Alibaba Cloud, and Amazon Web Services (AWS) (subservice organizations) to provide the following services:

Sub-Service Organization	Service
Equinix	WiseTech uses Equinix to provide co-location data center services and co-location data backup storage for short term immutable backups.
Alibaba Cloud	WiseTech uses Alibaba Cloud to provide Cloud instances for CargoWise for customers operating out of People’s Republic of China and Kingdom of Saudi Arabia offices.
Microsoft Azure	WiseTech uses Microsoft Azure to provide data backup and storage services.
Amazon Web Services (AWS)	WiseTech uses AWS to provide client data storage services.

The description of the boundaries of the system presented at Appendix A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with related controls at WiseTech**,** to provide reasonable assurance that WiseTech’s service commitments and system requirements are achieved based on the applicable trust service criteria. The description of the boundaries of the system presents the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at Equinix, Microsoft Azure, Alibaba Cloud and AWS. Our procedures did not extend to the services provided by Equinix, Microsoft Azure, Alibaba Cloud and AWS and we have not evaluated whether the controls management assumes have been implemented at Equinix, Microsoft Azure, Alibaba Cloud and AWS have been implemented or whether such controls were suitably designed and operating effectively throughout the period 1 October 2024 to 30 September 2025.

Management's responsibilities

WiseTech's management is responsible for its service commitments and system requirements, and for designing, implementing, operating, and monitoring effective controls within the system to provide reasonable assurance that WiseTech's service commitments and system requirements were achieved. WiseTech management is also responsible for providing the accompanying assertion about the effectiveness of controls within the System, 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 service commitments and system requirements and the risks that would threaten the achievement of the service commitments and service requirements that are the objectives of the System.

Our responsibilities

Our responsibility is to express an opinion on the controls over the System, based on our examination. Our examination was conducted in accordance with the 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). This standard requires that we plan and perform our examination to obtain reasonable assurance about whether the controls over the System operated effectively, in all material respects. An examination involves performing procedures to obtain evidence about the controls over the System, which includes: (1) obtaining an understanding of WiseTech'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 consider 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'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 are required to be independent of WiseTech and to meet our other ethical responsibilities, in accordance with the relevant ethical requirements related to our examination engagement.

We apply International Standard on Quality Management I, Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services engagements, which requires that we design, implement and operate a system of quality management including 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's 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's controls over the System were effective throughout the period 1 October 2024 to 30 September 2025, to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria.

Ernst & Young

30 January 2026
Sydney, Australia

Section 2 - Management’s Report of its Statements on the Effectiveness of Its Controls Over WiseTech Global CargoWise Application Based on the Trust Services Criteria for Security and Availability

30 January 2026

We, as management of, WiseTech are responsible for:

- Identifying the CargoWise Application Hosted on CargoWise Cloud (System) and describing the boundaries of the System, which are presented in Attachment A

- Identifying our service commitments and system requirements

- Identifying the risks that would threaten the achievement of our service commitments and system 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 service commitments and system requirement

- Selecting the trust services categories and associated criteria that are the basis of our assertion

WiseTech uses Equinix, Microsoft Azure, Alibaba Cloud, and Amazon Web Services (AWS) to provide the following services:

Sub-Service Organization	Service
Equinix	WiseTech uses Equinix to provide co-location data center services and co-location data backup storage for short term immutable backups.
Alibaba Cloud	WiseTech uses Alibaba Cloud to provide Cloud instances for CargoWise for customers operating out of People’s Republic of China and Kingdom of Saudi Arabia offices.
Microsoft Azure	WiseTech uses Microsoft Azure to provide data backup and storage services.
Amazon Web Services (AWS)	WiseTech uses AWS to provide client data storage services.

The description of the boundaries of the system presented in Attachment A indicates that complementary controls at Equinix, Microsoft Azure, Alibaba Cloud, and AWS that are suitably designed and operating effectively are necessary, along with controls at WiseTech to achieve the service commitments and system requirements. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of WiseTech’s controls. It does not disclose the actual controls at Equinix, Microsoft Azure, Alibaba Cloud, and AWS.

We confirm to the best of our knowledge and belief that the controls over the System were effective throughout the period 1 October 2024 to 30 September 2025, to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services 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*, in AICPA *Trust Services Criteria.*

Very truly yours,

WiseTech Global Limited Management

Attachment A

CargoWise Application Hosted on CargoWise Cloud

CargoWise Application Hosted on CargoWise Cloud

About WiseTech Global

WiseTech 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 193 countries. Our customers include over 17,000 of the world's logistics companies, including 47 of the top 50 global third-party logistics providers and 24 of the 25 largest global freight forwarders worldwide.

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

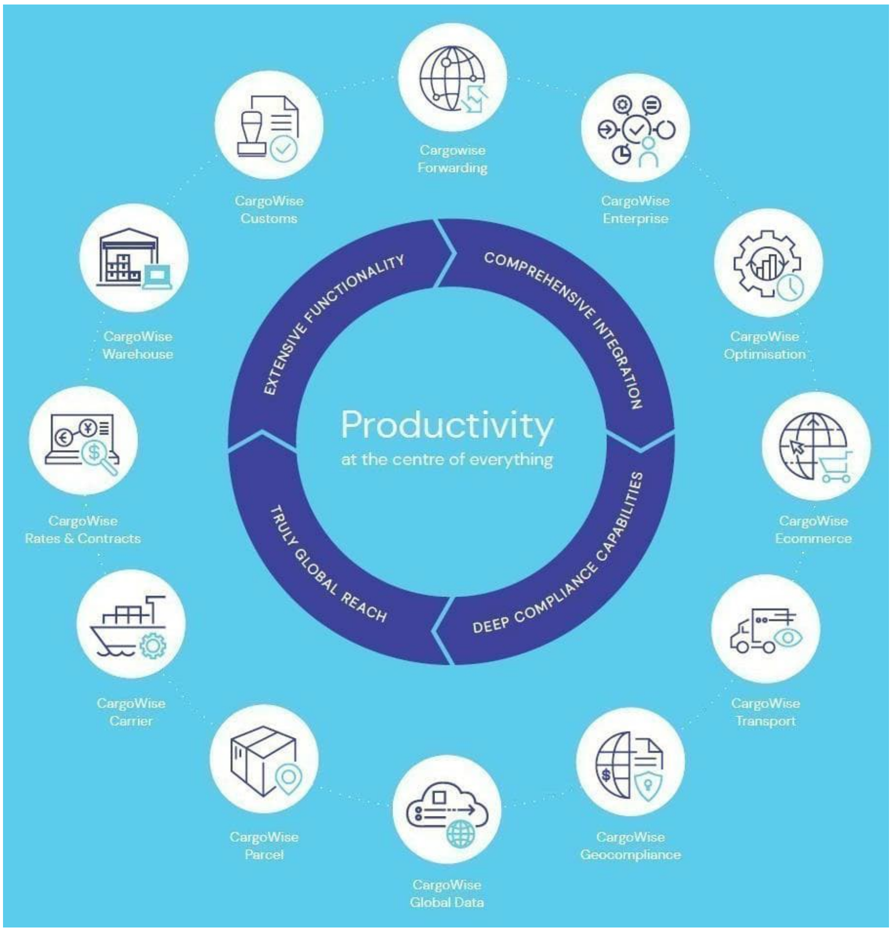
Our flagship global platform, CargoWise, has deep functionality and integration to help our customers run their businesses more efficiently and profitably.

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.

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

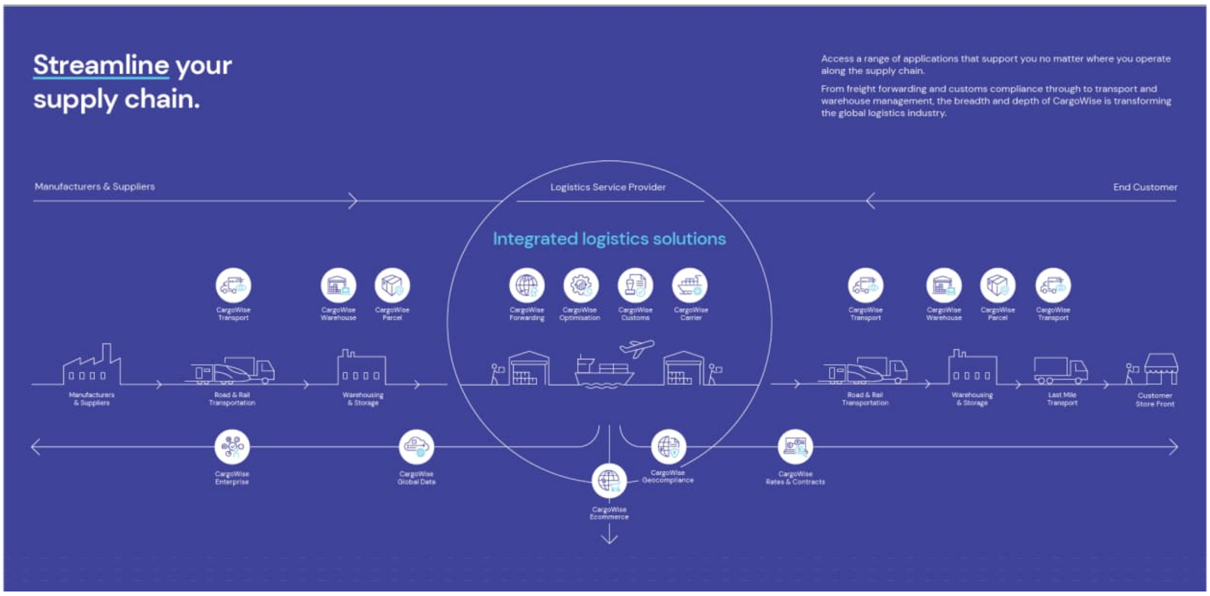
For ease of reference the CargoWise application and CargoWise Cloud together will be referred to in this document as the CargoWise “ecosystem”.

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. More information is available here: https://www.cargowise.com/

Figure 2. Supply Chain Diagram



Streamline your supply chain.

Access a range of applications that support you no matter where you operate along the supply chain.

From freight forwarding and customs compliance through to transport and warehouse management, the breadth and depth of CargoWise is transforming the global logistics industry.

- **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 – A co-location data center managed by Equinix Sydney
- Chicago Data Center – Hosted and managed by WiseTech.
- Hamburg Germany Data Center – A co-Location data center managed by Equinix
- China Cloud Instance – Hosted in Alibaba Cloud Services.
- Kingdom of Saudi Arabia Cloud Instance - Hosted in Alibaba Cloud Services.

In-scope Systems

All CargoWise systems and the internal information systems that support them are within the scope of this report. WiseTech considers critical information systems as those that form part of the CargoWise ecosystem, which include:

- CargoWise application modules, underlying databases which host customer data.

- Related infrastructure services including cloud hosting services provided by subservice organizations that store customer data.

Internal Information systems are the applications and tools that support the CargoWise ecosystem, which include:

- On-premise and cloud-based access and identity directory service
- Network firewall tool
- Backup and recovery management solution
- Password management vault
- Source code repository tools
- System center configuration manager
- Vulnerability management platform
- Monitoring platform for on-premises infrastructure, applications, and workloads.
- Monitoring and analytics platform for virtualized environments, capacity planning, and performance optimization.

- IT infrastructure monitoring and network management platform
- Ticketing and workflow management application

Organizational Level Practices

Leadership

WiseTech 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. This is performed at various levels across the business such as:

- Board Meetings,
- Senior Management Forums,
- Audit and Risk Committee (ARC) advises the Board on any material issues, including operational, financial and tax risk management, internal audit, and internal control systems.
- Information Security Committee Forums

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

Management Review and Continual Improvement

WiseTech have an established formal reporting structure to define reporting lines, accountabilities, and responsibilities as they relate to information security commitments. Risks and audit findings are socialized with leaders at the appropriate level via the various forums described under **paragraph A: Leadership.** This ensures visibility and support with the intent to correct and improve upon any risks/findings in an expedient manner.

Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of WiseTech's assets and to reduce the risk of fraud, error and bypassing of information security controls, through the use of appropriate access management controls. To this end control owners are identified and have responsibilities for the design, development, implementation, operation, maintenance and monitoring of the controls.

Continual improvement processes are in place to reduce risk and to process audit findings. Depending on the criticality, corrective actions may also be used for BCP/DR tests, high severity incidents, and security events. The status of corrective actions is reported to leadership.

Risk Management

Addressing risks and opportunities is a fundamental process for any business. 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*.

The Enterprise Risk Management framework has been established and is reviewed at least annually. This process includes the governance and management of IT risks.

Frequency of risk reviews are dependent on the risk type and the leadership forum to which it is issued. For example, Information Security risks are reviewed at least quarterly. Risk is also assessed at other operational levels such as in Supplier Risk Assessments and within our technical change management process.

Policy, Procedure and Awareness

An Information Security Framework and an Information Security Policy have been established. Policies and underlying Standards are determined and issued by senior management. Policies and Standards are reviewed regularly or as changes/risks present themselves. Critical policies such as Information Security Policies are reviewed annually at minimum. Changes to policy are communicated to relevant staff through the established training and awareness processes utilizing the company's learning management system.

To support our policies and ensure the uptake, acknowledgement and adherence by staff, WiseTech also utilizes WiseTech Academy training modules. Training progress for staff is tracked and reported to senior management. Where required, such as with Information Security Awareness, modules are released annually at a minimum to ensure the information remains relevant to staff.

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

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

Where relevant, policy acknowledgement is also conducted via employee contracts and training modules. Policy deviations are reported and monitored, including through incident reporting, whistle-blower reporting and HR mechanisms. Staff performance evaluation processes are undertaken at least annually; non-compliance with company policy forms part of this evaluation.

Communication

Security and availability commitments are communicated to external customers through use of Maintenance and License Agreements (MLAs). Each WiseTech customer is required to formally sign the MLA for use of the CargoWise application. Included within the agreement is information regarding the operation of the CargoWise application, its boundaries, and the roles and responsibilities for both WiseTech and the customer.

Security and availability commitments and associated system requirements are communicated 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 WiseTech 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 has been formalized and made available to internal users within the WiseTech Incident Management Procedure and Customer Service Team Enterprise Support Process documents, and to external users within each customer MLA.

WiseTech 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 portal (https://myaccount.cargowise.com/). The MyAccount portal 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 periodically sends email campaigns to designated customer technical or administrative contacts. WiseTech 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 plans have details on what, how and when to communicate to stakeholders, including our customers.

- Data Breaches – WiseTech has established Data Breach Notification processes in order register and take action on identified data breaches. These processes also align with GDPR notifiable data breach requirements.

Audits and Assurance Reporting

WiseTech undergoes a number of assurance and compliance programs both internally and by external providers/bodies. The results of these programs are communicated to leadership and any corrective actions are monitored to resolution.

Legal and Regulatory Compliance

WiseTech is required to adhere to the legal, regulatory, and contractual requirements of the countries and/or regions within which it operates. Via the forums listed under Leadership, new requirements or changes to any legislation are reviewed by our Legal Counsel and reported to senior management. These changes are then incorporated into the relevant business processes.

Operational Controls

Human Resource Security

WiseTech 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.

Prior to new staff onboarding, identity and criminal checks are performed. Once the hire is approved, the onboarding process initiates the asset and role-based access allocation as well as our extensive induction and compliance training programs. All new hires sign contractual agreements that contain security clauses such as policy adherence, disciplinary action details, and confidentiality statements for current and post-employment stages.

The “exit” process includes a revisiting of the post-employment obligations to ensure staff that are leaving are reminded of the confidentially obligations made to our company and for our customers information. Any relevant company assets are identified and returned.

Vendor Management

All new vendors go through a rigorous vendor selection process. WiseTech conducts security risk assessments as set out by the Supplier Relationship Security Standard for critical suppliers. This process includes a regular risk assessment for said suppliers.

Contracts with third parties include provisions relating to the movement and governance of information/data, where applicable. Confidentiality clauses and non-disclosure agreements are also included, where required. Service Level Agreements are included in contracts, where applicable.

Asset Management

WiseTech has an ICT Asset Management Standard established, describing how assets should be identified, tracked, and disposed. ICT Assets have an asset owner recorded in the ISMS Asset Register.

Asset disposal follows the ICT Equipment Disposal Procedure. Secure disposal includes secure removal of all data from the devices, removal of all company related identification and secure disposal. A record is retained of all assets handed over for disposal and certificates of destruction are kept as a proof of secure disposal.

Incident Management

WiseTech has established responsibilities and procedures for addressing security weaknesses, events, and security incidents in order to ensure quick, effective, consistent and orderly response to information security incidents, including effective tracking and communication on these information security weaknesses, events and security incidents.

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.

Incidents related to the CargoWise application may be raised by customers at any time via the e-Request function of the CargoWise application. Where incidents relate to a complete system outage or loss of functionality for an entire module with no manual workaround, incidents may be raised via telephone. All other incidents, however, are to be raised via the e-Request function of the CargoWise application.

Internal processes are also in place to monitor WiseTech’s network and system activities.

For high severity incidents senior management can initiate a Post Incident Review (PIR). The PIR results in lessons learnt to improve incident management and to minimize the risk of reoccurrence.

Information Classification

WiseTech has established an Information Classification and Handling Policy to ensure that information is managed and protected at an appropriate level, including encryption where appropriate.

Change Management

CargoWise Application Change Management Process

The WiseTech Software Development Change Management Process has been implemented by WiseTech management for the documentation, approval, testing and deployment of the CargoWise application software changes. CargoWise application changes follow a defined secure software development standard, which mandates secure coding principles.

This standard requires that security concerns are factored in from design through to deployment of the system development lifecycle.

Software changes to the CargoWise application are managed via workflow templates encompassing an agile System Development Life Cycle. Developers are required by the internal software code management system, which manages the life cycle, to complete mandatory tasks, such as build design reviews and code reviews. Testing is performed in a separate non-production environment prior to release into production.

WiseTech developers are responsible for writing and reviewing code based on the design prepared by the product team members. In conjunction to writing code, WiseTech developers are also responsible for writing code-failing test cases for each developed change. These tests are compiled and added to an automated testing and release tool’s test case repository. Manual user acceptance testing or functional review is then performed by a product team member to ensure that the change is functioning as designed. Prior to check-in, another series of test cases is automatically applied to all developed software changes. After each test case completes successfully, the automated testing and release tool (DAT) marks the source code (including the change) as “checked-in”. Once checked-in, the tool can compile and prepare a readable release package for distribution to customer environments. All changes must pass through the prepared test scripts in the automated testing tool and be approved prior to implementation.

Each customer is assigned their own unique automated service tasks scheduled within their own instance of the CargoWise application, and customers may choose when to perform their release deployment. The scheduling and execution of each customer's unique release task(s) is based upon a customer's nominated release ring subscription.

Release rings are used as a means of structured deployment of developed CargoWise application changes from WiseTech to individual customer environments. Release rings dictate the branch of CargoWise application updates received per the arrangements below:

- Development Partner Release (DPR) branch receive updated releases every week;
- Standard (STD) branches from the DPR release on a monthly basis;
- General Product 1 (GP1) branches from Standard release on a quarterly basis; and
- General Product 2 (GP2) branches from GP1 release on a bi-annual basis.

Access to manual release of code to production is restricted to authorized IT personnel only.

Emergency CargoWise application changes are often the result of critical incidents and are addressed as a priority. Such changes still follow the standard CargoWise application change management process; they are immediately assigned to developers and pass through expedited approvals. All emergency changes must be approved prior to implementation.

IS Infrastructure Change Management Process

Changes to information system (IS) hardware and infrastructure are controlled via the WiseTech Information Services Change Management Standard. Changes are categorized and measured against risk to ensure an adequate amount of oversight and review is performed. Changes are "templated" to ensure staff are aware of what information is required before changes will be approved.

The 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 lends itself to continually providing service reliability as we manage and improve our solutions.

Emergency infrastructure changes are often the result of critical incidents and are addressed as a priority. Such changes still follow the standard infrastructure change management process, they are immediately assigned to IT personnel, and pass through expedited Senior Team Leader review and approval, with change plans created and documented retrospectively. All infrastructure changes, including emergency changes, must be approved prior to implementation.

Technical Controls

Access Management

Access Provisioning/Modification

Internal users are assigned unique user IDs for standard or admin accounts. 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. Staff are assigned access to standardized groups within the application and/or infrastructure based upon their role within the organization.

The ability to create and modify the capabilities of CargoWise application or infrastructure user groups is restricted to authorized personnel, as privileged users, only. 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 regular basis.

Privileged Access

Privileged access includes both the ability to create new user accounts or assign authorizations to systems, applications, and data. Non-human accounts are included in the review.

Management performs a review of privileged system access on an annual basis to validate that it is restricted to authorized personnel.

Password Management

WiseTech uses centralized domain management of accounts and computer objects. An authentication solution enables users to securely authenticate with multiple applications and websites by using just one set of credentials.

Access authentication via the use of passwords has been configured across the environment, and includes requirements for password length, complexity, and re-use. Normal user accounts do not have expiration due to other controls in place, such as multi-factor authentication and password complexity.

Access Deactivation

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

Use of Service Accounts

A process has been established to manage the use of service accounts by authorized personnel. Access to service accounts within the WiseTech environment is governed via a password management tool.

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. Logs are synchronized to a single source Network Time Protocol where appropriate.

Monitoring is also performed across the CargoWise application and underlying IS infrastructure for capacity, performance, and uptime thresholds. More information can be found in specific topics throughout this document.

Network Security

WiseTech 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 Network Services Management team with secure firewall and SIEM solutions. Threat updates are automatically downloaded and installed on network security devices. In the event of network security errors or events, automated email alerts are raised by the alerting software and sent to members of the Network Services Management team for action.

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. Access to modify monitoring threshold configurations is restricted to authorized personnel only.

Cryptography

Public key infrastructure encryption is used for all user sessions connecting to CargoWise application. These keys are stored in an encrypted key vault within the WiseTech corporate network (not the CargoWise Cloud network but a separate isolated domain) and access to that is restricted to a small group of WiseTech senior engineering administrators.

Internally, WiseTech has a Cryptography Security Standard which drives aspects of cryptography implementations across the business. WiseTech continually review the system environment for areas where adequate encryption can be balanced for information security needs versus efficiency of service. Areas where encryption policies are implemented include data in transit, data at rest and in back up data.

Backups and Recovery

Backups at WiseTech are performed as follows:

- Backup of virtual images or systems is performed at each WiseTech location (WiseTech managed data centers, Equinix co-location data center, and Alibaba Cloud), which includes scheduled full and incremental backups. Backups are then copied to backup storage within MS Azure Cloud and/or Equinix bunkers.

- AWS S3 service is used to support the management and storage of CargoWise eDocs files. Each customer is provided with a dedicated S3 bucket where eDoc files are stored and accessible via the CargoWise application.

- Database log shipping is performed by an internally developed WiseTech log shipping replication tool, MultiCopy (MC), as soon as backups become available. In this way, replication to the destination location is typically completed shortly after backups are taken. MC utilizes the output of the disk backup service tasks to replicate data from one location to another, such that 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 plans within the program, is reviewed and components tested at least annually.

In the event of a major disaster, such as a site failure, the WiseTech Disaster Recovery Plan (DRP) will be invoked. The following supporting processes and documentation are also reviewed and tested annually at a minimum:

- Disaster Recovery Plan
- Crisis Management Plans
- Business Continuity Plans
- Incident Management Procedure
- Security Incident Response Playbooks

In the case of the Alibaba Cloud, there is no site failover; instead, uptime requirements are established via supplier contracted SLA and the SSO undergoes an annual review of the systems and organizational controls report.

Cyber Security

Vulnerability Management

The WiseTech 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 vulnerability scanners.

Anti-malware tools are used to protect systems and data from malicious software, and virus definition updates are automatically applied. WiseTech utilize a third-party software tool to synchronize and apply anti-spyware, anti-malware and virus definition updates on a daily basis. Real Time scanning along with active regular monitoring is performed over the WiseTech environment to identify potential vulnerabilities of system components to security and availability breaches.

Where applicable, WiseTech uses automated patching processes to minimize effort and increase the efficiency and timeliness of updates. For critical security threats, communications are issued to impacted teams as soon as the threat of a new critical vulnerability is confirmed. Vulnerability management effectiveness is continually monitored against target remediation timeframes and reported to management.

Development and Application Security

As a software company, application security is critical to WiseTech's services and its customers' needs. WiseTech has established a Secure System Development Standard.

Although development practices have a raft of security controls embedded, WiseTech invest further by employing expert AppSec staff. Some of the tools and techniques include:

- Code review enforcement
- Pull requests
- Mandated Unit Testing
- Vulnerability assessments

Physical and Environmental Security

Physical and environmental controls are documented in the Physical & Environmental Security Standard for WiseTech managed sites. Periodic maintenance of all environmental protection devices, including sensors, alarm systems and generators, are performed by the respective service providers or third-party specialists. Results of maintenance reports are retained.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

WiseTech's principal service commitment to end user entities is to provide reliable and secure software solutions and to protect customer data that is in WiseTech's possession. WiseTech's service commitments are communicated through Maintenance and License Agreements, the WiseTech Corporate Governance Statement, the WiseTech Information Security Statement, the Legal Terms of Use, and include but are not limited to the following:

Trust Service Category	Service Commitments
Security	WiseTech is committed to securing customer data and complying with relevant laws and regulations. To uphold this commitment, WiseTech implements comprehensive security measures including source code protection, data encryption, strong authentication mechanisms, physical security and other relevant security controls.
Availability	WiseTech is committed to ensuring the availability of the CargoWise ecosystem in line with customer Maintenance and License Agreements. This includes maintaining optimized service performance, reliable connectivity, and robust disaster recovery capabilities to minimize downtime and support uninterrupted access for customers.

WiseTech has established operational requirements that support the achievement of these service commitments, relevant laws and regulations, and other system requirements. Such requirements include the following:

Trust Service Category	**System Requirements**
Security	• WiseTech maintains appropriate Policies and Standards which provide guidance to WiseTech staff on the requirements for adherence to applicable information security controls. • WiseTech implements an information security program to protect customer data maintained within the CargoWise Application environment from unauthorized access. • WiseTech implements security processes and tools for change, vulnerability, and incident management to prevent, detect, and remediate security threats and vulnerabilities or potential data breaches. • WiseTech addresses risks relating to potential abuse, theft, misuse and improper access to in scope systems. • WiseTech implements a risk management program to assess Information Security risks and take corrective actions on the above.
Availability	• WiseTech maintains appropriate Policies and Standards which provide guidance to WiseTech staff on the requirements for adherence to applicable availability controls. • WiseTech ensures CargoWise application and CargoWise cloud environment availability to end users and recoverability of customer data by maintaining optimal infrastructure performance through continuous monitoring, backups and disaster recovery plans for quick and effective recovery in case of an incident. • WiseTech implements a risk management program to assess Information Security risks and take corrective actions on the above.