Independent service auditor's ISAE 3000 assurance report on A.P. Møller - Mærsk A/S's description of the design and operating effectiveness of controls relevant for the Trust Service Principles security, availability and confidentiality related to Integrated Transport and Logistics IT services

SOC 3 Report

Period: 1 January 2024 – 31 December 2024

Opinion: In our opinion, management's assertion that the controls within Maersk's Integrated Transport and Logistics IT services were effective throughout the period 1 January 2024 to 31 December 2024, to provide reasonable assurance that Maersk's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Contents

The report on Maersk's description of its Integrated Transport and Logistics IT services is confidential. This report is intended solely for use by the management of Maersk and Maersk's customers and should not be used by anyone other than these parties

1 Independent auditor's report

To: Management of Maersk A/S

Scope

We have examined Maersk's accompanying assertion titled "Management's assertion" (assertion) that the controls within Maersk's Integrated Transport and Logistics IT services (system) were effective throughout the period 1 January 2024 to 31 December 2024, to provide reasonable assurance that Maersk's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality (applicable trust services criteria) set forth in *TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Maersk uses subservice organisations to provide managed support services and data centre facilities. The description of the boundaries of the system (Chapter 3 of this report) indicates that certain applicable trust services criteria can only be met if controls at the subservice organisations are suitably designed and operating effectively. The description of the boundaries of the system of Maersk's Integrated Transport and Logistics IT services also indicates the complementary subservice organisation controls assumed in the design of Maersk's controls. The description does not disclose the actual controls at the subservice organisations. Our examination did not include the services provided by the subservice organisations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organisation controls.

The description of the boundaries of the system (Chapter 3 of this report) indicates that certain applicable trust services criteria can be achieved only if complementary user-entity controls contemplated in the design of Maersk's controls are suitably designed and operating effectively, along with related controls at the service organisation. The description presents Maersk's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Maersk's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organisation's Responsibilities

Maersk 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 Maersk's service commitments and system requirements were achieved. Maersk has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Maersk is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service auditor's independence and quality management

We have complied with the independence and other ethical requirements in the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct, as well as ethical requirements applicable in Denmark.

Our firm applies International Standard on Quality Management 1, ISQM 1, which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organisation's service commitments and system requirements were achieved based on the applicable trust services criteria.

We conducted our assurance engagement in accordance with ISAE 3000 (revised), "Assurance engagements other than audits or reviews of historical financial information", and additional requirements applicable in Denmark in order to obtain reasonable assurance to express our opinion about whether management's assertion i fairly stated, in all material respects.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its Integrated Transport and Logistics IT services and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment of risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our conclusion.

Our examination included:

- Obtaining an understanding of the system and the service organisation's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Maersk's service commitments and system requirements based on the applicable.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Maersk's service commitments and system requirements based the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent limitations

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 organisation's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Maersk's Integrated Transport and Logistics IT services were effective throughout the period 1 January 2024 to 31 December 2024, to provide reasonable assurance that Maersk's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Copenhagen, 3 June 2025
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper P. M

Jesper Parsberg Madsen
State-Authorised Public Accountant
MNE 26801

2 Management's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within A.P. Møller - Mærsk's (Maersk's) Integrated Transport and Logistics IT services (system) throughout the period 1 January to 31 December 2024, to provide reasonable assurance that Maersk's service commitments and system requirements relevant to security, availability and confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA, Trust Services Criteria. Our description of the boundaries of the system is presented in Chapter 3 and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period 1 January to 31 December 2024, to provide reasonable assurance that Maersk's service commitments and system requirements were achieved based on applicable trust services criteria. Maersk's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Chapter 4.

Maersk use subservice organisations to provide managed support services and data centre facilities. The description of the boundaries of the system (described in Chapter 3 of this report) indicates that certain applicable trust services criteria can only be met if controls at the subservice organisation are suitably designed and operating effectively. The description of the boundaries of the system of Maersk's Integrated Transport and Logistics IT services also indicates the complementary subservice organisation controls assumed in the design of Maersk's controls. The description does not disclose the actual controls at the subservice organisation. Our evaluation did not extend to controls of subservice organisations.

The description of the boundaries of the system (Chapter 3 of this report) indicates that certain applicable trust services criteria can be achieved only if complementary user-entity controls contemplated in the design of Maersk's controls are suitably designed and operating effectively, along with related controls at the service organisation. The description presents Maersk's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Maersk's controls. This report does not comprise the suitability of the design or operational effectiveness of such complementary user-entity controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organisation may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period 1 January 2024 to 31 December 2024, to provide reasonable assurance that Maersk's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed for and on behalf of Management:

Andy Powell – Chief Information Security Officer, Maersk

3 June 2025

3 Maersk's description of Integrated Transport and Logistics IT services

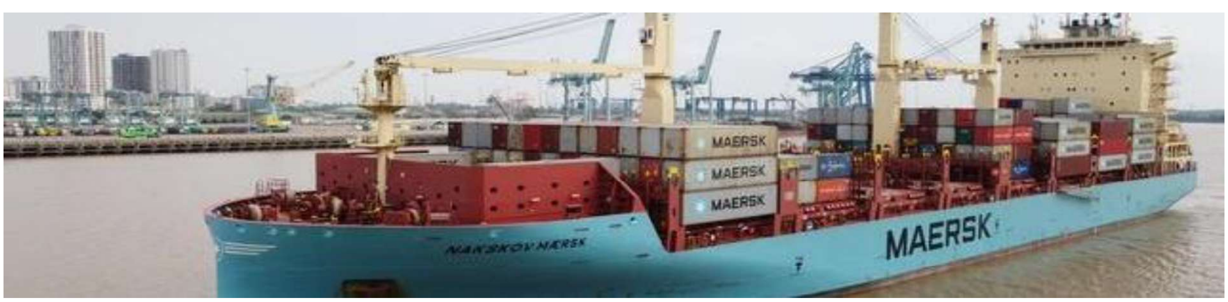
Business description

True industry-leading customer experience is not just a vision but our passion. A passion for our customers whose business is dependent on moving the right products to the right market at the right time. As Maersk strives to be a true integrator of container logistics, connecting and simplifying our customers' supply chains through global end-to-end solutions, we just made our customers´ lives a lot easier. We can manage the entire product journey for them including Inland Services, Maersk Customs Services, Ocean Freight, Warehouse Management and Distribution to name but a few, which have resulted in us moving a significant proportion of world trade everyday all the way.

Bringing opportunity and growth to every corner of the world.

Bringing cargo from one part of the world to another can be seen by our customers as a complex and unreliable process. We aim to deliver better reliability, more visibility and simplicity with our strategy: to become the global integrator of container logistics, connecting and simplifying our customers' supply chains. We will continue to leverage technology in the parts of the business that bring most value to the customer, and digital innovation remains key to offer customers a simple end to-end solution.

We are able to offer our customers services ranging from scheduled container shipping, through to complete end-to-end supply chain management. This breadth of capability is represented by our three service models: Transported by Maersk, Fulfilled by Maersk and Managed by Maersk.



Transported by Maersk is the foundation of our Integrator Strategy. It caters for customers who have a logistics department capable of managing their supply chain and want Maersk to transport their cargo in a container, where we are accountable for delivering the transportation outcome across Ocean and L&S products. The differentiating part of this model is that we take full accountability for the agreed outcome, offer customers speed and flexibility during the journey, and do it in a simple and cost-efficient way.

This service model caters for customers who want Maersk to move up the value chain to manage their cargo at the SKU level (stock keeping unit) and thereby also manage a larger part of the supply chain. In addition to Transported by Maersk, these customers desire physical fulfilment at the final destination, holding Maersk accountable for having the right goods at the right place at the right time, delivered through warehousing and specialty solutions such as e-commerce logistics and cold chain logistics. This further simplifies customers' supply chains by removing the need for a separate party to manage the last mile transportation.

Managed by Maersk caters for customers who don't have a comprehensive distribution or shipping department because they want to focus on developing a product or their business' core competency. Because these customers outsource all or part of their supply chain, they want Maersk to manage it according to their desired service level. For example, Maersk can manage the part of a customer supply chain from vendors to stores in the fashion, retail, and lifestyle verticals. We can take over from Purchase Order and then work with vendors and decide, based on the customer's pre-set KPIs, the mode of transportation that should be used, or whether it should be consolidated in the logistics network. Our specialisation is to act as 3rd Party Logistics (3PL) or 4th Party Logistics (4PL) for our customers. In this model, we become a proactive and trusted advisor to drive true strategic integration with customers.

Scope of the Audit Report

This report focuses on processes and controls applicable to Maersk's internal control environment. The scope of this report covers critical systems, applications, networks, human resources, and information assets connected with the handling of customer information.

Application	Description
Active Directory / Domain Controller	Controls authentication and access to the network on which the applications in scope reside.
GCSS (Global Customer Service System)	End-to-end customer service and order handling application (i.e., from receipt of booking through to delivery of cargo). It is used in offices, ports, depots and terminals. Key functionality includes: • Keeps track of all required activities to a shipment, their status, the order in which they must be executed, and by who. • Automatically finds a route and ship for the transport, based on the customer's preferences. • Sends out instructions to trading partners and associated companies (such as trucking companies) about where and when to pick up or deliver a given container. • Calculates the expected arrival and departure time for each container, on each location point on the route, and watches the actual movement of the containers, reporting deviations in the process. Automatically prices and invoices the shipment when due
MEPC (Maersk Electronic Product Catalogue)	Dynamic electronic product catalogue where Maersk staff create and search for products (e.g., cargo route information) to offer customers.
AFLS Cargo & Price (Accenture Freight and Logistics Software)	AFLS is an application that allows Maersk to register and manage quotes, contracts, tariff and market rates. The application acts as a rating engine to support calculation of rates and charges when, for example, GCSS needs to price a shipment. Note that AFLS is being replaced by Athena during 2024 and 2024.
RKEM (Rederiets Kontainer Division Equipment Management)	RKEM is used to control Maersk's equipment fleet and assets. It records equipment characteristics (dimensions, weights, machinery etc.) and equipment moves (gate, load, discharge, shift) for all owned or leased containers, and for Vessel Sharing Agreement (VSA)/Shipper Owned containers when moving on our vessels.
USI (Unified Security Infrastructure)	An identity and access management solution, which provides the following features to Maersk applications: • Customer registration & approval process • Single sign-on • Authentication and authorization • Role based access control • Attribute based access control

	There are two clusters of USI deployed: one for customer-facing applications over the internet and another for internal applications accessed over the intranet. Note that USI is being replaced by ForgeRock during 2024.
SSIB (Self Service Instant Booking)	SSIB provides a digital self-service automated booking process, which allows the customer to make a booking directly from a quote or from an existing contract, with instant confirmation.
ForgeRock - cIAM	A customer identity and access management (cIAM) platform, which was implemented to replace the existing Unified Security Infrastructure (USI) solution during 2024. ForgeRock will handle authentication mechanisms, customer access token provision and role-based access control for most of Maersk's customer platforms, including maersk.com.
Athena	Athena is a new core pricing product replacing AFLS during 2024 and 2024.
Network Devices (LAN/WAN/Firewalls)	Maersk's networking infrastructure facilitates connectivity of Maersk devices and systems within, and across, our operational facilities and offices. Firewalls act as the first line of perimeter defence for Maersk's networks, protecting us from attacks.
MODS (Maersk Logistics Operational Documentation System)	MODS is the core Maersk Supply Chain Management (SCM) system handling all the documents and operational activities. It handles logistics and operational documents including purchase orders, shipping orders, and container stuffing.
MORE (MODS Realtime Extract)	MORE is responsible for receiving and distributing data in a harmonised, synchronised, and consistent fashion within the Maersk SCM (Supply Chain Management) platform. By virtue of storing data beyond the availability in source systems and by implementing a common data model, MORE is the de facto data warehouse for the Maersk SCM platform and is designed to operate in near real time.

BluJay TMFF (Transport Management for Forwarders)	Freight Forwarding operational application covering booking, customs filing, job costing and invoicing, across Ocean, Air and Value Added Services (VAS) products.
CargoWise One	Transport Management System (incl. several modules like Forwarding, WMS, Accounting etc), backbone of SENATOR's whole operations worldwide; used by all operational staff (and accounting staff where CW1 is used for GL accounting).
Maersk Warehouse Management System (WMS)	Maersk WMS is a software solution specifically designed to manage and optimise warehouse operations within the supply chain. Maersk WMS offers functionalities to efficiently control and track the movement, storage, and handling of goods within a warehouse or distribution centre.
NFTP/SAP S4HANA Finance	With NFTP, Maersk is building the right technological foundation, with SAP S/4HANA at the core, to provide real-time, trustworthy Finance and Tax analytics through a standard model for data capture, in one enterprise-wide platform.
New Supply Chain Platform (NSCP)	Maersk's New Supply Chain Platform to connect and simplify global supply chains. NSCP will eventually replace MODS. The SCM platform provides a suite of applications and services that support the complex world of supply chain management enabling our customers/partners to bring their goods to market with maximum efficiency and minimum risk.
SAP TMS	SAP Transportation Management (SAP TM) supports all activities connected with the physical transportation of goods from one location to another.
myMaersk Supply Chain	myMaersk Supply Chain is a one-stop logistics portal which comprises several modules including Shipper, Reporting and Track & Trace, Document Management, and Communication & Exceptions (C&E). It provides a single, web-based access point for end-to-end supply chain information. Its main purpose is to make it more convenient for users to access various SCM applications.

Company Overview

Organisational Structure Board of Directors

The Board of Directors is responsible for the overall and strategic management of the Company and for ensuring that the company is properly organised. In addition, it is the obligation of the Board of Directors to follow up on adopted plans and forecasts and to consider the Company's significant dispositions, overall insurance matters, cash flows and special risks.

Executive Board/Executive Leadership Team (ELT)

The ELT serves as the link between the Board of Directors and operational level management. The ELT is responsible for overall operations, financial results and business growth. It plays a critical role in the operations of the company. The ELT has representation from all business functions and serves as the multidisciplinary decision-making body of the company.

Sales, Service, Support & Marketing

The sales, services, support and marketing functions are organised into the geographical segments in which they operate. These divisions spearhead the marketing, sales and service initiatives and are responsible for positioning Maersk's services in the global market.

Technology Team

Technology and data are the key enablers for creating customer value and integrating container logistics. Our technology strategy aims to create sustainable competitive advantage and superior customer and business outcomes, enabled by digitalisation, standardisation, automation and by leveraging data as a discrete asset.

Cyber Security Team

The Cyber Security team is led by the Chief Information Security Officer. The team is responsible for controlling and mitigating risks, issues and events arising from interconnected systems, information, applications, IT infrastructure and operational environments. The Maersk Cyber Security team comprises 300 highly skilled and experienced colleagues and their goal is daily excellence in anticipating, withstanding and adapting to adverse conditions, stresses, attacks or compromises, and leading company responses across people, process and technology.

Criteria and Controls

The criteria for the Security, Confidentiality and Availability principles are organised into (a) the criteria that are applicable to all principles (common criteria) and (b) criteria applicable only to a single principle. The common criteria constitute the complete set of criteria for the Security principle. For the principle of Confidentiality and Availability, a complete set of criteria is comprised of all the common criteria and all of the criteria applicable to the principle being reported on.

Common Criteria for Security, Confidentiality and Availability

The common criteria are organised into seven categories as described further below.

ORGANISATION AND MANAGEMENT

Maersk's organisation and management

Maersk's organisational structure provides the framework within which its activities for achieving entity wide objectives are planned, executed, controlled and monitored. The organisation has established documented procedures to ensure that those criteria relevant to how the organisation is structured, and the process that the organisation has implemented to manage and support people within its operating unit, are satisfied. Maersk operates under the general direction of its Board of Directors and is managed day-to-day by the Executive Board/Executive Leadership Team (ELT).

Job descriptions are in place and define roles and responsibilities, skills and knowledge requirements. Maersk's organisational structure, reporting relationships, authorities and responsibilities are evaluated and reviewed at least annually by the ELT. Once approved by the ELT any changes are communicated to employees.

Maersk Technology

Maersk is continuously looking at how the company can effectively connect and simplify customers' supply chains as the global integrator of container logistics. Leveraging the power of technology is essential to deliver the connected experience and products that customers need. To this end, digital platforms are the key to unlocking a real acceleration in Maersk's ability to launch new products, grow our business and create a market-leading customer experience.

The Chief Technology & Information Officer (CTIO) is a member of the Executive Leadership Team (ELT) and leads the technology transformation strategy and evolution of digital platforms. Our digital platforms are the glue that connect data, business applications, processes, and their underlying systems, from across different parties, to create a networked effect that everyone benefits from.

Maersk Cyber Security

Maersk has developed an organisation-wide Cyber Security Management Framework aligned with the NIST Cybersecurity Framework. Included in the framework are policies, standards and controls relating to Confidentiality, Integrity and Availability of information and information systems.

Pause

Think

Protect.

The Chief Information Security Officer (CISO) has overall responsibility for Maersk's security framework. Cyber Security is a standing item on the agenda of the Audit Committee meetings, which includes deep dives on cyber risk and independent assessments of the maturity of the Cyber Security organisation. The Chairman and Chief Executive Officer (CEO) of the group have visibility of cyber reporting by the CISO to the Audit Committee, and progress on mitigating cyber risk is also reported quarterly to Enterprise Risk Management. In addition, the CISO routinely briefs ELT members and company Vice Presidents (VPs) on cyber security and reports to the Main Board at least once per year.

The CISO is responsible for reviewing Maersk's Cyber Security Policy on an annual basis and for aligning the changes in policy to new business and technology requirements as they are identified. Changes to any of Maersk's policies and standards, including the Cyber Security Policy, are reviewed, and approved by the ELT as part of the company's Commit framework of controls.

Kyndryl provides managed support services including backup as part of the service it provides to Maersk and is ISAE 3402 certified.

Human Resources

The Human Resources Team defines policies and procedures for recruitment and termination of employment. The policies define terms and conditions of employment (including requirements for adherence to the cyber security acceptable use policy), education and training, termination or change of employment and pre-employment checks.

All policies, standards and procedures are documented and made available to personnel through Maersk's intranet.

Before being granted access to the Company's Information:

- The Human Resources Team performs background screening and requisite verification checks for the candidate/employee, commensurate with the sensitivity of the role. The background checks are used to assess a candidate's education, training/ qualifications, previous employment and experience as well as any criminal record (where applicable). These checks are carried out in accordance with applicable local laws.
- The employee is required to sign an Employment Agreement with the company which includes clauses for maintaining confidentiality and non-disclosure of information.
- The employee must read and acknowledge their understanding of Maersk's Cyber Security Policies and Cyber Security Awareness Training including the Acceptable Use Booklet.

Following termination of employment (either by Maersk or the employee), the HR Team works with the employee's manager to ensure a separation checklist is followed and all tasks are completed.

COMMUNICATION

Internal Communication

Maersk maintains communication with personnel using internal collaboration tools, knowledge databases and e-mail. The communication includes, but is not limited to, communication of Maersk's Cyber Security policies and procedures, corporate events, new initiatives, new employee onboarding and Education, Awareness and Training.

Changes and updates to Maersk's Cyber Security policies and standards, and implementation of changes on Maersk network and security infrastructure are communicated to relevant Maersk personnel through internal collaboration tools.

Policies and procedures specific to Maersk's operations, including those for managing confidentiality, integrity and availability are made available to Maersk personnel through the company intranet.

Cyber Security Awareness training is provided to personnel at least annually, which provides employees with an understanding and awareness of their responsibility and accountability for Maersk's security posture.

Training materials are developed jointly by the Strategic Learning & Development, Awareness and Human Factors Engineering teams, all under the Senior Director responsible for Cyber Security Governance, and are maintained annually or more frequently as changes occur. Periodic town hall meetings are conducted by the Technology Leadership Team for the benefit of all Technology employees.

Maersk's security intranet describes security measures that Maersk has in place, including policies, standards, controls, and processes for reporting security incidents and raising cyber risks.

External Communication

Maersk utilises its website and email to communicate to external customers, vendors, and other parties. A list of services and initiatives is available on Maersk's main website: www.maersk.com. Maersk's Master Services Agreement (or equivalent customer contract) clearly communicates to customers the functionality of the services provided, and the responsibilities of each party in relation to such services (this includes information

We're using technology to shape a paradigm shift

on the Terms and Conditions that exist between Maersk's provision of the services, and a customer's use of the services). Links on the website include details about Maersk's services, its intended use and privacy policy.

An impact analysis is performed prior to contracting with any third-party service provider in line with the Supplier Security Standard. A non-disclosure agreement is signed by third parties prior to confidential information being shared with those parties.

All non-disclosure agreements, and third-party contracts, communicate Maersk's security commitments and required security obligations, terms, conditions, and responsibilities and are signed by authorised approvers to signify management agreement.

RISK MANAGEMENT AND DESIGN AND IMPLEMENTATION OF CONTROLS

Risk Identification

Maersk generates information on cyber security risks from the following sources:

- Risk and threat modelling by the Cyber Threat Intelligence team in relation to business assets.
- Risk and threat modelling by internal business and software development teams during the development of new or updated product features.
- Regular penetration testing by third-party specialists and our in-house red team.
- Regular vulnerability assessments of applications.
- Alerting services providing real-time information on cyber security trends and threats.
- Operational data and alerts from application and infrastructure log analysis.
- Ongoing monitoring of compliance activities and trends by the CISO and Chief Technology and Information Officer.
- Review of user logs showing system log in attempts and failures.
- Subscription to relevant newsletters and attendance at relevant forums.

Cyber security risks are managed through several processes:

- Application-level controls for risks that have been identified by risk and threat modelling, penetration or vulnerability testing are managed using the normal "systems development lifecycle" workflow management and tracking tools, with defined fast track processes for high-risk vulnerabilities or bugs in production systems.
- Infrastructure risks, including infrastructure patching and configuration, are managed as an integral part of operational management processes by the Technology organisation, who are also responsible for infrastructure security monitoring.
- Application security monitoring, including anomalous application behaviour detection and response, is managed by the Technology organisation.
- Enterprise security monitoring (threat management, vulnerability management and incident management) is conducted by the Technology organisation.

Risk Management

Oversight of cyber security risk at a corporate level is undertaken by the Audit Committee on behalf of the Main Board and by Enterprise Risk Management on behalf of the Executive Leadership Team (ELT) and is managed by the Chief Information Security Officer. Cyber security is a standing item on the agenda of Audit Committee meetings and reporting to Enterprise Risk Management is undertaken quarterly.

To embrace change
you have to be willing
to go all the way.

Maersk has a formalised cyber risk management process and maintains a Cyber Risk Register that tracks all cyber risks to the enterprise. Risk assessments include a review of internal and external factors that threaten the achievement of business objectives.

Mitigating controls are identified, and risks with residual scores above the acceptable risk threshold have mitigating actions agreed that are then tracked by the Cyber Security team.

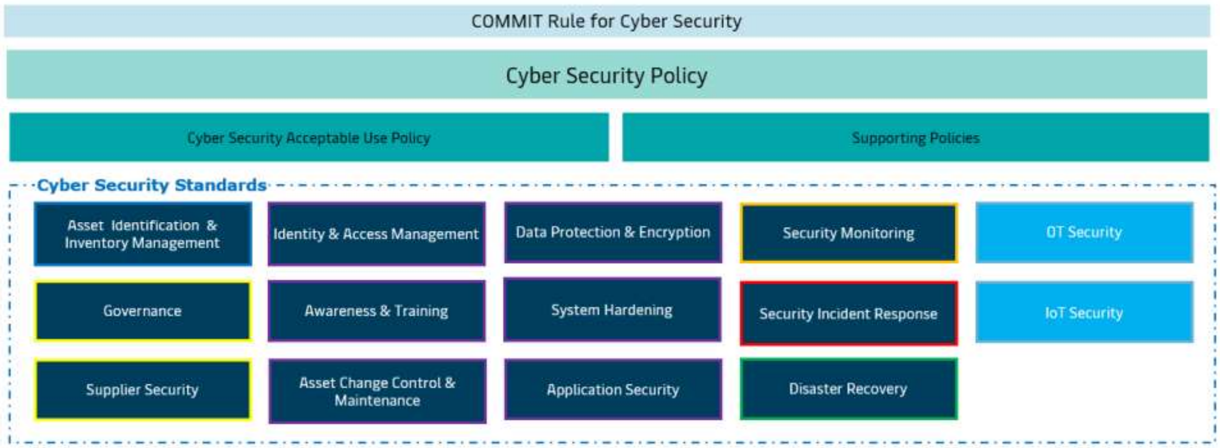
Controls Overview

Maersk has developed formal company-wide policies and standards for meeting the requirements related to Security, Confidentiality and Availability. Policies and standards are available via the company intranet to all personnel.

The cyber security policy framework describes the cyber security policies, standards and controls that are required to protect Maersk's assets which include people, information and infrastructure. It focuses on the outcomes that are required to achieve a proportionate and risk-based approach to cyber security that enables our business to function effectively, safely and securely. It comprises the top-level Cyber Security Policy, the Cyber Security Acceptable Use Policy Booklet (which defines expected behaviour for all employees and contractors when handling information and using IT systems), 12 IT Cyber Security Standards, as well as the IoT Security and OT Security standards, as shown below.

All policies are kept up to date and are reviewed and approved by the Executive Leadership Team (ELT) on an annual basis, or more frequently as necessary (for example, based on an updated risk assessment).

Cyber Security Policy and Standards Structure



MONITORING OF CONTROLS

Security

Maersk's cyber security assurance operating model has 3 lines of defence:

- First Line of Defence - automated checks for exploitable weaknesses and misconfigurations.
- Second Line of Defence - internal Assurance team measuring deviation against cyber standards, augmented by PwC who assist with our SOC2 Type2 assessment and certifications and independently assess our Cyber Security maturity.
- Third Line of Defence - audits, conducted by Group Internal Audit and/or external auditors focusing on deep dive assessments in specific technical areas.

Technology teams conduct quarterly compliance checks against the security policy and access control standards. This includes checks that quarterly user access reviews are performed for production systems and network access. Password settings for systems are also included in the review.

On an annual basis, the Cyber Security Third Party Risk team completes supplier reviews. This includes receiving compliance reporting from subservice organisations and reviewing the reports for any issues. Review results are fed into the risk triage process and are presented to Vendor Management for discussion and approval of the ongoing supplier relationship. Should any issues be identified, they will be logged and assessed to determine the impact on the Maersk environment. All issues will be tracked through to successful resolution.

The Cyber Security Function performs an annual internal audit to review the design and operating effectiveness of internal controls. The results of these reviews are reported to the ELT with response plans developed in relation to material deficiencies.

Ongoing Monitoring

Maersk uses a wide variety of automated monitoring systems, which cover security, service performance and availability. Monitoring tools are implemented to detect and protect against external and internal threats. System performance including availability is also continuously monitored through a specific set of tools and Maersk Controls.

A dedicated Customer Services team is in place to service customer requests and monitor customer feedback for performance, which makes its way back to the Technology teams to action for resolution.

LOGICAL AND PHYSICAL ACCESS CONTROL

Maersk has a defined and documented Identity and Access Management Standard that governs the processes for identification and authentication of authorised users, restriction of user access to authorised system components and prevention and detection of unauthorised system access.

A tech-enabled logistics company

Logical Access Path

All access to Maersk systems and applications requires authentication.

System Administrators connect to the production environment hosted by Kyndryl via a two-factor user authentication process, and this is required at every logon.

Maersk personnel access their code version control and change management systems via Single Sign On (SSO) using their Maersk user ID and password.

Password Security

Password policies are in place across production environments in line with the password requirements stipulated in the Identity and Access Management Standard.

Separate security policies are implemented across company workstations (desktops/laptops) and servers within the Maersk network. Access to the network environment is controlled via two-factor authentication.

Unattended workstations are locked using a password protected screen saver after a defined period of inactivity.

Identity & Access Management

User Account Management: Access to in-scope systems is granted on a need to know and least privilege basis. Role-based access privileges are enforced by access control systems. General access to in-scope systems is authorised by both the Business Managers and the Technology team. The initial setting of, and subsequent changes to, access privileges is approved by the Business Managers. Revocation of access for terminated personnel is performed in a timely manner via a process managed by the HR Team and supported by an automated service management tool.

User Access Review: A periodic review of user access rights is completed by the Business Managers and Technology teams to ensure the level of access is appropriate. Any access which is deemed to be no longer required, is identified and disabled.

Customer Access Management: Access to the Customer Portal is provisioned for an authorised customer representative following execution of a customer agreement. The customer administrator is responsible for managing and monitoring access to the customer portal, including optional enforcement of two-factor authentication. All customer accounts and access to the Customer Portal will be revoked following termination of a customer agreement. The customer portal enforces minimum required password settings including the disabling of user accounts after a limited number of unsuccessful logons for a specified duration.

Physical Security

Production Environment Physical Access: Servers holding Maersk and its customer data are hosted within ISAE3402-certified data centres (private cloud) or within secure and trusted public cloud services. Controls for ensuring physical and environmental security are implemented and managed by Kyndryl and public cloud providers and are therefore out of scope for this report. Physical access is tracked and logged and follows an approval process to gain access.

The Identity & Access Management Standard sets out the minimum-security standards for Data Centre facilities. Maersk relies on third-party attestation reports provided by Kyndryl and public cloud providers for ascertaining the design and operating effectiveness of physical and environmental security controls.

Network Security and Vulnerability Management: Periodic internal and third-party security reviews, vulnerability assessments and penetration tests are completed. Vulnerabilities identified are logged, reviewed to determine expected remediation timeframes, and tracked through to resolution with reporting to the ELT on a quarterly basis.

We are committed to sustainable growth

Firewall rules limit incoming connections and define the types of activities and service requests that can be performed from external connections. Intrusion detection and prevention systems (IDS/IPS) are also utilised to analyse and report network events. Automated alerts from IDS/IPS are logged and resolved in a timely manner.

SYSTEM OPERATIONS

Backups

Maersk has a Disaster Recovery Standard that governs the performance of data backups and data restoration. Kyndryl is utilised to maintain a 7-day rolling and incremental backup of all information. Alerts for failed backups are raised for resolution via log monitoring processes.

Restorability and integrity of backups is periodically assessed and provides confirmation of Disaster Recovery capabilities.

Patch Management

Maersk has a System Hardening Standard and related patching processes, which define how to identify and deploy patches, and include criteria for deploying fast-tracked critical and standard patches.

The patching environment for business-critical assets is a thoroughly documented process and covers all areas of patching, including testing approval, deployment and roll back of patches. Patches are applied based on scheduled timelines and follow an established change management process.

All patches requiring deployment are raised as a change through the change management process. Once approved, the patches are deployed onto the IT assets. All information for the required patch is logged through the change ticket.

For critical patches, the same process is followed; however, an exception change is raised to expedite deployment. Before patches are applied to the production environment, they are tested in the test or pre-production environment. Once successful deployment is confirmed in the lower environments, they are then rolled out to the production environment through automated tools.

Security Incident Management

Security Incidents: The Technology organisation follows documented incident response plans for specific scenarios that could impact security. Security incidents that arise are notified to the Respond team in the Cyber Security Operations team. The Respond team manages the security incident management process and will involve adequate resources to resolve the incident as quickly as possible. Incidents are recorded in the automated service management system, and if relevant, and not customer sensitive, the status page in the Maersk platform is also updated to communicate any relevant breaches, incidents and threats.

Post Incident Reviews: If the incident was categorised as a major security incident, the SOC will conduct a post incident review. The main purpose of the post incident review is to evaluate the response to an incident and derive lessons learnt from it. Any major security incidents are raised and discussed with the Technology Leadership team.

Audit Logging & Monitoring

Logging and monitoring software is used to collect data from in-scope systems to monitor system performance, potential security threats and vulnerabilities, and resource utilisation; and to detect unusual system activity or service requests.

Logs are reviewed as required to investigate issues and as part of formalised weekly reporting. Any issue identified via log review is logged and tracked through to resolution.

CHANGE MANAGEMENT

Overview

Improving life for all by integrating the world

Maersk follows a formal development process that includes being able to iteratively roll out functional and non-functional changes while targeting both high quality and availability. Management has documented system development, change and release management policies and processes to communicate Management's expectations regarding performing changes to the production environment. These policies and processes apply to all changes to the production environment and convey the change control process including assessing the impact of changes, testing, rollback procedures, approval requirements and change communication to relevant stakeholders. In addition, change management personnel involved in the change management process agree on their meeting cadence to discuss the prioritisation of current and proposed changes.

Change Request Initiation and Control

Infrastructure Changes: Infrastructure changes (such as new servers, server patches, firewall rule changes, configuration changes, changes to the hypervisor, network or storage components etc.) are raised through the service management system. Requests are fielded by the Technology Leadership team who will form an implementation plan.

System Changes: The Technology Leadership team have created a Global Product Roadmap which details the projects expected to be undertaken for the next 12 months and provides visibility to the business around what is planned. The projects are then placed onto a priority listing, which forms the basis of upcoming work. The Leadership team meet regularly to assess upcoming work for scope, resourcing and effort required, and reprioritise if required. The roadmap is reviewed periodically and posted on the intranet. Planned developments impacting external users are communicated as required.

When changes are identified, the change requestor creates a ticket in the task management system to track the change through implementation to ensure the Maersk change management process is followed. Relevant stakeholders are notified when a change is identified and kept informed of all changes through the task management system. Change stakeholders populate key fields on the ticket, including the change request description, desired outcomes, and importance to the business.

For larger projects, the project details are defined within a project poster, which includes details of the impact to users, problem being solved and the solution design. Potential risks, including impacts on security, privacy, access and performance, are considered as a part of the project planning process and regularly during the project lifecycle. Chief Technology and Information Officer approval and sign-off is required for all larger projects.

Impact Assessment

Developers work in a separate developer environment and merge their changes once all local tests are passed. They will initiate a pull request within the Software Development tool used for version control, which requires the Quality Assurance (QA) team or a senior developer to perform a code review. Once the code review is completed, the change is integrated into a staging environment.

Further regression and user acceptance testing is performed. Once completed, the release is merged into a pre-production environment to ensure stability. Before the change is released, it is reviewed by a member of the Technology Leadership team to assess impact and risks and any communication required. Once assessed, the change is released into Production. Access to the different environments utilised in the change management process is logically restricted to provide segregation.

Control of Changes & Monitoring

Maersk uses continuous integration software to manage, track and provide control over versions of source code for releases. Development personnel check out source code and store it locally. Once the team are ready to update the code repository, they check the code back in and it is assigned a different version number. This allows users to roll back code to previous versions when necessary. The ability to merge and pull-down source code during development from the version control software is restricted to relevant Technology team members.

The release of compiled builds is managed by a release management system. Before a migration to production can occur, a manual approval step by a designated approver is enforced. Key activities that occur during the change and release process are automatically logged with details about the change, including timestamp and user information. Teams are also notified automatically of key changes that occur to their applications through the collaboration messaging system, which is integrated with the release management software.

The Application Management team works with Development teams to schedule releases and confirm all testing, QA and documentation review for the release that has been performed.

Emergency Changes & Rollbacks

Multiple historic release versions are retained and mapped in the Continuous Integration application. This, along with the version control tool, allows for any changes or releases which cause unexpected behaviour to be efficiently rolled back to the last, stable release.

Additional Criteria for Confidentiality

DATA CLASSIFICATION AND DATA ACCESS CONTROL

Maersk assets and information systems are categorised based on the criticality to the continued operation of the organisation. An IT asset is defined as Business Critical if, as a result of completing a Business Impact Assessment (BIA), the application scores above a threshold rating against the Confidentiality, Integrity or Availability criteria. In addition, information/data are classified as Confidential/Internal/Public. The classification enables personnel to determine the standards of protection that must be applied, as unauthorised disclosure could adversely impact Maersk, customers, suppliers, business partners or employees.

Personnel requesting access to sensitive data/information relating to Business-Critical Assets (BCA) as part of their work are required to raise a service request, which is approved by the Business Managers and the Technology Leadership team.

Personnel connecting to the production environment network require two-factor authentication. There are separate environments for development, testing, pre-production and production. Production data is housed only in the Production environment.

Maersk performs quarterly user access reviews. During the review, Business Managers and Technology team review user accounts to ensure that all access is appropriate and has been approved. If any accounts are found to be violating Maersk's Identity & Access Management Standard, the respective accounts are disabled.

DATA ENCRYPTION

Web sessions are encrypted between the customer's browser and Maersk's servers using industry-standard encryption. All web traffic is allowed only through a HTTPS protocol.

Data travelling over public networks, e.g., EDI, eCommerce and booking data, is encrypted using industry-standard TLS algorithms and certificate configurations. Relevant encryption standards such as TLS are applied to data in transit moving across public networks.

Communication between Maersk's data centre environments is over encrypted secure VPNs. During storage, all production data is encrypted using industry-standard encryption.

Information is encrypted in transit and at rest. Hardware-based full-disk encryption is enabled for all staff workstations as part of the initial set-up.

The Data Protection & Encryption Standard specifies the expected levels of cryptographic controls.

CONFIDENTIALITY ENABLERS

The Cyber Security team is responsible for changes to confidentiality practices and commitments, which are communicated to relevant internal and external stakeholders as required.

Maersk Cyber Security Policies and the Acceptable Use Booklet are communicated to personnel when joining. With the acceptance of the employment offer, the employees acknowledge that they will abide by the policies communicated by the HR Team. All new hires undergo induction within the first month of employment which includes introductory sessions around cyber and information security and its importance to Maersk.

Maersk ensures that it has applicable clauses relating to confidentiality and non-disclosure in service agreements with vendors and suppliers, as well as in its agreements with its customers.

As part of onboarding a customer, Maersk performs a gap analysis between customer confidentiality requirements and internal policies. Customer security requirements that are more onerous than existing Maersk cyber security policy requirements are reviewed for incorporation into Maersk's policy or logged for change on an as needed basis.

Maersk disposes of customer data in accordance with requirements of the customer contract being terminated.

Maersk creates test data using data masking software that replaces confidential information with test information prior to the creation of test databases; no real customer data can be used for testing / development without a robust justification and suitable management authorisation.

CHANGES TO THE CONTROL ENVIRONMENT IN 2024

During the period covered by the report Maersk has continued to enhance and develop its global digital estate. The roll-out of the Maersk Warehouse Management System (MWMS), CargoWise One and the New Supply Chain Platform (NSCP) has occurred during 2024 and has proven to enhance our central security monitoring capability.

SIGNIFICANT EVENTS AND CONDITIONS; OTHER THAN TRANSACTIONS

If significant events and conditions arise, Maersk has Disaster Recovery Plans designed to ensure the systems continue to provide customers with the services covered by this report.

Complementary Subservice Organisations Controls

Maersk uses private and public cloud providers as subservice organisations to provide services, which form part of the Maersk booking service to be used by Maersk's customers, including data centre hosting, backup and storage, application development and support.

Controls of subservice organisations providing the aforementioned services have been clearly defined within the description of service requirements for the benefit of Maersk's Customers.

In the design of internal controls and procedures, Maersk has assumed the following procedures and controls are implemented by the subservice organisations:

Applicable Trust Services Criteria	Controls Expected to be Implemented at the Subservice Organisation
CC2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Establish mechanisms for consistent and effective internal communication, ensuring clarity in roles and responsibilities pertaining to internal controls.
CC2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.	Develop and maintain formal communication channels with external parties to address matters impacting internal control processes and expectations.
CC6.1 The entity implements logical access security software, infrastructure and architecture over protected information assets to protect them from security events to meet the entity's objectives.	Deploy comprehensive logical access security mechanisms to ensure the protection of information assets from unauthorised access.
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorises new internal and external users whose access is administered by the entity. For users whose access is administered by the entity, user system credentials are removed when user access is no longer authorised.	Implement rigorous authorisation processes for the registration, authorisation, and timely deactivation of user credentials.
CC6.3 The entity authorises, 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.	Establish procedures to ensure access rights are role-based, adhere to least privilege principles, and are regularly reviewed and updated.
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 authorised personnel to meet the entity's objectives.	Enforce strict physical access controls to sensitive facilities and information assets, ensuring access is granted only to authorised personnel.

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.	Ensure the secure disposition of physical assets to prevent unauthorised data recovery once protections are no longer necessary.
C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Execute secure disposal procedures for confidential information, ensuring that no unauthorised access occurs post-disposal.
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Implement advanced security measures, such as firewalls and intrusion detection systems, to guard against external threats and unauthorised access.
CC6.7 The entity restricts the transmission, movement and removal of information to authorised internal and external users and processes, and protects it during transmission, movement or removal to meet the entity's objectives.	Establish controls to authorise and safeguard the transmission, movement, and removal of information, ensuring protection from unauthorised access.
CC6.8 The entity implements controls to prevent or detect and act on the introduction of unauthorised or malicious software to meet the entity's objectives.	Implement preventive and detective controls to mitigate the risk and impact of unauthorised or malicious software.
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.	Adopt robust detection and monitoring procedures to identify configuration changes and vulnerabilities, assessing their potential security impact.
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 analysed to determine whether they represent security events.	Establish a systematic approach to monitoring system components for anomalies, analysing potential threats to operational integrity and security.
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.	Develop and maintain procedures to evaluate security events, promptly addressing any incidents that threaten the achievement of control objectives.
CC7.4 The entity responds to identified security incidents by executing a defined incident response programme to understand, contain, remediate and communicate security incidents as appropriate.	Implement a structured incident response program to effectively manage, remediate, and communicate security incidents.

CC7.5 The entity identifies, develops and implements activities to recover from identified security incidents.	Formulate and implement recovery activities to ensure timely restoration of operations following a security incident.
CC8.1 The entity authorises, designs, develops or acquires, configures, documents, tests, approves and implements changes to infrastructure, data, software and procedures to meet its objectives.	Establish comprehensive change management protocols for the authorisation, design, testing, and implementation of changes to meet organisational objectives.
CC9.1 The entity identifies, selects and develops risk mitigation activities for risks arising from potential business disruptions.	Identify and develop effective risk mitigation strategies to ensure continuity and resilience in the face of potential business disruptions.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.	Implement thorough risk assessment and management processes for vendor and business partner relationships to maintain organisational security.
A1.1 The entity maintains, monitors and evaluates current processing capacity and use of system components (infrastructure, data and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Conduct regular evaluations of current processing capacity and system component usage to efficiently manage demand and ensure scalability.
A1.2 The entity authorises, designs, develops or acquires, implements, operates, approves, maintains and monitors environmental protections, software, data backup processes and recovery infrastructure to meet its objectives.	Establish and maintain robust environmental protections, backup processes, and recovery infrastructures to ensure operational continuity.
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Regularly validate recovery plan procedures to ensure effective system restoration and continuity in the event of a disruption.

Subservice organisations' compliance with Maersk's security requirements are assessed on an annual basis as part of the third-party and vendor systems review, either through attestation reports or independent assessments based on Maersk's vendor management process.

Complementary User Entity Controls

The design of the integrated transport and logistics IT services was made under the assumption that certain controls are in operation within user entity organisations. This section identifies customer responsibilities considered in developing the controls in this report. Customers must evaluate their controls to ensure the listed minimum controls are in place. This list is not exhaustive regarding the security, confidentiality, and availability assertions of the customer's control environment in this audit's scope.

Applicable Trust Services Criteria	Complementary User Entity Controls
CC2.3	Customers are responsible for understanding internal control responsibilities and ensuring their team is informed about relevant policies to support these controls.
CC6.2	Customers are responsible for implementing logical and physical access controls to prevent unauthorized access based on user roles and responsibilities.
CC6.3	Customers are responsible for authorising, modifying, or removing user access based on roles and responsibilities while adhering to least privilege and segregation of duties principles.
CC6.4	Customers are responsible for implementing measures to restrict physical access to facilities and sensitive locations, ensuring only authorised personnel have access.
CC6.8	Customers are responsible for implementing controls to prevent, detect, and respond to unauthorised or malicious software within their systems.
CC7.1	Customers are responsible for using detection and monitoring procedures to identify changes to configurations that introduce new vulnerabilities and susceptibilities to newly discovered vulnerabilities.
CC7.3	Customers are responsible for establishing processes for timely detection and reporting of deviations in security operations to ensure quick remediation and compliance with security protocols.
CC7.4	Customers are responsible for ensuring they have adequate incident response capabilities to address and mitigate the impact of security incidents affecting their data or systems.
CC7.5	Customers are responsible for identifying, developing, and implementing activities to recover from identified security incidents.
A1.2	Customers are responsible for implementing and maintaining environmental protections, software, data backup processes, and recovery infrastructure to support business objectives.
A1.3	Customers are responsible for testing recovery plan procedures to ensure effective system recovery and alignment with their objectives.

4 Principal Service Commitments and System Requirements

Maersk’s principal service commitments are foundational to our strategy as a global integrator of container logistics. These commitments are defined through customer agreements, internal policies, and alignment with industry standards, ensuring that we consistently fulfill our promise of trusted and reliable services.

Security

Maersk commits to securing customer data and complying with relevant legal and regulatory requirements. These commitments are addressed through measures such as data encryption, robust authentication mechanisms, physical security controls, and continuous security monitoring.

Availability

Maersk has made commitments related to high availability and reliability of its logistics services, including maintaining operational continuity through system redundancies and failover protocols.

Confidentiality

Maersk commits to maintaining the confidentiality of customer data through data classification policies, encryption, access controls, and regular audits.

System Requirements

Maersk has established operational requirements that support the achievement of service commitments, compliance with relevant laws and regulations, and other system requirements. These include but are not limited to:

- **Information Security Policies:** These policies outline an organisation-wide approach to protecting systems and data. They encompass how services are designed, developed, and managed, as well as employee training protocols.
- **Standard Operating Procedures:** Documented procedures guide specific manual and automated processes essential for the operation and development of Maersk's logistics services.
- **Data Access and Management:** Procedures ensure that the access, collection, use, and deletion of customer data are in line with service commitments and privacy policies.
- **Third-Party Management:** Policies for controlling and monitoring third-party service providers contributing to Maersk’s logistics services are documented and communicated.
- **System Redundancy:** Services are designed to maintain high availability through redundancy and replication strategies.
- **System Monitoring:** Critical systems are monitored using both third-party and internal tools to maintain availability and performance.
- **Access Controls:** Access to physical and logical assets is restricted to authorized users based on role requirements to mitigate the risk of unauthorised access.
- **Incident Management:** Procedures are established for detecting, escalating, and resolving incidents impacting internal and customer systems.

- **Change Management:** Development of new features and major changes to Maersk's services are conducted in accordance with predefined policies and procedures.
- **Security Incident Response:** Upon becoming aware of a security breach affecting customer data, Maersk will: (1) notify impacted customers, (2) investigate the incident and provide details, and (3) take appropriate steps to mitigate the incident.

Maersk's service commitments and system requirements are designed to ensure that we consistently uphold the standards of Security, Availability, and Confidentiality for our customers. Through strategic integration of technology and robust security measures, Maersk continues to simplify global supply chains, delivering reliable and trusted logistics solutions.