



# Statement of Applicability

ISO/IEC 27001:2022 | Marad B.V.

**VERSION 1.2**

Author: CISO

Release Date: August 13, 2025

Classification: Public

Approved by: Executive Board

ISO Clause	Title	Control	Applicability (Y/N)	Status	Justification / Notes
<b>5. Organizational controls</b>					
5.1	Policies for information security	Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.2	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.4	Management responsibilities	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.

5.5	Contact with authorities	The organization shall establish and maintain contact with relevant authorities.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.6	Contact with special interest groups	The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.7	Threat intelligence	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.8	Information security in project management	Information security shall be integrated into project management.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.10	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.

5.11	Return of assets	Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.12	Classification of information	Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.13	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.14	Information transfer	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.15	Access control	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.

		business and information security requirements.			
5.16	Identity management	The full life cycle of identities shall be managed.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.17	Authentication information	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.18	Access rights	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.19	Information security in supplier relationships	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.

5.20	Addressing information security within supplier agreements	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.21	Managing information security in the information and communication technology (ICT) supply chain	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.22	Monitoring, review and change management of supplier services	The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.23	Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.24	Information security incident management planning and preparation	The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.

5.25	Assessment and decision on information security events	The organization shall assess information security events and decide if they are to be categorized as information security incidents.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.26	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.27	Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.28	Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.29	Information security during disruption	The organization shall plan how to maintain information security at an appropriate level during disruption.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.30	ICT readiness for business continuity	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.

5.31	Legal, statutory, regulatory and contractual agreements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.32	Intellectual property rights	The organization shall implement appropriate procedures to protect intellectual property rights.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.33	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.34	Privacy and protection of personal identifiable information (PII)	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Y	Implemented	This control is applicable due to Marad's obligation to comply with applicable data protection laws and regulations, including the EU General Data Protection Regulation (GDPR) and Dutch privacy legislation. Marad processes limited volumes of PII and has implemented appropriate technical and organizational measures to ensure its confidentiality, integrity, and lawful handling. Contractual requirements and internal policies govern the collection, storage, and transfer of PII to ensure compliance and reduce privacy-related risks.

5.35	Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.36	Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
5.37	Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
<b>6. People controls</b>					
6.1	Screening	Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.

6.2	Terms and conditions of employment	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
6.3	Information security awareness, education and training	Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
6.4	Disciplinary process	A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
6.5	Responsibilities after termination of change of employment	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.

6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
6.7	Remote working	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
6.8	Information security event reporting	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
<b>7. Physical controls</b>					
7.1	Physical security perimeters	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	Y	Implemented	Applicable to Marad's office premises. Not applicable to cloud infrastructure, as physical security perimeters are managed by Microsoft and Leaseweb under contractual and certified agreements.

7.2	Physical entry	Secure areas shall be protected by appropriate entry controls and access points.	Y	Implemented	Applicable to Marad's office premises. Not applicable to cloud infrastructure, as physical security perimeters are managed by Microsoft and Leaseweb under contractual and certified agreements.
7.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and implemented.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
7.4	Physical security monitoring	Premises shall be continuously monitored for unauthorized physical access.	Y	Implemented	Applicable to Marad's office premises. Not applicable to cloud infrastructure, as physical security perimeters are managed by Microsoft and Leaseweb under contractual and certified agreements.
7.5	Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	Y	Implemented	Applicable to Marad's office premises. Not applicable to cloud infrastructure, as physical security perimeters are managed by Microsoft and Leaseweb under contractual and certified agreements.
7.6	Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	Y	Implemented	This control is applicable to cloud-hosted infrastructure. All secure area requirements (including access restrictions and monitoring) are implemented and managed by Microsoft and Leaseweb under ISO 27001-certified and SOC-audited procedures. Marad does not operate or manage any secure areas internally.
7.7	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate

		information processing facilities shall be defined and appropriately enforced.			risks identified as a result of risk assessment.
7.8	Equipment siting and protection	Equipment shall be sited securely and protected.	Y	Implemented	Applicable to Marad's office premises. Not applicable to cloud infrastructure, as physical security perimeters are managed by Microsoft and Leaseweb under contractual and certified agreements.
7.9	Security of assets off-premises	Off-site assets shall be protected.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
7.10	Storage media	Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
7.11	Supporting utilities	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Y	Implemented	Marad's information processing relies on cloud-hosted infrastructure managed by Microsoft and Leaseweb. Supporting utilities, including power and cooling, are provided and maintained by these service providers in accordance with ISO 27001 and SOC 2 certified controls. Marad does not own or operate any data centers.

7.12	Cabling security	Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	Y	Implemented	Applicable to Marad's office equipment. Not applicable to cloud infrastructure, as physical security perimeters are managed by Microsoft and Leaseweb under contractual and certified agreements.
7.13	Equipment maintenance	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	Y	Implemented	Applicable to Marad's office equipment. Not applicable to cloud infrastructure, as physical security perimeters are managed by Microsoft and Leaseweb under contractual and certified agreements.
7.14	Secure disposal or re-use of equipment	Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Y	Implemented	Applicable to Marad's office equipment. Not applicable to cloud infrastructure, as physical security perimeters are managed by Microsoft and Leaseweb under contractual and certified agreements.
<b>8. Technological controls</b>					
8.1	User end point devices	Information stored on, processed by or accessible via user end point devices shall be protected.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.2	Privileged access rights	The allocation and use of privileged access rights shall be restricted and managed.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.

8.3	Information access restriction	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.4	Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.5	Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.6	Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.7	Protection against malware	Protection against malware shall be implemented and supported by appropriate user awareness.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.

		vulnerabilities shall be evaluated and appropriate measures shall be taken.			
8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.10	Information deletion	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.11	Data masking	Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.12	Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.

8.13	Information backup	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.14	Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.15	Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.16	Monitoring activities	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.17	Clock synchronization	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.18	Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.

8.19	Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.20	Networks security	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.21	Security of network services	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.22	Segregation of networks	Groups of information services, users and information systems shall be segregated in the organization's networks.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.23	Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.

8.25	Secure development life cycle	Rules for the secure development of software and systems shall be established and applied.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.26	Application security requirements	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	Y	Implemented	Information security requirements are integrated into the development lifecycle to ensure systems meet defined confidentiality, integrity, and availability standards.
8.27	Secure system architecture and engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.28	Secure coding	Secure coding principles shall be applied to software development.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.29	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.30	Outsourced development	The organization shall direct, monitor and review the activities related to outsourced system development.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.

8.31	Separation of development, test and production environments	Development, testing and production environments shall be separated and secured.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.32	Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.33	Test information	Test information shall be appropriately selected, protected and managed.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.
8.34	Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	Y	Implemented	Controls were deemed applicable due to Marad's strategic business objectives and internal control implementations to mitigate risks identified as a result of risk assessment.