MARINE INFORMATION SOLUTIONS LTD

YEAR 2 ISO 27001:2022 AUDIT REPORT

Client Name (As per the Certificate):	**Marine Information Solutions Ltd**
Certificate Scope:	**The Provision of Innovative Marine Assurance Software Products**
SOA Date and Version Number:	**Version: 2.2** **Date: 1st August 2025**
Certificate Expiry Date:	**8th October 2027**
Certificate Number:	**ISM7799351**
Certification Date:	**19th August 2020**
Next Audit Due:	**November 2026**

Audit Date(s):		**24th November 2025**	
Time Started:	**9:30**	**Time Left Client:**	**13:45**
Business Contact Name:		**Steve Campbell**	
Business Contact Details:		**Tel: 0121 277 4900** **Email: steve.campbell@mismarine.com**	
Address for Site of Audit:		**Barnett Waddingham** **3 Devon Way** **Birmingham** **B31 2TS**	
Auditor Name(s):		**Chris Sheppard**	

I confirm that the information in this report is correct and I am happy with the content and conduct of the work carried out and the findings recorded by my appointed Auditor.			
Client Lead:	**Steve Campbell**	**Signed:**	Steve Campbell Steve Campbell (Nov 25, 2025 12:02:04 GMT)
Position:	**IMS Manager**	**Dated:**	Nov 25, 2025

Notes:	Marine Information Solutions Ltd have a fully robust Information Security Management System, which meets all of the requirements of ISO27001:2022. There were zero non-conformances raised during this audit with 1 observation noted.

Auditor's Recommendation:

1 **~~PASS~~**	PASS with Rectification at Next Annual Audit	Probationary PASS with Rectification and Re-inspection within 6 months	Certificate Suspension Subject to Re-inspection within 3 months	FAIL

INTRODUCTION:

This document has been prepared for you in order to establish your level of compliance against the ISO/IEC 27001:2022 Standard. The body of the audit report will contain questions that your auditor will have asked during their visit along with the findings as a result. The identified non-conformances and observations are summarised in the "Report Summary" at the end of this document.

METHOD OF AUDIT:

This audit was conducted remotely, therefore certain assumptions may have been made.

An initial meeting took place with the management representative to confirm the scope and boundaries of your certification and discuss any changes to the Information security Management System.

A full analysis of a selection of your operating processes took place against the requirements of the ISO/IEC 27001:2022 Standard to prepare this Audit Report, detailing all areas of compliance and non-compliance. This has been obtained through interview, witnessed evidence, sample auditing and site tour.

NB: It may not be possible to identify all existing non-conformances within the organisation as we carry out sample audits.

Based on the auditor's findings, this report has been compiled at the conclusion of the audit and your auditor will have discussed the actions you must address in order to maintain your certification.

AUDIT SUMMARY:

Grade 1 Pass (Full Pass):

Marine Information Solutions Ltd has a fully effective management system that meets all of the requirements.

ISO/IEC 27001:2022 AUDIT REPORT

REPORT LEGEND:

PASS	**Your Organisation meets the requirements of this section**
N/A	**This section is currently not applicable to your Organisation**
OBS	**Observation**
MINOR	**Minor non-conformance**
MAJOR	**Major non-conformance**

CATEGORISATION OF MAJOR AND MINOR NON-CONFORMANCES AND OBSERVATIONS FOR IMPROVEMENT

Major Non-conformance – Where you have not complied with a whole clause or sub-clause of the Standard OR the non-conformance has the potential to have a major impact on the organisation. Examples of a Major Non-conformance include no evidence of Management Review, no evidence of any actions to address risk etc.

Minor Non-conformance – Where you do not meet some requirements of a whole clause or sub-clause of the Standard but do meet others. Examples of a minor non-conformance could include carrying out the management reviews but not covering all of the review inputs or you have addressed risk and opportunities but not evaluated the effectiveness of the actions taken.

Observations for Improvement – These are areas where your auditor has identified an area of possible improvement within your management system. You should consider these items (usually as part of your management review process) and record your decision as to whether you wish to address such actions.

REPORT BODY

PROCESS NAME: CONTEXT OF THE ORGANISATION

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
1.	4.1	Has the Organisation determined external and internal Versions that could affect its ISMS and its ability to achieve compliance to their ISMS and the ISO 27001:2022 Standard?	P	Interview with top management confirmed that external and internal Versions have been determined, reviewed and documented into the Scope document. *Document Evidenced:* *Scope Document* • *Ref: MIS_002* • *Version: 4.1* • *Reviewed: 1st August 2025*	N/A
2.	4.1	Has the organisation determined whether climate change is a relevant Version?	P	The impact of climate change is not considered, to be a significant factor, relative to the organisations business activities.	N/A
3.	4.2	Has the organisation determined and reviewed: a) the interested parties that are relevant to the information security management system (ISMS); b) the requirements of these interested parties that are relevant to the ISMS?	P	The needs and expectations of all interested parties have been determined, reviewed and documented into the Scope Document.	N/A
4.	4.3	Has the organisation determined and documented the scope of its information security management system, including:- a) the external and internal Version referred to in 4.1; b) the requirements referred to in 4.2; c) interfaces and dependencies between activities performed by the organisation and those that are performed by other organisations?	P	The Scope document includes the relevant external and internal issues, needs and expectations of interested parties. Interfaces and dependencies between activities performed by the organisation and those that are performed by other organisations, are referenced in the Scope document.	N/A

REPORT BODY

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
5.	4.4	Has the management system been established, implemented, maintained and continually improved?	P	The Information Security Management System (ISMS) has been fully established, implemented, maintained and improved.	N/A

REPORT BODY

PROCESS NAME: LEADERSHIP

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
1.	5.1	Has top management demonstrated leadership and commitment with respect to the information security management system by: • ensuring that the information security policy and objectives are established and are compatible with the strategic direction of the organisation; • ensuring the integration of the ISMS requirements into the organisation's processes; • ensuring resources needed for the ISMS are available; • communicating the importance of effective information security management and of conforming to the ISMS requirements; • ensuring that the ISMS achieves its intended results; • directing and supporting persons to contribute to the effectiveness of the ISMS; • promoting improvement; and • supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility?	P	Top management have ensured that the Information Security Management System has been fully established and implemented. They have communicated throughout the organisation their commitment and expectations regarding the system. All of the required resources have been made available in order to implement the management system. The organisation has established Information Security Objectives & an Information Security Policy, based on the strategic direction of the Organisation. Risk Management & elements of information security, have been implemented into the processes of the organisation. The organisation has ensured that adequate resource is available in order to manage the ISMS. The principles of the Information Security Policy have been communicated to all employees and other interested parties. All employees are aware of the potential consequences of departure from specified operating procedures. The organisation has ensured that control methods are in place to achieve the intended outcomes of the ISMS, through the establishment of policies. The organisation has ensured that people are encouraged to contribute to the ISMS through risk assessment & risk treatment. Top management promote continual improvement by establishing and implementing improvement actions at management review.	N/A

REPORT BODY

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
2.	5.2	Has top management established, implemented and maintained an Information Security Policy that: • Is appropriate to the purpose of the organisation; • Includes ISMS objectives or provides a framework for setting them; • Includes a commitment to satisfy requirements of the ISMS; • Includes a commitment to continual improvement; • Is documented; • Communicated within the organisation; • Available to interested parties, as appropriate?	P	An Information Security Policy has been established and meets all of the content requirements stated in this clause. *Document evidenced:* *Information Security Policy* • *Ref: MIS_018* • *Version: 2.2* • *Reviewed: 1st August 2025*	N/A
3.	5.3	Have responsibilities and authorities for roles been assigned, communicated and understood?	P	All staff are fully aware of the management structure and the relevant roles of individual members of staff. Responsibilities and authorities for the roles within the business are communicated appropriately. Roles & Responsibilities are documented within the Organisation Chart. *Document evidenced:* *Organisation Chart* • *Ref: MIS_011* • *Version: 1.5* • *Reviewed: 1st August 2025*	N/A
4.	5.3	Has top management assigned the responsibility and authority for: • ensuring that the ISMS conforms to the requirements of the ISO 27001 Standard; • reporting on the performance of the ISMS to top management?	P	Steve Campbell has been assigned the role of IMS Manager having responsibility for ensuring compliance with the ISMS, ISO27001:2022 & for reporting on the performance of the management system.	N/A

REPORT BODY

PROCESS NAME: PLANNING

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
1.	6.1.1	Has the organisation considered the Versions in 4.1 and the requirements in 4.2 and determined the risks and opportunities that need to be addressed to: • give assurance that the ISMS can achieve its intended result(s); • prevent, or reduce, undesired effects; • achieve improvement?	P	A Master Risk Register has been established & is reviewed on a regular basis, or as & when there are changes made. Actions to address risks and opportunities have been documented onto the Master Risk Register , which demonstrates compliance with all elements of this clause. *Document Evidenced* *Master Risk Register* • *Ref: MIS_007* • *Version: 2.1* • *Reviewed: 1st August 2025*	N/A
2.	6.1.1	Has the organisation planned: • actions to address these risks and opportunities; • how to: - integrate and implement the actions into its ISMS processes (see 4.4); - evaluate the effectiveness of these actions?	P	Actions to address risk have been implemented into working practice through training and where necessary written into documented procedures. The effectiveness of the treatment plans is measured & monitored through the review of the Master Risk Register	N/A

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
3.	6.1.2	Has the organisation defined, documented and applied an information security risk assessment process that: a) establishes and maintains information security risk criteria that including: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments; b) ensures that repeated information security risk assessments produce consistent, valid and comparable results; c) identifies the information security risks: 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and 2) identify the risk owners; d) analyses the information security risks: 1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialise; 2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and 3) determine the levels of risk; e) evaluates the information security risks: 1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and 2) prioritise the analysed risks for risk treatment?	P	Risk analysis, risk acceptance criteria and methods for performing risk assessment have been documented within the Master Risk Register. Risk assessments undertaken have been consistent, valid and comparable to the previous risk assessments. The results of risk assessments appear on the Master Risk Register; these were evidenced during this audit & were found to be in good order. Risk assessments have covered loss of confidentiality, integrity and availability of information. The risk assessments undertaken by the organisation have addressed potential consequences, likelihood and severity if the event that they materialise. Risk treatment has been prioritised based on the severity of the risk. Risk Assessments have been documented as was evidenced during this audit, along with treatment plans. The results of risk assessments have been added to the Master Risk Register.	N/A

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
4.	6.1.3	Has the organisation defined, documented and applied an information security risk treatment process to: a) select appropriate information security risk treatment options, taking account of the risk assessment results; b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen; c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted; d) produce a Statement of Applicability that contains: - the necessary controls (see 6.1.3 b) and c)); - justification for their inclusion; - whether the necessary controls are implemented or not; and - the justification for excluding any of the Annex A controls. e) formulate an information security Master Risk Register ; and f) obtain risk owners' approval of the information security Master Risk Register and acceptance of the residual information security risks?	P	Risk Treatment has been defined within the Master Risk Register and applied in line with the planned actions. A Statement of Applicability has been documented, , which determines the applicable clauses & justifications for those that do not apply. Risk treatment is documented within the Master Risk Register; residual risks have been calculated. Risk owners have reviewed & approved the risks. *Document evidenced:* *Statement of Applicability* • *Ref: MIS_001* • *Version: 2.2* • *Reviewed: 1st August 2025*	N/A

REPORT BODY

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
5.	6.2	Has the organisation established and documented ISMS objectives at relevant functions and levels that are; • Consistent with the ISMS policy; • Measurable (if practicable); • Take into account ISMS requirements and results of risk assessment results and risk treatment; • Monitored; • Communicated; • Updated as appropriate?	P	ISMS objectives have been established & documented within the Quality and Security Objectives document. The objectives were evidenced during this audit & were found to be compliant with all elements of this clause. *Document Evidenced* *Information Security & Business Objectives* • *Ref: MIS_003* • *Version: 3.1* • *Reviewed: 1st August 2025*	N/A
6.	6.2	Has a plan to achieve these objectives been formulated that determines; • What will be done; • The resources required; • Who will be responsible • Time scales for completion • How the results will be evaluated?	P	Plans as to how the specified objectives are to be met are documented within the Information Security & Business Objectives document & demonstrate compliance with all requirements of this clause.	N/A
7.	6.3	When changes to the ISMS are required, have the changes been carried out in a planned manner?	N/A	There have been no major changes that could impact on the effectiveness of the ISMS during the current audit period.	N/A

PROCESS NAME: SUPPORT

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
1.	7.1	Has the organisation determined and provided resources necessary for the establishment, implementation, maintenance and continual improvement of the ISMS?	P	Human and physical resource has been provided as required for the establishment and implementation of the ISMS. Staffing levels are reviewed periodically to ensure adequacy.	N/A
2.	7.2	Has the organisation: a) determined the necessary competence of person(s) doing work under its control that affects its information security performance; b) ensured that these persons are competent on the basis of appropriate education, training, or experience; c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and d) retain appropriate documented information as evidence of competence?	P	The organisation have determined the competence of all employees, with each member of staff being provided with sufficient training, where appropriate, in order for them to carry out their activities. The necessary competences required in order to fulfil job requirements are also defined within job descriptions. Information Security is a key topic & forms part of the induction process. Where it is deemed further training is required, the organisation will provide it. Evidence of Staff Security Awareness was evidenced during this audit & further demonstrates the organisations commitment to raising awareness. *Documents Evidenced* *Job Descriptions:* • *Infrastructure Engineer* • *Senior Business Analyst* *Training Matrix* • *Ref: MIS_016* • *Version: 1.4* • *Reviewed: 1st August 2025* *Job Requirements & Skills* • *Ref: MIS_015* • *Version: 1.3* • *Reviewed: 1st August 2025*	N/A

REPORT BODY

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
3.	7.3	Are persons doing work under the organisations control aware of; • the ISMS Policy; • their contribution to the effectiveness of the ISMS including the benefits of improved ISMS performance; • the implications of not conforming with the ISMS requirements?	P	The Information Security Policy is available to all staff and staff are made aware of their contribution to the ISMS through the induction process and regular discussions during risk treatment.	N/A
4.	7.4	In relation to internal and external communication relevant to the ISMS, has the organisation determined; • what to communicate; • when to communicate; • with whom to communicate; • how to communicate?	P	Internal communications are carried out to convey the results of management review and audits, performance against objectives and any applicable corrective actions. External communication regarding the results of any corrective actions as they apply to interested parties has also been carried out. The following evidence of communication was provided during this audit & demonstrates compliance with the requirements of this clause: • *Communication to staff about ISMS changes & current policies* • *Meeting minutes discussing ISMS changes*	N/A
5.	7.5.1	Does the organisation's ISMS include: • documented information required by the ISO 27001 Standard; • documented information determined to be necessary for the effectiveness of the ISMS?	P	All documentation pertaining to the ISMS is in place & meets all the requirements required by the Standard. All other documents required for the effective implementation of the ISMS are in place.	N/A

REPORT BODY

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
6.	7.5.2	Has the organisation ensured all documents are; • identifiable and descriptive (e.g., title, date, author, reference etc) • appropriately formatted for use (e.g., language, software version, paper, electronic etc) • reviewed and approved for suitability and adequacy?	P	All documents and records viewed at this audit were suitably identified through the document; Documents are in electronic format & all documents have been reviewed for suitability by the Information Security Manager. Controls have been applied to all documented information at document level, each containing the following information: • *Issue Date* • *Review Date* • *Version* • *Scope* • *Associated Documentation* • *Review & Consultation Process* • *Responsibility for Implementation & Training* • *Information Classification* • *Retention*	N/A
7.	7.5.3	Has the documented information required by the information security management system and by the ISO 27001 Standard been controlled to ensure: • it is available and suitable for use, where and when it is needed; • it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity); • correct distribution, access, retrieval and use; • appropriate storage and preservation, including preservation of legibility; • control of changes (e.g. version control); • suitable retention and disposal?	P	All documents are available at the point of use; this was demonstrated through the documents viewed during this audit. Documented information is controlled through permission settings to SharePoint, restricting editable access only to those who are authorised.	N/A

REPORT BODY

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
8.	7.5.3	Has documented information of external origin, necessary for the planning and operation of the information security management system, been identified as appropriate, and been controlled?	P	Documents of external origin have been identified and regularly updated to ensure that the latest version is the most up to date.	N/A
9.	7.5.3	Are documents of external origin, necessary to form part of the planning and operation of the ISMS, identified and controlled as appropriate?	P	Documents of external origin necessary to form part of the planning and operation of the ISMS, are identified and controlled as appropriate.	N/A

REPORT BODY

PROCESS NAME: OPERATION

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
1.	8.1	Has the organisation planned, implemented and controlled the processes needed to meet requirements, and to implement the actions determined in Clause 6, by: - establishing criteria for the processes; - implementing control of the processes in accordance with the criteria?	P	All actions planned as a result of the risk assessment process have been implemented and controlled. Work processes have been adopted, controlled and reviewed to ensure that they meet the ISMS requirements. The organisations approach to risk management is defined within the Master Risk Register, as referenced in section 6.1.2 of this report.	N/A
2.	8.1	Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.?	P	Records have been established to demonstrate that processes have been carried out as planned.	N/A
3.	8.1	Has the organisation controlled planned changes and reviewed the consequences of unintentional changes, as well as taking action to mitigate any adverse effects of unintentional change?	P	Planned and unplanned changes are reviewed at Management Review to ensure that there is no adverse impact on the ISMS.	N/A
4.	8.1	Has the organisation ensured that any externally provided processes, products or services are determined and controlled?	P	Purchased products or services are carried out by those who have been approved as part of the organisations supplier approval process. The criteria for this approval have been recorded. Ongoing review of these suppliers takes place on a regular basis or as required.	N/A
5.	8.2	Has the organisation performed and documented information security risk assessments at planned intervals and when significant changes occur?	P	ISMS risks assessments have been performed at regular intervals and when significant changes occur. These were viewed as part of the Master Risk Register , as evidenced during this audit.	N/A
6.	8.3	Has the organisation implemented the documented security risk treatment plan?	P	Security risk treatment plans, as defined within the Master Risk Register have been fully implemented and evidence of this was viewed at this assessment.	N/A

REPORT BODY

PROCESS NAME: PERFORMANCE EVALUATION

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
1.	9.1	Has the organisation evaluated and documented the performance of the ISMS by determining; • what is to be monitored and measured, including processes and controls • the method for monitoring, measurement, analysis and evaluation to ensure valid results • when monitoring and measurement should be performed • who shall carry out monitoring and measurement; • when results should be analysed and evaluated • who is responsible for analysis and evaluation?	P	The organisation has monitored and measured their performance against the Master Risk Register, Information Security Objectives and the Statement of Applicability. Additionally, internal audits & management reviews are indicative of compliance with this clause.	N/A
2.	9.1	Has the organisation evaluated the information security performance and the effectiveness of the information security management system?	P	The evaluation of performance and effectiveness of the ISMS has been carried out as part of the management review and internal audit process.	N/A
3.	9.2	Has the organisation conducted internal audits at planned intervals to provide information on whether the information security management system: • conforms to: - the organisation's own requirements for its information security management system; - the requirements of the ISO 27001 Standard; • is effectively implemented and maintained?	P	The organisation conducts internal audits, which covers internal procedures, all of the clauses within ISO27001:2022 & the Statement of Applicability	N/A

REPORT BODY

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE

4.	9.2	Has the organisation:
		• planned, established, implemented and maintained an audit programme(s) including the frequency, methods, responsibilities, planning requirements and reporting, which take into consideration the importance of the processes concerned, changes affecting the organisation, and the results of previous audits;
		• defined the audit criteria and scope for each audit;
		• selected auditors and conducted audits to ensure objectivity and the impartiality of the audit process;
		• ensured that the results of the audits are reported to relevant management?
			P	The organisation has planned, established, implemented and maintained the internal audit schedule, as referenced in section 9.2, (3), of this report. The audit criteria and scope for each audit is defined within each report; auditors are independent of the process being audited. The results of internal audits are provided as input into management reviews.
				
				Documents Evidenced
				Internal Audit Reports
				• *Annex A – 5.0 Organisational Controls*
				  ⚓ *Clauses 5.1 – 5.37*
				  ⚓ *Date: November 2024*
				• *Annex A – 6.0 People Controls*
				  ⚓ *Clauses 6.1 – 6.8*
				  ⚓ *Date: December 2024*
				• *Context of the Organisation*
				  ⚓ *Clauses 4.1 – 4.4*
				  ⚓ *Date: March 2025*
				• *Leadership*
				  ⚓ *Clauses 5.1 – 5.3*
				  ⚓ *Date: April 2025*
				• *Planning*
				  ⚓ *Clauses 6.1 – 6.3*
				  ⚓ *Date: May 2025*
				• *Support*
				  ⚓ *Clauses 7.1 – 7.5*
				  ⚓ *Date: June 2025*
				• *Operation*
				  ⚓ *Clauses 8.1 – 8.3*
				  ⚓ *Date: July 2025*
				• *Performance Evaluation*
				  ⚓ *Clauses 9.1 – 9.3*
				  ⚓ *Date: August 2025*
					N/A

REPORT BODY

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
5.	9.3	Has top management reviewed the organisation's information security management system, at planned intervals, to ensure its continuing suitability, adequacy, effectiveness and alignment with the strategic direction of the organisation, taking into consideration:- • the status of actions from previous management reviews; • changes in external and internal Versions that are relevant to the ISMS; • changes in the needs and expectations of interested parties; • information on the performance and effectiveness of the ISMS, including trends in: 1) nonconformities and corrective actions; 2) monitoring and measurement results 3) audit results 4) the extent to which information security objectives have been met; • feedback from relevant interested parties; • results of risk assessment and status of the Master Risk Register ; • opportunities for continual improvement?	P	Management review of the Information Security management system has been carried out and addresses all of the input requirements stated in this clause. Management review was carried out on the 23rd July 2025; the meeting minutes were evidenced & meet all of the requirements of this clause.	N/A
6.	9.3	Do the results of the management review include decisions related to continual improvement opportunities and any needs for changes to the information security management system and have they been documented?	P	The results of management review have been documented onto the management review minutes and include actions to demonstrate improvement.	N/A

REPORT BODY

PROCESS NAME: IMPROVEMENT

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
1.	10.1	Has the organisation continually improved the suitability, adequacy and effectiveness of the ISMS?	P	Continual improvement has been evidenced by way of implementation of the management review, internal audit, corrective action and risk treatment processes.	N/A
2.	10.2	When a nonconformity occurs, including any arising from complaints, has the organisation: • reacted to the nonconformity and, as applicable: - take action to control and correct it; - deal with the consequences; • evaluated the need for action to eliminate the cause(s) of the nonconformity, in order that it does not recur or occur elsewhere, by: - reviewing and analysing the nonconformity; - determining the causes of the nonconformity; - determining if similar nonconformities exist, or could potentially occur; • implemented any action needed; • reviewed the effectiveness of any corrective action taken; • made changes to the ISMS, if necessary; • ensured that corrective actions are appropriate to the effects of the nonconformities encountered • retained records of the nature of the nonconformities and results of any correction action implemented?	P	A process has been established for the identification and investigation of non-conformance against the requirements of the organisations information security management system or ISO 27001:2022. Root cause analysis of the source of the problem will be carried out and actions instigated to correct the initial problem then to establish corrective action to attempt to prevent recurrence of the non-conformance. *Document Evidenced* *Non-Conformance Register* • *Ref: MIS_008* • *Version: 1.3* • *Reviewed: 1st August 2025* The following non-conformances were evidenced: ***NC50061*** ***Date:*** *18th August 2025* ***Details:*** *Post-it note with password found on desk* ***Severity Level:*** *Major* ***Corrective Action (CA40061):*** *Staff reminded of clear desk policy and all ISMS.* ***NC50056*** ***Date:*** *14th June 2025* ***Details:*** *Staff member attempted to work from a different country without permission* ***Severity Level:*** *Major* ***Corrective Action (CA40060):*** *Staff discipline as action was unauthorised. Staff training for all staff.*	N/A

REPORT BODY

PROCESS NAME: STATEMENT OF APPLICABILITY

Clause 6.0 People Controls

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
1.	SOA 6.1	Have background verification checks been carried out on all candidates to become personnel prior to joining the organisation and on an ongoing basis taking into consideration applicable laws, regulations and ethics and is this proportional to the business requirements, the classification of the information to be accessed and the perceived risks?	P	The organisation conducts background verification checks on all new personnel prior to joining the organisation, taking into consideration applicable laws, regulations and ethics. These checks appear to be proportional to the business requirements, the classification of the information to be accessed and the perceived risks	N/A
2.	SOA 6.2	Do employment contractual agreements state the personnel's and the organisation's responsibilities for information security?	P	All new staff must sign a contract & terms of employment and abide by the staff handbook. They are inducted into the organisations Information Security documentation as noted within the New Starter Induction Checklist. *Documents Evidenced* *New Starter Induction Checklist* • *Ref: MIS_013* • *Version: 2.2* • *Reviewed: 1st August 2025* *Staff Handbook* • *Ref: MIS_010* • *Version: 1.7* • *Reviewed: 1st August 2025*	N/A
3.	SOA 6.3	Have personnel and relevant interested parties received appropriate information security awareness, education and training and regular updates of the organisation's information security policy, topic-specific policies and procedures, as relevant for their job function?	P	Regular ISMS training is undertaken as part of the Induction Training and also have access to SharePoint at any time to reference policies which are updated as required.	N/A

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
4.	SOA 6.4	Has a disciplinary process been formalised and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation?	P	The organisations disciplinary procedure has been documented, within the Disciplinary Policy & Procedure which is communicated to all staff through the Staff Handbook.	N/A
5.	SOA 6.5	Have information security responsibilities and duties that remain valid after termination or change of employment been defined, enforced and communicated to relevant personnel and other interested parties?	P	The IT Process and Operating Procedures document defines the responsibilities that remain applicable after termination or change of employment. The identity of any leavers will be communicated to interested parties, as required, to process any access revocation activities. Access revocation activities are also defined within the IT Process and Operating Procedures document. *Document Evidenced* *IT Process and Operating Procedures* • *Ref: MIS_017* • *Version: 4.2* • *Reviewed: 1st August 2025*	N/A
6.	SOA 6.6	Have confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information been identified, documented, regularly reviewed and signed by personnel and other relevant interested parties?	P	Confidentiality agreements, (NDA's) are part of the employee contract along with agreements signed with suppliers and customers where appropriate. *Document Evidenced* *Mutual NDA Template* • *Ref: Unknown* • *Version: Unknown* • *Reviewed: Unknown* The Mutual NDA Template is an uncontrolled document.	**OBS 1**
7.	SOA 6.7	Have security measures been implemented when personnel are working remotely to protect information accessed, processed or stored outside the organisation's premises?	P	As defined within the Information Security Policy, (section 15.7)	N/A

REPORT BODY

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
8.	SOA 6.8	Has the organisation provided a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner?	P	Information Security Events are reported in line with the process documented within the Incident Management Procedure, which defines the mechanism that has been established. *Document Evidenced* *Incident Management Procedure* • *Ref: MIS_025* • *Version: 3.6* • *Reviewed: 1st August 2025*	N/A

Clause 7.0 Physical Controls

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
9.	SOA 7.1	Have security perimeters been defined and used to protect areas that contain information and other associated assets?	P	MIS offices are continuously monitored for unauthorised physical access. There are several controls in place to guard against this including CCTV (around the building and all entry/exit points), intruder alarm, and door access controls. The entry is always manned during opening times and anyone entering the premises are questioned and identified.	N/A
10.	SOA 7.2	Have secure areas been protected by appropriate entry controls and access points?	P	Only authorised personnel who have a valid and approved business need are given access to areas containing information systems or stored data. Access to MIS offices and facilities are controlled by physical barriers and an auditable process and procedure.	N/A
11.	SOA 7.3	Has physical security for offices, rooms and facilities been designed and implemented?	P	Physical security elements for offices, rooms and facilities have been designed and implemented	N/A
12.	SOA 7.4	Have premises been continuously monitored for unauthorised physical access?	P	All visitors must report to reception and enter their details in the visitors' book. A temporary visitors pass is given and must be always worn. Visitor must sign-out before leaving the building and hand pass back. As noted in section SOA 7.1; CCTV is installed, covering all entry/exit points.	N/A
13.	SOA 7.5	Has protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure been designed and implemented?	P	Protection against a range of different incidents is covered within the organisations Business Continuity & Disaster Recovery Plan. *Document Evidenced* *BCDR Plan* • *Ref: MIS_023* • *Version: 3.5* • *Reviewed: 1st August 2025*	N/A

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
14.	SOA 7.6	Have security measures for working in secure areas been designed and implemented?	N/A	The organisation have justified an exclusion to this clause	N/A
15.	SOA 7.7	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced?	P	A Clear Desk & Screen Policy has been implemented & documented within the Information Security Policy document, (section 7.0).	N/A
16.	SOA 7.8	Has equipment been sited securely and protected?	N/A	All processing and storage of product and data is conducted within Microsoft Azure. MIS do not self-host any servers or other infrastructure. Only standard office environment conditions are required for device access.	N/A
17.	SOA 7.9	Have off-site assets been protected?	P	Asset management is covered within the Information Security Policy, (section 15.0) & are protected in line with the following rules: • *Each information asset, (hardware, software, application, or data) shall have a named custodian who shall be responsible for the information security of that asset.* • *The asset owner is responsible for keeping that asset safe and in good condition.* • *Each information or physical asset ownership shall be recorded within the MIS asset register.* • *The asset must be kept in a safe place, especially if it being transported around, and must adhere to the lock screen policy and all other polices relating to the asset.* • *The asset must be signed for on receipt (see asset sign-off and return form) and condition noted.* • *Once the asset is returned then this will be checked, and any additional damage will be noted.* • *Under hybrid working arrangements any assets kept at home must adhere to these policies the same as in the office.*	N/A

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
18.	SOA 7.10	Has storage media been managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organisation's classification scheme and handling requirements?	P	A procedure for the management of Removable Media has been implemented, as documented within the Information Security Policy, (section 15.6) & reads as follows: • *Only company provided removable media (such as USB memory sticks and recordable CDs/DVDs) shall be used to store business data and its use shall be recorded (e.g., serial number, date, issued to, returned).* • *Removable media of all types that contain software or data from external sources, or that has been used on external equipment, require the approval of Operations Manager before they may be used on business systems. Such media must be scanned by anti-virus before being used.* • *For confidential or commercial classified data this must be encrypted on the removable media using a method approved by operations.* • *Where indicated by the risk assessment, systems shall be prevented from using removable media.* • *MIS have controls in place to block removable media, no staff should attempt to bypass those controls and should report to operations if those controls are not working.* • *Users breaching these requirements may be subject to disciplinary action.* • *Operations hold a log of all loaned removable media, the person receiving this media is responsible for its safe return to operations, the log will be updated once returned.*	N/A
19.	SOA 7.11	Have information processing facilities been protected from power failures and other disruptions caused by failures in supporting utilities?	P	All data storage and processing is conducted by Microsoft Azure, subject to Cloud Services Supplier Review. The organisations management of cloud services is documented within the Information Security Policy, (section 21.0)	N/A
20.	SOA 7.12	Have cables carrying power, data or supporting information services been protected from interception, interference or damage?	N/A	MIS assumption is that all internet access is insecure, so all network traffic is encrypted. In the event of an incident that interrupts power or networking, BCDR procedures will be executed.	N/A

	Standard Clause(s)	QUESTION	STATUS P-PASS, F-FAIL, n/a	EVIDENCE AUDITED / FINDINGS	NCR TABLE
21.	SOA 7.13	Has equipment been maintained correctly to ensure availability, integrity and confidentiality of information?	P	All equipment has been maintained correctly to ensure availability, integrity and confidentiality of information. This is demonstrated through the information contained within the organisations Asset Register. *Document Evidenced* *Asset Register* • *Ref: MIS_031* • *Version: 1.3* • *Reviewed: 1st August 2025*	N/A
22.	SOA 7.14	Have items of equipment containing storage media been verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use?	P	The organisation have established & implanted a procedure for the Disposal of media within the IT Process and Operating Procedures document, (section 12.0). The established rules are as follows: *'**Device re-use*** *For re-use (i.e. re-distributing a hard drive or complete pc/laptop to another user) then operations will format all drives using an approved method, as part of the setup process. A device should never be given to another user unless it has been fully wiped of all data beforehand.* ***Disposal*** *Physical drives must have a low-level wipe by operations before being disposed of, using approved software. This will be done even if encryption (e.g. BitLocker) is set on that drive. Software used is Easeus Partition Manager.* *Virtual data (e.g. data stored in Azure) – for any data stored by Microsoft, an automated approved method is used for secure data deletion, compliant with National Institute of Standards and Technology Special Publication 800-88 (NIST SP 800-88 Guidelines for Media Sanitization).* *Physical disposal of the media must be done in an environmentally acceptable manner and follow guidance from NCSC. Operations will physically dismantle the device and destroy component parts, then recycle these parts using local council facilities'.*	N/A

REPORT SUMMARY

MAJOR NON-CONFORMANCE SUMMARY

Clause(s)	Nature of Non-conformance	Agreed Actions to Remedy	Responsibility
	NONE		

The items above MUST be rectified in order to retain certification. You will not retain certification unless evidence of the rectification of the non-conformances above are provided to your auditor as part of a reaudit.

MINOR NON-CONFORMANCE SUMMARY

Clause(s)	Nature of Non-conformance	Agreed Actions to Remedy	Responsibility
	NONE		

The items above MUST be rectified prior to your next annual external audit by CQS. If these actions are not completed, the level of non-conformance will be upgraded to a Major Non-Conformance at the next audit. Your grade of pass will depend on you rectifying these points.

OPPORTUNITIES FOR IMPROVEMENT SUMMARY

Clause(s)	Nature of Observation	Agreed Actions to Remedy (if required)	Responsibility
SOA 6.6, 7.5	The Mutual NDA Template is an uncontrolled document.	Add document controls to the Mutual NDA Template.	SC

The items above should be considered prior to your annual external audit by CQS and evidence must be provided.

Marine Information Solutions Ltd - ISO 27001_2022 Year 2 Audit Report 24112025 CS

Final Audit Report 2025-11-25

Created:	2025-11-25
By:	Audits Department (audits@cqsltd.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAA5B_QUjdm4Fx0k6LGQ4baQ60YrRh6tq7W

"Marine Information Solutions Ltd - ISO 27001_2022 Year 2 Audit Report 24112025 CS" History

Document created by Audits Department (audits@cqsltd.com)
2025-11-25 - 9:53:57 AM GMT- IP address: 86.128.79.163

Document emailed to steve.campbell@mismarine.com for signature
2025-11-25 - 9:54:37 AM GMT

Email viewed by steve.campbell@mismarine.com
2025-11-25 - 9:54:42 AM GMT- IP address: 172.186.8.134

Signer steve.campbell@mismarine.com entered name at signing as Steve Campbell
2025-11-25 - 12:02:02 PM GMT- IP address: 94.174.81.99

Document e-signed by Steve Campbell (steve.campbell@mismarine.com)
Signature Date: 2025-11-25 - 12:02:04 PM GMT - Time Source: server- IP address: 94.174.81.99

Agreement completed.
2025-11-25 - 12:02:04 PM GMT