

CHARTING THE FUTURE 

ClassNK

**Guidelines for Cyber Security Management
System for Ships
[Second Edition]
[English]**



ClassNK

Revision History

No.	Date	Category	Details of revision
1.0	April 1, 2019	New	First issue
2.0	October 2, 2026	Amendment	Full revision

Contents

Introduction	1
1 General	1
2 Background	1
3 Structure of the Guidelines	1
4 Definitions	1
PART 1: REQUIREMENTS	3
Chapter 1 Scope and Core Requirements	3
1.1 Purpose of Cyber Security Management	3
1.2 Purpose of the Cyber Security Management System (CSMS)	3
1.3 Compatibility with Relevant Rules, Regulations, Codes, and Guidelines	3
1.4 Application	3
1.5 Elements of a Cyber Security Management System (CSMS)	3
Chapter 2 Leadership and Policy Requirements	5
2.1 Establishment of Cyber Security Policy	5
2.2 Implementation and Maintenance of Cyber Security Policy	5
Chapter 3 Governance and Responsibility Requirements	6
3.1 Roles and Responsibilities	6
3.2 Responsibility of Top Management	6
3.3 Company Cybersecurity Officer	6
3.4 Ship Cybersecurity Officer	6
3.5 Master's Authority	7
Chapter 4 Resource and Competence Requirements	8
4.1 Provision of Resources	8
4.2 Competence Requirements	8
4.3 Training and Awareness	8
Chapter 5 Supply Chain Management Requirements	9
5.1 Requirements for Suppliers	9
5.2 Evaluation of Suppliers	9
Chapter 6 Cyber Risk Assessment Requirements	10
6.1 Role of Cyber Risk Assessment	10
6.2 Scope of the Cyber Risk Assessment	10
6.3 Management of Cyber Risk Assessment Process	10
6.4 Identification and Evaluation of Cyber Risks	10
6.5 Review of Cyber Risk Assessment	11
Chapter 7 Configuration Management Requirements	12
7.1 Configuration Management	12
7.2 Change Management	12
7.3 Configuration Review	12
Chapter 8 Controls	13
8.a Access & Use Control	13
8.a.1 Identity & Authentication Management	13
8.a.2 Authorization & Privilege Management	13
8.a.3 Remote & Third-Party Access Control	13
8.a.4 Acceptable Use & User-Initiated Risks	13

8.b	Network & Communication Security	13
8.b.1	Network Segmentation & Zoning	13
8.b.2	Protection of Communication	13
8.b.3	External Connectivity Management	13
8.c	System Configuration & Maintenance	13
8.c.1	Secure Configuration & Hardening	13
8.c.2	Patch & Update Management	13
8.c.3	Obsolescence Management	13
8.c.4	Malware & Endpoint Protection	13
8.c.5	Hardware & Software Control	13
8.d	Media & Physical Interface Control	13
8.d.1	Removable Media Control	13
8.d.2	Physical Port & Interface Protection	13
8.d.3	Direct Connection Management	13
8.d.4	Physical Access Control	13
8.e	Monitoring, Logging & Detection	13
8.e.1	Event Logging	13
8.e.2	Security Monitoring	13
8.e.3	Log Protection & Retention	13
8.e.4	Log Review & Anomaly Investigation	13
8.f	Backup & Recovery	13
8.f.1	Backup Policy & Implementation	13
8.f.2	Recovery Procedures	13
8.f.3	Verification & Recovery Measures	13
Chapter 9	Emergency Preparedness Requirements	14
9.1	Establishment of Procedures to Respond to Emergency Situations	14
9.2	Establishment of Programs to Respond to Emergency Situations	14
9.3	Provision of Measures Ensuring Response to Emergency Situations	14
Chapter 10	Non-conformity and Corrective Action Requirements	15
10.1	Reporting and Analysis of Non-conformities	15
10.2	Corrective Action and Prevention of Recurrence	15
Chapter 11	Documentation Requirements	16
11.1	Establishment and Maintenance of Document Control Procedures	16
11.2	Cyber Security Management Manual	16
Chapter 12	Verification, Review and Evaluation Requirements	17
12.1	Internal Cyber Security Audit	17
12.2	Evaluation of the Cyber Security Management System	17
PART 2:	ASSESSMENT CRITERIA AND OBJECTIVE EVIDENCE	18

Introduction

1 General

Ship operation has become dependent on digital systems and networks. Cyber risks can therefore directly affect the safety of the ship, the protection of the environment, and the continuity of operations.

Technical measures alone do not manage these risks. They remain effective only within whole management processes that select, maintain, and review them. Under such processes, the Company develops a policy and the organizational structure to execute it, assesses its risks, selects and implements controls, reviews the results, and in parallel, prepares for emergencies. Only such governance, sustaining consistent implementation and continuous improvement, addresses cyber risks effectively.

These Guidelines set out the requirements for a Cyber Security Management System (hereinafter referred to as the "CSMS"). The CSMS provides the governance and management structure through which the Company addresses cyber risks in the operation of its ships. **Chapter 8** additionally sets out the controls applicable to ships and shipboard systems under that management; the selection and scope of those controls follow from the cyber risk assessment under **Chapter 6**.

2 Background

In 2017, the International Maritime Organization adopted Resolution MSC.428(98), which recommended that cyber risks were addressed under the Company's Safety Management System based on the ISM Code. To help stakeholders respond to this recommendation, the Society issued the first edition of these Guidelines in April 2019, setting out a set of CSMS requirements aligned with the framework of the ISM Code.

Since the publication of the first edition, the Society has accumulated knowledge through its audits. Building on this experience, the second edition, issued in 2026, updates the Guidelines with reference to ISO/IEC 27001 and ISO/IEC 27002, standards widely used internationally for managing cyber security within an organization, and clarifies the assessment criteria applied in the Society's audits.

3 Structure of the Guidelines

These Guidelines consist of Part 1 and Part 2. Part 1 sets out the requirements for the CSMS, and each chapter opens with an overview of what that chapter provides. Chapter 8 of Part 1 lists the controls for shipboard IT and OT systems by control domain. Part 2 sets out, for the requirements and controls in Part 1, the assessment criteria applied in the Society's audits and the objective evidence required.

4 Definitions

The following definitions apply to Parts 1 and 2 of this document.

4.1 Cyber Security

"Cyber Security" means the activities performed in the company and onboard the ship to ensure the safety of operation and maintain proper implementation of shipboard operations by protecting equipment, information communication devices, networks, and information related to operation from threats.

4.2 Company

"Company" means the owner of the ship or any other organization or person such as the manager, or the bareboat charterer, who has assumed the responsibility for operation of the ship from the

shipowner and who, on assuming such responsibility, has agreed to take over all the duties and responsibility imposed by the NK-CSMS.

4.3 Administration

"Administration" means the Government of the State whose flag the ship is entitled to fly.

4.4 Cyber Security Management System (CSMS)

"Cyber Security Management System" means a structured and documented management system enabling Company personnel to implement effectively the Company cyber security policy.

4.5 Cyber Security Management Certificate

"Cyber Security Management Certificate" means a document issued to a ship which signifies that the Company and its shipboard management operate in accordance with the approved CSMS.

4.6 Objective Evidence

"Objective Evidence" means quantitative or qualitative information, records or statements of fact pertaining of cyber security or to the existence and implementation of a CSMS element, which is based on observation, measurement or test and which can be verified.

4.7 Non-Conformity

"Non-conformity" means an observed situation where objective evidence indicates the non-fulfillment of a specified requirement.

4.8 Major Non-Conformity

"Major non-conformity" means an identifiable deviation that poses a serious threat to the cyber security of personnel or the ship or a serious risk to the environment that requires immediate corrective action or the lack of effective and systematic implementation of a control of the CSMS.

4.9 Convention

"Convention" means the International Convention for the Safety of Life at Sea, 1974 as amended.

PART 1: REQUIREMENTS

Chapter 1 Scope and Core Requirements

This Chapter sets out the objectives and application of these Guidelines and the elements to be developed as a CSMS. The development and implementation of a CSMS rest on the fundamentals set out here, and all subsequent chapters are to be read on that basis.

1.1 Purpose of Cyber Security Management

The objective of cyber security management is for the Company to systematically assess and manage cyber risks in ship operation and to ensure the safety of operation, protection of the environment, and continuity of operation.

1.2 Purpose of the Cyber Security Management System (CSMS)

The purpose of the Cyber Security Management System (CSMS) is for the Company to develop, conduct and maintain a framework to implement the cyber security management of ships, and to achieve the following:

- 1. Identify and assess cyber risks relating to the IT and OT systems of the ship;
- 2. Determine and implement appropriate controls for the assessed cyber risks;
- 3. Ensure response to and recovery from cyber incidents, as well as preparedness for emergencies; and
- 4. Continuously improve the effectiveness of management in the Company and onboard the ship.

1.3 Compatibility with Relevant Rules, Regulations, Codes, and Guidelines

The CSMS shall ensure:

- 1. Compliance with applicable mandatory rules and conventions
- 2. That applicable codes, guidelines, and standards recommended by the Organization, the Administration, classification societies, and other maritime industry organizations are taken into account.

1.4 Application

These Guidelines apply to the Company and to the ships that the Company includes within the scope of its CSMS.

1.5 Elements of a Cyber Security Management System (CSMS)

The Company shall develop, implement, and maintain a CSMS that includes the following:

- 1. Cyber security policy
- 2. Procedures for conducting cyber risk assessment

- 3. Instructions and procedures to ensure the cyber security of the ship in accordance with relevant conventions and flag State legislation
- 4. Clear definition of levels of authority and lines of communication within and between shore-based and shipboard organizations
- 5. Procedures for reporting accidents and non-conformities with the provisions of these Requirements
- 6. Procedures to prepare for and respond to emergency situations
- 7. Procedures for internal audits and management reviews

Chapter 2 Leadership and Policy Requirements

This Chapter sets out the requirements for the establishment and implementation of the cyber security policy. A policy is not merely a document to be kept on file: it has meaning only when it is established as the Company's own commitment under the leadership of top management and implemented throughout the organization.

2.1 Establishment of Cyber Security Policy

The Company shall establish a cyber security policy that includes measures to achieve the objectives set out in **1.2**.

2.2 Implementation and Maintenance of Cyber Security Policy

The Company shall ensure that the policy is implemented and maintained at all levels of the shore-based and shipboard organization.

Chapter 3 Governance and Responsibility Requirements

This Chapter sets out the roles and responsibilities necessary for the implementation of the CSMS. Cyber risk management cannot be established simply by delegating it to designated staff. It becomes effective only when top management bears ultimate responsibility, the operational structure is defined, including the responsible persons ashore and on board, and each fulfills their role within that structure.

3.1 Roles and Responsibilities

-1. The Company shall identify, define, and document the roles and responsibilities necessary for the effective implementation of the CSMS, including but not limited to the Company Cybersecurity Officer and the Ship Cybersecurity Officer referred to in this Chapter. The responsibilities specified in these Guidelines are minimum requirements and do not limit any additional responsibilities or authorities established by the Company.

-2. The responsibilities, authorities, and interrelationships of personnel managing, performing, or verifying cyber security-related activities shall be clearly defined and documented.

3.2 Responsibility of Top Management

-1. Top management shall bear ultimate responsibility for the establishment and effective implementation of the CSMS.

-2. Top management shall appoint the Company Cybersecurity Officer and any other roles necessary for the effective implementation of the CSMS.

3.3 Company Cybersecurity Officer

-1. The Company Cybersecurity Officer shall have overall responsibility for the effective implementation and oversight of the CSMS.

-2. The Company Cybersecurity Officer shall be able to report directly to top management.

-3. The Company Cybersecurity Officer shall have the authority to raise to top management the need for resources necessary for the effective implementation of the CSMS.

-4. The responsibilities and authority of the Company Cybersecurity Officer shall be defined and documented, and shall include, at a minimum:

- (1) Monitoring the implementation and effectiveness of the CSMS;
- (2) Reporting to top management on the performance of the CSMS.

-5. Nothing in these Guidelines shall restrict the Company from assigning additional responsibilities or authorities to the Company Cybersecurity Officer.

3.4 Ship Cybersecurity Officer

-1. The Ship Cybersecurity Officer shall have responsibility for the implementation of the CSMS on board each ship.

-2. The responsibilities and authority of the Ship Cybersecurity Officer shall include, at a minimum:

- (1) monitoring the implementation and effectiveness of the CSMS onboard the ship;
- (2) reporting to the Company Cybersecurity Officer on the performance of the CSMS onboard the ship.

3.5 Master's Authority

The Company shall ensure that, within the implementation of the CSMS on board, the overriding authority of the Master as provided in paragraph 5.2 of the ISM Code is preserved and applies to decisions relating to the safety of the ship and the prevention of pollution, including those arising from cyber security events.

Chapter 4 Resource and Competence Requirements

This Chapter sets out the requirements concerning the organization's internal resources and the competence of personnel necessary for the implementation of the CSMS. Resources support the implementation of the CSMS as a whole, from its development through continuous improvement. Above all, it is the people of the Company who implement a CSMS: developing the competence appropriate to each role and raising awareness across the organization form the foundation of its implementation.

4.1 Provision of Resources

- 1. The Company shall determine and provide the resources necessary for the establishment, implementation, maintenance, and continuous improvement of the CSMS.
- 2. Such resources shall include, as applicable, human resources, technical capabilities, financial resources, and organizational support necessary to manage cyber risks within the scope of this Guideline.
- 3. In considering such resources, the Company shall take into account reports and requests from the Company Cybersecurity Officer as set out in 3.3.

4.2 Competence Requirements

- 1. The Company shall define the competence required for each role established under **Chapter 3**, taking into account the responsibilities and authorities assigned to that role.
- 2. The Company shall ensure that personnel assigned to those roles meet the defined competence requirements.
- 3. Competence shall be determined based on appropriate education, training, experience, or a combination thereof.
- 4. The Company shall retain appropriate documented information as evidence of competence.

4.3 Training and Awareness

- 1. The Company shall ensure that all employees are aware of:
 - (1) the cyber security policy of the Company;
 - (2) the requirements in the CSMS manual;
 - (3) their roles and responsibilities within the CSMS; and
 - (4) the potential consequences of failing to comply with CSMS requirements.
- 2. The Company shall provide basic cyber security awareness training to all employees.
- 3. The Company shall provide training appropriate to the responsibilities and authorities assigned to personnel holding roles defined under **Chapter 3**.
- 4. Training and awareness activities specified in -2. and -3. above shall be conducted at intervals not exceeding 12 months.
- 5. The Company shall retain documented records of the training and awareness activities conducted.

Chapter 5 Supply Chain Management Requirements

This Chapter sets out the management of external resources involved in the implementation of the CSMS. It addresses contractors, suppliers, and service providers relevant to the scope of the CSMS. The Company's cyber risk management is complete only when the Company also sets cyber security requirements for these parties and verifies that they are met.

5.1 Requirements for Suppliers

- 1. Where relevant to the scope of the CSMS, the Company shall ensure that contractors, suppliers, and service providers (hereinafter referred to as "suppliers") are aware of the applicable cyber security requirements relevant to their activities and are capable of appropriately addressing such requirements.
- 2. The Company shall define the level of competence or management controls required of suppliers.
- 3. The Company shall verify that suppliers meet the defined requirements and retain records of such verification.

5.2 Evaluation of Suppliers

The Company shall periodically verify that suppliers performing activities related to the CSMS meet the requirements specified in **5.1**.

Chapter 6 Cyber Risk Assessment Requirements

This Chapter sets out the definition and scope of the cyber risk assessment and its implementation process, including planning, conduct, and review. The cyber risk assessment provides the basis for understanding the cyber risks to be managed and for determining the controls to be applied. This Chapter does not prescribe any particular risk assessment methodology.

6.1 Role of Cyber Risk Assessment

Cyber risk assessment lies at the core of the cyber security management under these Guidelines, and is a common decision-making process to identify and evaluate cyber risks associated with the shipboard IT and OT environment and to determine controls appropriate to the Company and the ship.

6.2 Scope of the Cyber Risk Assessment

-1. The cyber risk assessment covers IT and OT systems that may affect the safe operation, protection of the environment, or continuity of operation of the ship. This includes onboard systems and may also cover shore-side systems that are directly connected to onboard systems or that affect the operation of the ship.

-2. General corporate IT systems that are neither connected to onboard systems nor affect the operation of the ship are, in principle, not subject to the cyber risk assessment.

6.3 Management of Cyber Risk Assessment Process

-1. The Company shall document the process for conducting cyber risk assessments. The documented process shall define at least the following:

- (1) Personnel responsible for conducting cyber risk assessments;
- (2) Personnel responsible for reviewing and approving the results of cyber risk assessments;
- (3) The concept (definition) of acceptable residual risk;
- (4) Personnel responsible for reviewing residual risks and deciding whether to accept them; and
- (5) The process for reviewing cyber risk assessments.

-2. The Company shall conduct cyber risk assessments in accordance with the documented process and shall retain records demonstrating that the process has been applied.

6.4 Identification and Evaluation of Cyber Risks

-1. The Company shall identify the IT and OT systems subject to assessment under 6.2 and the network configurations and, on that basis, identify and evaluate the cyber risks.

-2. In identifying and evaluating cyber risks, the Company shall consider at least the following factors:

- (1) Cyber threats associated with the relevant IT and OT assets and network configurations;
- (2) Vulnerabilities or weaknesses in the relevant assets and configurations (e.g.,

- technical vulnerabilities, misconfigurations, operational weaknesses);
- (3) The potential impact on ship operations, safety, the environment, or business if such threats occur;
 - (4) The likelihood of such threats occurring;
 - (5) Ship-specific operational conditions (e.g., navigation patterns, cargo carried); and
 - (6) Applicable legislation, regulations, contractual requirements, and other relevant requirements.

-3. Based on the results of the cyber risk assessment, the Company shall select appropriate controls specified in **Chapter 8**, determine the scope to be applied, and, having determined additional measures where necessary, implement them accordingly.

-4. Where the Company does not implement a control specified in Chapter 8, it shall identify the risk that remains as a result and record the rationale and the acceptance decision.

-5. These Guidelines do not prescribe any specific risk assessment methodology.

6.5 Review of Cyber Risk Assessment

-1. The Company shall review the cyber risk assessment at intervals not exceeding 12 months, and shall carry it out again where the review shows it necessary.

-2. Where a change subject to change management under **Chapter 7** has occurred, the cyber risk assessment shall be carried out again for the scope affected by the change at an appropriate time.

Chapter 7 Configuration Management Requirements

This Chapter sets out configuration management for the scope of the cyber risk assessment under **Chapter 6**. Maintaining and managing the configuration of the assets and their operating environment is the starting point for reducing cyber risks, and this Chapter ensures that changes, in particular, are handled in a controlled manner.

7.1 Configuration Management

The Company shall manage the current configuration and change history of the IT/OT assets and network configurations that are subject to the cyber risk assessment under **Chapter 6**.

7.2 Change Management

The Company shall establish procedures to manage changes to IT/OT assets, network configurations, software, or external connections. Such procedures shall provide for assessing cyber risks in advance of a change in accordance with the cyber risk assessment process under **Chapter 6**, reviewing the application of the controls under **Chapter 8** based on the results, and approving and implementing the change.

7.3 Configuration Review

The Company shall periodically verify that configurations and settings remain consistent with the approved state.

Chapter 8 Controls

This Chapter sets out the controls applicable to shipboard IT/OT systems, organized by control domain. The selection of individual controls is determined based on the results of the cyber risk assessment under **Chapter 6**. The content of each control is described in **Part 2**.

8.a Access & Use Control

- 8.a.1 Identity & Authentication Management
- 8.a.2 Authorization & Privilege Management
- 8.a.3 Remote & Third-Party Access Control
- 8.a.4 Acceptable Use & User-Initiated Risks

8.b Network & Communication Security

- 8.b.1 Network Segmentation & Zoning
- 8.b.2 Protection of Communication
- 8.b.3 External Connectivity Management

8.c System Configuration & Maintenance

- 8.c.1 Secure Configuration & Hardening
- 8.c.2 Patch & Update Management
- 8.c.3 Obsolescence Management
- 8.c.4 Malware & Endpoint Protection
- 8.c.5 Hardware & Software Control

8.d Media & Physical Interface Control

- 8.d.1 Removable Media Control
- 8.d.2 Physical Port & Interface Protection
- 8.d.3 Direct Connection Management
- 8.d.4 Physical Access Control

8.e Monitoring, Logging & Detection

- 8.e.1 Event Logging
- 8.e.2 Security Monitoring
- 8.e.3 Log Protection & Retention
- 8.e.4 Log Review & Anomaly Investigation

8.f Backup & Recovery

- 8.f.1 Backup Policy & Implementation
- 8.f.2 Recovery Procedures
- 8.f.3 Verification & Recovery Measures

Chapter 9 Emergency Preparedness Requirements

This Chapter sets out the requirements for emergency response. It requires the Company to define the events to be reported in the implementation of the CSMS, to establish the reporting lines and content that enable ship and shore to respond in coordination, including contact with third-party specialists where necessary, and to conduct regular drills; together, these constitute preparedness for emergencies.

9.1 Establishment of Procedures to Respond to Emergency Situations

The Company shall identify potential cyber incidents and emergency situations arising therefrom on board its ships, and establish procedures to respond to them.

9.2 Establishment of Programs to Respond to Emergency Situations

The Company shall establish drill programs to prepare for the response to cyber incidents and emergency situations arising therefrom.

9.3 Provision of Measures Ensuring Response to Emergency Situations

The Company shall ensure that the support necessary to respond to cyber incidents is secured in advance.

Chapter 10 Non-conformity and Corrective Action Requirements

This Chapter sets out the handling of non-conformities identified through the implementation of the CSMS. For continuous improvement, non-conformities are subject to investigation of their causes, response, and corrective actions.

10.1 Reporting and Analysis of Non-conformities

The Company shall establish procedures ensuring that non-conformities are reported to the Company and investigated and analyzed with the objective of improving the effectiveness of the CSMS.

10.2 Corrective Action and Prevention of Recurrence

The Company shall establish procedures for implementing corrective action, including measures to prevent recurrence.

Chapter 11 Documentation Requirements

This Chapter sets out the control of documents relating to the CSMS. The creation, revision, and withdrawal of such documents are controlled in accordance with the document control procedures established under this Chapter.

11.1 Establishment and Maintenance of Document Control Procedures

- 1. The Company shall establish and maintain procedures to control all documents and data which are relevant to the CSMS.
- 2. The document control procedures in accordance with -1 above shall ensure that:
 - (1) valid documents are available at all relevant locations;
 - (2) changes to documents are reviewed and approved by authorized personnel; and
 - (3) obsolete documents are promptly removed.

11.2 Cyber Security Management Manual

The Company shall prepare the documents used to describe and implement the CSMS as the "Cyber Security Management Manual" and maintain them as official documents of the Company. The Manual shall consist of documents applicable to the Company and documents applicable to each ship within the scope. Documentation may be kept in a form that the Company considers most effective. Each ship shall carry on board all documentation applicable to that ship.

Chapter 12 Verification, Review and Evaluation Requirements

This Chapter sets out the review of the implementation of the CSMS through internal audits and reviews by top management, for the purpose of the continuous improvement of the CSMS.

12.1 Internal Cyber Security Audit

-1. The Company shall carry out internal cyber security audits on board and ashore at intervals not exceeding twelve months to verify whether cyber security activities comply with the CSMS.

-2. Personnel carrying out audits shall be independent of the areas being audited and shall have the competence necessary to carry out cyber security audits appropriately.

-3. The results of the audits shall be brought to the attention of all personnel having responsibility in the area involved. Non-conformities found in the audits shall be dealt with in accordance with the corrective action procedures specified in **Chapter 10**.

12.2 Evaluation of the Cyber Security Management System

Top management shall periodically review the effectiveness of the CSMS. The results of the review shall be brought to the attention of all personnel having responsibility in the area involved.

PART 2: ASSESSMENT CRITERIA AND OBJECTIVE EVIDENCE

For the requirements and controls in **Part 1**, **Part 2** sets out the criteria the Society applies in its audits and the objective evidence it requires.

Whereas **Part 1** sets out the requirements for the CSMS that the Company is to develop, **Part 2** sets out, requirement by requirement, the criteria against which the Society audits whether the Company has developed, implemented, and maintained each requirement, and the objective evidence verified in the audit. By referring to **Part 2**, the Company can see, for each requirement, what it needs in order to develop its own CSMS and what will be verified in the audit.

For each control in **Chapter 8** of **Part 1**, the assessment criteria state in concrete terms what the control requires in order to be regarded as implemented. These criteria do not require any particular technical solution or product. The Company determines and implements appropriate controls taking into account the results of the cyber risk assessment, the characteristics of its ships, its operating patterns, and the applicable external requirements.

Chapter 1 Scope and Core Requirements

1.1 Purpose of Cyber Security Management

Corresponding Part 1 Requirement

The objective of cyber security management is for the Company to systematically assess and manage cyber risks in ship operation and to ensure the safety of operation, protection of the environment, and continuity of operation.

Assessment Criteria

Not assessed separately; assessed through the subsequent paragraphs

Required Objective Evidence

Not assessed separately; assessed through the subsequent paragraphs

External References

—

1.2 Purpose of the Cyber Security Management System (CSMS)

Corresponding Part 1 Requirement

The purpose of the Cyber Security Management System (CSMS) is for the Company to develop, conduct and maintain a framework to implement the cyber security management of ships, and to achieve the following:

- 1. Identify and assess cyber risks relating to the IT and OT systems of the ship;
- 2. Determine and implement appropriate controls for the assessed cyber risks;
- 3. Ensure response to and recovery from cyber incidents, as well as preparedness for emergencies; and
- 4. Continuously improve the effectiveness of management in the Company and onboard the ship.

Assessment Criteria

Not assessed separately; assessed through the subsequent paragraphs

Required Objective Evidence

Not assessed separately; assessed through the subsequent paragraphs

External References

—

1.3 Compatibility with Relevant Rules, Regulations, Codes, and Guidelines

Corresponding Part 1 Requirement

The CSMS shall ensure:

- 1. Compliance with applicable mandatory rules and conventions
- 2. Applicable codes, guidelines, and standards recommended by the Organization, the Administration, classification societies, and other maritime industry organizations are taken into account.

Assessment Criteria

The CSMS Manual makes reference to applicable legislation, conventions, or relevant guidelines.

Required Objective Evidence

CSMS Manual

External References
—**1.4 Application****Corresponding Part 1 Requirement**

These Guidelines apply to the Company and to the ships that the Company includes within the scope of its CSMS.

Assessment Criteria

The CSMS Manual clearly defines the scope of the applicable ships, the IT and OT systems, and the shore-side systems that affect ship operation.

Required Objective Evidence

CSMS Manual,

Risk assessment documentation, etc. (documents that define the scope of application of the CSMS, or the scope of the risk assessment)

External References

DryBMS / Subject Area No. 28: Excellence

TMSA 3 / Element 13: Stage 1; §13.1.1

MSC-FAL.1/Circ.3/Rev.3: §2.3.1

IACS Rec. 194: §§3.2–3.3

1.5 Elements of a Cyber Security Management System (CSMS)**Corresponding Part 1 Requirement**

The Company shall develop, implement, and maintain a CSMS that includes the following:

- 1. Cyber security policy
- 2. Procedures for conducting cyber risk assessment
- 3. Instructions and procedures to ensure the cyber security of the ship in accordance with relevant conventions and flag State legislation
- 4. Clear definition of levels of authority and lines of communication within and between shore-based and shipboard organizations
- 5. Procedures for reporting accidents and non-conformities with the provisions of these Requirements
- 6. Procedures to prepare for and respond to emergency situations
- 7. Procedures for internal audits and management reviews

Assessment Criteria

The CSMS Manual sets out the elements indicated in **Part 1, 1.5 -1** through **-7**.

Required Objective Evidence

CSMS Manual

External References

DryBMS / Subject Area No. 28: Basic

SIRE 2.0 / Section 7.5

TMSA 3 / Element 13: Stage 1; §§13.1, 13.1.1

Chapter 2 Leadership and Policy Requirements

2.1 Establishment of Cyber Security Policy

Corresponding Part 1 Requirement

The Company shall establish a cyber security policy that includes measures to achieve the objectives set out in 1.2.

Assessment Criteria

The cyber security policy is documented and establishes the company's commitment to achieving the objectives set out in 1.2

The policy is formally approved by top management, with evidence of commitment (e.g., signature or equivalent approval record)

The policy addresses at minimum the following:

- Alignment with the objectives stated in 1.2.
- The company's approach to managing cyber risks in ship operations.
- The process for creating, approving, and managing changes to the policy is established.

Required Objective Evidence

The cyber security policy is documented and includes at least the following:

- The measures to achieve the objectives set out in 1.2 (the company's approach to managing cyber risks in ship operations) are described in the policy.
- The company's commitment is expressly stated.

Approval records show at least the following:

- The policy was formally approved by top management (e.g., a signature, or an approval record identifying the approver and the date of approval).

External References

RISQ 3.2 / Section 12: §12.7

DryBMS / Subject Area No. 28: Basic

TMSA 3 / Element 13: Stage 2; §§13.2.3, 13.3.3

MSC-FAL.1/Circ.3/Rev.3: §§3.3, 3.5.1

2.2 Implementation and Maintenance of Cyber Security Policy

Corresponding Part 1 Requirement

The Company shall ensure that the policy is implemented and maintained at all levels of the shore-based and shipboard organization.

Assessment Criteria

The policy is implemented at all levels of the organization, both ashore and on board, and is communicated to relevant personnel

The policy is maintained in a current state through periodic review and update, whether as part of the review under 12.2 or otherwise

Required Objective Evidence

Evidence that the policy is communicated to relevant personnel exists, confirming at least the following:

- The policy or reference to it is accessible to shore-based and shipboard personnel.
- Training records, familiarization records, or equivalent show that relevant personnel have been informed of the policy and its requirements.

Review records show the policy is kept current, including at least the following:

- Records of periodic review exist (e.g., management review minutes, revision history).

External References

Chapter 3 Governance and Responsibility Requirements

3.1 Roles and Responsibilities

Corresponding Part 1 Requirement

-1. The Company shall identify, define, and document the roles and responsibilities necessary for the effective implementation of the CSMS, including but not limited to the Company Cybersecurity Officer and the Ship Cybersecurity Officer referred to in this Chapter. The responsibilities specified in these Guidelines are minimum requirements and do not limit any additional responsibilities or authorities established by the Company.

-2. The responsibilities, authorities, and interrelationships of personnel managing, performing, or verifying cyber security-related activities shall be clearly defined and documented.

Assessment Criteria

-1. All roles and responsibilities necessary for the effective implementation of the CSMS are identified, defined, and documented, including at minimum the Company Cybersecurity Officer and the Ship Cybersecurity Officer(s).

-2. The following requirements are met:

-The responsibilities, authorities, and interrelationships of all personnel managing, performing, or verifying cyber security-related activities are clearly defined and documented.

-The interfaces between shore-based management and vessels are addressed in the documented structure.

-Roles for which the assignment of responsibility is specifically called for by external requirements (e.g., the person responsible for managing user profiles and passwords in the vessel network) are identified.

Required Objective Evidence

The Company documents the CSMS organizational structure, showing at least the following:

Documents such as the company organization chart and cyber security organization chart identify the roles necessary for the effective implementation of the CSMS, including at minimum the Company Cybersecurity Officer and the Ship Cybersecurity Officer(s), as well as any additional roles the company has established.

The person responsible for managing user profiles and passwords in the vessel network is identified.

The document is subject to change management (e.g., date of approval, approving authority, revision history).

Procedures or other CSMS documents describe, for each cyber security-related role, at least the following:

the responsibilities, authorities, and interrelationships of the role;

the interfaces between shore-based management and shipboard personnel.

External References

DryBMS / Subject Area No. 28: Basic

SIRE 2.0 / Section 7.5

TMSA 3 / Element 13: Stage 1; §13.1.1

3.2 Responsibility of Top Management

Corresponding Part 1 Requirement

- 1. Top management shall bear ultimate responsibility for the establishment and effective implementation of the CSMS.
- 2. Top management shall appoint the Company Cybersecurity Officer and any other roles necessary for the effective implementation of the CSMS.

Assessment Criteria

- 1. Top management bears ultimate responsibility for the establishment and effective implementation of the CSMS, as demonstrated through its approval of the cyber security policy (see **2.1**) and equivalent acts.
- 2. Top management bears responsibility for the appointment of the roles necessary for the effective implementation of the CSMS (including at minimum the Company Cybersecurity Officer), and such roles are confirmed to have been appointed.

Required Objective Evidence

Records show that top management holds ultimate responsibility for the CSMS, including at least the following:

- Top management has approved and signed the cyber security policy (see **2.1**), thereby demonstrating its ultimate responsibility for the CSMS.

Appointment records show that the roles necessary for the effective implementation of the CSMS have been assigned, including at least the following:

- The roles necessary for the effective implementation of the CSMS have been appointed under the responsibility of top management (e.g., appointment documentation, statements of appointment in the CSMS manual, designation of positions, or delegation of appointing authority).
- The appointments include at minimum the Company Cybersecurity Officer.

External References

3.3 Company Cybersecurity Officer

Corresponding Part 1 Requirement

- 1. The Company Cybersecurity Officer shall have overall responsibility for the effective implementation and oversight of the CSMS.
- 2. The Company Cybersecurity Officer shall be able to report directly to top management.
- 3. The Company Cybersecurity Officer shall have the authority to raise to top management the need for resources necessary for the effective implementation of the CSMS.
- 4. The responsibilities and authority of the Company Cybersecurity Officer shall be defined and documented, and shall include, at a minimum:
 - (1) Monitoring the implementation and effectiveness of the CSMS;
 - (2) Reporting to top management on the performance of the CSMS.

-5. Nothing in these Guidelines shall restrict the Company from assigning additional responsibilities or authorities to the Company Cybersecurity Officer.

Assessment Criteria

- 1. The Company Cybersecurity Officer is positioned as the person with overall responsibility for the effective implementation and oversight of the CSMS.
- 2. The Company Cybersecurity Officer is positioned to have direct access to top management.
- 3. The Company Cybersecurity Officer has the authority to raise to top management the need for resources necessary for the effective implementation of the CSMS.
- 4. The responsibilities and authority of the Company Cybersecurity Officer are defined and documented, including at minimum:
 - (1) monitoring the implementation and effectiveness of the CSMS across the Company and vessels under management
 - (2) reporting to top management on the performance of the CSMS.

Required Objective Evidence

A document defining the responsibilities and authority of the Company Cybersecurity Officer (CSMS manual etc.) exists, confirming at least the following:

- The Company Cybersecurity Officer is described as the person with overall responsibility for the effective implementation and oversight of the CSMS.
- The responsibilities and authority include monitoring the implementation and effectiveness of the CSMS and reporting to top management.
- The authority to raise to top management the need for resources necessary for the effective implementation of the CSMS is described.

The organizational structure shows a direct reporting relationship from the Company Cybersecurity Officer to top management.

- The organization chart or description of reporting lines shows direct reporting to top management.

External References

DryBMS / Subject Area No. 28: Basic

SIRE 2.0 / Section 7.5

TMSA 3 / Element 13: Stage 1; §13.1.4

MSC-FAL.1/Circ.3/Rev.3: §§3.5.1–3.5.2

IACS Rec. 194: §4.2, Item 11

3.4 Ship Cybersecurity Officer

Corresponding Part 1 Requirement

- 1. The Ship Cybersecurity Officer shall have responsibility for the implementation of the CSMS on board each ship.
- 2. The responsibilities and authority of the Ship Cybersecurity Officer shall include, at a minimum:
 - (1) monitoring the implementation and effectiveness of the CSMS onboard the ship;
 - (2) reporting to the Company Cybersecurity Officer on the performance of the CSMS onboard the ship.

Assessment Criteria

- 1. The Ship Cybersecurity Officer is positioned as the person with responsibility for the implementation of the CSMS on board each vessel.
- 2. The responsibilities and authority of the Ship Cybersecurity Officer include at minimum:
 - (1) monitoring the implementation and effectiveness of the CSMS on board the ship;
 - (2) reporting to the Company Cybersecurity Officer on the performance of the CSMS on board the ship.

Required Objective Evidence

For each vessel in scope, a document defining the responsibilities and authority of the Ship Cybersecurity Officer (CSMS manual etc.) exists, confirming at least the following:

- The Ship Cybersecurity Officer on each vessel is identified by name or title.
- The responsibilities and authority include monitoring the implementation and effectiveness of the CSMS on board the ship and reporting to the Company Cybersecurity Officer.

External References

DryBMS / Subject Area No. 28: Basic
SIRE 2.0 / Section 7.5
MSC-FAL.1/Circ.3/Rev.3: §§3.5.1–3.5.2

3.5 Master's Authority

Corresponding Part 1 Requirement

The Company shall ensure that, within the implementation of the CSMS on board, the overriding authority of the Master as provided in paragraph 5.2 of the ISM Code is preserved and applies to decisions relating to the safety of the ship and the prevention of pollution, including those arising from cyber security events.

Assessment Criteria

The CSMS documentation preserves the Master's overriding authority under paragraph 5.2 of the ISM Code and states that it applies to decisions relating to the safety of the ship and prevention of pollution, including those arising from cyber security incidents.

Required Objective Evidence

The CSMS manual or equivalent document confirms the following:

- A statement of the Master's overriding authority that references or is consistent with paragraph 5.2 of the ISM Code.
- The authority extends to decisions relating to cyber security incidents.

External References

Chapter 4 Resource and Competence Requirements

4.1 Provision of Resources

Corresponding Part 1 Requirement

- 1. The Company shall determine and provide the resources necessary for the establishment, implementation, maintenance, and continuous improvement of the CSMS.
- 2. Such resources shall include, as applicable, human resources, technical capabilities, financial resources, and organizational support necessary to manage cyber risks within the scope of this Guideline.
- 3. In considering such resources, the Company shall take into account reports and requests from the Company Cybersecurity Officer as set out in **3.3**.

Assessment Criteria

The Company Cybersecurity Officer is given the opportunity to raise reports or requests regarding resources, including at defined occasions such as the management review, and a process exists for the Company to consider them.

Note: The assessment under this requirement covers whether a mechanism exists for the Company to consider reports or requests regarding resources. The Company's decision on the resources to be provided is not itself assessed.

Required Objective Evidence

The Company has a mechanism by which the Company Cybersecurity Officer raises views on resources and the Company considers them:

- At defined occasions such as the management review, the Company Cybersecurity Officer is given the opportunity to make reports or requests regarding resources (e.g., management review minutes, rules of the relevant meeting body).
- Records exist showing that reports or requests regarding resources were considered by the Company (e.g., meeting minutes).

External References

MSC-FAL.1/Circ.3/Rev.3: §2.3.2

4.2 Competence Requirements

Corresponding Part 1 Requirement

- 1. The Company shall define the competence required for each role established under **Chapter 3**, taking into account the responsibilities and authorities assigned to that role.
- 2. The Company shall ensure that personnel assigned to those roles meet the defined competence requirements.
- 3. Competence shall be determined based on appropriate education, training, experience, or a combination thereof.
- 4. The Company shall retain appropriate documented information as evidence of competence.

Assessment Criteria

- 1. For each role designated under **Chapter 3**, the competence required is defined, taking into account the responsibilities and authorities of that role.
- 2. The Company has confirmed that personnel assigned to those roles meet the defined competence requirements.
- 3. Competence is determined based on appropriate education, training, experience, or a combination thereof.
- 4. Documented information is retained as evidence of competence.

Required Objective Evidence

A document defining competence requirements per role (job description, competence matrix, statement in the CSMS manual, etc.) exists, confirming at least the following:

- For the Company Cybersecurity Officer, the knowledge and experience required to perform the role (e.g., cyber risk management, maritime IT/OT, understanding of relevant standards and external requirements) are set out specifically as requirements.
- For the Ship Cybersecurity Officer and other roles, the knowledge and skills required for their respective responsibilities are set out.

Records showing that each person meets the competence requirements exist, confirming at least the following:

- For each person, it is recorded by which means (education, training, experience, or a combination) each defined requirement is met (e.g., training certificates, qualifications, work history, competence assessment records).
- Requirements and actual competence are matched, so that fulfilment against each requirement can be traced.

External References

DryBMS / Subject Area No. 28: Basic
MSC-FAL.1/Circ.3/Rev.3: §§3.5.1–3.5.2
IACS Rec. 194: §4.2, Item 9

4.3 Training and Awareness

Corresponding Part 1 Requirement

- 1. The Company shall ensure that all employees are aware of:
 - (1) the cyber security policy of the Company;
 - (2) the requirements in the CSMS manual;
 - (3) their roles and responsibilities within the CSMS; and
 - (4) the potential consequences of failing to comply with CSMS requirements.
- 2. The Company shall provide basic cyber security awareness training to all employees.
- 3. The Company shall provide training appropriate to the responsibilities and authorities assigned to personnel holding roles defined under **Chapter 3**.
- 4. Training and awareness activities specified in -2. and -3. above shall be conducted at intervals not exceeding 12 months.
- 5. The Company shall retain documented records of the training and awareness activities conducted.

Assessment Criteria

- 1. All employees are ensured to be aware of:
 - (1) the cyber security policy of the Company;
 - (2) the requirements in the CSMS manual;
 - (3) their roles and responsibilities within the CSMS; and
 - (4) the potential consequences of failing to comply with CSMS requirements.
- 2. The following requirements are met:
 - Basic cyber security training is provided to all employees.
 - Measures for training and awareness called for by external requirements are taken (e.g., inclusion of response to and recovery from a cyber incident in the basic training; active promotion of cyber security awareness on board using posters, CBT, or online courses; provision of a security briefing as part of the familiarization process, including at crew changes).
- 3. The following requirements are met:
 - Training appropriate to the responsibilities and authorities is provided to personnel holding roles defined under **Chapter 3**.
 - Such personnel understand the Company's cyber risk management procedures relevant to their responsibilities.
- 4. The training and awareness under -2. and -3. is conducted at intervals not exceeding 12 months.
- 5. Documented records of the training and awareness conducted are retained.

Required Objective Evidence

Records of training and awareness for all employees exist, confirming at least the following:

- Basic cyber security training has been provided to all employees, with content addressing the cyber security policy, the requirements in the CSMS manual, individual roles and responsibilities, and the consequences of non-compliance.
- The interval does not exceed 12 months, as shown by records of the dates conducted.
- Measures for training and awareness required by external requirements are in place (e.g., the basic training includes response to and recovery from a cyber incident; means of awareness promotion are in place on board such as posters, CBT, or online courses; a security briefing is provided as part of the familiarization process, including at crew changes).

Records of role-specific training for personnel holding roles under **Chapter 3** exist, and interviews show their understanding:

- The content of the training is appropriate to the responsibilities and authorities of the role.
- Dates and completion are documented.
- An interview with the personnel responsible for cyber risk management shows their understanding of the Company's cyber risk management procedures relevant to their responsibilities (including back-up arrangements for OT systems critical to navigation and propulsion).

External References

DryBMS / Subject Area No. 28: Basic
SIRE 2.0 / Section 7.5

TMSA 3 / Element 13: Stage 1; §13.1.3

MSC-FAL.1/Circ.3/Rev.3: §§3.5.3.6, 3.5.4.2, 3.5.5.3, 3.5.6.2, 3.7

ClassNK

Chapter 5 Supply Chain Management Requirements

5.1 Requirements for Suppliers

Corresponding Part 1 Requirement

- 1. Where relevant to the scope of the CSMS, the Company shall ensure that contractors, suppliers, and service providers (hereinafter referred to as "suppliers") are aware of the applicable cyber security requirements relevant to their activities and are capable of appropriately addressing such requirements.
- 2. The Company shall define the level of competence or management controls required of suppliers.
- 3. The Company shall verify that suppliers meet the defined requirements and retain records of such verification.

Assessment Criteria

- 1. Where relevant to the scope of the CSMS, suppliers are ensured to be aware of the applicable cyber security requirements relevant to their activities and capable of appropriately addressing them.
- 2. The level of competence or management controls required of suppliers is defined.
- 3. The following requirements are met:
 - The Company verifies that suppliers meet the requirements defined in -2. and retains records of such verification.
 - Measures for supplier management called for by external requirements are taken (e.g., pre-contract due diligence and a defined scope of work for independent specialist support used to mitigate threats; use of due diligence or independent auditor's reports prior to granting access to systems).

Required Objective Evidence

Documentation defining requirements for suppliers relevant to the CSMS scope exists, confirming at least the following:

- The applicable cyber security requirements that suppliers must be aware of or comply with are identified.
 - The level of competence or management controls required of suppliers is defined.
- Records of supplier verification exist, confirming at least the following:
- Evidence that relevant suppliers have been informed of applicable requirements exists (e.g., contract clauses, communication records, pre-qualification assessments).
 - Fulfilment of the requirements has been verified and records retained.
- Measures for supplier management called for by external requirements are in place (e.g., pre-contract due diligence and a defined scope of work for independent specialist support; use of due diligence or independent auditor's reports prior to granting access to systems).

External References

DryBMS / Subject Area No. 28: Advanced
TMSA 3 / Element 13: §13.4.2

MSC-FAL.1/Circ.3/Rev.3: §3.5.3.8

IACS Rec. 194: §4.2, Item 9

5.2 Evaluation of Suppliers

Corresponding Part 1 Requirement

The Company shall periodically verify that suppliers performing activities related to the CSMS meet the requirements specified in **5.1**.

Assessment Criteria

- Suppliers entrusted with activities relevant to the CSMS are verified, at intervals or timing determined by the Company, to conform to the requirements set out in 5.1 (including the level of competence or management controls determined by the Company under **5.1**).
- Where the requirements are found not to be met, the non-conformity is required to be handled under the procedures of Chapter 10.

Required Objective Evidence

Procedures and records for supplier evaluation exist, confirming at least the following:

- The interval or timing for evaluating suppliers is determined by the Company.
- The conformity of suppliers entrusted with activities relevant to the CSMS to the requirements determined by the Company under 5.1 (the level of competence or management controls) is verified at that interval or timing, and the results are recorded.
- The procedures require non-conformities identified through the verification to be handled under Chapter 10, and any such non-conformity has been handled accordingly. Actions taken as a result may include, for example, requesting corrective action from the supplier, requesting updates to the supplier's policies or procedures, reviewing the contract, or changing the supplier.

External References

DryBMS / Subject Area No. 28: Advanced

Chapter 6 Cyber Risk Assessment Requirements

6.1 Role of Cyber Risk Assessment

Corresponding Part 1 Requirement

Cyber risk assessment lies at the core of the cyber security management under these Guidelines, and is a common decision-making process to identify and evaluate cyber risks associated with the shipboard IT and OT environment and to determine controls appropriate to the Company and the ship.

Assessment Criteria

Not assessed separately; assessed through the subsequent paragraphs

Required Objective Evidence

Not assessed separately; assessed through the subsequent paragraphs

External References

—

6.2 Scope of the Cyber Risk Assessment

Corresponding Part 1 Requirement

-1. The cyber risk assessment covers IT and OT systems that may affect the safe operation, protection of the environment, or continuity of operation of the ship. This includes onboard systems and may also cover shore-side systems that are directly connected to onboard systems or that affect the operation of the ship.

-2. General corporate IT systems that are neither connected to onboard systems nor affect the operation of the ship are, in principle, not subject to the cyber risk assessment.

Assessment Criteria

Not assessed separately; assessed through the subsequent paragraphs

Required Objective Evidence

Not assessed separately; assessed through the subsequent paragraphs

External References

—

6.3 Management of Cyber Risk Assessment Process

Corresponding Part 1 Requirement

-1. The Company shall document the process for conducting cyber risk assessments. The documented process shall define at least the following:

- (1) Personnel responsible for conducting cyber risk assessments;
- (2) Personnel responsible for reviewing and approving the results of cyber risk assessments;
- (3) The concept (definition) of acceptable residual risk;
- (4) Personnel responsible for reviewing residual risks and deciding whether to accept

- them; and
- (5) The process for reviewing cyber risk assessments.
- 2. The Company shall conduct cyber risk assessments in accordance with the documented process and shall retain records demonstrating that the process has been applied.

Assessment Criteria

- 1. The process for conducting cyber risk assessments is documented and defines at least:
- (1) Personnel responsible for conducting assessments;
 - (2) Personnel responsible for reviewing and approving the results of cyber risk assessments;
 - (3) the definition of acceptable residual risk;
 - (4) Personnel responsible for approving and accepting residual risks and deciding whether to accept them;
 - (5) the method for reviewing assessments.
- 2. Cyber risk assessments are conducted in accordance with the documented process, and records demonstrating that the process has been applied are retained.

Required Objective Evidence

A documented cyber risk assessment process exists, confirming at least the following:

- The five elements set out in **6.3-1** are defined.

Completed cyber risk assessment records exist, confirming at least the following:

- Review and approval by designated persons have been carried out.
- Residual risks have been identified and the acceptance decision is recorded.

External References

DryBMS / Subject Area No. 28: Basic

SIRE 2.0 / Section 7.5

TMSA 3 / Element 13: Stage 2; §13.2.1

MSC-FAL.1/Circ.3/Rev.3: §3.5.3

6.4 Identification and Evaluation of Cyber Risks

Corresponding Part 1 Requirement

- 1. The Company shall identify the IT and OT systems subject to assessment under 6.2 and the network configurations and, on that basis, identify and evaluate the cyber risks.
- 2. In identifying and evaluating cyber risks, the Company shall consider at least the following factors:
- (1) Cyber threats associated with the relevant IT and OT assets and network configurations;
 - (2) Vulnerabilities or weaknesses in the relevant assets and configurations (e.g., technical vulnerabilities, misconfigurations, operational weaknesses);
 - (3) The potential impact on ship operations, safety, the environment, or business if such threats occur;
 - (4) The likelihood of such threats occurring;
 - (5) Ship-specific operational conditions (e.g., navigation patterns, cargo carried); and
 - (6) Applicable legislation, regulations, contractual requirements, and other relevant

requirements.

-3. Based on the results of the cyber risk assessment, the Company shall select appropriate controls specified in **Chapter 8**, determine the scope to be applied, and, having determined additional measures where necessary, implement them accordingly.

-4. Where the Company does not implement a control specified in **Chapter 8**, it shall identify the risk that remains as a result and record the rationale and the acceptance decision.

-5. These Guidelines do not prescribe any specific risk assessment methodology.

Assessment Criteria

- 1. The IT and OT systems subject to assessment under **6.2** and network configurations are identified, and the resulting cyber risks are identified and evaluated on that basis.
- 2. In identifying and evaluating cyber risks, the factors set out in **6.4-2.(1)** through (6) are considered.
- 3. Based on the results, appropriate controls are selected from those specified in **Chapter 8**, the scope to be applied is determined, additional measures are determined where necessary, and they are implemented accordingly.
- 4. Where a control is not implemented, the risk that remains as a result is identified, and the rationale and acceptance decision are recorded.

Required Objective Evidence

The Company maintains an inventory of shipboard IT/OT assets, such as a list of the equipment and systems in scope, recording at least the following for each system. Where shore-side systems fall within the scope of the cyber risk assessment under **6.2**, the inventory or equivalent records cover those systems as well:

- equipment type, manufacturer, software version, and patch update status
- The inventory includes at minimum (where fitted): cargo management systems, bridge systems, propulsion and machinery management and power control systems, access control systems, administrative and crew welfare systems, and communication systems.
- The inventory is maintained and kept updated (e.g., date of last update confirmed).

The Company maintains a network configuration diagram showing at least the following:

- Network zones and their names are defined.
- Connections between zones and external connection points are shown.

Completed cyber risk assessment records (assessment results, records of residual risks, acceptance decisions) show at least the following :

- The factors set out in 6.4-2 are addressed, including identification of both external and internal threats.
- Threats applicable to the vessel's trading areas are addressed.
- The controls selected and the residual risks accepted are documented with rationale.
- The perspective of reducing both the likelihood of vulnerabilities being exploited and the impact if exploited is reflected.

External References

SIRE 2.0 / Section 7.5

TMSA 3 / Element 13: Stage 1, Stage 2, Stage 4; §§13.1.2, 13.1.5, 13.1.3, 13.2.1, 13.2.3, 13.4.1

MSC-FAL.1/Circ.3/Rev.3: §§3.4, 3.5, 3.5.2, 3.5.2.1, 3.5.2.2, 3.5.2.3

IACS Rec. 194: §4.2, Item 1, Item 2, Item 3, Item 4, Item 5, Item 6, Item 7, Item 10, and Item 13

6.5 Review of Cyber Risk Assessment

Corresponding Part 1 Requirement

- 1. The Company shall review the cyber risk assessment at intervals not exceeding 12 months, and shall carry it out again where the review shows it necessary.
- 2. Where a change subject to change management under **Chapter 7** has occurred, the cyber risk assessment shall be carried out again for the scope affected by the change at an appropriate time.

Assessment Criteria

- 1. The cyber risk assessment is reviewed at intervals not exceeding 12 months and, where the review shows it necessary, carried out again.
- 2. Where changes subject to change management under **Chapter 7** occur, it is carried out again for the scope affected at an appropriate time.
- 3. A mechanism exists to obtain current security-related information from appropriate external sources (e.g., industry advisories, flag state guidance, classification society Guidelines etc), and the information obtained is reviewed and, where relevant, reflected in the cyber risk assessment or procedures.

Required Objective Evidence

Records of cyber risk assessment reviews exist, confirming at least the following:

- The latest review date does not exceed 12 months from the previous review.
- The review outcomes, including the judgement on whether the assessment needs to be carried out again, are recorded.
- Where a change subject to change management under Chapter 7 occurred, the assessment has been carried out again in association with that change.

Procedures or records for obtaining and reflecting external information exist, confirming at least the following:

- A mechanism to obtain current security-related information from appropriate external sources exists (e.g., industry advisories, flag state guidance, classification society guidelines).
- Records show that the information obtained has been reviewed and, where relevant, reflected in updates to the cyber risk assessment or procedures.

External References

TMSA 3 / Element 13: §§13.1.4, 13.2.1, 13.3.2

Chapter 7 Configuration Management Requirements

7.1 Configuration Management

Corresponding Part 1 Requirement

The Company shall manage the current configuration and change history of the IT/OT assets and network configurations that are subject to the cyber risk assessment under **Chapter 6**.

Assessment Criteria

- The current configuration of the IT/OT assets and network configurations subject to the cyber risk assessment under **Chapter 5** is documented and maintained.
- The history of updates to the configuration information (when and which configuration information was updated) is recorded and maintained as part of the register.

Required Objective Evidence

Documents recording configuration information (asset inventory, network configuration diagram, etc.) exist, confirming at least the following:

- The current state of the IT/OT assets and network configurations subject to the cyber risk assessment under Chapter 5 can be ascertained.
- The asset inventory is maintained and kept updated throughout the life of the ship (including updates and maintenance by suppliers or third parties).
- The update history of the configuration information is retained as part of the register, so that the point in time of the current configuration can be traced.

External References

IACS Rec. 194: §4.2, Item 9

7.2 Change Management

Corresponding Part 1 Requirement

The Company shall establish procedures to manage changes to IT/OT assets, network configurations, software, or external connections. Such procedures shall provide for assessing cyber risks in advance of a change in accordance with the cyber risk assessment process under **Chapter 6**, reviewing the application of the controls under **Chapter 8** based on the results, and approving and implementing the change.

Assessment Criteria

- Procedures are defined to manage changes to IT/OT assets, network configurations, software, or external connections.
- Where changes are made to IT/OT assets, network configurations, software, or external connections, cyber risks are assessed before the change in accordance with the cyber risk assessment process under **Chapter 6**, and the application of the controls under **Chapter 8** is reviewed based on the results.
- Where new technology or equipment is introduced, a procedure for assessing it from a cyber security perspective prior to introduction is defined.

- For each change, its course (assessment, approval, implementation) is recorded so that it can be traced.

Required Objective Evidence

Change management procedures exist, confirming at least the following:

- The changes subject to change management (changes to IT/OT assets, network configurations, software, or external connections) are defined.
- Assessment of cyber risks prior to a change in accordance with the process under Chapter 6, and review of the application of the controls under Chapter 8 based on the results, are required.
- The approving authority or approval process for changes is defined.
- A procedure for cyber security assessment prior to the introduction of new technology or equipment is defined.
- Changes or maintenance are required to be carried out by qualified and authorized personnel.

Where records of changes exist, at least the following can be confirmed:

- For each change, the pre-change risk assessment, its evaluation, and the course of implementation can be traced.
- The assessment results are reflected in the cyber risk assessment under Chapter 6 and the review of controls under Chapter 8.

Note: Routine software updates are addressed under **8.c.2**.

External References

DryBMS / Subject Area No. 28: Advanced
IACS Rec. 194: §4.2, Item 1 and Item 9

7.3 Configuration Review

Corresponding Part 1 Requirement

The Company shall periodically verify that configurations and settings remain consistent with the approved state.

Assessment Criteria

- Configurations and settings are periodically verified to remain consistent with the approved state.

Required Objective Evidence

Records of periodic configuration verification exist, confirming at least the following:

- A mechanism to verify whether configurations and settings match the approved state is defined.
- Periodic verification has been carried out, and where deviations from the approved state are identified, the response is recorded.

External References

IACS Rec. 194: §4.2, Item 9

Chapter 8 Controls

8.a.1 Identity & Authentication

Assessment Criteria

- Unique credentials are assigned to individual users where practicable. Where shared or generic credentials are used for operational reasons, such credentials are kept under control (e.g., limiting the range of users, designating a person responsible, changing passwords at crew changes).
- Default passwords on all devices have been changed.
- A password policy is defined and applied.
- Generic user profiles and passwords are not passed on at crew changes, and passwords are changed regularly.
- Passwords are not posted at workstations or otherwise left uncontrolled.
- Accounts for personnel who have left or changed roles are deactivated promptly.

Required Objective Evidence

Access control policies and procedures exist, confirming at least the following with respect to identity and authentication management:

- Requirements for unique credentials, password policy, and account management (including deactivation upon departure or change of role) are defined.
- Requirements for the change of generic user profiles and passwords at crew changes, and for prohibiting their handover, are defined.

Records of access control implementation through identity and authentication management exist, confirming at least the following:

- User account lists show no uncontrolled generic or shared accounts; where shared or generic credentials are used, the records show how such credentials are controlled (range of users, person responsible, changes at crew changes, etc.).
- Accounts for personnel who have left or changed roles are confirmed to have been deactivated.

Note: The user account list is the same document as that referred to in **8.a.2**. The confirmation points under this item are uncontrolled generic/shared accounts and deactivation of accounts for departed personnel.

External References

DryBMS / Subject Area No. 28: Intermediate

SIRE 2.0 / Section 7.5

TMSA 3 / Element 13: §§13.1.3, 13.2.4, 13.4.5

MSC-FAL.1/Circ.3/Rev.3: §§3.5.3.1–3.5.3.2

IACS Rec. 194: §4.2, Item 4 and Item 6

8.a.2 Authorization & Privilege Management

Assessment Criteria

- Administrator privileges are restricted to designated senior officers or authorized personnel only.

- User profiles restrict systems to their intended purposes.
- User profiles are actively managed and redundant profiles deleted.
- The person responsible for maintaining user profiles and passwords in the vessel network is designated.

Required Objective Evidence

Procedures or other CSMS documents confirm at least the following with respect to authorization and privilege management:

- The personnel to whom administrator privileges may be granted are defined.
- The designation of the person responsible for managing user profiles and passwords is documented.

Records of implementation of authorization and privilege management exist, confirming at least the following:

- Holders of administrator privileges are limited to the defined scope.
- Redundant profiles have been deleted.

Note: The user account list is the same document as that referred to in **8.a.1**. The confirmation points under this item are the restriction of administrator privilege holders and the deletion of redundant profiles.

External References

DryBMS / Subject Area No. 28: Intermediate

SIRE 2.0 / Section 7.5

TMSA 3 / Element 13: §§13.1.3, 13.4.5

MSC-FAL.1/Circ.3/Rev.3: §§3.5.3.1–3.5.3.2

IACS Rec. 194: §4.2, Item 4

8.a.3 Remote & Third-Party Access Control

Assessment Criteria

- Procedures govern access to IT and OT systems by third parties (including visitors such as surveyors and technicians, regardless of the means of access), and formal approval is required before granting access to sensitive equipment.
- Remote access (i.e. access from outside the ship, including by the Company's shore-based personnel) requires explicit onboard approval, is managed by authorized shore-based personnel, and uses strong authentication (including multi-factor authentication where the means of remote access supports it) and encryption.
- Measures for remote access called for by external requirements are taken (e.g., limits on unsuccessful login attempts, manual termination by onboard personnel or automatic termination after a period of inactivity, activity logs of remote sessions).
- Records of approval for third-party access and remote access to sensitive IT/OT systems are maintained.

Required Objective Evidence

Procedures for third-party and remote access exist, confirming at least the following:

- An approval process for access (local and remote) to sensitive IT/OT systems is

defined.

- Remote access security requirements (authentication including MFA where applicable, encryption, limits on unsuccessful login attempts, session termination, session logging) are stated.

Records of access exist, confirming at least the following:

- Records of formal approval for third-party access exist (identity of accessing party, authorizing officer, and date/time recorded).
- Remote access session logs exist where remote access has been used.

Note: Remote session activity logs are the same records as those referred to in **8.e.1**. The confirmation point under this item is their correspondence with approval records.

External References

DryBMS / Subject Area No. 28: Intermediate, Advanced

SIRE 2.0 / Section 7.5

TMSA 3 / Element 13: §§13.1.3, 13.2.4, 13.4.5

IACS Rec. 194: §4.2, Item 6

8.a.4 Acceptable Use & User-Initiated Risks

Assessment Criteria

- Rules to be observed by authorized users (crew and shore-based personnel) when using IT and OT systems are defined and communicated. These cover the scope of acceptable use and prohibited acts, such as locking unattended workstations, not using unauthorized software, and responsible use of social media.
- Procedures govern the use of personal devices on board.
- Network use by crew is controlled within the permitted scope.

Required Objective Evidence

- Rules on user conduct, the use of personal devices, and crew network use are set out in procedures or other CSMS documents.
- Records show that these rules have been communicated to personnel (e.g., training or distribution records).

Note: Conformity with **8.a.4** is assessed by cross-referencing evidence across related domains, including **8.a.3**, **8.b.1**, **8.c.5**, and **8.d.1**.

External References

DryBMS / Subject Area No. 28: Intermediate

SIRE 2.0 / Section 7.5

TMSA 3 / Element 13: §§13.1.3, 13.2.4, 13.4.5

IACS Rec. 194: §4.2, Item 4 and Item 5

8.b.1 Network Segmentation & Zoning

Assessment Criteria

- Shipboard IT and OT systems are configured in logically or physically separated network zones based on function and risk, with at minimum the following

separations implemented:

(1) separation of OT networks from IT networks, with communication between them controlled through firewalls or other security devices;

(2) separation of the crew personal-use network (Crew zone) from business IT and OT networks.

- External connections (e.g., satellite communications, remote access) are managed through a DMZ or equivalent security zone (a buffer segment preventing external connections from being directly connected to business and OT networks).
- Network zone configurations and inter-zone communication control rules are documented and the approved state is maintained.
- Zone design is based on the results of the cyber risk assessment under Chapter 6.

Required Objective Evidence

A shipboard IT/OT network diagram exists, confirming at least the following:

- Network zones and their names are defined (e.g., OT/Navigation, OT/Machinery, IT/Business, Crew, DMZ).
- Connectivity between zones and external connection points are shown.
- Type and location of security devices between zones are identified.

Documentation of inter-zone communication control rules exists (e.g., firewall policy, ACL), confirming at least the following:

- Approved rules for inter-zone communication are defined.

Cyber risk assessment records confirm at least the following:

- Network configuration and zone design are addressed as part of the risk assessment.
- The rationale for zone design decisions is linked to the results of the risk assessment.

Note: The network diagram is the same document as that referred to in **6.4** and **8.b.3**. The confirmation points under this item are zone design and inter-zone communication control.

External References

TMSA 3 / Element 13: Stage 4; §13.4.5

MSC-FAL.1/Circ.3/Rev.3: §§3.5.3.2–3.5.3.3

IACS Rec. 194: §4.2, Item 2 and Item 5

8.b.2 Protection of Communications

Assessment Criteria

- Communication protocols and services in use are identified and controlled.
- Unnecessary or unused communication services and ports are disabled.
- Encrypted communication is used where appropriate for sensitive data transmission.

Required Objective Evidence

Documents or configuration records concerning communication control exist,

confirming at least the following:

- Permitted communication protocols and services are identified.
- Configuration or inspection records confirm that unnecessary or unused communication services and ports are disabled.
- Encryption requirements for sensitive data transmission are defined.

Note: Configuration records are the same records as those referred to in **8.c.1**. The confirmation points under this item are the disabling of communication services and ports and encryption requirements.

External References

TMSA 3 / Element 13: Stage 4; §13.4.5

IACS Rec. 194: §4.2, Item 2, Item 5, and Item 6

8.b.3 External Connectivity Management

Assessment Criteria

- External connections (i.e. connection channels to networks or systems outside the ship, including satellite communications, remote maintenance, and shore-to-ship interfaces, irrespective of the connecting party and of whether they are used for remote access) are identified, documented, and controlled.
- An approval process governs the establishment of new external connections.

Required Objective Evidence

A list of external connections or a network diagram exists, confirming at least the following:

- All external connection points are identified and documented.

A procedure for approving new external connections exists; where approval records exist, they show the approving authority and the date of approval.

Note: The list of external connections or network diagram is the same document as that referred to in **8.b.1** (and **6.4**). The confirmation points under this item are the completeness of external connection points and the approval procedure for new connections.

External References

SIRE 2.0 / Section 7.5

TMSA 3 / Element 13: Stage 4; §13.4.5

8.c.1 Secure Configuration & Hardening

Assessment Criteria

- A process is established for reviewing vendor default configurations for systems used on board and implementing necessary hardening, including disabling unnecessary services, protocols, and accounts. For OT systems, hardening is implemented to the extent permitted by the supplier.
- Reviews and hardening are carried out in accordance with that process.

Required Objective Evidence

Configuration standards or configuration records exist, confirming at least the following:

- Requirements for disabling unnecessary services, protocols, and accounts are defined, or records confirm their implementation.
- Records confirm that default vendor configurations have been reviewed and hardening carried out.

Note: Configuration records are the same records as those referred to in **8.b.2**. The confirmation points under this item are the disabling of unnecessary services, protocols, and accounts, and the implementation of hardening.

External References

DryBMS / Subject Area No. 28: Intermediate

TMSA 3 / Element 13: Stage 4; §13.4.5

8.c.2 Patch & Update Management

Assessment Criteria

- A process for managing software and firmware updates for shipboard IT and OT systems exists, defining at least:
 - (1) the frequency or schedule for applying updates (including application per supplier recommendations or agreements with suppliers);
 - (2) the personnel carrying out updates (including that updates are carried out by qualified and authorized personnel);
 - (3) consideration of supplier involvement or permission for OT systems.
- Updates and patches are applied in accordance with the defined process.
- Patch and update status records are maintained.

Required Objective Evidence

Patch and update management procedures exist, confirming at least the following:

- The items set out in **(1)** through **(3)** of the Assessment Criteria are covered.

Records of implementation exist, confirming at least the following:

- Records of update and patch application status for shipboard systems are maintained.
- Rationale for deferred or unimplemented updates is documented.

Note: Patch application status may be verified through the same source as the asset inventory under **6.4** (patch update status). The confirmation points under this item are the application process/schedule and the rationale for unimplemented updates.

Note: Routine updates applied in accordance with the defined process or schedule are addressed under this item. Changes beyond routine updates (e.g., version upgrades affecting system functionality or configuration) are addressed under the change management provisions of **7.2**.

External References

DryBMS / Subject Area No. 28: Intermediate

SIRE 2.0 / Section 7.5
TMSA 3 / Element 13: Stage 4; §13.4.5
MSC-FAL.1/Circ.3/Rev.3: §§3.5.3.3, 3.5.3.7
IACS Rec. 194: §4.2, Item 9

8.c.3 Obsolescence Management

Assessment Criteria

- A process is defined for identifying systems and software that are no longer supported by the manufacturer or whose end of support is known.
- Risks associated with the identified unsupported systems are considered in the cyber risk assessment under **Chapter 6**, and necessary controls (e.g., compensating controls) are determined and implemented.

Required Objective Evidence

A documented process for identifying unsupported systems exists (e.g., as part of procedures or asset inventory maintenance rules), confirming at least the following:

- How support status is identified and recorded is defined .

Records concerning unsupported systems exist, confirming at least the following:

- Unsupported or end-of-life systems and software have been identified.
- Associated risks and the controls determined (including compensating controls, e.g., strengthened network segregation, restriction of external connections, remote access, and physical ports, enhanced monitoring, replacement planning) are documented.

Note: Support status may be verified through the same source as the asset inventory under **6.4** (software version, patch update status). The assessment of risks itself is addressed under **6.4**. The confirmation points under this item are the identification of unsupported systems and the implementation of controls.

External References

DryBMS / Subject Area No. 28: Intermediate
TMSA 3 / Element 13: Stage 4; §13.4.5

8.c.4 Malware & Endpoint Protection

Assessment Criteria

- Provisions concerning malware protection for shipboard computers exist, defining at least:
 - (1) that antivirus or equivalent malware protection is applied where technically feasible and not restricted by suppliers;
 - (2) for OT systems, such protection is applied only if allowed or provided by the system supplier;
 - (3) malware protection definitions or equivalent are kept up to date.
- In accordance with **(1)** through **(3)** above, malware protection is applied to applicable shipboard computers, including ECDIS, and is maintained current.

Required Objective Evidence

Provisions concerning malware protection exist (e.g., procedures), confirming at least the following:

- The items set out in (1) through (3) of the Assessment Criteria are covered.
- Records of implementation exist, confirming at least the following:
- Antivirus or equivalent malware protection is applied to applicable shipboard computers, including ECDIS.
 - For OT systems, it is documented whether malware protection is allowed or provided by the system supplier.
 - Update records for malware protection definitions or equivalent show they are maintained current.

External References

RISQ 3.2 / Section 12: §12.8

DryBMS / Subject Area No. 28: Intermediate

SIRE 2.0 / Section 7.5

TMSA 3 / Element 13: Stage 4; §13.4.5

MSC-FAL.1/Circ.3/Rev.3: §3.5.3.4

IACS Rec. 194: §4.2, Item 3

8.c.5 Hardware & Software Control

Assessment Criteria

- A process for approving hardware and software before use on board is established, and the cyber resilience of equipment and systems by design (e.g., conformity with international standards such as IACS UR E27, availability of type approval, or conformity with conditions for onboard use defined by the company) is a consideration within that process.
- Unauthorized software is not installed on shipboard systems.
- Procedures exist for the secure disposal of equipment, including data destruction.

Required Objective Evidence

Hardware and software control procedures exist, confirming at least the following:

- An approval process for hardware and software before use on board is defined.
- The approval includes as a consideration the cyber security conformity or equivalent status of the equipment or system (e.g., conformity with international standards such as IACS UR E27, availability of type approval, or conformity with conditions for onboard use defined by the company).
- The procedure addresses secure disposal including data destruction.

Records of implementation exist, confirming at least the following:

- Records of approval of hardware and software exist.
- Installed software on shipboard systems is inventoried and verified against approval records to confirm that no unauthorized software is present.

Note: The approval process before use may be verified through the same document as the change management procedure under 7.2. The confirmation points under this item are the approval and disposal of hardware and software.

External References

DryBMS / Subject Area No. 28: Intermediate

SIRE 2.0 / Section 7.5

TMSA 3 / Element 13: Stage 2, Stage 4; §§13.2.4, 13.4.5

MSC-FAL.1/Circ.3/Rev.3: §§3.5.3.3, 3.8

8.d.1 Removable Media Control

Assessment Criteria

- A policy is documented prohibiting the normal use of removable media (e.g., USB memory sticks, CDs/DVDs, external hard drives) for data transfer to controlled systems.
- Where the use of removable media is unavoidable, an exception management process with defined conditions and approval requirements exists.
- Removable media are required to be scanned before use, using malware protection that is kept up to date. Where required by external requirements, scanning is carried out in the manner they require (e.g., on a computer not connected to the ship's control network).

Required Objective Evidence

A removable media policy and procedure exists, confirming at least the following:

- Removable media are not normally used for data transfer to controlled systems.
- Exceptional use is subject to defined conditions and approval.
- Removable media must be scanned for malware before use.

Records of implementation exist, confirming at least the following:

- Records of approved exceptional use exist (approving authority and date recorded).
- Records confirm that removable media were scanned for malware (including, where required by external requirements, scanning on a computer not connected to the ship's control network).
- Records show the policy and procedures have been communicated to shore-based and shipboard personnel (e.g., training or distribution records).

External References

RISQ 3.2 / Section 12: §12.8

DryBMS / Subject Area No. 28: Intermediate

SIRE 2.0 / Section 7.5

TMSA 3 / Element 13: Stage 1, Stage 2, Stage 4; §§13.1.3, 13.2.4, 13.4.5

MSC-FAL.1/Circ.3/Rev.3: §3.5.3.5

IACS Rec. 194: §4.2, Item 7

8.d.2 Physical Port & Interface Protection

Assessment Criteria

- Unused physical ports (e.g., USB, RJ-45) are consistently and permanently blocked by physical plugs or equivalent measures.
- Keys or blocking devices are maintained by authorized personnel only.
- All physically accessible computers and network ports identified in the asset

- inventory are subject to protection measures.
- Access to USB and RJ-45 ports on critical systems such as ECDIS is controlled by disabling or locking the ports.

Required Objective Evidence

An inventory of equipment and ports under protection exists, confirming at least the following:

- It identifies each piece of equipment and its port types (USB, RJ-45, etc.).
- It covers critical systems such as ECDIS, including their USB and RJ-45 ports.
- It records the protection measure applied to each port.

Records verifying the physical protection measures exist (e.g., inspection records, photographs), confirming at least the following:

- The installation of port blockers or equivalent devices is evidenced by records or photographs.
- The person responsible for keys or blocking devices is identified.

Note: Where the inventory of protected equipment and ports is based on the asset inventory under **7.1**, the same document may serve both. The confirmation points under this item are the protection measures applied and their implementation.

External References

SIRE 2.0 / Section 7.5

TMSA 3 / Element 13: Stage 4; §13.4.5

IACS Rec. 194: §4.2, Item 7

8.d.3 Direct Connection Management

Assessment Criteria

- A procedure governs direct connections to shipboard systems (e.g., via laptops, maintenance terminals, or external devices), prohibiting unauthorized connections.
- The approval process, connection conditions, and monitoring requirements during direct connections are defined.
- Control requirements for third-party direct connections are defined, and records of connections are maintained.

Required Objective Evidence

A procedure for managing direct connections exists, confirming at least the following:

- Direct connections without approval are prohibited.
- It sets out the approval process, the conditions under which connections may be made, and the controls applicable to third parties.

Records of approved direct connections exist, confirming at least the following:

- Each record shows the purpose of the connection, the connecting party, the approving authority, and the date and time.

Note: Approval of third-party direct connections may be evidenced by the same records as third-party access approval under **8.a.3**. The confirmation points under this item are the conditions for connection (including prior verification of the connecting device),

supervision during the connection, and the records of connections made.

Note: Where supervision and escort of personnel during the connection rely on the visitor control provisions of the Ship Security Plan (SSP) under the ISPS Code, it is sufficient to confirm that the CSMS documentation refers to those provisions. Verification of conditions for the connecting device remains subject to this item.

External References

TMSA 3 / Element 13: Stage 4; §13.4.5

8.d.4 Physical Access Control

Assessment Criteria

- Spaces containing sensitive IT/OT control equipment (e.g., engine room, bridge, server room) are kept locked, preventing access by unauthorized persons. Network components that cannot be protected on a space-by-space basis are protected by other means, such as locked enclosures or secured locations.
- Personnel authorized to access such spaces are defined and documented.
- Unauthorized entry, or signs of it, must be reported when found (subsequent response is addressed under **9.1**).

Required Objective Evidence

A physical access management procedure exists, confirming at least the following:

- It identifies the controlled spaces and any equipment outside those spaces that requires protection.
- It defines who is authorized to access each controlled space.
- It requires that unauthorized entry, or signs of it, be reported.

A list of authorized personnel exists, confirming at least the following:

- Authorized personnel are identified for each controlled space, and the list is kept current.

Note: Where control of access to spaces relies on the relevant provisions of the Ship Security Plan (SSP) under the ISPS Code, it is sufficient to confirm that the CSMS documentation refers to those provisions. The adequacy of the SSP itself is not subject to this assessment.

External References

SIRE 2.0 / Section 7.5

TMSA 3 / Element 13: Stage 4; §13.4.5

IACS Rec. 194: §4.2, Item 4

8.e.1 Event Logging

Assessment Criteria

- Shipboard IT and OT systems are required to log security-relevant events, covering, where technically feasible, at least:
 - (1) authentication events;
 - (2) use of administrator privileges;

- (3) configuration changes;
- (4) remote session activity;
- (5) traffic at network boundaries and external connection points.
- Logging is enabled on the relevant systems and devices, including network security devices.
- The logs captured are collected and retained in a referable state so that they can be used for intrusion detection and incident response (protection of stored logs is addressed under **8.e.3**).

Note: Companies are encouraged to collect logs centrally (including transfer ashore), where practicable, as this enhances the effectiveness of investigations and log reviews in the event of an incident.

Required Objective Evidence

Documented provisions on logging exist (e.g., procedures), confirming at least the following:

- They specify which log types are captured and on which systems and devices, covering items **(1)** through **(5)** of the Assessment Criteria where technically feasible.
- They specify how logs are collected and stored, taking into account storage capacity constraints (e.g., overwriting of locally stored logs).

Evidence that logs are being captured exists (e.g., configuration records, actual logs), confirming at least the following:

- Logging is configured on network security devices (e.g., firewalls at the IT/OT boundary).

Logs are collected and stored as specified.

Note: Configuration records of network security devices are the same documents as those referred to in **8.e.2**. The confirmation points under this item are log types and storage. Remote session activity logs are shared with **8.a.3**.

External References

DryBMS / Subject Area No. 28: Excellence

TMSA 3 / Element 13: Stage 4; §13.4.5

MSC-FAL.1/Circ.3/Rev.3: §§3.5.3.3, 3.4, 3.4.1

IACS Rec. 194: §4.2, Item 6 and Item 10

8.e.2 Security Monitoring

Assessment Criteria

- Where technically feasible, network traffic monitoring and logging are available at network boundaries and external connection points.
- At the IT/OT boundary, firewalls or equivalent network security devices have the functionality for network traffic monitoring, anomaly detection, real-time alerting, and logging.
- Traffic at network boundaries and external connection points is actively monitored in operation.
- A contact for detected anomalies, on board or ashore, is designated.

Required Objective Evidence

Documents showing the functionality of network security devices (e.g., firewalls, UTM appliances, or communication gateways with firewall functionality) exist (e.g., specifications, configuration records), confirming at least the following:

- The devices provide network traffic monitoring, anomaly detection, real-time alerting, and log generation.
- Traffic at the IT/OT boundary is monitored.

Documented provisions or records for the operation of monitoring exist, confirming at least the following:

- It is defined who is notified when an anomaly is detected (personnel on board or ashore, or the point of contact where an external monitoring service is used).

Note: Specifications and configuration records of network security devices are the same documents as those referred to in **8.e.1**. The confirmation points under this item are the monitoring and alerting functionality and the notification arrangements.

External References

TMSA 3 / Element 13: Stage 4; §13.4.5

MSC-FAL.1/Circ.3/Rev.3: §§3.5.3.3, 3.4, 3.4.1

IACS Rec. 194: §4.2, Item 2 and Item 10

8.e.3 Log Protection & Retention

Assessment Criteria

- Logs are stored in a manner that protects them from unauthorized modification, deletion, or overwriting.
- Access right to the stored logs are managed in accordance with **8.a.2**.
- A minimum log retention period is defined and applied.

Required Objective Evidence

Documented provisions on log retention exist (e.g., procedures), confirming at least the following:

- A minimum retention period is defined.
- The method of protecting logs from unauthorized modification, deletion, or overwriting is defined (e.g., restricting physical access to the devices, or transferring logs ashore).

Management of access rights to stored logs is defined (the content of such management is addressed under **8.a.2**).

Evidence of stored logs exists, confirming at least the following:

Logs are retained as specified (e.g., by checking the range and period of stored logs).

External References

TMSA 3 / Element 13: Stage 4; §13.4.5

MSC-FAL.1/Circ.3/Rev.3: §3.5.3.3

IACS Rec. 194: §4.2, Item 10

8.e.4 Log Review & Anomaly Investigation

Assessment Criteria

- A process is defined for reviewing stored logs at a frequency, or upon triggers, determined by the company (including review by an external party).
- A process is defined for investigating anomalies or suspicious events that have been detected or reported, and for escalating them where necessary. The process provides for the use of stored logs in such investigations.
- Responsibilities for log review, investigation, and escalation are defined.

Required Objective Evidence

Procedures for log review and for investigating and escalating anomalies exist, confirming at least the following:

- The frequency or triggers for log review are defined.
- Responsibility for log review and investigation is assigned (including the point of contact where an external service is used).
- Stored logs are used in investigations.
- The escalation path is defined.

Note: Detection of anomalies and notification arrangements are addressed under **8.e.2**; assessment of reported events and incident response under **9.1**. The confirmation points under this item are the review of logs and the flow from detection or report to investigation and escalation. The procedures under this item may be confirmed through the same document as the cyber incident response procedures under **9.1**.

External References

TMSA 3 / Element 13: Stage 4; §13.4.5

8.f.1 Backup Policy & Implementation

Assessment Criteria

- A backup policy exists for shipboard digital systems critical to navigation, propulsion, and operations.
- Backups are performed on a defined schedule and retained in a manner that enables recovery.
- Backup functionalities are in place and available to assist recovery following a cyber incident.
- For OT systems, at least one of the following is in place: duplication of systems and equipment as required by flag state statutory regulations or class rules, or backup and restore procedures provided by the supplier or developed by the company.

Required Objective Evidence

A backup policy exists (e.g., procedures), confirming that at least the following are defined:

- What: the systems to be backed up (those critical to navigation, propulsion, and operations, as determined by the company based on the risk assessment under **Chapter 6**)
- When: the frequency or triggers for backups (e.g., periodic, after chart or configuration updates, or every voyage)
- How retained: where backups are stored and how they are kept (e.g., on external media kept on board, or copies sent ashore)
- For OT systems: whether duplication, backup and restore procedures, or both apply.

Records of backups exist, confirming at least the following:

- Backups are performed on the defined schedule (e.g., backup logs, records of the most recent backup).
- For OT systems, the basis for duplication (the applicable statutory or class requirements) or the existence of supplier or company backup and restore procedures is confirmed.

Note: Where duplication applies, conformity with the statutory regulations or class rules themselves is not subject to this assessment. It is sufficient to confirm that the CSMS documentation refers to those requirements as the basis.

Note: Duplication as a safety requirement is intended to provide redundancy against equipment failure and does not in itself ensure the ability to recover from a cyber incident (e.g., where the two ECDIS units carried under statutory requirements share the same network or update path, a malware infection may affect both). Companies are encouraged to consider this in the cyber risk assessment under **Chapter 6** for systems that have interfaces with external sources.

External References

SIRE 2.0 / Section 7.5

TMSA 3 / Element 13: Stage 4; §13.4.5

MSC-FAL.1/Circ.3/Rev.3: §3.5.1

IACS Rec. 194: §4.2, Item 13

8.f.2 Recovery Procedures

Assessment Criteria

- Documented recovery procedures cover the systems subject to the backup policy under **8.f.1**. For each system, the procedures identify a suitable recovery method — such as restoring from backup, switching over to a duplicated system, replacing the unit with a spare, or recovery by the supplier — and assign responsibility for carrying it out. OT systems critical to navigation and propulsion receive specific treatment to enable quick and safe recovery.
- The procedures address recovery priorities or a recovery sequence for incidents affecting multiple systems.
- Restored systems are returned to operation only after they are confirmed to be operating normally. Where a duplicated system or spare unit has been used to continue operation, the procedures define how the original configuration is to be restored.

Note: The overall response to cyber incidents is addressed in **Chapter 9** (response arrangements and reporting under **9.1**, drills under **9.2**, and securing support under **9.3**). The confirmation points under **8.f.2** and **8.f.3** are the technical procedures for restoring systems, including the approach to recovery priorities, and the verification of those procedures, for which the drills under **9.2** may be used. The procedures under this item may be confirmed through the same document as the cyber incident response procedures under **9.1**.

Required Objective Evidence

Recovery procedures exist, confirming at least the following:

- They cover the systems subject to the backup policy under **8.f.1**.
- For each system, they identify a suitable recovery method — such as restoring from backup, switching over to a duplicated system, replacing the unit with a spare, or recovery by the supplier — and who carries it out or is to be called upon (including supplier contact details).
- They set out specific provisions for OT systems critical to navigation and propulsion so that these can be recovered quickly and safely.
- They address recovery priorities or a recovery sequence for incidents affecting multiple systems.
- They require restored systems to be confirmed as operating normally before returning to operation.
- They define how the original configuration is restored after operation on a duplicated system or spare unit.

External References

SIRE 2.0 / Section 7.5

TMSA 3 / Element 13: Stage 4; §13.4.5

MSC-FAL.1/Circ.3/Rev.3: §§3.5.1, 3.5.3.7

IACS Rec. 194: §4.2, Item 13

8.f.3 Verification of Backups & Recovery Procedures

Assessment Criteria

- Backups taken and held by the company are periodically verified as restorable, through restore testing or equivalent verification (e.g., trial restoration, or checking that backup media and files are readable).
- The recovery arrangements under **8.f.2** are subject to the following:
 - (1) periodic confirmation that they remain current (e.g., that supplier contact details are valid and the duplication arrangements are unchanged);
 - (2) confirmation that they work (e.g., confirmation of switchover to duplicated systems (including during statutory or class surveys), or use of the recovery procedures in drills under **9.2**).

Note: The overall response to cyber incidents is addressed in **Chapter 9** (the response framework and reporting under **9.1**, drills under **9.2**, and securing support under **9.3**). The confirmation points under **8.f.2** and **8.f.3** are the technical procedures for restoring systems (including the approach to recovery priorities) and their verification; drills under **9.2** may be used for such verification. The procedures under this item may be confirmed through the same document as the cyber incident response procedures under **9.1**.

Required Objective Evidence

Records of backup verification exist, confirming at least the following:

- The frequency or triggers for verification are defined.
- Restore testing or equivalent verification has been carried out and the results recorded.

Records of confirmation of the recovery arrangements exist, confirming at least the following:

- Periodic confirmation that the arrangements remain current (supplier contact details, duplication arrangements, etc.) has been carried out and recorded.
- Confirmation that the arrangements work has been carried out and recorded (e.g., records of switchover confirmation during surveys, or drill records).

External References

TMSA 3 / Element 13: Stage 4; §13.4.5

MSC-FAL.1/Circ.3/Rev.3: §3.5.1

IACS Rec. 194: §4.2, Item 13

Chapter 9 Emergency Preparedness Requirements

9.1 Establishment of Procedures to Respond to Emergency Situations

Corresponding Part 1 Requirement

The Company shall identify potential cyber incidents and emergency situations arising therefrom on board its ships, and establish procedures to respond to them.

Assessment Criteria

- Potential cyber incidents and emergency situations arising therefrom have been identified.
- Procedures to respond to the identified situations are documented.
- The procedures include at least the following:
 - (1) a mechanism to identify events that may indicate a cyber incident and report them to the Company. Such events include anomalies in digital equipment or networks that cannot be determined on board to constitute a cyber incident.
 - (2) a mechanism to assess whether a reported event constitutes a cyber incident;
 - (3) onboard response procedures and reporting lines;
 - (4) coordination between the ship and the shore-based organization, including shore-side point(s) of contact;
 - (5) reporting to external authorities;
 - (6) recording of cyber incidents.
- The procedures are available in non-electronic form.
- Situations called for by external requirements are addressed in the procedures (e.g., loss of availability of navigational equipment, loss of availability or integrity of external data sources such as GNSS, loss of connectivity with the shore including GMDSS communications, loss of control systems for critical systems such as propulsion and steering, ransomware or denial of service incidents).

Required Objective Evidence

Cyber incident response procedures (plans) exist, confirming at least the following:

- Potential cyber incidents and emergency situations arising therefrom are listed.
- Onboard response procedures and reporting lines (internal, ship-to-shore, and to external authorities) are defined.
- Shore-side point(s) of contact are identified.
- Requirements for recording cyber incidents are defined.
- Situations called for by external requirements are addressed (loss of navigational equipment, GNSS, GMDSS, propulsion/steering, ransomware/DoS).

The procedures are confirmed to be available in non-electronic form (e.g., hard copy).

Contact details for technical support (company IT department or external IT contractors) are readily accessible.

External References

DryBMS / Subject Area No. 28: Basic

SIRE 2.0 / Section 7.5

TMSA 3 / Element 13: Stage 1; §§13.1.3, 13.1.5

MSC-FAL.1/Circ.3/Rev.3: §§3.5.3, 3.5.3.7, 3.5.5, 3.5.5.1, 3.5.5.2, 3.5.6, 3.5.6.1

IACS Rec. 194: §4.2, Item 12 and Item 14

9.2 Establishment of Programs to Respond to Emergency Situations

Corresponding Part 1 Requirement

The Company shall establish drill programs to prepare for the response to cyber incidents and emergency situations arising therefrom.

Assessment Criteria

- A program of drills is established to prepare for response to cyber incidents and emergency situations arising therefrom.
- Drills are conducted in accordance with the program.
- Following each drill, the results are reviewed and identified improvement points are recorded.

Required Objective Evidence

A document defining the drill program exists, confirming at least the following:

-The frequency or schedule is defined.

Records of drills conducted exist, confirming at least the following:

-Drills have been conducted in accordance with the program.

-The date of conduct and participants are recorded.

-A post-drill review (e.g., debrief) has been conducted, and identified improvement points and agreed corrective actions are recorded.

External References

TMSA 3 / Element 13: Stage 1; §13.1.3

MSC-FAL.1/Circ.3/Rev.3: §§3.5.3.6, 3.4, 3.5.5

9.3 Provision of Measures Ensuring Response to Emergency Situations

Corresponding Part 1 Requirement

The Company shall ensure that the support necessary to respond to cyber incidents is secured in advance.

Assessment Criteria

- The support necessary to respond to cyber incidents is secured in advance.
- At minimum, supplier contacts or points of contact capable of responding to cyber incidents are identified for the systems fitted on board.
- Where necessary, contracts or arrangements with specialist cyber support (e.g., consultants) are in place.

Required Objective Evidence

Documents or records showing support arrangements for cyber incident response exist, confirming at least the following:

-Supplier contacts or points of contact capable of responding to cyber incidents are identified and recorded for the systems fitted on board.

-Where applicable, records of contracts or arrangements with specialist cyber support exist.

External References

SIRE 2.0 / Section 7.5

IACS Rec. 194: §4.2, Item 11 and Item 14

ClassNK

Chapter 10 Non-conformity and Corrective Action Requirements

10.1 Reporting and Analysis of Non-conformities

Corresponding Part 1 Requirement

The Company shall establish procedures ensuring that non-conformities are reported to the Company and investigated and analyzed with the objective of improving the effectiveness of the CSMS.

Assessment Criteria

- Procedures ensuring that non-conformities are reported to the Company are documented.
- The recipient of non-conformity reports is clearly defined.
- A mechanism is defined whereby reported non-conformities are investigated and analysed, including root cause analysis, with the objective of improving the effectiveness of the CSMS.
- The person responsible for conducting the analysis and the timing are defined.

Required Objective Evidence

Procedures for reporting and analyzing non-conformities exist, confirming at least the following:

- The recipient of non-conformity reports (the role or department receiving the report) is clearly defined.
- The route, method, and form for reporting are defined.
- Root cause analysis of reported non-conformities is required.
- The person responsible and timing for conducting the analysis are defined.

Where records of non-conformity handling exist, at least the following can be confirmed:

- Root cause analysis has been conducted for reported non-conformities.

External References

—

10.2 Corrective Action and Prevention of Recurrence

Corresponding Part 1 Requirement

The Company shall establish procedures for implementing corrective action, including measures to prevent recurrence.

Assessment Criteria

- Procedures are documented for developing and implementing a corrective action plan, including measures to prevent recurrence, based on results of the root cause analysis.
- The person responsible for implementation, the timing, and the approver of the corrective action plan are defined.

Required Objective Evidence

Procedures for corrective action exist, confirming at least the following:

- A corrective action plan, including measures to prevent recurrence, is developed based on the results of the root cause analysis.
- The person responsible for implementation, the timing, and the approver of the corrective action plan are clearly defined.

Where records of corrective action exist, confirming at least the following:

- A corrective action plan has been developed and approved.
- Corrective action has been implemented in accordance with the plan, and the results are recorded.

External References

Chapter 11 Documentation Requirements

11.1 Establishment and Maintenance of Document Control Procedures

Corresponding Part 1 Requirement

- 1. The Company shall establish and maintain procedures to control all documents and data which are relevant to the CSMS.
- 2. The document control procedures in accordance with -1 above shall ensure that:
 - (1) valid documents are available at all relevant locations;
 - (2) changes to documents are reviewed and approved by authorized personnel; and
 - (3) obsolete documents are promptly removed.

Assessment Criteria

- 1. Procedures to control all documents and data relevant to the CSMS are documented and maintained.
- 2. The document control procedures in accordance with -1. above includes at least the following:
 - (1) valid documents are available at all relevant locations and on board the ships;
 - (2) changes to documents are reviewed and approved by authorized personnel;
 - (3) obsolete documents are promptly removed or controlled to prevent unintended use; and
 - (4) documents and data relevant to the CSMS are protected from unauthorized access, deletion, or tampering.

Required Objective Evidence

Document control procedures exist, confirming at least the following:

- The method for controlling documents and data relevant to the CSMS is defined.
- Control of versions and distribution (use of valid versions at relevant locations) is defined.
- The responsible personnel and process for reviewing and approving document changes are defined.
- The method for removing obsolete documents is defined.
- How documents and data are protected is defined (e.g., access permissions, controlled storage) .

External References

MSC-FAL.1/Circ.3/Rev.3: §3.6

11.2 Cyber Security Management Manual

Corresponding Part 1 Requirement

The Company shall prepare the documents used to describe and implement the CSMS as the "Cyber Security Management Manual" and maintain them as official documents of the Company. The Manual shall consist of documents applicable to the Company and documents applicable to each ship within the scope. Documentation may be kept in a form that the Company considers most effective. Each ship shall carry on board all documentation applicable to that ship.

Assessment Criteria

- The documents describing the CSMS are prepared as the "Cyber Security Management Manual" and maintained as controlled documents of the Company.
- The Manual consists of documents applicable to the Company and documents applicable to each ship within the scope.
- The documents in which the requirements of these Guidelines are addressed are identified.
- The documents applicable to each ship are carried on board that ship.

Note: The Manual applicable to each ship is expected to be developed from the Manual applicable to the Company, supplemented with information specific to that ship.

Required Objective Evidence

A Cyber Security Management Manual (by whatever name) exists, confirming at least the following:

- The documents describing the CSMS are positioned as controlled documents of the Company (approval or issuance as controlled documents can be confirmed).
- The documents in which the requirements of these Guidelines are addressed are identified (e.g., document list, mapping table).
- The Manual consists of documents applicable to the Company and documents applicable to each ship within the scope.
- For each ship within the scope, the documents applicable to that ship are carried on board.

External References

Chapter 12 Verification, Review and Evaluation Requirements

12.1 Internal Cyber Security Audit

Corresponding Part 1 Requirement

- 1. The Company shall carry out internal cyber security audits on board and ashore at intervals not exceeding twelve months to verify whether cyber security activities comply with the CSMS.
- 2. Personnel carrying out audits shall be independent of the areas being audited and shall have the competence necessary to carry out cyber security audits appropriately.
- 3. The results of the audits shall be brought to the attention of all personnel having responsibility in the area involved. Non-conformities found in the audits shall be dealt with in accordance with the corrective action procedures specified in **Chapter 10**.

Assessment Criteria

- 1. With respect to the implementation and method of internal cyber security audits, the following requirements are met:
 - Internal cyber security audits of the Company and ships are carried out at intervals not exceeding 12 months to verify whether cyber security activities are carried out in accordance with the CSMS.
 - The audits are carried out in accordance with documented procedures and an audit plan.
- 2. With respect to the independence and competence of auditors, the following requirements are met:
 - Persons carrying out audits are independent of the area being audited.
 - Persons carrying out audits have the competence necessary to carry out cyber security audits appropriately.
- 3. With respect to audit results and the handling of non-conformities, the following requirements are met:
 - The results of audits are brought to the attention of the personnel responsible for the areas concerned.
 - Non-conformities found in audits are dealt with in accordance with the corrective action procedures set out in **Chapter 10**.

Required Objective Evidence

Internal audit procedures and an audit plan exist, confirming at least the following:

- The scope, frequency (intervals not exceeding 12 months), and method of audits are defined.
 - The scope of audits includes, in addition to conformity with CSMS documents (policies and procedures), their implementation status.
 - Requirements for auditor independence and necessary competence are defined.
- Records of audits conducted exist, confirming at least the following:
- Audits of the Company and ships have been carried out at intervals not exceeding 12 months.
 - The persons who carried out the audits are independent of the area audited and have the competence necessary to carry out cyber security audits appropriately (competence confirmed through the records under Chapter 4).

- The results of audits are brought to the attention of the personnel responsible for the areas concerned.
- Non-conformities found are dealt with in accordance with the corrective action procedures set out in Chapter 10.

External References

DryBMS / Subject Area No. 28: Intermediate, Excellence
 TMSA 3 / Element 13: Stage 3; §13.3.3
 MSC-FAL.1/Circ.3/Rev.3: §3.5.3.9

12.2 Evaluation of the Cyber Security Management System

Corresponding Part 1 Requirement

Top management shall periodically review the effectiveness of the CSMS. The results of the review shall be brought to the attention of all personnel having responsibility in the area involved.

Assessment Criteria

- Top management reviews the effectiveness of the CSMS at intervals determined by the Company.
- The review evaluates the suitability, adequacy, and effectiveness of the CSMS.
- The review covers at least the following:
 - The results of internal audits.
 - the status of cyber risk assessments
 - the status of cyber incidents and non-conformities
 - the status of corrective actions
- The results of the review are brought to the attention of the personnel responsible for the areas concerned.

Required Objective Evidence

Records of management review exist, confirming at least the following:

- Top management reviews the effectiveness of the CSMS at intervals determined by the Company (e.g., management review minutes).
- The review covers at least the results of internal audits, the status of cyber risk assessments, the status of cyber incidents and non-conformities, and the status of corrective actions.
- The review evaluates the suitability, adequacy, and effectiveness of the CSMS.
- The results of the review are brought to the attention of the personnel responsible for the areas concerned.

External References

DryBMS / Subject Area No. 28: Advanced
 MSC-FAL.1/Circ.3/Rev.3: §§3.5.3.9, 3.6

