DNV·GL

CLASS GUIDELINE

DNVGL-CG-0325 Edition October 2020

Cyber secure

DNV GL AS

FOREWORD

DNV GL class guidelines contain methods, technical requirements, principles and acceptance criteria related to classed objects as referred to from the rules.

Any comments may be sent by e-mail to *rules@dnvgl.com*

This service document has been prepared based on available knowledge, technology and/or information at the time of issuance of this document. The use of this document by others than DNV GL is at the user's sole risk. Unless otherwise stated in an applicable contract, or following from mandatory law, the liability of DNV GL AS, its parent companies and subsidiaries as well as their officers, directors and employees ("DNV GL") for proved loss or damage arising from or in connection with any act or omission of DNV GL, whether in contract or in tort (including negligence), shall be limited to direct losses and under any circumstance be limited to 300,000 USD.

CHANGES – CURRENT

This is a new document.

CONTENTS

SECTION 1 GENERAL

1 Introduction

Recognizing that maritime safety relies on cyber-physical systems that are increasingly integrated with networks and designed with commercial-off-the-shelf (COTS) products, cyber security has become a concern which needs to be specifically addressed. It is no longer considered enough to focus only on reliability and availability of such systems to ensure safety in the maritime industry.

DNV GL class notation **Cyber secure** addresses cyber security by providing requirements and verification of technical barriers, processes and people awareness based on management of cyber risks on board DNV GL classed vessels.

2 Objective

The objectives of this document are to guide owners, yards and manufacturers in implementing the DNV GL class rules for class notation **Cyber secure** and to describe the required content of the cyber security management system (CSMS).

3 Scope

This document describes how to implement DNV GL class notation **Cyber secure** in:

1) newbuilding projects, i.e. construction of new ships or offshore units
2) alteration projects, i.e. modification of ships or offshore units in operation.

4 Application

This document is intended to be applied in conjunction with DNV GL rules for class notation **Cyber secure**.

See design rules for this class notation in DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 and rules for survey requirements in DNVGL-RU-SHIP Pt.7 Ch.1 Sec.6 [41].

5 References

Table 1 DNV GL documents

Document code	*Title*
DNVGL-RU-SHIP Pt.1 Ch.1	General regulations
DNVGL-RU-SHIP Pt.6 Ch.5	Equipment and design features
DNVGL-RU-SHIP Pt.7 Ch.1	Survey requirements for fleet in service
DNVGL-RU-SHIP Pt.4 Ch.9	Control and monitoring systems
DNVGL-RP-0496	Cyber security resilience management for ships and mobile offshore units in operation

Table 2 External documents

Document code	*Title*
IMO MSC.428(98):2017	Maritime cyber risk management in safety management systems
IMO MSC-FAL.1/Circ.3:2017	Guidelines on maritime cyber risk management
ISO/IEC 27001:2017	Information technology, Security techniques, Information security management systems, Requirements
ISO/IEC 27005:2011	Information technology, Security techniques, Information security risk management
ISO/IEC 27035-1:2016	Information technology, Security techniques, Information security incident management, Part 1: Principles of incident management
IEC 62443-1-1:2009	Industrial communication networks, Network and system security, Part 1-1: Terminology, concepts and models
IEC 62443-2-1: 2010	Industrial communication networks, Network and system security, Part 2-1: Establishing an industrial automation and control system security program
ISA/IEC 62443-3-2:2017	Security for industrial automation and control systems Security Risk Assessment, System Partitioning and Security Levels
IEC 62443-3-3:2013	Industrial communication networks, Network and system security, Part 3-3: System security requirements and security levels
IEC 62443-4-2:2019	Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components

6 Definitions and Abbreviations

Table 3 Definitions

Term	*Definition*
compensating countermeasure	countermeasure (e.g. security barrier) in lieu of a required security capability. Provides an alternate and equivalent solution to the stated requirement. The compensating countermeasure shall reduce the cyber risk introduced by the missing required security capability.
information technology	application of computers to store, study, retrieve, transmit and manipulate data, or information, often in the context of a business or other enterprise
operational technology	hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices such as valves, pumps, etc.

Table 4 Abbreviations

Abbreviation	*Description*
BCP	business continuity plan
CAT	customer acceptance test
COTS	commercial off-the-shelf

Abbreviation	*Description*
CSMS	cyber security management system
DP	dynamic positioning
FAL	Convention on Facilitation of International Maritime Traffic
FAT	factory acceptance test
IACS	International Association of Classification Societies
IEC	International Electrotechnical Commission
IMO	International Maritime Organisation
ISA	International Society of Automation
ISO	International Organisation for Standardization
IT	information technology
HAT	harbour acceptance test
MOC	management of change
MSC	Maritime Safety Committee
OT	operational technology
SAT	site acceptance test
SL	security level
SP	security profile
SuC	system under consideration
USB	universal serial bus

SECTION 2 CLASS NOTATION CYBER SECURE

1 Introduction

There are four possible variants of class notation **Cyber secure** as illustrated in Figure 1. Each variant represents a level of cyber risk reduction applied to a defined 'system under consideration', (SuC). The expression 'system under consideration' signifies the cyber-physical systems to be secured. For all variants of the class notation, the same default SuC has ben defined, see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [2.3]. This default SuC may be extended by use of class notation **Cyber secure(+)**, see further description in [4].

The different levels of cyber risk reduction are represented by security profiles (SP) which are further described in [3].

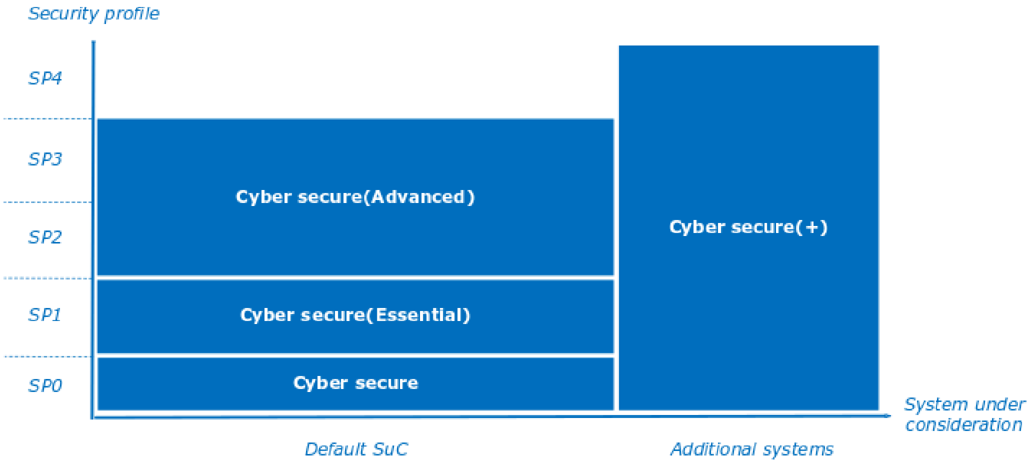

Figure 1 Class notations

2 Risk assessment

2.1 General

IMO resolution MSC.428(98) and guideline MSC_FAL.1/Circ 3 provide high-level recommendations for maritime cyber risk management.

DNV GL class notation **Cyber secure** meets these recommendations both providing a framework for addressing cyber risks on essential ship functions and selected additional systems. In addition to assessing the safety and environmental risk, other risks like financial risk, reputation risk etc. may be taken into consideration.

An initial risk assessment to determine the appropriate **Cyber secure** class notation is described in [2.2] and [2.3].

Risk management in the operational phase is described in Sec.4 [2.4].

For further explanation of the risk management process, see ISA/IEC 62443-3-2.

2.2 Risk assessment of default SuC

DNV GL has pre-selected 11 functions as described in the class rules DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 Table 10 and DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 Table 11. These functions are based on IACS (International Association of Classification Societies) primary essential and secondary essential services. Primary essential services are those services which need to be in continuous operation to maintain propulsion and steering. Secondary essential services are those services which need not necessarily be in continuous operation to maintain propulsion and steering but which are necessary for maintaining the vessel's safety.

The ship owner shall do a cyber security risk assessment to define the needed risk reduction measures for these functions. This needed risk reduction will guide the selection of class notation **Cyber secure**, **Cyber secure(Essential)** or **Cyber secure(Advanced)**, see example in Figure 2. The recommended practice DNVGL-RP-0496 may be used for further guidance on cyber security risk assessment which shall be documented.

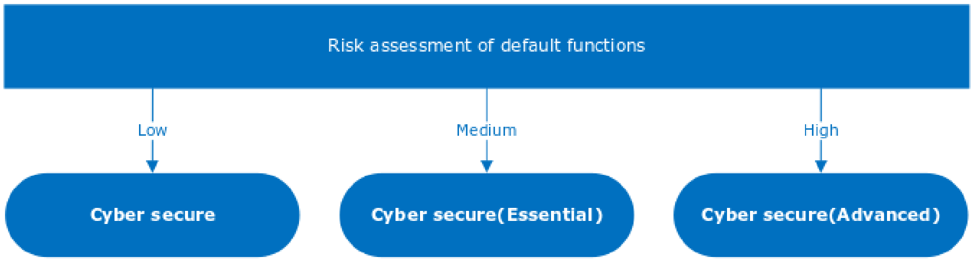

Figure 2 Risk assessment of default SuC

If the risk assessment determines that the 11 functions should have different security profile, the **+** qualifier may be added to the notation. **Cyber secure(+)** may also be used to reach SP2 or SP4, if required. See example in Figure 3.

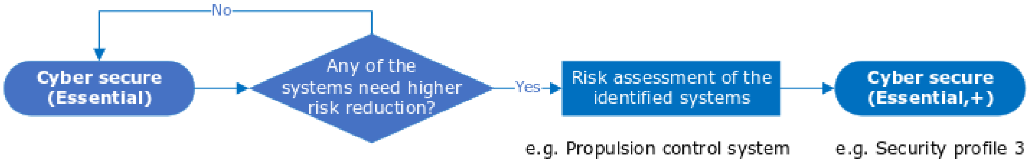
No
Cyber secure (Essential)
Any of the systems need higher risk reduction?
Yes
Risk assessment of the identified systems
Cyber secure (Essential,+)
e.g. Propulsion control system
e.g. Security profile 3

Figure 3 Selected systems in default SuC to have higher SP

2.3 Risk assessment of additional systems

When performing the cyber security risk assessment of the vessel, other systems than the 11 pre-selected may be considered as important for the cyber risk. Such systems should be added in the scope by using **Cyber secure(+)**. For the systems covered by **Cyber secure(+)**, the ship owner shall use the documented risk assessment to define the needed risk reduction measures for these added systems. This risk reduction need will guide the selection of security profile for these systems. See example in Figure 4.

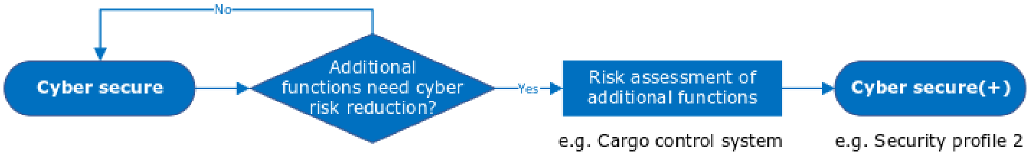
No
Cyber secure
Additional functions need cyber risk reduction?
Yes
Risk assessment of additional functions
e.g. Cargo control system
Cyber secure(+)
e.g. Security profile 2

Figure 4 Risk assessment of additional functions

3 Security profiles

The security level (SL) concept is introduced in the IEC 62443 standard to align the requirements with cyber risk reduction. Security profiles (SP) are intended for different industry/groups sectors or organizations to tailor the selection of requirements to their need. DNV GL has defined five incremental security profiles (SP0 to SP4) and the highest security profile represents the greatest risk reduction.

- Security profile 0 provides an initial level of risk reduction. It focuses on the most prominent security threats and barriers and is considered to meet the intention of MSC.428(98). This security profile is mandatory for class notation **Cyber secure** and constitutes common requirements for all **Cyber secure** notation qualifiers.
- Security profile 1 is based on IEC 62443 security level 1 and provides protection against casual or coincidental cyber threats. This security profile is mandatory for **Cyber secure(Essential)** and may be selected for **Cyber secure(+)**.
- Security profile 2 is based on IEC 62443 security level 2 and provides protection against intentional violation by threat actors possessing low resources and low motivation. This security profile may be selected for **Cyber secure(+)**.
- Security profile 3 is based on IEC 62443 security level 3 and provides protection against intentional violation by threat actors possessing moderate resources and specific OT-system skills. This security profile is mandatory for **Cyber secure(Advanced)** and may be selected for **Cyber secure(+)**.
- Security profile 4 is based on IEC 62443 security level 4 and provides protection against intentional violation by threat actors possessing extended resources, high motivation and specific OT-system skills. This security profile may be selected for class notation **Cyber secure(+)**.

4 System under consideration

4.1 General

The expression 'system under consideration' is a collective term for all cyber-physical systems to be considered in a **Cyber secure** project. Hence, there will always be only one SuC in a project and the SuC will typically consist of many cyber-physical systems, some of which are interconnected, and others may be 'stand-alone'.

4.2 Default SuC

For all **Cyber secure** class notation qualifiers, the SuC will by default consist of the cyber-physical systems providing control, monitoring, alarm and safety functions needed for operation of the functions listed in DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [2.3.1] and DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [2.3.2].

Any systems in the SuC satisfying the criteria in DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [2.2] are considered to represent negligible risk and hence out of scope for verification in the project. The criteria are illustrated by the three questions in Figure 5.

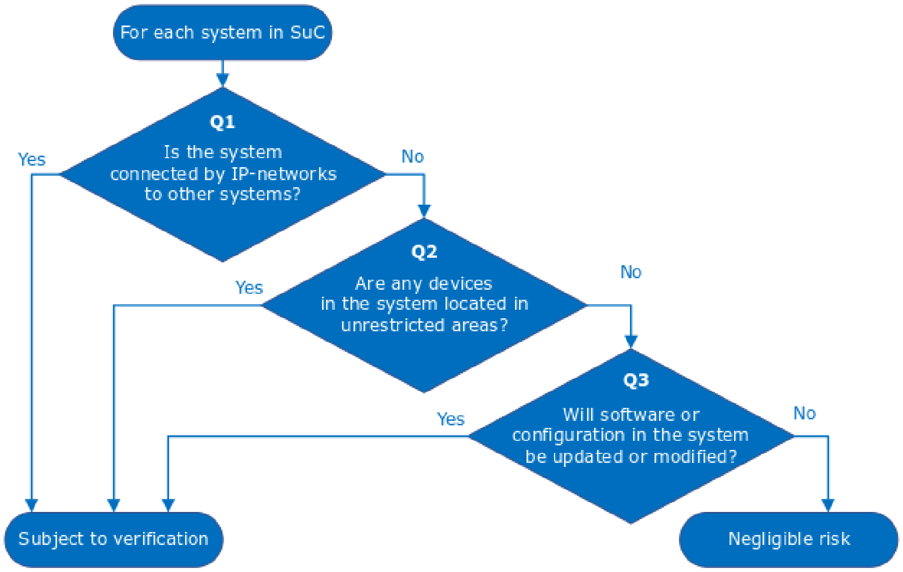
For each system in SuC
Q1
Is the system connected by IP-networks to other systems?
Yes
No
Q2
Are any devices in the system located in unrestricted areas?
Yes
No
Q3
Will software or configuration in the system be updated or modified?
Yes
No
Subject to verification
Negligible risk

Figure 5 Initial system selection

If cyber-physical systems additional to the default SuC shall be included in the class notation project, these shall be added by applying the qualifier **+**.

Table 1 illustrates an example of a project where systems in the default SuC are identified and selected based on cyber security risk.

Table 1 Example of system selection in default SuC

Systems in default SuC	*Q1*	*Q2*	*Q3*	*Selected*
(I) - Propulsion *Systems needed for local and remote control of propulsion*				
1. Main engine control and safety system	Y	N	Y	Selected
2. Gear and clutch control system	N	N	N	
3. Propeller pitch control system	N	N	Y	Selected
4. Propulsion remote control system	Y	N	Y	Selected
5. Integrated automation system	Y	N	Y	Selected
(II) - Steering *Systems needed for local and remote control of vessel direction*				
6. Steering gear control and monitoring system	N	N	N	
(III) - Watertight integrity *Systems required to ensure watertight integrity of the vessel*				

Systems in default SuC	*Q1*	*Q2*	*Q3*	*Selected*
7. Shell door control and monitoring system	N	Y	Y	Selected
8. Internal watertight doors control and monitoring system	N	N	Y	Selected
9. Water ingress detection system	Part of #5			
(IV) Fire protection *Systems required to detect and mitigate fire*				
10. Fire detection and alarm system	Y	N	N	Selected
11. Fire door control system	Part of #10			
12. Engine room fixed fire extinguishing system	N	N	N	
13. Local application fire-fighting system	N	N	Y	Selected
14. Fire pump control system	Part of #5			
(V) Bilge and Ballast *Systems required to carry out ballast and bilge operations*				
15. Bilge and ballast valve control system	N	N	N	
16. Bilge alarms	Part of #5			
(VI) - Auxiliary thrusters *Systems needed to control auxiliary thrusters*				
17. Thruster control and monitoring system	N	N	Y	Selected
(VII) - Electrical power *Systems needed to generate and distribute electrical power*				
18. Auxiliary engine control and safety system	Y	N	Y	Selected
19. Emergency generator engine control and safety system	N	N	N	
20. Battery management system	Y	N	Y	Selected
21. Switchboard protection system	Y	N	Y	Selected
22. Electrical drive control system	N	N	N	
23. Power/energy management system	Part of #5			
(VIII) - Auxiliary services *Systems needed to provide necessary auxiliary services for the essential and important functions*				
24. Control of fuel supply	Part of #5			
25. Control of cooling water	Part of #5			
26. Control of lubrication oil	Part of #5			
27. Control of compressed air	N	N	N	
28. Control of ventilation	Part of #5			
(IX) - Safety *Systems needed to provide required safety functions*				
29. Gas detection system	Part of #5			

Systems in default SuC	*Q1*	*Q2*	*Q3*	*Selected*
30. Ignition source control	Part of #5			
31. Emergency shutdown system	Part of #5			
(X) - Navigation *Systems providing navigational functions required by statutory regulations*				
32. Integrated navigation system (INS)	Y	N	Y	Selected
33. Heading reference	Part of #32			
34. Electronic Chart Display and Information System (ECDIS)	Part of #32			
35. Global Navigation Satellite System (GNSS) receiver	Part of #32			
36. Bridge Navigation Watch Alarm System (BNWAS)	Part of #32			
37. Echo sounder	Part of #32			
38. RADAR	Part of #32			
39. Conning	Part of #32			
40. Speed log	Part of #32			
(XI) - Communication *Systems providing internal and external communication functions required by statutory regulations*				
41. Automatic identification system (AIS)	N	N	N	
42. Two-way voice communication	N	N	N	
43. Public address system	Y	Y	Y	Selected
44. General alarm system	Part of #43			
45. VHF radio	N	N	N	
46. Search and rescue locating device	N	N	N	
47. NAVTEX receiver	N	N	N	
48. INMARSAT radio	N	N	N	
49. Emergency Position Indicating Radio Beacon (EPIRB)	N	N	N	

The final SuC will consist of the default SuC plus any additional systems selected for **Cyber secure(+)** as a result of the risk assessment in [2.3]. To find the systems with negligible risk for these additional systems, a similar exercise as described above should be done.

5 Cyber secure

Class notation **Cyber secure** may be assigned without any qualifiers. The default SuC described in [4.2] will apply. These systems will be subject to the requirements of security profile 0 (SP0) as described in DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [3] as follows:

1) separation of OT-systems into zones and conduits
2) remote access
3) removable devices
4) malware protection

5) incident response
6) cyber security management system (CSMS).

Since this initial-level class notation contains few requirements for system security capabilities, it is considered feasible for any vessel and may be particularly relevant for vessels in operation (alteration projects) which seek to only conform to the guidance in IMO resolution MSC.428(98) and MSC_FAL.1/Circ 3. See illustration in Figure 6.

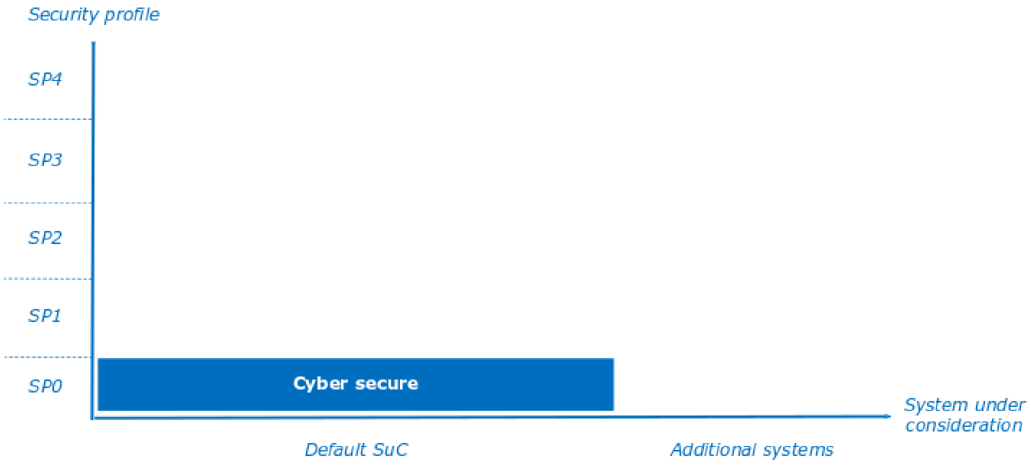

Figure 6 Cyber secure

6 Cyber secure(Essential)

Class notation **Cyber secure(Essential)** includes the initial-level notation **Cyber secure** and in addition increases the level of risk reduction to security profile 1 for the default SuC, see Figure 7.

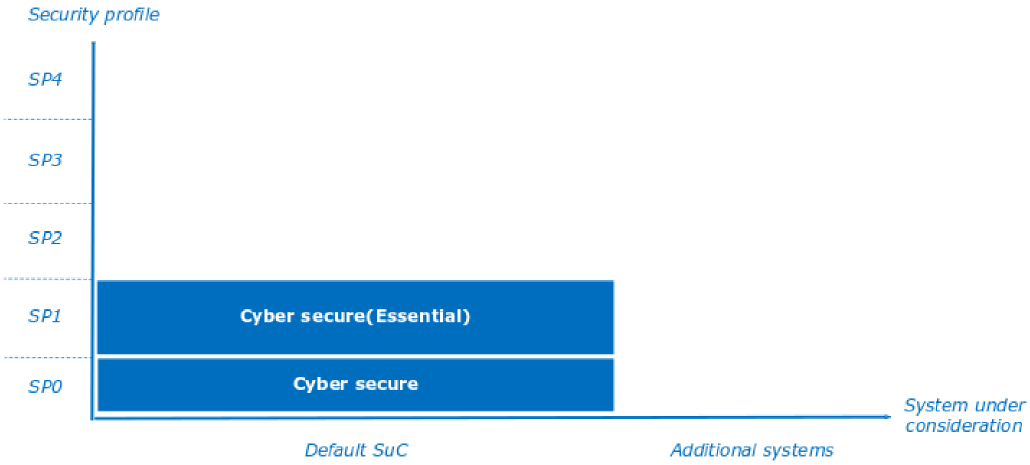

Figure 7 Cyber secure(Essential)

7 Cyber secure(Advanced)

Class notation **Cyber secure(Advanced)** includes the initial-level notation **Cyber secure** and in addition increases the level of risk reduction to security profile 3 for the default SuC, see Figure 8.

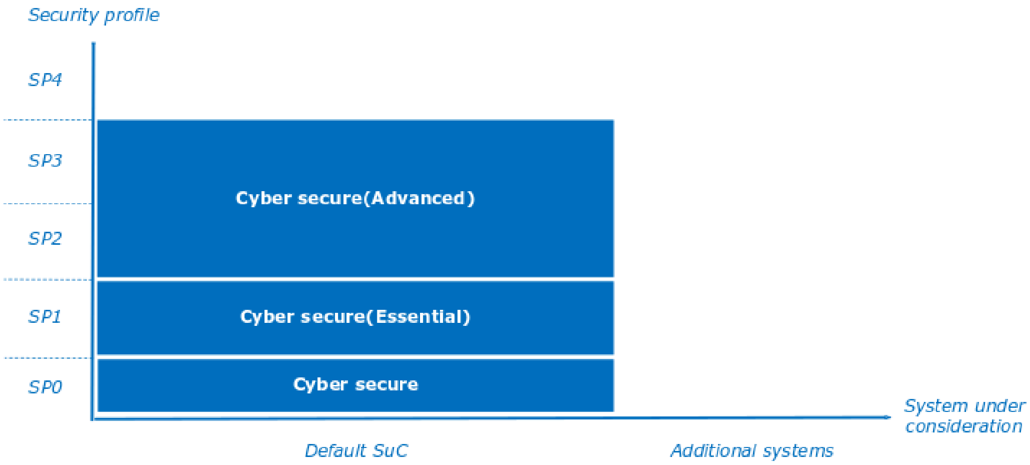

Figure 8 Cyber secure(Advanced)

8 Cyber secure(+)

Class notation **Cyber secure (+)** intends to offer flexibility, both with respect to system under consideration and risk reduction level.

This class notation includes the initial-level notation **Cyber secure** and in addition allows for an increased level of risk reduction for selected/chosen systems. The chosen systems may be part of the systems in scope for **Cyber secure(Essential)** or **Cyber secure(Advanced)** or other systems such as industrial-purpose systems listed in DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [2.3.3]. The chosen systems and corresponding security profile will be listed in the vessel's appendix to the class certificate, see DNVGL-RU-SHIP Pt.1 Ch.1 Sec.2 [3.1.5].

Examples of class notation **Cyber secure(+)** are illustrated from Figure 9 to Figure 12.

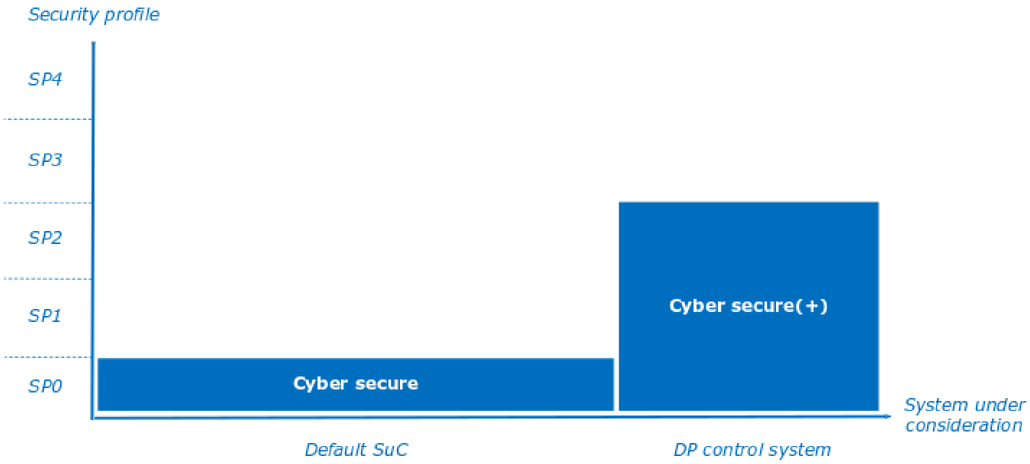

Figure 9 Cyber secure(+) for the DP control system

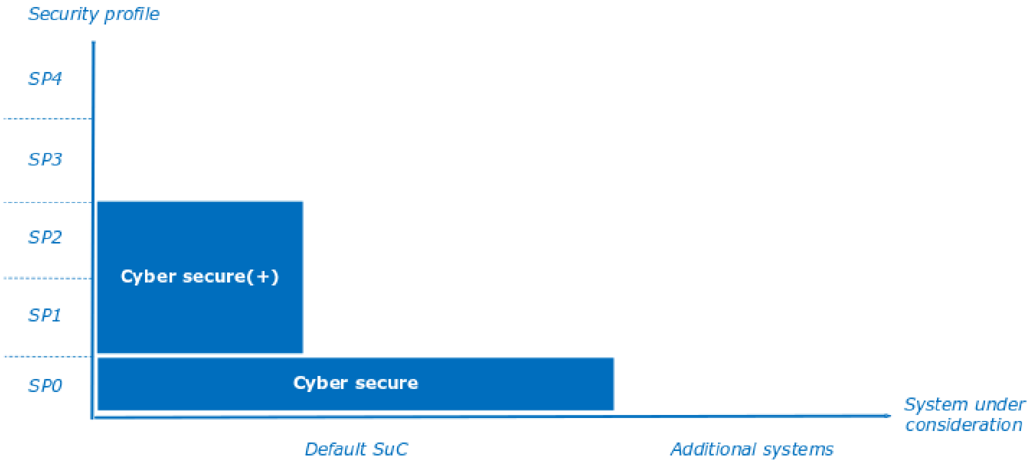

Figure 10 Cyber secure(+) where some systems in default SuC shall achieve SP2

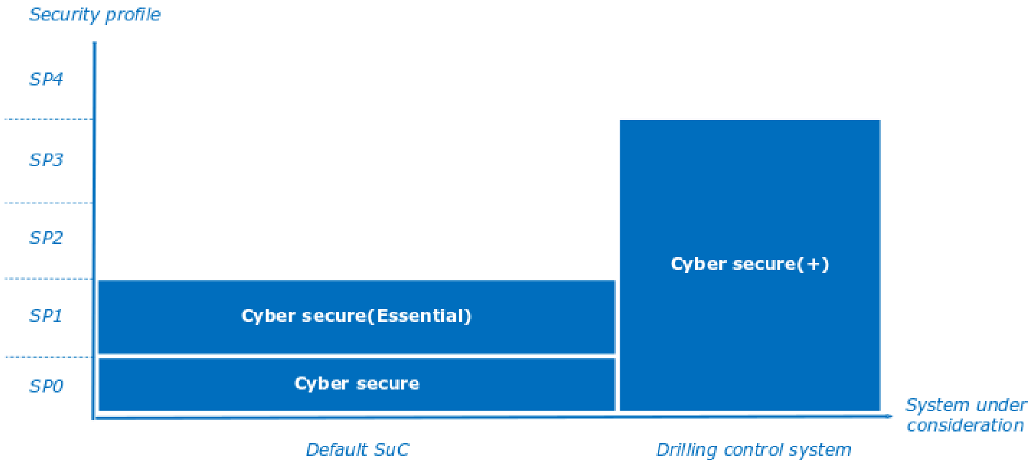

Figure 11 Cyber secure(Essential, +) where drilling control system is added to SuC at SP3

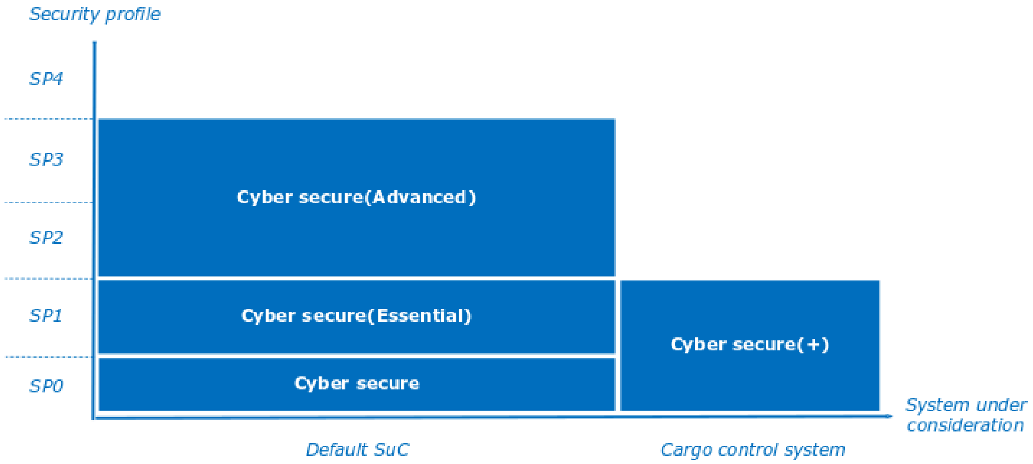

Figure 12 Cyber secure(Advanced, +) where cargo control system is added to SuC at SP1

SECTION 3 IMPLEMENTATION

1 Introduction

This section describes how to implement DNV GL class notation **Cyber secure** in newbuilding and alteration projects.

2 Newbuilding projects

2.1 Roles

The following roles take part in a newbuilding project:

- owner: company which will own the vessel/unit after delivery from the shipyard. If another company will operate the vessel after delivery, the cyber security management system will be operated by this operator.
- integrator: company responsible for high-level design and integration of systems on board. This role is typically performed by the shipyard.
- supplier: company supplying cyber-physical systems and components that is part of the SuC.
- verifier: DNV GL maritime classification is the independent party to verify compliance with the rules for class notation **Cyber secure**.

Further description of roles and activities are given in the following subsections.

2.2 Project phases

A **Cyber secure** project should be executed as per the phases and main activities in Table 1. It is assumed that before start of high-level design, the class notation has been decided as described in Sec.2 [2].

Table 1 Newbuilding project phases and documentation

High-level design	*System design*	*Construction*	*Acceptance*	*Operation*
Integrator activities: Define cyber-physical systems in SuC according to DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [2] and Sec.2 [4.2]. Define zones and conduits according to DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [3.1].	*Supplier activities*: Design each system in the SuC according to technical security requirements in DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4].	*Integrator activities*: Produce, install and commission the systems.	*Integrator activities*: Test each system in SuC for compliance with technical security requirements. Test the complete integrated SuC for compliance with technical security requirements.	*Owner activities*: Operate the SuC in accordance with the approved cyber security management system.

High-level design	*System design*	*Construction*	*Acceptance*	*Operation*
Integrator documentation: Submit zones and conduit diagram (I101) as per DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 Table 7. Submit cyber security design philosophy (Z102) as per DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 Table 7.	*Supplier documentation*: Submit cyber security system documentation in DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 Table 8 as part of documents required for product certification by main class rules, e.g. DNVGL-RU-SHIP Pt.4 Ch.9 Sec.1 Table 5.	*Integrator documentation*: Submit test procedures for acceptance testing of each system in SuC (Z253) as per DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 Table 9. Submit integration test procedure (Z256) as per DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 Table 9.	*Integrator documentation*: Submit inventory list of system in SuC (I071) as per DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 Table 7.	*Owner documentation*: Submit cyber security management system documentation as per DNVGL-RU-SHIP Pt.7 Ch.1 Sec.6 [41.2.2].

2.3 High-level design

The activities in Table 2 should be done in the high-level design phase.

Table 2 High-level design activities

Role	*Activities*
Owner	Contribute to the integrator's design activities by informing about risk assessments forming the basis for selection of class notation. Specifically, the integrator shall be informed of SuC, SP and desired class notation, see Sec.2 [2].
Integrator	The following high-level design activities should take into account contribution by owner and suppliers: Conclude definition of system under consideration by identifying systems with negligible risk. See Sec.2 [4] and DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [2.2]. Make zone and conduit diagram in accordance with requirements for zones, conduits, network segmentation and zone boundary protection in the rules. See DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [3.1], DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.6.2], and DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.6.3]. Produce cyber security design philosophy. The document should specify security profile for each system and zone in the SuC and how to design the systems to comply with the common requirements in the rules (i.e. zones, conduits, remote access, removable devices, malware protection and incident handling as per DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [3]). Compensating countermeasures in the event of any known non-compliances should also be described in the cyber security design philosophy. The cyber security design philosophy shall describe how each system in the SuC complies with applicable requirements. For details, the design philosophy may refer to explicit parts of the system documentation by the suppliers (see Table 3).
Supplier	Contribute to cyber security design philosophy by informing integrator about security capabilities and best practices. See also DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.8.7].
Verifier	Verify zone and conduit diagram and cyber security design philosophy for compliance with applicable security requirements.

2.4 System design

The activities in Table 3 should be done in the system design phase.

Table 3 System design activities

Role	*Activities*
Owner	Cooperate with integrator to ensure design of security barriers are consistent with operational principles.
Integrator	Ensure suppliers are informed of high-level design and security requirements for the selected class notation. Follow-up system design by suppliers and revise high-level design if needed.
Supplier	Design the systems in accordance with integrator's cyber security design philosophy and applicable technical security requirements for the class notation / security profile. See DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4]. Produce system design documentation with the objective to describe compliance with technical security requirements. This documentation should be submitted as part of required system documentation for DNV GL product certification. See DNVGL-RU-SHIP Pt.4 Ch.9 Sec.1 Table 5. For systems that have been type approved as per DNVGL-CP-0231, the security capabilities are generally not required to be submitted for approval (this will be stated in the type approval certificate).
Verifier	Assess system test procedures for satisfactory test coverage and methods to demonstrate applicable security requirements.

2.5 Construction

The activities in Table 4 should be done in the construction phase.

Table 4 Construction activities

Role	*Activities*
Owner	Cooperate with integrator to ensure design of security barriers are consistent with operational principles.
Integrator	Ensure secure installation and commissioning of the systems. Request suppliers to produce test procedure for the systems and submit test procedures for all systems in the SuC in one compiled transmittal to DNV GL. The test procedures should demonstrate compliance with technical security requirements in DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4].
Supplier	Produce test procedures for each system in the SuC to demonstrate compliance with security requirements of the class notation. Produce integration test procedure and submit to DNV GL for approval. Before the systems are delivered to the shipyard, ensure the software is updated and provide the following to the integrator: system inventory documentation, manuals/kits for security patching, backup and restore. Ensure secure transportation of the system to the shipyard.
Verifier	Assess test procedures for satisfactory test coverage and methods to demonstrate applicable security requirements.

2.6 Acceptance

The activities in Table 5 should be done in the acceptance phase.

Table 5 Acceptance activities

Role	*Activities*
Owner	Participate in system testing and integration testing, and gain knowledge of system security mechanisms.
Integrator	During normal test activities on board (e.g. SAT/HAT/CAT), perform cyber security system testing in cooperation with respective suppliers. The integrator may agree with suppliers to perform system testing at the manufacturer's location as part of factory acceptance test (FAT) for DNV GL product certification of the control system. In such case, specific agreements should be made since this will extend the scope of FAT. When all system in the SuC are integrated and finalized on board, facilitate integration testing to demonstrate compliance with security requirements of the class notation. The results from all tests should be recorded and signed by involved parties.
Supplier	Contribute in system testing and integration testing as needed.
Verifier	Witness system and integration testing. Assess documentation of test results.

2.7 Operation

The activities in Table 6 should be done in the operation phase.

Table 6 Operation activities

Role	*Activities*
Owner	Establish and submit cyber security management system (CSMS) for approval. Align the CSMS with the design philosophy, roll out implementation activities (e.g. training), operate and maintain the CSMS. See Sec.4 for guidance to content of CSMS.
Supplier	Ensure that systems are updated with security patches as per agreement with owner and in accordance with cyber security management system (CSMS).
Verifier	Assess CSMS for compliance with requirements in DNVGL-RU-SHIP Pt.7 Ch.1 Sec.6 [41] and Sec.4. Within first year of operation, audit implementation and adherence to CSMS.

3 Alteration projects

3.1 General

The following implementation guidelines should be used for alteration projects where the systems constituting the SuC are not intended to undergo major re-design or upgrades. In such alteration projects it is assumed that the owner assumes the role as integrator. For alteration projects where major re-design- or upgrades are needed, the implementation activities for newbuilding projects in [2] may be more suitable.

3.2 Roles

The following roles take part in an alteration project:

- Owner: company which owns the vessel/unit. If another company operates the vessel, the cyber security management system will be operated by this operator.
- Integrator: company responsible for high-level design and integration of systems on board. This role is typically performed by the shipyard in large alteration projects, and may not be needed for smaller alterations.
- Supplier: company which has supplied the cyber-physical systems and components that is part of the SuC.
- Verifier: DNV GL Maritime Classification is the independent party to verify compliance with the rules for class notation **Cyber secure**.

Further description of roles and activities are given in the following subsections.

3.3 Project phases

A **Cyber secure** project should be executed as per the phases and main activities in Table 7. It is assumed that before start of high-level design, the class notation has been decided as described in Sec.2 [2].

Table 7 Alteration project phases and documentation

High-level design	*System re-design*	*Modifications*	*Acceptance*	*Operation*
Owner activities: Define cyber-physical systems in SuC according to DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [2] and Sec.2 [4.2]. Document existing zones and conduits and define alterations and/or compensating countermeasures to meet requirements in DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [3.1].	*Supplier activities*: Identify gaps between existing system capabilities and technical security requirements in DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4]. Re-design systems if needed and/or define compensating countermeasures.	*Owner activities*: Modify the systems, if needed, and/or implement compensating countermeasures.	*Owner activities*: Test each system in SuC for compliance with technical security requirements. Test the complete integrated SuC for compliance with technical security requirements.	*Owner activities*: Operate the SuC in accordance with the approved cyber security management system.

High-level design	*System re-design*	*Modifications*	*Acceptance*	*Operation*
Owner documentation: Submit zones and conduit diagram (I101) as per DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 Table 7.	*Owner documentation*: Submit cyber security design philosophy (Z102) as per DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 Table 7. Submit documentation of system modifications as relevant.	*Owner documentation*: Submit test procedures for acceptance testing of each system in SuC (Z253) as per DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 Table 9. Submit integration test procedure (Z256) as per DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 Table 9.	*Owner documentation*: Submit inventory list of system in SuC (I071) as per DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 Table 7.	*Owner documentation*: Submit cyber security management system documentation as per DNVGL-RU-SHIP Pt.7 Ch.1 Sec.6 [41.2.2].

3.4 High-level design

The activities in Table 8 should be done in the high-level design phase.

Table 8 High-level design activities

Role	*Activities*
Owner	The high-level design should start after SuC, SP and the appropriate **Cyber secure** class notation has been determined, See Sec.2 [2] Conclude definition of SuC by identifying systems with negligible risk. See Sec.2 [4] and DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [2.2]. Document topologies and interfaces of the existing cyber-physical system in the SuC (i.e. document existing zones and conduits). Identify gaps between the existing zones/conduits and the requirements in DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [3.1]. Design alterations and compensating countermeasures (i.e. segmentation of networks and installation of zone boundary protection).
Supplier	Contribute to cyber security design philosophy by informing owner about security capabilities and best practices. See also DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.8.7].
Verifier	Verify zone and conduit diagram for compliance with applicable security requirements.

3.5 System re-design

The activities in Table 9 should be done in the system re-design phase.

Table 9 System re-design activities

Role	*Activities*
Owner	Produce cyber security design philosophy. For an alteration project, this document should serve as requirement specifications for any needed system modifications and document how the systems will comply with the applicable requirements. There are mainly three alternative ways to achieve compliance: — The system has the required security capabilities. — The system will be modified to have the required security capabilities. — The system is lacking one or more required security capabilities and compensating countermeasures are proposed. Consequently, a comprehensive gap analysis should be carried out for all systems in the SuC considering both common requirements in DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [3] and technical security requirements in DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4]. The cyber security design philosophy should, for each system and each applicable requirement, document compliance by either of the three ways listed above.
Supplier	Support as needed and agreed with owner.
Verifier	Verify cyber security design philosophy for compliance with applicable security requirements.

3.6 Modifications

The activities in Table 10 should be done in the modification phase.

Table 10 Modification activities

Role	*Activities*
Owner	When the cyber security philosophy document has been approved, the specified modifications should be done. Modifications to a system in the SuC should be carried out by qualified personnel (typically by the supplier) and the owner shall ensure that management of change (MOC) procedures are followed. Major changes to certified systems should be documented/submitted to DNV GL. See DNVGL-RU-SHIP Pt.7 Ch.1 Sec.2 [3.1.6] and DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [5.4]. Updated system documentation should be available on board. Any revisions to zone and conduit diagram or cyber security design philosophy should be submitted to DNV GL. Ensure that combined test procedure for system testing and integration testing is written and submitted to verifier. The procedure should demonstrate compliance with security requirements of the class notation.
Supplier	Support and perform modifications as agreed with owner.
Verifier	Verify MOC-records and any revised documents. Assess test procedure for satisfactory test coverage and methods to demonstrate applicable security requirements.

3.7 Acceptance

The activities in Table 11 should be done in the acceptance phase.

Table 11 Acceptance activities

Role	*Activities*
Owner	Perform the combined cyber security system testing and integration testing in cooperation with respective suppliers, if needed. The results from all tests should be recorded and signed by involved parties.
Supplier	Contribute in system testing and integration testing as requested and agreed with the owner.
Verifier	Witness system and integration testing. Assess documentation of test results.

3.8 Operation

The activities in Table 12 should be done in the operation phase.

Table 12 Operation activities

Role	*Activities*
Owner	Establish and submit cyber security management system (CSMS) for approval. Align the CSMS with the design philosophy, roll out implementation activities (e.g. training), operate and maintain the CSMS. See Sec.4 for guidance to content of CSMS.
Supplier	Ensure that systems are updated with security patches as per agreement with owner and in accordance with cyber security management system (CSMS).
Verifier	Assess CSMS for compliance with requirements in DNVGL-RU-SHIP Pt.7 Ch.1 Sec.6 [41] and Sec.4. Within first year of operation, audit implementation and adherence to CSMS.

SECTION 4 CYBER SECURITY MANAGEMENT SYSTEM (CSMS)

1 Introduction

1.1 General

In the context of class notation **Cyber secure**, the cyber security management system (CSMS) is a program implemented by the operator of the ship/offshore unit to govern the activities related to cyber security of the system under consideration. The term CSMS normally applies for OT-systems, whereas the corresponding security program for an IT-system is often referred to as information security management system, see ISO/ IEC 27001.

The CSMS should be coordinated with- or part of other vessel management systems, e.g. safety management system, quality management system, information security management system.

This section includes requirements and guidance to the cyber security management system.

1.2 Purpose of the CSMS

It is recognized that a complete cyber security framework relies on a cyber security management system (CSMS) that governs behaviour of people and specifies principles for the functionality of technical security barriers. Hence, as illustrated in Figure 1, people, process and technology are often called 'the three main pillars of cyber security'.

The CSMS shall provide a framework for governing human activities and behaviour based on policies and procedures. The CSMS shall also ensure that cyber security risks are adequately and systematically managed, i.e. that the risks are identified, evaluated and mitigated to a tolerable level.

Mitigation of the risks is achieved by implementing barriers (countermeasures). Barriers may be technical (such as network segmentation) or organisational (such as awareness training or procedures).

Most technical barriers are not feasible unless supported and managed by policies or procedures in the CSMS (e.g. roles and responsibilities shall be defined before user accounts and privileges are configured in a control system).

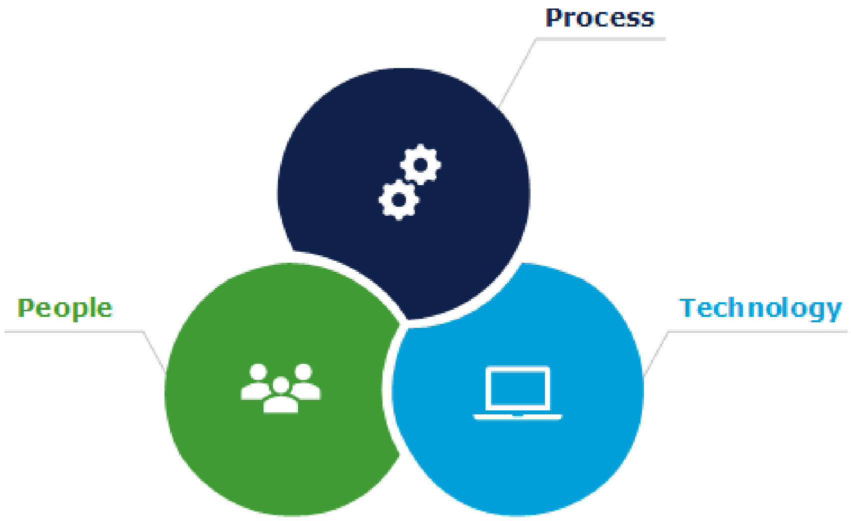

Figure 1 People, process and technology

1.3 Assignment and retention of the class notation

Class notation **Cyber secure** will be assigned after the design documents have been approved, and after system- and integration tests have been accepted, see Sec.3. To maintain the class notation, the cyber security management system (CSMS) shall be audited by DNV GL, see DNVGL-RU-SHIP Pt.7 Ch.1 Sec.6 [41.2]. The audit will consist of verification that CSMS includes the required content and that the policies and procedures in the CSMS are adhered to (i.e. by producing records, logs or other traceable evidence). Audit of CSMS shall also be carried out in annual and complete surveys as specified in DNVGL-RU-SHIP Pt.7 Ch.1 Sec.6 [41].

2 CSMS content

2.1 General

The CSMS shall include policies, procedures and records covering at least the requirements described in the following subsections. For a compiled list, see App.A.

Each requirement is accompanied with guidance notes providing the following information, as relevant:

- supplementary guidance
- reference to related section in ISO/IEC 27001
- reference to related section in IEC 62443-2-1
- reference to related technical security capabilities in DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 and IEC 62443-3-3.

2.2 Scope

A formal written scope for the cyber security management system shall exist.

Guidance note:

- The information, systems and vessel services that are protected by the technical and organizational security barriers should be identified. Identify also personnel and organizations that are expected to follow policies and procedures in the CSMS. The intention is to ensure relevant stakeholders understand and agree on boundaries of the CSMS.
- See ISO/IEC 27001 section 4.3: *Determining the scope of the information management security management system*
- See IEC 62443-2-1 section 4.3.2.2: *CSMS scope*.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2.3 Policies and procedures

The CSMS shall include policies stating security objectives and procedures describing how to achieve them. Records, logs or other documented evidence of adherence to the policies shall be generated and stored.

Guidance note:

- The policies and procedure should govern the activities related to cyber security. Note that security policies define overall principles needed to specify configuration of technical security capabilities in the system under consideration (SuC).
- See ISO/IEC 27001:
  - section 5.2: *Policy*
  - section 6.2: *Information security objectives and planning to achieve them*
  - clause A.5.1.1: *Policies for information security*
  - clause A.12.1.1: *Documented operating procedures*
- See IEC 62443-2-1 section 4.3.2.6: *Security policies and procedures*
- See ISM Code section 2: *Safety and Environmental Protection Policy*.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2.4 Risk management

The CSMS shall include a framework for managing cyber security risks. The risk management process shall be documented, and the actions shall be traceable.

Guidance note:

- The risk management process should include the activities illustrated in **Figure 2**.
  - Identification of threats and vulnerabilities requires that a detailed inventory of the systems in the SuC is kept up to date and that security-related configuration is maintained and documented. E.g. hardware devices and operating systems, software applications and versions, firewall settings, etc. This inventory information is then evaluated based on updated threat and vulnerability information, typically provided by subscribing to advisory/alert services by manufacturers and other specialized organizations providing cyber security alerts, warnings and response services. See also https://en.wikipedia.org/wiki/Computer_emergency_response_team.
  - The identified risks should be analysed to determine potential consequences and realistic likelihood of occurrence. See e.g. the 'ease of access method' described in DNVGL-RP-0496.
  - Evaluation of the risks entails comparing the consequences with established acceptance criteria and setting priorities for risk treatment. The risks may entail different consequences for confidentiality, integrity and availability and there may be different acceptance criteria for these properties.
  - Treatment of risks implies management of technical and/or organizational barriers in accordance with the determined consequences and priorities. This means risks may be treated by applying barriers at different levels in the defense-in-depth model (e.g. policies/procedures, zones/conduits, or system security functions). Risk treatment may also entail implementing preventive barriers and/or responsive barriers. In principle, there are four options for risk treatment as follows:

    1) reduce likelihood and/or consequence of risk
    2) omit the risk
    3) transfer the risk
    4) accept the risk.

    Examples of risk treatment may be e.g. installing security patches, updating antivirus signature files or initiating security awareness training for personnel.
- See DNVGL-RP-0496
- See ISO/IEC 27001:
  - section 6.1.2: *Information security risk assessment*
  - section 6.1.3: *Information security risk treatment*
  - section 8.2: *Information security risk assessment in operation*
  - section 9.1: *Monitoring, measurement, analysis and evaluation*
  - section 10.1: *Nonconformity and corrective action*
  - clause A.12.6.1: *Management of technical vulnerabilities*
- See ISO/IEC 27005: *Information technology - Security techniques - Information security risk management*
- See IEC 62443-2-1: section 4.2.3: *Risk identification, classification and assessment*

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

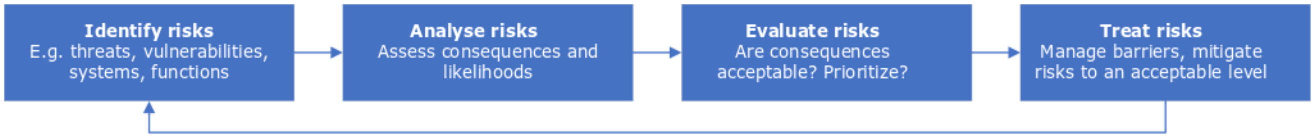
Identify risks
E.g. threats, vulnerabilities, systems, functions
Analyse risks
Assess consequences and likelihoods
Evaluate risks
Are consequences acceptable? Prioritize?
Treat risks
Manage barriers, mitigate risks to an acceptable level

Figure 2 Risk management

2.5 Management support

The vessel captain and other relevant management roles on board shall demonstrate ownership and knowledge of the CSMS.

Guidance note:

- See ISO/IEC 27001:
  - section 5.1: *Leadership and commitment*
  - section 9.3: *Management review*
- See IEC 62443-2-1: section 4.3.2.3: *Organizing for security*

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2.6 System documentation

Documentation of the systems in the SuC shall be kept up to date, protected from unauthorized access and be available on board.

Guidance note:

- the system documentation should typically include:
  - cyber security design philosophy/specification
  - a complete inventory of all devices, hardware components, software components and communication protocols/ports used in the systems
  - physical and logical network topology diagrams
  - configured parameters and settings in the SuC
  - relevant product documentation describing security capabilities, location of equipment, configuration guidelines and recommendations, etc.
  - test procedures and records.
- see ISO/IEC 27001:
  - clause A.8.1.1: *Inventory of assets*
  - clause A.8.2.1: *Classification of information*
- see IEC 62443-2-1:
  - section 4.3.4.4: *Information and document management*
  - section 4.2.3.5: *Network diagrams*
- see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [1.8] *Documentation requirements*
- see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.8.7] (IEC 62443-3-3 SR 7.6) *Network and security configuration*
- see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.8.9] (IEC 62443-3-3 SR 7.8) *Control system component inventory*
- see ISM Code section 3: *Company Responsibilities and Authority*
- see ISM Code section 4 *Designated Person(s)*.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2.7 Roles and responsibilities

Responsibilities for security-related activities shall be defined and documented. This includes responsibilities assigned to personnel on board as well as external parties (e.g. contractors, suppliers, consultants).

Guidance note:

- examples of security-related activities are:
  - grant physical access to locations on board
  - communicate security awareness information
  - conduct security-related training and drills
  - manage accounts, authorizations and password policies
  - manage changes to hardware and software
  - update software/patches
  - update malware protection
  - perform backup/restore
  - respond to incidents
- see ISO/IEC 27001: clause A.6.1.1 *Information security roles and responsibilities*
- see IEC 62443-2-1: section 4.3.2.3.3 *Define organizational responsibilities*
- see ISM Code section 6 *Resources and Personnel*.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2.8 Personnel security

Policies and procedures shall be developed to ensure that employees and other personnel on board are informed about appropriate behaviour to maintain the security objectives.

Guidance note:

- The policies should include expectations, responsibilities and describe the disciplinary process in case the policies are breached. Visiting personnel such as contractors, suppliers and passengers should be included as appropriate. Examples of aspects to be addressed are:
  - management of IT-equipment brought on board by crew, passengers, suppliers, etc.
  - access to confidential information
  - use of email
  - use of web services
  - private use of corporate devices
  - responsibilities related to reporting of theft, illegal disclosure of information or other breaches of policy
  - contractual obligations of employees after termination of employment
- see ISO/IEC 27001:
  - clause A.7.1.2: *Terms and conditions of employment*
  - clause A.8.1.3: *Acceptable use of assets*
  - clause A.15.1.1: *Information security policy for supplier relationships*
- see IEC 62443-2-1: section 4.3.3.2: *Personnel security*.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2.9 Competence

All personnel on board shall receive security awareness training.

Guidance note:

- Specific training should be conducted for all roles having been assigned responsibility for security-related activities. The training should be relevant/updated and be conducted periodically. Visiting personnel such as contractors, suppliers and passengers should be included as appropriate.
- See ISO/IEC 27001: clause A.7.2.2: *Information security awareness, education and training.*
- See IEC 62443-2-1: section 4.3.2.4: *Staff training and security awareness.*
- See ISM Code section 6: *Resources and personnel.*

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2.10 Network segmentation

Policies for segregation or segmentation of networks shall be established.

Guidance note:

- the principles for zones, conduits and network segmentation should be described in a policy. Examples that should be addressed are:
  - segmentation of the different zones (logical, physical, air-gap). Examples: IT, OT, bridge, safety systems, wireless systems
  - segmentation of system within the zones (if applicable). Examples: Redundant systems, systems by different manufacturers
  - boundary protection principles, usage and type of firewalls. Examples: packet filtering, stateful inspection, proxy/application-level firewall, software firewall.
- see ISO/IEC 27001: clause A.13.1.3: *Segregation in networks*
- see IEC 62443-2-1: section 4.3.3.4: *Network segmentation*
- see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [3.1] *Zones and conduits*
- see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.6.2] (IEC 62443-3-3 SR 5.1) *Network segmentation*
- see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.6.3] (IEC 62443-3-3 SR 5.2) *Zone boundary protection*
- see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.6.5] (IEC 62443-3-3 SR 5.4) *Application partioning*
- see DNVGL-RU-SHIP Pt.4 Ch.9 Sec.4 [3.1.2] *Control system networks and data communication links*.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2.11 Access control

Policies and procedures for access control shall be established.

Guidance note:

- the policies should provide a basis for configuration of required technical security capabilities related to identification, authentication and use control, and should cover at least the following:
  - human user access (management of accounts, identifiers, authenticators and privileges)
  - access by software processes and wireless devices
  - access from other zones and from untrusted networks, including remote connections and export of data
- see ISO/IEC 27001 clause A.9:*Access control*
- aee IEC 62443-2-1:
  - section 4.3.3.5 *Access control – Account administration*
  - section 4.3.3.6 *Access control – Authentication*
  - section 4.3.3.7 *Access control – Authorization*
- see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.2] (IEC 62443-3-3 FR 1) *Identification and authentication*
- see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.3] (IEC 62443-3-3 FR 2) *Use control*.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2.12 Removable or portable devices

Policies and procedures for secure use of removable or portable devices such as USB memory sticks and portable computers shall be established.

Guidance note:

— see ISO/IEC 27001 clause A.8.3.1 *Management of removable media*

— see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [3.3] *Removable devices*

— see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.3.4] (IEC 62443-3-3 SR 2.3) *Use control of portable and mobile devices*.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2.13 Malware protection

Policies and procedures for protecting the systems from malware shall be established.

Guidance note:

— see ISO/IEC 27001 clause A.12.2.1 *Controls against malware*

— see IEC 62443-2-1 section 4.3.4.3.7 *Establish and document antivirus/malware management procedure*

— see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [3.4] *Malware*

— see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.4.3] (IEC 62443-3-3 SR 3.2) *Malicious code protection*.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2.14 Security patches

The systems in the SuC shall be kept updated with security patches in accordance with defined policies. The patch-status shall be documented and kept up to date.

Guidance note:

— authenticity, integrity and compatibility of the security patches should be ensured. Any systems that are not kept updated with security patches should be justified by documented compensating countermeasures

— see ISO/IEC 27001:

  — clause A.11.2.4 *Equipment maintenance*

  — clause A.12.6.1 *Management of technical vulnerabilities*

— see IEC 62443-2-1 section 4.3.4.3.7 *Establish and document a patch management procedure*

— see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [5.4] *Alterations and additions of approved systems*

— see IEC 62443-4-2 CR 3.10 *Support for updates*

— see ISM Code section 10 *Maintenance of the ship and equipment*.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2.15 Physical security

Policies, procedures and other relevant documentation addressing physical security of the SuC shall be established.

Guidance note:

- the following are relevant examples to address:
  - workstations located in control rooms. These are typically always accessible by operators without need for identification and authentication. Means to restrict access in case the control room is unattended should be addressed.
  - computers located in locked rooms (e.g. instrument rooms). If such devices can be used without need for identification and authentication, other means to monitor and control access should be addressed
  - computers with processes running with administrator rights. Physical barriers to compensate for the "least privilege principle" should be addressed
- see ISO/IEC 27001 clause A.11 *Physical and environmental security*
- see IEC 62443-2-1 section 4.3.3.3 *Physical and environmental security*
- see ISPS Code.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2.16 Information classification

Policies and procedures shall be established to define, label and manage classified information

Guidance note:

- see ISO/IEC 27001 clause A.8.2 *Information classification*
- see IEC 62443-2-1 section 4.3.4.4.2 *Define information classification levels*
- see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.5.2] (IEC 62443-3-3 SR 4.1) *Information confidentiality*
- see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.5.3] (IEC 62443-3-3 SR 4.2) *Information persistence*
- see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.5.4] (IEC 62443-3-3 SR 4.3) *Use of cryptography*
- see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.4.10] (IEC 62443-3-3 SR 3.9) *Protection of audit information*.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2.17 Change management

Modifications to the SuC shall be carried out in accordance with approved management of change (MoC) procedures.

Guidance note:

- see ISO/IEC 27001:
  - clause A.12.1.2 *Change management*
  - clause A.14.2 *Security in development and support processes*
- see IEC 62443-2-1 section 4.3.4.3.2 *Develop and implement a change management system*
- see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [5.4] *Alterations and additions of approved systems*
- see DNVGL-RU-SHIP Pt.4 Ch.9 Sec.1 [1.5] *Software and hardware change handling*
- see DNVGL-RU-SHIP Pt.7 Ch.1 Sec.2 [3.1.6] *Annual surveys extent – main class, machinery and systems*
- see ISM Code section 10 *Maintenance of the ship and equipment*.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2.18 Detection of anomalies

Policies and procedures for identifying security anomalies shall be established.

Guidance note:

- detection of anomalies includes e.g.:
  - logging of security events
  - audit of security event records
  - detection of failed security controls/barriers
  - detection of attempted, failed or successful security breaches
- see ISO/IEC 27001 clause A.12.4 *Logging and monitoring*
- see IEC 62443-2-1 section 4.3.4.5.7 *Identify failed and successful cyber security breaches*
- see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.4.4] (IEC 62443-3-3 SR 3.3) *Security functionality verification*
- see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.3.9] (IEC 62443-3-3 SR 2.8) *Auditable events*.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2.19 Incident response

The organization and the cyber-physical systems shall be capable of responding to- and recovering from cyber incidents.

Guidance note:

- an incident response and recovery plan may be summarized as follows:
  1) create a policy which includes:
     - the purpose, objectives and scope
     - policy owner and review cycle
     - definition of security incident
     - description of security incidents and categories
     - description of incident reporting
     - high-level overview or visualization of incident management process flow
     - definition of roles, responsibilities and decision-making authority
  2) create a plan describing detailed activities, procedures and other necessary information:
     - planning and preparation (event categorisation, escalation procedures, logging of incident handling, procedures for testing, contact information)
     - detection and reporting (collecting information related to the event)
     - response (procedures to: reduce consequences of the incident, recover from event and carry out forensics
     - lessons learned (reviewing and improving security barriers and incident response plans)
  3) create an incident response team, including establishing relationship to other organisations (CERTs, regulatory authorities, police, etc.)
  4) create incident training and awareness
  5) exercise and monitor the incident response capabilities
- see ISO/IEC 27035-1 *Principles of incident management*
- see ISO/IEC 27001 clause A.16.1 *Information security incident management*
- see IEC 62443-2-1 section 4.3.4.5 *Incident planning and response*
- see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [3.5] *Incident handling and reporting*
- see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.8.4] (IEC 62443-3-3 SR 7.3) *Control system backup*
- see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.8.5] (IEC 62443-3-3 SR 7.4) *Control system recovery and reconstitution*
- See ISM Code:
  - section 8 *Emergency preparedness*
  - section 9 *Reports and analysis of non-conformance, accidents and hazardous occurrences*.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2.20 Business continuity

Business continuity plans (BCP) shall be developed, maintained and exercised.

Guidance note:

- the objective of the BCP is to describe how to maintain business continuity after cyber incidents. Objectives, priorities, responsibilities and actions should be defined so that critical operations can be continued
- see ISO/IEC 27001 clause A.17.1 *Information security continuity*
- see IEC 62443-2-1 section 4.3.2.5 *Business continuity plan*.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2.21 Periodic review

The CSMS shall be regularly reviewed, evaluated and improved to maintain the security objectives and address changes in risks.

Guidance note:

- such periodic activities shall include risk management, see[2.4], internal audits and reviews, and assurance of compliance with relevant regulations and requirements
- see ISO/IEC 27001:
  - section 10.2 *Continual improvement*
  - section 9.2 *Internal audit*
  - clause A.18.2 *Information security reviews*
- see IEC 62443-2-1 section 4.4.3.2 *Review, improve and maintain the CSMS*
- see ISM Code section 12 *Company verification, review and evaluation*.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

APPENDIX A CYBER SECURITY MANAGEMENT SYSTEM (CSMS) DOCUMENTS

1 Policies and procedures

The required documentation may be structured according to ISO 27001, and should contain the items listed in Table 1 and Table 2.

Table 1 Policies and procedures

CSMS document	*Reference*
1. Scope of the CSMS	Sec.4 [2.2]
2. Cyber security objectives, policies and procedures	Sec.4 [2.3], Sec.4 [2.10], Sec.4 [2.12], Sec.4 [2.13], Sec.4 [2.14], Sec.4 [2.15], Sec.4 [2.16]
3. Risk assessment and risk treatment methodology	Sec.4 [2.4]
4. Statement of applicability	Sec.4 [2.4]
5. Risk treatment plan	Sec.4 [2.3], Sec.4 [2.4]
6. Risk assessment report	Sec.4 [2.4]
7. Definition of security roles and responsibilities	Sec.4 [2.7], Sec.4 [2.8]
8. Inventory of assets	Sec.4 [2.6]
9. Acceptable use of assets	Sec.4 [2.8]
10. Access control policy	Sec.4 [2.11]
11. Operating procedures	Sec.4 [2.3]
12. Secure system engineering principles	Sec.4 [2.17]
13. Supplier security policy	Sec.4 [2.8]
14. Incident management procedure	Sec.4 [2.19]
15. Business continuity procedures	Sec.4 [2.20]
16. Statutory, regulatory and contractual requirements	Sec.4 [2.21]

2 Records

Table 2 CSMS records

CSMS document	*Reference*
17. Records of leadership commitment	Sec.4 [2.5]
18. Records of training, skills, experience and qualifications	Sec.4 [2.9]
19. Monitoring and measurement results	Sec.4 [2.4]
20. Internal audit program	Sec.4 [2.21]

CSMS document	*Reference*
21. Results of internal audits	Sec.4 [2.21]
22. Results of the management review	Sec.4 [2.5]
23. Results of corrective actions	Sec.4 [2.4]
24. Logs of user activities, exceptions and security events	Sec.4 [2.18]

CHANGES – HISTORIC

There are currently no historical changes for this document.

About DNV GL
DNV GL is a global quality assurance and risk management company. Driven by our purpose of safeguarding life, property and the environment, we enable our customers to advance the safety and sustainability of their business. We provide classification, technical assurance, software and independent expert advisory services to the maritime, oil & gas, power and renewables industries. We also provide certification, supply chain and data management services to customers across a wide range of industries. Operating in more than 100 countries, our experts are dedicated to helping customers make the world safer, smarter and greener.

SAFER, SMARTER, GREENER