Current Situation of NK Cyber Security Rules

23rd April 2024
Cybersecurity Team
ClassNK

Background of revision

The increased use of computer-based systems has led to more sophisticated cyber attacks.

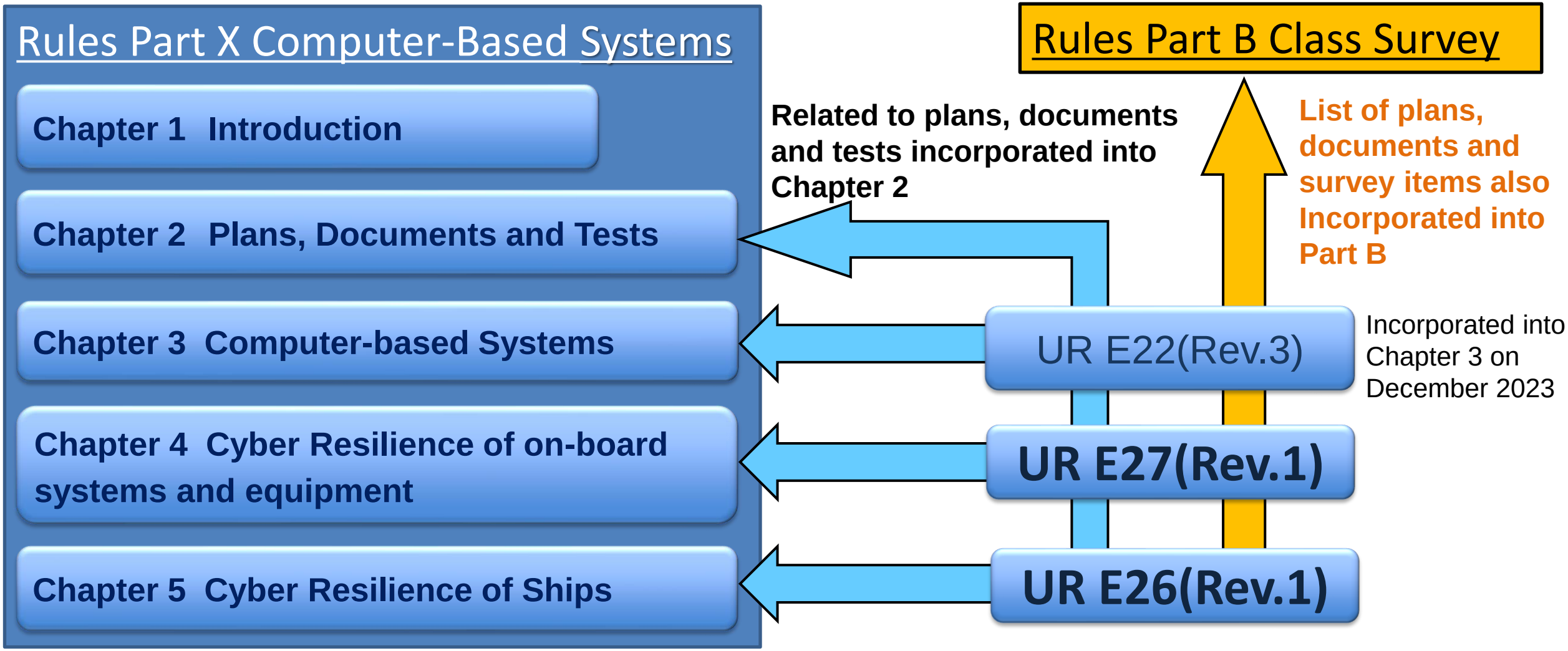
IACS adopts two new unified requirements (UR) in April 2022.

- **IACS UR E26 “Cyber resilience of ships”**
- **IACS UR E27 “Cyber resilience of on-board systems and equipment”**

IACS further reviews both URs in response to feedback received from relevant industries and decides to clarify requirements related to surveys. IACS adopts UR E27(Rev.1) in September 2023 and UR E26(Rev.1) in November 2023.

Incorporated into NK Rules

Incorporation of UR E26 and UR E27 into the ClassNK Rules



Amendment details

Part B of the Rules

Classification Surveys (Related to system integrators and shipowners)

Chapter 2 Classification Survey

2.1.6 Documents to be Maintained On Board

- Add documents, plans, drawings, manuals, etc. that are required to be maintained on board by Chapter 5, Part X.

Chapter 3 Annual Survey

3.9 Special Requirements for Ships Affixed with the Notation "CybR"

- Add requirements for Annual Survey in Chapter 5, Part X.
- Specify that ships affixed with "CybR" are to maintain a "Ship cyber security and resilience program" on board.
- Add Table B3.12 Special Requirements for Ships Affixed with the Notation "CybR" (list of items to be confirmed)
  ① First Annual Survey: Confirm 10 requirements from documents submitted for review.
  ② Subsequent Annual Survey: Confirm the implementation of ① upon request by the Society.

Chapter 4 Intermediate Survey

4.9 Special Requirement for Ships Affixed with the Notation "CybR"

- Add requirement for Intermediate Surveys requested by Chapter 5, Part X. These requirements are the same as the ones for subsequent Annual Survey

Chapter 5 Special Survey

5.9 Special Requirement for Ships Affixed with the Notation "CybR"

- Add requirement for Special Survey in Chapter 5, Part X.
- Table B5.32 Special Requirements for Ships Affixed with the Notation "CybR" (list of survey items)
  ① Tests in accordance with the "Ship Cyber Resilience Test Procedure" are to be carried out in the presence of a Society surveyor.

Amendment details

Target Ships for Chapter 4 and 5, Part X of the Rules

- Passenger ships engaged in international voyages (includes high speed passenger craft)
- Cargo ships of 500 GT and upwards engaged in international voyages
- High speed craft of 500 GT and upwards engaged in international voyages
- Mobile offshore drilling units of 500 GT and upwards
- Self-propelled offshore units engaged in construction (e.g. offshore wind turbine installation maintenance and repair, crane units, drilling tenders, accommodation etc)

Amendment details

Class Notations: 1.2.4, Part A of the Rules

Add the following to “1.2.4 Hull Construction and Equipment, etc.”

For ships complying with the provisions of Chapter 4 and 5, Part X, the notation of “Cyber Resilience” (abbreviated to CybR) is affixed to the Classification Characters.

Amendment details

Chapter 4 and 5, Part X of the Rules

Target systems:

System type	Example
Propulsion	Engine control sys., Main boiler control sys., etc.
Steering	Steering control sys., Azimuth thruster control sys. etc.
Anchoring and mooring	Windlass control sys. Mooring winch control sys. etc.
Electrical power generation and distribution	Generator engine control sys., Electric power converters, etc.
Fire detection and extinguishing systems	Fire detection and alarm sys., Fixed deck foam sys. etc.
Bilge and ballast system, loading computer	Ballast transfer valve remote control sys. Loading computer
Watertight integrity and flooding detection	Watertight door power opening/closing devices, etc.
Lighting (e.g. emergency lighting, low locations, navigation lights, etc.)	Emergency lighting, Low location lighting, Navigation lighting control sys. etc.
Any required safety system	Inert gas sys. Cargo monitoring control sys. etc.
Navigation system required by statutory regulations (For navigation equipment and communication systems, equivalent standards such as IEC 61162-460 can be applied in place of the required security function)	Radar, Transmitting heading devices(THD) etc.
Internal and external communication system required by class rules and statutory regulations	General emergency alarm, Public addressor. etc.
Others	DPS , Passenger service sys. etc.

Chapter 4 and 5, Part X of the Rules

Definition of Various Stakeholders

Shipowner/Company:

The owner of the ship or any other organization or person, such as the manager, agent or bareboat charterer, who has assumed the responsibility for operation of the ship from the shipowner and who on assuming such responsibilities has agreed to take over all the attendant duties and responsibilities. The shipowner could be the Shipyard or systems integrator during initial construction. After vessel delivery, the shipowner may delegate some responsibilities to the vessel management company.

Supplier:

A manufacturer or provider of hardware and/or software products, system components or equipment (hardware or software) comprising of the application, embedded devices, network devices, host devices etc. working together as system or a subsystem. The Supplier is responsible for providing programmable devices, sub-systems or systems to the System Integrator.

Systems Integrator:

The specific person or organization responsible for the integration of systems and products provided by suppliers into the system invoked by the requirements in the ship specifications and for providing the integrated system. The system integrator may also be responsible for integration of systems in the ship. Until vessel delivery, this role is to be taken by the Shipyard unless an alternative organization is specifically contracted/assigned this responsibility.

Amendment details

Chapter 2, Part X of the Rules

Plans, Documents and Tests

2.1.1 “Submission of Plans and Documents”

- Add plans and documents specified in UR E26(Rev.1) and UR E27(Rev.1).

2.2.2 “Tests (Related to Chapter 4)”

- Add factory acceptance and other tests required to be carried out by suppliers by UR E27(Rev.1)

2.2.3 “Tests (Related to Chapter 5)”

- Add requirements related to tests for demonstrating compliance with relevant requirements required to be carried out by systems integrators and shipowners by UR E26(Rev.1)

Chapter 4: Cyber Resilience of On-board Systems and Equipment
Chapter 5: Cyber Resilience of Ship

Table X2.3 “Supplier’s Plans and Documents to be Submitted (Related to Chapter 4)”

- Clarify correspondence between the plans and documents required by UR E27(Rev.1) and Part X.
- Clarify which documents are to be submitted for reference and which are to be submitted for approval.
- Clarify which documents are to be submitted for approval of use.

Table X2.4 “Systems Integrator’s or Shipowner’s Plans and Documents to be submitted (Related to Chapter 5)”

- Clarify which plans and documents are required to be submitted by UR E27(Rev.1), when they are to be submitted and who is to submit them.

Table X2.5 “Summary of Requirements and Documents (Related to Chapter 5)”

- Clarify the correspondence between plans and documents required by UR E26(Rev.1) and Part X.

Amendment details

Chapter 2, Part X of the Rules

Table X2.3 "Supplier's Plans and Documents to be submitted (Related to Chapter 4)"

Table X2.3 Supplier's Plans and Documents to be Submitted (Related to Chapter 4 CYBER RESILIENCE OF ON-BOARD SYSTEMS AND EQUIPMENT)

#	Document (Referenced requirements)	Requirements (Referenced requirements)	Reference	Approval
1	Computer-based system asset inventory (4.4.1(1))	To be incorporated in vessel asset inventory (5.4.2(1))	-	○(1)
2	Topology diagrams (4.4.1(2))	Enabling system integrator to design security zones and conduits (5.4.3(1))	-	○(1), (2)
3	Description of security Capabilities (4.4.1(3))	Required security capabilities (4.4.2) Additional security capabilities, if applicable (4.4.3)	-	○(1)
⋮				
		(No.27 in Table X4.1)		
9	Management of change plan (4.4.1(9))	Management of change process (Chapter 3)	○(1)	-
10	Test reports (4.4.1(10))	Configuration of security capabilities and hardening (4.4.1(5) and 4.5.8)	○(2)	-

(Notes)

Approval: Plans and documents to be submitted for approval

Reference: Plans and documents to be submitted for reference

○: Submission required

(1): Submitted when type approval has not been obtained in accordance with Chapter 10, Part 7 of the Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use

(2): Submitted when type approval has been obtained in accordance with Chapter 10, Part 7 of the Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use

References for relevant requirement in Part X of the Rules

References to description of documents in Part X of the Rules

Notes added clarifying handling of documents submitted for approval of use

Amendment details

Chapter 2, Part X of the Rules

Table X2.4 “Systems Integrator’s or Shipowner’s Plans and Documents to be submitted（Related to Chapter 5）”

Table X2.4 Systems Integrator’s or Shipowner’s Plans and Documents to be submitted
(Related to **Chapter 5 CYBER RESILIENCE OF SHIPS**)

#	Document (Referenced requirements)	Systems integrator			Shipowner			
		Design	Construction	Commissioning	Operation	1st AS	AS/IS	SS
1	Approved supplier documentation (2.2.3)	-	Maintain	Maintain	Maintain	-	-	-
2	Zones and conduit diagram (2.2.3-3(4))	Submit	Maintain	Maintain	Maintain	-	-	-
3	Cyber security design description (2.2.3-3(5))	Submit	Maintain	Maintain	Maintain	-	-	-
⋮								
	(5.4.6(1)(d)iv))							

(Notes)

* : If applicable

Submit: The stakeholder is to submit the document to the Society for verification and approval of compliance with requirements in **Chapter 5.**

Maintain: The stakeholder is to keep the document updated in accordance with procedure for management of change (MoC). Updated document and change management records are to be submitted to the Society as per **Table X2.2.**

Demonstrate: The stakeholder is to demonstrate compliance to the Society in accordance with the approved document.

1st AS : First annual survey

AS/IS : Subsequent annual survey/Intermediate survey

SS : Special survey

Who, when and what for each plan and document

Reference to relevant require-ment in Part X of the rule

Details explaining what is required

Amendment details

Chapter 4, Part X of the Rules

Requirements for Suppliers

Chapter 4 Cyber Resilience of on-board system and equipment

4.1 General
4.2 Definitions and Abbreviations
4.3 Security Philosophy
- Essential Systems Availability
  ⇒ Implementation of safety measures is not to close the loss of safety functions, control functions, monitoring functions or other functions which could result in health, safety or environmental consequences.
- Compensating Countermeasures
  ⇒ May be employed in lieu of or in addition to inherent security capabilities.

4.4 Requirements for Cyber resilience of on-board systems and equipment
- 4.4.1 Documentation for Cyber resilience of on-board systems and equipment（10 items）
- 4.4.2 Required security capabilities（30 items）
  ⇒ Requirements for computer-based systems falling within the scope of application of Chapter 4.
- 4.4.3 Additional security capabilities（11 items）
  ⇒ Requirements for computer-based systems with network communication to untrusted networks (i.e. systems interfacing with networks outside the scope of application of Chapter 4).

4.5 Secure Development Lifecycle Requirements
⇒ Documentation addressing the handling of security at all stages of system or equipment development

4.6 Demonstration of compliance

Amendment details

Chapter 4, Part X of the Rules

Requirements for Suppliers

4.3.4 Compensating Countermeasures

Compensating countermeasures may be employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements. Such countermeasures are to meet the intent and rigour of the original stated requirement and follow the principles specified in 4.4.1(3) in consideration of the standards referenced, the differences between each requirement and the related items on the standards.

Details related to the adoption of compensating countermeasures are to be included in the “Description of Security Capabilities” that is required to be submitted to the Society

4.4.1(3) Description of Security Capabilities (Required to submitted by Chapter 4)

(e) If any requirement in not fully met, this is to be specified in the description, and compensating countermeasures which meet the following are to be proposed.

i) Protect against the same threats as the original requirement.
ii) Provide an equal level of protection as the original requirement.
iii) Not be a security control required by other requirements in Chapter 4.
iv) Not introduce a higher security risk.

Example of compensating countermeasure

[Requirement]

- No.10 in Table X4.1 “Use control for portable and mobile devices”
  - a) Limit use to only those permitted by design
  - b) Restrict code and data transfers

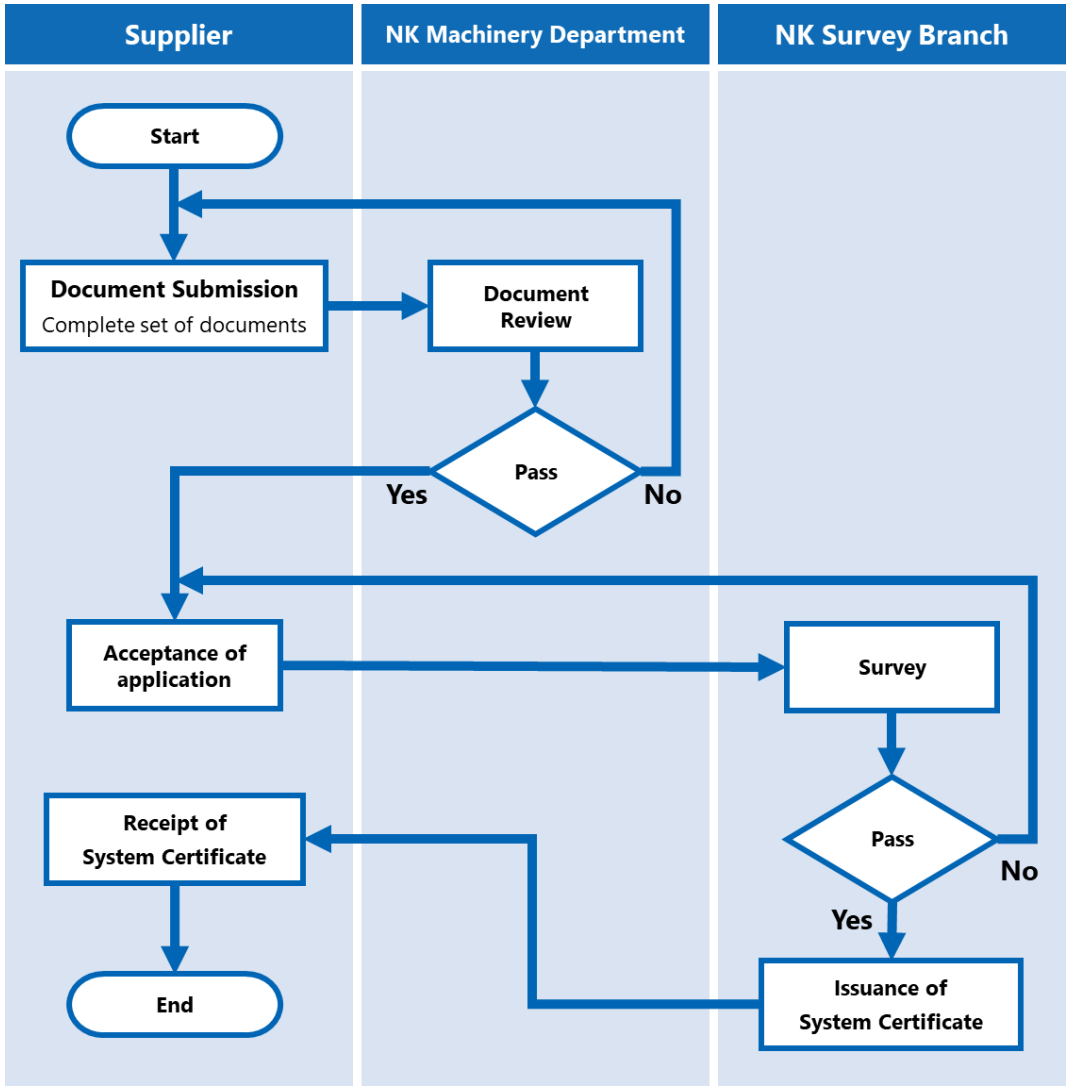
【Compensating Countermeasures】

- Use port blocker
- Scan system for malware

Amendment details

System Approval Flow Chart

System is Not Type Approved



Type approval not mandatory

Items 1 to 9 in Table X2.3 are to be submitted for review or approval, and the following surveys are to be carried out in the presence of a Society surveyor.

2.2.2 Tests (Related to Chapter 4)

- Factory acceptance and other tests required to be carried out by suppliers by UR E27(Rev.1).

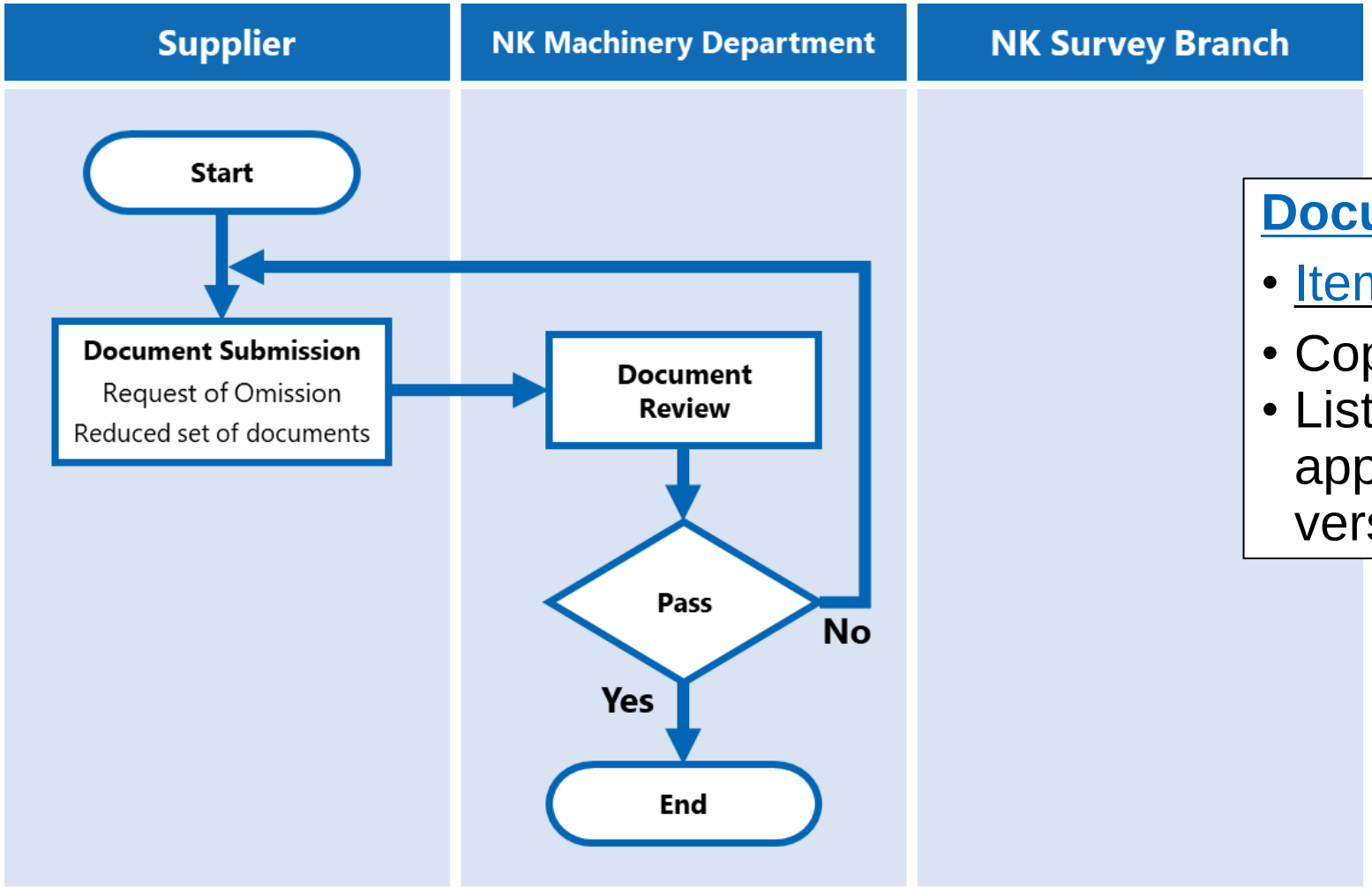
	Documentation required for surveys
☐	CBS asset inventory
☐	Topology diagrams
☐	Test procedure of security capabilities
☐	Security configuration guidelines
☐	Secure development lifecycle documents

	Survey items
☐	General survey items
☐	Test of security capabilities
☐	Correct configuration of security capabilities
☐	Secure development lifecycle

Amendment details

System Approval Flow Chart

System is Type Approved



Type approval not mandatory

Document Review

- Items 1, 2 and 10 in Table X2.3
- Copy of type approval certificate
- List of any differences from the type approved product, including software versions

Amendment details

Chapter 5, Part X of the Rules

Requirements for Systems Integrators or Shipowners

Chapter 5 Cyber Resilience of Ships

- 5.1 General
- 5.2 Definitions
- 5.3 Goals and Organisation of Requirements
- 5.4 Requirements for Cyber Resilience of Ships
  - ✓ 5.4.1 General
  - ✓ 5.4.2 Identify (1 item)
  - ✓ 5.4.3 Protect (7 items)
  - ✓ 5.4.4 Detect (2 items)
  - ✓ 5.4.5 Respond (4 items)
  - ✓ 5.4.6 Recover (3 items)

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271.pdf

- 5.5 Risk Assessment for Exclusion of Computer-based Systems from the Application of the Requirements

  ⇒ Computer-based systems within the scope of applicability of Chapter 5 need not comply with the chapter's requirements in cases where a risk assessment shows that system risks use are of a level deemed to be acceptable by the Society.

Amendment details

Chapter 5, Part X of the Rules

Requirements for Systems Integrators or Shipowners

5.4 Requirements for Cyber Resilience of Ships

Each specific security related requirement (i.e. 5.4.2 to 5.4.6) is organised as follows.

(a) Requirement
(b) Rationale
(c) Requirement details
Specific requirement details
(d) Demonstration of compliance
i) Design phase
ii) Construction phase
iii) Commissioning phase
iv) Operation phase
1) General requirements
2) 1st Annual Survey
3) Subsequent Annual Surveys
4) Special Surveys

Important items

Systems integrator responsibility

Shipowner responsibility

(d) Demonstration of compliance
Specifies details related to the documentation that needs to be created and the tests that need to be carried out for phases i) to iv)

Amendment details

Chapter 5, Part X of the Rules

Requirements for Systems Integrators or Shipowners

5.5 Risk Assessments for Exclusion of Computer-based Systems from the Application of Requirements (To be submitted by systems integrators and thereinafter maintained (updated) by shipowners)

Risk assessments are to consider the following

(1) Asset vulnerabilities
(2) Threats (internal and external)
(3) Potential impact of cyber incidents on human safety, ship safety and environmental safety
(4) Possible effects related to system integration, system interfaces (including systems not on board if remote access to onboard systems is provided)

Acceptance criteria

Exclusion of systems not fully meeting the following criteria may still be granted when supporting evidence and a rational explanation supporting evidence are submitted.

- System is isolated (i.e. no IP connections to other systems or networks).
- System has no accessible physical interface points.
- System is in an area where physical access is controlled.
- System is not an integrated control system.

Systems integrators are to risk assess systems for which exclusion from the application of relevant requirements is sought and are to submit a "Risk Assessment for Exclusion of Computer-based Systems" to the Society.

Maintenance

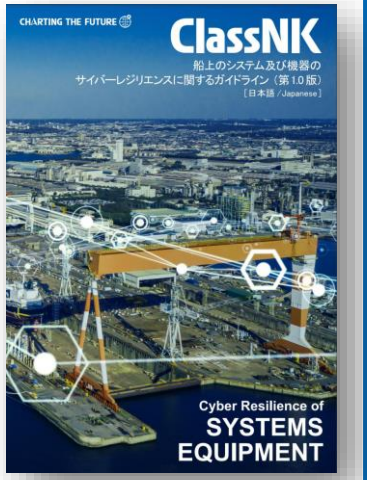
- Shipowners are to update existing risk assessments or carry out new risk assessments during the operational life of a ship as part of a process of continuous improvement based on cyber scenario change and new vulnerability identification.
- Shipowners are to notify the Society and submit updated risk assessments for review when cyber scenario changes elevate risks above acceptable existing risk assessment thresholds.

Chapter 4 Cyber Resilience of On-board Systems and Equipment (Incorporate UR E27(Rev.1))

Guideline for Cyber resilience and on-board systems and equipment (Edition 1.0)

Issued on 2 Nov. 2023

- Application scope
- Approval process
- Explanation of requirements
- Items to be confirmed during document reviews and surveys
- Type approval process



Chapter 5 Cyber Resilience of Ships (Incorporate UR E26(Rev.1))

Guideline for Cyber resilience of ships

Scheduled to be issued in May 2024

- Application scope
- Explanation of requirements
- Items to be confirmed during document reviews and surveys
- Explanation of exclusions from the application of relevant requirements based on risk assessments

- “Guidelines for Cyber Resilience of On-board Systems and Equipment” supplements Chapter 4, Part X and UR E27(Rev.1)
- “Guidelines for Cyber Resilience of Ships” supplements Chapter 5, Part X and UR E26(Rev.1)
- Both guidelines include references to the Rules for the Survey and Construction of Steel Ships and correspond to its requirements.

Effective Date

Applicable to ships for which the date of the contract for construction is on or after 1 July 2024.