

**Explanation for
Shipowner/Ship management company**

Cyber resilience of ships

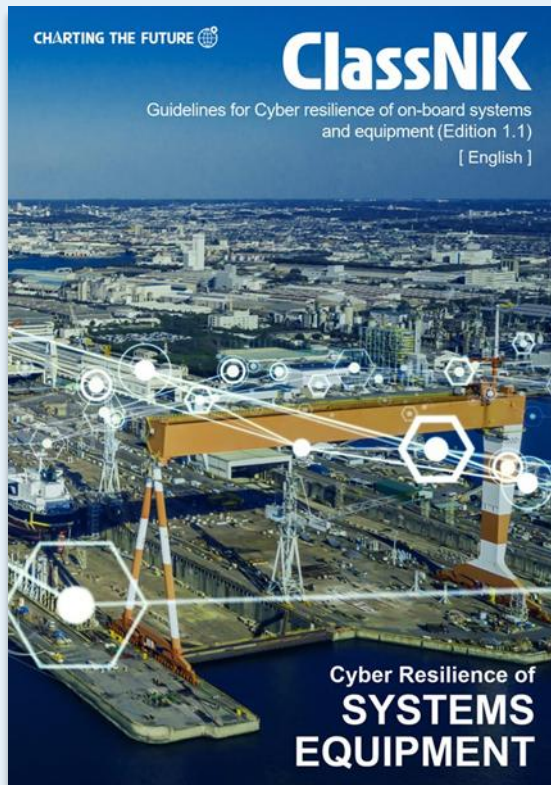
- IACS UR E26 Rev.1 -

June, 2026

ClassNK Machinery Department

We issued **guidelines explaining rules** for support

Guidelines for Cyber resilience of on-board systems and equipment



UR E27 (Part X, Ch.4)

Traget: Manufacturers

Updated: Aug. 2025
Contents: Application
Approval process
Requirements
Documents
Witnessed test
Type Approval

etc.

Guidelines for Cyber Resilience of Ships



UR E26 (Part X, Ch.5)

Traget: Shipyard
Shipowner

Updated: Aug. 2025
Contents: Application
Network
configuration
Requirements
Documents
Witnessed test
Omission

etc.



Portal page (Guidelines / Movies / FAQ etc.)

<https://www.classnk.or.jp/hp/en/activities/cybersecurity/ur-e26e27.html>

IACS UR E27 (Rev.1)

(Part X Chapter 4 of the Rules)

Cyber resilience of onboard systems and equipment

 **Manufacturers (Suppliers)**
supply products
considered cyber resilience



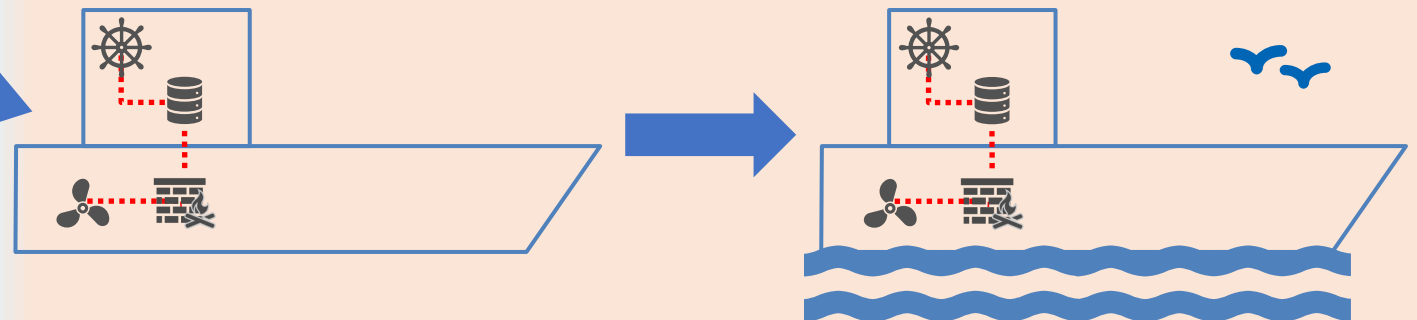
IACS UR E26 (Rev.1)

(Part X Chapter 5 of the Rules)

Cyber resilience of ships

 **Shipyards (integrators)**
build cyber resilient ships

 **Shipowners**
maintain cyber resilience in operation

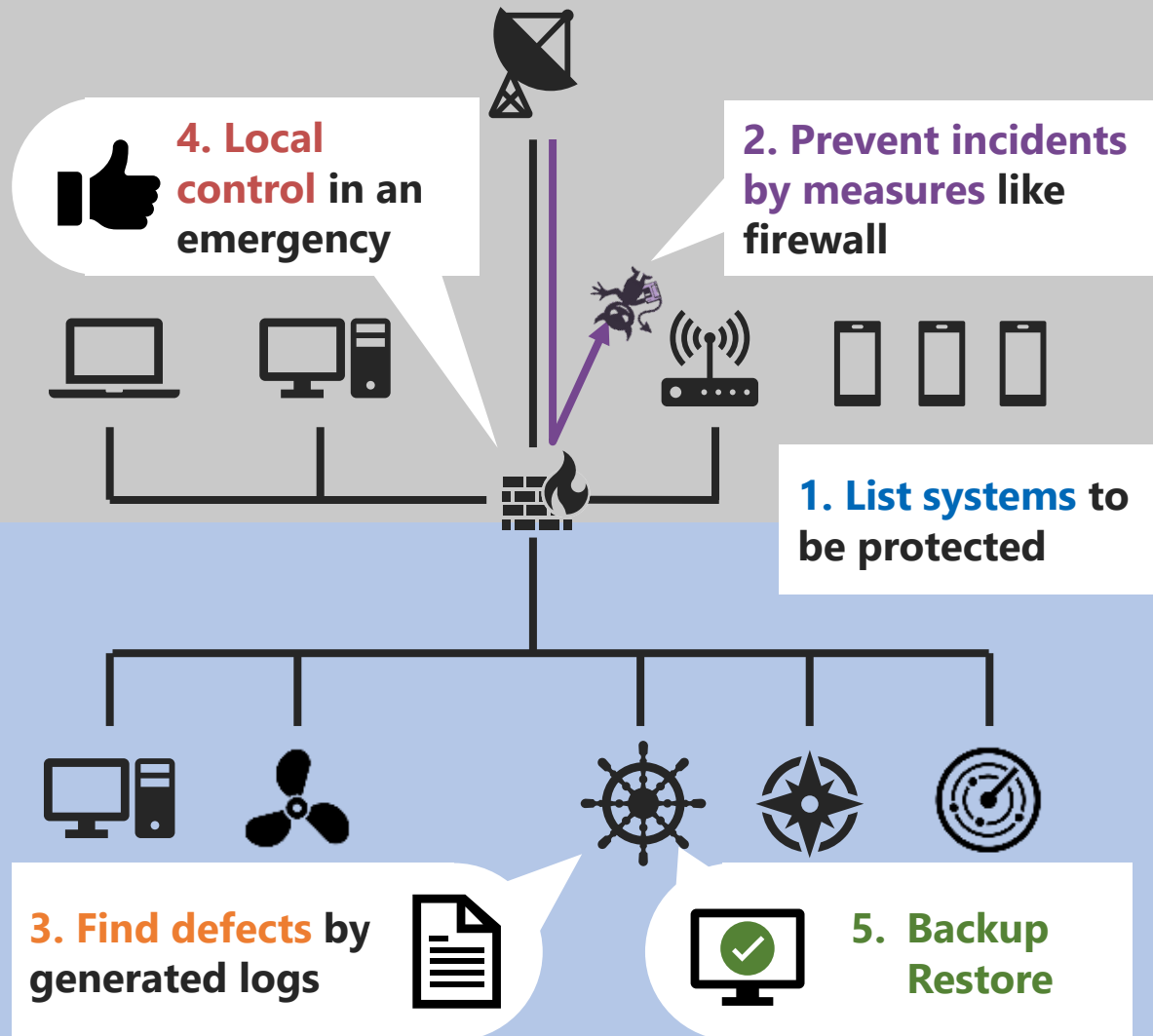


UR E26 classifies measures required to maintain cyber resilience into 5 functional factors



**Reducing cyber risks and ensuring safe operation of ships
by satisfying the requirements of the 5 factors**

Cyber resilient ship / systems



Identify

- **List** and manage systems to be protected

Protect

- **Prevent incidents by measure** like firewall

Detect

- **Discover anomalies** through logs and displays.

Respond

- **Isolation** in case of emergency
- Switch to **Local steering control**

Recover

- **Restore** equipment with **backup** data

Applicable ships

The following ships contracted on or after **July 1st, 2024** are applicable

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

💡 Not applicable for

- **Non-international vessels** and
- **ships contracted before July 1st, 2024**

Applicable systems and equipment

OT : Operational Technology

Systems used for ship's physical operation or control

① Applicable OT systems

Systems directly involved in the operation and control of ships



Propulsion Steering Navi.

② Applicable network devices

Network devices that control and manage communications for the applicable systems



Firewall Router Switch

③ Applicable systems other than "applicable OT systems"

Network devices which control communications of applicable systems



VDR/ECDIS Data Server

④ Not applicable systems

Systems other than applicable devices that communicate outside of security zone as applicable devices



VSAT Office PC

NOT applicable systems and equipment

IT : Information Technology

Systems used for ship's information management

① Applicable OT systems

Systems directly related to ship operation and control



Propulsion



Steering



Anchoring and mooring



Electrical power generation and distribution



Fire detection and extinguishing systems



Bilge and ballast systems, loading computer



Watertight integrity and flooding detection



Lighting



Any required safety system whose disruption or functional impairing may pose risks to ship operations

(e.g. emergency shutdown system, cargo safety system, pressure vessel safety system, gas detection system, etc.)



Navigational systems required by statutory regulations



Internal and external communication systems required by class rules and statutory regulations

① Examples of Applicable OT Systems

Propulsion

Engine control systems	Engine remote control systems
Main boiler control systems	CPP control systems
Electric propulsion control systems	Fuel supply system control unit (e.g., FGSS control systems)
Machinery alarm and monitoring systems (including data loggers)	Waterjet propulsion control systems

Steering

Steering system control systems	Azimuth thruster control systems
---------------------------------	----------------------------------

Anchoring and mooring

Windlass control systems	Mooring winch control systems
--------------------------	-------------------------------

Electrical power generation and distribution

Generator engine control systems (including power management systems)	Electric power converters (for electric propulsion ship)
Battery management systems (consisting of lithium-ion batteries with total capacities of 20 kWh or more, and associated equipment)	

Fire detection and extinguishing systems

Fire detection and alarm systems	Fixed foam fire extinguishing systems
Fixed CO ₂ fire extinguishing systems	Fixed deck foam systems
Fixed local application fire-fighting systems	Water-spraying systems
Dry chemical fire-extinguishing equipment	

Bilge and ballast system, loading computer

Ballast transfer valve remote control systems	Loading computers
---	-------------------

Watertight integrity and flooding detection

Watertight door power opening/closing devices	Water level detection and alarm systems
---	---

Lighting (e.g. emergency lighting, low locations, navigation lights, etc.)

Emergency lighting	Low location lighting
Navigation lighting control systems	

 Any required **safety system** whose disruption or functional impairing may pose risks to ship operations (e.g. emergency shutdown system, cargo safety system, pressure vessel safety system, gas detection system, etc.)

Inert gas systems	Cargo monitoring control systems
Liquefied gas emergency shutdown systems	Flammable gas detection systems
Reliquefaction plants	Auxiliary boiler control systems
GCU control systems	Gas fuel tank monitoring and control systems

Navigational systems required by statutory regulations

Radar	Transmitting heading devices (THD)
Electronic plotting aids (EPA)	Automatic identification systems (AIS)
Automatic tracking aids (ATA)	Voyage data recorders (VDR)
Target Track (TT) (ARPA)	Heading control systems (HCS)
Echo sounding devices	Track control systems (TCS)
Global navigation satellite systems (GNSS)	Long range identification and tracking systems (LRIT)
Sound reception systems	Bridge navigational watch alarm systems (BNWAS)
Speed and distance measuring devices	Electronic chart display and information systems (ECDIS)

Internal and external communication systems required by class rules and statutory regulations

General emergency alarm	Public addressor
NAVTEX receiver	VHF DSC device
EGC receiver	DSC device
VHF DSC continuous watch device	DSC continuous watch device
GMDSS radio installation	

Others

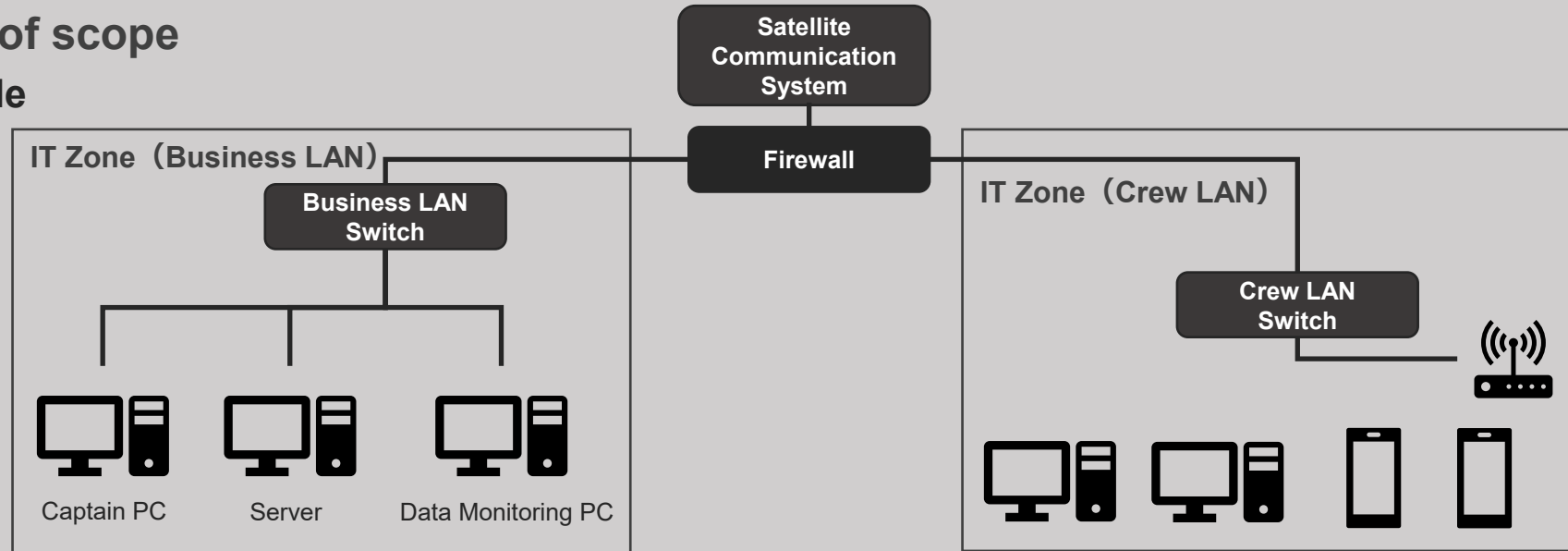
Dynamic positioning systems (DPS)

 Same examples are described in the guidelines

2. Application of IACS UR E26

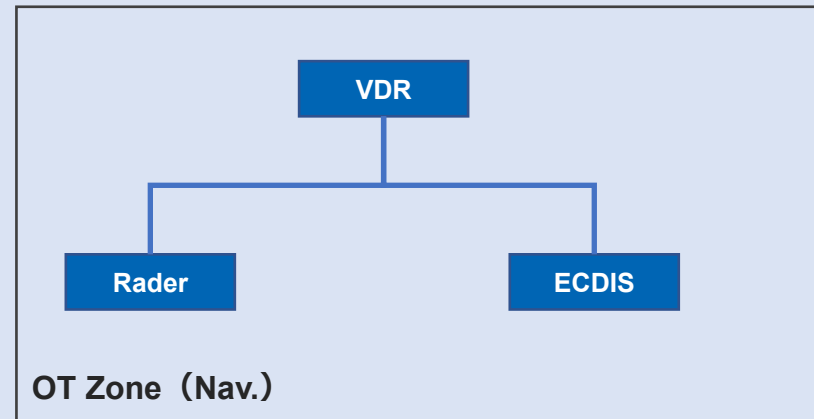
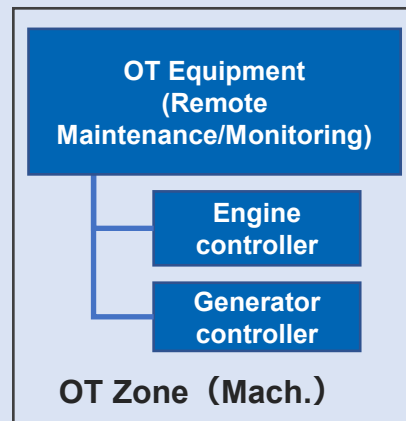
E26 out of scope

※Example



④ Not applicable systems

① Applicable OT systems



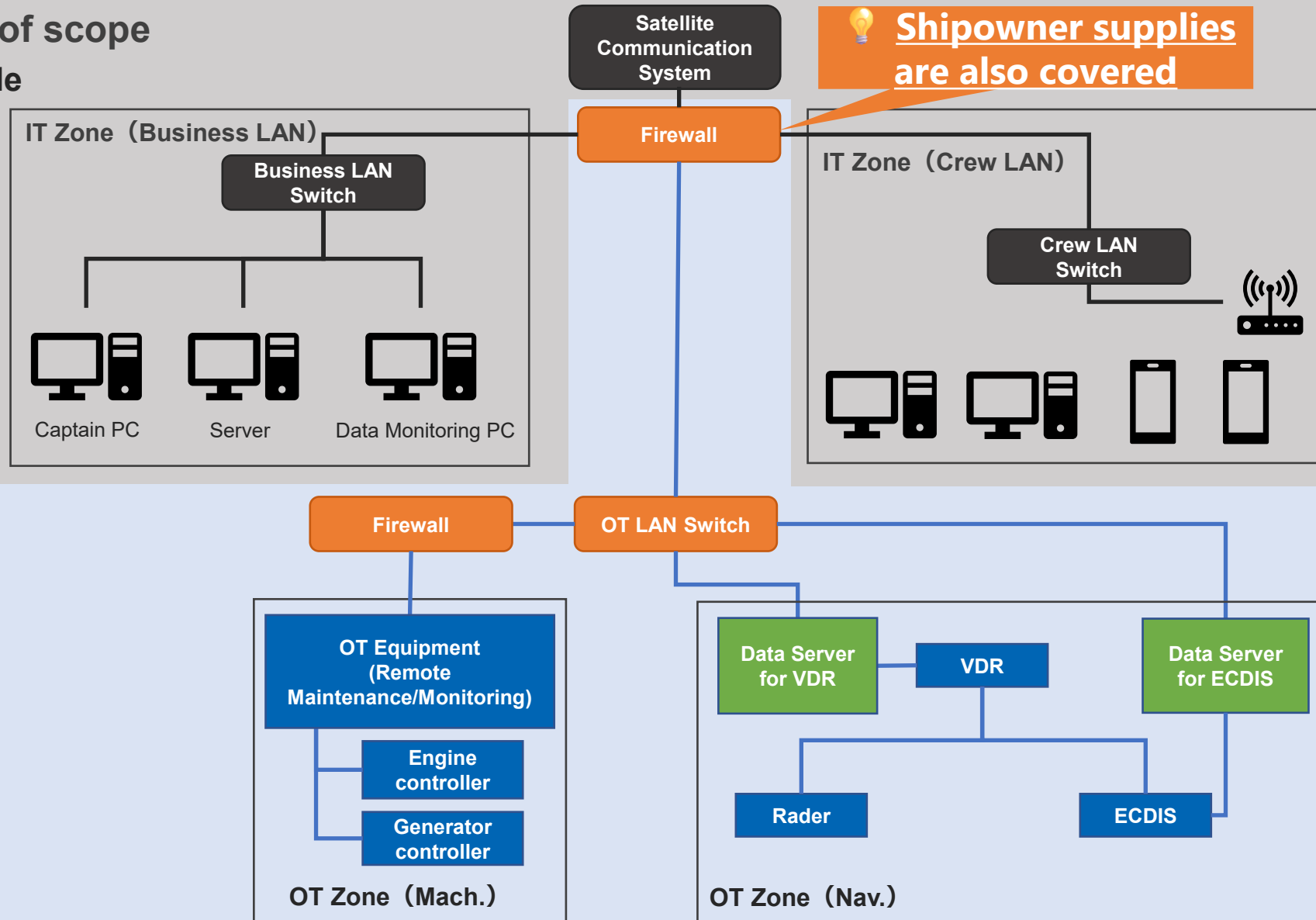
Systems other than ① are not applicable if they are not connected to the onboard network at all.

E26 in scope

2. Application of IACS UR E26

E26 out of scope

※Example



④ Not applicable systems

「Security Zone」

A set of devices with equivalent security levels bounded by **Zone boundary device** ※
(Network equipment that has a communication control function to protect the applicable system)

① Applicable OT systems

② Applicable network devices

③ Systems other than applicable devices that communicate in the same security zone as applicable devices

E26 in scope

Key points in application



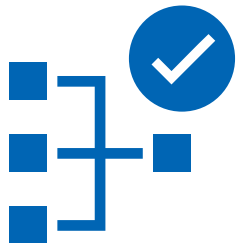
Whether UR is applicable to the ship or not

⇒ **Contract date of the ship is on/after July 1st, 2024.**
(Cargo ships / 500 GT or above / international voyages)



Providing information on shipowner supply items

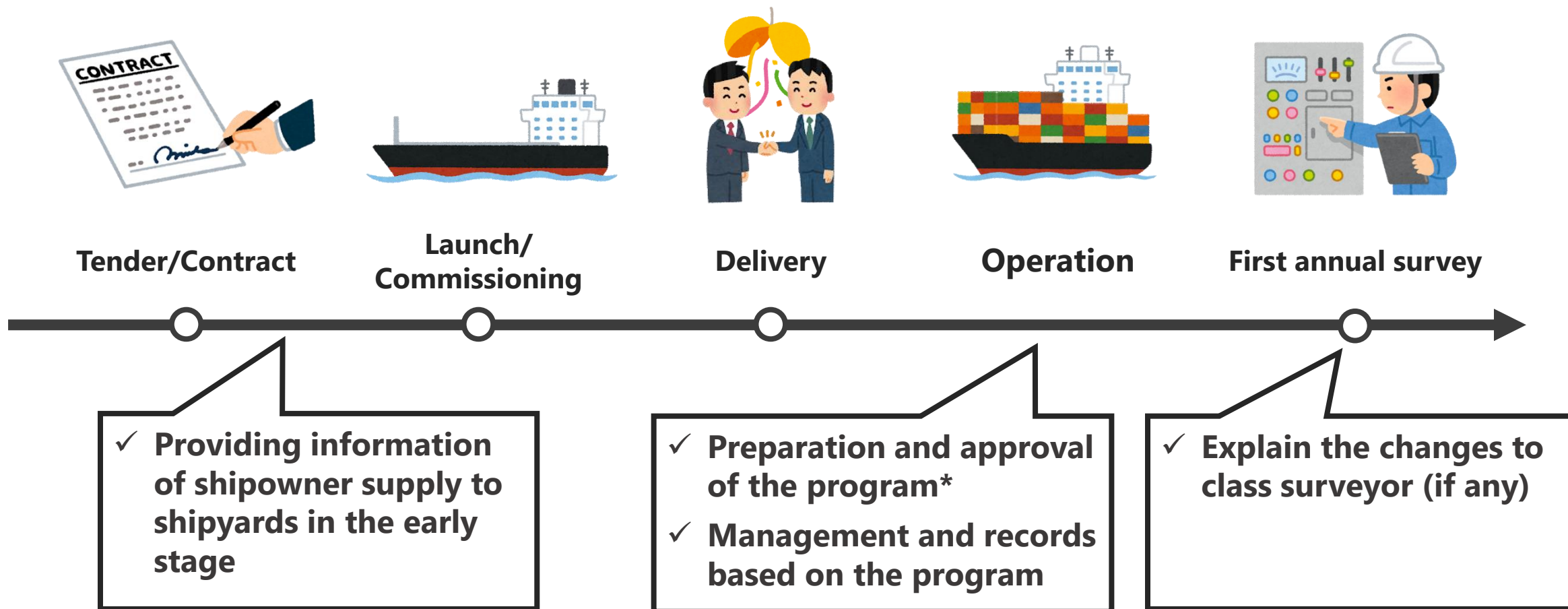
⇒ **To determine applicable systems.**



Possibility that shipowner supply items are in the scope

⇒ **Please select the systems with E27 approval.**

Brief timeline (from contract to first annual survey)



*The program = Ship Cyber Security and Resilience Program

Overview

A program* describing cyber-related policies, procedures with records
The set of the **program itself** + **its record** to be kept onboard
*Such as “Management Plan + Record Book” required by BWM

Recover

Recovery plan for **cyber incidents**

- Development of **recovery plan**

Respond

Response policy for **cyber incidents**

- Development of **incident response plan**

Detect

Measures for error detection to be specified

- **Network monitoring**
- **Security functionality verification**

Contents of the

Program

(Ship cyber security and resilience program)



Identify

Onboard asset management

- **Management of change**
- **Management of software updates**

Protect

Management of the **protective measures**

- **Firewall**
- **Anti-malware**
- **Access control**
- **Confidential information**
- **Remote access**
- **Portable and mobile devices**

- ✓ **Necessary to submit to the class for approval prior to first annual survey**
- ✓ Based on this program, **creating records in daily operation is required**
- ✓ Utilize for Annual, Intermediate and Special survey **document confirmation**
- ✓ Possible to prepare most items based on **documents submitted by suppliers and shipyards**



Supplier / E27

- Computer-based system asset inventory
- Topology diagram

- Description of security capabilities

- Test procedure for security capabilities
- Security configuration guidelines

- Secure development lifecycle

- Plans for maintenance and verification

- Information supporting incident response and recovery plans

- Management of change plan
- Test reports



Shipyard / E26

- Ship asset inventory
- Zones and Conduit Diagram

- Cyber Security Design Description

- Risk assessment for exclusion of computer-based systems
- Description of compensating countermeasures
- Ship cyber resilience test procedure



Shipowner / E26

Ship cyber security and resilience program

Management of change (MoC)

Management of software updates

Management of firewalls

Management of malware protection

Management of access control

Management of access control

Management of remote access

Management of mobile and portable devices

Detection of security anomalies

Verification of security functions

Incident response plans

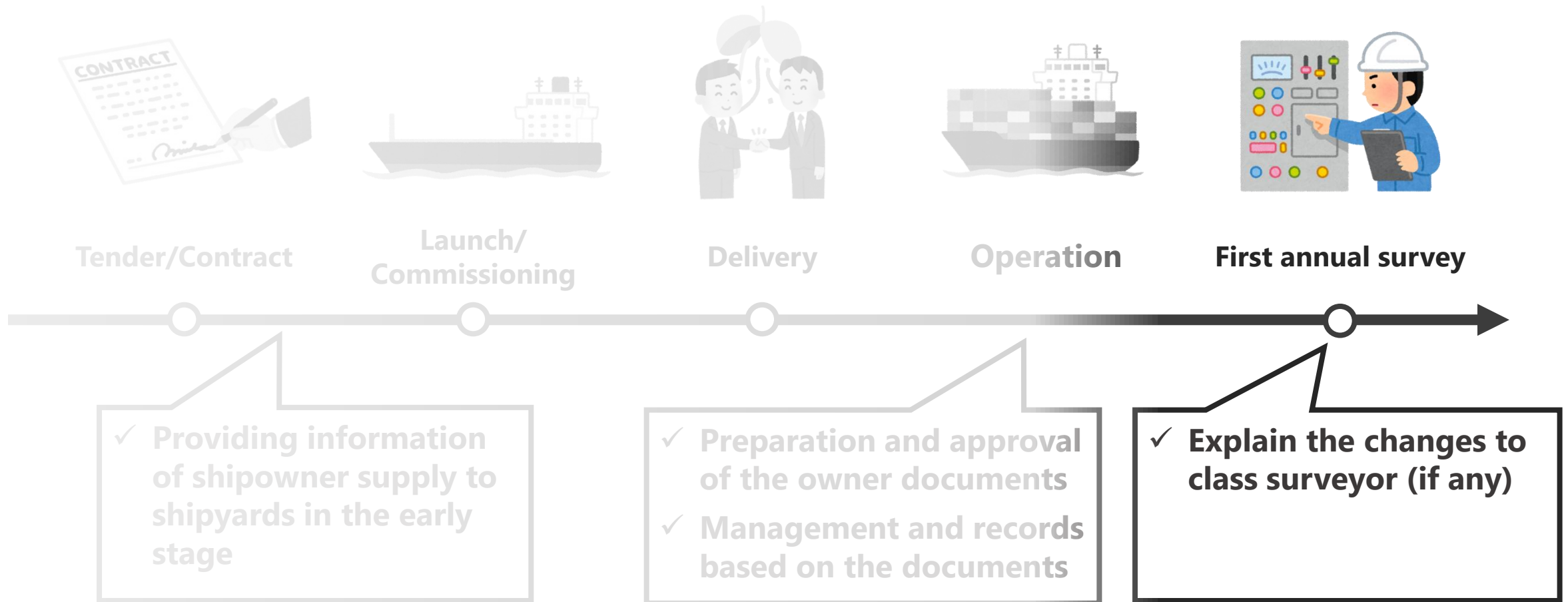
Recovery plans

The first step is to develop

“Ship cyber security and resilience program”

based on documents of the supplier / the shipyard

Brief timeline (from contract to first annual survey)



Periodical surveys

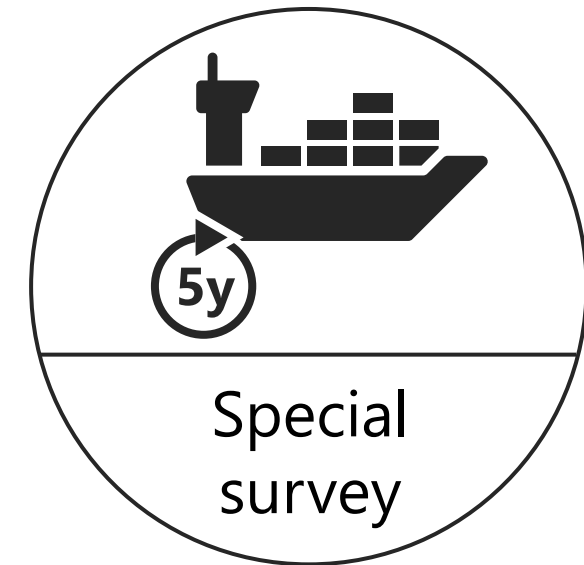


Prior to the first annual survey,
to submit the program to class and obtain approval

During the survey, to show the
record based on the program

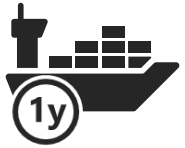


In case there are changes to the program or systems, to show the
record based on the program



In addition to annual intermediate,
conduct the witnessed survey based on the test procedures*

- > Mandatory items
- > Items to be conducted in case of changes



Review of **Approved Program + its records** in the first annual survey

Review of the Approved program onboard and Records based on it

Identify	Vessel asset inventory - Management of change, Software Updates
Protect	Security zones and network segments Antivirus, antimalware, antispam and other protections from malicious code Access control Remote access control and communication with untrusted networks Use of Mobile and Portable Devices
Detect	Network operation monitoring Verification and diagnostic functions of CBS and networks
Respond	Incident response plan
Recover	Recovery plan

Review of change management

In case of changes to systems or the program,
confirm the following items

Changes to the program	• Submission and reapproval of the program • Inspection of changes to the program
-------------------------------	--

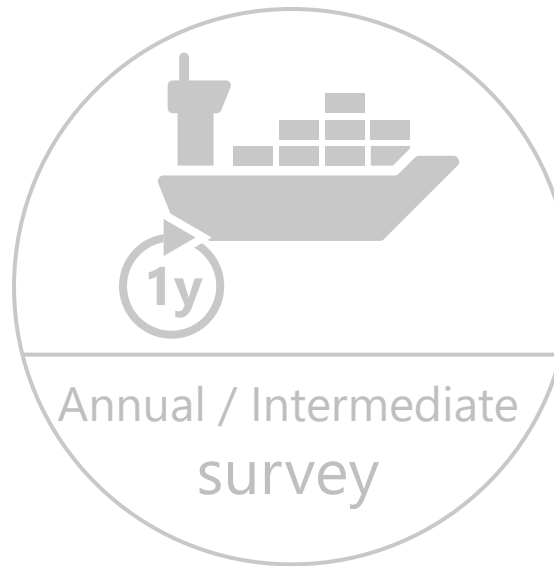


Periodical surveys

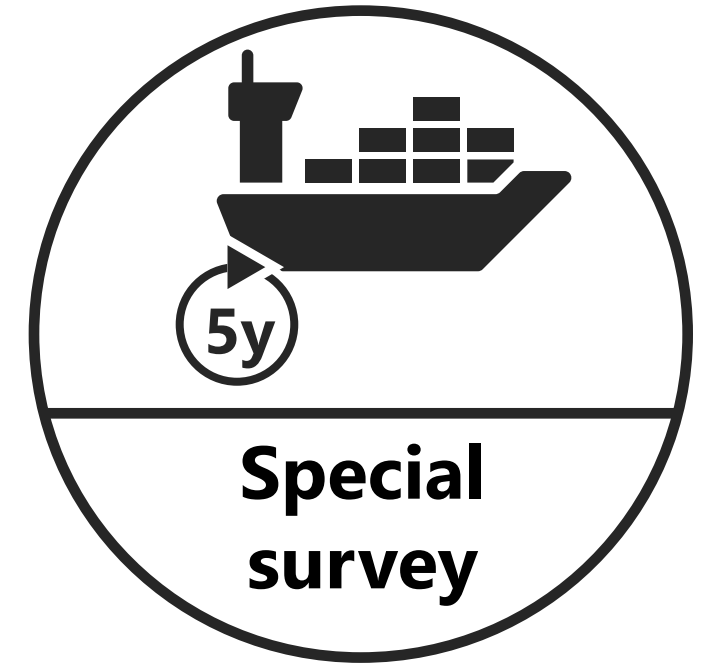


Before the first annual survey,
**submit the program to class
and obtain approval**

In the survey, show the
record based on the program



In case there are changes to the
program or systems, to show the
record based on the program



In addition to annual intermediate,
**to conduct the witnessed survey
based on the test procedures***

- > Mandatory items
- > Items to be conducted in case of changes



Review of records based on the program (If there are changes to the program or systems)

+ Tests are required based on the test procedures in special survey

Conduct at every Special Survey

- ✓ Confirm basic security is maintained.

Identify

Vessel asset inventory

Protect

Security zones and network segmentation

Antivirus, antimalware, antispam and other protections from malicious code

Remote access control and communication with untrusted networks

Use of Mobile and Portable Devices

Additional inspection when there are changes

- ✓ Confirm functionality is not impaired by modification.

Protect

Network protection safeguards

Wireless communication

Detect

Network operation monitoring

Respond

Local, independent and/or manual operation

Network isolation

Fallback to minimum risk condition

Recover

Backup and restore capability

Controlled shutdown, reset, roll-back and restart

The test procedures prepared for the new shipbuilding survey are available.

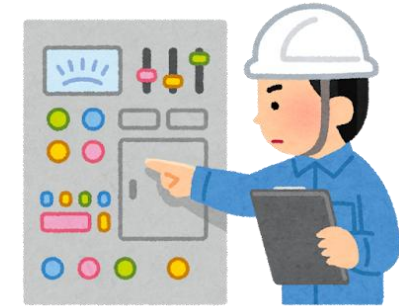
In case of change of ship management company



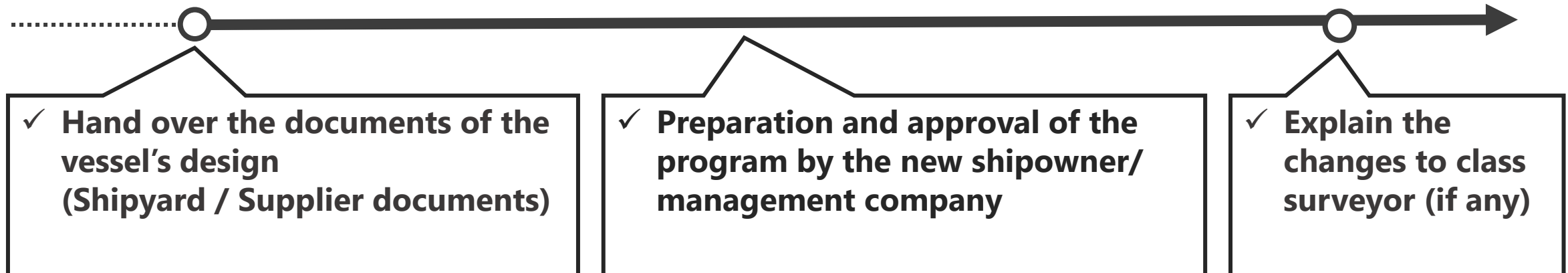
Take over



Operation



First annual survey



- ✔ **Sharing information of shipowner supplies to the shipyard in early stages** (Even if provisional)
- ✔ **Approval of the program prior to the first annual survey**
- ✔ **[Annual surveys] records demonstrating implementation based on the program**
- ✔ **[Special surveys] tests accordance with the test procedure.**

THANK YOU

for your kind attention