International Standard

ISO 23799

First edition
2024-01

Ships and marine technology — Assessment of onboard cyber safety

Reference number
ISO 23799:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

With the development of digitalization, intelligence and the networking of ships, an increasing number of control systems, communication and navigation systems, information management systems and equipment are constantly connected to the ship network to access external information. The hidden danger of shipborne equipment suffering from network threats is growing. Network security risk assessment uses scientific methods and means to systematically analyse the threats faced by ship borne systems and their existing vulnerabilities, assess the degree of harm that can be caused once the security time occurs, propose targeted countermeasures and measures, and control the risks at an acceptable level.

Based on the urgent need to enhance the awareness of network risk threats, this document brings together content from IEC 31010:2019, MSC-FAL.1/Circ 3. IACS Rec.171, IACS UR E26 and UR E27, to provide the elements of shipboard network security risk assessment and the basic criteria for assessment process, assessment preparation, security risk identification, security risk analysis and security risk assessment. The recommended method of shipboard network security risk assessment which is specified in this document can help improve the ship's network security defence capability, and provide assistance to stakeholders, including:

a) identifying onboard network security risks;

b) evaluating the consequences and possibility of shipboard network security risks;

c) prioritizing shipboard network security risk disposal.

Ships and marine technology — Assessment of onboard cyber safety

1 Scope

This document establishes the elements of onboard cyber risk assessment and specifies requirements for the assessment process, assessment preparation, risk identification, risk analysis and risk evaluation.

This document applies to the risk assessment of onboard cyber systems based on network technologies which mainly include bridge systems, cargo management systems, propulsion and machinery management and power control systems, access control systems, passenger or visitor servicing and management systems, passenger-facing networks, core infrastructure systems, administrative and crew welfare systems and communication systems.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 31000, *Risk management — Guidelines*

IEC 31010, *Risk management — Risk assessment techniques*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
onboard cyber safety
situation where the hardware and software of the shipboard network system and the data in the system are protected from damage, alteration and leakage due to accidental or malicious reasons, and the system operates continuously, reliably and normally without interruption of network services

3.2
onboard cyber risk
combination of the likelihood and impact loss of a security incident

Note 1 to entry: In the onboard network system, damage can be caused to assets by taking advantage of the vulnerabilities that exist in the system and by adopting specific means to attack the onboard network so that the information in the onboard network is leaked, and the network functions are missing.

3.3
onboard cyber risk assessment
entire process of risk identification, risk analysis and risk evaluation

Note 1 to entry: An onboard cyber risk assessment is performed by establishing the value of information assets; identifying the existence (or potential existence) of applicable threats and vulnerabilities, existing controls and their impact on the identified risks; and determining potential consequences. Finally, derive risks are prioritized and ranked against the risk assessment guidelines in the environment creation.

3.4
onboard cyber risk identification
process of discovering, enumerating and describing the elements of *onboard cyber risks* (3.2)

Note 1 to entry: This involves identifying risk sources, the scope of impact, incidents and their causes and potential consequences that can have an impact on the ship's voyage. This helps to determine what can occur in onboard cyber systems that will result in potential loss, and also gives insight into how (threat identification), where (asset identification), and why (vulnerability identification, existing control measures identification) the potential loss will occur.

3.5
onboard cyber risk analysis
analysis of the likelihood and impact loss of consequences for the security incident onboard

3.6
onboard cyber risk evaluation
risk metrics for accident scenarios encountered by the ship to assess the risk level of the accident situation

3.7
onboard cyber asset
existing resources that are valuable to the system onboard

3.8
onboard cyber threat
potential causes of damage to the shipboard network system or environmental factors causing damage to the shipboard network

3.9
onboard cyber security incident
events that have an actual or potential negative impact on shipboard systems, networks and computers or the information they process, store, or transmit, and that require response measures to eliminate their consequences

3.10
impact loss of consequences of incident scenarios
damage caused by a security event to the software, hardware, functions and data of the onboard system, resulting in interruption of system operations

Note 1 to entry: The severity of such loss depends primarily on the cost of restoring the system to normal operation and eliminating the negative impact of the security incident.

4 Elements and process of risk assessment

4.1 Relationship of elements

The basic elements of risk assessment include assets, threats, vulnerabilities, and security measures. The relationship of the basic elements is shown in Figure 1.

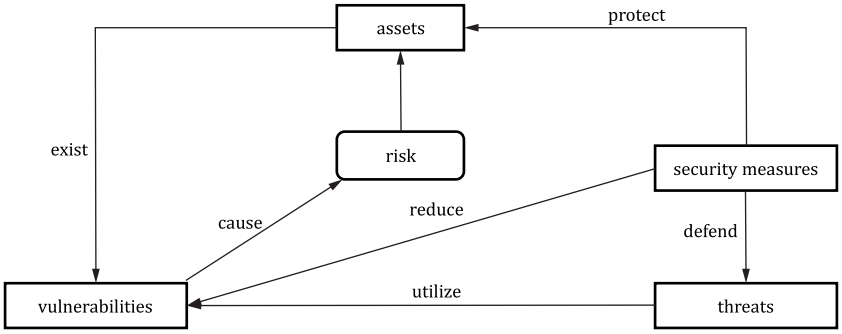


Figure 1 — Relationships of risk assessment elements

The core of the risk element is the asset, but assets are vulnerable. Security measures are used to make it more difficult for asset vulnerabilities to be exploited, to defend against external threats, and to achieve asset protection. Threats cause risk by exploiting vulnerabilities created by assets. When a risk is transformed into an onboard cyber security incident, it has an impact on the operational status of the asset.

4.2 Process of risk assessment

Onboard cyber risk assessment shall comply with ISO 31000 and IEC 31010, which includes four processes: assessment preparation, risk identification, risk analysis and risk evaluation (see Figure 2).

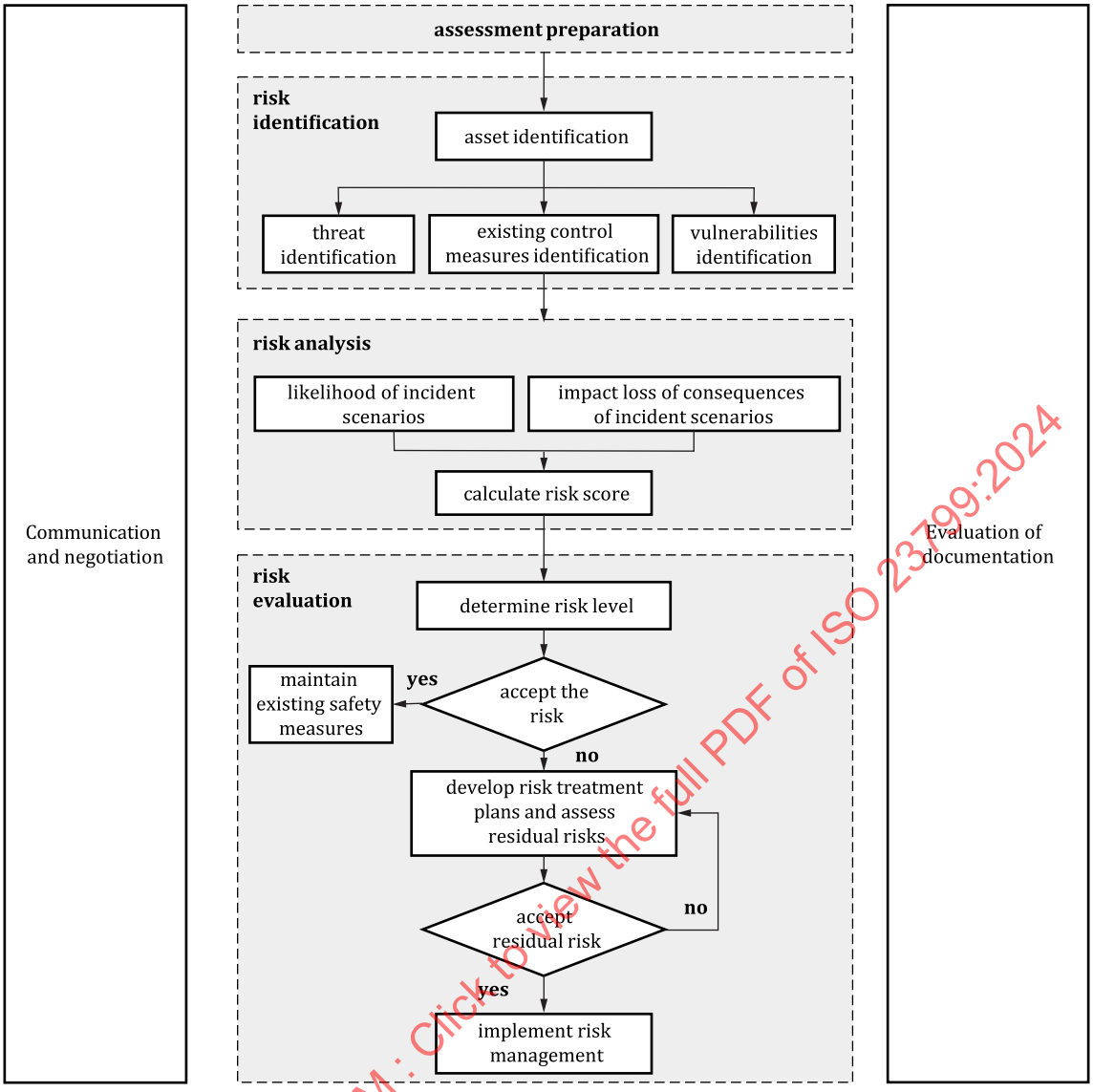


Figure 2 — Process of onboard cyber risk assessment

Assessment preparation includes the development of an assessment work plan, the formation of an assessment team according to the needs of the assessment work, and the clarification of the responsibilities of each party.

Risk identification includes carrying out asset identification, threat identification, identification of existing security measures and vulnerability identification.

Risk analysis includes the calculation of risk values based on the results of identification.

Risk evaluation includes determining the risk level based on risk evaluation guidelines.

Communication, negotiation, and evaluation of documentation for the evaluation process should be carried out throughout the entire risk assessment process.

During the risk assessment, in the absence of relevant statistical data, experts are required to make judgements based on experience for the process of risk identification and risk analysis. A judgement matrix or other methods can be used to analyse whether the consistency of expert judgement meets the requirements.

Risk assessment is an ongoing activity, and should be conducted again when the policy environment, external threat environment, business objectives and security objectives of the assessment target change.

5 Assessment preparation

Determine the objectives of the risk assessment on the basis of the work form, the stage in the life cycle and the safety assessment needs of the assessed unit.

The object, scope and boundaries of the risk assessment should be determined before the assessment.

According to the needs of the evaluation work, an evaluation team is formed; the evaluation methods are clarified, and evaluation tools and manual methods should be used for evaluation.

Conduct preliminary research and analysis, including: reviewing detailed documentation of shipboard system maintenance and support and analysing potential impact levels, identifying key manufacturers of shipboard system equipment using a risk-based approach, identifying shipowners' potential for onboard network and equipment maintenance and support have contractual requirements and obligations.

Risk assessment criteria should be established and comply with the requirements of in ISO/IEC 27005:2022, 6.4 to ensure that risk assessment results can be graded and the organization's later risk control strategies can be determined.

Develop a complete risk assessment plan, determine the assessment basis, and obtain the support and approval of the organization's top management.

6 Risk identification

6.1 Identification of asset

Asset identification should include physical, software and data assets throughout the shipboard network.

Onboard cyber assets are generally classified as information technology (IT) systems and operational technology (OT) systems. IT systems are usually used to manage data and support business functions through data; OT systems can directly control or monitor physical equipment and operations through software and hardware.

IT systems are more vulnerable to security risks because they are usually associated with networks and data transmission. Since the OT system can directly issue control commands to the ship, once it is attacked by the network, the navigation of the ship is affected, and has higher security requirements in terms of security assurance level.

According to the difference of security level and vulnerability, the assets are divided into IT systems and OT systems. Physical assets, software assets and data assets are listed in Figure 3.

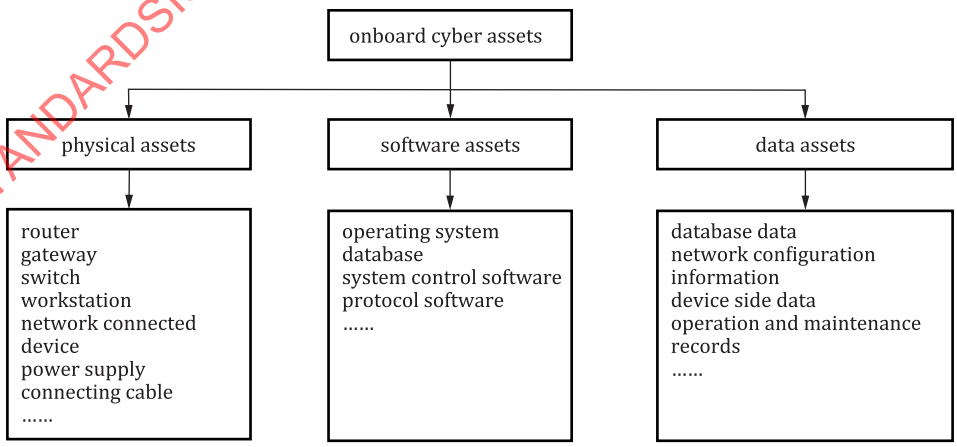


Figure 3 — Classification of onboard cyber assets

The identification of onboard cyber assets should be combined with the onboard environment and operating business characteristics. At least nine categories of ship risk systems should be included, as shown in Table 1.

For different ship types, different technical characteristics and specific requirements, ship risk systems can be supplemented in the subclass system.

Table 1 — Identification content of onboard cyber assets

Serial number	Class	Division
1	Communication systems (IT+OT)	— integrated communication systems — satellite communication equipment — voice over internet protocols (VOIP) equipment — wireless networks (WLANs) — systems used for reporting mandatory information to public authorities
2	Bridge systems (OT)	— integrated navigation system — positioning systems (GPS, etc) — Electronic Chart Display Information System (ECDIS) — Dynamic Positioning (DP) systems — systems that interface with electronic navigation systems and propulsion/ manoeuvring systems — Automatic Identification System (AIS) — Global Maritime Distress and Safety System (GMDSS) — radar equipment — Voyage Data Recorders (VDRs) — Bridge Navigational Watch Alarm System (BNWAS) — Shipboard Security Alarm Systems (SSAS)
3	Propulsion, machinery management and power control systems (OT)	— engine governor — power management — integrated control system — alarm system — bilge water control system — water treatment system — emissions monitoring — heating, ventilation and air-conditioning monitoring — damage control systems — other monitoring and data collection systems e.g. fire alarms
4	Access control systems (IT)	— surveillance systems such as CCTV network — electronic “personnel-on-board” systems

Table 1 *(continued)*

Serial number	Class	Division
5	Cargo management systems (OT)	— Cargo Control Room (CCR) and its equipment — onboard loading computers and computers used for exchange of loading information and load — plan updates with the marine terminal and stevedoring company — remote cargo and container tracking and sensing the system's level indication system — valve remote control system — ballast water systems — reefer monitoring systems — water ingress alarm system
6	Passenger or visitor servicing and management systems (IT)	— property management system (PMS) — ship management systems (often including electronic health records) — financial related systems — ship passenger/visitor/seafarer boarding access systems — infrastructure support systems like domain naming system (DNS) and user authentication/authorization systems — incident management systems
7	Passenger-facing networks (IT)	— passenger wi-fi or Local Area Network (LAN) internet access, e.g. where onboard personnel can connect their own devices — guest entertainment systems
8	Core infrastructure systems (IT and OT)	— security gateways — routers — switches — firewalls — Virtual Private Network(s) (VPN) — Virtual LAN(s) (VLAN) — intrusion prevention systems — security event logging systems
9	Administrative and crew welfare systems (IT and OT)	— administrative systems — crew Wi-Fi or LAN internet access, e.g. where onboard personnel can connect their own devices

According to the importance of the asset (economic value of the asset, the degree of impact on the business) and security attributes, the onboard cyber assets are assigned values and divided into three levels. The higher the level, the more important the asset is, as shown in Table 2.

Table 2 — Assignment of assets value levels

Level	Mark	Class	Description
1	Low	Not so important	The destruction of its security properties can cause very small losses, and the specific amount can be defined by each country. For example, the direct economic loss is less than US $10 000, and the IT system is temporarily interrupted.
2	Moderate	Important	The destruction of its security attributes can cause serious losses, and the specific amount can be defined by each country. For example, the direct economic loss is US $10 000 to US $ 20 000, and the OT system is temporarily interrupted or ineffective.
3	High	Very important	The destruction of its security attributes can cause very serious losses, and the specific amount can be defined by each country. For example, the direct economic loss is greater than US $20 000, and the network system cannot be recovered.

6.2 Identification of threat

The content of threat identification includes the source, subject, type, motive and frequency of threats.

The onboard cyber threat types and vulnerabilities are shown in Table 3.

Table 3 — Threat types and vulnerabilities of onboard cyber safety

Threat types	Threat vulnerabilities
Hardware and software malfunction	Lack of troubleshooting plans and process
	Lack of periodic component replacement schemes
	No periodic maintenance of the communication links
	Using unstable new version software
	Lack of effective software version
	Unclear or incomplete specifications for developers
Physical environment threat	Sensitivity to humidity, dust, corrosion
	Sensitivity to voltage variations, electromagnetic interference, temperature variations
Denial of actions or error in use	Lack of sufficient security training
	Incorrect use of software and hardware
	Lack of security awareness
Ineffective management	Lack of regular management reviews
	Lack of procedures for reporting security weaknesses
Malicious code and virus	No start-up or timely replacement of anti-virus software
	Unprotected sensitive traffic
	No disabled system function of automatic running
	Lack of back-up
Abuse and forging of rights	Lack of formal process for access right review (supervision)
	No “logout” when leaving the workstation
	No or insufficient software testing
	Well-known flaws in the software
	Disposal or re-use of storage media without proper erasure
Hacking techniques	Insecure network architecture
	Unprotected public network connections
	Transfer of passwords in clear

Table 3 *(continued)*

Threat types	Threat vulnerabilities
Physical damage	Lack of defined disciplinary process in case of information security incident
	Lack of formal policy on mobile computer usage
	Lack of control of off-premise assets
	Lack of established monitoring mechanisms for security breaches
Leak	Unprotected storage
	Lack of disposition control of medium or data
	Uncontrolled copying
Tampering	Uncontrolled downloading and use of software
	Lack of back-up copies of software or data

The threat level is assigned according to the frequency of threat occurrence, as shown in Table 4. The threat frequency should be judged according to experience and relevant statistical data, taking into account the following aspects:

— threats which have appeared in past security incident reports and their frequency statistics;

— threats which have been discovered through detection tools and various logs in the actual environment and their frequency statistics;

— threats which have been detected by monitoring in the actual environment and their frequency statistics;

— societal or industry-specific threats which have been publicly released and their frequency statistics, as well as threat warnings issued.

Table 4 — Assignment of threats level

Threat level	Frequency/probability	Definition	Frequency (ships/year)
5	Super high	Can happen once a week on one ship	50
4	High	Can happen once a month on one ship	10
3	Moderate	Can happen once a year on ten ships	0,1
2	Low	Can happen once a year on one thousand ships	10^{-3}
1	Super low	Can happen once a life cycle on five thousand ships	10^{-5}

6.3 Identification of vulnerability

For the assets protected by ships, identify the vulnerabilities that can be exploited by threats, and evaluate the influence severity of the vulnerabilities.

Vulnerability identification is mainly carried out from two aspects: technology and management. Technical vulnerability involves security issues at various levels such as the physical layer, network layer, system layer, and application layer of ships. Management vulnerability is mainly divided into technical management vulnerability and organizational management vulnerability. Technical management vulnerability is related to specific technical activities, and organizational management vulnerability is related to management environment.

In the process of vulnerability identification, the difficulty level of exploiting the vulnerability and the influence severity of the vulnerability should be judged from the perspective of the organization's security strategy.

The content of vulnerability identification objects is shown in Table 5.

Table 5 — Vulnerability identification content

Type	Identify objects	Identify content
Technical vulnerability	Physical environment	Compartment layout, fire protection, water and air tightness, power supply and distribution, electromagnetic protection, line protection, area protection, equipment management, etc.
	Network structure	Border protection measures, shipboard computer network design, third-party access control to assets and networks, network security configuration, etc.
	System software	From system updates, system software patches, antivirus and malware protection, etc.
	Application middleware	Protocol security, interface security, routing configuration, data transaction integrity, data integrity, etc.
	Operating system	Software update, access, ship access control, remote access control, data integrity, backup and recovery of functional modules such as cargo systems, integrated bridge systems, main and auxiliary equipment and control systems, communication systems, and ship/fleet management systems mechanism, etc.
Management vulnerability	Technical management	Cabin and environment security, network management, administrator account and password, malicious code prevention, operation management, etc.
	Organizational management	Critical equipment or systems always connected to shore, staff training and skills, contingency plans and procedures, network asset registry updates, etc.

Using the identification results of vulnerabilities and existing security control measures, combined with the requirements of vulnerability access paths and trigger requirements, levels shall be established to show how difficult it is to exploit vulnerabilities. The higher levels represent the vulnerabilities which can be more easily exploited.

The difficulty level assigned to exploiting vulnerabilities should be determined by the ability of the ship's existing network security measures to resist network threats. The method of assigning these difficulty levels is shown in Table 6.

Table 6 — Assigning the difficulty level of exploiting vulnerabilities

Level	Mark	Description
5	Super high	After implementing the control measures, vulnerabilities remain very easily exploited
4	High	After implementing the control measures, vulnerabilities are easily exploited
3	Moderate	After implementing the control measures, vulnerabilities are generally exploited
2	Low	After implementing the control measures, vulnerabilities are hard to exploit
1	Super low	After implementing the control measures, vulnerabilities are almost impossible to exploit

According to the vulnerability identification results, it is also necessary to assign a value to the influence level of the vulnerability. The influence level of the vulnerability refers to the impact on the value of ship assets after the occurrence of security incidents due to the exploitation of the vulnerability.

The influence level assigned to the vulnerability should comprehensively consider the impact of security incidents on the confidentiality, integrity and availability of assets, and adopt the classification method. The higher the level value, the higher the degree of influence. The method of assigning the influence levels is shown in Table 7.

Table 7 — Assigning the influence level of the vulnerability

Level	Mark	Description
5	Super high	If the vulnerability is exploited by threats, there will be particularly significant damage to assets
4	High	If the vulnerability is exploited by threats, there will be significant damage to assets
3	Moderate	If the vulnerability is exploited by threats, there will be general damage to assets
2	Low	If the vulnerability is exploited by threats, there will be less damage to assets
1	Super low	If the vulnerability is exploited by threats, damage to assets is negligible

6.4 Identification of existing control measures

Based on the threats and vulnerabilities in the cyber onboard ships system, the existing security control measures are taken as technical measures, which can be divided into preventive security measures and protective security measures. The former can reduce the possibility of a threat exploiting a vulnerability to cause a security accident, the latter can reduce the loss to an organization or system after a security accident.

The existing security control measures identification process should include the existing security control measures, and its current operation effectiveness. On the basis of that, the need for supplementary security control measures to effectively deal with risks should be determined.

The existing control measures identification process shall incorporate the following methods:

— Review documents containing control measures, such as a risk handling implementation plan. If there is full record of the cyber information security management process, the existing or planned control measures can be adopted.

— For the control measures which have been implemented by the cyber information onboard ships system, check the personnel and users who are responsible for the cyber information security onboard ships.

— Perform an on-site review of physical control measures, then compare the control measures on-site with the control measures list that should be implemented, and check their correctness and effectiveness.

— Check the review results.

7 Risk analysis

7.1 Risk analysis process

Onboard cyber risk analysis process can be qualitative or quantitative, or a combination of these, depending on the circumstances. Risk analysis process is shown in Figure 4.

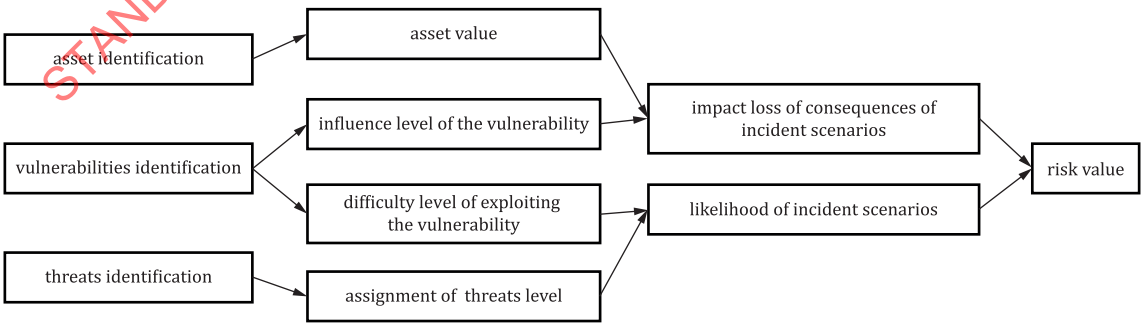


Figure 4 — Risk analysis methodology process

On the basis of onboard cyber risk identification, risk analysis shall be carried out.

— According to the influence level of the vulnerability and asset value caused by the security incident, calculate the impact loss of consequences of incident scenarios.

— Take account of the threat level, and the difficulty level of exploiting vulnerabilities when assessing the likelihood of incident scenarios.

— Calculate the risk value according to the risk assessment criteria and determine the risk level which is used for risk decision-making.

7.2 Risk calculation method

Multiplication is suitable for the situation where the value of two elements is multiplied to determine the value of another element. It is a quantitative calculation method, that is, the function $z = f(x, y) = x \times y$.

The matrix method is suitable for the case where the value of another element is determined by two elements, that is, the function $z = f(x, y)$. A two-dimensional matrix is constructed with the values of x and y, the row value of the matrix is the values of y, the column value of the matrix is the value of x, and the $m \times n$ values in the matrix are the values of the function z, which are as follows.

— $x = \{x_1, \ldots, x_m\}$, $1 \le i \le m$, x_i is a positive integer;

— $y = \{y_1, \ldots, y_n\}$, $1 \le j \le n$, y_j is a positive integer;

— z_{ij} should be calculated by the function of $z_{ij} = x_i + y_j$, $z_{ij} = x_i \times y_j$, $z_{ij} = \alpha \times x_i + \beta \times y_j$, where α and β are normal coefficients, and the calculation formula should have a uniform trend of increase and decrease.

7.3 Impact loss of consequences of incident scenarios

The impact loss of consequences of incident scenarios should be calculated according to Formula (1).

$$F(I_a, V_a) = I_a \times V_a \tag{1}$$

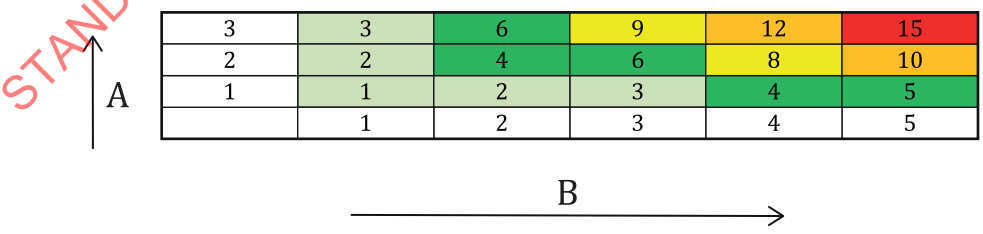
where

F is the impact of consequences;

I_a is the asset value;

V_a is the influence level of the vulnerability.

Construct a two-dimensional matrix of asset value and influence level of the vulnerability, and use Formula (1) to calculate impact value (see Figure 5), of which the value range is 1 to 15.



Key

A asset value

B influence level of the vulnerability

Figure 5 — Calculation matrix for impact loss of consequences $F(I_a, V_a)$

The impact loss value of consequences is divided into five levels and the impact degree is marked (see Table 8).

Table 8 — Impact loss level of consequences

Impact value of security incident	Level	Mark	Description
1–3	1	Super low	No health effect/injuries. No damage to environment, assets, finances, or company's reputation.
4–6	2	Low	Very slight health effect/injuries. Very slight damage to environment, assets, finances, or to company's reputation.
7–9	3	Moderate	Some health effect/minor injuries. Minor damage to environment, assets, finances, or to company's reputation.
10–12	4	High	Major health effect/relatively serious injuries. Local but major damage to environment, assets, finances, or to company's reputation.
13–15	5	Super high	Fatality or permanent disabilities. Widespread, significant damage to environment, assets, finances, or company's reputation.

7.4 Likelihood of incident scenarios

According to the statistics and analysis of the threat intelligence of cyber security incidents occurring in the current period, month or quarter by experts, a comprehensive assessment of the frequency and possibility of threats should be carried out.

The likelihood of incident scenarios is calculated according to Formula (2).

$$L(T,V) = T \times V \tag{2}$$

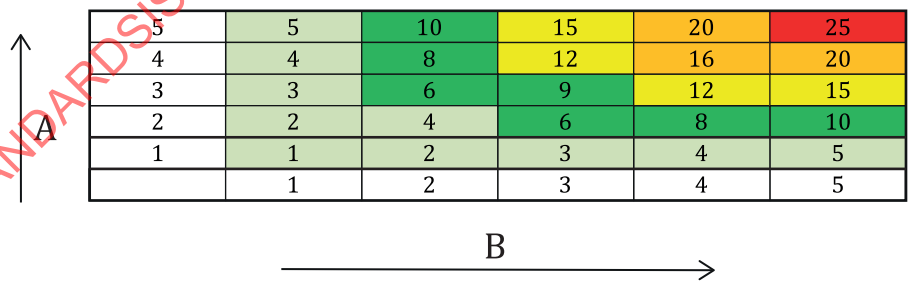
where

L is the likelihood of incident scenarios;

T is the assignment of threats level;

V is the difficulty level of exploiting the vulnerability.

Construct a two-dimensional matrix of threat level and the difficulty level of exploiting the vulnerability. Use Formula (2) to calculate the value of likelihood (see Figure 6), of which the value range is 1 to 25.



Key

A threats level

B difficulty level of exploiting the vulnerability

Figure 6 — Computational matrix for the likelihood of incident scenarios $L(T,V)$

The likelihood value of incident scenarios is divided into five levels and the level description is shown in Table 9.

Table 9 — Likelihood level of incident scenarios

Likelihood value of security incident	Level	Mark	Description
1–5	1	Very low	Not existing. Close to being something unimaginable.
6–10	2	Low	Almost not existing, but only extremely rarely and as the result of a chain of many unfortunate events.
11–15	3	Moderate	Incident has probably occurred in own company, but in the context of faulty equipment or by surprising mistakes made by people involved.
16–20	4	High	Happens occasionally in own company, typically in the context of faulty equipment or by mistakes by people involved (the kind of mistakes that tend to happen on board from time to time).
21–25	5	Very high	Happens frequently when undertaking the work in question

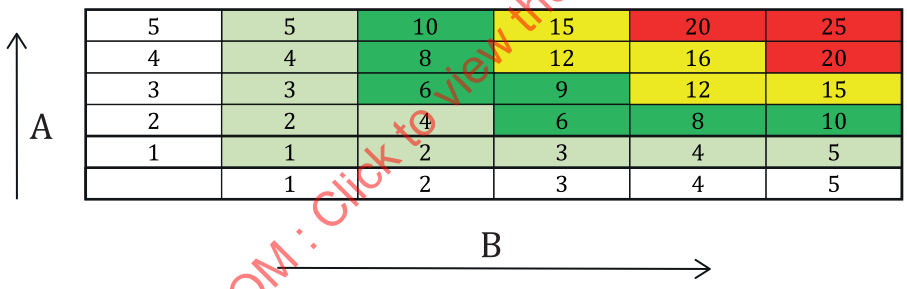
7.5 Risk calculation of onboard cyber security

Calculate the risk value according to the level of likelihood of incident scenarios and the impact loss of consequences of incident scenarios. See Formula (3).

$$R[L(T, V),F(I_a, V_a)]= L(T, V) \times F(I_a, V_a) \quad (3)$$

where R is the risk value.

Construct a two-dimensional matrix of the level of likelihood of incident scenarios and the impact loss of consequences of incident scenarios. Use Formula (3) to calculate the risk value (see Figure 7), of which the value range is 1 to 25.



Key

A level of likelihood

B level of impact loss of consequences

Figure 7 — Computational matrix for the risk value $R(L(T, V),F(I_a, V_a))$

8 Risk evaluation

The determination stage of risk evaluation results includes two work processes: evaluating the risk levels and evaluating the risk status comprehensively.

According to the formulated onboard cyber risk evaluation criteria, all risk calculation results are graded into four levels. Every level represents the severity of the corresponding risk. The evaluation results of risk levels are shown in Table 10.