Designation: F3449 – 20

An American National Standard

Standard Guide for Inclusion of Cyber Risks into Maritime Safety Management Systems in Accordance with IMO Resolution MSC.428(98)—Cyber Risks and Challenges[1]

This standard is issued under the fixed designation F3449; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This guide is designed to provide the maritime industry guidance, information, and options for incorporating cyber elements into safety management systems (SMS) in accordance with the International Safety Management (ISM) Code and other national (United States) and international requirements.

1.2 This guide will support U.S. maritime operating companies but is a guide only and does not recommend a specific course of action. However, this guide is to be used to improve cyber safety, address vulnerability, recommend and outline training, and raise knowledge and awareness of cyber threats by leveraging documented, auditable SMS mechanisms.

1.3 The purpose of this guide is to offer guidance, information, and options based on a consensus of opinions but not to establish a standard practice. Each organization shall evaluate their SMS, their information management systems at sea and ashore, and the level of cyber risk that exists within the organization to determine the best methods of compliance with the cybersecurity requirements of the ISM Code or other legal or self-imposed requirements or both.

1.4 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety, health, and environmental practices and determine the applicability of regulatory limitations prior to use.*

1.5 *This international standard was developed in accordance with internationally recognized principles on standardization established in the Decision on Principles for the Development of International Standards, Guides and Recommendations issued by the World Trade Organization Technical Barriers to Trade (TBT) Committee.*

2. Referenced Documents

2.1 *2.1 ISO Standards:*[2]

ISO 9001:2015 Quality Management Systems — Requirements, Section 7.5, Documented Information

ISO/IEC 27000:2018 Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary

2.2 *USCG Guidance and Policy:*[3]

NVIC 05-17 Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities

USCG CG-5P Policy Letter 08-16 Reporting Suspicious Activity and Breaches of Security

2.3 *Other Standards:*

46 CFR Subchapter M Towing Vessels[4]

BIMCO The Guidelines on Cybersecurity Onboard Ships[5]

IMO Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems[6]

The International Safety Management (ISM) Code Chapter IX of the International Convention for the Safety of Life at Seal (SOLAS)[7]

MSC-FAL.1/Circ.3 Interim Guidelines on Maritime Cyber Risk Management[7]

[1] This guide is under the jurisdiction of ASTM Committee F25 on Ships and Marine Technology and is the direct responsibility of Subcommittee F25.07 on General Requirements.

Current edition approved June 1, 2020. Published July 2020. DOI: 10.1520/F3449-20.

[2] Available from American National Standards Institute (ANSI), 25 W. 43rd St., 4th Floor, New York, NY 10036, http://www.ansi.org.

[3] Available from the U.S. Coast Guard (USCG), U.S. Coast Guard Headquarters, 2703 Martin Luther King Jr Ave Se Stop 7318, Washington, DC 20593, https://www.dco.uscg.mil.

[4] Available from U.S. Government Printing Office, Superintendent of Documents, 732 N. Capitol St., NW, Washington, DC 20401-0001, http://www.access.gpo.gov.

[5] Available from https://iumi.com/news/news/bimco-the-guidelines-on-cyber-security-onboard-ships.

[6] Available from the International Maritime Organization, http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428(98).pdf.

[7] Available from International Maritime Organization (IMO), 4, Albert Embankment, London SE1 7SR, United Kingdom, http://www.imo.org.

3. Terminology

3.1 *Definitions:*

3.1.1 *access control, n*—practice of selective limiting of the ability and means to communicate with or otherwise interact with a system, use system resources to handle information, gain knowledge of the information the system contains, or control system components and functions.

3.1.2 *antivirus software, n*—software utility that detects, prevents, and removes viruses, worms, and other malware from a computer.

3.1.3 *application programming interface, API, n*—set of routines, protocols, and tools for building software and applications.

3.1.4 *archive, n*—long-term physically separated storage.

3.1.5 *authentication, n*—security measure designed to establish the validity of a transmission, message, or originator or a means of verifying an individual's authorization to receive specific categories of information.

3.1.6 *availability, n*—ensuring timely and reliable access to and use of information.

3.1.7 *backup, n*—copy of files and programs made to facilitate recovery, if necessary.

3.1.8 *binding, v*—process of associating two related elements of information.

3.1.9 *botnet, n*—number of internet-connected computers communicating with other similar machines in which components located on networked computers communicate and coordinate their actions by command and control or passing messages to one another.

3.1.10 *capability, n*—ability to execute a specified course of action.

3.1.11 *certificate, n*—digital representation of information that, at least: (*1*) identifies the certification authority issuing it, (*2*) names or identifies its subscriber, (*3*) contains the subscriber's public key, (*4*) identifies its operational period, and (*5*) is digitally signed by the certification authority issuing it.

3.1.12 *client (application), n*—system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server..

3.1.13 *communications, n*—means for a vessel to communicate with another ship or an onshore facility.

3.1.14 *compression, n*—reduction in the number of bits needed to store or transmit data.

3.1.15 *confidentiality, n*—preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

3.1.16 *cyberattack, n*—any type of offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices.

3.1.17 *cyber intrusion, n*—unauthorized access to your computer/service/or data is called intrusion.

3.1.18 *cyber risk, n*—potential of an undesirable or unfavorable outcome resulting from a given cyber action, activity, or inaction, or combination thereof.

3.1.19 *cybersafety, n*—guidelines and standards for computerized, automated, and autonomous systems that ensure those systems are designed, built, operated, and maintained so as to allow only predictable, repeatable behaviors, especially in those areas of operation or maintenance that can affect human, system, enterprise, or environmental safety.

3.1.20 *cybersecurity, n*—activity or process, ability or capability, or state whereby information and communication systems and the information contained therein are protected from and defended against damage, unauthorized use or modification, or exploitation.

3.1.21 *cyber vulnerability, n*—flaw in a system that can leave it open to attack.

3.1.22 *data, n*—quantities, characters, or symbols on which operations are performed by a computer being stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media.

3.1.23 *data assurance, n*—perception or an assessment of data's fitness and integrity to serve its purpose in a given context.

3.1.24 *detection processes, n*—methods of detecting intrusions into computers and networks.

3.1.25 *encryption, n*—conversion of electronic data into another form called ciphertext, which cannot be easily understood by anyone except authorized parties.

3.1.26 *exposure, n*—measure of a system at risk that is available for inadvertent or malicious access.

3.1.27 *firewall, n*—logical or physical break designed to prevent unauthorized access to information technology (IT) infrastructure and information.

3.1.28 *file transfer protocol, FTP, n*—standard network protocol used to transfer computer files between a client and server on a computer network.

3.1.29 *flaw, n*—unintended opening or access point in any software.

3.1.30 *human system, n*—interaction and contact between a human user and a computer system.

3.1.31 *hypertext transfer protocol, HTTP, n*—primary technology protocol on the web that allows linking and browsing.

3.1.32 *hypertext transfer protocol over secure socket layer, HTTPS, n*—protocol to transfer to encrypted data over the web.

3.1.33 *information security management system, ISMS, n*—set of policies with information security management or IT-related risks.

3.1.34 *information technology, IT, n*—equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

3.1.35 *inside threat, n*—entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.

3.1.36 *integrity, n*—guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity.

3.1.37 *International Safety Management (ISM) Code, n*—required international regulation in the marine industry and a vital component of the SOLAS Convention (Safety of Life at Sea) requiring a company's operating vessels to submit a safety management system (SMS) for audit and subsequent approval by Flag Administration or Recognized Organization (RO).

3.1.38 *International Maritime Organization, IMO, n*—specialized agency of the United Nations responsible for regulating international shipping, primarily focused on ensuring and improving safety, security, and environmental stewardship.

3.1.39 *internet of things, IoT, n*—internetworking of physical devices, such as vessels, vehicles, buildings and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.

3.1.40 *intrusion detection system, IDS, n*—device or software application that monitors a network or systems for malicious activity or policy violations.

3.1.41 *local area network, LAN, n*—computer network that interconnects computers within a particular area and does not connect to the internet; this applies to onboard ship networks.

3.1.42 *machinery control systems, MCS, n*—IT systems that report operating parameters or control operation of equipment, which commonly use programmable logic controllers (for example, fuel tank level indicators or throttle control systems).

3.1.43 *management of change, n*—systematic way to deal with change within an organization to deal effectively with the change and capitalize on change opportunities.

3.1.44 *network, n*—infrastructure that allows computers to exchange data by wireless or cable wireless network interactions.

3.1.45 *network topology diagram, n*—shows how the elements of a computer network are arranged.

3.1.46 *non-repudiation, n*—assurance that the sender is provided with proof of delivery and the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.

3.1.47 *operational technology, OT, n*—information system used to control industrial processes such as manufacturing, product handling, production, and distribution.

3.1.47.1 *Discussion*—Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes.

3.1.48 *original equipment manufacturer, OEM, n*—company that makes parts or subsystems that are used in another company's end product.

3.1.49 *outside threat, n*—unauthorized entity from outside the domain perimeter that has the potential to harm an information system through destruction, disclosure, modification of data, or denial of service, or combination thereof.

3.1.49.1 *Discussion*—Such an e-mail may also request that an individual visit a fake website using a hyperlink included in the e-mail.

3.1.50 *phishing, v*—sending e-mails to a large number of potential targets asking for particular pieces of sensitive or confidential information.

3.1.51 *programmable logic controller, PLC, n*—digital computer used for automation of industrial electromechanical processes.

3.1.52 *public key infrastructure, PKI, n*—framework established to issue, maintain, and revoke public key certificates.

3.1.53 *ransomware, n*—malware that encrypts data on systems until the distributor decrypts the information.

3.1.54 *remote desktop protocol, RDP, n*—proprietary protocol developed by Microsoft that provides a user with a graphical interface to connect to another computer over a network connection.

3.1.55 *resilience, n*—characteristic that enables a system to resist disruption and adapt to minimize the impact of disruptions.

3.1.56 *Resolution MSC.428(98), n*—encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

3.1.57 *risk, n*—potential or threat of undesired consequences occurring to personnel, assets, or the environment as a result of vulnerabilities in systems, staff, or assets.

3.1.58 *risk assessment, n*—process that collects information and assigns values to risks for informing priorities, developing or comparing courses of action, and informing decision making.

3.1.59 *risk management, n*—process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

3.1.60 *risk matrix, n*—matrix that is used during risk assessment to define the level of risk by considering the category of probability or likelihood against the category of consequence severity.

3.1.61 *router, n*—device that forwards data from one network to another network regardless of physical location.

3.1.62 *Safety Management System, SMS, n*—comprehensive management system designed to manage safety elements in the workplace.

3.1.63 *scanning, v*—procedure for identifying active hosts or potential points of exploit or both on a network either for the purpose of attacking them or network security assessment.

3.1.64 *sensitive information, n*—any digital data that can be classified as private or corporate not meant for public access.

3.1.65 *server, n*—system entity that provides a service in response to requests from clients.

3.1.66 *social engineering, n*—nontechnical technique used by potential cyber attackers to manipulate insider individuals into breaking security procedures, typically, but not exclusively, through interaction by means of social media.

3.1.67 *social media, n*—computer-mediated online tools that allow people, companies, and other organizations, including nonprofit organizations and governments, to create, share, or exchange information, career interests, ideas, and pictures/videos in virtual communities and networks.

3.1.68 *software, n*—set of instructions and its associated documentations that tells a computer what to do or how to perform a task.

3.1.69 *Subchapter M, n*—U.S. Coast Guard (USCG) regulations that legally define rules for the inspection, standards, and safety policies of towing vessels.

3.1.70 *Transportation Worker Identification Credential, TWIC, n*—provides a tamper-resistant biometric credential to maritime workers requiring unescorted access to secure areas of port facilities, outer continental shelf facilities, and vessels regulated under the Maritime Transportation Security Act of 2002 (MTSA) and all USCG credentialed merchant mariners.

3.1.71 *water holing, v*—establishing a fake website or compromising a genuine site to exploit visitors.

3.1.72 *wide area network, WAN, n*—network that can cross regional, national, or international boundaries.

3.1.73 *wi-fi, n*—all short-range communications that use electromagnetic spectrum to send and receive information without wires.

3.1.74 *zeroize, v*—method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data.

4. Summary of Guide

4.1 The need to protect information and data has grown proportionally with the expansion of IT and the reliance of organizations on the use of IT in the course of their business activities. This is as true for the maritime industry as with any other industry.

4.2 Within the maritime industry, regulators, ship operators, ship crews, ports, and the general public have recognized the risk associated with a cybersecurity incident. The safety of the ship, crew, cargo, and environment can be significantly affected in the event of a damaging cyberattack, not to mention the possible loss of revenue, cargoes, and personal or proprietary information that can result from a cyber intrusion.

4.3 The IMO has recognized the risk and, through the adoption of Resolution MSC.428(98), created a requirement that a company's SMS appropriately address cyber risks. This is required of all companies by 1 January 2021.

4.4 This guide has been created to provide guidelines that a company can use to evaluate the cyber risk appropriate to the company, implement mitigation processes or procedures, train employees on those processes and procedures, document the training, and audit the system to ensure that the risk has been adequately addressed, the personnel are properly trained, and those processes or procedures that are created effectively mitigate that risk to the greatest extent possible.

4.5 Addressing cyber risks is not a one-time process but shall be continual and ongoing. As one risk is identified and mitigated, another is sure to develop. It is up to each company or organization to manage this risk continually and ensure that their personnel; systems (IT and mechanical); and developed training, processes, and procedures are robust enough to protect the information, operating systems, and equipment from coming to harm through cyberattack.

5. Significance and Use

5.1 *ISM Code Requirement*—In 1989, IMO adopted guidelines on management for the safe operation of ships and pollution prevention that is now the International Safety Management (ISM) Code that was made mandatory for ships trading on international waters through the International Convention for the Safety of Life at Sea, 1974 (SOLAS). In 1995, the IMO Assembly adopted the guidelines on implementation of the ISM Code by administrations by Resolution A.788(19). These guidelines were revised and adopted as Resolution A.913(22) in 2001. The guidelines were further revised and adopted as Resolution A.1022(26) in 2009 and entered into force on 1 July 2010.

5.1.1 *ISM Code Purpose*—The ISM Code is designed to improve the safety of international shipping and reduce pollution by encouraging self-regulation and oversight for identifying safety issues, taking corrective action, and promoting overall organization safety culture. The ISM Code establishes an international standard for the safe management and operation of ships and for the implementation of a SMS operating internationally.

5.1.2 *ISM Code Intent*—The intent of the ISM Code is to support and encourage the development of a safety culture in shipping by moving away from a culture of "unthinking" compliance with external rules toward a culture of "thinking" self-regulation of safety and the development of a "safety culture" that identifies safety issues and concerns and promotes proactive corrective actions. The safety culture involves moving to a culture of self-regulation with every individual from the top to the bottom empowered to ownership, responsibility, and action for improving and addressing safety.

5.2 *Additional Applications*—In addition to the ISM Code requirements, Flag States, industry organizations, and companies have initiated mandatory and nonmandatory SMS. All of these systems are being instituted to improve operational safety, identify safety issues, promote implementation of corrective actions, and improve overall organizational safety culture.

5.2.1 *Application/Use of Guide*—The intention of this guide is to leverage mandatory or voluntary safety management systems already in place to identify and address proactively cybersecurity issues that is a critical and ever-increasing safety concern in maritime operations. The intent of this guide is to provide items for consideration, recommendations, and contribute to the thought process for incorporating cyber elements into existing SMSs by providing information, structure, and elements for consideration in working through the process.

5.2.2 *Limitation of Guide*—This guide is not all encompassing but provides a foundation for starting the process by leveraging existing resource to address cybersecurity issues beginning with basic cyber hygiene and running all the way through nefarious intentional cyberattacks. This guide is interned to serve the entire maritime community but will be most beneficial to resource constrained organizations that may not have significant infrastructure or resources or both to secure comprehensive cybersecurity services and solutions.

5.2.3 *Focus Topics for Applying the Guide*—Considerations that are covered in the guide include management of change, cyber risk assessment, development of mitigation strategies, implementation, training, documentation, auditing, as well as examples of template language that can be leverage in SMS applications.

6. Procedure

6.1 *Management of Change*—There are two kinds of change: change that is forced on an organization and change that is planned and managed. The way to ensure that change is planned and managed is to identify those processes, activities, outside influences, and so forth that will cause change within your organization and ensure that appropriate risk assessments, policies, procedures, mitigations, and training are developed.

6.1.1 *Importance of Identifying the Intended and Unintended Results of Change:*

6.1.1.1 Changes being considered shall be thoroughly evaluated for both the intended and unintended results of the change. If adding procedures, then the addition of the new procedures shall be evaluated to ensure that they do not conflict with other procedures or instructions, they achieve the intended result, they are clearly written and are unambiguous, and they do not cause other, unintended, changes to the system or process. One shall also evaluate the consequences of personnel not fully engaged in the new procedures or processes or who do not fully implement the change as required.

6.1.1.2 Things to consider include, but are not limited to, how the change will affect the workload of the personnel required to carry out the new process or procedures, that the change will not require extensive training or any training required is identified and readily available before the change, that the change will not require support that is not easily available to the vessel at its normal ports of call, or that any support required is readily available to the vessel.

6.1.1.3 In addition, the personnel selected to act on the change shall be evaluated to ensure that they have or can be provided the requisite level of knowledge to allow them to be successful when complying with the changed conditions. For example, a change that requires certain types of network certification or knowledge to implement properly would not be appropriate if assigned to vessel crewmembers whose primary duties and knowledge base do not include network configuration or LAN management.

6.1.2 *Identify How Change Will Affect Entire Enterprise Ashore and at Sea:*

6.1.2.1 As described in 6.1.1, any change contemplated shall be evaluated to ensure that the implementers have a full understanding of how the change will affect shoreside operations as well as the operation of ships' systems.

6.1.2.2 It is important to identify what resources will be required to implement the change within the shoreside organization and what resources will be required to implement the change onboard the vessels and ensure that they are readily available. For change to be successful, the requirements should be identified and mitigation strategies and support put in place before implementation.

6.1.2.3 The management of change process should be used to shed light on the who, what, where, when, and how the change is to be implemented. Consideration should be given to questions such as, will more personnel be required when the change is implemented, will those new personnel need to be IT certified, will those onboard the ships have an adequate understanding of both the intention and process for the change, how will this change affect the operation of the systems onboard the ship, how will it affect the shoreside network, will it change the method information is communicated between ship and shore, what security risks will be resolved, will any new risks be created as a result of change, and so forth. The foregoing is not a complete list of what should be considered but provides examples of what should be considered when implementing the change.

6.1.3 *Ensure Full Enterprise Understanding of the Need for Change:*

6.1.3.1 It shall be emphasized that all personnel who will be affected by any changes to processes and procedures to implement cybersecurity procedures within the SMS should have a full understanding of why the change is necessary, what is their role in regard to the change, and how will it affect their work processes. This is as important for those ashore as it is for those onboard.

6.1.3.2 Without a full understanding of the need to implement cybersecurity procedures, human nature being what it is, personnel may not have full buy in, may consider the change one more thing that is being forced upon them against their will, may not fully implement or comply with the process, and will not take ownership of the process in relation to their assigned job.

6.1.3.3 As such, any planning for implementation of cybersecurity procedures into an SMS should include some type of familiarization and training. This should be scaled in relation to an individual's position, ashore and onboard, and their responsibility in regard to implementation and operation of the new procedures and processes. But all personnel affected should have some familiarization with the why of the implementation and how it will affect them and the importance of compliance.

6.1.4 *Reporting and Documenting the Management of Change Process:*

6.1.4.1 As the implementation of cybersecurity processes into an SMS are changes to the basic structure of the SMS and will affect the way the SMS is operated, complied with, and audited, the management of change process should be documented as evidence that the implementation of the cybersecurity procedures was investigated by the organization, the effect on the organization was examined, and the proper implementation process was determined.

6.1.4.2 In addition, as this is a change to the SMS, it should be reported during the management review process to ensure

that senior management is aware of the change and its effects on the organization. This will also be useful during the audit process as it will document that the organization has properly and appropriately managed the change to the SMS to ensure compliance by all levels of the organization.

6.2 *Cybersecurity Risk Assessment:*

6.2.1 *Introduction:*

6.2.1.1 The purpose of the cybersecurity risk assessment is to identify an organization's cyber posture. This will provide organizations with a comprehensive understanding of the probability of cybersecurity threat occurring and the impact on the organization in the event a specific threat occurs. The determination of risks will allow organizations to evaluate existing safeguards and make cost-effective decisions on the extent of applying controls to protect the organization effectively from cyber risks and threats malicious, unintended, internal, and external.

6.2.1.2 As the landscape of cyber threats is continuously evolving and numbers of cyberattacks are increasing rapidly across all industries, the IMO recognized the urgent need to raise awareness across the maritime industry by adopting Resolution MSC.428(98) supported with MSC-FAL.1/Circ.3 on guidelines on maritime cyber risk management.

6.2.2 *Preparation before Risk Assessment*—Initially, the cyber risk assessment process should be defined, including definition of assumptions and boundary of the systems to be protected. An example of the process is described in Fig. 1.

6.2.2.1 As a mandatory prerequisite, the organization shall determine its valuable assets to be protected. Typically, a list of critical data, intellectual property, hardware, and software technologies related to the people, processes, regulatory requirements, and responsibilities (asset and risk owners) of the organization are essential to define, in detail, as the initial activities to prepare for risk assessment. This should be documented to understand systemic risk on a vessel, related operations, processes, or combination thereof, that interact with the critical hardware and software technologies. There are tools or software than can be used for this preparation stage and the methodology should follow a common risk assessment process. Furthermore, the creation of an overall network or topology diagram describing interconnection of the systems and their connections into the public or third-party network is helpful. Fig. 1 clarifies system connectivity and how to identify cyber risks as well as visualize the effect of system segregation.

6.2.2.2 Risk can be understood as likelihood times consequence. A risk assessment should determine:

(1) What can go wrong,

(2) How likely is it, and

(3) What are the impacts.

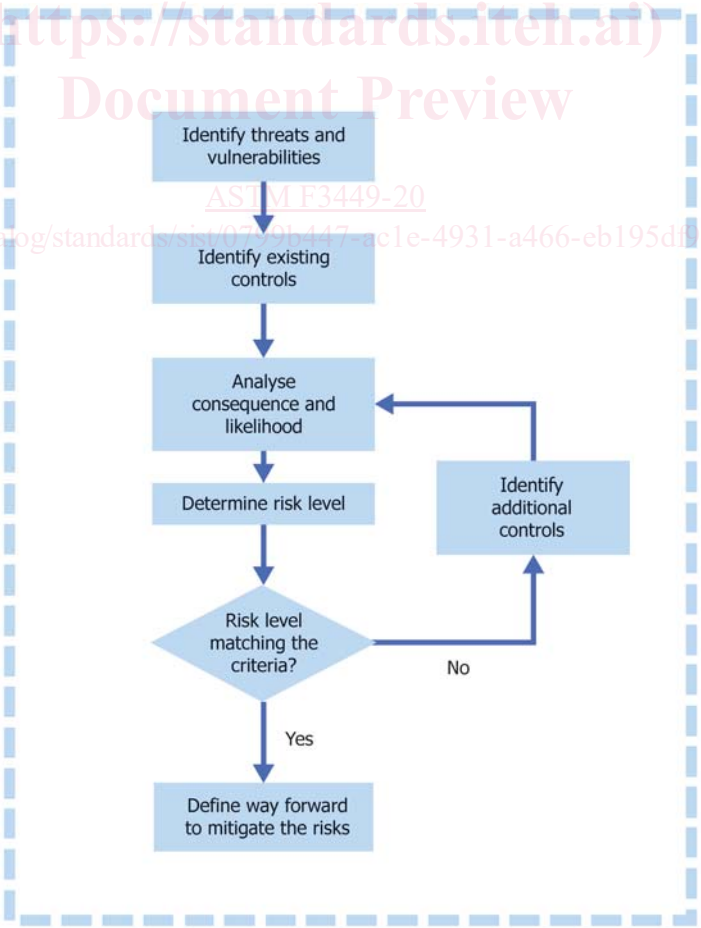

FIG. 1 Example of Cyber Risk Assessment Process

6.2.2.3 For the organization to determine current cyber risk and how to manage cyber risks on a long-term perspective, the organization should define consequence and likelihood rankings and assessment methodologies as well as risk acceptance criteria. These should include the following aspects:

(1) The consequence in terms of how people, environment, and property could be affected;

(2) The likelihood (probability) of an undesirable cybersecurity event; and

(3) The risk acceptance with definition of non-acceptable, as low as reasonably practicable (ALARP), and acceptable risks.

6.2.2.4 Furthermore, risk options (accepted, avoided, transferred, or mitigated) and process should be defined as per the decision of the organization.

6.2.2.5 Table 1 and Table 2 are examples of probability and impact tables that can be used to develop a risk matrix (Table 3).

6.2.3 *Risk Identification:*

6.2.3.1 Based on the inventory of identified assets, related threats and vulnerabilities should be identified. For this purpose, threats and vulnerabilities catalogues as listed in the BIMCO guidelines could be used. Other relevant reference resources include previous incidents and lessons learned, external reports and publications from recognized and trusted sources, and as well from identified IT and OT hardware and software descriptions and network diagrams.

6.2.3.2 Once the related threats and vulnerabilities are identified, the organization needs to analyze the current infrastructure, system setup, and software configuration to identify existing controls. These controls include three dimensions:

(1) People (for example, awareness training, responsibilities and tasks, and cyber incident drills),

(2) Processes (for example, cybersecurity policy and software configuration procedures), and

(3) Technologies (for example, firewalls, antivirus, encryption, and IDS).

6.2.4 *Risk Analysis:*

6.2.4.1 After risks have been identified, they need to be assessed with consequence and likelihood analysis. Assessment of consequences should evaluate the three main principles of the "CIA" model for information cybersecurity: confidentiality, integrity, and availability.

(1) Confidentiality—Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Tools to avoid unauthorized disclosure include encryption, access control, and physical security.

TABLE 1 Threat Occurrence Ranking
(What is the probability the threat will occur?)

Value	Probability
Very low	Remote (10 %)
Low	Unlikely (30 %)
Medium	Likely (50 %)
High	Highly likely (70 %)
Very high	Near certainty (90 %)

(2) Integrity—Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity. Tools to support data integrity include backups, archiving, and using data-correcting codes.

(3) Availability—Ensuring timely and reliable access to and use of information. Use physical protections and computational redundancies that can serve as backups in the case of failures.

6.2.4.2 The factors are assessed by means of relevant questions aiming at recording the worst possible scenarios. The likelihood analysis determines the occurrence of the possible events considering each of three factors: confidentiality, integrity, and availability. The methodology of this analysis should consider the identified threats, vulnerabilities, and foreseen safeguards. A valid approximation of this is to assess the "ease of access" to the systems. Combination of the likelihood with the consequence of a successful cyberattack will determine the level of the cybersecurity risk of the specific asset.

6.2.5 *Risk Evaluation*—At the end of the risk assessment, the organization shall decide on appropriate actions and the need for risk control measures. The response should be aligned with the criteria that were set at the beginning of the risk assessment. The organization should decide which risks could be accepted, avoided (for example by change of the process), or transferred (for example to a third party). Risks not covered by the initially foreseen controls need to be mitigated and, therefore, covered with risk treatment plans describing appropriate mitigation actions (see 6.3 for further information). Risk mitigation strategies and controls are discussed in 6.4. The NIST Special Publication 800-30[8] provides additional information on risk determination, contains representative threat events, and templates for developing risk tables.

6.3 *Development of Mitigation Strategies:*

6.3.1 *General Guidelines on the Development of Mitigation Strategies:*

6.3.1.1 With knowledge of the ship manager, ship operator, and ship's assets and systems that have critical roles or impacts on the ship and crew, the owner or operator can develop strategies to mitigate risks in a prioritized way.

6.3.1.2 The cyber-enabled systems onboard will be categorized for management and potential safety impacts based on the risk assessment and failure modes and effects analysis (FMEA) performed previously. The most important aspects of these systems include the asset management requirements, including software and hardware under positive control, and the anticipated impacts of any failures of these systems, especially in regard to safety of crew, systems, ship, or environment.

6.3.1.3 When organized into a cyber-enabled asset management system, the owner or operator will find it much easier to look across assets to prioritize efforts and resource use. Expected prioritization of risks only, however, can be performed with a simple risk management matrix as generated from the risk assessment.

6.3.2 *Determining the Need for Mitigation:*

[8] NIST Special Publication 800-30, *Guide for Conduction Risk Assessments–Information Security*, Special Publication 800-30 rev 1, September 2012, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.