MSC-FAL.1/Circ.3/Rev.3 通函

（2025年4月4日）

海事网络风险管理指南

1 便利委员会在其第41届会议（2017年4月4日至7日）和海上安全委员会在其第98届会议（2017年6月7日至16日）上，审议了增强网络风险威胁和安全隐患意识的迫切需求，批准了《海事网络风险管理指南》。

2 本指南提供关于海事网络风险管理的高级建议，以保护船舶免于当前和新出现的网络威胁和安全隐患的危害。本指南亦包括支持有效网络风险管理的功能要素。

3 海上安全委员会在其第104届会议（2021年10月4日至8日）和便利委员会在其第46届会议（2022年5月9日至13日）上，批准了对本指南第4.2段所列附加导则和标准的更新。

4 海上安全委员会在其第108届会议（2024年5月15日至24日）和便利委员会在其第49届会议（2025年3月10日至14日）上，批准了对《海事网络风险管理指南》的修订，载于本通函附件。

5 提请各成员国使所有相关利益方注意到本通函的内容。

6 本通函及其任何修订取代 MSC.1/Circ.1526 通函中包含的暂行指南。

附件

海事网络风险管理指南

1 引言

1.1 本指南为海事网络风险管理提供高级建议。就本指南而言，**海事网络风险**系指对**计算机系统（CBS）**在多大程度上受到潜在环境或事件威胁的一种量度；该环境或事件可能因信息或系统被篡改、丢失或遭到破坏，而导致与航运相关的操作、安全或保安故障。

1.2 利益相关方应采取必要措施，保护航运免于与航运进程和系统的数字化、整合与自动化相关的当前和新出现的威胁与安全隐患。

1.3 对于与特定风险管理进程的发展与实施相关的细节与指导，本指南使用者应参照特定成员国政府和船旗国主管机关的要求与导则，以及相关国际和行业标准与最佳操作方式。

1.4 风险管理对于安全和保安的航运操作至关重要。风险管理传统上主要聚焦实际领域的操作，但由于对数字化、整合、自动化和基于网络系统的依赖性不断增强，航运业对网络风险管理的需求日益增加。

1.5 本指南以支持安全和保安的航运为目标，使其在操作上可适应网络风险，并提供可纳入现有风险管理进程的建议。就此而言，本指南与本组织确立的安全与保安管理操作方式相互补充。

2 一般规定

2.1 关键定义

计算机系统（CBS）：指可编程电子设备，或为实现一个或多个特定目的（例如信息的收集、处理、维护、使用、共享、传播或处置）而组织形成的可互操作的可编程电子设备组合。船上CBS包括信息技术（IT）系统与操

作技术（OT）系统。CBS可由通过网络连接的若干子系统组成。船上CBS可直接或通过公共通信方式（例如互联网）与岸基CBS、他船CBS和/或其他设施相连接。

网络事件（Cyber incident）：指一次发生或一系列发生，实际或潜在地对CBS或其处理、存储或传输的信息造成不利后果，并可能需要采取响应行动以减轻后果。

网络风险管理：指识别、分析、评定并传达网络相关风险，并在考虑利益相关方所采取行动的成本与效益的基础上，将风险接受、终止、转移或减轻至可接受程度的过程。

信息技术（IT）：指以将数据用作信息为重点的CBS，包括软件、硬件与通信技术（例如商业信息，或关于船员的数据，如工资、证书等）。

操作技术（OT）：指以使用数据控制或监控实际过程为重点的CBS（例如主机润滑油温度水平并转发至控制室）。

2.2 背景

2.2.1 数字技术（包括CBS）已成为众多对航运安全与保安以及海洋环境保护至关重要的系统运行与管理所必需的技术。在某些情况下，这些系统用于满足国际标准与主管机关要求。然而，访问、互联或联网所带来的安全隐患可能导致需要处理的网络威胁与风险。相关系统可包括但不限于：

(1) 驾驶室系统（如航行系统、船舶安全系统、通信系统等）；

(2) 货物、加油、润滑、压载及其他泵送装卸与管理系统；

(3) 推进、燃油与机舱管理及动力控制系统；

(4) 保安、出入控制与监视系统；

(5) 乘客与船员服务及管理系统；

(6) 面向乘客、船员及分包服务人员的公共网络；

(7) 行政与船员福利系统；

(8) 船舶—港口接口；以及

(9) 船岸一体化系统（例如远程控制系统/海上自主水面船舶）。

2.2.2 在考虑CBS时，应区分信息技术（IT）与操作技术（OT）系统。此外，还应考虑在这些系统内进行数据交换、存储与使用过程中对信息的保护。OT系统中的安全隐患可能增加船舶操作安全风险，从而危及船员与乘客安全。因此，OT系统应与IT系统进行分段隔离，并与面向互联网的系统隔离，且配备适当的防护工具。

2.2.3 虽然这些技术与系统为海事行业带来显著效率提升，但也对航运关键系统的运行带来威胁与风险。一旦相关系统受到影响，将产生安全、保安与环境方面的影响。这些风险可能源于系统在安全性设计、运行、整合、维护或补丁更新方面的不足所引发的安全隐患，也可能源于有意或无意的行为。

2.2.4 网络风险既可能来自恶意行为（例如黑客入侵或引入恶意软件），也可能来自良性但疏忽行为的非预期后果（例如软件维护或用户权限配置不当）。一般而言，这些行为会暴露或利用CBS中的安全隐患（例如软件过期或防火墙无效）。有效的网络风险管理应同时评估与处理两类威胁。

2.2.5 安全隐患可起因于系统设计、整合和/或维护方面的不足，以及网络卫生（cyber hygiene）的疏忽。一般而言，当CBS中的安全隐患被暴露或被利用时，无论是直接（例如弱密码和/或不当的密码管理导致未授权访

问）还是间接（例如缺乏网络隔离），都可能影响数据的机密性、完整性与可用性，并可能影响船舶的安全与保安，尤其是在关键系统（例如驾驶室航行、主推进系统、货物装卸系统）遭到破坏的情况下。

2.2.6 有效的网络风险管理还应考虑第三方供应商、嵌入式系统，以及与航运所用系统软硬件供应链相关的网络威胁所带来的风险。亦应考虑CBS维护设备与系统。

2.2.7 技术与威胁快速变化，使得仅通过技术标准来处理这些风险变得困难。因此，本指南建议采用一种具有韧性、并作为现有安全与保安管理操作方式自然延伸的网络风险管理方法。

2.2.8 在考虑潜在威胁源、安全隐患及相关风险减轻策略时，应将若干网络风险管理控制选项纳入考虑，包括但不限于管理控制、操作或程序控制，以及技术控制。

2.3 应用

2.3.1 本指南主要面向船舶，旨在促进网络领域的安全与保安管理操作方式。

2.3.2 认识到航运业中没有两家符合《国际安全管理规则》（ISM）的公司是相同的，本指南以广义术语表述，以便广泛适用。数字系统有限的船舶可能只需简单应用本指南即可；然而，数字系统复杂的船舶可能需要更高程度的关注，并应通过信誉良好的行业与政府合作伙伴获取附加资源。

3 网络风险管理要素

3.1 就本指南而言，网络风险管理系指标识、分析、评定并传达网络相关风险，并在考虑利益相关方所采取行动的成本与效益基础上，将风险接受、终止、转移或减轻至可接受程度的过程。

3.2 海事网络风险管理的目标是支持安全与保安的航运，使其在操作上可适应网络威胁与风险。保护船舶及船舶—港口接口系统免于新出现威胁，应采取一系列持续演进的控制措施。因而，应在船舶设备与系统的设计、制造、整合、运行与维护各阶段纳入具备网络韧性的安全特性。

3.3 有效的网络风险管理应从高级管理层开始。高级管理层应接受相关培训，将网络风险意识文化贯穿于组织各级，并确保建立整体、灵活的网络风险管理制度，该制度应持续运行，并通过有效反馈机制不断评估。

3.4 为实现上述目标，一个公认的方法是全面评定并对比组织当前与期望的网络风险管理态势。该对比可揭示CBS中的网络安全差距，可通过基于风险的方法加以处理，以实现网络韧性目标。该基于风险的方法应结合船型与营运特征，以及船上系统的复杂性与连通性，对网络风险进行评估，从而使组织能够以最具成本效益与最高效率的方式配置资源。

3.5 本指南提出支持有效网络风险管理的功能要素。这些功能要素并非顺序性的，实践中应并行且持续开展，并应适当纳入风险管理框架。各功能要素下所列功能/技术性网络安全控制代表应实施的最低控制措施；根据已识别网络风险的评估，还可考虑附加控制措施。

(1) **治理（Govern）**：制定并监督风险管理战略、预期与政策。界定网络风险管理的人员角色与职责。确保业务连续性（如备份管理、灾难恢复）以及危机管理。

(a) 指定对网络安全活动的规划、资源配置与执行负有责任的人员或实体；

(b) 确保该指定人员或实体具备履职所需的授权与支持，并具有充足的网络风险管理知识与专门能力。

(2) **标识（Identify）**：确定船舶及船舶—港口接口的当前网络风险。 (a) 标识系统、资产、服务、数据与能力，以及安全关键系统之间的相互依赖关系（包括信息流）。当其受扰动时，会对船舶营运、人员安全、船舶安全和/或环境造成风险，包括与软硬件供应链相关者；

(b) 建立并维护船上数字系统清单。相关系统与资产可包括本指南第2.2.1段所列系统。标识内部与外部系统依赖关系及网络连接；

(c) 对对船舶营运至关重要、其突然失效可能导致危险情况的系统、服务、资产、数据与能力开展风险评定。标识网络相关威胁，标识安全隐患，并评估网络事件对相关要素的安全性、可用性、完整性与机密性的影响及发生可能性。

(3) **保护（Protect）**：实施风险控制过程与措施以保护CBS，并制定应急计划以防范网络事件并确保航运营运、人员安全、船舶安全和/或环境不受威胁的业务连续性。

(a) 为所有用户分配唯一凭证，区分普通账户与特权账户，收回安全设备并注销离职员工或用户账户；

(b) 更改所有设备默认密码，执行强密码策略，并考虑建立其他账户访问控制管理措施，以防范暴力破解、网络钓鱼等恶意尝试；在适当情况下采用多因素认证或持续认证解决方案，使用加固的语音、视频与文本通信，以及加固的应急通信系统；

(c) 限制互联网可被利用的服务，建立软硬件审批流程，收集并安全存储日志用于入侵检测与事件响应，并将OT设备网络与IT网络分段隔离；确保在网络与信息系统采购、开发与维护中的安全性，包括安全隐患处置与披露；

(d) 对任何可访问互联网或公司内联网、或与第三方/岸基网络与信息系统交互的船上数字系统与设备（尤其是船舶—港口接口相关者）实施安全措施（如防火墙或杀毒）；制定关于密码技术使用的政策与程序；

(e) 建立控制措施，防止系统被用于未经授权的可移动介质；

(f) 要求所有员工每年接受基础网络安全培训，OT用户接受OT专项网络安全培训；所有船员上船任职时应进行网络安全熟悉培训。培训应包含网络卫生、正在发生网络事件的识别与检测，以及响应与恢复等内容；并应不时通过演练与练习对网络安全知识进行测试；

(g) 定期进行系统备份与软件更新，并制定、维护网络事件响应（IR）计划；

(h) 对已识别为关键的系统与资产建立软硬件供应链安全政策；

(i) 建立政策与程序以评估网络风险管理措施的有效性（如审核），并定期审查与更新这些措施。

(4) **发现（Detect）**：制定、实施并演练及时发现网络事件所必需的活动；采取适当措施发现CBS上的非预期活动，并及时识别网络事件。

(a) 维护相关威胁、威胁行为体战术/技术/程序（TTP）的清单，并主动监视系统以发现相关威胁；

(b) 所有员工的年度基础网络安全培训应包括识别与检测正在发生网络事件的培训。

(5) **响应（Respond）**：制定、实施并演练活动与计划，以提供适应性并恢复因网络事件而受损的航运与船舶—港口操作或服务所必需的系统；采取适当措施将已发现网络事件对船舶系统其他部分的影响降至最低。

(a) 按主管机关规定的时限向必要方报告事件；

(b) 保存网络事件记录；

(c) 所有员工的年度基础网络安全培训应包括网络事件响应培训。

(6) **恢复（Recover）**：识别并实施措施，以恢复受网络事件影响的船上CBS（包括网络），以支持航运营运。

(a) 制定、维护并实施恢复与复原策略，以恢复可能受网络事件影响的关键业务或任务资产/系统；

(b) 所有员工的年度基础网络安全培训应包括网络事件恢复培训；

(c) 对网络事件开展根本原因分析，旨在解决深层问题与安全隐患，防止类似事件再次发生。

3.6 上述功能要素涵盖了影响海上营运与信息交换的关键系统中有效网络风险管理的活动与期望结果，并构成具有有效反馈机制的持续过程。为满足这些功能要素而形成的任何文件或文件部分，均应通过程序予以保护，以防止未经授权的访问、删除、销毁或篡改。

3.7 有效的网络风险管理应确保组织各级对网络风险具备适当程度的认识。该认识与准备程度应与网络风险管理体系中的角色与职责相适应。

3.8 应考虑实施具备网络韧性的设备与系统。作为技术措施的一部分，设备与系统应按国际标准与导则进行设计与测试，以保证船上网络韧性。

4 实施网络风险管理的标准与最佳操作方式

4.1 本指南所述的网络风险管理方法为更好理解与管理网络风险提供基础，从而使风险管理方法能够应对网络威胁与安全隐患。对于网络风险管理的具体导则，本指南使用者亦应参照主管机关要求，以及相关国际与行业标准与最佳操作方式。

4.2 附加标准可包括但不限于：

(1) ISO/IEC 27001 标准：信息技术—安全技术—信息安全管理系统—要求（由国际标准化组织ISO与国际电工委员会IEC联合发布）；

(2) IACS UR E26：国际船级社协会统一要求E26——船舶网络韧性；

(3) IACS UR E27：国际船级社协会统一要求E27——船上系统与设备的网络韧性。

4.3 附加导则与行业最佳操作方式可包括但不限于： (1) ICS、IUMI、BIMCO、OCIMF、INTERTANKO、INTERCARGO、InterManager、WSC与SYBAss制定并支持的《船上网络安全指南》；

(2) IACS关于网络韧性的综合建议（Rec.166）；

(3) 美国国家标准与技术研究院（NIST）《提高关键基础设施网络安全框架》（NIST 2.0框架）；

(4) 国际港口协会（IAPH）《港口与港口设施网络安全指南》。

4.4 使用任何导则或标准时，应参照其最新版本。

4.5 进一步参考资料可在IMO网站“Maritime cyber risk（海事网络风险）”栏目下获得，并鼓励IMO成员向IMO秘书处转送相关导则与标准的参考信息，以便纳入IMO公共网站。

注：上述附加导则与标准作为非穷尽性参考，供本指南使用者获取更为详尽的信息。所引用的导则与标准并非由本组织发布，其使用由本指南各使用者自行决定。