MSC-FAL.1/Circ.3/Rev.4 通函
（2026 年 5 月 28 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）上，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漏洞意识的迫切需求，批准了海上网络风险管理指南。

2　本指南提供关于海事网络风险管理的高层建议，以保护船舶免于当前和新出现的网络威胁和安全漏洞的危害。本指南也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）上，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 4.2 中的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）上，便利委员会在其第 49 届会议（2025 年 3 月 10 日至 14 日）上，批准了对本指南的修订。

5　 便利委员会在其第 50 届会议（2026 年 3 月 23 日至 27 日）上，海上安全委员会在其第 111 届会议（2026 年 5 月 13 日至 22 日）上，批准了对海事网络风险管理指南的进一步修订，其文本载于附件。

6　提请各成员国使所有相关利益方注意到本通函的内容。

7　本通函和任何修订取代 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层建议。就本指南而言，海事网络风险系指计算机系统受到潜在环境或事件威胁的一种量度，其可能引起信息或系统的损坏、丢失或泄露而造成航运相关的操作、安全和安保故障。

1.2 利益相关方应采取必要措施，保护航运免于当前和新出现的与航运进程和系统的数字化、集成化和自动化相关的威胁和安全漏洞。

1.3 如需获取与特定风险管理流程制定和实施相关的细节和指导，本指南的使用者应参照各成员国政府和船旗国主管机关的要求和导则，以及相关国际标准、行业标准和最佳实践。

1.4 风险管理是安全可靠航运操作的基础。传统的风险管理主要聚焦于实体领域的操作，但随着航运对数字化、集成化、自动化和基于网络系统的依赖性的增加，航运业对网络风险管理的需求日益增多。

1.5 基于支持安全可靠的航运目标，使其在操作上具备抵御网络风险的能力。本指南提供的建议可纳入现有风险管理流程。就这一点而言，本指南是对本组织建立的安全和安保管理实践的补充。

2 一般规定

2.1 关键定义

*计算机系统*系指一种可编程电子设备，或一组可互操作的可编程电子设备，为达到一个或多个特定目的而组织起来，如收集、处理、维护、使用、共享、传播或处置信息。船载计算机系统包括 IT 和 OT 系统。计算机系统可以是通过网络连接的子系统的组合。船载计算机系统可以直接或通过公共通信方式（如互联网）与岸上的计算机系统、其他船舶的计算机系统和/或其他设施进行连接。

*网络事件*系指发生或连续发生的事件，实际或可能会对计算机系统或其处理、存储或传输的信息造成不利后果，且可能需要采取响应措施来减轻后果。

*网络风险管理*系指识别、分析、评价和沟通网络相关风险的过程，并通过考虑利益相关方采取行动的成本和收益，将风险容忍、终止、转移或处理至可接受的程度。

*信息技术（IT）*系指侧重于使用数据作为信息的计算机系统，包括软件、硬件和通信技术（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）*系指侧重于使用数据来控制或监测物理过程（例如主发动机的油温水平，并将其转发到控制室）的计算机系统。

2.2 背景

2.2.1 对航运安全和海洋环境保护至关重要的许多系统的操作和管理而言，数字技术（包括计算机系统）已必不可少。在某些情况下，这些系统应符合国际标准和主管机关的要求。然而，访问、互相连接或网络连接这些系统产生的漏洞，进而引起的网络威胁和风险，应予以处理。相关系统包括但不限于：

.1 驾驶室系统（例如航行系统、船舶安全系统、通信系统等）；

.2 货物、燃油加注、润滑、压载和其他泵送处理和管理系统；

.3 推进、燃料和机械管理和动力控制系统；

.4 安全、访问控制和监控系统；

.5 乘客和船员服务和管理系统；

.6 乘客、船员和分包服务人员公共网络；

.7 行政和船员福利系统；

.8 船-港接口；和

.9 船-岸综合系统(例如远程控制系统/海上自主水面舰艇)。

2.2.2 当查看计算机系统时，信息技术（IT）和操作技术（OT）系统之间的差别应予以考虑。此外，还必须考虑在这些系统内的数据交换、存储和使用期间对信息的保护。OT 系统中的安全漏洞可能会增加船舶的操作安全风险，从而危及船员和乘客的安全。因此，应将 OT 系统与 IT 系统隔离，保护 OT 系统免受面向互联网的系统的影响，并拥有适当的保护工具。

2.2.3 虽然这些技术和系统使航运业效益大幅提升，其也对航运系统的运行构成威胁和风险，如果受到影响，将对安全、安保和环境产生影响。这些风险可能起因于系统或系统补丁的不当安全设计、操作、集成和维护以及有意或无意的行为引起的安全漏洞。

2.2.4 网络风险以恶意行为（例如，黑客入侵或引入恶意软件）或良性疏忽行为（例如，软件维护或用户权限）的非预期后果呈现。一般来说，这些行为会暴露或利用计算机系统中的安全漏洞（例如，软件过时或防火墙无效）。有效的网络风险管理应考虑评估和解决这两种威胁。

2.2.5 安全漏洞可起因于不足的系统设计、集成和/或维护以及网络卫生的疏忽。一般来说，如果计算机系统中的安全漏洞直接（例如，弱密码和/或粗心的密码管理导致未授权的访问）或间接（例如，无网络分段）地暴露或被利用，可能会影响数据的保密性、完整性和可用性，以及船舶的安全和安保，特别是涉及关键系统（例如驾驶室航行、主推进系统、货物装卸系统）时。

2.2.6 有效的网络风险管理也应考虑第三方供应商、嵌入式系统以及与航运中使用的系统的软硬件供应链相关的网络威胁所带来的风险。还应考虑到计算机系统的维护设备和系统。

2.2.7 这些快速变化的技术和威胁使只通过技术标准处理这些风险变得困难。因此，本指南推荐一种针对网络风险的风险管理方法，该方法具有韧性且不断演进，是现有安全和安保管理实践的自然延伸。

2.2.8 考虑潜在的威胁源、安全漏洞和相关风险减轻策略时，应虑及网络风险管理的潜在控制选项，包括管理、操作或程序以及技术控制。

2.3 应用

2.3.1 本指南主要适用于船舶，鼓励船舶在网络领域的安全和安保管理实践。

2.3.2 认识到航运业中没有两个 ISM 公司是一样的，本指南以广义的术语进行表述以广泛应用。对于数字系统有限的船舶，简单应用本指南已足够；然而，具有复杂数字系统的船舶可能会要求更大程度的关注，并应通过声誉良好的行业和政府合作伙伴寻找附加资源。

3 网络风险管理要素

3.1 就本指南而言，网络风险管理的定义见 2.1。

3.2 海事网络风险管理的目标是支持安全航运，其在操作上可适应网络威胁和风险。保护船舶和船舶-港口接口系统免受新出现的威胁应涉及一系列升级的控制措施。因此，在设计、制造、集成、运行和维护阶段，应将网络韧性安全特征纳入船舶设备和系统。

3.3 有效的网络风险管理应从高级管理层开始。高级管理应接受相关的培训，将网络风险意识文化深入各级组织，并确保整体灵活的网络风险管理制度，其连续操作并通过有效的反馈机制不断评估。

3.4 实现上述目标的一个可接受的方法是对组织当前和预期的网络风险管理态势进行全面评估和对比。这种对比可以揭示出计算机系统中的网络安全差距，并通过基于风险的方法填补这些差距，以实现网络韧性目标。该基于风险的方法应评估网络风险，虑及船舶类型和营

运概况以及船上系统的复杂性和连通性，以使一个组织能以最具成本效益和效率的方式最好地应用其资源。

3.5 本指南提出支持有效网络风险管理的功能要素。这些功能要素不是有顺序的—所有这些要素在实际中应同时发生并连续，并应适当纳入风险管理框架。每个功能要素下列出的功能/技术网络安全控制代表应实施的最小控制。根据对已识别的网络风险的评估，可考虑采取额外的网络安全控制。

.1 管理：建立和监控风险管理策略、期望和政策。明确网络风险管理人员的角色和职责。确保业务连续性，例如备份管理、灾难恢复和危机管理。

.1 指定一个人或实体负责网络安全活动的规划、资源配置和执行；

.2 确保被指定的个人或实体获得必要的授权和支持以履行其职责，并确保其在网络风险管理方面拥有足够的知识和专业技能。

.2 识别：确定当前船舶和船舶/港口接口的网络风险。

.1 识别一旦中断会对船舶营运、人员安全、船舶安全构成风险和/或环境构成威胁的系统、资产、服务、数据、能力以及安全关键系统（包括信息流）之间的相互依赖关系，包括与软件和硬件供应链相关者；

.2 建立和维护船上的数字系统清单。这些系统和资产可包括本指南第 2.2.1 段所列的系统。识别内部和外部系统的依赖关系和网络连接；

.3 对船舶营运至关重要的系统、服务、资产、数据和能力进行风险评估，其突发性操作故障可能导致危险情况。识别网络相关威胁。识别系统、服务、资产、数据和功能的安全漏洞。评估网络事件对这些要素的安全性、可用性、完整性和保密性的可能性和影响。

.3 保护：实施保护计算机系统的风险控制过程和措施以及应急计划，以抵御网络事件并确保航运业务连续性、人员安全、船舶安全和/或防止对环境造成威胁。

.1 为所有用户分配唯一的凭据，将用户和特权帐户分开，收集安全设备，并停用离职员工或用户的帐户；

.2 更改所有设备的默认密码，实施强密码政策，并考虑建立其他用户帐户访问控制管理措施以防范暴力破解攻击、网络钓鱼等恶意企图。在适当的情况下，使用多因素认证或连续认证的解决方案，安全语音、视频和文本通信以及安全的紧急通信系统；

.3 限制互联网上可利用的服务，建立硬件和软件审批流程，收集并安全存储用于入侵检测和事件响应的日志，并将 OT 设备网络与 IT 网络分段分割开来。确保网络和信息系统的获取、开发和维护的安全，包括漏洞处理和披露；

.4 为任何可访问互联网或公司内网、或与第三方及岸上网络和信息系统（尤其是船舶 / 港口接口）交互的船舶数字系统和设备实施安全措施（如防火墙或防病毒软件）。落实与密码学应用相关的政策和程序；

.5 建立控制措施，防止系统使用未经授权的可移动介质；

.6 要求对所有员工进行年度基本网络安全培训，对 OT 用户进行 OT 特定的网络安全培训，并要求所有船员在船上工作时熟悉网络安全。针对所有员工和 OT 用户的培训应包括网络卫生、正在发生的网络事件的识别和检测以及响应和恢复等内容。网络安全知识应不定期进行测试，例如通过演练和演习；

.7 执行定期的系统备份和软件更新，并制定和维护事件响应（IR）计划；

.8 为那些已确定为关键的系统和资产建立软件和硬件供应链安全政策；

.9 建立政策和程序来评估网络风险管理措施（例如审计）的有效性，并定期审查和更新这些措施。

.4 发现：制定、实施和实践及时发现网络事件所必需的各项行动。实施适当的措施来发现计算机系统上的意外活动，并确保及时识别网络事件。

.1 维护相关威胁、威胁行为者策略、技术和程序的清单，并积极监控系统以防范那些威胁；

.2 所有员工的年度基本网络安全培训应包括识别和检测正在发生的网络事件的培训。

.5 响应：制定、实施和实践行动和计划以提供韧性，并恢复由于网络事件而受损的船舶和船-港营运或服务所必需的系统。实施适当的措施，尽量减少检测到的网络事件对船舶系统其他部分的影响。

.1 在主管机关规定的时限内向有关方面报告事件；

.2 应保存网络事件的记录；

.3 所有员工的年度基本网络安全培训应包括应对网络事件的培训。

.6 恢复：确定和实施恢复船载计算机系统（包括受到网络事件影响的航运操作必需的网络系统）的措施。

.1 制定、维护和实施恢复可能受到网络事件影响的重要业务或关键任务资产或系统的策略；

.2 所有员工的年度基本网络安全培训应包括从网络事件中恢复的培训；

.3 对网络事件进行根本原因分析，以解决潜在问题和安全漏洞，防止类似事件再次发生。

3.6 这些功能要素包含涉及影响海上营运和信息交换的各关键系统的有效风险管理的各项行动和期望结果，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制定的任何文件或文件章节都应通过旨在防止未经授权的访问、删除、销毁或修正的程序加以保护。

3.7 有效网络风险管理应确保组织的各级具有适当水平的网络风险意识。意识程度和准备状态应适于网络风险管理系统中的角色和职责。

3.8 应考虑网络韧性设备和系统的实施。作为技术措施的一部分，应按照国际标准和导则设计和测试设备和系统，以确保船舶的网络韧性。

4 实施网络风险管理的标准和最佳实践

4.1 所述的网络风险管理方式为更好理解和管理网络风险提供基础，从而使风险管理方式能解决网络威胁和安全漏洞。对于网络风险管理的具体导则，本指南的使用者也应参见主管机关的要求，以及相关国际和行业标准以及最佳实践。[1]

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。国际标准组织（ISO）和国际电工委员会（IEC）共同发布；

.2 IACS UR E26 -国际船级社协会统一要求 E26 -船舶的网络韧性；

.3 IACS UR E27 -国际船级社协会统一要求 E27 -船上系统和设备的网络韧性。

4.3 附加指南和行业最佳实践可包括但不限于：

.1 ICS、IUMI、BIMCO、OCIMF、INTERTANKO、INTERCARGO、InterManager、WSC 和 SYBAss 制定和支持的船舶网络安全指南；

.2 IACS 关于网络韧性的综合建议案（Rec 166）；

.3 美国提高关键基础设施网络安全的国家标准和技术框架研究院（NIST2.0 框架）；

.4 IAPH 港口和港口设施网络安全指南；

[1] 附加导则和标准列为本指南使用者获得更详细信息的非全面参照。参考的导则和标准未经本组织发布，其使用仍由本指南的个人用户决定。

.5 IAPH 海事供应链新兴技术网络韧性指南。

4.4 应参见使用的任何导则或标准的最新版本。

4.5 更多参考资料可在 IMO 网站“海事网络风险”下找到，并鼓励 IMO 成员国向 IMO 秘书处提交相关导则和标准的参考资料，以便纳入 IMO 公共网站。